DISSERTATIONES
INFORMATICAE
UNIVERSITATIS
TARTUENSIS
64

MARIIA BAKHTINA

A Method for Information Security and Privacy Management in Smart Solutions

DISSERTATIONES INFORMATICAE UNIVERSITATIS TARTUENSIS
64

MARIIA BAKHTINA

A Method for Information Security and Privacy Management in Smart Solutions

UNIVERSITY OF TARTU
Press
1632

Institute of Computer Science, Faculty of Science and Technology, University of Tartu, Estonia.

Dissertation has been accepted for the commencement of the degree of Doctor of Philosophy (PhD) in Computer Science on April 1, 2025 by the Council of the Institute of Computer Science, University of Tartu.

Supervisor

Prof. Dr.	Raimundas Matulevičius University of Tartu, Estonia

Opponents

Prof. Dr.	Siv Hilde Houmb Norwegian University of Science and Technology (NTNU), Norway
Prof. Dr.	Manfred A. Jeusfeld University of Skövde, Sweden

The public defense will take place on May 5, 2025 at 12:15 in Narva Rd. 18-1020.

The publication of this dissertation was financed by the Institute of Computer Science, University of Tartu.

ISSN 2613-5906 (print) ISSN 2806-2345 (pdf)
ISBN 978-9916-27-860-4 (print) ISBN 978-9916-27-861-1 (pdf)

University of Tartu Press
`http://www.tyk.ee/`

“Imagine all the people
Livin’ life in peace”
by John Lennon

ABSTRACT

The increasing interconnectedness of systems, facilitated by the convergence of global megatrends like hyperconnectivity and the demand for super platforms, elevates the development of smart solutions based on the system of systems. Although these smart solutions enable cross-organisational collaboration and data-driven decision-making, they also introduce new attack vectors and significant security and privacy challenges. Traditional information security management approaches often struggle to effectively support multidisciplinary expert groups in navigating the complexities of collaborative, dynamic environments, such as those found in smart solutions.

To bridge this gap, first, this thesis proposes a FISP-ProCOP framework. FISP-ProCOP (Framework for Information Security and Privacy Management – Processes, Countermeasures, Organisation, and People) provides a structured approach to assessing the current state of security and privacy management within organisations. It considers four crucial dimensions: processes, countermeasures, organisation, and people. By analysing these dimensions, organisations can identify gaps and potential threats to their security and privacy posture.

Second, this thesis presents a tool-supported privacy analysis method. This method leverages open-source DPO and Pleak tools to identify privacy violations in collaborative business processes and recommends a way to assess suitable privacy-enhancing technologies. By integrating privacy analysis into business processes, organisations can enhance compliance with data protection regulations, such as GDPR, and mitigate privacy risks.

Third, this thesis proposes two alternative designs based on different trust models (decentralised and distributed) for smart systems enabled by the X-Road data exchange system. Supported by the proof-of-concept implementations and designs' assessment, organisations can make informed decisions about their identity management strategies considering such factors as security, control, usability, and maintainability.

This thesis includes six studies in the context of intelligent transportation systems to evaluate the proposed framework's and methods' usability. These studies demonstrates the applicability and effectiveness of the proposed methods in scenarios of intelligent transportation systems. Finally, FISP-ProCOP, the privacy analysis method, and the method for evaluating identity management systems are combined into the method for information security and privacy management in smart solutions.

Thus, this thesis contributes to information security and privacy management by helping data protection officers, information security officers, business analysts, and security architects coordinate their security and privacy assurance efforts. By addressing the challenges posed by the increasing interconnectivity of systems, this research empowers organisations to enhance their security posture and protect sensitive data.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AV Autonomous Vehicle 80–82, 84, 90

BPMN Business Process Model and Notation 42, 104

CA Certification Authority 45, 98, 102–105, 108, 110, 111, 114, 116, 118, 131, 132
CIA Confidentiality Integrity Availability 33, 35
CISO Chief Information Security Officer 18, 59, 76, 78, 86
CS Central Server 98, 116
CSP Credential Service Provider 45

DID Decentralized Identifier 46, 48, 111–116, 118
DKG Distributed Key Generation 51–53
DKMS Distributed Key Management System 124, 131, 132
DLT Distributed Ledger Technology 48
DPKI Decentralised Public Key Infrastructure 102, 103, 111–114, 135, 136, 140
DPO Data Protection Officer 18, 40, 58
DSR Design Science Research 22, 23

GDPR General Data Protection Regulation 20, 37, 39, 55, 73, 95

HSM Hardware Security Module 52, 53, 105, 126

ICT Information and Communication Technology 17, 20, 37
IdM Identity Management 11, 29, 43, 49, 53, 98, 99, 103, 105, 108, 110–112, 117–121, 123, 124, 131–136, 140, 141, 143
IS Information System 29, 37, 40, 97, 99, 110, 120, 122, 124, 125, 127, 130, 134
ITS Intelligent Transportation System 54, 55, 60, 61, 65, 68, 72

MPC Multi-Party Computation 83, 89

NIST National Institute of Standards and Technology 19, 32, 34
NIST SP NIST Special Publications 37, 43

OCSP Online Certificate Status Protocol 105, 110–112
ODI Organisational Digital Identity 47, 102, 122, 124, 134

PE-BPMN Privacy-Enhancing Business Process Model and Notation 39, 42, 77–79, 87, 94
PET Privacy-Enhancing Technology 38, 39, 42, 43
PKI Public Key Infrastructure 49, 50, 96, 103, 108, 124, 129
PLT Parking Lot Terminal 87–89, 128
PoC Proof of Concept 103, 115–117, 119, 129, 132, 135
PSP Parking Service Provider 87, 88, 128

RoT Root of Trust 45, 46, 108, 114

SoS System of Systems 17, 19, 38, 93
SS Security Server 104, 116, 127, 130
SSI Self-Sovereign Identity 46, 102, 111, 112, 114, 116–119, 133

VC Verifiable Credential 47, 48, 105, 112–119
VDR Verifiable Data Registry 48, 111–114, 116, 117, 119
VP Verifiable Presentation 48, 114, 117

ZT Zero Trust 49, 120

LIST OF ORIGINAL PUBLICATIONS

Publications included in the thesis

I **Mariia Bakhtina**, Raimundas Matulevičius, and Lukaš Malina. "Information Security and Privacy Management in Intelligent Transportation Systems". In: *Complex Systems Informatics and Modeling Quarterly* 38 (2024), pp. 100–131. DOI: 10.7250/csimq.2024-38.04
Author contribution: Lead author - substantially contributed to the study design, evaluation, and writing.

II **Mariia Bakhtina**, Raimundas Matulevičius, and Mari Seeba. "Tool-supported method for privacy analysis of a business process model". In: *Journal of Information Security and Applications* 76 (2023), p. 103525. DOI:10.1016/j.jisa.2023.103525.
Author contribution: Co-Lead author - substantially contributed to the study execution, evaluation, and writing.

III **Mariia Bakhtina**, Raimundas Matulevičius, Ahmed Awad, and Petteri Kivimäki. "On the Shift to Decentralised Identity Management in Distributed Data Exchange Systems". In: *Proceedings of the 38th ACM/ SIGAPP Symposium on Applied Computing.* Tallinn, Estonia: Association for Computing Machinery, 2023, pp. 864–873. DOI:10.1145/3555776.3577678.
Author contribution: Lead author - substantially contributed to the study design, evaluation, and writing.

IV **Mariia Bakhtina**, Kin Long Leung, Raimundas Matulevičius, Ahmed Awad, and Petr Švenda. "A Decentralised Public Key Infrastructure for X-Road". In: *Proceedings of the 18th International Conference on Availability, Reliability and Security*. Benevento, Italy: Association for Computing Machinery, 2023. DOI: 10.1145/3600160.3605092.
Author contribution: Lead author - substantially contributed to the study design, evaluation, and writing.

V **Mariia Bakhtina**, Jan Kvapil, Petr Švenda, and Raimundas Matulevičius. "The Power of Many: Securing Organisational Identity Through Distributed Key Management". In: *Advanced Information Systems Engineering*. Ed. by Giancarlo Guizzardi et al. Cham: Springer Nature Switzerland, 2024, pp. 475–491. DOI: 10.1007/978-3-031-61057-8_28.
Author contribution: Co-Lead author - substantially contributed to the study design, visualisation, resources search and analysis, and writing.

Publications not included in the thesis

VI **Mariia Bakhtina**, Zuzana Vémolová, and Vashek Matyás. "CHESS: Cybersecurity Excellence Hub in Estonia and South Moravia". In: *Proceedings of the Research Projects Exhibition Papers at the 36th International Conference on Advanced Information Systems Engineering*. 2024, pp. 10–17. *CEUR Workshop Proceedings.* https://ceur-ws.org/Vol-3692/paper2.pdf

VII **Mariia Bakhtina**. "Towards More Secure and Data Protective Intelligent Infrastructure Systems". In: *Proceedings of the Doctoral Consortium Papers Presented at the 35th International Conference on Advanced Information Systems Engineering*. Zaragoza, Spain, 2023, pp. 35–44 *CEUR Workshop Proceedings.* https://ceur-ws.org/Vol-3407/paper5.pdf

VIII Raimundas Matulevičius, Mubashar Iqbal, Emna Ammar Elhadjamor, Sonia Ayachi Ghannouchi, **Mariia Bakhtina**, and Slaheddine Ghannouchi. "Ontological representation of healthcare application security using blockchain technology". In: *Informatica* 33.2 (2022), pp. 365–397. DOI:10.15388/22-INFOR486.

IX **Mariia Bakhtina** and Raimundas Matulevičius. "Information Security Risks Analysis and Assessment in the Passenger-Autonomous Vehicle Interaction." In: *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 13.1 (2022), pp. 87–111. DOI: 10.22667/JOWUA.2022.03.31.087.

X **Mariia Bakhtina** and Raimundas Matulevičius. "Information Security Analysis in the Passenger-Autonomous Vehicle Interaction". In: *Proceedings of the 16th International Conference on Availability, Reliability and Security*. Vienna, Austria: Association for Computing Machinery, 2021. DOI:10.1145/3465481.3470045.

1. INTRODUCTION

Nowadays, we see the global megatrends of hyperconnectivity [1, 2] and super platforms which are driven by the rise of Gen Z's demand for all-in-one solutions per domain for seamless customer-centric experience [3]. The convergence of these megatrends elevates the development of *System of Systems (SoS)*. A SoS, in its classical definition, comprises multiple independently developed systems that collaborate synergistically towards a shared objective [4]. Meanwhile, *hyperconnectivity* encompasses the interconnectedness of digital entities, including systems, devices, objects, processes, activities, people, and data [5].

As a result, SoS implementations enable hyperconnectivity in various domains, ranging from consumer-oriented IoT devices for everyday usage to industrial-scale Industry 4.0 and domain-specific smart system solutions. These smart solutions, spanning sectors like government, transportation, and healthcare, enable cross-organisational collaboration through information systems' interactions [6]. Such heterogeneous system interconnections foster new data flows, empowering data-driven decision-making and new data-based features. However, they also introduce novel attack vectors and pose significant security and privacy challenges [7, 8] due to the non-compositional nature of SoS. Thus, the security of each component in the smart system does not refer to the security of the whole composed system.

As much as each separate system managed by an organisation should have its security and privacy objectives, additional information security and privacy management measures of the smart system as a whole must be in place. Traditionally, information security management has focused on stand-alone information systems. However, the growing concern over Information and communication technology (ICT) supply chain security [9, 10] necessitates the development of information security management methods tailored to the dynamic and complex nature of smart solutions. As real-world hyperconnected systems continue to emerge and evolve, ongoing research and development are crucial to address the associated security and privacy challenges.

Moreover, the need for security and security control to address specific security vulnerabilities has been the most frequent goal of the research; most of the results on smart systems are not easily reusable due to their limited scope. The design of new approaches would benefit from security studies focusing on replicable processes for information security assurance of smart systems [11]. Additionally, research on privacy and trust still has room for development along with the development of strategic security approaches that would be applicable to any smart systems as SoS [11].

The advancements in cryptography and post-quantum cryptography (including threshold cryptography [12, 13, 14]) boost the development and improvements of privacy-enhancing technologies. For example, Zero-Knowledge Proofs (ZKP) [15, 16, 17, 18], homomorphic encryption [19, 20, 21] and secure multi-

party computation [22, 23, 24] allow usable privacy and give rise of new identity and trust models. Despite the existing knowledge base, to the best of our knowledge, the guidelines for selecting information security and privacy protection measures tailored to collaborative smart solutions with a strong emphasis on privacy and inter-entity trust remain deficient. As a result, we see the need for a method to support information security and business development teams. This method should anticipate required changes to the organisation's information security management system and formulate new plans [25] in case the organisation transforms its information system towards a system that enables a collaborative smart solution.

Suppose we consider the transportation sector as an example of an industry where a smart solution are being established, such as systems for smart parking, ride-hailing, and traffic management. Our background study in [26] shows that, on average, each such system operates with the data of 2-3 external stakeholders. Based on our literature review results [26], the companies participating in such smart transportation solutions are using several security and privacy measures and mostly follow the standard ISO/IEC 27001 (information security, cybersecurity and privacy protection) [27]. However, they are still challenged by the need to preserve the security and privacy of users' data and the lack of industry regulations for information security assurance.

1.1. Motivation Scenario

Let us consider a multidisciplinary expert group from a selected organisation. The group aims to update the business processes and system to enable a collaborative data exchange with external entities as a part of a smart solution (e.g., smart parking). The expert group consists of people from the following (or analogous) roles: a data protection officer (DPO), a chief information security officer (CISO), a business analyst, and a security architect. The tasks of the expert group are (**T1**) to define a set of changes to the processes and the system, (**T2**) to define an acceptable data-sharing policy (what can be shared with whom and what not), (**T3**) to assure meeting of business requirements by the updated processes and the system. The group uses the current business process models and documentation on system components as input.

Such a group could take commonly used data protection standard along with frameworks of business analysis, business process management, and security risk management so that each expert applies the framework separately from their own field of expertise. However, none of these tools give instructions on how to combine their separate results. In the case of a shift to a smart system, such an expert

group is formed in each organisation involved in delivering a smart solution[1].

Each organisation that plans to contribute to providing smart solution changes their processes in parallel, assuming the static picture of partners with whom the integration is planned. In this work, we aim to assist multidisciplinary expert groups in fulfilling key tasks outlined in the European cybersecurity skills framework [25]. Specifically, we focus on supporting the assessment of an organisation's cybersecurity posture as it transitions its information systems towards cross-organisational smart solution provision by consolidating multiple stand-alone systems. The goal is to equip expert groups with a method for analysing necessary changes, defining security requirements and goals, and ensuring their alignment with organisational objectives.

1.2. Problem Statement & Research Objectives

Considering the motivation scenario, in the following section, we identify problems of interest to this thesis and specify the respective research objectives.

Framework for Information Security and Privacy Management. To understand how organisations handle information security and privacy, we should remember that information security is a multidisciplinary domain. To define how organisations handle it, we should consider multiple aspects of the organisations involved in information security and privacy management. Models and frameworks offer an abstract representation of concepts and their interrelationships within a specific domain, facilitating a shared understanding. Hence, the respective models and frameworks are supposed to guide one in understanding information security and privacy. There are numerous of those [28, 29, 30, 31], and they differ by the level of detail and the purpose. Additionally, there are also broader cybersecurity frameworks[2] reviewed in [34] that help policymakers (like governments or company executives) create cybersecurity strategies and policies which, however, are not limited to information security (e.g., NIST Framework for Improving Critical Infrastructure Cybersecurity [35]).

Although these models complement one another and are useful for summarising domain knowledge on information security management, they are too general to be used as a theoretical model for data extraction in the case of organisational

[1] If not specified otherwise, the term *"a smart system"* is used to refer to any *system of systems (SoS)*, *an intelligent infrastructure system*, cyber-physical system or any other system composed of multiple stand-alone integrated information systems that allow delivering a smart solution to the system end users thanks to a collaboration between systems and organisations.

[2] *Cybersecurity* refers to "safeguarding of people, society, organisations and nations from cyber risks" [32]. Meanwhile, *information security* refers to "preservation of confidentiality, integrity and availability of information" [33]. Thereby, overlapping in some methods and used countermeasures, the two fields differ in their goals. Cybersecurity focuses on preventing, detecting, and responding to cyber threats to any IT system assets (e.g., services, servers, data, protocols). Meanwhile, information security focuses on protecting all types of information, regardless of whether it is stored electronically or physically.

analysis in the motivation scenario. Therefore, we formulate the first research objective as follows:

- **Research Objective 1**: to develop a framework for information security and privacy management. The framework should support organisations in defining the static current state of information security and privacy management in the context of smart systems.

Personal Data Protection. Each organisation is responsible for assuring the privacy of its system users' personal data, which is tightly intertwined with information security management. The international standard ISO/IEC 27001:2022 (Information security, cybersecurity and privacy protection — Information security management systems — Requirements) [27] prescribes in controls 5.14, 5.19, and 5.21 to manage information security risks related to information transfers between the organisation and third parties (including the ICT supply chain) and assure preservation of privacy and protection of personal data according to applicable laws and regulations. Thus, each organisation should comply with the local data (privacy) protection regulation, e.g., the General Data Protection Regulation (GDPR) in the European Union (EU).

Despite the passage of time since GDPR implementation, the abstract nature of its requirements [36, 37], coupled with a lack of clarity regarding mandates, roles, and responsibilities [38, 37] and lack of standardised procedure for implementation continues to pose challenges, especially for small and medium enterprises (SMEs) which are more sensitive to large temporal and monetary efforts [39]. Further compounded by the skills gap among privacy professionals and the difficulty in assessing the efficacy of privacy technologies [39, 37, 40], these obstacles persist. Although outsourcing data processing is a common practice [39, 40], organisations must remain cautious to mitigate the risks of data leakages. While non-compliance with GDPR requirements may result in penalties, according to the GDPR Enforcement Tracker [41], 42 and 19 fines were issued monthly on average during 2023 and 2024, respectively. The Tracker indicates that a substantial number of violations arise from breaches of core data processing principles, and a deficiency in implementing adequate technical and organisational measures to protect data [41].

Numerous works describe methodologies for assessing information systems and their privacy policy compliance [42, 43, 44, 45, 46, 47, 48]. However, these approaches often fall short of practical application in real-world scenarios. For example, [42, 43] primarily focus on textual analysis of the privacy policy (not the actual data processing flow) or the law itself for eliciting or checking the GDPR-related requirements. Meanwhile, [44, 48] are fully theoretical and lack the implementation of the mandatory supporting tools. Alternatively, some approaches, such as in [43], address compliance in requirements engineering but fall short in providing support for privacy management activities or the implementation of privacy technologies.

Furthermore, the tools and approaches in [44, 46, 47, 48] are closed-access or require significant expertise to use, making them impractical for smaller organisations. Consequently, to the best of our knowledge, there are no commonly used procedures supported with openly accessible tools to guide privacy analysis and assurance for the organisations.

- **Research Objective 2**: to develop a method for privacy analysis of collaborative business processes. The method should support the expert group members in fulfilling local data protection regulations (i.e., GDPR for the EU) and assessing the effect of security measures on personal data protection to prevent insider access and data leakage.

Identity Management and Trust Assumptions. Both organisations and their systems rely on some trusted parties to coordinate the exchange and identity issuance and verification for securing the exchanged data in a smart system. The root of trust and trust model are the key assumptions of further collaboration between organisations and their systems. Traditionally, the trust model selection concerns only external entities, assuming full trust to the entities inside the organisation (including the organisation's employees) and inside the trusted network of the collaborating organisation. However, the increasing prevalence of insider threats (e.g., through privilege abuse), coupled with the exponential growth of data exchange and technological advancements, compels organisations to safeguard sensitive information from unauthorised access and manipulation. This necessitates ensuring the integrity of exchanged data and verifying the legitimacy of data exchange requests. As a result, the traditional centralised trust model, which is prone to a single point of failure, is being questioned [49, 50, 51, 52], and alternative trust models are being proposed. Still, while the research community is advocating the advantages of the shift towards decentralised or hybrid trust models, they do not provide guidelines on how to assess the changes in system quality enabled by the transition, how it will influence business operations or how to plan such a transition in the first place. In our research, we focus on organisational identities used in smart systems for securing cross-organisational data exchange leaving out of scope the personal identification. Thus, the last research objective of this thesis is the following:

- **Research Objective 3**: to develop a tool for trust model selection for smart systems' identity management system. The supporting tool should help organisations define the rules under which organisations exchange their data within a smart system and support the implementation of non-centralised identity management in smart systems. As a result, the tool should enable the making of informed decisions on trust model selection to protect organisational and personal data from unauthorised access.

To address the identified problem statements and reach the research objectives, in this work, we aim to answer the following main research question:

MRQ: *How to support an expert group in assessing the effect of cross-organisational collaboration on information security and privacy of the smart solution?*

1.3. Research Approach

The object under research presented in the thesis are information systems that are set up in a way that allows organisations to collaborate through continuous cross-organisational data exchange to enable a smart solution for end users.

1.3.1. Design Science Research

To answer the **MRQ** and reach the stated research objectives, we follow the *design science research (DSR) method* for information systems research proposed by Hevner et al. [53]. DSR is an approach based on a set of principles and an iterative process consisting of design cycles for defining the problem, designing a solution (i.e., artefact), and evaluating and refining the artefact. Thereby, DSR is based on the process of the continuous development and evaluation of artefacts in the field of information systems, which aims to solve real-world problems. Using DSR allows us to solve the identified problem of securing information systems and support the expert group in the motivation scenario by continuously developing artefacts based on the existing knowledge base of methods, theories, experiences and other artefacts.

The DSR cycle includes six steps [54]: (*i*) identify the problem and motivation; (*ii*) define the objective of a solution; (*iii*) design and develop the artefacts; (*iv*) demonstrate the designed artefacts in a suitable context; (*v*) evaluate; and (*vi*) communicate the artefacts. Figure 1 depicts key components of DSR and its implementation in this thesis. In this thesis, the problems are identified based on the background study and the motivation scenario. The results of each design cycle's evaluation contribute to the clarification of the research problem and the research objective of the next cycle.

While DSR is based on using the existing knowledge base for solving the real-life problem [53], we use the *literature review* and *background study* as the main sources for the developed artefacts. Thus, a literature review helps to establish a theoretical foundation for the research and provides evidence to support design decisions and justify the chosen approaches.

The research process starts by reviewing the academic and industry publications on the information security challenges in e-governance, e-health, and intelligent transportation to identify the problems. Then, for each problem, the additional literature review and background study of the problem cases, existing solutions and evaluation criteria is done.

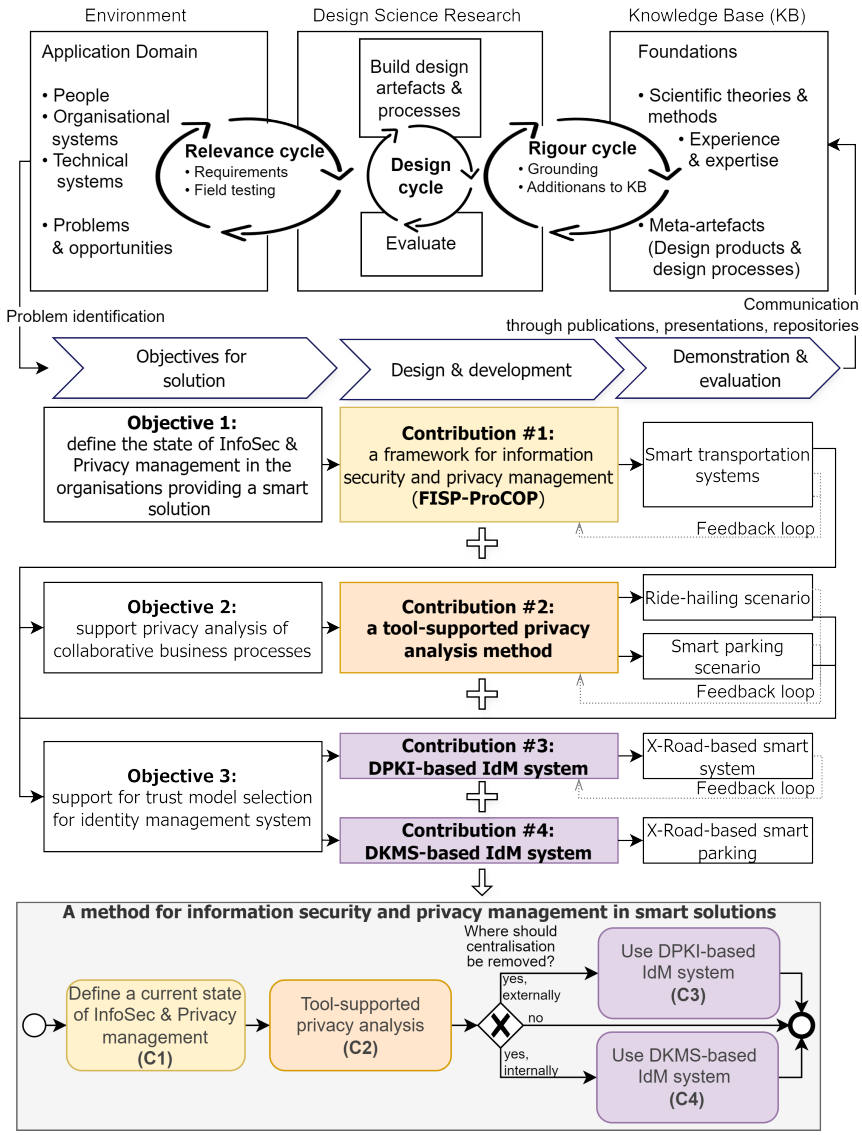


Figure 1: Research approach: DSR and its steps in the thesis (adapted from [53])

After developing the artefacts, we evaluated them through the evaluation or case studies. *Case study research* is an empirical investigation that examines a contemporary phenomenon within its real-world context [55]. Based on the evaluation results, we identified opportunities for further improvement and, when possible, enhanced them accordingly. A detailed description of how each artefact was developed using the DSR methodology is provided in the respective chapters of this thesis.

To reach the outlined objective, the main research question is further divided into three research questions (RQ). Each question answer results in an artefact which is developed through the design science cycle.

To achieve the first research objective, this work answers the research question $\mathbf{RQ}_1$: *How to depict the state of security and privacy management in an organisation?* Answering $\mathbf{RQ}_1$ includes:

- Reviewing the existing frameworks for information security and privacy
- Designing a framework (i.e., FISP-ProCOP) that allows depicting the state of security and privacy management in an organisation (*Contribution 1*)
- Validating the usability of the framework and its adaptability to the data extraction methods through two studies for smart transportation systems.

To achieve the second research objective, we answer the research question $\mathbf{RQ}_2$: *How can tools support privacy assurance for an organisation participating in a cross-organisational smart solution?* Answering $\mathbf{RQ}_2$ includes:

- Reviewing tools for compliance with European privacy legislation
- Reviewing tools for analysing the effectiveness of the privacy-enhancing technologies
- Designing a tool-supported method for privacy analysis (*Contribution 2*)
- Validating the usability of the method through two studies, namely autonomous vehicle-enabled ride-hailing and smart parking solutions.

To achieve the third research objective, this work answers the research question $\mathbf{RQ}_3$: *How does the trust model affect the security and privacy of an organisation participating in a cross-organisational smart solution?* Answering $\mathbf{RQ}_3$ includes:

- Reviewing the qualities of the information system which are affected by the trust model selection
- Designing a quality assessment model for an identity management (IdM) system which depicts qualities affected by the selection of trust model for the IdM system
- Designing and developing an identity management system based on the decentralised trust model, i.e. DPKI-based IdM system (*Contribution 3*)
- Designing and developing an identity management system based on distributed key management in the centralised trust model, i.e. DKMS-based IdM system (*Contribution 4*)
- Comparing the centralised, DPKI-based and DKMS-based IdM systems for the cross-organisational data exchange.

Finally, the four developed artefacts are combined together in a method for information security and privacy management in smart solutions w.r.t. situational method engineering. The motivation scenario in Section 1.1 focuses on the analysis and update of the existing information system which should be integrated to enable collaborative data exchange as a part of a smart solution. While we assume the existence of multiple (stand-alone) systems, the scenario takes place as a part

of a new software engineering – the one which enables the targeted smart solution. Thus, the answer to **MRQ** lies in the creation of a method to support such software engineering endeavours.

1.3.2. Situational Method Engineering

According to the *situational method engineering* (SME) [56], most projects have unique characteristics and situations and thus require a tailored approach rather than a one-size-fits-all methodology. Thus, having the specific context of the developed system formulated in the form of a motivation scenario, we follow the principles of situational method engineering and conduct the final design phase of the design science research method used for this thesis. While at the core of SME lies the notion that a method is composed of its components, the component-based approach for method engineering comes in hand. A component-based approach to method engineering is a strategy that involves breaking down methods into reusable, self-contained components [57].

Each method component consists of descriptions for ways of working (i.e., procedure [57]), notations and concepts. Each method component addresses a certain aspect of the problem at hand (i.e., perspective [57]) by following the framework used by actors who cooperate to document and capture answers to the problem. Using the component-based approach [57], we describe components of the proposed method based on three main thesis contributions.

1.3.3. Thesis Contribution Overview

The goal of the method is to support an expert group in assessing the effect of cross-organisational collaboration on the information security and privacy of the organisation's smart solution system components and identifying the changes for data protection. Based on the defined research objectives, Figure 2 depicts the process which the expert group should follow during the smart solution system engineering. The steps of the method correspond to the contributions of this thesis as follows: C1 - contribution 1, C2 - contribution 2, C3 - contribution 3, C4 - contribution 4.

First, the expert group should define the current state of information security and privacy management. For this, they should fill in the matrix of the FISP-ProCOP framework using the business goals for the smart solution agreed upon by all the parties that provide the smart solution. Additionally, the expert group should use the existing documentation within their organisation along with the experts' knowledge, which is not depicted in the documentation. Using the filled-in matrix, the expert group should analyse the measures of FISP-ProCOP across dimensions and define which of the technical countermeasures are missing with respect to business goals for the smart solution and organisational and people-oriented goals. The identified discrepancies result in the identified requirements for the next step of the method. Additionally, if an organisation follow some

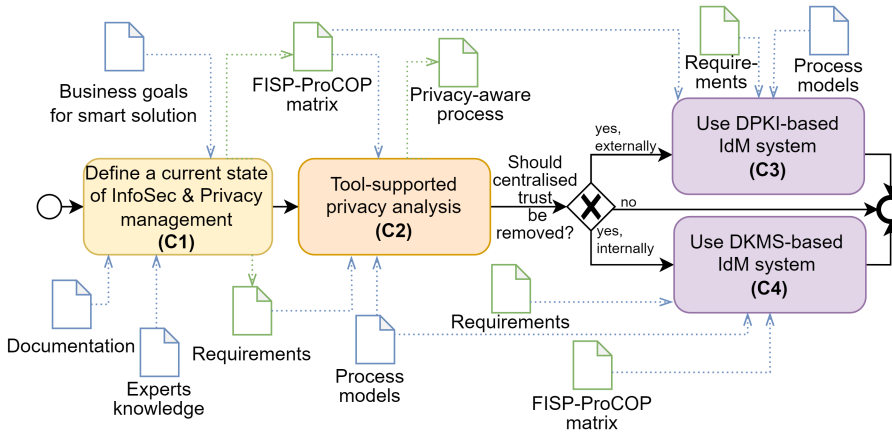


Figure 2: A method for information security and privacy management in smart solutions

information security standard (e.g., ISO/IEC 27001), the FISP-ProCOP matrix instance for the standard (i.e., the targeted state) can be directly compared with the organisation's matrix instance to identify the requirements to be addressed at the next stage.

The second step of the method aims to support the expert group in assuring compliance with the local data protection (privacy) legislation. At this stage, we propose to use existing privacy analysis tools to analyse the To-Be business processes for the smart solution. This method stage includes, first, checking compliance with GDPR and, second, selecting and analysing of efficiency of privacy-enhancing technologies to address the privacy goals and trust assumptions within data exchange in the smart solution. As a result, this step enables the expert group to create the artefacts that demonstrate compliance with GDPR and ensure that the existing data flows do not lead to data leakage.

Finally, the third step of the method should be executed only if an organisation is open to the change of trust assumptions for the new smart solution. The method's third step guides the expert group in analysing the transition to a new identity management system for collaborating organisations when trust assumptions change. This analysis considers the need to avoid internal centralisation and full trust (e.g., via implementation of zero trust strategy [58]) or to change the external root of trust. Thus, this stage allows the expert group to assess the quality of the current and potential IdM systems based on the proposed IdM system designs to make the decision about the appropriateness of the IdM system change with respect to the business objectives and the current security measures in place.

Actors Cooperation. The method is developed to be used by the expert group described in the motivation scenario (Section 1.1). Each member contributes to filling in the defined dimensions of FISP-ProCOP (see Chapter 3). Each member participates in the defined activities during the privacy analysis method (see Chap-

ter 4). Each member is responsible for sharing details of how IdM is implemented from their perspective (see Chapter 5).

Method Components. The proposed method consists of eight main components. The components and relationship between them are depicted in Figure 3 as a UML class diagram.

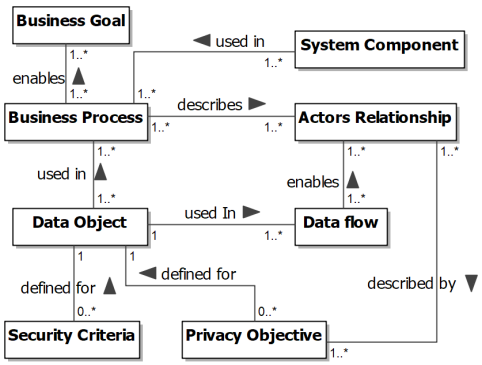


Figure 3: Components of the method for information security and privacy management in smart solutions

Business processes enables meeting the *business goals* of the developed smart solution. Such *business processes* describe *actor relationships* and use *system components*. The *business process* relies on the usage of *data objects* used in *data flows* that enable the defined *actor relationships*. Additionally, there should be defined *security criteria* and *privacy objectives* for each *data object*. Thereby, *actor relationships* and its trust assumptions are described by *privacy objective*, which are constraints on the data object flows.

Appendix A describes the procedure of defining the method components by the method users, namely the expert group, and the notation through which each component's concept should be depicted (Table 15). Additionally, Figure 38 and Table 16 specify the dependencies between data objects and method concepts operated within all the thesis contributions.

The business goal for the smart solution is the main input for the method which stays constant during the whole method execution. Meanwhile, the rest of the method components are either defined from the documentation or from the experts' knowledge and might be updated during the method steps. Thus, business processes, data objects, security criteria, privacy objectives, actors' relationships and data flow should be depicted in the FISP-ProCOP matrix instance and define the requirements for the second and third steps of the method. Thereby, the rest of the thesis elaborates on how each step of the final method proposed in this thesis is developed and validated.

1.4. Thesis Structure

This thesis comprises a method developed during the author's PhD studies, each step of which has been validated through the evaluation studies. Additionally, the implementation of the proposed IdM system design for the X-Road-enabled smart systems resulted in the developed proof-of-concept implementations of two alternative trust models. Table 1 summarises the research questions addressed, the contributions that address each research objective and the chapter of the thesis where this contribution is presented.

Table 1: Research question, thesis contributions and respective publication

Research Question	**Contributions**
RQ1. How to depict the state of security and privacy management in an organisation?	**C1**. a framework for information security and privacy management (FISP-ProCOP) (Chapter 3) **Publication**: - CSIMQ journal paper [26]
RQ2. How can tools support privacy assurance for an organisation participating in a cross-organisational smart solution?	**C2**. a tool-supported privacy analysis method (Chapter 4) **Publication**: - JISA journal paper [59]
RQ3. How does the trust model affect the security and privacy of an organisation participating in a cross-organisational smart solution?	**C3**. a DPKI-based identity management system (Chapter 5) **Publication**: - SAC'23 conference paper [60], - SP2I at ARES'23 workshop paper [61] **C4**. a DKMS-based identity management system (Chapter 5) **Publication**: - CAiSE'24 conference paper [62]

The rest of this thesis is organised as follows. Chapter 2 introduces the background of information security management in smart solutions. In Chapter 3, we introduce the framework for information security and privacy management (FISP-ProCOP) as a tool for depicting the current state of the assurance efforts in the organisation contributing to a smart solution. Chapter 4 presents a tool-supported privacy analysis method which, based on the depicted in FISP-ProCOP matrix requirements, should provide data protection for the business processes. In Chapter 5, we present the two identity management system designs for the smart systems enabled by the X-Road data exchange system. Finally, Chapter 6 concludes this thesis by providing answers to the research questions and discussing limitations and future research directions.

2. BACKGROUND

In this chapter, we provide the background of our study, presenting the key concepts used throughout the thesis. Thus, Section 2.1 provides examples of smart solutions in different domains and presents the secondary review results on the challenges of managing information security and privacy in two selected domains – e-government and e-health. Then, Section 2.2 reviews the commonly used information security and privacy management frameworks and reference models, standards and regulations. Finally, Section 2.3 discusses identity and trust management as one of the organisations' basic blocks of information security and privacy management. To this extent, we discuss the role of trust and identity management (IdM) systems in the collaborative data exchange between organisations, the characteristics that identity management systems help to achieve and the role of key management in trust management.

2.1. Smart Solutions

As we described in the previous chapter, the main research subject of this thesis is a cross-organisational smart system. Such systems are built by integrating multiple stand-alone information systems (ISs) with specialised data exchange systems or by connecting the information system with the Internet of Things (IoT) to enable cyber-physical systems. As a result of such integrations of systems managed by different organisations, cross-organisational business processes allow the development of unique value propositions to customers [63, 64] through leveraging data sharing.

Smart systems are finding their way into various fields of daily life. However, the most researched fields and their smart system examples are smart cities (including e-grids and traffic management), e-Health (including remote patient monitoring and diagnostics based on federated learning), intelligent transportation (including traffic management, ride-hailing, and smart parking), and e-Government (including systems digitalised governance services delivery, e-voting, citizens engagement).

2.1.1. Intelligent Transportation

Intelligent Transportation Systems (ITSs) are advanced systems that not only digitise transportation services but also aim to improve mobility and reduce its negative impacts. As emphasised by the Spanish Minister of transport, mobility, and urban agenda, ITS can enhance efficiency and sustainability [65]. The EU strongly supports ITS deployment through its ITS directive [66].

ITS operations necessitate the processing of diverse and often sensitive data, including publicly available traffic data, information about company resources, and personal data related to citizen identities and mobility patterns [67, 68, 69].

While access to individual data sources may pose limited risks, the intricate interconnections within ITS environments create a complex ecosystem where the manipulation of data in one area can trigger a cascade of security threats, potentially impacting both businesses and individuals significantly [70, 71].

One of the challenges in ITSs is the "privacy and security paradox" which arises from the trade-off between using private data to enhance safety features (like navigation) and the inherent reduction in individual privacy [71]. Drivers are often unwilling to sacrifice privacy for improved services, creating a significant challenge in developing transportation systems.

Meanwhile, traditional centralised approaches of ITS architecture, such as those relying on trusted third parties and cloud-based infrastructure, introduce vulnerabilities like single points of failure and latency issues [72]. To avoid the centralised ITS control, various decentralisation architectures, including the ones based on the blockchain, are introduced in [73, 74, 75, 76, 77, 78]. However, such solutions rely on developing a decentralised ITS from scratch with high reliance on end-user cooperation (drivers) who would participate in the ITS support and development of the systems from scratch, which poses the challenge for such system adoption in real-life scenario [70].

Furthermore, the effective implementation of ITS requires coordination among various stakeholders, including government agencies, private companies, and the public [70]. However, the state-of-the-art ITS solutions either, in contrast, focus on managing ITS by end users or focus on the physical and network security measures and privacy-preserving system designs, leaving out of scope the frameworks for coordinating security and privacy efforts of ITS stakeholders.

To sum up, ITS development faces a critical trade-off between utilising data for enhanced usability and preserving user privacy. Centralised systems are vulnerable to single points of failure and data breaches, while decentralised approaches require significant user involvement and development efforts. Moreover, effective coordination among government agencies, private companies, and the public is crucial for addressing these challenges and ensuring the secure deployment of ITS solutions.

2.1.2. e-Government

Countries worldwide work on digitalising their services and systems to enable electronic government. Electronic government (i.e., "e-Government" or "eGov") refers to the usage of digital systems and technologies to improve the quality of public services or reduce their cost, allow access to public information and increase engagement of public sector representatives, businesses and citizens in the decision-making [79, 80, 81]. However, during the development of eGov, countries faced a number of challenges, including the ones related to security and privacy due to the high reliance on sensitive national and personal data.

The studies in [80, 82] show that adoption of the eGov systems depends on the trust in governance and its ability to preserve the privacy of citizens' data along with ease of use of e-services and security assurance of the system. Additionally, [82] and [83] highlight that information security is not only a technology-based issue, as the majority of vulnerabilities and threats originate from humans and their system misuse. Thus, the holistic treatment of information security is multi-layered and combines technical, personnel, procedural, and physical security.

Among the challenges in securing eGov systems is the fact of building eGov services based on disintegrated stand-alone software systems used in eGov, where security mechanisms are not centrally managed, and users' identities are separately managed by each IS [84]. Thus, there is a need for a holistic approach to identity management in the integrated eGov system, along with an information security governance model at the strategic level. Meanwhile, Elisa et al. [85] show that most used electronic identity management systems are not interoperable, lack security due to centralised data storage, and, thus, are prone to a single point of failure.

Finally, a number of challenges in information security stem from personnel and procedures (or their absence). Thus, the study of Cameroon's eGov security [81] showed that 24% of vulnerabilities in eGov services are organisational. At the same time, the rate of implementing the recommended measures is not higher than 26% for each measures group among technical, organisational, and physical countermeasures. The negative factors of information security assurance include the low capacity of IT-related personnel and low involvement of IT units in managing or initiating IT-related projects (including the security-related) [81]. As a result, we see a lack of understanding of the interdependence between information security assurance and business needs and objectives.

To sum up, based on the studies in [79, 80, 81, 82, 83, 84, 85] on e-government implementations, we see the need in providing the eGov with a method to support multi-dimensional information security assurance considering technical, personnel, procedural, and physical security. In particular, the method should consider building eGov systems based on the multiple stand-alone systems and the need to develop eGov systems and secure the manipulated information simultaneously from the perspective of technologies and business needs.

2.1.3. e-Health

Electronic health (e-Health) is used to refer to healthcare processes and practices supported by information and communication technologies [86, 87], which were initially presented by healthcare information systems or systems for electronic health records. Meanwhile, nowadays, e-Health is extended into mHealth (mobile healthcare) or uHealth (ubiquitous healthcare) thanks to the integration of healthcare systems with various mobile devices, including smartphones, health trackers, on-body health sensors and IoT smart home-based health monitoring devices.

Based on the survey results, insider threat from the staff was defined as one of the most serious [88], along with threats to electronic and IoT devices, third-party entry software and network threats, and natural hazards. Throughout security surveys in smart healthcare [88, 89, 90, 91] authors stress the need to ensure staff education and integration of security guidelines, procedures and standards. Regarding healthcare professionals' information security practices, the mapping study [89] shows that insider data breaches in healthcare are caused mainly by (*i*) the lack of experience of healthcare professionals in information security, (*ii*) the lack of development of conscious care security practices. Even more noteworthy is the fact of the lack of security knowledge of mHealth systems developers and the lack of security practitioners to support the development process [92]. Finally, the review by Wani et al. [91] reveals the need to design security standards, protocols and guidelines considering both security and clinical workflow.

Meanwhile, the systematic mapping study in [87] indicates that 85% of publications in eHealth (including mHealth and uHealth) address only 6 out of 20 NIST security control families. As a result, the current knowledge base of security and privacy assurance is skewed towards basic technical controls, leaving organisational and managerial controls out of consideration. To address this gap, the authors argue that future research should explore organisational controls, as technical solutions alone cannot fully address security and privacy challenges without corresponding cultural and business model changes. Additionally, the evaluation studies of mHealth and uHealth systems primarily focus on evaluating a set of health mobile applications or their privacy policies [87]. Thus, there is a gap in the holistic evaluation of eHealth systems that would assess the privacy and security of the entire eHealth system components, jointly considering mobile applications, servers, and third-party servers.

Among the gaps in the knowledge base discovered in the previous systematic mappings and surveys are (*i*) the gap between existing technical security and privacy issues and the solutions, understanding of its impact and utility on the healthcare organisation management [88, 92, 93, 94]; (*ii*) the lack of knowledge and awareness of security and privacy assurance practices from both IT and healthcare staff [88, 89, 90, 91]; and (*iii*) the lack of privacy evaluation procedure to assess the used systems (mobile apps, information systems, external services, medical devices, etc.) [95, 96].

2.1.4. Incidents in Smart Solutions

While the studies of smart solutions in transportation, healthcare, and government domains stress the challenges of assuring information security and privacy, including intentional or unintentional attacks from humans, data breach incidents caused by insiders occur regularly. For instance, in 2022, there was a leak of Cash App's customer data by a disgruntled employee [97]. The reason for the leakage was that the fired employee's credentials were not terminated, so he abused the

user's access permission to access customers' personal data. Another case of data leakage is reported in [97], where a former employee of the South Georgia Medical Center in the US downloaded private data from the medical centre's systems to his USB drive without obvious reason the day after quitting. As it was found out, a former employee had legitimate access to the data he stole and had nothing preventing him from carrying through with his intentions. Both cases show that while there were some data protection measures in place, due to a lack of coordination between organisational policies and technical implementation of the security measures, sensitive data leaked.

Meanwhile, even the correct implementation of identification and authentication measures on all the organisation levels may be a reason for vulnerabilities. Thus, as the review of eGov and ITS system implementations pinpointed the centralisation of services, there are a few examples of attacks targeting such single points of failure, which are getting more common in case of an attack on the availability of critical services due to political reasons. As the report on Estonian national cybersecurity posture shows [98], distributed denial of service (DDoS) attack is one of the largest attack types and most visible collateral effects of the full-scale invasion of Ukraine. Thus, one case of the distributed denial of service (DDoS) attack on Estonia in 2024 caused the unavailability of public transport ticketing services, affecting all carriers across the country for a few hours. If such a DDoS attack is successfully implemented targeting the identity providers used by public agencies for identification in the national information system, the disruption of the public agencies' services can be achieved. A similar disruption happened in Estonia in 2023 [99] when all the primary identification services provided by SK ID Solutions were offline for three hours simultaneously. As a result, using the dependent system in these identification solutions was impossible.

2.2. Information Security and Privacy Management

As the review of smart solutions showed, the high reliance on digital data processing and integration of multiple stand-alone systems for delivering smart solutions make such systems prone to security attacks, which lead to high-impact risks due to the manipulation of numerous data (both internal operational data of organisations and personal data of the system users). The smart solution implementation experiences show the risks originate as much from technical vulnerabilities as vulnerabilities or gaps in organisational strategy, lack of security awareness or training, and incomplete policies in place. As a result, smart systems are proven to be attractive targets for data breaches by both external attackers and insiders who may abuse their access privileges.

Information security encompasses the protection of all types of information, whether digital or physical, against unauthorised access, use, disclosure, disruption, modification, or destruction, aiming to ensure confidentiality, integrity, and availability (i.e., CIA triad). *Privacy*, on the other hand, primarily focuses on the

protection of personal data, emphasising individual control over its collection, use, and disclosure. While both concepts share the goal of safeguarding information, their scopes differ significantly. Thereby, privacy primarily concerns protecting individual autonomy and preventing harm that can arise from the misuse of personal information.

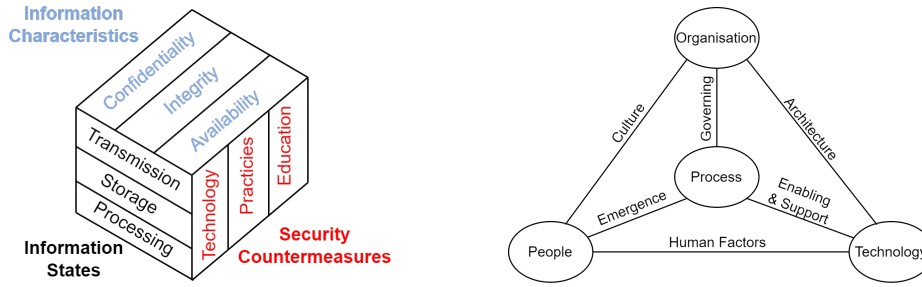
One of the steps of data protection for privacy assurance (e.g., with respect to European data protection regulation and ISO/IEC 27701) is the usage of appropriate security measures for personal data protection. However, while some security measures can contribute to privacy (e.g., encryption), they are not inherently designed to protect privacy and may not allow privacy at all if used inappropriately. For example, strong authentication mechanisms enhance security but may not address concerns about data minimization or purpose limitation, which are core privacy principles. Therefore, separating these concepts should allow for a more nuanced and effective approach to information protection, ensuring that both security and privacy are adequately addressed within their smart systems and that organisations comply with relevant regulations.

2.2.1. Frameworks and Reference Models

The screening of the literature on information security and privacy management in smart solutions, which we initially presented in [26], shows that the proposed measures for securing information in smart systems vary from the specific protocols for the data transfer and system architectures up to defining new roles of stakeholders and following security-related standards. Thus, to understand the whole picture of how organisations handle information security and privacy management (later referred to as *'InfoSec & PM'*), we should remember that information security is a multidisciplinary domain. To define how organisations handle it, we should consider multiple aspects of the organisations involved in the InfoSec & PM.

Models and frameworks are abstract ways of describing concepts and their connections to the selected domain, which helps unify the domain's understanding. These models and frameworks collectively serve as a valuable knowledge base for understanding and navigating the complexities of information security and privacy. However, there are numerous of those, and they differ by the level of detail and the purpose: descriptive, which describes the state, e.g., ISACA BMIS [28] and McCumber cube [29] that are depicted in Figure 4, or prescriptive, which prescribes actions to be performed (e.g., NIST CSF [31], HITRUST CSF [100]). Since, in our study, we want to understand the static view, we consider the descriptive InfoSec & PM models and frameworks as a theoretical background for data extraction.

McCumber Cube. Presented in [29], the McCumber cube is one of the earliest models that guide examining information security. The model proposes to examine security from three dimensions (Figure 4a). First, security principles, often



(a) McCumber cube [29]

(b) ISACA's BMIS [28]

Figure 4: Information security frameworks

called the CIA triad, describe the properties of the information that should be preserved, namely confidentiality, integrity, and availability. Second, the model proposes considering the state in which information can exist within the system: storage, processing, and transmission. Third, countermeasures are applied to maintain critical information properties while information resides or moves between the states. Countermeasures are primarily based on the technological solutions presented by hardware, firmware, or software. However, the second important building block of information security countermeasures is policy and practice, which describe the existing policies to follow using information systems and procedures to employ or enhance technological security countermeasures. Finally, while the first two countermeasure types enable security-enhanced information systems, the final countermeasure type (i.e. education) comprises people. Thus, ensuring that people understand the necessity of protecting information and being capable of its maintenance significantly contributes to the overall level of the system's information security.

ISACA business model for information security (BMIS). Proposed by Roessing in [28], BMIS is a framework of business-related elements used to describe information security in an organisation. The framework shows the dynamic connections between the four key dimensions of information security and privacy and how they affect each other through the depicted interconnections (Figure 4b).

Organisation refers to "a network of people, assets, and processes which are working together toward a common goal" [28]. Thus, organisational design and strategy describe how the organisation's strategy guides the processes based on the strategic objectives, how external factors guide the organisational design and strategy itself, and how the organisation's strategy drives the architecture of the technical security measures. The people element extends the BMIS model with a non-technical perspective by highlighting the importance of stakeholders' values, beliefs, and behaviours that influence information security and privacy in the organisation. The process element describes formal and informal processes that exist in an organisation. The organisation's strategy governs the processes, and at the same time, they enable the implementation of the strategy. The technology

element describes the IT solutions that enable and support the processes. This is the key element commonly addressed by information security and privacy management, as most of the proposed security and privacy countermeasures are technological measures. However, the BMIS model highlights the tight connection of the technical solutions with the existing organisation governance and objectives, processes, and people, which the IT systems support.

Reference Model of Information Assurance & Security (RMIAS). First proposed in [30], RMIAS is a high-level guide outlining the key components, relationships, and principles involved in ensuring information assets' confidentiality, integrity, and availability. Depicted in Figure 5, RMIAS consists of four dimensions: information system security life cycle, information taxonomy, security goals, and security countermeasures. The reference model aims to assist with developing and revising an information security policy document. The model considers four types of security countermeasures: organisational, human-oriented, technical, and legal.

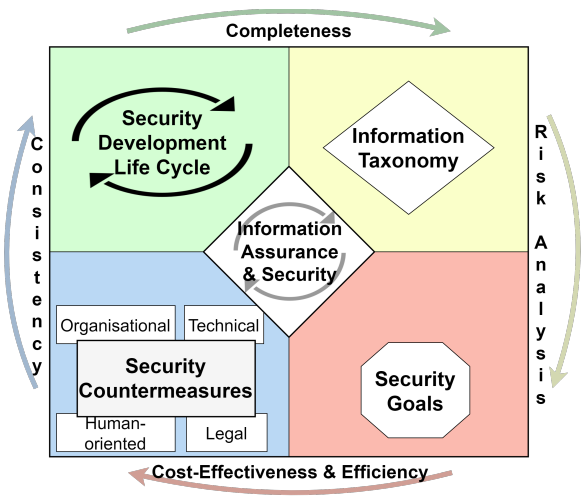


Figure 5: Key elements of a Reference Model of Information Assurance & Security [26, 30]

2.2.2. Industry Standards

Along with the reviewed information security frameworks, several standards and frameworks are known among industry representatives. *ISO/IEC 27001* [27] is an international standard for information security management systems that provides a framework for organisations to establish, implement, maintain, and continually improve an effective information security management system. The standard also contains a set of security controls for mitigating the selected threats. Having the possibility to be certified against it, ISO/IEC 27001 is a de facto industry-used framework for information security used by established organisations to demonstrate commitment to information security to customers and partners [101].

ISO/IEC 27701 [102] is another international standard built upon ISO/IEC 27001 and includes privacy information management system requirements. Other commonly used recommendations are NIST SP, which are Special Publications from the American National Institute of Standards and Technology. For instance, *NIST SP 800-39* [6] focuses on managing information security risks from an organisational perspective, and *NIST SP 800-37* [103] provides a structured framework for managing cybersecurity risks within the context of system development and operation. Meanwhile, *NIST SP 800-53* [104] is a catalogue of security and privacy controls that organisations can use to protect their information systems and data. Originating from the American agency, NIST SP is commonly used by U.S. government agencies and is more recognisable by U.S. organisations. While guidelines and frameworks from ISO/IEC and NIST SP are industry best practices and provide comprehensive recommendations on managing information security, they are proved to be of high complexity [105] and, thus, are resource-intensive, particularly for smaller organisations.

2.2.3. European Regulations

In the European Union, a number of unit-level regulations and directives regulate how organisations operating in the EU or manipulating the data of EU citizens should act to preserve information security and privacy. Among them are GDPR, Cybersecurity Act, and NIS2 directive.

Since 25 May 2018, the *General Data Protection Regulation* (EU) 2016/679 (GDPR) [106] is the primary personal data regulation framework in the European Union (EU). GDPR defines rules under which *personal data* about an identifiable person can be captured and governed by the data *controller* and processed by *processors* (both controller and processor are business organisations). The organisation which "determines the purposes and means of the processing of personal data" is called a *controller*, while *processing* refers to any operation which is performed on personal data [106]. Another organisation which provides services and processes personal data on behalf of the controller is called a *processor* [106]. The legislation also specifies the requirements for an information system (IS) (i.e., processing system) used by a processor for personal data manipulation. Finally, it defines the rights of a *data subject* regarding their personal data processing.

The *EU Cybersecurity Act* [107] is a regulation aimed at strengthening the EU's cybersecurity capabilities and creating a more secure digital environment. It sets out rules for cybersecurity coordination, certification, and cooperation across the EU. The Act grants a permanent mandate to the European Union Agency for Cybersecurity (ENISA), giving it more resources and authority to coordinate cybersecurity efforts across the EU. It also introduces a voluntary EU-wide certification framework for information and communications technology (ICT) products, services, and processes. This framework aims to improve the security of these products and services by setting common standards and procedures for certifica-

tion. The Act applies to all EU Member States, ensuring a consistent approach to cybersecurity across the EU.

Since 18 October 2024, *NIS 2 directive* [108] is a European regulation that aims to strengthen the cybersecurity resilience of essential services and critical infrastructure sectors in the EU. The directive requires organisations to conduct risk assessments, implement security measures, report incidents, and cooperate with other companies and authorities in the event of a cybersecurity incident. NIS 2 also introduces a new classification system for essential services, which divides them into two categories: essential services of general interest and essential services that are important for the economy or society. Organisations in both categories are subject to different requirements, depending on their level of importance.

Introduces on 10 December 2024, *Cyber Resilience Act* (CRA) is a harmonised regulatory framework that sets "rules for the making available on the market of products with digital elements" [109]. To safeguard consumers and organisations purchasing software or hardware products with a digital component, CRA mandates cybersecurity requirements throughout the lifecycle of products with digital elements, emphasising secure design, development, and maintenance. This is particularly critical for complex SoS as smart solutions, given their interconnected nature and inherent vulnerabilities. By fostering shared responsibility among manufacturers, retailers, and users, the act aims to enhance the security and resilience of these systems.

Except for the EU-level regulations, some EU state members also have local cybersecurity standards guiding public and private organisations. For example, *Eesti infoturbestandard* [110] (Estonian Information Security Standard, E-ITS), BSI-Standard 200-3 [111] and *Předpis 181/2014 Sb. (Zákon o kybernetické bezpečnosti)* [112] (Cyber Security Act in Czechia)) are the cybersecurity or information security standards in Estonia, Germany and Czechia, respectively.

2.2.4. Privacy Principles and Privacy-Enhancing Technologies

Data protection principles, as mandated by regulations like GDPR (Art. 47 [106]), are paramount for modern information systems. These principles, encompassing purpose limitation, data minimisation, and data security, emphasise a proactive approach to privacy. *Privacy by Design* (PbD) embodies this proactive approach, advocating for the integration of privacy considerations throughout the entire system development lifecycle [113].

PbD leverages design strategies during the initial phases of system conception and analysis, followed by the application of design patterns during the system design phase. Subsequently, the implementation phase necessitates the integration of *Privacy-Enhancing Technologies* (PETs) to ensure robust data protection [113, 114].

PETs encompass a range of technical measures that safeguard personal data while preserving essential system functionality [114, 115]. These technologies are categorised based on their intended goals: communication protection, data protection, entity authentication, privacy-aware computation, and human-data interaction [115]. For instance, achieving data protection often involves fulfilling the goals of integrity and confidentiality.

To facilitate the integration of PETs into system design, Privacy-Enhancing Business Process Model and Notation (PE-BPMN) was introduced as an extension of the standard BPMN 2.0 language [115]. PE-BPMN incorporates "general stereotypes" (e.g., ProtectConfidentiality, OpenConfidentiality) to represent high-level privacy goals and "concrete stereotypes" to signify specific PETs (e.g., PK encryption, PK decryption). By visually representing PETs within the BPMN framework, PE-BPMN supports system analysts in capturing and integrating privacy-preserving mechanisms into the system design [116].

Cryptographic algorithms constitute a significant subset of PETs. Cryptography fundamentally revolves around the concept of *encryption*, the transformation of original data (plaintext) into an unintelligible form (ciphertext) [117]. This transformation utilizes *keys* as parameters for both encryption and decryption processes.

By rendering data unreadable without the appropriate decryption key, encryption safeguards sensitive information during transmission and storage [117]. Encryption schemes vary in their underlying transformation techniques. In the context of personal data management, *Fully Homomorphic Encryption* (FHE) emerges as a particularly promising approach [118]. FHE enables computations to be performed directly on encrypted data, eliminating the need for decryption prior to processing. This capability has profound implications for data privacy, as it allows sensitive data to be processed by untrusted parties (e.g., cloud service providers) without compromising data confidentiality [118]. Examples of FHE implementations include public-key encryption and secret sharing schemes (also referred to as *SS computation*).

2.2.5. Supporting Tools for Personal Data Protection

One of the tools which can help achieve compliance with the European privacy legislation is the ISO/IEC 27701 standard [102]. It provides a set of recommended privacy requirements and controls for Privacy Information Management Systems used by personal data controllers and processors. While the standard provides a rough mapping of the recommended controls with requirements in GDPR, it neither guarantees compliance with the legislation nor provides explicit instructions or steps to be followed by organisations to apply the standard. Thereby, the standard mainly helps to "translate" requirements of GDPR from legal style. However, it is not an on-the-shelf solution, thanks to which organisations would be able to develop or assess their privacy management measures.

Organisations that act as controllers commonly have the role of data protection officer (DPO), who assists the organisation in complying with the regulations [119]. To assess the delivered privacy within the designed business process and IS, DPOs can use predefined tables, templates or questionnaires - to fill them in based on a manual analysis of the organisation's policies and systems. Alternatively, there are many commercial solutions offered by over 304 vendors [119]. The provided solutions range from simple questionnaires to more advanced software tools for privacy and compliance assessment and up to the services of an external data protection officer. However, a considerable part of the proposed software solutions checks a deployed application. Thereby, they are not applicable for the information systems in the early stages of development or for not a single web-based application (but a system of information systems as in the case of collaborative data processing [120]). According to [119], some commercial solutions lack scientifically proven methodologies or evidence to support their validity or utility. Furthermore, such tools are characterised by a lack of interoperability with other compliance systems relying on non-standardised semantics, making it hard for organisations to integrate them into the toolchain without locking a company to a vendor.

Conceptual GDPR model and DPO tool. Several conceptualisation models and approaches have been developed to decompose the legal text of the GDPR and structure it for potential automation [46, 121, 122]. One model that has resulted in its automated usage within the tool is the conceptual GDPR model refined in [121, 123]. The GDPR model defines the key legislation concepts that should be considered in the business processes and is depicted in a class diagram. The model is presented in Figure 6 and describes the main concepts and connections between them according to articles in [106]. Thus, the conceptual model captures the *personal data* (Art. 4(1)), data *processing task* (Art. 4(2), 4(23)), *legal ground* and *legal ground special categories* (Art. 45–59, 9(2)) for the data processing, including consent, privacy policy (Art. 13, 14). The model also depicts the roles of parties involved in the data handling (data subject, controller, processor, recipient and third party). Finally, the model defines the connection of the mentioned concepts with the technical implementation of the data processing task (Art. 30), including *processing system* used by the controller to produce a *record of data processing*, and which is secured with security measures (Art. 25).

DPO Tool[3] is a web application prototype that implements a model-based approach for achieving GDPR compliance of business processes. The method of achieving GDPR compliance with the DPO tool is presented in [123] (see Figure 7) and is based on the described above conceptual GDPR model.

The DPO tool uses the provided business process model. The model should be annotated with the concepts from the GDPR conceptual model. The annotation can be extracted directly from the model (in case the model follows the annota-

[3]DPO Tool can be accessed at `https://dpotool.cs.ut.ee/`

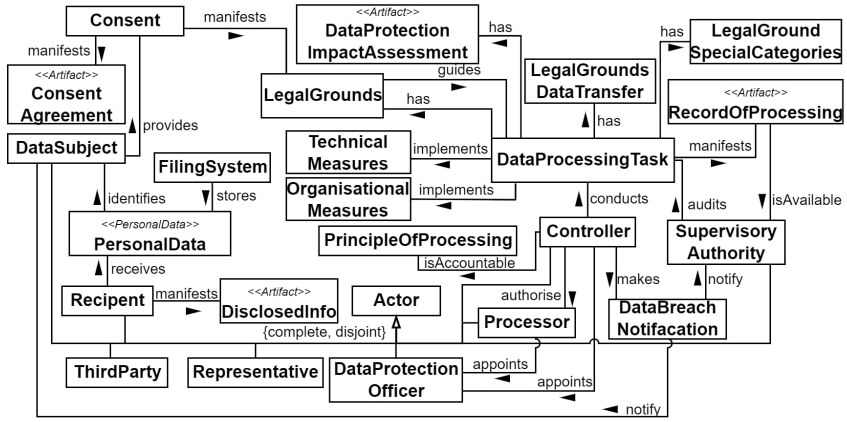


Figure 6: GDPR model [123, 59]

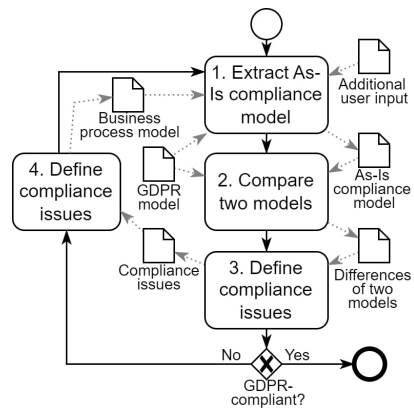


Figure 7: Model-based method for GDPR compliance [123, 59]

tion principles) or added by the DPO tool to the process model based on the user input. Then, after extracting the existing concepts from the business model (i.e., the As-Is compliance model), the tool compares the GDPR model with the As-Is compliance model. If the business model does not consider some concepts from the GDPR conceptual model, its absence is treated as a compliance issue. As a result, the GDPR compliance analysis approach results in the defined compliance issues that refer to the absence of the GDPR concept(s) in the business model. Thus, the approach helps to identify that, for example, the process does not consider the requirement of having the privacy policy presented to the data subject or that the system used for the data processing does not use any security measures.

The advantages of the DPO tool are as follows. First, the tool is an open-source prototype that can be freely accessed and is based on peer-reviewed academic publications. Second, the tool can be used for the GDPR compliance check of a business process during the whole software lifecycle - at the design, development, or operation phase - as it requires only the BPMN model for the input. Finally, the

comparison of the manual regulation compliance with the tool-supported analysis in [124] reveals significant correspondence of the identified non-compliance issues and points to the found non-compliance issues using the tool, which were omitted during the manual check. On the other hand, the tool methodology does not cover all the GDPR requirements (40 articles out of 90), and the national adaptations of GDPR are not considered. Thereby, the DPO tool is a proof-of-concept prototype that can be used as an alternative to the manual GDPR compliance check of business processes, keeping in mind the existing limitations of the used approach.

The tool has been applied to the scenarios of tollgate usage by the connected vehicles [123], the scenario with a North-European airline company, where a customer of airline company is making calls to support centre to purchase flight ticket [124], and for analysing the vehicle charging scenario [125, 126].

Privacy-enhancing technology selection. Pleak (Privacy LEAKage Analysis) Tool[4] is an open-source web application prototype for analysing business processes and detecting possible data leakages [127]. The tool helps analyse a business process, which includes collaborative data processing, by providing an overview of what data is leaked, to what extent, and to which process participants using mCRL2 toolset [128], which is in turn based on ACP-style process algebra and has an axiomatic view on processes. Pleak allows us to analyse the impact of the privacy-enhancing technologies (PETs) used in the context of business processes. The tool aims to help with risk analysis and impact assessment of data privacy within the existing system. Pleak primarily targets non-information security specialists, like software developers, process owners or data protection officers, who need to assess the effectiveness of the selected privacy-enhancing technologies. As an input, the tool gets the PE-BPMN model (an extension to BPMN) that depicts the analysed system through business actors and processes, data objects, and data analysis algorithms. As a result, Pleak provides the user with analysis reports of different depth levels. Overall, the report contains information about private data flows through the system and reveals the actors to which the data is disclosed and to which extent.

The major advantage of Pleak is its multi-functionality. The tool proposes several techniques of privacy analysis on the different levels of implementation details [127], namely, BPMN and SQL leaks-when analysis, sensitivity and differential privacy analysis. As the tool is under development, it currently supports a limited number of PETs. So far, the tool has been applied to the scenarios of critical situations. For example, the Pleak toolset was used to analyse the scenario when two countries interact to determine which ships of the aid-providing country should arrive at which ports of the aid-requesting country [127, 129]. The Pleak toolset was also applied to the scenario where the command centre of the

[4]Pleak can be accessed at `https://pleak.io/` (account: *demo@example.com*, password: *pleakdemo*, manual: `https://pleak.io/wiki/`) [127]

smart city requests from the citizen a photo of the specific place using privacy-preserving data search [115] in the mobile app RapidGather [130] that enables the usage of citizens' mobile phones to detect and respond to crisis situations. All in all, Pleak can analyse the currently supported PETs and define data leakages. Alternatively, Pleak can help compare PETs from one class in the context of the developed system to select the technology that enables better personal data protection.

2.3. Identity Management (IdM)

In this subsection, we outline the preliminaries necessary to understand an identity management system, its key conceptual components, and their contribution to managing identities and trust in cross-organisational data exchange. Moreover, here we define the system characteristics, which aim to be supported by the identity management (IdM) system. The section is based on the authors' publications in [60, 61, 131, 132] and may contain sentences or fragments of sentences from these publications.

2.3.1. Collaboration and Trust

During the last two decades, organisations have become increasingly reliant on information provided by other organisations aiming to deliver innovative services to customers. Such dependency results in the need to establish a trust relationship for the data exchange [6]. *Trust* is the decision of one party to be vulnerable to another party, which is believed to be *trustworthy*. Each party may have different requirements and procedures for defining *trustworthiness* of their *trust relationship* establishment [133].

Following, we regard trustworthiness as the beliefs of the system users in expected attributes. Thus, being trustworthy for the IdM system means being able to enable social trust [134]. NIST SP 800-39 defines trustworthiness as the ability of a person, organisation, or system to consistently deliver reliable and secure performance, based on their demonstrated qualifications and capabilities [6]. Assuming that trust is established between identities (represented by organisations, systems or people), *trust model* defines the rules for who can create, read, update, delete, and verify the mapping between the identity holders and the digital credentials for such identities[5]. Based on the selected trust model, the organisations' representatives make decisions on risk management.

[5] *Trust model* is also referred to as *(digital) identity model* in the latest version of NIST SP 800-63 [135] and in [52].

As a result, the collaboration between entities in smart solution systems happens with the predefined trust assumptions defined by the selected trust model. Meanwhile, the identity management system used by each collaborating entity implements the selected trust model in order to identify and authenticate. Thus, identification ensures that external identities can access assets only based on the rules defined by a trust model.

2.3.2. IdM System: Components and Operations

Digital identity is "a set of claims made by one digital subject about itself or another digital subject" [136]. *Identity management (IdM)* refers to the set of policies and technologies used to ensure that the resource users are eligible to access them based on their identity characteristics. Often, the IdM is split into identity management and access management. An identity management system defines the procedure based on which the entities are authenticated. An access management system defines the authorisation mechanisms, which control access to resources based on their identity. IdM system is built using the following elements [52, 135]:

(`Assumption`) **Trust model** that defines (*i*) actors involved in the interaction; (*ii*) social trust between actors and their dependencies on actions; (*iii*) resources that should be protected and/or shared during the interaction between actors;

(`Variable 1`) Type of **credentials** used for actors identification. *Credential* is an object or data structure that binds an identity via an identifier and (optionally) additional attributes (i.e., claims), to at least one authenticator possessed and controlled by an identity (i.e., identity holder) through credentials [135];

(`Variable 2`) **Policies** of using resources by actors which could be presented in the form of the following rules: $\{A_i, C_j, R_k, AR_l\}$, which define that actor A_i which can be identified using credential C_j can access resource R_k with the access right AR_l;

(`Variable 3`) **Measures** (business or technological) for the policies enforcement.

The first component of the IdM system (namely, `assumption`) defines the trust model and is the main input for implementing IdM. Based on the `assumption`, the rest of the IdM elements can be selected, while credentials (`variable 1`), policies (`variable 2`) and measures (`variable 3`) may vary depending on the selected trust model.

Roles. Regardless of the selected trust model, the IdM system defines rules of interaction between the following roles [52, 135]:

- **(Identity) Holder** is an actor who requests credentials and who is the subject of digital identity credentials. The identity holder can be presented by a physical person, organisation or system component (e.g., web service, server, information system);
- **Issuer** (also referred to as "Credential Service Provider (CSP)" or "Identity Provider (IdP)") is a trusted entity that issues digital identity credentials (i.e., authenticators) to actors to prove that they are characterised by the claims in the issued credentials;
- **Verifier** is an entity that verifies the claimant's identity by verifying the claimant's possession and control of one or more authenticators (based on the issued credentials) using an authentication protocol.

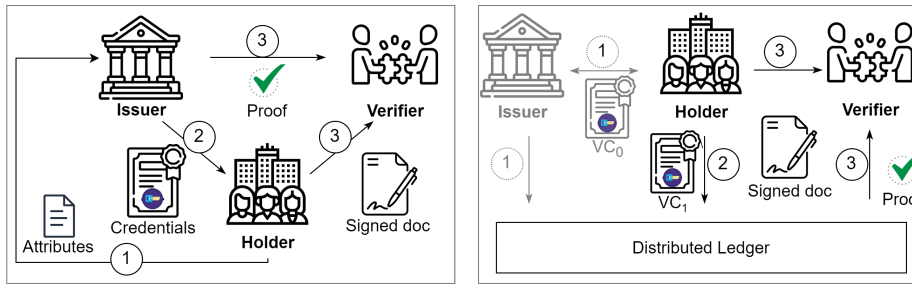
Operations. The IdM operations include (*i*) request for identity issuance based on the presented attributes, (*ii*) identity issuance, and (*iii*) credentials presentation and identity verification. Additionally, the credentials for identity may be revocated, and the status might change. In this thesis, we mainly focus on the first three operations.

Root of Trust. Depending on the selected trust model, there are different identification procedures for issuers, holders, and verifiers. But the main difference between the trust models is the used root of trust[6]. *Root of trust (RoT)* is the basis that provides evidence of identity attestations against the claims mentioned in the credentials [137]. Based on the RoT, the depending entities might form a chain of trust, while RoT is the only entity trust to which is axiomatically accepted without further verification during identity management [52].

In [52], there are three types of RoT defined. *Administrative RoT* assumes trust in certification authority (CA), which is an organisation that has a defined certification practice procedure used by the staff to ensure the quality and integrity of the digital credentials (i.e., certificates) they issue. Trust in administrative root of trust depends on the general reputation of a CA. *Algorithmic RoT* relies on computer algorithms that create secure systems where no single entity has complete control. These systems ensure that all participants agree on a shared source of truth. Examples include blockchains, distributed ledgers, and distributed file systems. *Self-certifying RoT* relies on secure random number generation and cryptography, which can be ensured through using specialised hardware like secure enclaves or trusted platform modules. Trust assumption is based on the hardware and software's specifications, testing, and reputation.

Trust Models. Depending on the selected root of trust, the execution of IdM operations and the involved parties vary. Therefore, there are a number of trust models, including a centralised trust model, a federated trust model, and a decentralised trust model. Figure 8 depicts the former and the latter, while the federated models are not discussed in this thesis as it is mainly used for individual entities and not organisational digital identity.

[6]The "root of trust" is also known as "trust root" or "trust anchor" [52, 135]



(a) A centralised trust model (b) A decentralised trust model

Figure 8: Trust models (1 - provide attributes, 2 - issue identity credentials, 3 - verify identity; activities and actors in grey are optional for the model) [52]

A *centralised trust model* is the most commonly used set-up which relies on an administrative RoT. Based on the selected administrative RoT, an organisation (identity holder) provides a set of attributes to the selected issuer with respect to the chain of trust. Second, based on the provided attestation attributes, an issuer issues credentials to a holder, and keeps the record of such credentials issuance. Third, the holder provides a signed document to a verifier where the signature corresponds to the attested signature of the credentials holder, and the verifier verifies the provided document by checking that the signature corresponds to trusted credentials and the issuer confirms the validity of the credentials.

A *decentralised trust model* relies on algorithmic RoT and aims to eliminate reliance on any centralised authorities. Thus, the holder may omit any interaction with external identity issuer and rely on self-issued verifiable credentials, the details of which are stored in a distributed ledger and, therefore, are (publicly) accessible for the verifiers. If necessary, a holder may connect the self-issued credentials to the issued before verifiable credentials from the commonly trusted issuer. During the data exchange between the holder and verifier, the verifier can access the distributed ledger and verify the identity of the received signed document.

Self-Sovereign Identity (SSI) is a paradigm for managing digital identities that relies on a decentralised trust model and aims to empower identities to take control of their identity-related data. According to SSI, each identity should be in full control of its own digital identity and, thereby, rely only on itself (not any government) for issuing credentials for its identification. For this reason, SSI implies the usage of algorithmic RoT, distributed identifiers (DID), verifiable credentials and digital wallets.

Credentials. *Credential* is any set of information that some authority (issuer) claims to be true about the identity of a subject of the credential and which enables the subject to convince others (who trust that authority) of these truths [52]. Commonly, the subject of the credentials is its identity holder. Credentials are used as a baseline for providing the verifier with proof of the credential's subject identity.

Except for the proof of some statement about the credentials' subject, the verifier must be able to determine the following from the presented credentials: (*i*) who issued the credentials; (*ii*) credentials have not expired or been revoked. A specific type of credential is *Verifiable credential (VC)* which is additionally tamper-resistant. Verifiable Credentials Data Model v1.1 [138] is an open standard of digital credentials format that ensures that credentials are cryptographically secure, privacy-respecting, and machine-verifiable. Also, credentials can be presented by digital certificates. For example, the European digital identity framework eIDAS defines the following types of credentials: (*i*) certificate for electronic signature (Article 3(14)) to link electronic signature validation data to a natural person; (*ii*) certificate for electronic seal (Article 3(29)) links electronic seal validation data to a legal person; (*iii*) certificate for website authentication (Article 3(38)) to authenticate a website and link the website to the natural or legal person to whom the certificate is issued.

Certificates are essential for secure communication across different layers of the OSI model of system communication within the network[7]. TLS certificates authenticate parties and encrypt data at the transport layer. Digital seals/signatures protect data integrity and authenticity at the presentation layer. End-user certificates can provide additional encryption at the application layer. The combination of these certificates ensures a secure and reliable communication channel.

Organisational Digital Identity (ODI)[8] defines an organisation and its attributes for other entities through credentials. It enables trust between business partners and ensures the authenticity and confidentiality of cross-organisational data exchanges [140]. ODI commonly relies on conventional centrally managed credentials and keys used in Public Key Infrastructure (PKI).

While different documents can play the role of (verifiable) credentials, each credential is characterised by an identifier. Such identifiers have been based on the public key infrastructure (PKI), where certificates are credentials issued by centralised certification authorities. With the emergence of self-sovereign identity (SSI), the idea of removing a centrally governed authority is gaining popularity as it allows removing a single point of failure and potentially bringing automation to the issuance of the credentials.

Conventional Public Key Infrastructure. Public Key Infrastructure using the X.509 standard (PKIX) is the most used conventional PKI implementation [141]. In the case of conventional PKI, there should be a root authority that accredits trusted third-party certification authorities (CAs). Additionally, each CA holds a (centralised) certificate registry. CAs follow X.509 standard [142] for issuing digital certificates by publicly trusted CAs. However, while the whole infrastructure is based on the CA's trust, compromising it or its registry of certificated negates the whole trust model. From the technical point of view, using a set of trusted

[7]OSI model "is a conceptual model that divides network communication and interoperability into seven abstract layers" [139]

[8]If not specified otherwise, we also use *identity* to refer to ODI.

certification authorities puts obligations on integration with each CA's system to verify credentials.

Decentralised Public Key Infrastructure. The main advantages of the decentralised PKI are based on decentralised identifiers (DIDs), which are permanent, resolvable, and cryptographically verifiable. Unlike X.509 certificate trees that rely on centralised registries under the control of a single authority, DIDs must help avoid single points of failure by using decentralised networks (i.e., verifiable data registry) for storage. A *verifiable data registry* (VDR) is commonly implemented using distributed ledger technology (DLT). Such DLT can be presented by general-purpose public blockchain networks or special-purpose distributed ledger networks. In principle, VDR can be implemented as distributed file systems (e.g., IPFS), key event logs (e.g., KERI), and distributed hash tables, but in this paper, we focus only on VDRs based on DLT.

A Decentralised Identifier (DID) identifies the subject. The DID subject can be a human, organisation or any resource that should be identified. An entity that has the capability to change the information associated with a DID and use it in a VC is called a *DID controller*. DID controller and DID subject may or may not be the same entities. *DID document* is an artefact of DID resolution controlled by the DID controller that is used to describe the DID subject [52]. A DID document itself is not a resource, therefore, it does not have a separate resource identifier. *Resolution* of DID refers to the transformation of the given DID to a DID document using the defined DID method. Regardless of the nature of the subject, the DID document is dynamically constructed by the *DID resolver* based on the provided DID and the transactions connected to this DID in the VDR. DIDs are globally unique, and no central authority manages them. The controller creates the DID on its own and has complete control over the data that can be accessed using the identifier.

Digital wallet stores the holder's credentials. A *digital agent* is a software that enables the credentials holder to operate their digital wallet. Additionally, digital agents establish secure connections with other agents to exchange credentials and DIDs. Commonly, the digital wallet is a part of a digital agent that enables secure storage of credentials. While digital agents may vary by their type (mobile and cloud), the interoperability on the client layer allows holders to select the preferred agent regardless of which agents are used by other entities or which registry is used for storing credentials. Finally, a digital agent allows the VC holder to define *Verifiable Presentations* (VP). VP is a data artefact containing data from one or more VCs shared with a verifier. VP may allow a holder to present a claim in a synthesised form instead of the original VC (e.g., through zero-knowledge proofs) to preserve the holder's privacy.

While Identity Management and Access Management systems are tightly connected, in this thesis, we mainly focus on identification and do not consider what kind of resources are protected and exchanged based on authentication. Thus, in the further chapters, we analyse how, based on the selected trust model (which

serves as the foundational assumption for information security and privacy management), the other variable component of the IdM system supports information security.

2.3.3. IdM System Characteristics

Kim Cameron, being a pioneer in the field of digital identity, in [136] proposes seven laws of digital identity. By following these principles, developers and organisations can create identity solutions that empower identities while protecting their interests. The laws with their description are the following:

1. *User Control and Consent*: Identity systems should disclose information about a user solely with their explicit permission;
2. *Minimal Disclosure for a Constrained Use*: The system should reveal the minimum amount of identifying data requisite for a particular purpose;
3. *Justifiable Parties*: Only entities possessing a legitimate requirement for the information should be granted access to it;
4. *Directed Identity*: Users should retain control over the utilisation and disclosure of their identity;
5. *Pluralism of Operators and Technologies*: The identity ecosystem should support multiple providers and technologies;
6. *Human Integration*: Identity systems must be designed with human needs and experiences;
7. *Consistent Experience Across Contexts*: Users should encounter a seamless and uniform identity experience across different settings.

Digital identity enables participants of the data exchange systems to confirm the authenticity of involved entities. Credentials associated with identities are the documents enabling the verification, with issuance procedures determined by a trust model. While the procedures of issuing credentials in decentralised and centralised identity models vary [60], PKI stays essentially the same. Thus, the key management is equally relevant regardless of the trust and identity model. Therefore to study the security of an ODI and Identity Management (IdM) system, we consider characteristics targeted by identity and key management mechanisms. The need for the characteristics depends on the scenario.

Targeted System Characteristics. Through the literature review, we gather a set of non-functional characteristics that affect ODI's security. In [132], we describe the literature procedure and provide a mapping of system characteristics reviewed in Section 2.3.4 mechanisms.

The following business-oriented characteristics may be targeted, primarily reflecting the trust among the individual business entities. *Trustlessness* is a part of the zero trust (ZT) paradigm and refers to the ability of the system to operate without relying on the honest behaviour of internal or external entities [143, 58]. To react to the dishonest behaviour, the IdM system may target to deliver *traceability*

that refers to the ability to know who did what, when, and how [144, 145]. The more proactive approach to secure the system against internal attacks is *privilege escalation prevention*, which aims to restrict users from gaining unauthorised access. In this research, we consider privilege escalation as a result of both privilege escalation attacks and privilege misuse. Another way of enabling zero trust is *decentralisation*, which refers to distributing the responsibility for managing ODI and its keys across multiple entities to enhance security, resilience, and user control. As a result, the organisation can differentiate between *multiple users* of the ODI. Another business-demanded aspect of its system's security is *availability*, which is the ability to deliver its value continuously. System availability [145] is crucial both in the everyday data exchange and in the case of extraordinary trigger events – e.g., a loss of access to the keys or if an employee that is involved in the ODI management leaves or becomes malicious. Finally, the *usability* refers to the feasibility and convenience of the identity and key management. Usability encompasses the backwards compatibility of the proposed design with the existing infrastructure. Besides, usability defines whether the end-users will use the ODI following the defined interaction set-up with ODI [143, 145, 146].

From a cryptographic standpoint, digital signatures are the principal method for establishing data authenticity and integrity. The following are the classical target characteristics. *Unforgeability* ensures that a valid signature cannot be generated by an unauthorised entity without possessing the private key [144, 147]. Assuming the private key is been compromised, a digital signature provides *non-repudiation* – the holder of the private key cannot deny the origin of a valid signature. For commonly used signing schemes, such as the Elliptic Curve Digital Signature Algorithm (ECDSA [148]) or Rivest-Shamir-Adleman (RSA), signatures generated using the same private key are interconnected via the single public key that verifies them. This *linkability* of signatures or keys determines whether two or more signatures or public keys originate from the same identity [144, 149]. The option to link different signatures may or may not be desired. Consequently, unforgeability, non-repudiation and linkability contribute to the authenticity and integrity of exchanged data.

2.3.4. Key Management Mechanisms

Assuming that IdM relies on PKI, key management is an enabler of digital identity per se and ensures the security of IdM systems. The key management includes pre-operational, operational, post-operational and destroyed phases [150]. IdM is involved in the four stages: (*i*) generation and distribution of asymmetric key pairs (i.e., private and public keys) for the key generation during the pre-operational phase; (*ii*) the key registration and the public key certification during the pre-operational phase; and (*iii*) storage, usage and backup of keys during the operational phase. The certification is crucial for establishing trust within the system as it enables verification of the integrity of the exchanged data. Our research

aims to comply with the existing verification process to remain IdM backwards compatible. Thus, we exclude the second stage from our analysis. Figure 9 depicts artefacts used for key management that are discussed in this section.

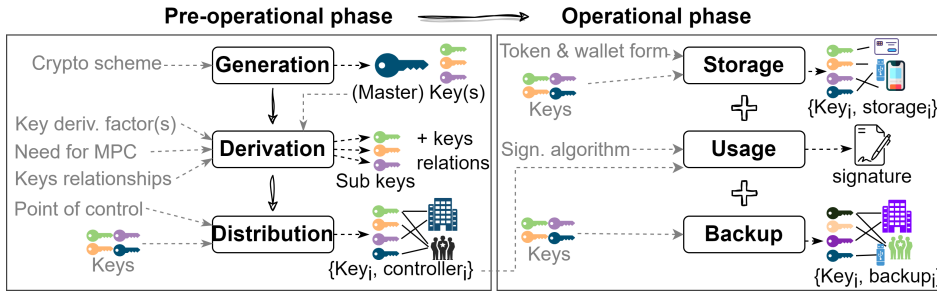


Figure 9: Key management phases: stages, parameters and artefacts [62]

Here, we overview the cryptographic and business mechanisms found through the literature review, details of which can be found in [132]. The paper focuses on asymmetric cryptographic schemes that provide digital signatures.

Pre-operational Key Phase

Key generation. Implementation of digital signature schemes necessitates the generation of a master key pair. The signature schemes vary in key and signature size, underlying mathematical structures, computational demands, and security assumptions. Irrespective of the scheme employed, the key pair generation process relies on a cryptographically secure pseudorandom number generator, which requires seed initialisation. Seed derivation from user-provided input, such as a password, is possible via a password-based key derivation function, albeit with potential security implications. Multi-factor key derivation functions [151] can be implemented to enhance trustlessness and resilience by mitigating reliance on single points of failure. Distributed Key Generation (DKG) protocols, such as FROST [152], enable multiple parties to collaboratively generate secret shares of a key in a distributed manner, ensuring that the complete key never exists at a single location. Following generation, a digital certificate can be issued to bind the master public key to a designated entity.

Sub-keys derivation. Data signing can be performed using the master private key or through sub-keys derived therefrom. Bitcoin Improvement Proposal No. 32 (BIP32) [153] specifies deterministic key derivation, wherein sub-keys are generated via a derivation path from the master key. This path is also a required input for the signature verification algorithm. Deterministic derivation is applicable to specific schemes based on elliptic curves, as employed in Bitcoin, or lattices [154].

An alternative approach is threshold signatures. It requires a minimum of K signers out of N total participants to collaborate in generating a valid signature. This mechanism requires the compromise of at least K signers by an attacker to forge a valid signature. The key shares can be derived using Distributed Key Generation (DKG) protocols, such as FROST [152], or distributed by a trusted

dealer, as exemplified in RSA-based threshold signature schemes [155].

Key distribution. The key distribution phase establishes a control point for ODI keys and their delivery to controllers. The degree of control is determined by the custody level of the keys. A non-custodial, or self-custodial, approach [156] confers increased control but imposes a higher operational burden, as the ODI owner assumes controller responsibilities, including key security.

Instead, a fully outsourced, or custodial, approach [143] reduces operational overhead for the ODI owner while waiving control. Custodial ODI directly contradicts the Zero Trust (ZT) strategy by placing complete trust in a third-party custodian. The custodian manages the keys and retains the capability to execute operations on behalf of the organization. Consequently, neither methodology addresses trustlessness, resilience, or protection against privilege escalation.

Operational Key Phase

Key storage. Cryptographic keys are stored on tokens that facilitate their generation, protection, and management. These tokens may be implemented as software applications installed on general-purpose devices, such as those initiating signature requests, or as specialised external hardware, including Hardware Security Modules (HSMs).

Dedicated hardware devices for key storage include USB tokens, smart cards (e.g., JavaCards), and Trusted Platform Modules integrated into end-consumer devices. Hardware wallets also serve as key storage mechanisms. Notably, deterministically derived keys do not necessitate persistent storage, as they can be generated dynamically, requiring the minimum threshold of factors in the case of DKG. The physical form of the token impacts the portability and usability of ODI.

Key usage. Key usage includes data signing and signature verification procedures. In instances involving a single signer and a pre-generated key, the key must be accessible either directly, as with software tokens, or through a signing interface, as with dedicated hardware signing devices.

When the master key is derived, the necessary quantity of valid factors must be provided to generate the signing key. If BIP32 deterministic derivation is employed, the derivation path from the master key to the child key is also required.

Threshold signature schemes, involving multiple signers, enhance recoverability and resilience. Any quorum exceeding the threshold of signers can produce a signature using their respective key shares. The substitution of a single ODI controller with a threshold group, configured as K-out-of-N, mitigates the risk of privilege escalation. In the majority of threshold signature schemes, the participating signers' identities are not disclosed to the verifier, potentially providing signer anonymity. However, all signers remain accountable within N-out-of-N threshold groups.

Furthermore, sophisticated policies, such as time-bounded signing, can be enforced through automated signer applications. Threshold groups can be nested, exemplified by a top-level 3-out-of-3 group with two shares held by individ-

ual representatives and the remaining share managed by an automated employee signer, which activates upon signature provision from a *K*-out-of-*N* employee subgroup. These mechanisms allow the ODI owner to determine the key shareholders involved in signature generation or to enforce specific policy mandates.

Key backup. Key recovery following loss necessitates the creation of a secret key backup in a location distinct from the storage used for routine key operations. This backup storage may consist of an auxiliary HSM, a trusted execution environment dedicated to key backup [146], or a third-party custodial service. However, the latter introduces the risk of identity compromise via privilege escalation [146]. To augment security, an identity holder can implement multiparty computation and Shamir's Secret Sharing, distributing key shares among multiple custodians [146]. Multiparty computation requires key generation via DKG protocols, whereas secret sharing mandates the distribution of subsequently derived components of a single key. A predetermined minimum threshold of custodians must provide their respective key shares to the identity holder to facilitate recovery of the backed-up key [146].

To sum up, the described key management mechanisms serve as measures (`variable 3`) enabling the identity management system. Based on the assumed trust model (`variable 1`) and type of credentials (`variable 1`), the key management mechanisms together with policies (`variable 2`) allow the components of the smart solution provide the targeted assets protection level by enabling the targeted system characteristics.

2.4. Summary

In this chapter, we discussed the information security- and privacy-related challenges faced by smart solution systems in two of the most researched and developed domains, namely e-governance and e-health. The review showed the proneness of the smart solution systems to data leakages and the need to ensure the privacy of data not only from the external parties but also from the insiders (e.g., collaborating parties and employees). Additionally, we reviewed the information security and privacy models and frameworks (both academic- and industry-based). The reviewed models complement one another and are useful for summarising the domain knowledge on information security management. However, the models are too general to be used as a theoretical model for data extraction by the expert group to define the current state of factors that define the security and privacy goals and measures used for achieving them. Finally, we discussed identity management as a tool for protecting information assets from illegitimate access. We discussed the key roles that entities can play in the identification and identity management system components, their goals, and what is the role of key management in achieving these goals. Finally, we proposed a quality assessment model for the IdM system to support the expert team in checking the IdM system's ability to meet the targeted business and security objectives.

3. A FRAMEWORK FOR INFORMATION SECURITY AND PRIVACY MANAGEMENT

The background study shows that the reviewed information security models complement one another and are useful for summarising the domain knowledge on information security management. While the models explain the dependencies between aspects of information security and the recommended general flow of actions, they do not have accompanying guidelines on how these models can be instantiated to depict the state of a selected organisation. To address this gap, in previous chapter we reviewed the information security frameworks and models (see Section 2.2.1). Based on the background and considering the need for a model to analyse the state of information security and privacy management on smart systems, we developed a new framework for information security and privacy management.

This chapter is based on [26] and contains sentences or fragments of sentences from this publication. Here, we present the motivation, development and application of a framework for information security and privacy management in organisations involved in the delivery of a cross-organisational smart solution. Thus, this chapter answers the research question $\mathbf{RQ}_1$: *How to depict the state of security and privacy management in an organisation?*

The outcome of this chapter is a framework for information security and privacy management (i.e., FISP-ProCOP), which is built based on the existing similar frameworks and models, overcoming the limitation of being a guiding method for risk management operations and depicting primarily dependencies of the operations and countermeasure type. In contrast, the proposed framework is presented in the form of a matrix and allows use as a theoretical model or template for depicting the static view of information security and privacy management in organisations.

The validation of the framework is undertaken through two empirical studies in Section 3.3 where insights gained from applying the framework in these studies are discussed. Section 3.4 explores the implications of this contribution, while Section 3.5 reviews the related work, leading to the conclusion in Section 3.6.

3.1. Framework Development

The literature review on information security and privacy management within Intelligent Transportation Systems (ITS), eHealth and eGov indicates that the proposed measures for ensuring information security range from specific data transfer protocols and system architectures to the establishment of new stakeholder roles and adherence to security-related standards. Therefore, to comprehend the overall approach of organisations towards managing information security and privacy, it is essential to recognise that information security is a multidisciplinary

field. Consequently, understanding how organisations address this issue necessitates consideration of multiple facets of the organisations involved in information security and privacy management.

Models and frameworks serve as abstract representations of concepts and their relationships within a given domain, thereby facilitating a unified understanding of that domain. Consequently, these models and frameworks are intended to assist in comprehending information security and privacy. Security frameworks come in various forms, offering either descriptive overviews of the security state (like ISACA's BMIS) or prescriptive guidance for improving it (like NIST CSF). In our study, as we aim to understand the static view, we utilise descriptive information security and privacy management models and frameworks as the theoretical foundation for data extraction.

The reviewed models complement each other and are valuable for summarising domain knowledge in information security and privacy management. However, they are too general to serve as theoretical models for data extraction in empirical studies of ITS. While these models explain the interdependencies among various aspects of information security, they lack specific guidelines on how they can be implemented to represent the conditions of a particular organisation. Therefore, drawing upon the information security frameworks and models reviewed and recognising the necessity for a framework to analyse the state of information security and privacy management in smart systems, we formulate a new framework termed the Framework for Information Security and Privacy Management (i.e., FISP-ProCOP).

3.2. Framework Description

The proposed framework is presented in Table 2 and is built upon the BMIS, McCube, and RMIAS models. Given the direct relationship between ensuring the privacy of users' data and securing it (e.g., in accordance with GDPR), our study views information security management and privacy management as closely interconnected tasks. Therefore, the proposed framework does not distinguish between context attributes that affect only privacy or security without influencing the other.

The FISP depicts four key aspects, i.e., *dimensions*, that, from the business point of view, affect the management of information security and privacy assurance – ***Pro****cesses*, *security and privacy* ***C****ountermeasures*, ***O****rganisation*, and ***P****eople* (ProCOP). Each dimension consists of multiple categories, which are divided by the attributes. Finally, each attribute may have one or more instances of such attribute that correspond to the instantiation of the model to the selected context of the smart system used in an organisation.

Table 3 depicts the source of the FISP-ProCOP categories and attributed by mapping them to concepts depicted in the BMIS, McCube, and RMIAS models. Thus, we can see that while the selected models overlap in the concept coverage,

Table 2: FISP-ProCOP: Framework for information security and privacy management (adapted from [26])

Dimension	Category	#	Attribute
P. People	PA. Actors	1	Actors, stakeholders, entities
		2	Goals, tasks, motives
	PR. Relationships	3	Relationships and dependencies between actors
O. Organisation	OS. Strategy	4	Purpose for the system usage, org. design & strategy
		5	Challenges to address
	OC. Formal Constraints	6	Legislation, regulation, standard
	OI. Information Involved	7	Type of information used
		8	How the information is manipulated
		9	Security criteria
		10	Privacy objectives
C. Sec. & Privacy Countermeasures	CP. Policies & Practices	11	Policies & practices
	CE. Training & Education	12	Training & education
	CT. Technology	13	Architectural measures
		14	Use case-oriented technological measures
		15	Cryptographic building blocks
		16	Others technological measures
Pr. Processes	PrL. System Lifecycle	17	Security as a part of the system lifecycle
	PrU. Usage of the System	18	Use cases of the system as a part of the business processes

they differ by the level of granularity. Aiming to address $\mathbf{RQ}_1$, the final version of the FISP-ProCOP matrix has the highest level of granularity among the three other selected models as it has additional attributes and some of the attributes from the original models are extended to depict cross-organisational collaboration within a smart system.

- The dimension of *People* aims to answer the question: what are the stakeholders (including physical and legal entities) that have an interest or are involved in the smart system lifecycle (design, developments, support, or usage)? Thus, the category *Actor* describes (*i*) who the stakeholders are (including internal and external) and (*ii*) which goals, tasks, and motives they have towards the system. Another category of *Relationships* depicts the relationships and dependencies between the identified actors.
- The dimension of *Organisation* aims to answer the question: what are the business goals that guide and restrict the system? The category of *Strategy* describes the internal organisational constraints: (*i*) the purpose for the system usage, and (*ii*) the existing challenges faced by the organisation. The category of *Formal constraints* describes the goals that affect the system and are set up by the external entities – through (*i*) legislation and regulations and (*ii*) standards. The category of *Information involved* describes the goals of manipulating information in the context of the other two categories, namely strategy and formal constraints: (*i*) the expected types of information to be manipulated with, (*ii*) how such information is manipulated (e.g., based on which data), (*iii*) the security criteria to be achieved for the information assets, and (*iv*) the privacy objectives to be achieved for the information assets.

FISP-ProCOP				BMIS		McCube		RMIAS	
Dimension	**Category**	**Attribute**	**New attributes**	**Coverage**	**Original attribute**	**Coverage**	**Original attribute**	**Coverage**	**Original attribute**
P. **People**	PA	Actors, stakeholders, entities	Ext.	◑	People*, Culture	○	-	◑	Sec. Countermeasures [human-oriented]*
		Goals, tasks, motives	Added					○	-
	PR	Relationships and dependencies between actors	Added					○	-
O. **Organisation**	OS	Purpose for the system usage, org. design & strategy	Added	●	Organisation, Governing	○	-	○	-
		Challenges to address	Added		Organisation,	○	-	○	-
	OC	Legislation, regulation, standard			Governing	○	-	●	Sec.
	OI	Type of information used			Organisation	○		●	Information Taxonomy
		How the information is manipulated				●	Information		
		Security criteria				●	Information Characteristics	●	Security Goals
		Privacy objectives	Added			○	-	○	-
C. **Sec. & Privacy Countermeasures**	CP	Policies & practices	Ext.	◑	Culture*, Human Factors*, Emergence, Enabling & Support	●	Security Countermeasures	●	Sec. Countermeasures [organisational]
	CE	Training & education	Ext.	◑	Human Factors*	●		◑	Sec. Countermeasures [human-oriented]*
	CT	Architectural measures	Ext.	●	Architecture	●		●	Sec. Countermeasures [technical]
		Use case-oriented technological measures	Added	●	Technology				
		Cryptographic building blocks	Added						
		Others technological measures	Added						
Pr. **Processes**	PrL	Security as a part of the system lifecycle		◑	Culture	○	-	●	Sec. Dev. Lifecycle
	PrU	Use cases of the system as a part of the business processes	Ext.	◑	Enabling & Support*	○	-	○	-

* - considers only internal context (internal actors, system components, trainings, etc.)

○ - does not cover; ◑ - covers partially; ● - fully covers Ext. - extended with external context Added - a new attrubute

Table 3: Mapping FISP-ProCOP with BMIS, McCube, RMIAS

- The dimension of *Security & Privacy countermeasures* aims to answer the question: which measures are used to ensure information security and data privacy in the context of People and Organisation dimensions? The measures in the dimension are divided into three categories. The category of *Policies & practices* describes the policies and practices in the organisation that enable achieving the goals from the Organisation dimension, including the existence of written policies on InfoSec&Privacy management, training and practices established internally in the organisation and externally with the relevant actors. The category of *Training & education* describes the educational practices used in the organisation for the identified internal and external actors of the smart system. The category *Technology* describes the technological solutions that enable ensuring information security and data privacy. The category consists of four attributes: (*i*) architectural solutions, (*ii*) use case-oriented technological measures, (*iii*) cryptographic measures used, and (*iv*) any other technological solutions (e.g., technologies, protocols, tools) which do not fall under the other attributes and support the security and privacy objectives. The technological countermeasures in all the four categories should cover both architecture of the organisation's own system and the architecture established in a smart solution through integration with external systems.

- The dimension *Processes* aims to answer the question: how the dimensions of People, Organisation, and Countermeasures are integrated together in the processes in the organisation? The category of *Usage of the system* describes the use cases of the system as a part of the business processes of a smart solution. Meanwhile, the category of *System lifecycle* describes how the security and privacy countermeasures are incorporated into the system lifecycle (e.g., either the security and privacy countermeasures are once implemented and never updated or they are regularly reassessed through a risk management framework and updated if needed). The attributes in the Process dimension include processes established both within the organisation itself, collaborative business processes and system maintenance practices established between partners contributing to a smart system.

The expert group can use the framework in two stages as depicted in Figure 10. The first stage involves all the actors from the expert group in the motivation scenario (Section 1.1). Each expert specifies attributes in the FISP-ProCOP matrix. The second stage may be conducted by the whole expert group together and aims to merge experts' matrices and identify requirements for a securing smart solution.

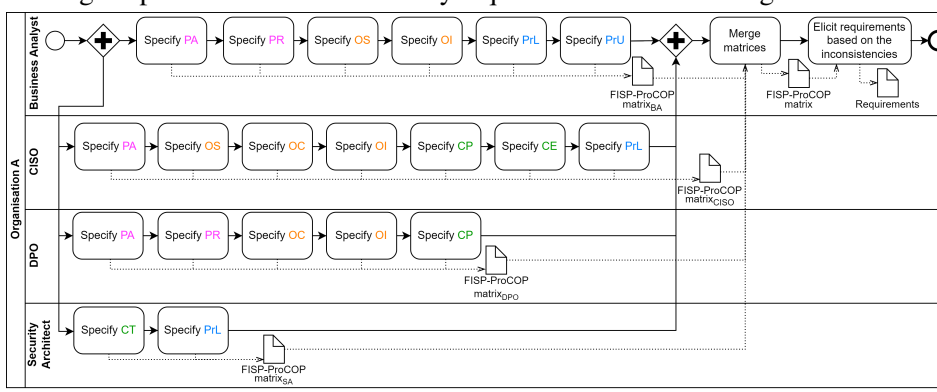


Figure 10: Process of using FISP-ProCOP

1. **Specify FISP-ProCOP attributes.** The framework's matrix can be used as a template for aggregating information about the aspects affecting information security and privacy in the organisation dealing with a smart system.
    - A business analyst should provide input on the business needs-related categories, such as PA (Actors), PR (Relationships), OS (Strategy), OI (Information Involved), PrL (System Lifecycle), and PrU (Usage of the System).
    - A data protection officer (DPO) should primarily contribute to filling in instances of attributes in the categories related to data protection regulations and their implications to the organisation and system, such as PA (Actors), and PR (Relationships, specifying whose data is considered sensitive and with which actors it may or may not be shared), OC (Formal Constraints), OI (Information Involved, specifying the

sensitive information to be protected and its privacy objectives), CP (Policies & Practices).

- A chief information security officer (CISO) should provide information on cybersecurity vision, strategy, policies and procedures [25]. Therefore, CISO is expected to contribute to filling in the attributes in the categories of PA (Actors, specifying cybersecurity-related authorities), OS (Strategy) and OC (Formal Constraints, addressing the security-related organisational strategies, legislation and standards), OI (Information Involved, defining security objectives), CP (Policies & Practices, elaborating on the existing security policies, including but not limited to the followed standards, frameworks and certifications), CE (Training & Education, elaborating on the existing security training), PrL (System Lifecycle, specifying how security risk management is integrated into the system lifecycle).
- A security architect oversees the secure development, integration, and maintenance of cybersecurity components [25]. Thus, they should provide information to PrL (System Lifecycle, specifying how security risk management is integrated into the system lifecycle) and fill in the last category, namely CT (Technology).

2. **Merge matrices and elicit requirements for information security and privacy management.** Although FISP-ProCOP is not designed to depict dependencies between the attributes, the matrix may be structured or filtered out after the first stage in a way that reflects which instances of one attribute are related to instances in the other attributes. Thereby, an organisation representative (e.g., CISO) may validate the consistency of information security and privacy management aspects in the organisation. To identify the inconsistencies within the created matrix, the expert group may use the guiding questions depicted in Table 18. The guiding questions help compare attributes and define the inconsistencies among attributes which serve as a ground for new requirements for information security and privacy management. Thus, the framework allows the identification of conflict stemming from multiple stakeholders and operation areas within an organisation, while conflict resolution is out of the scope of the framework itself.

While FISP-ProCOP is presented in the form of a matrix, it does not depict relationships between dimensions, categories, and attributes, for instance, in contrast to RMIAS. On the other hand, due to the tabular structure, our hypothesis is that the model is a useful tool for depicting the static view of information security and privacy management in the complex information system compared to other reviewed frameworks and models. The UML class diagram in Figure 38 shows the relationships between the FISP-ProCOP attributes and their relations to the data objects used within the presented later thesis contributions.

Additionally, the assumption is that such a representation of dimensions that affect information security and privacy in the system can help depict the effect of attributes on one another by considering measures usage from multiple perspectives. As a result, FISP-ProCOP should help to cross-validate the assumption of the direct effect of some security and privacy countermeasures on meeting the stated organisational goals (e.g., stated by the standard).

3.3. Framework Evaluation

We evaluate the correctness and usability of the framework through two studies. Both studies aim to define how information security and privacy are managed in organisations enabling intelligent transportation systems (ITSs). First, to validate the correctness, we conduct a literature review using FISP-ProCOP to define state-of-the-art aspects and measures for smart transportation systems. Second, survey-based analysis of operational passenger ITSs in the selected regions of the European Union offers insights into real-world ITS implementations, allowing for a comparison with the proposed state-of-the-art measures.

3.3.1. Study 1: State-of-the-Art Measures for ITSs

During the first evaluation study, we aim to validate the correctness of the framework by checking its ability to depict the recommended state by the research community (i.e., state-of-the-art) of security and privacy management measures for the organisations involved in enabling intelligent transportation systems. For this, we conduct the literature review where the proposed FISP-ProCOP is used as a theoretical model for the data extraction from the selected sources. While the detailed procedure of the literature review and its results are documented in our previous publications in [26] and [157], here we describe the general study set-up and results.

Study Set-up. The state-of-the-art measures are identified through the literature review (LR) following the guidelines in [158]. The literature search was conducted using Scopus, ACM Digital Library, and Web of Science databases. These databases were chosen because they include peer-reviewed papers and support the use of complex search queries with logical expressions.

For the literature review, we used the following query: ((“security” OR “privacy protection” OR “data protection”) AND (“technologies” OR “measure”)) AND (`Industry_name`), where instead of `Industry_name`, we use “vehicle sharing”, “ride-hailing”, “smart parking”, “toll”, “connected vehicles” and their synonyms. The search strategy resulted in 283 papers found.

Using the inclusion and exclusion criteria, 24 papers were selected for the data extraction. Table 4 contains the paper selected for further data extraction grouped by the ITS area.

Results. The first version of the FISP-ProCOP matrix has been developed based on the concepts and categories depicted by BMIS, McCube, and RMIAS

Table 4: Study 1 - Selected papers for data extraction (adapted from [26])

ITS area	Selected for the data extraction papers
Smart Parking	[159], [160], [161], [68], [75], [69], [67], [162], [163], [74], [164], [165], [76]
Ride-Sharing	[73], [166]
Connected Vehicles	[167], [168]
Toll Collection	[161], [169], [170], [78], [77], [171]

models. However, as depicted in Table 3, some of the concepts (like "organisation" in BMIS) are too wide, and some do not consider the external entities, systems, or activities as the ones affecting the organisation's information security and privacy.

Therefore, to depict the specific factors of cross-organisational collaboration in smart systems, FISP-ProCOP is extended with the new attributes. The new attributes are extracted based on the literature review in Study 1 by defining concepts which the original FISP-ProCOP does not cover or covers partially. As shown in Table 3, we have added 8 attributes compared to BMIS, McCube, and RMIAS models. Additionally, 5 attributes were extended by specifying in their description the need for considering external entities (actors, systems, policies, processes) which affect the organisational information security and privacy management through smart solution collaboration.

The FISP-ProCOP usage during the data extraction results in an overview of the state-of-the-art aspects of managing security and privacy in intelligent transportation systems. The result is a matrix that depicts the state-of-the-art technological countermeasure used to assure security and privacy in the selected ITS areas (see Table 5) along with the mentioned actors involved in the ITS, organisational objectives and constraints, and existing processes that affect security and privacy management of the ITS (see Table 6). In this work, the results are split into two separate matrices only for the reason of fitting them into the page.

When presenting the review results, any omitted dimensions or attributes indicate that we did not find corresponding data in the selected literature. Additionally, we do not include architectural or technical measures that primarily provide the main system functionality and do not represent information security or privacy measures in ITS.

The literature review shows that within ITSs, the information assets to be protected are related to the information about a vehicle, driver and passenger, and transportation service usage. For example, in systems for smart parking, ride-sharing and vehicle-to-vehicle communication, the confidentiality of passenger's/driver's data is of primary security concern, along with assuring the availability and integrity of parking slots usage data. Therefore, the state-of-the-art measure for ITSs security management includes mitigating threats that negate the integrity of the parking slots payments status [75] to enable public verifiability (e.g., by the parking officer), which can be abused by the driver's motive for pay-

Table 5: Study 1 - State-of-the-Art technological countermeasures (adapted from [26])

Attribute		**Attribute instances**			
Architectural		Blockchain-based system	Anonymous authenti- cation	Storage of sensitive personal data on the data subject device	
		Secret- sharing	Multi-party computation (MPC)	Securing data in transit	
Use case-oriented	Authentication & Access control	Anonymous credential system	Attribute- based credentials and access control	RFID authentication	Pseudo- random identity assignment
		Biometric- based authentication			
	Secure communication	TLS protocol	IPSec protocol	VPN solution	Other secured communica- tion protocol
		Customer end-to-end encryption		Custom asymmetric encryption	
	Navigation and routing	Privacy- preserving navigation systems		Location obfuscation	
	Payment	Automated payment using smart contract		Anonymous payment	
	Location- based search	Hashmap storing of parking slot/ toll/ vehicle locations		Location- based search	Search based on the exact location
	Pass document creation	Blind signature	Anonymous reservation	Presenting proof-of- knowledge	
Cryptographic		RSA digital signature	Homomor- phic encryption	Zero- Knowledge Proof	Oblivious pseudo- random function (OPRF)
		Trusted execution environment (TEE)	Private set intersection (PSI)	Blind signature	Elliptic curve cryptography
		Diffie-Hellman group key exchange	Hash-based message authentication codes	Oblivious transfer protocol	

ment avoidance (e.g., harvesting attack). A significant amount of studies also aim to mitigate the threats to negating the confidentiality of passengers' or drivers' personal data caused by the storage of such data in a centralised manner by the service providers. Additionally, the reviewed studies aim to mitigate the threat of violating passengers' or drivers' privacy by linking the data instances of service usage or payment history. More details on motives and level of trust in the actors (which are mentioned in Table 6), along with other security threats the reviewed papers aim to mitigate, can be found in the supplementary report in [157].

Lessons Learnt. Through this study, we extended the framework and evaluated the correctness of the defined attributes as a tool for data extraction by the thesis author. Additionally, as a result of this study, the framework was extended with the category of OS (Strategy), and the categories for some attributes were redefined.

Table 6: Study 1 - State-of-the-Art attributes: people, processes and organisation dimensions (adapted from [26])

Dimension & Attribute		**Attribute instances**			
People	Actor	Driver	Passenger	City Government	Trusted Authority
		Time-stamping authority	Organisation employee	Parking Service Provider	SLA-based System provider
Organisation	Purpose of ITS usage	Decrease the traffic congestion	Resolve the problem of air pollution	Improve of the city services	Improve parking facilities management
		Optimise driver's time spent on parking	Optimise parking spaces usage	Prevent unauthorized spots occupation	Enable on-demand mobility
	Challenges	Absence or lack of industry regulations and/or standards		The balance between privacy and system efficiency	
		Interoperability with other systems and/or providers		Heterogeneous network	Data minimisation principle
		Prevention of data leakage through data privacy and security of users' data		Providing the expected level of system security before the system is launched	
		High expectations from such system quality characteristics (e.g., platform independence, OS independence		Absence of national strategy for smart environments	Resource-constrained devices usage
	Legislation & regulations	General Data Protection Regulation (EU GDPR)	European Union directive 2010/40/EU (7 July 2010)	Consumer protection directives 2019/770 and 2019/771	UNECE regulation No 155 (from 2020)
	Standards	ISO/IEC 27001	ISO/IEC 27002	ETSI standards series	NIST Special Publications
		Other standards from ISO/IEC 27000-series			
	Information	Passenger' transactions history		Passenger's identity	Passenger's payment details
		Driver's identity	Driver's location	Driver's transactions history	Driver's payment details
		Available parking spaces	Vehicle's identity	Vehicle's location	Available tolls
		Vehicle's state details		Parking/ Ride/ Toll transaction	
Process	System support	Intrusion detection system	Vulnerability scanner	Behavioural analytics system	Network traffic analyser
		Security incident and event management systems (SIEM)			
	ITS in the business process	Navigation/ routing	Payment	Location-based search	Pass/Reservation document creation

Study 1 shows that in contrast to the reviewed frameworks, FISP-ProCOP offers higher granularity, making it more suitable for our study's objective of defining the static condition of information security and privacy management. Moreover, it covers not only the internal entities and measures used within the organ-

isation to manage security and privacy, but it also highlights the need for depicting external actors, systems and architectures which affect data exchanged within smart systems.

The main limitations of Study 1 are selection and interpretation bias that poses a threat to the internal validity of the study. In order to reduce the effects of these threats, we adhere to the guidelines for literature review in [158]. Thereby, the results of Study 1 evaluation of the FISP-ProCOP correctness are not affected by the mentioned limitations. Meanwhile, these threats to internal validity affect the extracted through the literature review security and privacy management measures as the measures might not present a full set of measures.

3.3.2. Study 2: Security and Privacy Management in the Running ITSs

The second study aims to evaluate the usability of the proposed framework for identifying the state of security and privacy management in organisations operating with intelligent transportation systems in selected European regions. Having the data extracted from the literature review during Study 1, we use it as a baseline for identifying the organisations' situation. Thus, Study 2 is a case study during which we surveyed targeted expert group representatives of organisations in the intelligent transportation sector using a FISP-ProCOP-based questionnaire to assess their information security and privacy management.

Study Set-up. This study has started with the development of a questionnaire as a tool for the data extraction. The questionnaire [172] is developed based on the technologies and measures identified in Study 1. We use Google Forms[9] to deliver the survey to respondents as it enables branching in the questionnaire depending on the answers, making it easier for respondents to navigate.

The questionnaire includes questions related to general information about the company and its intelligent transportation system. The rest of the questionnaire is organised in four parts and roughly aligned to the four dimensions of FISP-ProCOP. The questionnaire ends with a section of follow-up questions about the survey and practices used for communicating security and privacy measures to stakeholders (e.g., *Which sources did you use to answer this survey?*, *How easy was it for you to find the information asked in this survey?*). Most of the questions are multiple-choice questions where the options are the instances of attributes defined whether from the previous study or extended by the thesis author based on the industry standards or results from the literature on InfoSec & PM. The shortened version of the questionnaire and the mapping of questions with the framework's dimensions and attributes can be found in Appendix B. Four attributes, primarily related to actor relationships (PR.), information manipulation processes (OI. category), and the specification of security criteria and privacy objectives, were excluded from the questionnaire to minimise respondent burden and data

[9] `https://docs.google.com/`

sensitivity. While these attributes would have provided a more comprehensive view for subsequent analysis, their inclusion could have hindered data collection and compromised participant engagement.

As the population of this study, we select the organisations contributing to intelligent transportation systems in two selected regions – (*i*) Estonia and (*ii*) South Moravia region in Czechia. As we show in [26], these two regions have similar economic and digital development levels, specialising in information and communications technology. Additionally, both regions have similar expertise in information security.

In this study, we target organisations that develop solutions, systems, or devices for ITS or use ready-to-use intelligent transportation systems for their operations. The targeted organisations are not aiming to create a smart solution between themselves, but instead they are contributing to separate smart solutions in the transportation domain based on the integrations with systems managed by the other organisations. The initial pool of targeted organisations consists of 29 in Estonia and 29 in South Moravia.

The respondents were neither limited in time nor restricted from using external sources or consulting with colleagues to answer the questionnaire. Thereby, the study set-up is similar to the real-life situation within which the expert group participants (from the motivation scenario in Section 1.1) would fill in data to FISP-ProCOP.

Results. With a response rate of 24 % and 27 %, the study involved representatives from 7 organisations in South Moravia and 8 in Estonia (15 organisations in total). Table 7 shows the distribution of organisations that participated in the survey by their operation area in IT. Table 8 shows the distribution of roles of organisation representatives who filled in the questionnaire on behalf of their organisation.

Table 7: Study 2 - Operation areas of intelligent transportation systems [26]

ITS Area	N_{total}*	N_{EE}*	N_{SM}*	**ITS Area**	N_{total}*	N_{EE}*	N_{SM}*
Connected vehicles	6	2	4	EV charging	2	0	2
Traffic management	6	1	5	Autonomous vehicles	3	3	0
Parking service	5	2	3	Mobility analysis	1	1	0
Vehicle-sharing	3	2	1	Other (ITC services)	1	1	0
Ride-hailing	2	2	0				
Total	$N_{total} = 15$;		$N_{EE} = 8$;	$N_{SM} = 7$,			

where $N_{total}, N_{EE}, N_{SM}$ - number of participants in both regions, in Estonia and in SM respectively;
* some organisations operate in more than one area

Based on the data provided by the respondents, we defined the matrices with instances of attributes from FISP-ProCOP for each organisation. As such data is sensitive for organisations, we do not share matrices for public access. Instead, our study aimed to depict the overall state of security and privacy management in the selected regions. Therefore, Figure 11 depicts the distribution of security and privacy management measures and aspects among the surveyed organisations.

Figure 11: Study 2 - Distribution of the usage of the attributes' instances by the surveyed organisations [26]

Dimension	Category	Attribute	Attribute instances											
P. People	PA (Actors)	PA	Time-stamping authority	Defence	Parking/Toll Officer	Trusted Authority	Passenger	Parking Service Provider	System provider	Employee	City Government	Driver		
O. Organi-sation	OS (Strategy)	OS System purpose	Safety of urban traffic	Reduced cost for goods delivery	More livable cities	Improved parking facilities	Public transport control	Decreased the traffic congestion	Improved city services	On-demand mobility				
		OS Challenges	Hetero- geneous network	Resource constrained devices	High system quality expectations	Privacy vs efficiency	User data privacy and security	Data minimisation	Expected level of security	Lack of industry regulations	Interoperability			
	OC (Formal Constraints)	OC regulations	EU 2019/2144	EU 2018/858	ITS Directive	UN R155	GDPR							
		OC standards	NIST SP	Other standards from ISO/IEC 27000-series	E-ITS	ETSI standards series	Cyber Security Act in Czechia	ISO 27001						
	OI (Information types)	OI	Information about roadside units	Other information	Information about passenger	Information about transactions	Aggregated information	Information about driver	Information about vehicle					
C. Sec. & Privacy Counter-measures	CP (Practicies & Policies)	CP	Normal best practices	Penetration testing	Threat modelling	Security Development Lifecycle	Risk management	Security framework	Security strategy					
	CE (Training & Education)	CE Trainings Employees	Reading news about security isues	Cyber hygiene trainings	Trainings for raising awareness about security threats	Data protection trainings								
		CE Sources For Survey	Documentation	Colleagues	Knowledge of the organisation	Knowledge of the system								
	CT (Technology)	CT Crypto	Homomorphic encryption	Zero- Knowledge Proof	Oblivious pseudorandom function (OPRF)	Blind signature	Oblivious transfer protocol	Trusted execution environment (TEE)	Private set intersection (PSI)	Hash-based message authent. codes	Elliptic curve cryptography	Diffie-Hellman group key exchange	RSA digital signature	
		CT Secure Communication	Custom asymmetric encryption	IPSec protocol	Other secured communication protocol	Customer end-to-end encryption	VPN solution	TLS protocol						
		CT Architectural Measures	Blockchain- based system	Multi-party computation (MPC)	Storage of anotated data	Secret-sharing	Anonymous authentication	Storage of personal data on the data subject device	Securing data in transit					
		CT Authent. & Access Control	Biometric- based authentication	Pseudo- random identity assignment	Anonymous credential system	Attribute-based credentials and access control	RFID authenti-cation	2-factor authentication	Role-based access control	Public Key Infrastructure				
		CT UC Navigation & Routing	Location obfuscation	Third-party navigation system	Privacy- preserving navigation systems									
		CT UC Payment	Anonymous payment	Automated payment using smart contract	Cash	Direct carrier billing (DCB)	Token-based payment	Card-based payment						
		CT UC Location Based Search	Private information retrieval	Hashmap storing of parking slot/toll/vehicle locations	Search based on the exact location									
		CT UC Reserv. Document Creation	Blind signature	Anonymous reservation	Presenting proof-of-knowledge									
Pr. Proc-esses	PrL (System Lifecycle)	PrL Principles for System Development	Privacy-related testing and verification	Usage of sensor devices which have built-in security measures	Data minimisation	Secure programming	Privacy by design							
		PrL System Support Networkt	Firewall	VLANs	Security incident and event management systems (SEIM)	Intrusion detection system	Behavioural analytics system	Vulnerability scanner	Network traffic analyser					
	PrU (Usage of the System)	PrU Use Cases	Pass/reservation document creation	Navigation or routing	Payment	Location-based search								

Cell colour mapping: (by number of supporting responses) 0 | 3 | 6 | 14

Text colour mapping: **measure1 (black)** - state-of-the-art measure; **measure2 (grey)** - other

Table 8: Study 2 - The role of the study participants [26]

Role	No. of respond.	Role	No. of respond.
Software Developer	2	Product Manager	3
DevOps	1	Project Manager	2
ISO	2	Process Manager	1
CTO	2	Operations Specialist	1
SysAdmin	1		

Additionally, we want to validate whether the gathered data depicts any dependencies between the use of different information security and privacy measures based on the survey results. Each survey response provided by an organisation representative is treated as a separate observation. By manual comparison of the instances of FISP-ProCOP attributes within each observation using the guiding questions in Table 17, we cross-validate for each organisation the usage of security and privacy measures across or within the same dimension.

We see the dependencies between three pairs of variables. First, for all the observations the usage of the Security Development Lifecycle (mentioned within category CP) implicates the usage of Threat Modelling(mentioned within category CP, as threat modelling is a mandatory component of the Security Development Lifecycle. Another example of cross-validation is related to the GDPR. A need to comply with GDPR is mentioned within each observation (mentioned within category OC). However, only some of them mention the usage of privacy by design or data minimisation principles (within category PrL), even though the former should implicate the latter. Thus, by manual comparison of FISP-ProCOP matrices filled in by expert group members and the final merged one, the expert group can identify the inconsistencies and, as a result, elicit requirements to be met.

Having the distribution of FISP-ProCOP attributes' instances and comparing it with the state-of-the-art security and privacy measures, we come to the following findings and conclusions:

1. There is a gap between what is proposed in the latest academic literature and what is actually used in practice for assuring information security and privacy in intelligent transportation systems. Meanwhile, neither organisations using ITS nor academic papers specify how they select measures for privacy preservation or how they compare their effectiveness. Our assumption is that practitioners are not able to assess the utility of state-of-the-art results or make an informed decision on its usefulness and impact on the ITS compared to other, more commonly used, technologies and measures. Thus, we observe a theoretical gap in the procedure for the selection and comparison of security and privacy measures.

2. All the systems in the surveyed organisations and theoretical ITS from the literature are integrated with external systems. On average, each ITS has integration with 4 external systems, which are considered in this thesis as cross-organisational data exchange. Meanwhile, the study shows that interoperability with the systems is the most common challenge faced during the ITS lifecycle. Considering that the system integration is primarily needed for ITS for gathering data from multiple data sources, such data (exchange) ecosystems [173] (also referred to as data sharing networks or data exchange platforms) as Gaia-X, X-road, UXP, or AWS Data Exchange, which enables system interoperability for the data exchange, are one of the options for building ITS around [174, 175].
3. A collaborating smart system commonly relies on some trusted party for coordination identity or identity handling. The PKI and role-based access control are the most common tools for access control to the data exchange services and securing data in transit. Meanwhile, the state-of-the-art literature questions reliance on one trusted party for security assurance due to proneness to a single point of failure. Ledger-based systems for distributing responsibilities are the commonly discussed solutions to prevent system failure and ensure system availability and traceability assurance.
4. While some of the organisations are certified with respect to ISO/IEC 27001 standard (or aim to be certified), which guides information security management, none of the respondents mentioned using the standard ISO/IEC 27701 for privacy information management system. The background check of the survey organisation also showed none of them are certified with respect to ISO/IEC 27701. Thus, we conclude that organisations operating in ITS within the survey regions are not as rigorous about privacy management as about security management. Meanwhile, based on the survey results, the assurance of user data privacy and data minimisation is another common challenge faced during the ITS lifecycle.

Lessons Learnt. Within Study 1 and Study 2, we used FISP-ProCOP as a theoretical model for the data extraction of measures for securing intelligent transportation systems. As the studies used different methods for data extraction, namely literature review and questionnaire, the fact that comparable results were obtained validates the framework's usability and adaptability.

The study shows that employees of exclusively technical positions struggle to answer questions about security and privacy-related regulations and standards. On the other hand, the results show that process, project, and product managers, to a large extent, are unaware of the ITS security and privacy level and the used technical measures. Therefore, this study validates our hypothesis about the need for the involvement of the whole expert group in documenting information security and privacy management aspects with respect to FISP-ProCOP.

Based on the evaluation studies, we developed a user guide [176] to support further usability and independent evaluation studies of the framework. The user guide includes instructions on the filling in FISP-ProCOP matrix (either manually or using the questionnaire) and usage of cross-validation questions for identifying inconsistencies across attributes of InfoSec & Privacy management.

3.4. Discussion

Both evaluation studies were conducted not in a setting of the motivation scenario – for depicting the state of security and privacy management in a selected organisation. In contrast, the first study aimed to depict the theoretical aggregated state based on the academic knowledge base. The second study was conducted in a way that only one company representative filled in the questionnaire to create the matrix representing the organisation's state. In the second study, due to the study set-up and conducting the research from the outside perspective, we did not conduct an analysis of each organisation's state but investigated only aggregated data to avoid organisational data leakage.

Nevertheless, the two studies confirmed the hypotheses that had been initially stated. First, FISP-ProCOP is able to depict a static view of the security and privacy management aspects, regardless of whether it is based on the written form data sources (like academic papers) or undocumented knowledge of the experts (extracted through questionnaires). Thereby, the studies validated the framework's usability for the information security and privacy management state and adaptability to the data extraction source. We come to the conclusion that the proposed framework should also be usable in an organisation to depict the state based on internal documentation (including manuals, guidelines, and technical documentation) and non-documented knowledge (acquired through direct data collection from the employees). Second, in planning the change of security and privacy management measures in the organisation aligned with the motivation scenario, FISP-ProCOP can assist the expert group in depicting the As-Is and To-Be matrices. The continuous update of the As-Is matrix throughout the transition project, alongside its comparison with the To-Be matrix using data analysis, provides project management with evidence of the project's progress.

Limitations. The presented evaluation studies focused on the correctness and usability of the proposed FISP-ProCOP framework. However, the usability study had a limited scope and a low number of participants. A more comprehensive evaluation, including a full case study, would further strengthen the validation of FISP-ProCOP. Future work should include the framework evaluation with the targeted user group to evaluate its effectiveness, usability, and efficiency in real-world scenarios. We have identified partnerships with a government agency (e.g., the Information System Authority in Estonia) that would enable us to conduct a more extensive evaluation in future research, similar to the collaboration during Study 2 depicted in the thesis.

3.5. Related Work

The ISO/IEC 27000-family standard is considered the main industrial standard that guides the components of the information security management system (ISMS). Having the goal of depicting the current state of the information security management system extended with the privacy management considerations, the proposed FISP-ProCOP can be used as a complementary tool to the ISO/IEC 27001 standard. In Appendix B, Table 20, we show the mapping of FISP-ProCOP attributes with the clauses in ISO/IEC 27001 [27]. The mapping reveals that 12 out of 30 clauses of the standard are directly covered by the framework's attributes. Additionally, 16 out of 30 clauses are covered not explicitly, which means that these clauses may and may not be covered by the framework depending on the usage and level of provided details. Finally, only 2 out of 30 clauses are not covered in the framework. The non-covered clauses refer to resources and competencies required to support information security management in the organisation.

Table 9 depicts the mapping of the controls from ISO/IEC 27002 [177] recommended by ISO/IEC 27001 [27]. As shown in the mapping, the dimensions 'Organisation' and 'People' of FISP-ProCOP provide the base of requirements for ISMS as prescribed by the organisational control 5.1 of ISO/IEC 27001 [27]. Meanwhile, the dimension of 'Countermeasures' is roughly equivalent to the controls proposed in ISO/IEC 27001. The category 'Policies & Practices' covers the organisational and some people controls from ISO/IEC 27001 and 27002. The category 'Training & Education' covers those people controls from ISO/IEC 27001 that require active training and raising awareness of stakeholders. The 'Technology' category of FISP-ProCOP corresponds to technological and physical controls from the standard. Finally, the categories in the dimension 'Processes' could be aligned with information security policy topics provided by the organisational control 5.1 in ISO/IEC 27001.

Table 9: Mapping of FISP-ProCOP with information security risk treatment control from ISO/IEC 27002 [177] recommended by ISO/IEC 27001 [177]

FISP-ProCOP		**Relation type**	**ISO/IEC 27002**
Dimension	Category		Control
P. People	PA., PR.	provides input to $\rightarrow$	Organisation 5.1
O. Organisation	OS., OC., OI	provides input to $\rightarrow$	Organisation 5.1
C. Security & Privacy Countermeasures	CP.	corresponds to $\leftrightarrow$	Organisational and People
	CE.	corresponds to $\leftrightarrow$	People
	CT.	corresponds to $\leftrightarrow$	Technological and Physical
P. Processes	PrL., PrU.	corresponds to $\leftrightarrow$	Policy topics from Organisation control 5.1, other Organisational

Considering that one of the goals of the expert group is to ensure that their organisation successfully enables a smart solution, the framework of the work system is a useful tool. The work system method [178] is a systems analysis method for thinking about systems in organisations. In a sense, it is the framework that defines how work gets done within an organisation. Particularly, the work system refers to the organised arrangement of people, technology, and processes within an organisation to achieve specific goals. It encompasses the entire structure and operation of a company, including its departments, roles, workflows, and the tools used to carry out tasks. The research in [178, 179] stresses that security (and, therefore, privacy) assurance is as much a component of the work system as other organisational processes. Thereby, FISP-ProCOP is aligned with a work system framework [179, 178] as we also consider security and privacy management as an integral component of an organisation and, thus, its work system.

There is the following mapping of work system components with FISP-ProCOP: *customers* and *participants* refer to the People dimension; *products and services* together with *processes and activities* refer to Processes, while the later is also addressed in the People dimension and the category CE. of Countermeasures; *information* is depicted in analogues category of the Organisational dimension (i.e., OI.); *technology* refers to CT. in the Countermeasures dimension; and finally, *environment*, *infrastructure* and *strategy* are depicted in the Organisation dimension.

Additionally, as highlighted in the empirical study in [179], organisation employees often engage in two distinct work systems simultaneously. The first system focuses on achieving operational objectives through task performance. The second system centres on maintaining security and privacy, which may involve specific activities or guidelines (e.g., prescribed by the legislation, organisation strategy or standard). The activities in the second system can be perceived as hindering the pursuit of business goals within primary responsibilities. Therefore, as we have shown in Study 2, the expert group should cross-validate that the fact of having the attributes in one dimension of FISP-ProCOP corresponds to it being addressed by countermeasures in other framework dimensions for the organisation's matrix instance. Thereby, FISP-ProCOP allows the expert group to make sure that both working systems (operational objectives-oriented and security-oriented) work harmoniously.

Thereby, the proposed FISP-ProCOP stands as a bridge between the organisational point of view and technical view on information security and privacy assurance. On one hand, the framework is aligned with the work system perspective, defining the key aspects of an organisation through which value to end users of smart solutions is created. On the other hand, FISP-ProCOP is built based on the reference models of information security [30, 29, 28] and is aligned with the worldwide used ISO/IEC 27001 and ISO/IEC 27002 standards.

3.6. Summary

In this chapter, we answered $\mathbf{RQ}_1$: how to depict the state of security and privacy management in an organisation? For this, we developed FISP-ProCOP – a framework for information security and privacy management – as a tool for depicting aspects and measures used in organisations to ensure security and privacy management. We validated the framework through two evaluation studies in the context of intelligent transportation systems. The studies confirmed the correctness and usability of the framework for depicting the measure based on both written documents and based on the experts' knowledge.

Additionally, the studies revealed a number of challenges for the organisations involved in the operation of intelligent transportation systems. Based on our results, the assurance of user data privacy is one of the challenges faced during the ITS lifecycle. Meanwhile, none of the respondents mentioned using the standard ISO/IEC 27701 for privacy information management systems. Our assumption is that, first, companies are not yet motivated by the market to formally prove privacy assurance and, second, lack a usable procedure to integrate into their system management lifecycle to approach privacy management systems systematically. Therefore, in the next chapter, we propose a method for privacy analysis which helps to comply with local privacy regulations in the EU and assess the efficiency of the used privacy and security preserving measures. Afterwards, considering the tendency of centralised or outsourced control over identities in ITS, in Chapter 5 we address the problem of centralised control over organisational identity for protecting the exchanged sensitive data to assure data privacy.

Third, on average, each ITS has integration with four external systems, and there is a need to achieve interoperability between such systems. Therefore, in Chapter 5, we focus on data exchange systems (e.g., X-Road) as enablers of system interoperability for smart solutions as they may address the challenge of achieving interoperability between built-as-stand-alone information systems.

Finally, the study showed that public key infrastructure (PKI), together with role-based access control and using the services of a trusted third party for identity management, are the most common tools for access control. A growing body of literature explores alternative approaches to security assurance that mitigate the risks associated with single points of failure, such as decentralised or distributed trust models. Therefore, in Chapter 5, we investigate the usage of distributed ledger and zero trust strategy for identity management in cross-organisation data exchange.

Thus, having defined a framework for depicting the state managing information security and privacy in a selected organisation, in the next chapter, we address the identified need for a privacy analysis tool.

4. PRIVACY ANALYSIS OF AN INTELLIGENT SYSTEM

Considering the findings from the background analysis and the scenario of an intelligent transportation system being enabled, let us focus on the tasks of the expert group in one of the contributing organisations. The group's main goal is to plan the changes to the business processes and the systems of their organisation so that the planned state assures information security and privacy. As we showed in the previous chapter, the proposed framework (FISP-ProCOP) is a tool that helps to depict aspects affecting the information security and privacy management of a selected organisation. This chapter is based on [59] and answers the research question $\mathbf{RQ}_2$: *How can tools support privacy assurance for an organisation participating in a cross-organisational smart solution?*

In this chapter, first, Section 4.1 demonstrates how an expert group can continue using FISP-ProCOP as a tool for checking privacy analysis. Second, Section 4.2 presents a method for privacy analysis based on the results of using FISP-ProCOP. The method seeks to analyse expected alterations in business processes and systems, ensuring compliance with internal policies and legal regulations. If violations are identified, the method should facilitate their resolution through minor adjustments to the processes and smart system components. Within this work, we focus on the smart solutions implemented in the EU, and therefore, our study is limited to the privacy regulation in the EU, i.e., General Data Protection Regulation (GDPR) [106]. The method's usability and effectiveness are evaluated through two studies in Section 4.3. In Section 4.4, we review the related work, while Section 4.5 explores the implications of this contribution. Finally, Section 4.6 concludes this chapter.

4.1. Scope and Goals of Privacy Analysis

For ensuring privacy in a newly established smart solution, the expert group should ensure that the transition towards a smart system does not negate the users' privacy. For this, the experts should scrutinise actors and their relationships, the information and data objects involved in the established data exchange relationships of the actors, the formal constraints of such exchange (including local data protection regulations), and countermeasures for assuring security and privacy. Figure 12 depicts the scope of such analysis within FISP-ProCOP by marking the mentioned categories in light blue colour.

Let us assume that an expert group starts its work when the collaboration between organisations contributing to the final smart system solution is in the phase of planning system integration. Within this work, we assume that at this phase, the expected collaborating organisations have already agreed on the expected business processes to be established. Thus, a business analyst within the expert group is

Dimension	Category	Attribute
P. People	PA. Actors	Actors, stakeholders, entities
		Goals, tasks, motives
	PR. Relationships	Relationships and dependencies between actors
O. Organisation	OS. Strategy	Purpose for the system usage, org. design & strategy
		Challenges to address
	OC. Formal Constraints	Legislation, regulation, standard
	OI. Information Involved	Type of information used
		How the information is manipulated
		Security criteria
		Privacy objectives
C. Sec. & Privacy Countermeasures	CP. Policies & Practices	Policies & practices
	CE. Training & Education	Training & education
	CT. Technology	Architectural measures
		Use case-oriented technological measures
		Cryptographic building blocks
		Others technological measures
Pr. Processes	PrL. System Lifecycle	Security as a part of the system lifecycle
	PrU. Usage of the System	Use cases of the system as a part of the business processes

Figure 12: The scope of privacy analysis within FISP-ProCOP

able to provide details of the expected systems' behaviour and the information flows in the form of business requirements and business processes.

In this work, we focus on two key tasks of the expert group needed for privacy assurance in the system where the set of interacting actors and the exchanged information are assumed to be fixed. First, the requirements for privacy assurance of personal data according to the local legislation should be defined (as a part of **T1**). Second, the technical measures for fulfilling the requirements should be selected considering their effectiveness in the business process context (**T2**). Thereby, to answer $\mathbf{RQ}_2$ and support the execution of tasks **T1** and **T2**, we propose a method for tool-supported privacy analysis. The method aims to analyse the expected changes in the business process and the system against the existing privacy-enhancing measures and validate that the new business processes and data flows do not violate privacy requirements (internal and stipulated by the legislation). In case of the found violations, the method should help address them with minor changes to the process and system.

The FISP-ProCOP matrix, developed in Contribution 1, provides the input for the privacy analysis method in Contribution 2. Specifically, the attributes captured in the matrix, as detailed in Table 16, inform the selection of data sources and analysis techniques within the privacy analysis process. This ensures that the privacy analysis is directly aligned with the organisation's specific security and privacy requirements identified through FISP-ProCOP.

4.2. Tool-Supported Privacy Analysis Method

The proposed method takes a BPMN 2.0 model [180] of the process and the business requirements as input that should be provided to an expert group member by a business analyst. The business process model should describe the expected collaborative business process in the smart system, which should be enabled by the systems integration by contributing organisations.

Figure 13 depicts the steps of the proposed method (Contribution 2), along with the experts involved and the input/output artefact of each step.

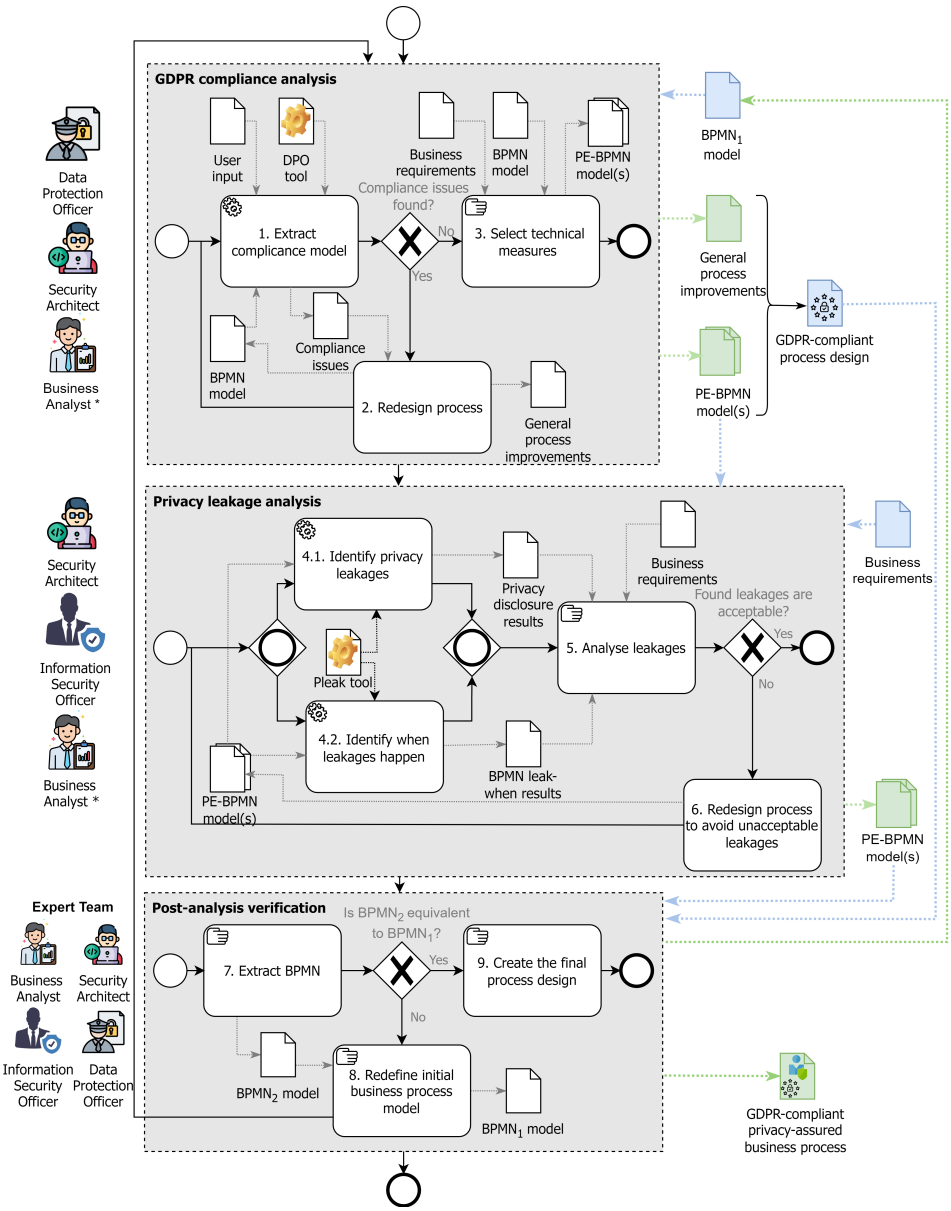


Figure 13: The method for assuring the privacy of a business process (adapted from [59])

The method is presented in the form of an internal process that includes three sub-processes: (*i*) GDPR compliance analysis, (*ii*) privacy leakage analysis, and (*iii*) post-analysis verification. The first stage should be done by a data protection officer (DPO) and a security architect based on input from the business analyst.

The second stage involves a security architect and a (chief) information security officer (CISO). During both two first stages, input from a business analysis may be needed to consult on the specifics of the business process execution and business requirements. The whole expert group should do the post-analysis verification tasks together to verify the results and decide whether to repeat the process.

The proposed method is based on the usage of the selected tools for process model-based privacy analysis, namely, DPO tool[10] [181] and Pleak tool[11] [127]. The used as an input BPMN model, which depicts cross-organisation data exchange as a part of a smart system, should depict the following information: (1) the data objects with the personal data to be protected; (2) how the data is captured from the data subject (whose personal data is manipulated) in the process. The business requirements should specify the required visibility to the process participants.

4.2.1. GDPR Compliance Analysis

The steps of the "GDPR compliance analysis" stage aim to identify the non-compliance issues of the business process model and define a GDPR-compliant design(s) of the business process(es). The stage results in a set of defined general process improvements together with privacy-enhanced BPMN models that depict the desired process's privacy characteristics.

Extract Compliance Model. First, we use the DPO tool [123] to check the compliance of the designed business process model with the GDPR requirements. The tool takes as input a BPMN model of the process and asks a user to provide general characteristics of the process to map its components with the GDPR concepts. A DPO who is familiar with the main concepts of GDPR can do this step with the help of a business analyst who is more aware of the expected business process and the system requirements. If the new process is established based on the existing well-established process and the organisation has privacy policies in place, the DPO uses such policies to supply the requested process characteristics to the DPO tool. During this step, the analysed process should be characterised with respect to the definitions from the GDPR and include the following elements:

- Roles assignment: data subject, controller, processor, recipient, and third party w.r.t. Art.4 [106];
- Purpose of processing and consent: (*i*) category of the personal data w.r.t. Art.9 [106]; (*ii*) legal ground under which the personal data is collected; (*iii*) whether the data subject's consent was collected before the processing tasks performed by the controller; (*iv*) whether required information was provided to the data subject before data collection (e.g., in the privacy policy);

[10] DPO Tool can be accessed at `https://dpotool.cs.ut.ee/`

[11] Pleak can be accessed at `https://pleak.io/` (account: *demo@example.com*, password: *pleakdemo*, manual: `https://pleak.io/wiki/`) [127]

- Personal data to be protected;
- Processing task corresponding to the identified personal data;
- Processing system and technical measures: (*i*) security/privacy attributes of the processing system; (*ii*) data storage characteristics; (*iii*) secure technologies implemented; (*iv*) whether the controller implements organisational measures such as adherence to a security/privacy standard (e.g., ISO/IEC 27001); (*v*) whether a record of processing is maintained.

Based on the supplied BPMN model and user input, the tool produces reports identifying instances of non-compliance detected within the process. The report also specifies the articles of GDPR wherein the violated requirements are declared.

Redesign Process. If the report from the first step identifies non-compliance issues, the expert group redesigns the process. The data protection officer, together with a business analyst, conducts this step manually by introducing general process improvements to the business process based on the found issues. Then, the transformed process is rechecked following the first step. Steps 2 and 1 are repeated until no non-compliance issues are identified.

Technical Measures Selection. With respect to Article 25 [106] of GDPR, the data controller should use technical measures to "implement data-protection principles." Then, technical measures should be selected considering business requirements (e.g., who and to what extent they require access to the sensitive data, what the technologies stack is used in the organisation, which standards are followed, and what the system architecture is). The PE-BPMN model(s) depict the proposed technical measure(s). If the method is applied for analysing the mostly well-established process with minor changes needed to integrate into a smart system solution and the technical measures are already implemented in the system, this stage serves the purpose of documenting how data-protection principles are met in the context of the business process. Here, a DPO with a security architect may propose an alternative process design with different state-of-the-art technologies, for example, based on industry standards or local cybersecurity guidelines. The selection of alternative technologies for privacy preservation allows for avoiding comparing technologies in general and, instead, comparing them during the next stage ("Privacy leakage analysis") in the context of the business process, considering the concrete data flows.

As a result, the "GDPR compliance analysis" stage facilitates defining general improvements to the business process and a set of PE-BPMN models which visualise technical measures to protect privacy in the process. Thereby, the stage delivers a GDPR-compliant process design(s) concluding **T1** of the expert group.

4.2.2. Privacy Leakage Analysis

As a result of the previous stage, a GDPR-compliant business process is designed, which means that it is privacy-assuring from a legal perspective. Meanwhile, being a part of a smart system solution and operating with sensitive data (both personal and non-personal), the organisation aims to protect such sensitive data from leakages or unnecessary usage that contributes to the customers' trust and loyalty [182, 183]. Having the GDPR-compliant process design, we propose to analyse the effectiveness of the selected technical measures. Such analysis is needed to confirm that the business objectives are met. Our method proposes to follow either one or both of the proposed leakage identification steps, which differ by the level of detail. Both steps are done using the PE-BPMN models developed in the previous step and with the support of the Pleak tool.

Identify Privacy Leakages. At this step, we propose a security architect and a CISO to rely on the functionality of the Pleak tool that conducts data disclosure analysis [129]. The analysis assesses the PE-BPMN model together with the data objects' dependencies. It depicts to which process participants' data objects are visible and to which extent, considering the applied privacy-enhancing technologies (i.e., technical measures). The disclosure analysis results are given in a tabular form where each column corresponds to a data object, and each row corresponds to a participant in the process model.

Identify Leakage Conditions. As an alternative to the previous step, leak-when analysis can be used [129]. For this, the security architect, CISO and business analyst enrich the PE-BPMN model with details about data objects and their flows. Thus, the structure of the data object containing the sensitive data is described using pseudocode scripts or as database schemas, and the transformation rules are depicted as pseudocode scripts or SQL queries attached to the processing tasks. Ergo, the expert group receives a report which describes conditions under which the object attributes can potentially leak. For example, the analysis can reveal that the data attribute D1.X can leak in case of leakage of the data attribute D2.Y due to the existing transformation dependencies between data objects D1 and D2.

Analyse Leakages. When leakages are identified, a CISO or a business analyst compares them with the business requirements. While some privacy leakages – disclosure of sensitive data – are either intentional or acceptable based on the risk profile, other leakages are unsatisfactory and endanger the business requirements, posing the threat of insider attack (the collaborating organisation which is partially trusted becomes an insider). This step aims to define which leakages conflict with requirements and, therefore, are unacceptable. Another goal of this step is to compare privacy leakages identified from different PE-BPMN models and decide on the benefits of alternative privacy-enhancing technologies in the context of the business process.

Redesign Process. The expert group redesigne the process if unacceptable leakages are found in the previous fifth step. The security architect also decides on the most optimal PETs to be used, considering the results from the previous step. Thus, the process redesign results in new PE-BPMN models. The newly produced models are analysed again to identify and assess leakages using the aforementioned steps.

4.2.3. Post-Analysis Verification

At the final stage, the whole expert group verify the result. Thus, they need to check whether they have not introduced any changes to the business logic during previous steps of the privacy analysis and the process redesign. For this reason, we propose the following steps.

Extract BPMN. Based on the GDPR-compliant process design and the selected PE-BPMN model, the team extracts a pure BPMN model (i.e., $BPMN_2$) that depicts only the main business process. If this business process is equivalent to the original one (i.e., $BPMN_1$) provided as an input to the method, the team proceeds to the step of creating the final process design.

Redefine Initial Business Process Model. Suppose this business process is not equivalent to the original one (i.e., $BPMN_1$), for example, due to the specifics of the selected privacy-enhancing technology. In that case, the team redefines the initial process to be analysed and start the method from the beginning, considering $BPMN_2$ as $BPMN_1$. This verification is needed to ensure the legitimacy of the GDPR compliance analysis step. The reason is that if the underlying business process has been changed during the privacy leakage analysis stage, the results of the GDPR compliance are not relevant anymore.

Create the Final Process Design. In the end, the whole expert team documents the final process design. The ultimate process design incorporates general process improvements and specific technical measures outlined in the business process model supported with the intermediate analysis results from the tools which serve as explanations for technical measures selection and documents how GDPR requirements are met. Thus, a GDPR-compliant and privacy-ensured business process is established.

To sum up, Contribution 2 is depicted as a business process in Figure 13, and it explains how to use DPO and Pleak tools together in a way that would allow the definition of a GDPR-compliant and privacy-ensured business process. The described above steps extend the original user manuals of the tools with instructions for the expert group to achieve their tasks. Meanwhile, the method users are recommended to use additionally the original Pleak tool manual for execution of steps 4.1. and 4.2. to solve the tool-specific usage issues. It should be noted that the expert group may opt for the usage of underlying methods of the selected tools presented in [181, 127, 129] instead of the usage of tools in the respective process steps. Namely, the conceptual GDPR model and the model-based approach

for achieving GDPR compliance of business processes [181, 123] can be applied manually for the GDPR compliance step. Meanwhile, the mCRL2 toolset [128] based on ACP-style process algebra can be used for the privacy leakages analysis step instead of automated analysis of enriched PE-BPMN within the Pleak tool.

4.3. Method Evaluation

The initial concept of the proposed method was first presented in the author's master's thesis [184]. During the doctoral studies, this method has been formalised and further evaluated w.r.t the usability and effectiveness. The method is evaluated by applying it to two transportation smart system cases – autonomous vehicle ride-hailing (Section 4.3.1) and smart parking (Section 4.3.2). In both cases, an analysed smart system includes three main components – (*i*) a user device, (*ii*) a system embedded into the physical object with which a user wants to interact being in physical proximity to it, and (*iii*) a centrally-managed service providers system which orchestrates the interaction between the first two. In both cases, the smart system manipulates the user's personal data needed to provide the service. However, the cases differ in the scope of the analysed business process and, thus, the amount of details.

4.3.1. Study 3: Autonomous Vehicle Ride Hailing

The first case scenario describes the ride fulfilment process by an Autonomous Vehicle (AV). The process is designed as a part of an autonomous driving project in the Autonomoud Driving Lab [185], founded in 2019 in collaboration of the University of Tartu with Estonian mobility company Bolt Technology OÜ. The author has conducted the evaluation of the method effectiveness as depicted in [59] based on the initial results presented in her master thesis [184].

Scenario. Let us examine the ride fulfilment process within a ride-hailing company where the rides are executed by an autonomous vehicle with which passengers can engage [184]. For the evaluation study, we will depict the ride fulfilment business process using BPMN notation. The As-Is model (i.e., $BPMN_1$) of the process is depicted in Figure 14.

The ride fulfilment process involves collaborative data processing by the following systems: (*i*) an information system that controls the automated driving system and provides infotainment services to the passenger (hereafter 'AV system'); (*ii*) a central IS of the ride-hailing company that enables passengers to order rides and establish passenger-AV interactions (hereafter 'Central System'); and (*iii*) the system used by the passenger (hereafter referred to as a single entity called 'Passenger'). We assume that the AV system and Central System are managed by different entities.

The passenger's data requiring privacy assurance is their geographic location during the ride. Such data are stored in several information artefacts: Ride Details,

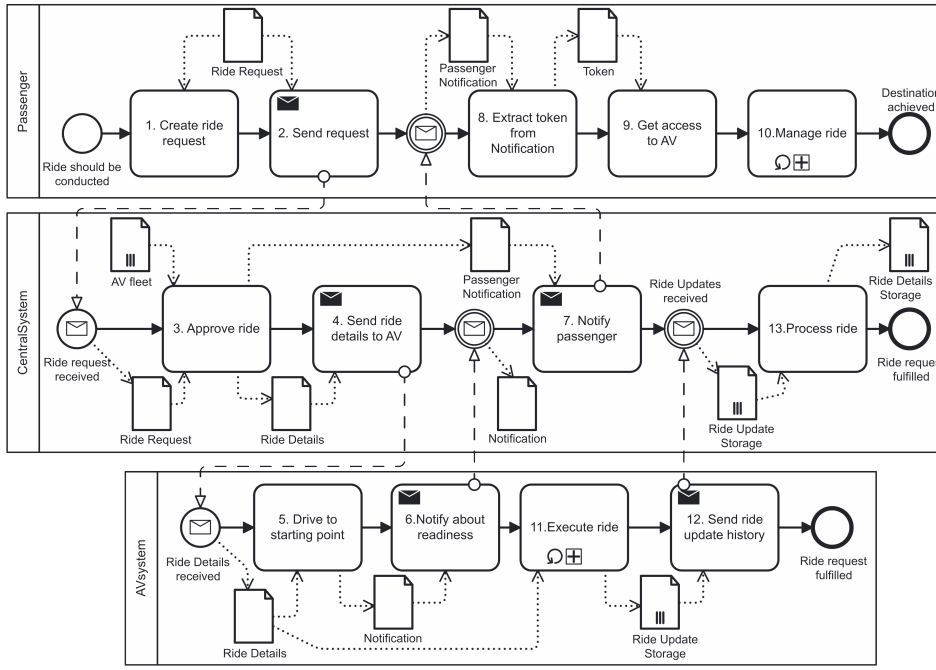


Figure 14: Study 3 - As-Is ride fulfilment business process [59]

Ride Update Storage, and Ride Details storage. The following requirements must be considered:

- Passenger's location should be available to the AV assigned to a ride.
- Passengers can get access to the AV using the provided Token.
- Token should be generated based on the data from Ride Request and the assigned AV details.
- The assigned to the ride AV should verify the token provided by a Passenger.
- Central System should process the ride changes history after the ride is finished.
- Central System should not have access to the current Passenger's location during the ride.
- An authorised representative of the ride-hailing company should access the ride details (including the Passenger's location) on demand after the ride is finished.
- The Central System and AV system should verify one another and have an established secure connection.

GDPR Compliance Analysis. Aiming to analyse how a ride-hailing company should manage passengers' data privacy, we conduct the compliance check with the following role assignments. In the researched As-Is process data, the subject is a passenger, the Central System is a controller, and the AV system is a processor for the tasks '3. Approve ride' with 'Ride Details' as personal data. Such

role assignments are based on the case of the ride fulfilment process where the passenger (data subject) initially makes a request to the owned by the ride-hailing company Central System (controller) about the ride conduction, providing Ride Request with the starting point, destination and other information about the passenger (personal data). Therefore, the Central System controls the personal data provided about passengers and stores it as Ride Details. Central System asks AV System to conduct the Ride Details processing on its behalf based on the existing agreement to resolve the request. In this way, all the Central system's activities can be considered as one activity – 'Resolve request'. To resolve the request, the Central System (controller) provides an AV system (processor) with Ride Details (personal data) to be processed.

One can also analyse the existing Privacy Policy for passengers to extend the researched business process with attributes mentioned in the policy and only afterwards analyse the process with the DPO tool. However, we intentionally do not consider existing in the organisation's privacy policy as it can be interpreted differently and does not reflect the transformation process. Therefore, conducting the research as an external entity that does not have access to the deployed systems or internal organisational policies, we are inclined to assess the process that initially does not consider privacy policy measures.

Using the compliance check tool, we receive the instantiated GDPR model for processing task '3. Approve ride' in Figure 39, which can be found in Appendix C.1. The analysis identified the following non-compliance issues: (*i*) a missing privacy policy (Articles 13 and 14 of [106]); (*ii*) a lack of consent (Article 7 of [106]); (*iii*) missing attributes in the processing systems (Central System and AV System) (Article 32 of [106]); (*iv*) processing tasks are not being recorded (Article 30 of [106]); the record of processing should include name, purpose, contact details, personal data category, data storage period, security measures, and recipients (Article 30 of [106]); and (*v*) the Central System, as a data processor, should be secured with security measures, including standards (e.g., ISO/IEC 27001) and concrete technologies (e.g., PETs).

To address GDPR non-compliance and implement privacy-by-design, we initially considered multiple designs with varying PETs, namely *PK encryption* and *(Shamir's) secret sharing*. Figure 40 illustrates general redesign aspects (derived from GDPR) in blue and PET application areas in green. General redesign aspects should be prioritised.

Design 1 implements public key (PK) encryption of the data object containing personal data. PK encryption is a confidentiality-assuring PET that can also use the FHE scheme for privacy-aware computation (PK computation) [115]. In the ride fulfilment process, 'Ride Details' contains sensitive passenger location data and should be protected. Before transmitting data to external systems, it must be encrypted using the public key. Intermediate processing systems can use PK computation. Only the system needing sensitive personal data (the AV system) has the corresponding private key for data decryption.

Design 2 employs another PET, (Shamir's) secret sharing, an alternative data protection mechanism to PK encryption. Secret sharing data computation is conducted using secure multiparty computation (MPC) requiring multiple participants. Each party holds one private share and executes computation over this share to produce output using homomorphic properties of the sharing. The organisation can implement secret sharing using existing external resources for processing and storing at least two shares, in addition to the server where the Central System currently runs (owned by the company). Secret sharing can be used twice during the process: (*i*) for initial Ride Details processing when approving a ride, and (*ii*) for post-processing of 'Ride Update storage'.

Expert Evaluation of GDPR Compliance Analysis. Additionally, we have evaluated the effectiveness of GDPR compliance analysis [59]. The goal of the evaluation was to get feedback for the UML and BPMN models and the DPO Tool evaluation result from several perspectives: accuracy and completeness (missing or wrong classes and attributes); usability and reliability of the models used; practical suggestions for additional functionality to the DPO Tool. The evaluation study included an evaluation of GDPR compliance analysis with the 4 expert groups composed of professionals with experience in the implementation of GDPR, including (*i*) legal advisors, (*ii*) lawyers specialised in data protection consultation services and data audits, (*iii*) data protection officers and (*iv*) representatives of the data protection authority. All expert groups had a legal background but not any experience with BPMN or UML models. The evaluation was planned and performed using semi-formal interviews with expert group members. Each interview was conducted face-to-face with the expert groups, and each interview lasted 1.5-2 hours. During the interview, we introduced the business process compliance models produced by the DPO tool. The demonstration was performed via the tool. The demo used active participation from expert group members.

The experts highlight that the visualisation of how the GDPR requirements are met in the form of a business model helps to save a significant amount of time during the compliance evaluation procedure as opposed to the textual description of the business situation. Among the drawbacks, the experts have pinpointed the limitation of the tool, namely not covering such corner cases as public interest, joint-controller, and parental control, while this limitation originates from the limited coverage of the used in the tool GDPR conceptual model. Some of the evaluation results about missing artefacts and ambiguous class names have been used to improve the GDPR conceptual model and the DPO tool. Expert groups, initially unfamiliar with the notations, quickly grasped them and effectively identified compliance issues. BPMN was favoured for its intuitive visualisation, while the compact UML Class diagram representation of GDPR requirements proved highly efficient for understanding legal obligations and identifying non-compliances, reducing document overhead. DPOs were identified as the ideal evaluators of compliance results due to their legal expertise.

Privacy Leakage Analysis. Data visibility, technology disadvantages, business process context, implementation difficulty, and system impact must be considered when selecting a privacy-enhancing technology. Prioritising personal data leakage minimisation, we compare two proposed designs using Pleak to analyse PET effectiveness in personal data disclosure.

Based on these findings and the nature of PETs, we draw the following conclusions:

- Using secret sharing to protect the confidentiality of 'Ride Request' requires passengers' devices to have minimum processing capabilities for conducting secret sharing, as this procedure is more complex than PK encryption. Consequently, using secret sharing might increase the processing time of the ride fulfilment process, offering limited privacy benefits.
- Based on the disclosure analysis, both PETs equally impact personal data storage. However, an adversary can more easily access 'Encrypted Ride Details Storage' compared to the distributed storage with secret sharing. PK encryption only requires a private key and storage access. For secret shares reconstruction, an adversary must access both 'Central System Server 1' and 'External Server 2' to obtain two shares and conduct identity spoofing of the authorised stakeholder who can reconstruct shares. Therefore, unauthorised access to 'Ride Details Storage' is more likely to be achieved in the case the PK encryption.

Based on the analysis results, requirements, and organisational capabilities, the optimal design should use the initially proposed security measures (Figure 15). PK encryption protects early-stage data, while secret sharing protects 'Ride Update Storage' and derived 'Ride Details Storage' for post-processing privacy.

The final design is analysed in Pleak another time. The results of BPMN leakwhen analysis in Pleak allow us to assess computation scripts attached to the process tasks (see Table 10) to define the possible leakage of outputs. The scripts are represented by pseudocode. The field `data` of the data objects contains information about the passenger's location.

The results of data disclosure analysis in Pleak are presented in Figure 41, and they show data artefacts visibility considering employed PETs. Figure 16 indicates that the passenger's location (stored in `RideDetails.data` and `RideDetailsStorage_1.data`) may leak only when provided by the passenger input is leaked to an adversary (cells marked by red).

The data disclosure analysis confirms that both PETs effectively protect passenger's location throughout the process. The Central System only processes encrypted data, and the AV system receives only necessary location details. Secret sharing allows privacy-preserving post-processing of ride updates by separate entities without access to raw location data. Moreover, the analysis indicates that passenger data leakage is only possible if the passenger leaks its input data. Otherwise, the proposed PETs prevent leakage to other process participants.

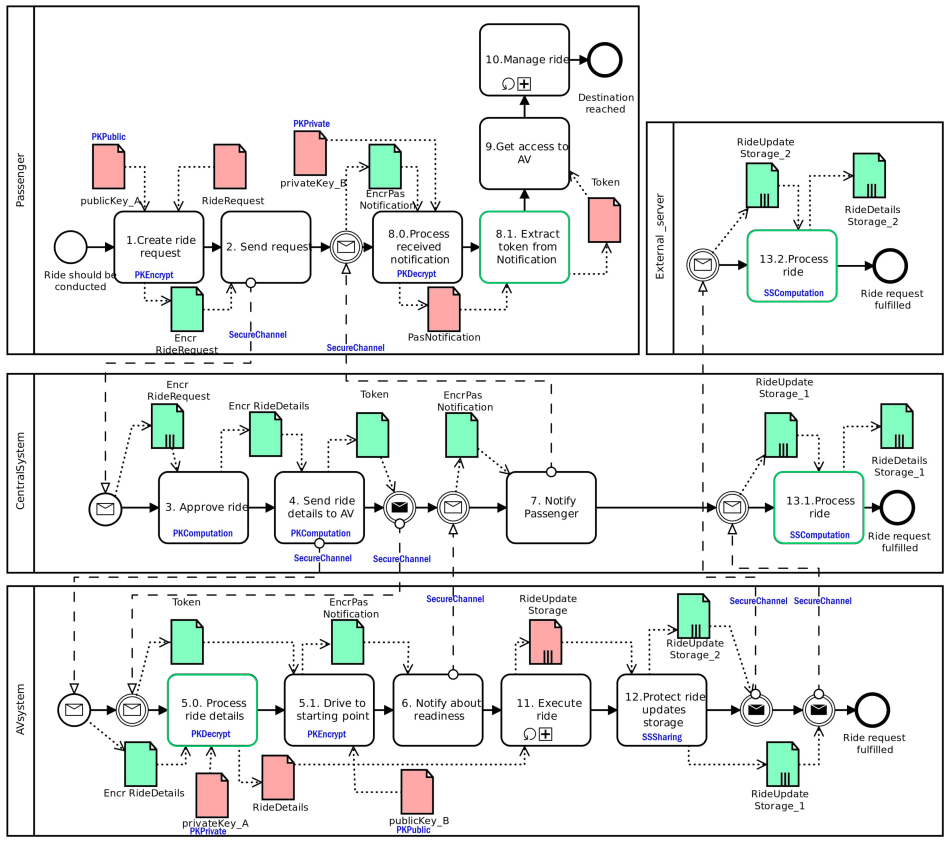


Figure 15: Study 3 - The proposed design extended with the technical measures (the red data objects represent the publicly available data, and the green - protected data hidden from access to sensitive information; the green activities represent the changes activities) [59]

	Master_randomness_for_a.rnd	RideRequestInput.PasId	AV_fleet.AvId	RideRequestInput.data
RideDetails.AvId	always	never	never	never
RideDetails.RideId	never	never	always	never
RideDetails.data	never	never	never	always
RideDetailsStorage_1.data	never	never	never	never

Figure 16: Study 3 - BPMN leak-when analysis results

Post-Analysis Verification. During this study, the proposed method [59] consisted of only the first 7 steps (in contrast to 9 as it is presented in Section 4.1). Thus, no post-analysis verification has been done.

Results. The results of Study 3 demonstrate that the proposed tool-supported method for privacy analysis effectively guides the development of a GDPR-compliant business process design. Experts's evaluation of the DPO tool compliance

Table 10: Study 3 - The script per task is used for specifying data artefacts dependencies

1. Create ride request:	***5.1. Drive to starting point:***
`RideRequest.data =`	`PasNotification.data =`
`RideRequestInput.data`	`getNotification(IntermToken.data)`
`RideRequest.PasId =`	***11. Execute ride:***
`RideRequestInput.PasId`	`RideUpdateStorage.RideId =`
3. Approve ride:	`RideDetails_1.RideId`
`EncrRideDetails.data =`	`RideUpdateStorage.data =`
`EncrRideRequest.data`	`cur_loc(RideDetails_1.data)`
`EncrRideDetails.AvId =`	***12.1. Create share 1:***
`find_AV(AV_fleet.AvId)`	`RideUpdateStorage_1.data =`
`EncrRideDetails.RideId =`	`getShare(RideUpdateStorage.data,1)`
`getId(EncrRideRequest.data,`	***12.2. Create share 2:***
`EncrRideRequest.PasId)`	`RideUpdateStorage_2.data =`
3.1. Generate token:	`getShare(RideUpdateStorage.data,2)`
`IntermToken.data =`	
`getAVtoken(EncrRideDetails.RideId)`	

analysis step confirms the usability and reliability of the compliance analysis results. The proposed process design utilises privacy-enha-ncing technologies to ensure the desired level of personal data visibility. Thereby, the study confirms the usability of the method to support the expert group with the execution of **T1** (to define a set of changes to the processes and the system) and **T2** (to define an acceptable data-sharing policy) with respect to the GDPR and privacy requirements for the smart solution.

Lessons Learnt. The case results in the identification of the following limitations of the proposed method. Based on these limitations, the method is updated.

First, the assumption for the study in [59] was that the whole method could be conducted by a data protection officer (DPO) and process manager (or process analyst). However, the study showed that the method differs in the level of detail about the business process model from one step to another. So, while the GDPR compliance analysis necessitates a low-granularity process model, the privacy leakage analysis requires knowledge of key entities in the information system beyond just the business process. Therefore, the method has been updated to the one presented in this thesis version, which extends the pool of roles needed to be involved in the method execution. In particular, we recommend to involve a business analyst (who can also act as a process manager) in the execution of the method. A business analyst should be able to illustrate the anticipated state of the business process for the smart solution, based on the given requirements and the current state measures and aspects outlined in FISP-ProCOP (see Chapter 3). Additionally, we involve a CISO and a security architect as actors who can elaborate on the implementation of security measures which enable privacy assurance (especially for the second stage of the method).

Second, during the study, we came to the conclusion that there is a lack of repetition of the assessment for GDPR compliance following the process redesign at the privacy leakage analysis stage. As per the proposed approach in [59], we operated under the assumption that the business process at the privacy leak analysis stage does not undergo substantial changes, and the original BPMN model aligns with the final PE-BPMN model. Therefore, based on the evaluation results, two more steps have been added to the method to enable the validation of the produced process redesign against the original input process. To address the scenario when privacy-enhancing technology usage significantly changes the business process, the method has been extended with a post-analysis verification stage for identifying such cases and reiterating the method.

Finally, this evaluation study has been conducted primarily by the author of the method. Therefore, the usability should be further evaluated (especially from the perspective of the method's easiness of learning and error tolerance [186]).

4.3.2. Study 4: Smart Parking

The second usability evaluation study is based on a smart parking process described in [187]. The study has been conducted as a part of the computer science bachelor thesis [188] under the supervision of this thesis author. The student who conducted the evaluation study of the proposed method did not undergo any training on the tools used in the method. The student studied at the computer science program and had taken the course on computer security and the course about the Estonian cybersecurity standard (i.e., "Eesti Infoturbestandardi (E-ITS) ABC"[12]). Additionally, the student worked as an IT Specialist in the bank. Thereby, he can be considered as a junior security engineer from the expert group in the motivation scenario while the thesis author represented a business analyst by consulting the student on the business goals of the smart parking based on the study in [187].

Scenario. The smart parking scenario involves collaborative data processing by the following systems: (*i*) a parking service provider (PSP), (*ii*) a parking lot terminal (PLT); (*iii*) the system used by the smart parking user-driver (hereafter referred to as a single entity called 'Driver'). Additionally, PSP may involve a trusted third-party payment provider and user identity provider. We assume that the PLT and PSP are different organisations. The smart parking scenario involves five key sub-processes depicted in Figure 17.

The detailed As-Is models (i.e., $BPMN_1$) of the smart parking sub-processes are provided in Appendix C.2. First, a driver registers (if not yet) as a PSP user by providing their digital identity details. Next, a driver creates a parking permit request and conducts payment, based on which a driver receives a parking permit from the PLT. To park, a driver authenticates, sends their permits for verification, and enters the parking lot if the permit is valid. Driver may also request parking extension, which is granted based on permit validity. Finally, while the driver

[12] `https://digiriigiakadeemia.ee/`

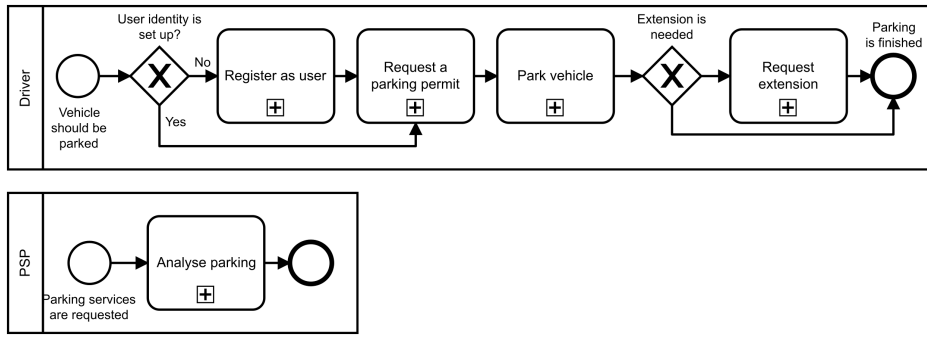


Figure 17: Study 4 - Overview of the smart parking process (adapted from [188, 187])

may initiate the described sub-process, the PSP analyse the activities of a smart parking solution by logging the statistical data for later performance analysis.

The driver's personal data requiring protection are the digital identity and payment information. Such data are stored in several information artefacts: 'Digital Identity', 'Payment Information', and 'Parking Permit' (which is based on both personal data instances). Considering that a PSP is a semi-trusted party facilitating the generation of parking permits for drivers, the following requirements must be considered:

- Details of the Driver's digital identity should be available to the PSP only.
- PSP validates that the Driver is allowed to use the parking lot based on the driver's digital identity details.
- The Driver can get access to the parking lot using a valid parking permit.
- PLT creates a parking permit based on the parking request and digital identity data.
- PSP should not have access to the driver's payment details.
- PSP should not have access to the parking permit.

As the parking process contains two objects to be protected, we split sub-processes so that each manipulates only one personal data object (digital identity or payment details). Thus, the request parking sub-process has its own sub-process, which is the conduct payment sub-process. In this thesis, we present the results of applying the method for the request parking sub-process, while details of the method usage for the rest of sub-processes can be found in [188].

GDPR Compliance Analysis. In the Request parking sub-process, the Driver (representing also the used driver's device) is the Data Subject. The PSP transfers the data and is a Controller, while the PLT is responsible for processing the data and is a Processor. The processing task is 'Generate parking permit'. These details are provided to the DPO tool as the input and are mandatory for the initial analysis, while other parameters can remain at their default values. Table 11 shows the exact inputs for the Request Parking sub-process analysis.

The analysis using the DPO tool defined the missing privacy-preserving measures and corresponding articles from GDPR. The analysis highlighted that the sub-process lacks a privacy policy, consent form, and necessary attributes for privacy-preserving design. This violates GDPR requirements by failing to record processing tasks, provide an overview of the data processing activities, and implement security measures. Based on the results, the model was updated to address the violated GDPR articles, and the changed model was verified using the tool.

Table 11: Study 3 - DPO Tool inputs for the request parking sub-process

Sub-Process	**Data subject**	**Controller**	**Processor**	**Processing task**	**Personal Data object**
Request a parking permit	Driver	PSP	PLT	Transfer parking permit	Parking Request (based on Digital Identity)

Similarly to Study 3, the request for a parking permit sub-process is extended with the usage of encryption based on the PKI as a selected technical measure required by GDPR. To protect the driver's privacy, the 'Parking Request' data is encrypted using a public key from key pair A (PLT's key pair). This encryption occurs before sending the data to the processor. The PLT must decrypt the 'Parking Request' using the private key from key pair A before generating a parking permit. After generating the permit, the system encrypts it using a public key from key pair B (driver's key pair). This ensures only the driver can decrypt and understand the 'Parking Permit' data using their private key from key pair B.

Privacy Leakage Analysis. During this step the sub-process extended with PKI-based encryption is analysed for the leakages. The simple disclosure analysis in Pleak showed that PKI-based encryption could provide secure data transfer between different system counterparts, and the data contents are visible to only the required parties with respect to the requirements.

Post-Analysis Verification. Finally, the redesigned sub-process depicted $BPMN_2$ was compared with the original $BPMN_1$. As the models did not differ in the business flow, there was no need to start the process from the first step; thereby, the analysis was finished.

Results. Our privacy analysis for the smart parking business process resulted in privacy-preserving models for driver registration, parking requests, payment management, and statistical parking analysis. These models outline the flow of sensitive data and ensure compliance with the EU privacy regulations.

The analysis resulted in the processes being enhanced with data protection technologies. Thus, the registration, payment, and permit generation sub-processes are extended with PKI-based encryption to encrypt personal data during transfers, while the data is decrypted only for processing by the processors. Additionally, multi-party computation (MPC) has been tried out to protect digital identity and payment details for the sub-processes. While MPC did not prove itself fea-

sible for registration, payment, and permit generation sub-processes, we demonstrated the possibility of splitting processing logs, securing them, and storing them separately which take place within the analyse parking sub-process. This ensures information security and prevents any single party from having access to the gathered statistical data about parking used for the performance analysis.

Study 4 evaluated such aspects of the proposed method usability [186] as ease to learn, effectiveness, and error tolerance. The ability to learn how to use the method is confirmed by the fact that during the study, the method was used by an external person (not the method author) without formal learning of the method usage. A computer science bachelor student without work experience in data protection but with work experience in IT support was able to reproduce the method with a set of business process models and existing security measures as input. Thus, this study confirms the hypothesis that the method is reproducible and effective, first, by an external person and second, in a scenario other than the initial one (AV ride-hailing fulfilment).

The error tolerance for the method itself has been validated, and the additional validation step added after Study 3 has confirmed its utility for improving the method's effectiveness. Yet, the tools used in the method (i.e., DPO tool and Pleak) have a low tolerance to errors as they are syntax-sensitive and do not provide extensive error recovery options (due to being prototypes). Thus, the tools do not always provide information about the nature of the error or enough instructions on how to solve it. On the other hand, the method itself does not include evaluation mechanisms of the final result as it largely depends on the subjective interpretation of the final result meeting the business requirements.

Lessons Learnt. While this study has been conducted by a person who had neither any previous experience with using the DPO and Pleak tools nor had the formal tools usage training, the following lessons were learnt.

- **Need for training on privacy analysis tools usage.** Understanding how to use privacy analysis tools and interpret their feedback is essential for making informed model changes. This skill allows the user to identify non-compliant processes and missing or incorrectly implemented PETs. The Pleak tool assists in analysing the correct application of selected PETs and their effectiveness in secure data processing. Further, understanding the visibility matrix helps us identify potential data leakages within the system.
- **Analyse personal data components individually.** The privacy analysis should be conducted for each instance of personal data separately as they may have different flows and thus should be protected separately. First, we analysed the entire permit issuance process without segmenting personal data objects, resulting in erroneous evaluations. By partitioning the process into sub-processes based on individual data objects, we can effectively assess privacy compliance. Identifying personal data objects at the initial stages of process analysis facilitates accurate evaluation.

- **Need for having access to the formalised syntax of the tools.** Both tool inputs rely on BPMN models; thus, adhering to BPMN syntax is crucial. The DPO Tool provides immediate feedback on syntax errors in input models, facilitating the identification and correction of mistakes. On the other hand, both tools also use BPMN extensions and have additional rules for using those extensions within the tools. Thus, such rules should be provided to the user to avoid wasting time on solving the tool-related errors instead of focusing on the process analysis itself.

4.4. Related work

Aiming to support organisations, the works in [42, 43, 44, 48, 45, 46, 47] proposed multiples tools that should help check systems' compliance with privacy legislations.

Torre et al. [42] introduced a model-driven technique to evaluate GDPR compliance of the privacy policy documents. Their work primarily focused on textual analysis, neglecting the broader context of business processes. Subsequent research [189] leveraged AI to identify key GDPR concepts within privacy policy text. This approach aimed to assess the comprehensiveness of privacy policies; however, it left the challenge of verifying regulatory compliance in future work.

A tool-supported methodology for ensuring software systems' compliance with legal requirements has been presented in [43]. This approach facilitates the derivation of system requirements from legal texts during the early system engineering phase and the resolution of conflicts between existing software and regulatory stipulations. However, its primary limitation lies in its emphasis on requirements engineering. While it effectively addresses the incorporation of regulatory requirements, it falls short in supporting privacy management practices and evaluating the implementation of privacy-enhancing technologies.

Ghanavati et al. [44] introduced a legal-URN framework to assess the legal compliance of business processes. This framework leverages model-based compliance analysis by comparing goal-oriented requirement models. While the framework is potentially applicable to GDPR compliance, it necessitates the creation of a goal model for GDPR from scratch. To our knowledge, such a goal model does not currently exist, and goal-oriented languages are not widely adopted in business practices.

ENISA sought to assist organisations in implementing GDPR technical and organisational measures by developing a tool for data controllers [48]. While this pilot project did not yield a widely accessible product for PET assessment, it highlighted the ongoing challenge of selecting appropriate PETs. The Pleak tool, a collaborative effort between academic researchers and a cybersecurity company, provides a potential solution by aiding organisations in evaluating PETs.

Cambronero et al. [45] introduced GDPRValidator, a tool designed to assist companies using cloud services in achieving GDPR compliance. This tool, pri-

marily composed of a questionnaire based on GDPR checklists [190], focuses on assessing an organisation's compliance to specific GDPR requirements (e.g., "*Does the company protect personal information through encryption, pseudonymisation, or anonymisation?*"). While this approach aids in identifying compliance gaps and generating document templates, it does not directly facilitate the implementation of measures within information systems and business processes. In contrast, our proposed method prioritises the implementation of measures, leaving the creation of specific documentation outside its scope, yet creating the supporting artefacts for decision on such measures selection which could be later used for the documentation.

The BPR4GDPR project offers a comprehensive approach to GDPR compliance, emphasising a process-oriented perspective [46, 47]. Similar to our work, BPR4GDPR focuses on the entire process lifecycle, from discovery to monitoring. To assess GDPR compliance, they propose comparing the ontological representation of process flows with compliance directive rules extracted from GDPR. This approach, like ours, relies on a formalised representation of regulations, employing policy model and information model ontologies [46]. While the project claims to be supported by various tools, the current stage of development limits its accessibility to SMEs due to a lack of open-access reports on tool usage and concrete use cases. Nonetheless, the BPR4GDPR project presents a potential alternative approach to our method, and our method could be integrated as a component of their process planning and re-engineering phase.

Compared to other research, our proposed method focuses on two major points: (*i*) checking a business process on compliance with the GDPR requirements and (*ii*) assessing the effectiveness of technical measures for assuring the privacy of personal data. Similarly to [45], and in contrast to work in [47], our method explicitly highlights which of the GDPR articles are addressed. Compared to approaches in [43, 44, 45, 47], in this research, we also aim to support the selection of privacy-enhancing measure in the context of the process to support the GDPR requirements.

4.5. Discussion

In this chapter, we proposed a tool-supported privacy analysis method. The usability of the method was evaluated by the application to two cases of transportation smart solutions – (*i*) a ride fulfilment process in a ride-hailing company enabled by an autonomous driving system, and (*ii*) a smart parking solution that allows the users access the parking lots based on the parking permits created by parking service providers. For Study 1, the method was applied by the thesis author, and the results' correctness was verified by the autonomous driving lab members. For Study 2, the method was used by an external person, and the thesis author verified the results' correctness. The proposed process designs utilise privacy-enhancing technologies to ensure the desired level of personal data visibility. Thereby, the

studies evaluated the usability of the method to support the execution of **T1** (to define a set of changes to the processes and the system) and **T2** (to define an acceptable data-sharing policy) defined earlier in Section 1.1 with respect to the GDPR and privacy requirements for the smart solution. Additionally, the final step of the method of post-analysis verification guides the expert group in **T3** (to ensure the meeting of business requirements by the updated process and the system). Each study resulted in at least 6 identified non-compliance issues, the addition of at least 3 new activities to the system design, and the selection and justification of at least 1 privacy-enhancing measure.

Except for the method evaluation and improvements through two cycles of design science research, the studies resulted in the findings about the proposed method. Namely, the evaluation studies experiences allow us to conclude on the method application scenarios in the generalised context. The proposed method can be applied in three scenarios: (*i*) process (re)design, (*ii*) established formalised process analysis, and (*iii*) analysis of executed non-formalised processes.

- The two studies presented in this thesis demonstrated the method's application to process (re)design. In such a case, the method should be applied to an already (re)designed but not yet launched business process, guiding its privacy compliance.
- For established formalised business processes, the method can verify GDPR compliance and the contribution of selected PETs to business and GDPR privacy requirements. The method should consider existing organisational privacy policies reflected in the process itself, as these policies should have guided the existing business process. As a result, the method helps to prepare artefacts that demonstrate compliance with the GDPR as prescribed in Article 5 (2) [106].
- The method can also be applied to analyse executed non-formalised processes. In this case, the analyst should use process logs and process mining techniques to create an actual As-Is business process model for input into the proposed method. This helps verify whether the actual executed business process is GDPR compliant and meets business and GDPR privacy requirements at the implementation level.

As the proposed method includes process and system redesign, the results show that it is recommended to be applied early in the process definition and system development stages. This can help avoid costly revisions to established processes, systems, and privacy policies. Protecting personal data contributes to customer trust, loyalty, and avoiding penalties [182, 183].

The proposed method relies on using collaborative business process models. The use of collaborative business process models in Contribution 2 directly addresses the SoS dimension by explicitly modelling the interactions and dependencies between different organisations within the smart system. These models capture the flow of information and control across organisational boundaries, high-

lighting potential privacy risks and enabling the design of appropriate protection.

Limitations. Meanwhile, the studies have two key limitations. First, our studies were limited to evaluating the usability of the method execution by only one person per study. Thus, in future work, the method's usability by the whole expert group should be validated. Second, while the study focused on evaluating the effectiveness of the method in identifying and mitigating privacy risks, a more in-depth analysis of its efficiency should be done. Future work should involve an evaluation of the time and resources required to execute the method across multiple case studies. Furthermore, a comparative analysis of the method's effectiveness and efficiency against traditional compliance checks (e.g., using questionnaires and existing company practices) would provide valuable insights into its potential advantages and limitations.

The primary limitation of the proposed tool-supported method for privacy analysis is the prerequisite of having a formalised business process model in place. This prerequisite may be an obstacle for organisations to use it for the first time. The required details about the business process model are another limitation of the proposed method. While the GDPR-compliance analysis needs a low granularity process model, the privacy leakages analysis requires knowledge about key entities in the IS except for the business process.

The used tools are proof of concept tools and, therefore, have a limited scope. The DPO tool currently covers only the selected articles of GDPR, which are focused on data processing as part of the value delivery for the users, not considering the required supporting activities by the data controller (e.g., addressing data breach accidents and having data protection impact assessment). At [115] the limitations of the Pleak tool are pointed out. In the current version of Pleak, the whole process is expected to be described in one diagram so that data objects are initially publicly accessible and then protected or processed. As the tool is under development, it currently supports the limited combinations of PE-BPMN stereotypes that restrain the analysis of privacy-enhancing technologies. Alternative tools of higher maturity that allow analogous results could be used to address this limitation. On the other hand, the expert group may opt for conducting the steps of the proposed method without reliance on the specialised tools and prefer manual comparison of the business processes in place with the GDPR reference model [123] and analyse the data flows for identifying the potential data leakages through binary analysis or leakage analysis [127, 191, 192].

Further, the current method evaluation is limited to the qualitative assessment of the method's effectiveness. Given the novelty of our integrated approach to privacy analysis in this context, there are currently no established benchmarks for comparison. Future research will focus on developing metrics for evaluating the efficiency and effectiveness of our method, enabling comparisons with emerging best practices and alternative approaches as they develop. Additionally, the expert group representatives should subjectively evaluate the method's efficiency and effectiveness within the real-life setting.

Lastly, one of the requirements of NIS2 directive [108] is that its subject organisations should address supply chain security. To this end, the concerned organisations have to address the risks of personal data leakages to their digital service providers. Therefore, the proposed method (especially the privacy leakage analysis step) could potentially support organisations in managing the supply chain risks by identifying limitations of the data protection technologies used and the conditions of the data leakages.

4.6. Summary

This chapter answers $\mathbf{RQ}_2$: How can tools support privacy assurance for an organisation participating in a cross-organisational smart solution? In this Chapter, we proposed a tool-supported privacy analysis method. The proposed method supports the elicitation of requirements for the business processes based on the European data protection regulation, i.e., GDPR, and a further selection of privacy-enhancing technologies (PETs).

Both parts of the method rely on the usage of the selected tools, namely the DPO tool and the Pleak toolset, which are open-access solutions which were developed based on academically proven analysis methods. The method has been evaluated through two evaluation studies for intelligent transportation solutions. The evaluation confirmed the effectiveness of the method to allow privacy requirements elicitation and comparison of the PETs' ability to support business requirements and prevent data leakages. As a result, the method addresses the problem of the difficulty in assessing the efficacy of privacy technologies [37, 40]. The second study evaluated such aspects of the method usability as the ease of learning, effectiveness, and error tolerance, but also resulted in recommendations for method users. Finally, having the instance of FISP-ProCOP matrices for organisations enabling the business process and applying the proposed privacy analysis method allows us to integrate the privacy management aspects reflected in the matrix into the business process. As a result, the expert group in the organisation, through following the proposed method, creates the artefacts that demonstrate compliance with the GDPR as prescribed in Article 5 (2) [106].

To sum up, in this chapter, we showed how the expert group working on the analysis of established collaborative data processing for a smart solution should approach privacy management and use the tool for assuring compliance with GDPR. The proposed method assumes having the trust requirements fixed and allows privacy enhancement within the established trust model. Meanwhile, in the next chapter, we release this assumption and propose a method for comparison of trust models for organisation identity management in the cross-organisation data exchange and define the implications of the trust model usage for the security of organisational identity and privacy of the user's and organisational data.

5. SECURING ORGANISATIONAL IDENTITY

After establishing a secure and privacy-preserving data exchange process within the smart system, organisations may still need to revisit their security measures. For example, the organisation may update its risk profile during the integration to create a smart solution and change the security assumptions. As we discussed in Chapter 2, identity management and trust assumptions form the base for securing cross-organisational data exchange. The most common identity management system relies on a centralised Public Key Infrastructure (PKI). However, this approach is prone to a single point of failure, and it can be exploited by attackers (either external or internal) to leak sensitive personal or business data during cross-organisational data exchange or cause delays due to its limited capacity for identity issuance or verification.

Suppose an organisation updates its identity and trust model aiming to eliminate a single point of failure in the identity management system in the smart solution. In that case, the expert group's primary focus becomes evaluating changes to their business processes and systems. This evaluation ensures the planned modifications will maintain information security and privacy and align with the smart solution's business requirements.

Following the structure of FISP-ProCOP, the expert group needs to narrow the scope even more compared to the privacy analysis, as shown in Figure 18 (scope is marked with dark blue colour). Particularly, for the trust model update, the expert group should scrutinise (*i*) actors involved in the cross-organisational data exchange, their goals, tasks, roles, and relationships; (*ii*) security criteria for the exchanged information; (*iii*) policies that enforce security criteria through access control of actors to the information; and (*iv*) technologies (including architectural and cryptographic measure) which enforce the policies. The data model in Table 16 (Appendix A) guides the expert group in selecting the data source for each analysis step by specifying relevant FISP-ProCOP matrix attributes. Assuming these tasks of the expert group, in this chapter, we answer the research question $\mathbf{RQ}_3$: *How does the trust model affect the security and privacy of an organisation participating in a cross-organisational smart solution?*

As we described in Chapter 2, there are multiple trust models used as the baseline for the data exchange. The centralised trust model relies on the trust of the majority of organisations in a selected root of trust, presented by an entity that tells others who can be trusted. The centralised trust model is the most commonly used. However, being prone to a single point of failure, an alternative solution has been proposed and is under active research. The alternative trust model is a decentralised one where, in the network of organisations, no single party can decide for others who are trustworthy or not. Instead, the organisation rely on the algorithmic root of trust, which allows each party to decide the rules under which another party is trustworthy for them. This Chapter is derived from [60, 61, 62, 131] and contains sentences or fragments of sentences from these prior publications.

Dimension	Category	Attribute
P. People	PA. Actors	Actors, stakeholders, entities
		Goals, tasks, motives
	PR. Relationships	Relationships and dependencies between actors
O. Organisation	OS. Strategy	Purpose for the system usage, org. design & strategy
		Challenges to address
	OC. Formal Constraints	Legislation, regulation, standard
	OI. Information Involved	Type of information used
		How the information is manipulated
		Security criteria
		Privacy objectives
C. Sec. & Privacy Countermeasures	CP. Policies & Practices	Policies & practices
	CE. Training & Education	Training & education
	CT. Technology	Architectural measures
		Use case-oriented technological measures
		Cryptographic building blocks
		Others technological measures
Pr. Processes	PrL. System Lifecycle	Security as a part of the system lifecycle
	PrU. Usage of the System	Use cases of the system as a part of the business processes

Figure 18: The scope of trust model analysis within FISP-ProCOP

5.1. An X-Road-based Smart System

To answer $\mathbf{RQ}_3$ following the design science [53] cycle, we narrow down the motivation scenario in Chapter 1 to make the problem more specific. We assume that to enable a smart solution, the organisations select the X-Road data exchange system as an interoperability enabler. Thus, X-Road enables data exchange between stand-alone information systems used by each party, contributing to a smart system. Meanwhile, the end users of the smart system interact with existing information systems as they are before integration but with newly enabled data exchanges. X-Road is a widely used data exchange system and serves as the backbone of digital infrastructure in the public sector (e.g., enabling Estonia's digital public services) and private sector (e.g., enabling clients' data exchange in the Japanese energy sector)[13].

The X-Road Data Exchange System. X-Road is a centrally coordinated distributed data exchange system that facilitates the standardised and secure production and consumption of web services within a trusted network [194]. It establishes a framework for information system interaction, enabling organisations to exchange data securely. The X-Road ecosystem comprises four key roles:

- Governing Authority: This entity owns a specific instance of X-Road and defines the regulations and practices that must be adhered to within that ecosystem.
- Operator: This organisation manages a particular instance of the X-Road ecosystem, ensuring its operation.
- Member: An organisation that joins an X-Road instance to provide and/or consume services by exchanging messages with other members. Members are organisations with their ISs used for operations by internal users (e.g. employees) and external users (e.g., customers).

[13]There are 24 X-Road instances deployed by governments or other organisations worldwide, which enables data exchange for 542 million end users [193]

- Trust Services Provider(s): These organisations, which may be third-party or managed by the Operator, function as time-stamping authorities (TSA) and/or certification (or certificate) authorities (CA)[14]. They contribute to the trust infrastructure within the X-Road ecosystem.

In essence, X-Road Members are the primary system users who rely on a foundation of mutual trust to exchange services. The Operator and Trust Services Providers act as facilitators, enabling this trust through the Identity Management (IdM) system implemented within X-Road.

The X-Road ecosystem functions as a trusted network, where organisations utilise the same software instance to provide and consume services. The system is comprised of two primary components: the Central Server (CS) and the Security Server (SS). The Central Server, under the management of the X-Road instance Operator, is responsible for Member registration, including the addition, authentication, and removal of their Security Servers. Meanwhile, individual Members manage the Security Server(s), which is the entry point from the Member's information system to X-Road. It facilitates the mediation of service calls and responses between the information systems of Members. Each Member may use its own Security Server (i.e., a Member is the owner of the server and manages it), or a Member may use a Security Server owned and managed by another network Member (i.e., use an outsourced Security Server). Additionally, Members have the option to utilise multiple Security Servers as proxies (i.e., act as SS clients).

5.1.1. Problem Statements

As a result, in a smart system enabled by the X-Road data exchange system, PKI would enable smart system contributors who act as data providers to validate the identities of the data clients (and vice versa). However, in this setup, organisations are prone to two problems.

Problem 1: Centralised credentials issuance. The PKI-based identity management system is prone to a single point of failure due to the centralisation of identity certificate issuance and verification in a potentially single national authority. Thus, the issuance of centralised credentials threatens the availability and integrity of organisations that participate in the data exchange. Thus, in our study, we aim to solve the problem of a single point of failure of centralised identity management in the X-Road-enabled smart system.

Problem 2: Centralised identity control. As we showed in Chapter 2, centralised identity control threatens the authenticity of identity usage and, therefore, the confidentiality of the exchanged data. Organisational Digital Identity (ODI) often relies on the credentials and keys being controlled by a single person-representative. Moreover, some organisations may outsource the key management

[14]In this study, we do not differentiate a certification authority (CA) from a registration authority (RA), which is an optional system to which a CA delegates certain management functions [142]. Thus, we assume that all the activities of the certificate service provider needed for the certificate assertion and issuance are conducted by a CA.

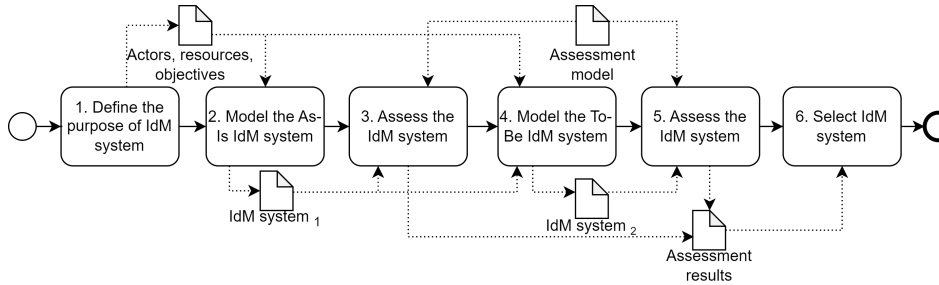


Figure 19: Method for identity management system analysis

to a third-party controller. Both the centralisation and outsourcing of the keys threaten data integrity within the IS, allegedly provided by a trusted organisation. Also, outsourcing the control prevents an organisation from cryptographically enforcing custom policies, e.g., time-based, regarding the data originating from it.

5.2. Research Method

To assist the expert group in solving the mentioned problems, we develop two IdM system designs each addressing one of the stated problems. For the designs' development, we follow the method presented in Figure 19, which is based on the business analysis process [195]. The targeted research project of changing the identity management model aims to identify business needs and recommend a solution that enables the organisation to achieve its goal. For this reason, the research falls under the scope of the classical scope of business analysis project [195, 196].

First, we define stakeholders involved in the data exchange and identity management, the identities that should be managed, the credentials used for these identities, their purpose in the business operations, and how they support social dependencies. Second, we model the current IdM system implementations in the business context. Third, we design and model an alternative IdM system that addresses as many of the purposes identified in the first step as possible. After each modelling activity, the IdM system is evaluated using the IdM quality assessment model. Finally, we compare the current (i.e., As-Is) and alternative (i.e., To-Be) IdM systems. Thereby, we evaluate the effectiveness of the proposed To-Be IdM system designs to achieve the stated design goals and provide an IdM system.

Following the depicted in Figure 19 process, we conduct two separate design science cycles. Each of the studies proposes an alternative design of an identity management system based on the selected problem statement. During the studies, we use the following sources of input about the data exchange system: (*i*) X-Road Academy courses [194], (*ii*) official documentation [197, 198], and (*iii*) stakeholder's expertise from the NIIS[15].

[15]Nordic Institute for Interoperability Solutions (NIIS) is a non-profit association dedicated to open-source X-Road development, along with "strategic management of digital government solutions that allow its members to provide excellent digital public services" [199]

5.2.1. IdM Quality Assessment Model

Based on the background literature review we identified no standard model or framework for identity management systems or identity model assessments. Thus, for the evaluation of the IdM system design, we develop the quality assessment model for an identity management system as depicted in Table 12. This model is based on the literature review which resulted in the extracted quality measures discussed in the literature as the ones affected by the followed trust model, or the system quality measures targeted by the identity management system components (including the key management mechanisms discussed in Section 2.3.3 and 2.3.4). Initially, we proposed and validated the assessment model in [60, 61]. Afterwards, based on the validation results, we additionally extended the model with the business-driven characteristics of the IdM system and key management mechanisms [62]. As a result, the presented IdM assessment model is based on Cameron's digital identity laws [136] and aligned with the recent studies in [52, 200, 201, 202] on the identity management systems.

The model consists of four key quality criteria, which are broken down into more granular sub-criteria. For each sub-criteria, we provide an indicator that gives an example of how sub-criteria can be assessed, and each indicator has a respective example of its measurement units. The indicators and their measurement units provided in Table 12 do not reflect the full set of criteria assessment measures and can be further extended. The provided indicators and measurement units are oriented to IdM systems which handle organisational identity for the cross-organisational data exchange.

First, the model includes the criteria of **security**. An IdM system's security entails safeguarding organisational identity and sensitive data (operational or personal data) from unauthorised access, breaches, and threats. As a cornerstone of an organisation's security posture, it protects valuable assets and ensures operational continuity. Based on the previous studies [60, 62], security assurance in an IdM system includes the ability to mitigate high-impact risks stemming from insider attacks, centralised control, system unavailability, and the absence of trustlessness (both to internal organisation representative and external entities as a core idea of zero-trust security strategies [58]). Insider attacks can exploit organisational identity to access and manipulate personal data, resulting in data breaches, reputational harm, and financial penalties [203]. Centralised control over an IdM system introduces a single point of failure [52, 201]. Therefore, decentralisation can enhance security and reliability. For assessing the mentioned sub-criteria, the IdM system architecture can be checked on the facts of having the built-in respective mitigation mechanisms. Moreover, IdM system availability and, thus, operational access control mechanisms contribute to the IdM system's overall security [202]. For assessing the availability, the systematic operational delays for the key identity-related operations can be measured, for example, by estimating the time for credentials issuance, signing and verification.

Quality criteria	Quality sub-criteria	Indicators	How to measure
Security	**Preventing insider threat**	Fact of having built in prevention mechanism	Yes / No
	Decentralisation	Decentralisation of credentials issuance/verification	Yes / No
		Decentralisation of credentials and keys management	Yes / No
	Trustlessness	Not having a single of fully trusted external entity	Yes / No
		Not having a single of fully trusted internal entity	Yes / No
	Availability	Systematic operational delays	Time of credentials issuance / signing / verification
Control	**Responsibility over credentials**	Level of responsibility over credentials by the identity	{0, 1, 2}
	Control over identity attributes	Control over the revealed details	Number of entities to who the attributes from the credentials are revealed during issuance / verification
	Traceability	Fact of having built in traceability mechanism	Yes / No
Usability	**Portability**	Fact of having built in mechanism for portability	Yes / No
	Multiple users	Fact of having built in mechanism for having multiple users	Yes / No
Maintain-ability	**Backwards compatibility**	Fact of being backwards compatible with PKI	Yes / No
	Complexity	Dependence on social actors	Number of actors involved in the credentials issuance /signing / verification
		Dependence on external systems	Number of systems to be integrated with for issuance/ signing / verification

Table 12: Quality Assessment Model for Identity Management System

The second quality is aligned with the first three Cameron's laws [136], namely user control and consent, minimal disclosure and justifiable parties. Thus, the quality of **control** describes how much control over the credentials and the digital identity usage the identity holder has. The sub-criteria of responsibility over credentials aims to define how many responsibilities the identity holder has – whether the holder has to fully rely on the pre-setup system features fully delegating control over identity, credentials and cryptographic keys (refers to *level 0* of responsibility), the holder can optionally stay in control of keys (*level 1*), or the identity and its holder has to be actively involved in all the identity-related operations (*level 2*). To enable user control over identity, the model includes sub-criteria of control over identity attributes which are revealed to the parties. This can be measured by the number of entities to who the attributes from the credentials are revealed during issuance or verification. Finally, the fact of having a built-in mechanism in the IdM system for traceability enables the identity to verify that only justifiable parties are provided with the identity details and that the identity is used by the legitimate holder based on the agreed conditions (e.g., organisation's employees use the ODI only for the justified business needs).

The third included quality criteria is **usability** which is the ability of an IdM system to manage identity and key in a user-friendly and convenient manner. Acknowledging the need to include human-in-the-loop with respect to the sixth

Cameron's law [136], the IdM system should allow multiple users to manage organisational identity as (all) the employees (not only a selected one) are the key actors of organisation and, therefore, ODI should allow for multiple employees-users. Additionally, to support consistent experience across contexts (the seventh Cameron's law), an IdM system can enable portability (i.e., ability to access ODI on different devices [143]).

Finally, the quality of the IdM system is defined by its **maintainability**, which refers to the easiness with which the system can be set up and maintained [204]. As a smart solution in the motivation scenario is built based on the existing systems, the maintainability depends on whether the IdM system is backwards compatible (i.e., whether a new IdM system can work together with the older one) and how complex it is.

To sum up, we identified mechanisms that help secure keys and signatures and, thus, ODI itself. The commonly used approaches of key management can address the problem of centralisation or bring zero trust in a targeted manner, while none of them addresses the problem on their own. Therefore, in our research, we aim to show how the selection of IdM system components can enable organisations to meet both their business and security goals of IdM system quality. For this, we investigate the selection of the combination of reviewed mechanisms and evaluate it using the IdM quality assessment model.

5.3. Decentralised Identity Management System

To address problem 1 defined in Section 5.2, we aim to design an identity management system that would eliminate a single point of failure of organisational identity caused by reliance on a certification authority (CA) for credentials issuance, update and verification. Self-sovereign identity principles and decentralised public key infrastructure [52, 205, 206] are considered in the literature as alternative solutions for PKI-based identity management. However, this solution is researched from the perspective of identities for private identity holders (i.e., physical entities). Therefore, to address this gap, we investigate the effect of using decentralised PKI (i.e., DPKI) as an enabler of self-sovereign identity (SSI) for ODI.

5.3.1. Design Goals

During this study, we aim to answer the following sub-questions: $\mathbf{RQ}_{3.1}$: *What are the trust dependencies of actors in the data exchange system?* The research process begins with an analysis of the current business set-up. We define key actors and identities used, the purpose of credentials in X-Road, the procedure for issuing and usage of these credentials, the onboarding process for the X-Road network participants, and the trust model. To address $\mathrm{RQ}_{3.1}$, we illustrate social dependencies in X-Road using the i*/Tropos framework [207], which defines trust requirements.

RQ$_{3.2}$: *How are the defined trust dependencies supported by the system implementation?* To answer this question, we employ process modelling, class diagrams and sequence diagrams to define the system components and flows that facilitate meeting the trust requirements.

RQ$_{3.3}$: *How to establish trust between information systems using a decentralised public key infrastructure in X-Road?* In the next stage, we design the analogue credentials and actors in the context of DPKI. This step results in the redefined trust model and identified actors, system functionalities, components, and processes that should be in place for identity management using DPKI in X-Road.

RQ$_{3.4}$: *How well does the decentralised trust meet the system requirement?* Finally, using the identity management system quality assessment model, we assess the As-Is and To-Be identity management systems against the stated goals.

The study has two iterations of design and development of a decentralised identity management system. During the first iteration, depicted in [60], we elicit the IdM system architecture, business objective for the IdM system and credentials. Based on this, we develop a DPKI-based architecture for X-Road identity management, which substitutes the PKIX-based IdM system and does not change the business flow of data exchange within X-Road. We start the second iteration based on the feedback received from the communication of the first architecture solutions. As depicted in [61], we redefine design goals, functional requirements, and use cases for the proof of concept (PoC) IdM system at this stage. Next, we outline the technology setup needed for the PoC to meet the design goals and requirements. Based on this setup, we update the DPKI-based architecture for the X-Road system. Then, we develop the implementation of the PoC system. Finally, we check if the PoC meets the acceptance criteria and evaluate its quality using the assessment model.

5.3.2. Step 1. Define the Purpose of IdM System

In the X-Road network, there are two key classes of identities - identities of Members and identities of Security Servers. Currently, Public Key Infrastructure (PKI) based on the X.509 standard [142] underpins the management of these identities. To become a Member, an organisation should possess a *signing certificate* issued by a trusted Certification Authority (CA) included on a list defined by the Governing Authority. An Operator of the network may be one of the CAs on the list of trusted CAs. Each Security Server possesses its unique authentication certificate. The process of obtaining a signing or authentication certificate depends on the speed of processing certificate signing requests (CSR) by trusted CAs. This process varies for different CAs and may include several manual steps to check the characteristics of the prospective members, and it might require days, weeks, or even months to complete. As a result, the waiting time caused by the certificate assertion process may prevent Members from joining the network and, thus, threaten the availability of the potential data exchange messages.

The main goal of the signing certificate (credential for the Member's identity) is to make sure that the messages sent through X-Road originate from the organisation which is a registered Member in the X-Road instance. The goal of the authentication certificate (credentials for the Security Server's identity) is to ensure that the message requests are coming from the Security Servers registered in the X-Road instance and eligible for the data exchange.

Considering the defined IdM system objective and the project objectives, the To-Be IdM system design should meet the following design goals:

- $\mathbf{G}_1$: *Decentralised*: the To-Be system should allow secure connection creation between organisations using the system without an intermediary organisation involvement;
- $\mathbf{G}_2$: *Automated Member Onboarding*: the To-Be system should enable automated verification of identity without reliance on any third parties for the member onboarding processes.

5.3.3. Step 2. Model the As-Is IdM System

The modelling of the As-Is IdM system starts with modelling the processes manipulating credentials. The business process of a new Member onboarding is modelled using the Business Process Model and Notation (BPMN 2.0). Following the execution of a legal agreement between the Governing Authority and the prospective member, the Operator registers the member within the system. A critical aspect of member onboarding is establishing a client relationship with a Security Server (SS). This, ultimately, empowers the member to provide and consume services through the X-Road ecosystem. The full process of onboarding is presented in Appendix D.1.

If the Member wants to use its own SS, the Member first sets it up. For this, the signing key and corresponding certificate should be obtained for the Member; the authentication key and corresponding certificate should be obtained for the SS (the procedure of obtaining the authentication certificate is analogue to the subprocess 'Configure signing key and certificate'). Upon obtaining the certificates, they should be imported and activated in the SS. After obtaining the authentication certificate, the authentication certificate registration request (signed with the Member's signing key) is sent to the Central Server for approval. Once the Central Server approves the request to register the SS, Members of the network can initiate registration as the SS's clients.

Figure 20 illustrates the configuration process for a PKIX certificate. The process starts when the Member uses the SS UI (to which they have access as a Member of the network) to generate a signing key pair. The pair is saved as a PKCS #12 file. Based on this file, the Member applies for the certificate by sending a certificate signing request (CSR) following PKCS #10 format to the selected CA. Receiving the CSR, the CA checks the request, conducts some manual checks of the applier's identity, and in the case of approval, the CA generates the cer-

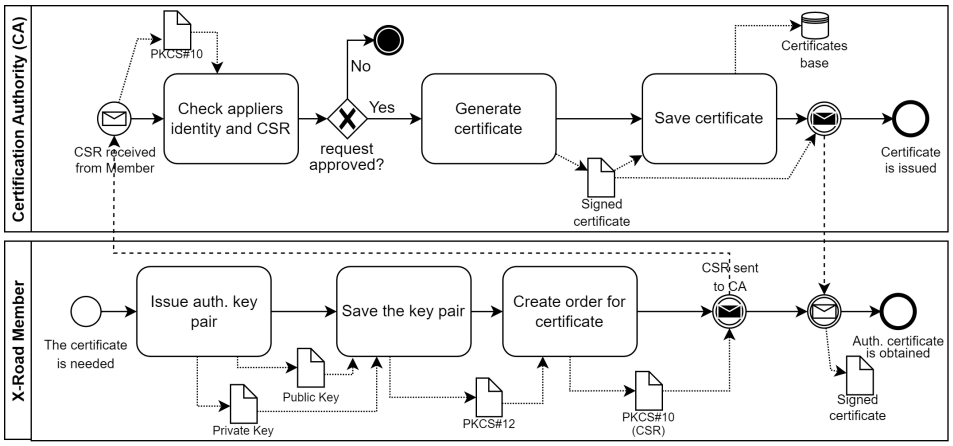


Figure 20: Credentials issuance using PKI

tificate for the provided authentication key pair. The certificate is stored in the certificate base to be accessed on-demand for verification. The credentials configuration happens off X-Road mostly manually. Exactly the mentioned manual check of the identity by CA causes waiting time during the Members' onboarding. While the X-Road Owner has no way to influence CA to reduce waiting time, we consider the shift to another IdM system where CA as a bottleneck is eliminated.

The configuration of signing and authentication certificates is essentially analogous. There are two peculiarities in the configuration of the signing certificate. First, the generation of a signing key pair may be outsourced to the CA. In this case, the signing key pair is stored in the HSM (hardware security module) device, and the SS administrator does not have to create it. Second, depending on the X-Road instance policy, the Operator may be an intermediary party between the Member and CA when the Member sends a CSR.

Regardless of the type of credentials, the verification process is essentially the same, and it is shown in Figure 21. When an identity holder (SS or Member) wants to exchange a message with a verifier (another SS or Member), the former sends the message signed using the private key corresponding to the credentials (e.g., authentication certificate) together with the VC's ID and the certificate itself. The verifier checks the credentials issued by the trusted CA and searches for information about the validity of the credentials (OCSP response) in the message. When issuing a connection between two SSs, In case of a missing OCSP response for VC_{auth}, the verifier requests it from the holder, who requests it from the certification authority that issued credentials. When it comes to VC_{sign}, the OCSP response is included in the message (request or response), and therefore, the verifier does not have to request it separately.

To depict the organisational entities involved in identity management, the credentials used in X-Road, and system components which enable or rely on IdM, we define a conceptual domain class diagram depicted in Figure 22.

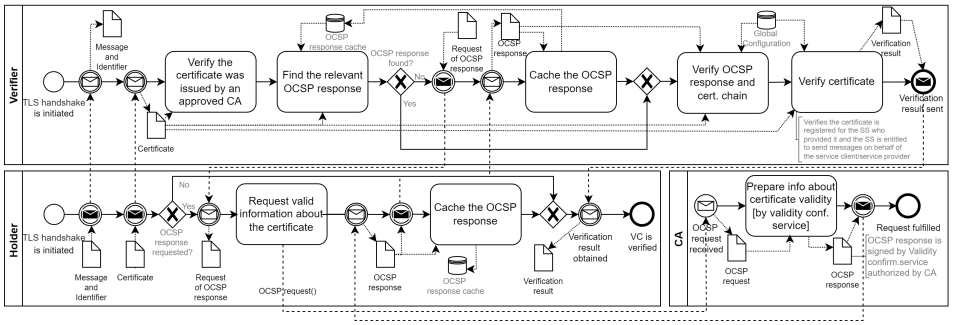


Figure 21: Credentials verification using PKI

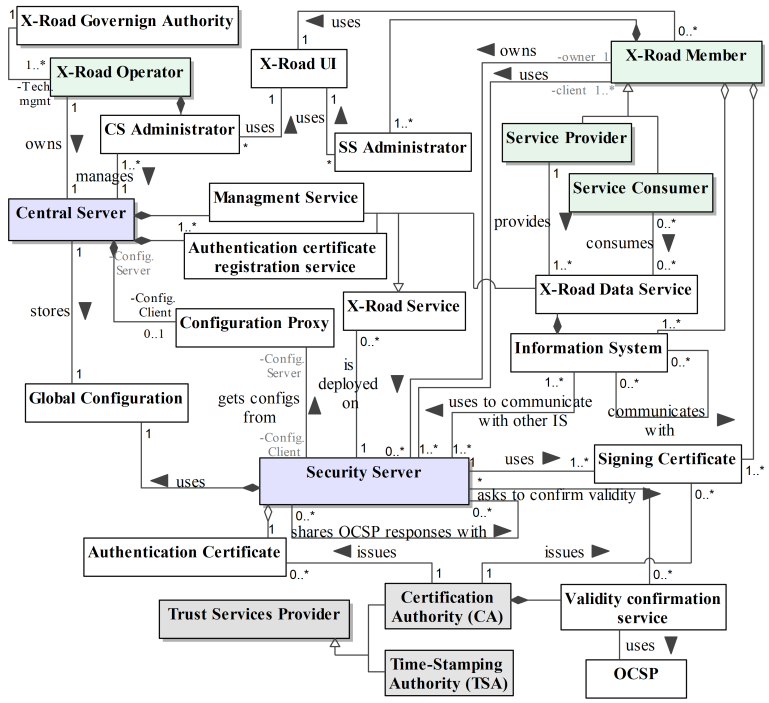
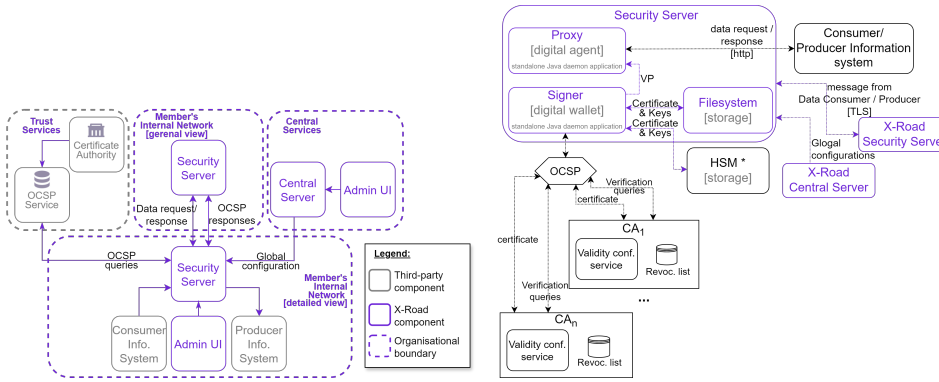


Figure 22: Entities in the X-Road system (green – network participant and their roles; purple – core system components; gray – external trusted service providers) [60]

The class diagram lets us depict formal dependencies between system components and their relationship (including the multiplicity of entities), however, it is too detailed due to depicting the key functionality along with identity management. Therefore, Figure 23a presents the conceptual security architecture of X-Road with a focus on identity management [198].

To understand the trust dynamics within the current system, we focus on the interdependencies among X-Road actors. Specifically, we analyse how actors rely on each other to achieve their respective goals. To model these social dependencies, we leverage the i*/Tropos framework, which, as demonstrated in [207],



(a) General security architecture (adapted from [61])

(b) Architecture of IdM in Security Server (adapted from [60])

Figure 23: PKI-based X-Road architecture

effectively captures the social context and stakeholder relationships that influence system requirements. Figure 24 illustrates the social dependency model within the X-Road ecosystem enabled by PKI. Three key actors – the X-Road Operator, the Certificate Authority (CA), and the X-Road Members – exhibit interdependencies.

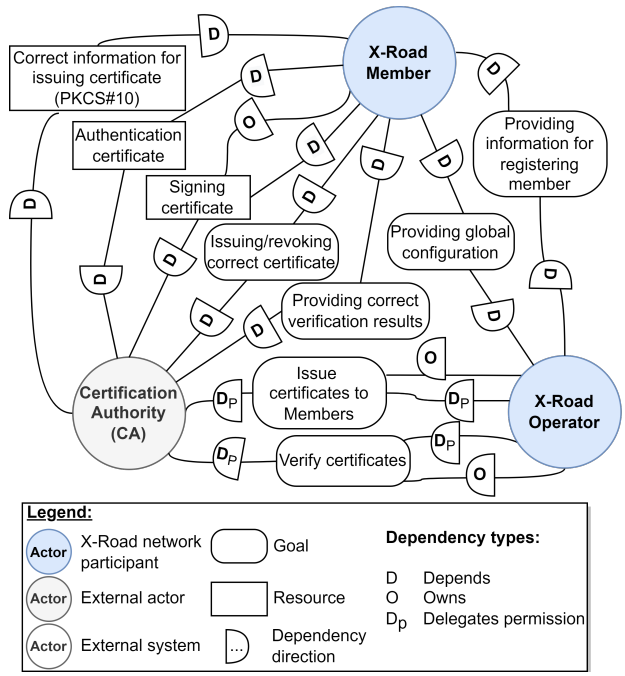


Figure 24: Social dependencies in the PKI-based X-Road

The X-Road Operator relies on the CA to fulfil critical functions, including issuing and verifying both signing and authentication certificates. This delegation of responsibility signifies a trust relationship between the Operator and the CA. Members have a stronger dependency on the CA, relying on it for accurate certificate issuance and revocation, reliable verification results, and the provision of authentication and signing certificates for their Security Servers. Conversely, the CA relies on Members to provide accurate information for certificate issuance.

Furthermore, the X-Road Operator and Members exhibit mutual dependencies. The Operator relies on Members to provide information for registering in the X-Road system, while Members depend on the Operator to provide the necessary global configuration. In summary, the CA plays a crucial role as a Root of Trust (RoT), and the entire X-Road ecosystem heavily relies on its services.

5.3.4. Step 3. Assess the As-Is IdM System

To assess the current PKI-based IdM system in X-Road, we use the IdM quality assessment model, presented in Section 5.2.1. In Table 13, the column called "PKI" contains the measurement of the As-Is IdM system, and the explanation of each measurement is elaborated in the following paragraphs.

Security. As the PKI-based IdM assumes the full trust of the identity owner to the credentials holder, there is no built-in mechanism for **preventing insider threat**. Thus, the access control to credentials should be implemented separately from the IdM system.

The PKI IdM relies on issuing and verifying credentials by a selected issuer (i.e., CA). Therefore, there is no **decentralisation of credentials issuance and verification** – both procedure and centrally managed by a CA.

Similarly to the prevention of privilege misuse, as the PKI-based IdM assumes the full trust of the identity owner to the credentials holder, organisation-identity in X-Road can define a holder (system administrator or third-party service provider that manages Security Server) of identity keys who is in full controller over key management. Thus, there is no **decentralisation of key management**.

Trustlessness of the IdM system is defined by the fact of not having the need for full trust of an organisation in a single external or internal entity. The current system has one trusted external entity (CA) and a trusted internal entity (Security Server, which is an identity holder). Thus, the current IdM system does not support trustlessness.

The **availability** of the IdM system is defined by the following systematic delays. First, the time of credentials issuance varies (i.e., P) and is defined by the procedure used by CA for identity registration and credentials issuance. Thus, based on the insights from the experts in NIIS [131], the time for credentials issuance may vary from days to months. Meanwhile, we do not recognise any systematic delay in the signing process, as signing is done automatically in the Security Server upon request. In contrast, there might be a delay in seconds for

Quality criteria	Quality sub-criteria	Indicators	How to measure	Measurement				
				PKI	DPKI	DPKI vs PKI	DKMS	DKMS vs PKI
Security	**Preventing insider threat**	Fact of having built in prevention mechanism	Yes / No	No	No	=	Yes	+
	Decentralisation	Decentralisation of credentials issuance/verification	Yes / No	No	Yes	+	No	=
		Decentralisation of credentials and keys management	Yes / No	No	No	=	Yes*	+
	Trustlessness	Not having a single of fully trusted external entity	Yes / No	No	Yes	+	No	=
		Not having a single of fully trusted internal entity	Yes / No	No	No	=	Yes	+
	Availability	Systematic operational delays	Time of credentials issuance / signing / verification	P / 0 / msec *	sec / 0 / sec*	+	P / msec* / msec *	-
Control	**Responsibility over credentials**	Level of responsibility over credentials by the identity	{0, 1, 2}	1	2	-	1 *	=
	Control over identity attributes	Control over the revealed details	Number of entities to who the attributes from the credentials are revealed during issuance / verification	1 / 1	1 / 0..1 *	+	1 / 1	+
	Traceability	Fact of having built in traceability mechanism	Yes / No	No	No	=	Yes*	+
Usability	**Portability**	Fact of having built in mechanism for portability	Yes / No	No	No	=	Yes*	+
	Multiple users	Fact of having built in mechanism for having multiple users	Yes / No	No	No	=	Yes	+
Maintainability	**Backwards compatibility**	Fact of being backwards compatible with PKI	Yes / No	--	No	-	Yes	+
	Complexity	Dependence on social actors	Number of actors involved in the credentials issuance /signing / verification	1 / 1 / 2	1/ 1 / 1	=+	1 / K / 2	-
		Dependence on external systems	Number of systems to be integrated with for issuance/ signing / verification	0 / 0 / 1	1..2 */ 1 / 1	-	0 / 1 / 1	-

Table 13: IdM system quality assessment results

the credentials verification due to the need to obtain credentials validity confirmation from the CA-issuer. A verifier relies on the OCSP caching managed by the Member (identity holder). The OCSP caching system is highly fault-tolerant and configurable [208] and includes delays in the scale of milliseconds [209]. As a result, the integration of Members' Security Servers with the CAs' validity confirmation services through the usage of OCSP and sharing the cached results of credentials verification between SSs provide a high level of system accessibility during the credentials usage.

Control. In terms of control over the keys, PKI may allow Members to recover the lost private keys (if the service provider generated them), giving the Members some flexibility and the right to make mistakes. On the other hand, Members cannot create credentials for joining the X-Road network independently or based on the previous credentials and should rely on a trusted CA for the assertion. Given the current system, we assign a responsibility level of medium (1) for credential management, indicating shared responsibility between the entity and the issuing authority.

In terms of **control over identity attributes**, during both credentials issuance and verification, the identity holder should fully reveal the attributes of the identity, as the whole PKIX certificate is presented to the verifier. In the case of Member's identity, it means that if based on the rules of the X-Road instance the signing certificate should contain attributes the Member-Client perceives as sensitive organisational data, the Member-Provider (verifier of the data request) would be able to see such sensitive organisational data. For example, such sensitive data may be presented by the details of the Member's certification (e.g., against information security standards) or the Member's organisation name (which would want to be kept secret for the data exchange).

Similarly to the prevention of privilege misuse, as the PKI-based IdM assumes the full trust of the identity owner to the credentials holder, the usage of the Member's signing certificate cannot be traced back, and only the Security Server (Member's identity holder) has the right of signing certificate usage. Meanwhile, the Member's information system should have its own logging mechanism for tracking the data request sent to the Security Server on behalf of an organisation. As a result, the system does not support **traceability**. In the case of X-Road, the signing certificate is used in a separate system component (Security Server) from the one where the data request originates from (Member's information system used by either end-users or its sub-components), therefore, such flow of the unsigned message from the place of origin to the place of its signing in the Security Server may lead to the Man-in-the-Middle attack (e.g., within IS or within Security Server) threatening the authenticity of the data request.

Usability. As PKIX-related keys should be stored in the predefined during the issuance form (as a software or hardware token, for signing certificate, and as a software token only for authentication certificate), the PKI-based IdM system is not **portable**. The standard PKI-based system does not have a built-in mechanism

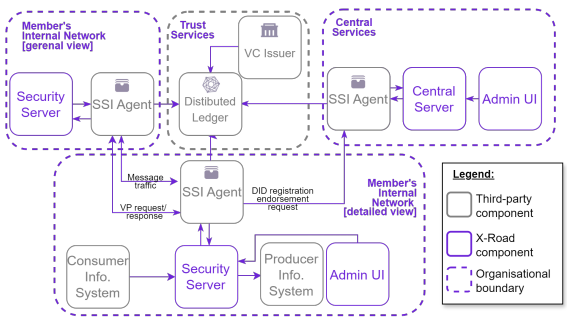
for differentiating users of credentials as it has only one holder at a time. Thus, it does not support **multiple users** per se.

Maintainability. As the PKI-based system is the currently used one, we do not assess its **backwards compatibility** as it is considered a baseline for the alternative IdM systems in X-Road. Finally, The assessment of **complexity** is defined by the dependence of organisational identity on the social actors and external systems. Thus, for credentials issuance, IdM depends only on CA and its ability to assert credentials, while in general, no system is required for it. For signing, IdM depends only on one identity holder and no external system is involved. Meanwhile, for verification, both the identity holder and CA should contribute, which requires the usage of one external system, namely, the CA's validity confirmation service that relies on OCSP.

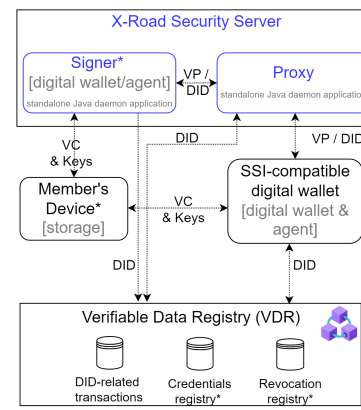
5.3.5. Step 4. Model the To-Be IdM System

In line with the principles of Self-Sovereign Identity (SSI), this section presents the integration of a Decentralised Public Key Infrastructure (DPKI) into the X-Road ecosystem. We detail the process of incorporating the DPKI within the data exchange system and the utilisation of newly introduced credentials by Members and Security Servers (SSs) for identity verification. The proposed design postulates a shift towards DID-based credentials primarily for Members' identities.

The conceptual architecture of the DPKI-based X-Road Security Server is depicted in Figure 25a. The components coloured in purple are part of the X-Road system, and the other black-coloured components are external entities.



(a) General architectures of the DPKI-based X-Road (adapted from [61])



(b) Architecture of IdM in Security Server (adapted from [60])

Figure 25: DPKI-based X-Road architecture

The proposed DPKI-based IdM relied on the set of preliminary decisions that the X-Road system owners should make. First, the owner should select a distributed ledger for the verifiable data registry (VDR) and the DID method to be used by Members for DID-related transactions. The ledger could also be used

to back up the credentials and revocation registries. Second, the owner should select the implementation of verifiable credentials (VCs). Third, the distributed IdM allows the Members to use an external SSI-compatible digital wallet as an alternative to the Signer component of the SS. Thus, the X-Road SS should enable integration with such SSI-compatible digital wallets. The Signer component in the to-be system may be used to store the credentials and key locally on the Member's device. However, its usage is optional, and the full control over identity-related operations may be delegated to an SSI agent and wallet. Thereby, SSI-agent becomes in control of the Members' identity, distributing the responsibilities over the communication control and identity management in X-Road between the Security Server and the SSI-agent. As a result of SSI-agent and VDR usage, the need for integration with the Online Certificate Status Protocol (OCSP) and CA's validity confirmation service is eliminated.

The DPKI-based X-Road should use verifiable credentials and DID-based signatures instead of PKIX certificates. Figure 26 contains a BPMN model which outlines the process of obtaining DID in the selected VDR needed for onboarding an organisation to X-Road. The procedure of obtaining DID for a Member is analogous to the signing certificate issuance in the PKI-based X-Road. This process includes creating a DID document with endorsement on a distributed ledger (a verifiable data registry). The process involves generating a DID by the prospect X-Road Member which binds his private and public key, preparing a DID document which binds the newly created DID with the previously existing identifiers (e.g., DID or other unique identifier which defines the organisation outside of X-Road), finding an endorser from a predefined set, obtaining their endorsement based on verifiable credentials, publishing the endorsed DID document. To endorse the DID creation in the X-Road specific VDR, an endorser should verify that the organisation meet the needed requirements based on the provided proofs (created based on the issued earlier VCs and bound to the DID or other unique identifier which defines the organisation outside of X-Road).

Additionally, each Security Server should obtain a DID for its own key. The difference with the Member's DID is that a Security Server can have a self-issued DID document without the need for an endorser. The specific process for obtaining DIDs by X-Road components can be found in Appendix D.2 (Figure 56 and 57). Thereby, the onboarding process of new organisations (including the set up of new Security Servers) stays the same as in the As-Is IdM system, with the difference that a signing certificate is replaced by a Member's DID document, and an authentication certificate is replaced by Security Server's DID document. Thus, the onboarding process depicted in Appendix D.2 stays the same for the To-Be IdM, while the sub-processes of configuring signing and authentication certificates are replaced by the sub-processes of configuring Member's and Security Server's DIDs (the colour-coding in the BPMN models in the To-Be system is saved from the As-Is system).

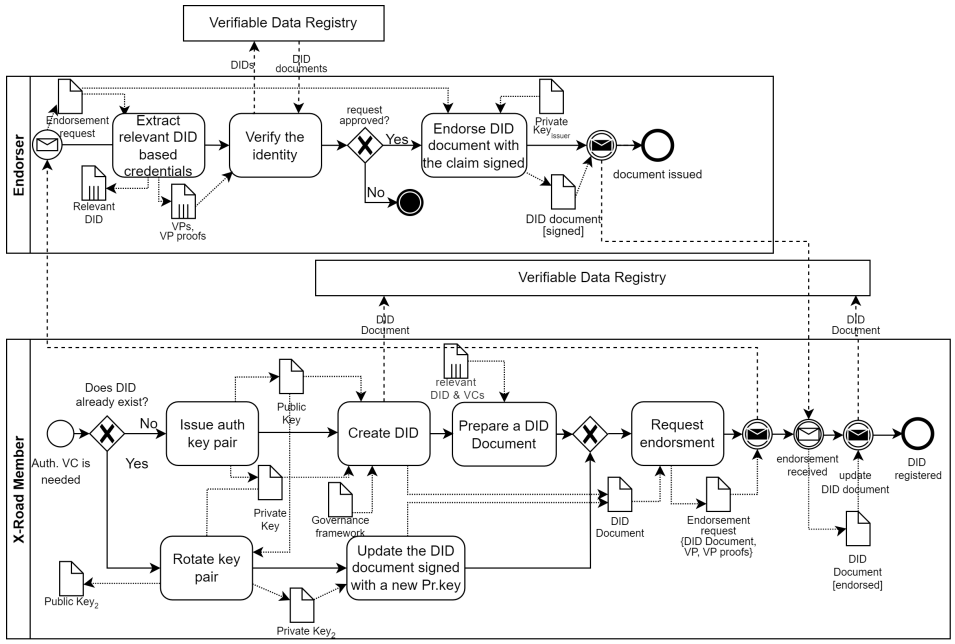


Figure 26: DID issuance to a Member (adapted from [60])

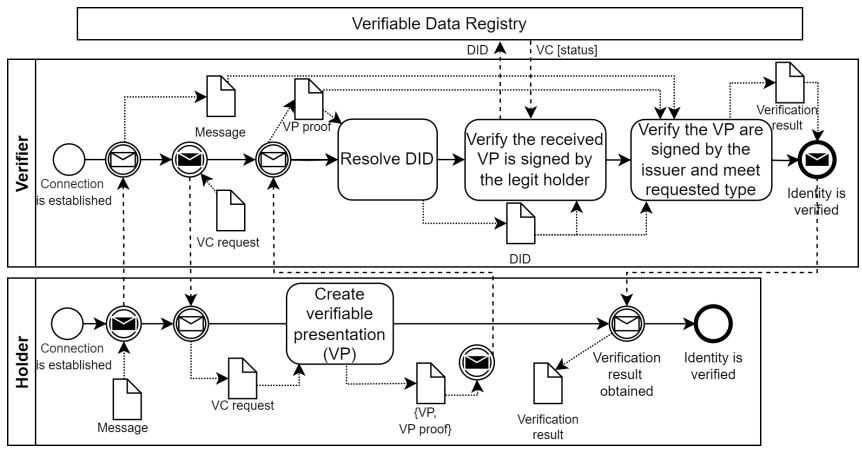


Figure 27: DPKI-based identity verification (adapted from[60])

Figure 27 depicts how the verification of identities should be done in the DPKI-based IdM. The verification of the identity (either Member's or Security Server's) is done based on the VCs issued to the identity outside of X-Road, and its possession should be confirmed by presenting a proof created based on X-Road-specific DID. As a result, the verifying should be able to resolve the DID document from the VDR and confirm that the proof (which is a signature) corresponds to the registered DID and that the VC identifier (or organisation name) is mentioned in the DID document.

There are a few options for the distributed ledger network: it can be explicitly created for X-Road, or the existing special-purpose SSI distributed ledger networks can be used (e.g., Sovrin, Veramo). The comparison of the state-of-the-art blockchain-based SSI solutions [210] shows that Sovrin [211, 212] and uPort are the solutions which are compliant with the most SSI principles compared to other existing solutions. Also, the method for generating DID in the ledger can be selected from the set of existing methods [213] or explicitly created for X-Road. We argue that for the SSI implementation in the data exchange system used predominantly in the governmental sector, GA would prefer the SSI ecosystem based on the private blockchain or at least public permissioned. The reasons are that private blockchains are faster, while both private and permissioned give more control over the network participants [214]. Consequently, Sovrin or the X-Road-specific SSI ecosystem are recommended to be used.

Also, we propose the unification of the credentials storage. Currently, Member should have a dedicated VC_{sign} for usage in X-Road and store such VC_{sign} in SS's filesystem. We suggest that the Member should have one digital wallet to store all its VCs to use for the proof presentation for any verifier – both in X-Road and outside of X-Road. As mentioned above, the Member can choose either an external SSI-compatible digital wallet that will be used or provided by X-Road. We propose to have only X-Road-specific DID per Member, so when the Member wants to prove the identity to another Member without creating any special verifiable credentials. Thereby, the Security Server requests the corresponding VPs from the global Member's digital wallet and only checks that the provided VPs belong to the registered in X-Road DID holder.

Figure 28 illustrates the model of social trust facilitated by DPKI among participants within the X-Road network. The Verifiable Data Registry, depicted as an external system, represents the distributed ledger technology that enables the decentralised storage and retrieval of DID documents (and VCs, if enabled). As a result, the DPKI-based IdM system in X-Road assumes the trust of X-Road Members and Operator in the VDR and cryptography on which VDR is based. Additionally, a Member delegates management of DIDs and trusts that the VDR setup enables the DID document resolution. Additionally, Member's reliance on external CA for verifying its credentials is eliminated, as Member becomes responsible for credentials (in the form of VCs) and providing the respective proof (VP proof) which other Members should be able to verify themselves based on the DID documents and the attributed in the presented VPs.

Comparing to the dependencies in Figure 24, instead of trust to a centralised certification authority, the RoT in the DPKI-based system shifts to the used distributed ledger (i.e. Verifiable Data Registry) and the cryptography on which the ledger is based.

As a result, based on the literature on SSI principles and decentralised public key infrastructure [52, 205, 206], and assuming the usage of a data exchange system for cross-organisational data exchange, we developed a DPKI-based IdM

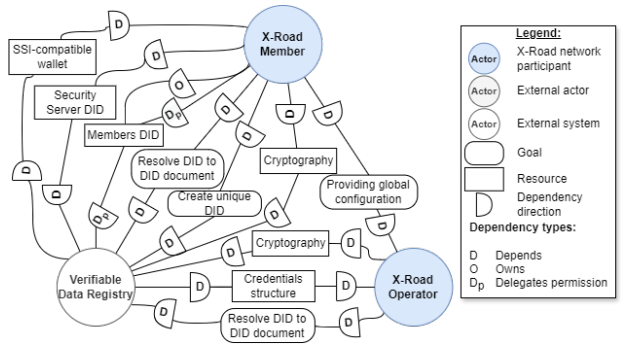


Figure 28: Social Dependencies in the DPKI-based X-Road

system design depicted in Figure 29. While the design is created initially for the X-Road data exchange system, it can be generally used for cross-organisational collaboration using any other data exchange system or for the direct integration of information systems.

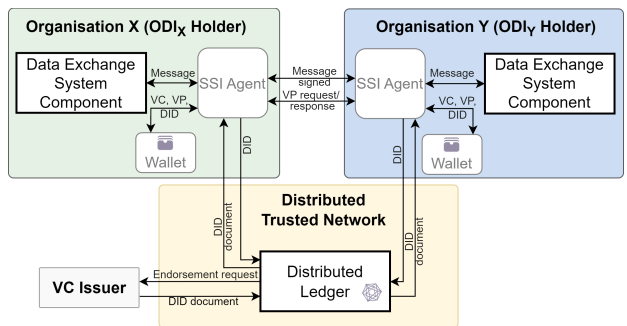


Figure 29: A DPKI-based IdM system

Thereby, the DPKI-based system design depicted primarily in Figure 25 and Figure 29 are the Contribution 3 of this thesis. This design allows securing cross-organisatio-nal data exchange in a smart system using X-Road through the elimination of trust in a centralised Certification Authority (CA).

Study 5: Proof of Concept Implementation. To evaluate the usability of the proposed DPKI-based X-Road, we develop a proof of concept (PoC) implementation. While the PoC corresponds to the proposed architecture, it is based on several set-up decisions. In DPKI-based PoC X-Road implementation, an organisation becomes a Member on the condition of presenting proof (in the form of verifiable presentations) of possessing the required verifiable credentials (VCs). Upon the presentation of valid proof, an organisation's Security Server creates a transaction with a new DID and a Central Server, which plays the role of endorser, is requested to endorse this transaction. Upon successful endorsement, the Security Server request the nodes contributing to the ledger to write the transaction to the ledger. As a result, the created DID document binds the Member's private and public keys, thereby, substituting the signing certificate.

In the PoC implementation[16], the following components are used which, however, should not be considered instructive. The selected technologies or solutions are mainly selected because they are open-source, free and fit together. Meanwhile, there are other alternative solutions that enable the stated functional requirement to be met.

- Hyperleder Indy is selected as a distributed ledger for the verifiable data registry (VDR) where DIDs are stored.
- Sovrin DID method is used as a DID method [216].
- As an SSI agent (and wallet), we use Hyperledger Aries Cloud Agent Python (ACA-Py).
- AnonCreds are selected as implementation for VCs. Aries Protocol, built on top of DIDcomm protocol, defines procedures to establish trusted connections using authentication keys in the DID document[17].

The PoC demonstrates the usage of ACA-Py by only one organisation, which is the X-Road Members. However, ACA-Py supports multi-tenancy [217], and thus, it can be used as a cloud wallet, similar to the As-Is Signer component.

In the PoC implementation, the primary goal is to show how Members can establish secure connections without reliance on a centralised authority (like a CA). Thus, we developed a system where the Member's signing certificate is replaced by a DID document for verifying that the Security Server, which requests the connection, corresponds to a registered Member, which is confirmed by the fact of having a DID document in the VDR. However, the implementation does not allow for the differentiation of Security Servers of the same Member. Thus, the PoC assumes the usage of one Security Server per Member, which is connected to an ACA-Py agent. To enable the differentiation, however, each Security Server may need to have a separate DID per Member.

Within the PoC, the ACA-Py agent replaces the Signer component within existing X-Road Security Servers. ACA-Py additionally assumes responsibility for transmitting messages through a secure channel utilising DIDcomm. This shift in functionality alleviates some of the burdens previously placed on the Security Server's Proxy component.

PoC assessment. An X-Road network instance has been set up with the PoC implementation for evaluating the functional requirements. To become a member of this instance, organisations must have obtained an X-Road membership contract with the X-Road governing authority as a verifiable credential in its SSI agent. In the network, there should be a single Central Server and two Security Servers. There should be a separate SSI agent (ACA-Py instance) for every CS and SS.

[16]The source code of the PoC is available at `https://gitlab.cs.ut.ee/ssi-xroad/ssi-xroad` [215].

[17]The source code of the modified Aries Cloud Agent Python is available at `https://gitlab.cs.ut.ee/ssi-xroad/aries-cloudagent-python` [215].

Two components have been implemented to assist with the evaluation. The first component is a web service as the service provider's information system (has been implemented using Java back-end programming language). It exposes REST APIs for adding and retrieving book records. The second component is a web service that automatically issues credentials on request. It consists of a controller server implemented using Java back-end programming language and an ACA-Py instance. Two types of credentials can be requested. The first one is called "X-Road Membership Contract" and is used for evaluating onboarding-related functional requirements. It contains three attributes, namely "name", "registryCode", and "established". The second credential type is called "Startup Estonia Membership" and is used for evaluating access control-related functional requirements. It contains three attributes, namely "name", "membershipCode", and "startDate". Based on the acceptance criteria of the elicited functional requirements, the PoC implementation meets the design goals and enables decentralised connection ($\mathbf{G}_1$), granular access control, and conditionally enables automated member onboarding ($\mathbf{G}_2$). Thus, depicted in Figure 25 architecture confirms the technical feasibility of the DPKI-based X-Road.

5.3.6. Step 5. Assess the To-Be IdM System

Using the assessment model presented in Section 5.2.1, we evaluate the changes in IdM system quality that define the trustworthiness of the X-Road. In Table 13, the column called "DPKI" contains the measurement of the To-Be IdM system.

Security. As the DPKI-based IdM assumes the full trust of the identity owner to the credentials holder, which is the SSI agent, there is no built-in mechanism for **preventing insider threat**. Thus, the access control to credentials should be implemented separately from the IdM system.

The DPKI-based IdM relies on issuing credentials needed for X-Road usage (substituted by the external VCs and X-Road-specific DIDs) in a decentralised manner. Thus, the issuance of DID documents is based on the distributed network of VDR and is supported by the set of endorsers. Meanwhile, the need for physical identity verification by the VC issuer is eliminated as the architecture assumes that an organisation has the VCs required to join the network in advance of signing the contract with the X-Road Governing Authority, and there is no need for the creation of X-Road-specific VCs. Additionally, the credentials verification (if needed) and verifying the message origin based on the Member's signature are verified against the cryptomaterial in the DID document by the verifiers themselves. Meanwhile, verifiers rely on the distributed ledger to confirm the validity of the VP proofs. Therefore, there is **decentralisation of credentials issuance and verification** – both procedures are managed by the network of nodes contributing to the VDR, a distributed ledger.

Similarly to the As-Is system, DPKI-based IdM assumes the full trust of the identity owner to the credentials holder. Thus, an organisation-identity in X-Road can define a holder (system administrator or third-party service provider that manages SSI-agent and/or digital wallet) of credentials and the respective cryptomaterial who is in full control over key management. As a result, there is no **decentralisation of key management**.

In terms of **trustlessness**, the designed system does not have a defined trusted external entity fully responsible for the organisation's identity verification (e.g., like a CA) thanks to the distributed ledger and network usage. However, a trusted internal entity (a manager of the SSI-agent) is still present. Thus, the designed IdM system partially supports trustlessness.

The **availability** of the IdM system is defined by the following systematic delays. First, the time of credentials issuance is measured in second as the DID issuance is done automatically and depends only on the selected DID method and automatic endorser approval. We do not recognise any systematic delay in the signing process, as signing is done automatically by the SSI-agent upon request. In contrast, there might be a delay in seconds for the credentials verification due to the need to obtain the DID documents and automatic proof verification. Thereby, there is an improvement in the system availability compared to the As-Is system.

As a result, thanks to the decentralisation of credentials issuance and verification, which partially enables trustlessness and improves availability in the DPKI-based X-Road, the new IdM system should allow for better security.

Control. As the DPKI-based IdM system defines itself as the requested attributed for credentials and is responsible for providing proofs based on the issued credentials, we assess the level of *responsibility over credentials* as high (2). Similarly to the PKI-based IdM system, the proposed solution does not have any built-in features for *traceability* because it relies on having a defined fully trusted internal actor responsible for SSI-agent set-up and giving access to its usage.

The proposed system allows organisations to use verifiable credentials for **control over identity attributes**. Thus, for issuing a new VC, an organisation reveals its attributes to the issuer. However, verification is done through the defined verifiable presentations to be presented instead of showing the full credentials. Thus, the attributes might not be shown at all and only the proof of meeting requirements is needed. Moreover, in the context of X-Road, if Members do not want to conduct extra identity verification based on VCs for each data exchange, and the data exchange is done only on having valid X-Road-specific DID, there is no reveal of Member's attributes.

As a result, while improved control over identity attributes comes with the cost of higher responsibility over credentials and no traceability is enabled, the shift to a DPKI-based system does not change the quality of control.

Usability. The new IdM system does not support portability or multiple users, and from the end user's perspective, there are no changes compared to the current system. Thus, the IdM system shift does not affect its usability.

Maintainability. Finally, the proposed system requires a lot of set-up efforts as it is not **backwards compatible**. Specifically, the infrastructure for VCs usage, VDR set up and SSI-agent selection should be done from a technical perspective. Additionally, the new trust model requires the definition of a new governance model for X-Road and assumes having a decentralised governance model for issuers which support VCs outside of the X-Road network.

The assessment of **complexity** is defined by the dependence of organisational identity on the social actors and external systems. As we assume that there are no X-Road-specific credentials per se for the X-Road onboarding and only a DID document is created, thus we assume having the need to obtain a pseudo credential (i.e., DID document) for which one actor, namely the endorser. Additionally, an SSI-agent should be used for these pseudo credentials issuance. Additionally, there might be a need for a decentralised application for writing transactions about DID in the ledger if the VDR is set up in the respective way. For signing, IdM depends only on one identity holder and SSI-agent as an external system. For verification, only the identity holder should contribute with the signature, which requires the usage of one external system, namely, SSI-agent. Thus, while the DPKI-based system relies on more external systems (including VDR and SSI agents) for different purposes, the number of dependencies increases, even though complexity is not bound to one organisation but comes from the network infrastructure. As a result, the system maintainability is downgraded.

5.3.7. Evaluation

Table 13 provides the overview of the evaluation results. Based on the qualitative evaluation results, which are grounded on the findings from the literature review and observation from PoC implementation, we conclude that the shift from the As-Is to the To-Be IdM system in X-Road would allow for an improvement of the IdM's security but worsen maintainability.

Thus, overall, a shift brings an improvement to the IdM system quality if organisations using the IdM have resources for more complex maintenance. Additionally, the gains from the decentralised approach are offset by the time and resources needed to build the underlying infrastructure, which includes establishing a new governance model in the ecosystem outside of X-Road itself along with the technical DPKI-based system setup. The ease of meeting prerequisites for a new system may vary depending on the industry, the specifics of the system, and the number of current system users.

To conclude, the evaluation results validate the effectiveness of the proposed DPKI-based IdM system (*Contribution 3*), and the PoC validates its usability in the running X-Road instances. Besides, the proposed DPKI-based IdM system has been presented to the X-Road community during the yearly X-Road event[18], where the community representatives pinpointed the analogous weaknesses of the

[18] `https://x-road.global/xroad-community-event-2022`

solution to the ones identified through our assessment. Thereby, while the proposed solution achieves the goal of removing a centralised trust over ODI by the Certification Authority (CA) for ODI's verification, the solution has limited usage in smart systems due to the complexity of its setup.

5.4. Distributed Key Management System

The results of the DPKI-based system evaluation show that while offering enhanced security and identity control, a DPKI-based identity management approach demands a new governance framework and substantial infrastructure changes. Implementing such systems, particularly for public sector actors using data exchange systems like X-Road [218] and Gaia-X [219], requires considerable time and potential legislative alterations.

Furthermore, although decentralised trust and IdM address external threats, internal actors may remain a primary source of data breaches through the misuse of privileges [220]. Consequently, the threat of centralised control used by internal actors persists, undermining the authenticity of messages transmitted on behalf of the organisational identity.

Regardless of the identity and trust model, organisations may use digital wallets or hardware security modules as a part of their Information System (IS) to store their identity's certificates and key material, with policies defining access rights [145]. Proprietary solutions like OpenID [175] control internal authorisation, determining who can initiate cross-organisational data exchange on behalf of ODI. Meanwhile, some organisations prefer external trusted partners to manage their identity and key materials [145, 143, 146], removing access control from their IS, but this raises concerns about potential compromise or misuse. Based on [145] and results of Study 5 in this Chapter, we recognise the need for a more secure yet backwards compatible identity model, which would allow enforcing security through custom access policies (under what conditions are ODI-related cryptographic keys used) for information systems that rely on a centrally issued ODI (Problem 2 in Section 5.2).

5.4.1. Design Goals

Assuming centrally issued PKI-based credentials, we aim to eliminate centralised usage of identity by embracing the zero trust (ZT) paradigm [221]. While key management enables digital identity per se, this study considers the following research question $RQ_{3.4}$: *how to secure a centrally issued organisational digital identity through key management mechanisms for achieving zero trust*? To address Problem 2 (see Section 5.2) of the As-Is PKI-based identity management system, we propose a Distributed Key Management System (DKMS) that eliminates the risks associated with centralised control over an organisation's identity and allows organisation-enforceable policies. The DKMS should use partial custody and threshold signatures to secure ODI in cross-organisational data exchange.

Thus, we aim to eliminate the delegation of an ODI to a single SS component and enable the zero trust principle to manage identity and improve security. The following goals should be achieved:

- $\mathbf{G}_1$. Member's ODI cryptomaterial is not in the sole control of one entity.
- $\mathbf{G}_2$. Member can trace back the internal initiator of the message sent on Member's behalf through X-Road.
- $\mathbf{G}_3$. Member can define the access of internal entities to operations on its behalf.
- $\mathbf{G}_4$. The system is backwards compatible.
- $\mathbf{G}_5$. No single entity can create a valid signature.

5.4.2. Step 1. Define the Purpose of IdM System

The purpose of the As-Is PKI-based IdM system in X-Road has been define during development of Contribution 4. Mainly, the IdM aims to support the establishment of trust between Members (organisations) during cross-organisational data exchange. For this, two types of PKIX certificates are used – signing certificate and authentication certificate. The former has the more important role in the establishment of social trust as it serves as an enabler of proving the authenticity and integrity of the exchanged data messages. In particular, the signing certificate and the corresponding cryptomaterial (including private and public keys) are used for signing the message before it leaves the trusted by a Member-creator environment so that a Member-receiver can verify the origin of the message using the respective PKIX certificate. Meanwhile, the latter certificate (authentication) primarily serves the role of establishing a secure connection between Security Servers. Thereby, the authentication certificates do not directly contribute to social trust establishment between Members and are not bound to a specific Member due to the Security Servers' multi-tenancy. Hence, in this study, aiming to mitigate the abuse of organisational identity in X-Road, we focus only on signing certificates for Member's identity verification by creating proof in the form of a digital signature.

5.4.3. Step 2. Model the As-Is IdM System

This step is built on the results of the same step within the DPKI-based system design. However, while in the previous design, we paid attention to the issuance of credentials and verification of Members' identities, in this study, we focus on how the credentials are used within each Member's system for creating the proofs. Using the same terminology for the X-Road ecosystem as in the previous study, let us describe in detail how the identity proof is created.

Figure 30 illustrates the trust relationships within the X-Road ecosystem enabled by PKI with a focus on key management. This social dependency model extends the dependency model created in the previous section with goals related to message signing.

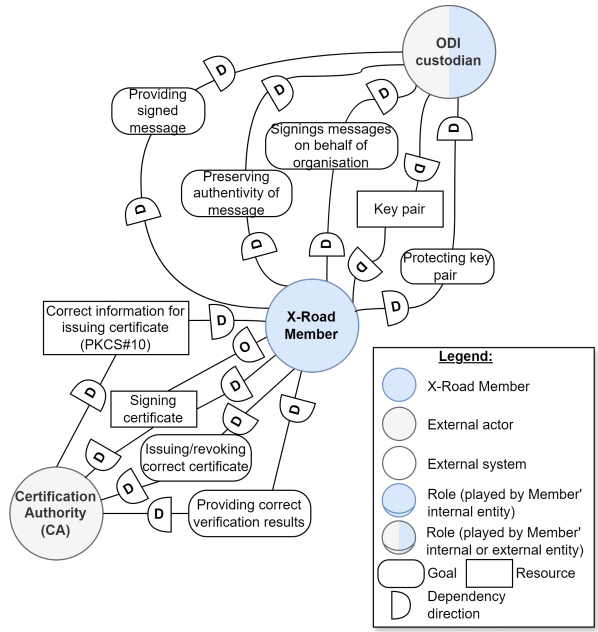


Figure 30: Social dependencies for ODI usage in the PKI-based X-Road

An organisation-Member that creates a message (e.g., Data Consumer who wants to send a data request) depends on the ODI custodian to sign the message on its behalf, preserve the authenticity of a signed message, and protect the provided Member's key pair. Meanwhile, the role of ODI custodian is played by a Security Server that can be presented either by a Member's employee or service or by an external entity (i.e., third-party) service provider. Thereby, the dependency model depicts the full reliance of the Member on the ODI custodian for message signing and its key pair management.

In the As-Is PKI-based system, a Member (ODI holder) should use a private key (corresponding to a public key in the Member's signing PKIX certificate) for signing a sent message (data service request or response). The signing is done by an X-Road Security Server on behalf of the Member who sent the unsigned message from its information system to the SS. When another Member's Security Server (verifier) receives a message through X-Road, the signature of the received message is verified against the public key mentioned in the signing certificate of the message's creator. Figure 31 depicts the described flow of the data exchange within X-Road.

The marked red and green data objects highlight that the message originates in the Member's IS and is sent in the plain (unprotected) to the Member's SS for being signed. Thereby, the message is vulnerable to manipulation by the SS, which is assumed to be fully trusted. Some organisations opt for full custody over their identity and key materials by an external trusted partner who manages the used SS. While such trusted internal and/or third-party entities have direct access

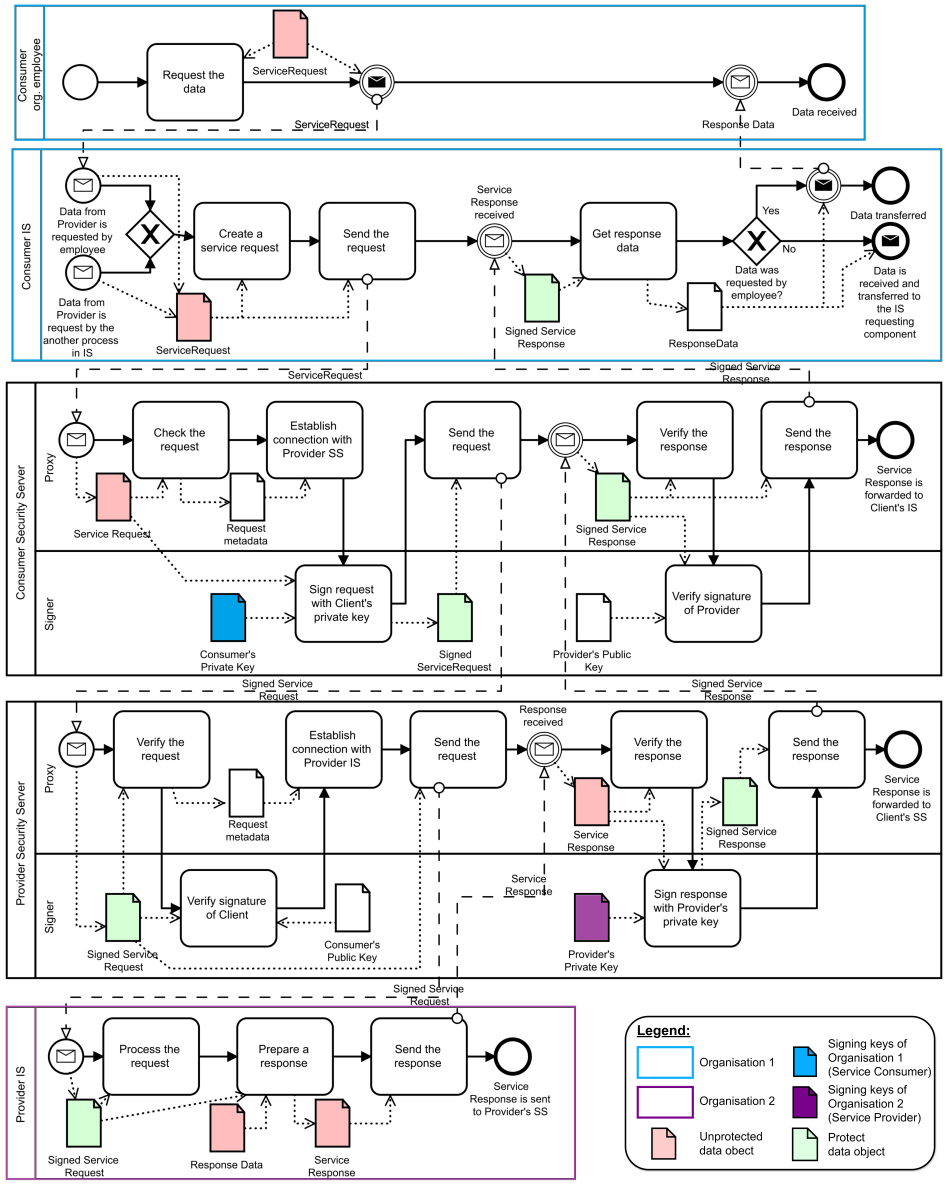


Figure 31: Message exchange within the PKI-based IdM system

to the ready-to-be-signed messages and the ODI keys, the organisation cannot be certain that such entities are not compromised and are not intended to misuse the privilege. Thereby, the Member becomes vulnerable to the negation of integrity or even authenticity of the messages sent on behalf of its identity as SS has full access to the unprotected message requests and responses, being able to (*i*) read or update its content; (*ii*) create new messages on behalf of its Members-Clients.

5.4.4. Step 3. Assess the As-Is IdM System

The assessment of the As-Is IdM system is not repeated for this study as it is the same as for the previous study. Thus, the results can be found in Table 12 in the column titled "PKI".

5.4.5. Step 4. Model the To-Be IdM System

This section presents the design of an IdM system with the distributed key management system. The proposed To-Be system assumes that a Member's identity credentials depend on PKI and PKIX certificates, thereby specifying a selection of cryptographic and business mechanisms for each stage of the key lifecycle. The design seeks to eliminate the centralisation of control over Organisational Digital Identity (ODI) throughout the keys' lifespan. Additionally, it aims to broaden the set of representatives or custodians to enable partial custody of ODI. Figure 32 depicts the conceptual model of a Distributed Key Management System (DKMS).

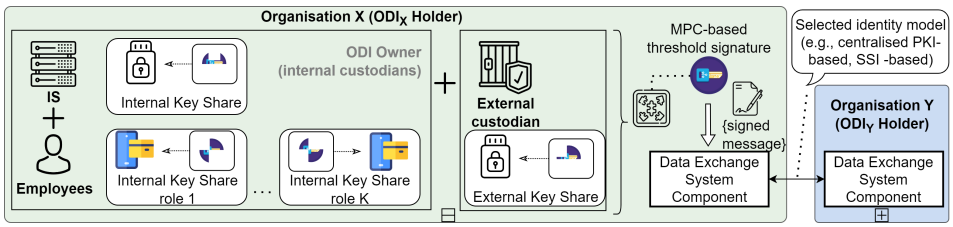


Figure 32: DKMS for organisational digital identity in cross-organisational data exchange [62]

To integrate zero trust principles into the management of ODI, we propose a combination of self-custodian and custodian control, i.e., *partial custody*. A Member's information system with centralised control over ODI is susceptible to a single point of failure [52] due to the reliance on a single fully trusted entity (i.e., Security Server) for signing messages on behalf of the Member. If the Security Server is compromised or its administrator becomes malicious, the Member's IS cannot ensure the authenticity and integrity of the provided information.

Partial custody introduces decentralisation of control and storage of keys for signing or recovery purposes. Consequently, the system can operate with reduced trust in any single entity. The distribution of keys eliminates the single point of failure, as multiple key controllers would need to collaborate to compromise the system's security. Thus, partial custody enhances the overall security posture of an IS and mitigates the risks associated with centralised key control.

To achieve zero trust through partial custody in DKMS, the decentralisation of key control can be introduced in one of two stages: during key generation or distribution. First, keys can be initially generated in a decentralised manner. This approach involves decentralising ODI by employing self-sovereign identity principles and decentralised key generation for all entities involved in ODI management and data exchange (similarly to what is proposed in Contribution 3). Second, if a

centrally generated master key is necessary (and what we assume to be the case for X-Road), decentralisation can be introduced during the distribution of the keys. This can be achieved through distributed key generation or key share derivation, ensuring that the derived sub-keys are used during the operational phase.

Regardless of the phase during which key shares are generated and distributed to semi-trusted custodians, a Member can derive multiple keys to enable distributed key storage and threshold signature creation. Semi-trusted custodians can include internal entities (IS components or employees) as well as external service providers (i.e., external custodians). When new employees join and old ones depart, distributed key generation re-sharing can be performed while maintaining the same (certified) public key.

For controlling the distribution of keys, we employ *partial custody* through the use of *threshold signatures*, where internal entities (such as employee roles and an information system component) and an external custodian collaborate in signing messages on behalf of a Member. Users' keys serve as key shares for the threshold signature, with access to these shares governed by the user's identity in accordance with the organisation's internal policy. Each entity can utilise *different token forms* to store its share. Thus, the proposed DKMS incorporates threshold signatures as a policy decision point component in alignment with zero trust architecture [58]. Thereby, a threshold of K shares protects the Member against a compromise of up to K – 1 signing parties.

We established the distributed key management system in X-Road, as illustrated in Figure 33, to assess its feasibility. In this diagram, white classes represent current X-Road entities, green classes denote the newly added DKMS components, and dark grey indicates the services used to implement DKMS within X-Road. Currently, each Member relies on a fully trusted custodian, represented by a Security Server (SS), who is responsible for managing the Member's keys and signing messages on behalf of the organisation. The key management can be handled either by an external service provider or by the Member itself.

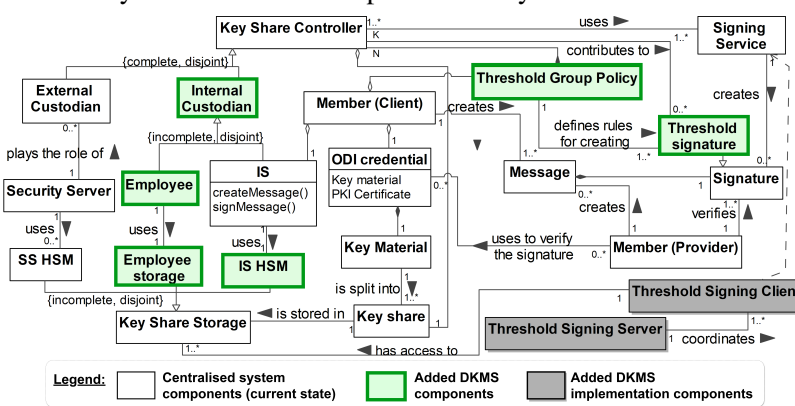


Figure 33: DKMS-based X-Road (N – the size of a group, K – threshold number of controllers contributing to a signature, K $\leq$ N) [62]

Figure 33 illustrates the design of the DKMS for the Consumer's side only. This implementation ensures the integrity of data requests sent on behalf of the Consumer's ODI. A similar DKMS can also be implemented on the Provider's side to ensure the authenticity of the response to the Consumer's request.

To eliminate centralised management, we employ threshold signatures, thereby increasing the number of key controllers from one to N, with at least $K \leq N$ controllers required to generate a valid signature. Each controller can enforce different policy rules for the use of its key. As a result, the DKMS-enables system enables another trust model additionally to the ones presented in Chapter 2 – distributed (or hybrid) trust model which is depicted in Figure 34.

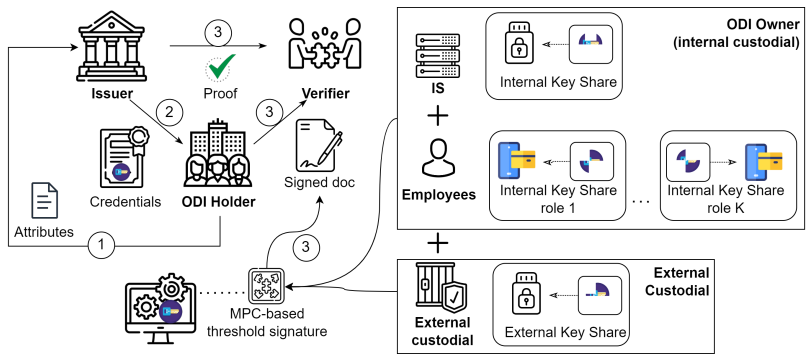


Figure 34: A distributed (or hybrid) trust model enables by a distributed key management system

One of the options for implementing the DKMS in X-Road is distributing the Member's identity key material among three key share controllers already involved in the message exchange process: (*i*) the Member's information system, which is used to create the message; (*ii*) the Member's (i.e., Consumer) employee, who creates a data request to ensure that the request originates from the Consumer's identity; and (*iii*) the Security Server (SS) used by the Member for message exchange. Figure 35 depicts the described key distribution process.

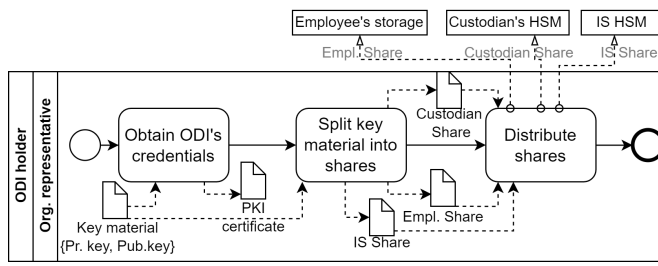
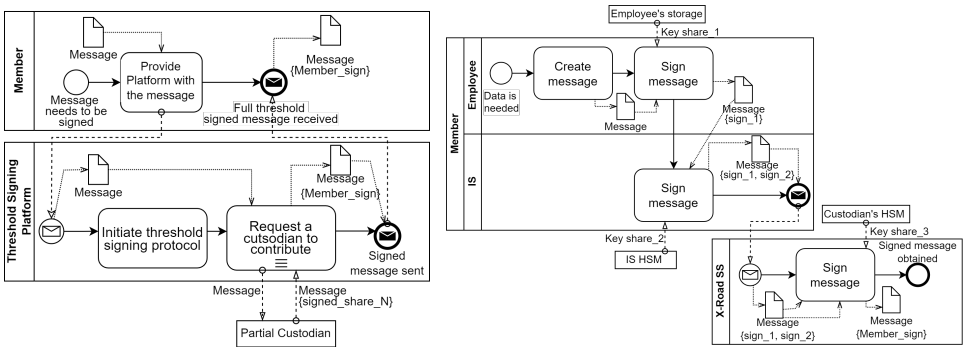


Figure 35: Shares distribution in a DKMS-based X-Road

Employees may store their key share on a cryptographic smartcard, while the external custodian (represented by the SS) and the Member's information system may use Hardware Security Modules (HSMs) as key share storage. The threshold signing scheme [155] ensures full backward compatibility with the latest X-

Road version 7.0.0. The chosen scheme requires a trusted dealer to generate and distribute the individual key shares [155]. We have designated the Member's appointed representative (e.g., an administrator) to serve as the dealer for ODI keys, granting them control over the distribution of individual shares. Once the shares are generated, the dealer must securely delete the private parameters used during the generation process.

For multiparty threshold signatures, a Member can use a selected threshold signing platform. The process of creating a signed message ready to be sent through X-Road using a threshold signing platform is outlined in Figure 36a from the signing platform's perspective. Figure 36b depicts the flow from the perspective of semi-trusted custodians when they are a Member's employee, IS and SS.



(a) Signing in a DKMS-based X-Road (b) Signing in a DKMS-based X-Road with 3 custodians

Figure 36: DPKI-based X-Road architecture

In Figure 37, we depict the new social dependencies established in the DKMS-based X-Road from the perspective of the ODI owner (i.e. X-Road Member). The social dependency model illustrates the distribution of dependencies to multiple ODI custodians coordinated by a threshold signing platform (an external system). Thereby, assuming that one of the custodians is the message originator and there are at least 2 custodians ($N \geq 2$) some of which are external entities, the DKMS-based X-Road allows the ODI owner avoids centralised trust.

To sum up, the DKMS-based system design depicted primarily in Figures 32 and 33 forms the Contribution 4 of this thesis. This IdM system design allows securing cross-organisational data exchange in a smart system using X-Road through the elimination of trust in a single ODI custodian within organisations contributing to a smart solution.

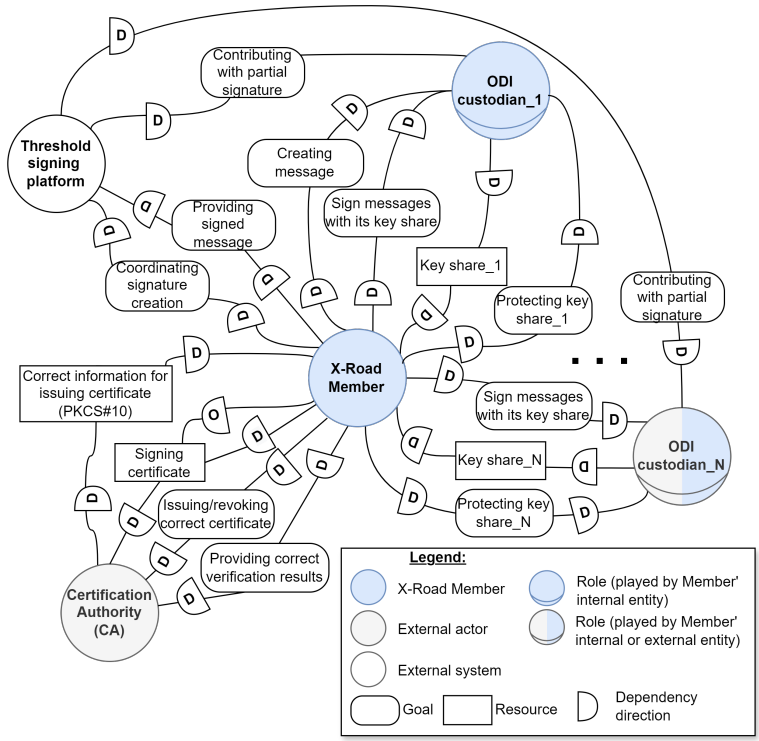


Figure 37: Social dependencies for ODI usage in the DKMS-based X-Road

Study 6: Proof of Concept Implementation.

Smart Parking Scenario. Within this study, we consider the scenario of the smart parking solution analogous to the one used in Case Study 4. However, in Case Study 4, the parking lot terminal (PLT) and parking service provider (PSP) have direct system integration. Meanwhile, in this study, we consider using the X-Road data exchange system as an enabler for data exchange among multiple parking service providers (PSP) with multiple parking lot terminals (PLT) and other parking enforcement agencies. Additionally, there is a national transport administration agency.

In this smart parking system, parking enforcement agencies (e.g., presented by PLTs) are tasked with ensuring compliance with parking laws and regulations by checking whether the parked vehicles have a valid parking permit, allowing access to the parking lots through tolls, and transferring fines to the transport administration agency. The parking service providers (PSPs) manage how drivers access the parking lots, issue parking permits and handle payments. A transport administration agency is a key smart parking system manager that defines rules for the parties' interactions and oversees X-Road. X-Road enables data exchange between stand-alone information systems used by each party.

In the smart parking scenario, where there might be more than one parking service provider and parking enforcement agency, each system participant wants to have guarantees that the entity requesting the data is a trusted entity. Therefore, each parking service provider, each parking enforcement agency, and each transport administration agency should have credentials for its systems (or system components) that would bind these systems with the organisation using PKI. As a result, PKI would enable smart system contributors who act as data providers to validate the identities of the data clients (and vice versa).

Implementation. In the DKMS PoC implementation[19], we integrate the threshold signing platform with X-Road to implement the proposed design via the supported cryptographic interface PKCS #11 protocol. The selected threshold signature scheme is compatible with the current Rivest-Shamir-Adleman (RSA) scheme used in X-Road. The threshold signing platform comprises a coordination server and client components (signing service). The threshold signing server can be deployed either by the Member or its SS, with clients needing to be accessible to the signing parties.

To evaluate the quality of the developed PoC, we first conduct a qualitative assessment to determine if the targeted goals are met. Additionally, we perform a quantitative assessment, measuring the time required for message signing and transfer, and comparing it to other commonly used signing tokens.

As the testing scenario, we consider the Smart parking solution described in Section 5.2. One Member is a parking service provider, and another is a parking enforcement agency. The parking enforcement agency (Consumer) has an information system IS_C. The consumer uses Security Server SS_C for the data exchange in X-Road. The parking service provider (Provider) has an information system IS_P that stores parking permit-related data. Provider uses Security Server SS_P for the data exchange. IS_C has a user interface for internal usage by three roles: street inspectors (who work in the field and check vehicles on the streets), gateway keepers (who check work in the field and check vehicles parked on private properties), and volunteers who are citizens that work as inspectors but for a short period of time. Volunteers only have a temporary need to use the system.

The Consumer's key material should be distributed among the IS_C, SS_C, and employees' roles, ensuring that at least five key shares are generated, with each role representative holding an identical share. To facilitate the exclusion of specific key shares, in the real-life implementation, there should be multiple key shares generated for volunteers. Thereby, once their volunteering period concludes, the volunteers' key shares can be marked as "deprecated" (rendering them unusable by the signing service), and other pre-generated key shares can be assigned to the next group of new volunteers. In the testing scenario, we have opted for a 3-out-of-5 threshold signing configuration.

[19]The repository containing the PoC implementations is available at `https://github.com/crocs-muni/xroad-threshold-signatures`

Goals achievement. In the operational phase, the keys required to create a signature on behalf of the Member are distributed among at least three entities — SS, IS, and selected employees ($\mathbf{G}_1$). The threshold group policy, set by the signing service, ensures that key share controllers from the threshold group all participate in the signature creation. This setup enables Members to partially trace the entities (at the role level) that initiated the message ($\mathbf{G}_2$). The Member's representative who defines the threshold group policy can determine which internal entities receive key shares, how the shares are derived, and how access is deprecated. Consequently, the signing service, following the threshold group policy, ensures that only active key shares are used for signature creation ($\mathbf{G}_3$). The implementation employs an RSA-based threshold signature scheme which is fully compatible with the standard RSA verification algorithm in As-Is X-Road ($\mathbf{G}_4$). Moreover, the threshold group policy ensures that IS, SS, and employees contribute to the signature creation ($\mathbf{G}_5$). Therefore, the proposed DKMS for X-Road successfully meets the specified goals, enabling distributed control over the Member's ODI during the operational phase of key usage.

PoC assessment. For time measurements, we used the testing scenario with the Consumer's IS_C, SS_C, and the Provider's IS_P and SS_P. All components ran on a single device as virtual machines. The Provider uses X-Road's SoftToken in SS_P, while the Consumer uses a 3-out-of-5 threshold signing group. The coordination server is deployed to IS_C and connected to SS_C via the PKCS #11 protocol. This setup allows us to measure system throughput with minimal network delay. In a real-world scenario, network requests within the signing group would impact timing, but modifications in X-Road could reduce these delays.

The Round Trip Time (RTT) measurement starts when IS_C requests data from IS_P and ends when the response is received, with the mean RTT over 1000 measurements shown in Table 14. We also measured the Client using SoftToken, SoftHSM, YubiKey (5C NFC), and TPM NTC 7.2.3.1. The DKMS introduced less than 200 ms of overhead compared to the centralised signing solution and even less (10-60 ms) compared to commercial hardware security modules.

Table 14: Round Trip Time (RTT) comparison for Consumer-Provider data exchange (adapted from [62])

Consumer's token*	**SoftToken**	**SoftHSM**	**YubiKey 5**	**TPM NTC 7.2.3.1**	***DKMS PoC***
mean RTT**	82 ms	75 ms	216 ms	260 ms	276 ms
slowdown	x1.0	x0.92	x2.65	x3.18	x3.38

* the Provider uses SoftToken, and the Consumer's signing token varies

** the mean is across 1000 measurements, SoftToken is used as a baseline

The primary limitation of the To-Be system implementation lies in its reliance on a trusted central party (dealer) during the pre-operational phase. This design assumes trust in the Member's representative who oversees key generation, certi-

fication, and the distribution of key shares. As a result, the system is vulnerable to a single point of failure during this phase, particularly before the threshold group policy and signing service are activated. This limitation could be mitigated, albeit at the cost of backwards compatibility, by employing distributed key generation.

5.4.6. Step 5. Assess the To-Be IdM System

As a final step, the changes in IdM system quality are evaluated using the assessment model described in Section 5.2.1. These evaluations are presented in Table 13, where the "DKMS" column shows the measurements for the To-Be PKI-based IdM system that integrates DKMS.

Security. The DKMS-based IdM does not assume the full trust of the identity owner to the credentials partial custodian. The reliance on threshold signature during the operational stage (and, optionally, during the pre-operational stage if distributed key generation is used) of the lifecycle of the keys provides a mechanism for **preventing insider threats**.

The DKMS-based IdM relies on issuing and verifying credentials by a selected issuer (i.e., CA). Consequently, both the issuance and verification of credentials remain centralised, with the CA acting as the sole authority for these processes. In contrast to the PKI-based system, the DKMS-based system does not assume the full trust of the identity owner to the credentials holders (i.e., partial custodians). Thus, organisation-identity in X-Road, with the support of an internal trusted dealer, can define a set of partial custodians-holders of identity key shares who are together responsible for key management and its usage for identity verification. Thus, there is **decentralisation of key management**.

The current system has one trusted external entity (CA) and multiple trusted internal entities-custodians. Thus, the DKMS-based IdM system supports partial **trustlessness**.

The **availability** of the IdM system is defined by the systematic delays which are higher compared to the PKI-based system. First, the time of credentials issuance and verification stay the same as in the As-Is PKI-based system and are defined by the procedure used by CA for identity registration, credentials issuance and the verification service. During the signing, the systematic delay is introduced due to the usage of threshold signing protocol and the added activities for multiple partial custodians (see Table 14). Thereby, there is a downgrade in the availability of the system in a range of milliseconds compared to the As-Is system.

As a result, thanks to the enables insider threat prevention, partial decentralisation and partial trustlessness, and in the cost of slightly downgraded availability, the new DKMS-based IdM system should allow for better security.

Control. In terms of control over the keys, the DKMS-based system gives the Members some flexibility and the right to make mistakes thanks to key backup and verification by a CA. On the other hand, Members within the X-Road network lack the autonomy to create their own credentials, necessitating reliance on a trusted

CA for credential assertion. As a result, we assess the level of **responsibility over credentials** as medium (1). As mentioned earlier, in the PKIX framework, identity holders have limited **control over identity attributes** disclosure, as the entire certificate, containing all attributes, is presented to the verifier. Thereby, these two indicators stay the same for DKMS-based system just as they are in the pure PKI-based system. The implementation of DKMS demonstrates that the system design helps to achieve **traceability** of signed message origin to the level of roles. As a result, the usage of DKMS allows improved control over identity.

Usability. The new IdM system supports portability and multiple users (i.e., partial custodians) allowing using different key token forms for different custodians. Thus, the IdM system shift improves the usability by end users (even though they should be more involved in the new system).

Maintainability. The proposed system is **backwards compatible** and can be used by only a few Members of X-Road on the side of their own IS without changes required from either other Members or the X-Road setup itself.

The **complexity** of the system is changed only for the credentials signing, where the number of social actors involved in the signing is increased to K (the required threshold of key shares contributors), and one more external system is used for it (i.e., a threshold signing service). As a result, the system maintainability is only slightly downgraded.

5.4.7. Evaluation

Table 13 depicts the evaluation results. Our analysis, informed by both literature review and observations from the PoC implementation, indicates that transitioning from the As-Is to the To-Be IdM system within X-Road would enhance security controls and usability but potentially compromise maintainability.

Thus, overall, a shift brings an improvement to the IdM system quality and allows the improved security of ODI without the need for X-Road update and is feasible to be used by separate organisations. Though the DKMS-based system introduces delays during the message signing, the system is backwards compatible, and the increased signing time is the cost for trustlessness.

Finally, the proposed DKMS-based IdM system has been presented to the X-Road community during the yearly *X-Road community event 2024*[20], where the community expressed their concerns on the decreased efficiency of the solution.

Though the study has been conducted in the context of the problem of centrally issued PKI certificates and certificate-based key management, the review of mechanism and system characteristics is agnostic to the trust model. Thus, the proposed DKMS design (i.e., Contribution 4) can be used for self-sovereign identity-based organisational digital identity where verifiable credentials are issued through a distributed ledger but based on the decentralised public key infrastructure (i.e., Contribution 3).

[20] `https://x-road.global/xroad-community-event-2024`

5.5. Related Work

Recent research has explored decentralised identity management from various angles. For instance, [222] highlighted the potential of distributed ledgers, particularly blockchain, to enhance audibility in healthcare. They argued that blockchain-enabled business processes and IdM can enhance patient privacy and provide more robust digital identity mechanisms compared to centralised or federated architectures. Yet, their research primarily focused on the benefits of blockchain for federated learning and protecting the identities of individuals. ENISA [223] similarly recognised that SSI as an effective approach to managing digital identities and ensuring data protection, emphasising the need for its coexistence with established methods like PKI X.509. Liu et al. [224] identified the trust model and data storage as key differentiators between centralised and distributed ledger-based IdM. They noted the increased complexity of maintaining privacy and implementing identity operations like deletion in decentralised systems. Our research aligns with this focus, examining how decentralised IdM and blockchain can foster trust within business processes and data exchange systems, particularly for cooperation with the public sector.

Grüner et al. [225] proposed a component-based architecture for integrating SSI solutions into web applications. They highlight that SSI solutions are focused on fulfilling users' requirements. But to foster the adoption of decentralised IdM by users, there is an urgent need to facilitate the embracing of SSI principles by the service providers. Huang et al. [134] claim that while technological advances stimulate the need for new technologies, products and services, the trustworthiness of IdM systems is a critical factor in systems design. The paper stresses a fragmented SSI landscape that halts service providers from the decentralisation of trust. To this end, our work proposed an approach of the initial enterprise system analysis, which should guide the service providers on how to move toward embracing SSI and which changes to expect in the dimensions of security, reliability and user control.

Assuming the transition to SSI and decentralised IdM is impossible, the potential usage of zero trust strategy for organisational identity control comes into question. Commonly, for managing the keys related to organisational identities, multiple access control models can be used (e.g. role-based, attribute-based, and discretionary [226]). But to the best of our knowledge, none of the traditional access control models considers the control over keys in view of the zero trust paradigm and the context of cross-organisational data exchange. The closest to our research focus is the architecture vision for the data exchange platform Simpl [175]. There, the authors review three Identity Management (IdM) models: centralised based on PKI [175], hybrid based on PKI and extensions for verifiable credentials [175], and DPKI-based self-sovereign identity with a distributed ledger [175, 227]. However, the three models differ in the procedure of trust establishment between the organisations, leaving out of scope users who act on

behalf of an organisation. Identification of such physical entities is proposed to be handled as a separate task through proprietary identification solutions (e.g., Microsoft Single sign-on, OpenID) [175], internal access control systems, or employee's wallet (digital or smart cards). As the review of zero trust implementations in [228] shows, only studies in [229] and [230] focus on the implementation of zero trust architecture for classical information system (i.e., enterprise systems). Meanwhile, most of the studies focus on cloud-based or IoT systems exclusively, aiming to support the identification of cloud components or IoT devices. Similarly to our work, in [229], the authors proposed to use threshold signature for enforcing zero trust within an enterprise. However, they position the proposed distributed identity management system as a way to protect the enterprise resources, which are used internally, from internal threats rather than as a way for securing organisational data identity in cross-organisational data exchange. Therefore, in Contribution 4, the proposed DKMS bridged two IdM systems – (*i*) for end-users of organisational IS and ODI, and (*ii*) for ODIs and cross-organisational data exchange. As a result, the novelty of the proposed DKMS is in its ability to enforce organisational identity policies for the system users through threshold signature. The proposed solution enables the hybrid trust model, which can be performed in an opt-in and backwards-compatible way directly applicable to existing information systems. The solution cryptographically guarantees compliance with the policies and, thus, enables zero trust within the information system.

Thereby, to the best of our knowledge, the proposed IdM system designs addresses the gap of not having an alternative supportive method that would help organisations make an informed decision about the used identity and trust model. While some studies [175, 222, 223, 224, 225, 229, 230] show how the specific IdM system setup enables solving the very specific security problem or would help to release some security and trust assumptions, they do not provide the procedure on how to make the transition or how to compare the new system with the currently used.

The types of requirements for the organisational identity management system have been defined in [231]. Through literature review and interviews, they have identified four clusters, namely, (*i*) security & compliance (which considers auditability, compliance, integrity and security), (*ii*) operability (which considers automation, availability, cost, effectiveness, efficiency, and manageability), (*iii*) user (which considers control, privacy, simplicity, and trust), and (*iv*) technology (which considers flexibility, interoperability, portability, and standardisation). The identified clusters are wider than the identity management assessment model we proposed (Section 5.2.1). However, most of the criteria and sub-criteria in our model are also present in [231]. Even having a wider scope, the defined cluster only acts as a guide for requirements elicitation, while the model we developed also contains the definitions and indicators for measurements, which allow measurable assessment of the IdM system.

To sum up, the proposed IdM system designs evaluated through the quality assessment model are aligned with the existing research direction. Yet, in contrast to the previous work, our research focuses on protecting organisational identity and investigating how evolving trust models can be instantiated in the context of cross-organisation data exchanges instead of peer-to-peer individual data exchange.

5.6. Discussion

Two design cycles described in this chapter resulted in the development of two alternative IdM systems and their evaluation using the supportive IdM quality assessment model. The two IdM designs were motivated by different problems of the same existing IdM system. Both designs are supported with the PoCs implementations, which illustrate the usage of the selected identity management and trust model in the context of an X-Road-based smart system.

The studies show how implementation of DPKI-based or DKMS-based IdM systems using the research method in Section 5.2 supports the expert group in defining necessary process and system changes (**T1**), establishing an acceptable data-sharing policy (**T2**) with respect to the updated trust assumptions and selected IdM system components. Additionally, the evaluation of the alternative IdM system implementations allows the expert group to ensure the meeting of business requirements by the updated process and the system (i.e., **T3**).

The first version of the IdM assessment model initially used in Study 5 [60, 61] contained only some of the criteria depicted in Section 5.2.1. However, through the multiple evaluation loops in Study 5, the model has been extended to the presented form during Study 6 [62]. Thus, the IdM system assessment results for Study 5 presented in the thesis are extended in comparison with the original publications.

Further, our analysis reveals that the optimal choice of trust and identity models for an IdM system depends on case-specific business objectives and desired system characteristics. All three examined IdM systems based on the various trust models – the centralised, decentralised, and hybrid trust models —- offer distinct advantages and disadvantages. However, the DPKI-based IdM system, which assumes full decentralisation of trust, is deemed impractical for most organisational contexts. PKI with distributed key management emerges as a more viable alternative, offering a degree of trustlessness and decentralisation while mitigating the challenges associated with DPKI.

The FISP-ProCOP matrix, developed in Contribution 1, informs the design of the IdM system in Contribution 3 and 4. Specifically, the attributes related to actors and their relationships, security and privacy criteria, and used policies (including the ones defining the trust assumptions) directly influence the selection of appropriate identity management solutions. For instance, if the FISP-ProCOP analysis reveals a high level of sensitivity for certain data types, this would necessitate the consideration of more privacy-preserving IdM solutions, such as

DKMS-based. In contrast, if the availability of the IdM system is mentioned as a challenge within the OS. Strategy attribute in FISP-ProCOP matrix, then the DPKI-based IdM system should be preferred. The process models from Contribution 2 further inform the analysis of the IdM system by depicting the privacy-enhancing technologies which might rely on the IdM system implementation and trust assumptions.

Limitations. The main limitation of the studies is that the proposed IdM designs were developed originally for the X-Road data exchange system, and thus, the trust model assessment results are system-specific and may differ for smart systems based on the other data exchange system. Additionally, the results rely on the IdM quality assessment model which is not complete. The model covers the most commonly targeted quality criteria based on our background study. However, the provided indicators for these criteria are only exemplary, and not all of them might be relevant changes in the context of another scenario of information systems integration. Moreover, the assessment model assumes that all the mentioned quality sub-criteria are equally important for the IdM system quality. Meanwhile, the expert group might have criteria prioritised that would change the interpretation of the quality measurement results. Finally, as the method has not been evaluated against its usability, supporting guidelines on the method and assessment model usage might be needed.

5.7. Summary

In this chapter, we addressed $\mathbf{RQ}_3$: How does the trust model affect the security and privacy of an organisation participating in a cross-organisational smart solution? To answer this question, we developed a two alternative designs for smart solutions' IdM system – DPKI-based and DKMS-based. Both designs assume the usage of the X-Road data exchange system as an enabler of a smart system. The first design eliminated the assumption of centralised trust to an external single entity (i.e. CA) for organisational identity issuance and verification. Meanwhile, the second design enables organisations to follow zero trust architecture and eliminate centralised trust in internal organisational identity controller. The designs and illustration of their implementation support the expert group in assessing the current identity management system and trust model against the business objectives and trust assumptions as well as assessing the feasibility and effect of changing the trust assumptions on the security of organisational identity.

The developed IdM system designs are not scenario-specific, which proves their applicability across diverse X-Road-based smart systems. The analysis revealed that the optimal choice of trust and identity models for an IdM system depends on specific business objectives and desired system characteristics. Additionally, the studies resulted in proof of concept implementations of the identity management systems in X-Road, which are accessible for usage by the X-Road community.

In conclusion, in this chapter, we developed identity management system designs for X-Road-based smart systems that should help organisations define the rules under which a set of organisations exchange their data. The systems designs and the IdM system quality assessment model enable the making of informed decisions on trust model selection to protect organisational and personal data from unauthorised access.

6. CONCLUSION

This chapter concludes the thesis. Here, we outline the contributions and how they answer the stated research questions. After, we discuss the external validity of the research results, limitations and future work directions.

Considering that the smart systems are usually built based on existing standalone information systems with pre-setup security and privacy countermeasures, the organisation should ensure that the updated business process, data flows, and security measures meet the security and privacy requirements for the new smart solution system. For this, we assume that an organisation should assemble a temporal expert group to analyse the changes in the organisation based on the new collaboration relationships and integration of the systems. While the existing information security and privacy frameworks are mainly focused on high-level management activities for security assurance within the organisation without highlighting the effect of cross-organisational collaboration, in this thesis, we aimed to investigate the effect of such collaboration on the way information security and privacy is assured through technical and organisational measures. Thus, this thesis addressed the main research question: **How to support an expert group in assessing the effect of cross-organisational collaboration on information security and privacy of the smart solution?**

To answer the main research question, we used a design science research method, which resulted in a method for information security and privacy management in smart solutions. The method serves as a contribution to information system engineering and security and management knowledge base by helping data protection officers, information security officers, business analysts, and security architects coordinate their security and privacy assurance efforts. By addressing the challenges posed by the increasing interconnectedness of systems, this research empowers organisations to enhance their security posture, protect sensitive data, and ensure compliance with relevant regulations.

6.1. Answers to Research Questions

RQ_1: How to depict the state of security and privacy management in an organisation?

Through a background literature review of studies on security and privacy management challenges in smart systems, we identified that one of the major challenges is security and privacy assurance against privacy leakages and human factors. The additional literature review of information security and privacy frameworks and models that guide organisational security efforts showed that despite an extensive number of existing guidelines and standards, they are mainly focused on guiding security management either on the high level of abstraction or on the level of examples of security measures. To address this problem, we developed a

framework for information security and privacy management, i.e., FISP-ProCOP (Contribution 1).

This framework builds upon existing models, overcoming their limitations of providing only one of the two – (*i*) a comprehensive guide for risk management operations and visualising the interdependencies between operations and countermeasures or (*ii*) set of potential security and privacy-preserving measures. Unlike previous frameworks, FISP-ProCOP is presented in a matrix format, enabling its use as a theoretical model or template for depicting the static state of information security and privacy management within organisations. FISP-ProCOP highlights four crucial dimensions that influence information security and privacy management from a business perspective: Processes, Countermeasures, Organisation, and People. Each dimension comprises multiple categories, which are further subdivided into attributes. These attributes can have one or more instances, allowing for the adaptation of the model to specific smart system contexts within an organisation.

The framework's usability and adaptability were evaluated through two studies in the context of intelligent transportation systems (ITS). These studies demonstrated the framework's usability and adaptability to depicting measures based on written sources (including documentation and academic papers) and expert knowledge. Additionally, the studies showed how the framework could allow the expert group to evaluate the consistency of information security and privacy management aspects across FISP-ProCOP dimensions. As a result, the framework can help identify security and privacy requirements for the newly established smart solution that are not met by the existing countermeasures. Furthermore, the study identified significant privacy and security challenges in ITS, including data privacy assurance and the lack of adoption of standardised privacy management systems.

RQ_2: How can tools support privacy assurance for an organisation participating in a cross-organisational smart solution?

To answer this question, we developed a tool-supported privacy analysis method (Contribution 2) which relies on the research-based tools for (*i*) EU data protection regulation compliance verification and (*ii*) analysis of the efficiency of privacy-enhancing technologies to meet data privacy requirements. By identifying potential privacy violations, the method helps address these issues through minimal adjustments to processes and systems. The method assumes that the expert group has defined business process models for the smart solution based on collaborative data processing. The proposed method leverages open-source tools like DPO and Pleak to analyse privacy requirements and assess the effectiveness of privacy-enhancing technologies (PETs).

We evaluated the method's usability through two studies in intelligent transportation systems (autonomous vehicle-based ride-hailing system and smart parking solution), demonstrating its ability to identify potential privacy violations and recommend suitable PETs. Additionally, by integrating privacy analysis into business processes as prescribed by the method steps, the method helps organisations comply with GDPR requirements, especially Article 5(2), which requires having artefacts to demonstrate compliance.

RQ_3: How does the trust model affect the security and privacy of an organisation participating in a cross-organisational smart solution?

The answer to this question consists of two parts. First, we developed a DPKI-based identity management (IdM) system (Contribution 3) that allows the distribution of trust for organisational identity management in data exchange system-enables smart systems. Second, we developed a DKMS-based (IdM) system (Contribution 4), which allows the smart system providers to implement a zero-trust strategy and avoid centralisation of internal control over ODIs.

Additionally, we developed a quality assessment model which is based on Cameron's digital identity laws and the commonly targeted IdM system quality criteria – security, control, usability, and maintainability. Each criterion is divided into multiple sub-criteria, and the respective indicators for measurement are provided. The proposed IdM system designs, along with the quality assessment model and the proof of concept implementations, assist experts in evaluating existing identity management systems and trust models against organisational objectives and assumptions. It also helps assess the potential impact of altering trust assumptions on system security, control, usability, and maintainability. Thereby, Contributions 3 and 4 facilitate informed decision-making regarding trust model selection to safeguard organisational and personal data from unauthorised access.

Further, the results of studies highlighted that the optimal selection of trust and identity models for an identity management system relies on specific organisational goals and desired system characteristics. While pure PKI-based, DPKI-based, and PKI-based with distributed key management IdM systems each offer unique advantages and disadvantages, DPKI is deemed impractical for most organisational settings due to the need for complex infrastructure and governance model establishment. A more viable alternative to the fully centralised PKI-based IdM system is the centralised IdM with the distributed trust, which offers a degree of decentralisation and trust minimisation while mitigating the challenges inherent in DPKI. Furthermore, the studies resulted in two proof-of-concept implementations of identity management systems for X-Road, which are now accessible for usage by the X-Road community.

6.2. Discussion

6.2.1. External Validity

While the evaluation of thesis contributions primarily focused on the Intelligent Transportation System (ITS) domain, the findings and developed artefacts have broader applicability across smart solution domains, particularly in sectors with similar security and privacy management challenges to ITS, such as e-Government and e-Health. These three domains are similar in their reliance on personal data and the involvement of a high number of employees in the systems' operations and regular users, necessitating consistent information security and privacy management strategies to protect individuals and maintain public trust.

The FISP-ProCOP framework is grounded on domain-agnostic frameworks and models. The evaluation studies intentionally included the usage of the framework for multiple types of smart transportation systems (including traffic management, smart parking and ride-hailing) that differ by their architecture, participants, operations and processes. Therefore, the framework could be adapted to assess security and privacy postures in domains other than transportation, including e-Health and e-Government. As described in the background study, in e-Health there is a critical gap in existing research due to an overemphasis on technical controls and a neglect of organisational and managerial aspects. FISP-ProCOP, by explicitly considering these dimensions, can address this gap serving as a tool for improving security and privacy management within e-Health systems and their providers' organisations, particularly by guiding the implementation of organisational controls and fostering a strong security culture.

The tool-supported privacy analysis method relies on the formalised business process models that depict the personal data flow within a smart system between system providers. Therefore, the method is expected to be applicable in any domain (e.g., e-Health and e-Government) for the smart systems assuming that the system contributors agree on the collaborative processes. While the proposed method prescribes the usage of the selected analysis tools for improving the privacy analysis efficiency and usability of the method, their underlying methodologies might be used instead of the tools to avoid tool dependencies.

The proposed identity management system designs are generally applicable for any smart system (or any other not smart system) that relies on the X-Road data exchange system for cross-organisational data exchange. Therefore, Contributions 3 and 4 and their evaluation results are generally applicable for any running X-Road instances and thus can be used by the X-Road community[21]. Additionally, the generalised designs, the IdM system assessment model and the illustration of the IdM system development process should allow the expert group to instantiate the system designs also for non-X-Road-based smart systems.

[21]There are 24 X-Road instances deployed by governments or other organisations worldwide, which enables data exchange for 542 million end users [193]

The particular scientific contribution of this thesis lies in the developed method which guides on the usage of technical security measures and security analysis methods by technical and non-technical roles within organisations to ensure information security and privacy. This research is based on the definition of separate security and privacy objectives identified through the FISP-ProCOP framework. The final developed method offers a procedure for selecting security measures which would allow the achievement of security objectives along with scenario-oriented privacy objectives in the smart systems.

6.2.2. Limitations and Future Work

The research and contributions presented in this thesis have limitations which offer several directions for future research:

- The contributions have been evaluated in the studies with limited scope focusing on usability. In particular, the usability and effectiveness of the FISP-ProCOP framework and the tool-supported privacy analysis method should be further evaluated directly by the targeted expert groups in organisations contributing to the smart solutions. Close collaboration with an external authority, such as a government agency or a large enterprise, would be crucial for conducting a comprehensive usability study. Such a partnership would provide access to potential users within the organisation, facilitating a more realistic evaluation of the framework in a real-world context.
- The presented approach assumes the manual identification of the current state measures for information security and privacy management by filling in the FISP-ProCOP matrix. However, suppose the organisation wants to use the matrix not only for the project of establishing a smart solution but also throughout its lifetime. In that case, the matrix should be regularly updated and could be used as a reference for regular security management activities. Therefore, a tool for FISP-ProCOP should be developed. This would allow the expert group members to fill in the categories separately without using a matrix itself for the data collection. Later on, other organisation employees could access the matrix as a part of the documentation. Additionally, the tool could allow AI-enabled automatic data extraction of FISP-ProCOP components from the documentation, system components, and process logs, which would enable the organisation to decrease the amount of employee evolvement and cut costs.
- In our research, we assumed that organisations have (or can define) collaborative business processes for a smart solution. Thus, the privacy analysis method included only tools that rely on the business process models. To address this limitation, the method should be extended with new privacy analysis tools, which allow the usage of system logs in addition to the business process models to consider non-formalised data exchanges allowed in smart solution system components.

- The proposed identity management quality assessment model allows an organisation to assess the ability to meet the included system criteria. However, the assessment model usage results could be interpreted differently depending on the priorities of those criteria. Therefore, the decision tree for the identity management system selection should be created to support the decision-making based on the organisation's context, trust assumptions and accepted risks. For example, the decision tree could be prepared based on the weights given by the expert group to the IdM quality assessment criteria based on the organisation's priorities.
- Our research focused on organisational trust assumptions and the management of organisational digital identity. However, smart solutions often involve not only organisational information systems but also personal devices and IoT devices, which have varying levels of trust and require separate identity management. In future work, it is essential to investigate the intersection of multiple identity and trust models within a smart system to ensure that the various trust chains relied upon by organisational system components do not conflict with each other.
- Finally, the method for information security and privacy management in smart solutions composed of the described four contributions of the thesis has not been applied to a case study as a whole. Instead, the final developed method is combined with the theoretical description of the data objects' usage among the thesis contributions, and we evaluated the effectiveness and usability of four contributions through separate studies. Thereby, there is a threat to the external validity of the final composed method due to the possibility of its limited generalisation to a single case. Future work should apply the ultimate method for information security and privacy management in smart solutions to one smart solution case study to validate its usability and effectiveness as a whole.

BIBLIOGRAPHY

[1] Special Secretariat of Foresight (Hellenic Republic). *Megatrends 2040. Volatility, Uncertainty, Resourcefulness*. Available at https://foresight.gov.gr/en/studies/Megatrends-2040-Volatility-Uncertainty-Resourcefulness/ (visited on 29 October 2024). 2022.

[2] Strategic Futures Group of the National Intelligence Council (US). *Global Trends 2040: A More Contested World*. Available at https://www.dni.gov/index.php/gt2040-home (visited on 29 October 2024). 2021.

[3] Gartner. *Top Strategic Technology Trends 2023*. Available at https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2023 (visited on 29 October 2024). 2022.

[4] Claus Ballegaard Nielsen et al. "Systems of Systems Engineering: Basic Concepts, Model-Based Techniques, and Research Directions". In: *ACM Comput. Surv.* 48.2 (2015). ISSN: 0360-0300. DOI: 10.1145/2794381.

[5] Simon Elias Bibri and Zaheer Allam. "The Metaverse as a virtual form of data-driven smart cities: the ethics of the hyper-connectivity, datafication, algorithmization, and platformization of urban society". In: *Computational Urban Science* 2.1 (2022), p. 22. ISSN: 2730-6852. DOI: 10.1007/s43762-022-00050-1.

[6] Joint Task Force Transformation Initiative and others. *NIST Special Publication 800-39. Managing Information Security Risk: Organization, Mission, and Information System View*. 2011. DOI: 10.6028/NIST.SP.800-39.

[7] Nico Mexis et al. "A Lightweight Architecture for Hardware-Based Security in the Emerging Era of Systems of Systems". In: *J. Emerg. Technol. Comput. Syst.* 17.3 (2021). ISSN: 1550-4832. DOI: 10.1145/3458824.

[8] Miguel Angel Olivero et al. "Addressing Security Properties in Systems of Systems: Challenges and Ideas". In: *Software Engineering for Resilient Systems*. Ed. by Radu Calinescu and Felicita Di Giandomenico. Cham: Springer International Publishing, 2019, pp. 138–146. ISBN: 978-3-030-30856-8.

[9] Kewei Sha et al. "On security challenges and open issues in Internet of Things". In: *Future Generation Computer Systems* 83 (2018), pp. 326–337. ISSN: 0167-739X. DOI: 10.1016/j.future.2018.01.059.

[10] European Union Agency for Cybersecurity et al. *Good practices for supply chain cybersecurity*. European Union Agency for Cybersecurity, 2023. DOI: 10.2824/805268.

[11] Miguel Angel Olivero et al. "A systematic mapping study on security for systems of systems". In: *International Journal of Information Security* 23.2 (Apr. 2024), pp. 787–817.

[12] Yehuda Lindell and Ariel Nof. “Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody”. In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’18. Toronto, Canada: Association for Computing Machinery, 2018, pp. 1837–1854. ISBN: 9781450356930. DOI: 10.1145/3243734.3243788.

[13] Ran Canetti et al. “UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts”. In: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’20. Virtual Event, USA: Association for Computing Machinery, 2020, pp. 1769–1787. ISBN: 9781450370899. DOI: 10.1145/3372297.3423367.

[14] Megan Chen et al. “Multiparty Generation of an RSA Modulus”. In: *Journal of Cryptology* 35.2 (Mar. 2022), p. 12.

[15] Chenkai Weng et al. “Mystique: Efficient Conversions for Zero-Knowledge Proofs with Applications to Machine Learning”. In: *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Aug. 2021, pp. 501–518. ISBN: 978-1-939133-24-3. URL: https://www.usenix.org/conference/usenixsecurity21/presentation/weng.

[16] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plançon. “Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General”. In: *Advances in Cryptology – CRYPTO 2022*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Cham: Springer Nature Switzerland, 2022, pp. 71–101. ISBN: 978-3-031-15979-4.

[17] Thibauld Feneuil, Antoine Joux, and Matthieu Rivain. “Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs”. In: *Advances in Cryptology – CRYPTO 2022*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Cham: Springer Nature Switzerland, 2022, pp. 541–572. ISBN: 978-3-031-15979-4.

[18] Helger Lipmaa. “Polymath: Groth16 Is Not the Limit”. In: *Advances in Cryptology – CRYPTO 2024*. Ed. by Leonid Reyzin and Douglas Stebila. Cham: Springer Nature Switzerland, 2024, pp. 170–206. ISBN: 978-3-031-68403-6.

[19] Kundan Munjal and Rekha Bhatia. “A systematic review of homomorphic encryption and its contributions in healthcare industry”. In: *Complex & Intelligent Systems* 9.4 (Aug. 2023), pp. 3759–3786.

[20] Thi Van Thao Doan et al. “A survey on implementations of homomorphic encryption schemes”. In: *The Journal of Supercomputing* 79.13 (Sept. 2023), pp. 15098–15139.

[21] Martin Albrecht et al. “Homomorphic Encryption Standard”. In: *Protecting Privacy through Homomorphic Encryption*. Ed. by Kristin Lauter, Wei Dai, and Kim Laine. Cham: Springer International Publishing, 2021,

pp. 31–62. ISBN: 978-3-030-77287-1. DOI: 10.1007/978-3-030-77287-1_2.

[22] David Byrd and Antigoni Polychroniadou. “Differentially private secure multi-party computation for federated learning in financial applications”. In: *Proceedings of the First ACM International Conference on AI in Finance*. ICAIF ’20. New York, New York: Association for Computing Machinery, 2021. ISBN: 9781450375849. DOI: 10.1145/3383455.3422562.

[23] Dengguo Feng and Kang Yang. “Concretely efficient secure multi-party computation protocols: survey and more”. In: *Security and Safety* 1 (2022), p. 2021001.

[24] Sanjaikanth E Vadakkethil Somanathan Pillai and Kiran Polimetla. “Enhancing Network Privacy through Secure Multi-Party Computation in Cloud Environments”. In: *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)*. 2024, pp. 1–6. DOI: 10.1109/ICICACS60521.2024.10498662.

[25] European Union Agency for Cybersecurity. *ECSF, European cybersecurity skills framework*. European Union Agency for Cybersecurity, 2022. DOI: 10.2824/859537.

[26] **Mariia Bakhtina**, Raimundas Matulevičius, and Lukaš Malina. *Information Security and Privacy Management in Intelligent Transportation Systems*. 2024. DOI: 10.7250/csimq.2024-38.04.

[27] International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 27001: 2022, Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements*. 2022.

[28] Rolf von Roessing. “The ISACA business model for information security: An integrative and innovative approach”. In: *ISSE 2009 securing electronic business processes*. Springer, 2010, pp. 37–47.

[29] John McCumber. *Assessing and managing security risk in IT systems: A structured methodology*. Auerbach Publications, 2004.

[30] Yulia Cherdantseva and Jeremy Hilton. “A Reference Model of Information Assurance & Security”. In: *2013 International Conference on Availability, Reliability and Security, ARES 2013*. IEEE Computer Society, 2013, pp. 546–555. DOI: 10.1109/ARES.2013.72.

[31] NIST. *Cybersecurity Framework*. Available at https://www.nist.gov/cyberframework (visited on 29 October 2024). 2018.

[32] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). *ISO/IEC 27032: 2023, Cybersecurity — Guidelines for Internet security*. 2023.

[33] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). *ISO/IEC 27000: 2018, Information tech-*

nology — Security techniques — Information security management systems — Overview and vocabulary. 2018.

[34] William Tibben Riza Azmi and Khin Than Win. "Review of cybersecurity frameworks: context and shared concepts". In: *Journal of Cyber Policy* 3.2 (2018), pp. 258–283. DOI: 10.1080/23738871.2018.1520271.

[35] Critical Infrastructure Cybersecurity. "Framework for improving critical infrastructure cybersecurity". In: *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP* 4162018 (2018), p. 7.

[36] Oleksandr Kosenkov et al. "Systematic mapping study on requirements engineering for regulatory compliance of software systems". In: *Information and Software Technology* 178 (2025), p. 107622. ISSN: 0950-5849. DOI: 10.1016/j.infsof.2024.107622.

[37] ISACA. *Privacy in Practice 2021: Data Privacy Trends, Forecasts and Challenges*. white paper. Schaumburg, IL, USA, 2021.

[38] Ze Shi Li et al. "Towards privacy compliance: A design science study in a small organization". In: *Information and Software Technology* 146 (2022), p. 106868. ISSN: 0950-5849. DOI: 10.1016/j.infsof.2022.106868.

[39] Lukas Waidelich and Thomas Schuster. "Privacy Pattern Catalog Approach for GDPR Compliant Appliance: From Legal Requirements to Technology Design". In: *Digital Transformation*. Ed. by Jacek Maślankowski, Bartosz Marcinkowski, and Paulo Rupino da Cunha. Cham: Springer Nature Switzerland, 2023, pp. 88–102. ISBN: 978-3-031-43590-4.

[40] Müge Fazlioglu. *IAPP-EY Annual Privacy Governance Report 2021*. white paper. IAPP, 2021.

[41] *GDPR Enforcement Tracker*. available at https://enforcementtracker.com/. (Accessed: 17 December 2024). CMS.

[42] Damiano Torre et al. "Model Driven Engineering for Data Protection and Privacy: Application and Experience with GDPR". In: *CoRR* abs/2007.12046 (2020).

[43] Priscila Engiel, Julio Cesar Sampaio do Prado Leite, and John Mylopoulos. "A tool-supported compliance process for software systems". In: *RCIS*. IEEE, 2017, pp. 66–76.

[44] Sepideh Ghanavati. "Legal-URN framework for legal compliance of business processes". PhD thesis. University of Ottawa (Canada), 2013.

[45] M. Emilia Cambronero et al. "GDPRValidator: a tool to enable companies using cloud services to be GDPR compliant". en. In: *PeerJ Computer Science* 8 (Dec. 2022). Publisher: PeerJ Inc., e1171. ISSN: 2376-5992. DOI: 10.7717/peerj-cs.1171. (Visited on 02/28/2023).

[46] Maria N. Koukovini et al. "Towards Inherent Privacy Awareness in Workflows". In: *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*. Ed. by Joaquin Garcia-Alfaro et al. Cham:

Springer International Publishing, 2015, pp. 95–113. ISBN: 978-3-319-17016-9.

[47] Georgios Lioudakis et al. “GDPR Compliance Made Easier: The BPR4GDPR Project”. en. In: *ARIS2 - Advanced Research on Information Systems Security* 1.1 (Dec. 2021). Number: 1, pp. 5–23. ISSN: 2795-4560. DOI: 10.56394/aris2.v1i1.1. (Visited on 02/28/2023).

[48] European Union Agency for Cybersecurity. *ENISA’s PETs Maturity Assessment Repository*. Available at https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository (visited on 29 October 2024). 2018.

[49] Pedro Garcia Lopez, Alberto Montresor, and Anwitaman Datta. “Please, do not Decentralize the Internet with (Permissionless) Blockchains!” In: *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*. 2019, pp. 1901–1911. DOI: 10.1109/ICDCS.2019.00188.

[50] Javad Zarrin et al. “Blockchain for decentralization of internet: prospects, trends, and challenges”. In: *Cluster Computing* 24.4 (Dec. 2021), pp. 2841–2866.

[51] Shantanu Pal et al. “A blockchain-based trust management framework with verifiable interactions”. In: *Computer Networks* 200 (2021), p. 108506. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2021.108506.

[52] Alex Preukschat and Drummond Reed. *Self-sovereign identity*. Shelter Island, NY: Manning Publications, 2021.

[53] Alan R. Hevner et al. “Design Science in Information Systems Research”. In: *MIS Q.* 28.1 (2004), pp. 75–105.

[54] Ken Peffers et al. “A Design Science Research Methodology for Information Systems Research”. In: *J. Manag. Inf. Syst.* 24.3 (2008), pp. 45–77.

[55] Peta Darke, Graeme Shanks, and Marianne Broadbent. “Successfully completing case study research: combining rigour, relevance and pragmatism”. In: *Information systems journal* 8.4 (1998), pp. 273–289.

[56] Brian Henderson-Sellers et al. *Situational Method Engineering*. Springer, 2014. ISBN: 978-3-642-41466-4. DOI: 10.1007/978-3-642-41467-1.

[57] Göran Goldkuhl, Mikael Lind, and Ulf Seigerroth. “Method integration: the need for a learning perspective”. In: *IEE Proceedings-Software* 145.4 (1998), pp. 113–118.

[58] Scott Rose et al. *NIST SP 800-207. Zero Trust Architecture*. 2020.

[59] **Mariia Bakhtina**, Raimundas Matulevičius, and Mari Seeba. “Tool-supported method for privacy analysis of a business process model”. In: *Journal of Information Security and Applications* 76 (2023), p. 103525. DOI: 10.1016/j.jisa.2023.103525.

[60] **Mariia Bakhtina** et al. “On the Shift to Decentralised Identity Management in Distributed Data Exchange Systems”. In: *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*. SAC ’23. Tallinn, Estonia: Association for Computing Machinery, 2023, pp. 864–873. DOI: 10.1145/3555776.3577678.

[61] **Mariia Bakhtina** et al. “A Decentralised Public Key Infrastructure for X-Road”. In: *Proceedings of the 18th International Conference on Availability, Reliability and Security*. ARES ’23. Benevento, Italy: Association for Computing Machinery, 2023. DOI: 10.1145/3600160.3605092.

[62] **Mariia Bakhtina** et al. “The Power of Many: Securing Organisational Identity Through Distributed Key Management”. In: *Advanced Information Systems Engineering*. Ed. by Giancarlo Guizzardi et al. Cham: Springer Nature Switzerland, 2024, pp. 475–491. ISBN: 978-3-031-61057-8. DOI: 10.1007/978-3-031-61057-8_28.

[63] Chengfei Liu, Qing Li, and Xiaohui Zhao. “Challenges and opportunities in collaborative business process management: Overview of recent advances and introduction to the special issue”. In: *Information Systems Frontiers* 11.3 (2009), pp. 201–209.

[64] Yulia Cherdantseva. “Secure* BPMN-a graphical extension for BPMN 2.0 based on a reference model of information assurance & security”. PhD thesis. Cardiff University, 2014.

[65] Council of the European Union. *Council adopts new framework to boost the roll-out of intelligent transport systems*. Available: https://www.consilium.europa.eu/en/press/press-releases/2023/10/23/council-adopts-new-framework-to-boost-the-roll-out-of-intelligent-transport-systems/. 2023.

[66] European Commission. *Directive (EU) 2023/2661 of the European Parliament and of the Council of 22 November 2023 amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport*. Available: https://eur-lex.europa.eu/eli/dir/2023/2661/oj. 2023.

[67] Ricard Borges and Francesc Sebé. “Parking Tickets for Privacy-Preserving Pay-by-Phone Parking”. In: *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society*. WPES’19. London, United Kingdom: ACM, 2019, pp. 130–134. ISBN: 9781450368308. DOI: 10.1145/3338498.3358638.

[68] Liehuang Zhu et al. “ASAP: An Anonymous Smart-Parking and Payment Scheme in Vehicular Networks”. In: *IEEE Transactions on Dependable and Secure Computing* 17.4 (2020), pp. 703–715. ISSN: 1545-5971. DOI: 10.1109/TDSC.2018.2850780.

[69] Mario Weber and Ivana Podnar Žarko. “A Regulatory View on Smart City Services”. In: *Sensors* 19.2 (2019). ISSN: 1424-8220. DOI: 10.3390/s19020415.

[70] Ramin Ranjbar Motlagh, Omid Ameri Sianaki, and Himanshu Shee. “A Survey on Cooperative Intelligent Transportation Systems (C-ITS): Opportunities and Challenges”. In: *Complex, Intelligent and Software Intensive Systems*. Ed. by Leonard Barolli. Cham: Springer Nature Switzerland, 2024, pp. 253–260.

[71] Achref Haddaji, Samiha Ayed, and Lamia Chaari Fourati. “IoV security and privacy survey: Issues, countermeasures, and challenges”. In: *The Journal of Supercomputing* 80.15 (2024), pp. 23018–23082.

[72] Misbah Kousar, Sanjay Kumar, and Mohammed Abdul Bari. “Design of a Decentralized Authentication and Off-Chain Data Management Protocol for VANETs Using Blockchain”. In: *Communications on Applied Nonlinear Analysis* 32.2 (2025), pp. 718–731. DOI: 10.52783/cana.v32.1917.

[73] Ryan Shivers et al. “Ride-Hailing for Autonomous Vehicles: Hyperledger Fabric-Based Secure and Decentralize Blockchain Platform”. In: *2021 IEEE International Conference on Big Data (Big Data)*. IEEE, 2021, pp. 5450–5459. DOI: 10.1109/BigData52589.2021.9671379.

[74] Wesam Al Amiri et al. “Privacy-Preserving Smart Parking System Using Blockchain and Private Information Retrieval”. In: *2019 International Conference on Smart Applications, Communications and Networking (SmartNets)*. 2019, pp. 1–6. DOI: 10.1109/SmartNets48225.2019.9069783.

[75] Zengpeng Li et al. “PriParkRec: Privacy-Preserving Decentralized Parking Recommendation Service”. In: *IEEE Transactions on Vehicular Technology* 70.5 (2021), pp. 4037–4050. DOI: 10.1109/TVT.2021.3074820.

[76] Yunyi Fang et al. “Blockchain-Based Privacy-Preserving Valet Parking for Self-Driving Vehicles”. In: *Transactions on Emerging Telecommunications Technologies* 32.4 (2021), e4239. ISSN: 2161-3915. DOI: 10.1002/ett.4239.

[77] Debashis Das, Sourav Banerjee, and Utpal Biswas. “Design of a Secure Blockchain-Based Toll-Tax Collection System”. In: *Micro-Electronics and Telecommunication Engineering. ICMETE 2021*. Vol. 373. Springer, 2022, pp. 183–191. DOI: 10.1007/978-981-16-8721-1_18.

[78] Xinyang Deng and Tianhan Gao. “Electronic Payment Schemes Based on Blockchain in VANETs”. In: *IEEE Access* 8 (2020), pp. 38296–38303. DOI: 10.1109/ACCESS.2020.2974964.

[79] Rabia Ihmouda, Najwa Hayaati Mohd Alwi, and Ismail Abdullah. “A systematic review on e-government security aspects”. In: *International Journal of Enhanced Research in Management and Computer Applications* 3.6 (2014), pp. 60–7.

[80] Nik Thompson, Antony Mullins, and Thanavit Chongsutakawewong. “Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand”. In: *Government Information Quarterly* 37.1 (2020), p. 101408. ISSN: 0740-624X. DOI: 10.1016/j.giq.2019.101408.

[81] Ebot Ebot Enaw and Njei Check. “Information Systems Security Audits in Cameroon’s Public Administration”. In: *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*. ICEGOV ’18. Galway, Ireland: Association for Computing Machinery, 2018, pp. 312–317. ISBN: 9781450354219. DOI: 10.1145/3209415.3209425.

[82] Rio Guntur Utomo, Gary Wills, and Robert Walters. “A Framework for Factors Influencing the Implementation of Information Assurance for e-Government in Indonesia”. In: *International Journal on Advanced Science, Engineering and Information Technology* 10.3 (2020), pp. 1025–1034. ISSN: 2088-5334. DOI: 10.18517/ijaseit.10.3.9186.

[83] Raymond Lutui, Semisi Hopoi, and Siaosi Maeakafa. “Security readiness evaluation framework for Tonga E-government initiatives”. In: 2017, pp. 14–24. DOI: 10.4225/75/5a84f2bd95b4a.

[84] Avinash Ramtohul and K M S Soyjaudah. “Information security governance for e-services in southern African developing countries e-Government projects”. In: *Journal of Science & Technology Policy Management* 7.1 (2016), pp. 26–42.

[85] Noe Elisa et al. “A framework of blockchain-based secure and privacy-preserving E-government system”. In: *Wireless Networks* 29.3 (2023), pp. 1005–1015.

[86] Sasan Adibi. *Mobile health: a technology road map*. Vol. 5. Springer, 2015.

[87] Leonardo Horn Iwaya, Aakash Ahmad, and M. Ali Babar. “Security and Privacy for mHealth and uHealth Systems: A Systematic Mapping Study”. In: *IEEE Access* 8 (2020), pp. 150081–150112. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3015962.

[88] Aqsa Fatima and Ricardo Colomo-Palacios. “Security aspects in healthcare information systems: A systematic mapping”. In: *Procedia Computer Science* 138 (2018), pp. 12–19. ISSN: 18770509. DOI: 10.1016/j.procs.2018.10.003.

[89] Prosper Kandabongee Yeng et al. “Mapping the psychosocialcultural aspects of healthcare professionals’ information security practices: Systematic mapping study”. In: *JMIR Human Factors* 8 (2 2021). DOI: 10.2196/17604.

[90] Ying He et al. “Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review”. In: *Journal of Medical Internet Research* 23 (4 2021). DOI: 10.2196/21747.

[91] Tafheem Ahmad Wani, Antonette Mendoza, and Kathleen Gray. "Hospital Bring-your-own-device security challenges and solutions: Systematic review of gray literature". In: *JMIR mHealth and uHealth* 8 (6 2020), e18175. DOI: 10.2196/18175.

[92] Bakheet Aljedaani and Ali Babar. "Challenges with developing secure mobile health applications: Systematic review". In: *JMIR mHealth and uHealth* 9 (6 2021). DOI: 10.2196/15654.

[93] Leonardo Horn Iwaya et al. "Mobile health systems for community-based primary care: identifying controls and mitigating privacy threats". In: *JMIR mHealth and uHealth* 7 (3 2019). DOI: 10.2196/11642.

[94] Alberto Sardi et al. "Cyber risk in health facilities: A systematic literature review". In: *Sustainability (Switzerland)* 12 (17 2020). DOI: 10.3390/su12177002.

[95] Jaime Benjumea et al. "Privacy Assessment in Mobile Health Apps: Scoping Review". In: *JMIR mHealth and uHealth* 8 (7 2020). DOI: 10.2196/18868.

[96] Farida Habib Semantha et al. "A systematic literature review on privacy by design in the healthcare sector". In: *Electronics* 9 (3 2020). DOI: 10.3390/electronics9030452.

[97] Ekran System. *7 Examples of Real-Life Data Breaches Caused by Insider Threats*. Available at https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches (visited on 29 October 2024). 2024.

[98] Information System Authority (RIA). *Cyber Security in Estonia 2024*. Available at https://www.ria.ee/sites/default/files/documents/2024-02/Cyber-security-in-Estonia-2024.pdf (visited on 29 October 2024). 2024.

[99] Information System Authority (RIA). *Cyber Security in Estonia 2023*. Available at https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf (visited on 29 October 2024). 2023.

[100] HITRUST Services Corp. *HITRUST Framework*. Available at https://hitrustalliance.net/hitrust-framework (visited on 29 October 2024).

[101] Afnan A. Alrehili and Omar H. Alhazmi. "ISO/IEC 27001 Standard: Analytical and Comparative Overview". In: *Lecture Notes in Networks and Systems* 891 (2024), pp. 143–156. DOI: 10.1007/978-981-99-9524-0_12.

[102] ISO. *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*. Standard ISO/IEC 27701:2019. Switzerland: International Organization for Standardization, 2019.

[103] NIST. *NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations*. 2018. DOI: 10.6028/NIST.SP.800-37r2.

[104] NIST. *NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations*. 2020. DOI: doi.org/10.6028/NIST.SP.800-53r5.

[105] Malina Adach, Kaj Hänninen, and Kristina Lundqvist. "Security Ontologies: A Systematic Literature Review". In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 13585 LNCS (2022), pp. 36–53. DOI: 10.1007/978-3-031-17604-3_3.

[106] European Parliament, Council of the European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Available at http://data.europa.eu/eli/reg/2016/679/2016-05-04 (visited on 29 October 2024). 2016.

[107] European Parliament, Council of the European Union. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. Available at http://data.europa.eu/eli/reg/2019/881/oj (visited on 29 October 2024). 2019.

[108] European Parliament, Council of the European Union. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. Available at http://data.europa.eu/eli/dir/2022/2555/oj (visited on 29 October 2024). 2022.

[109] European Parliament, Council of the European Union. *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*. Available at http://data.europa.eu/eli/reg/2024/2847/oj (visited on 18 February 2025). 2024.

[110] Estonian Information System Authority (RIA). *Eesti Infoturbestandard*. available at https://eits.ria.ee/. last accessed: 9 October 2024. 2023.

[111] Federal Office for Information Security (BSI). *BSI Standard 200-3: Risk Analysisbased on IT-Grundschutz*. Available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html (visited on 29 October 2024). 2017.

[112] Parliament of the Czech Republic. *Předpis 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. Available at https://www.psp.cz/sqw/sbirka.sqw?cz=181&r=2014 (visited on 29 October 2024). 2014.

[113] Jaap-Henk Hoepman. "Privacy design strategies". In: *IFIP Advances in Information and Communication Technology* 428 (2014), pp. 446–459. DOI: 10.1007/978-3-642-55415-5_38.

[114] Daniel Le Métayer et al. *Privacy and Data Protection by Design - from policy to engineering*. Tech. rep. European Union Agency for Network and Information Security (ENISA), 2015. DOI: 10.2824/38623.

[115] Pille Pullonen et al. "Privacy-enhanced BPMN: enabling data privacy analysis in business processes models". In: *Software and Systems Modeling* 18.6 (2019), pp. 3235–3264. ISSN: 1619-1374. DOI: 10.1007/s10270-019-00718-z.

[116] Pille Pullonen, Raimundas Matulevičius, and Dan Bogdanov. "PE-BPMN: Privacy-Enhanced Business Process Model and Notation". In: *Business Process Management*. Ed. by Josep Carmona, Gregor Engels, and Akhil Kumar. Cham: Springer International Publishing, 2017, pp. 40–56. ISBN: 978-3-319-65000-5. DOI: 10.1007/978-3-319-65000-5_3.

[117] Alfred J. Menezes, Scott A. Vanstone, and Paul C. van Oorschot. *Handbook of Applied Cryptography*. 1st. USA: CRC Press, Inc., 1996. ISBN: 0849385237.

[118] C. Gentry. "Fully Homomorphic Encryption Using Ideal Lattices". In: *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*. STOC '09. Bethesda, MD, USA: Association for Computing Machinery, 2009, pp. 169–178. ISBN: 9781605585062. DOI: 10.1145/1536414.1536440.

[119] Paul Ryan, Martin Crane, and Rob Brennan. "GDPR Compliance Tools: Best Practice from RegTech". In: *Enterprise Information Systems*. Ed. by Joaquim Filipe et al. Cham: Springer International Publishing, 2021, pp. 905–929. ISBN: 978-3-030-75418-1.

[120] European Union Agency for Cybersecurity. *Guidelines for SMEs on the security of personal data processing*. European Network and Information Security Agency, 2016. DOI: 10.2824/867415.

[121] Kaspar Kala. "Refinement of the general data protection regulation (GDPR) model: administrative fines perspective". MA thesis. University of Tartu, 2019.

[122] Orlando Amaral et al. “AI-Enabled Automation for Completeness Checking of Privacy Policies”. In: *IEEE Transactions on Software Engineering* 48.11 (2022), pp. 4647–4674. DOI: 10.1109/TSE.2021.3124332.

[123] Raimundas Matulevicius et al. “A Method for Managing GDPR Compliance in Business Processes”. In: *CAiSE Forum*. Vol. 386. Lecture Notes in Business Information Processing. Springer, 2020, pp. 100–112. DOI: 10.1007/978-3-030-58135-0_9.

[124] Eduard Sing. “A Meta-model Driven Method for Establishing Business Process Compliance to GDPR”. MA thesis. University of Tartu, 2018.

[125] Gianluca Roascio et al. “HArMoNICS: High-Assurance Microgrid Network Infrastructure Case Study”. In: *IEEE Access* 10 (2022), pp. 115372–115383. DOI: 10.1109/ACCESS.2022.3218412.

[126] *SPARTA project. Deliverable D6.3: First release of demonstration*. Available at https://www.sparta.eu/deliverables/ (visited on 29 October 2024). 2021.

[127] Aivo Toots et al. “Business Process Privacy Analysis in Pleak”. In: *Fundamental Approaches to Software Engineering*. Ed. by R. Hähnle and W. van der Aalst. Cham: Springer International Publishing, 2019, pp. 306–312. ISBN: 978-3-030-16722-6. DOI: 10.1007/978-3-030-16722-6_18.

[128] Olav Bunte et al. “The mCRL2 Toolset for Analysing Concurrent Systems”. In: *Tools and Algorithms for the Construction and Analysis of Systems*. Ed. by Tomáš Vojnar and Lijun Zhang. Cham: Springer International Publishing, 2019, pp. 21–39. ISBN: 978-3-030-17465-1.

[129] Marlon Dumas et al. “Multi-level privacy analysis of business processes: the PLEAK toolset”. In: *International Journal on Software Tools for Technology Transfer* 24.2 (2021), pp. 183–203. DOI: 10.1007/s10009-021-00636-w.

[130] Matthew Lepinski et al. “Privacy-Enhanced Android for Smart Cities Applications”. In: *Smart City 360°*. Ed. by Alberto Leon-Garcia et al. Cham: Springer International Publishing, 2016, pp. 66–77. ISBN: 978-3-319-33681-7.

[131] Mariia Bakhtina et al. *Rebooting Trust Management in X-Road*. Public Report. Available at https://www.niis.org/niis-publications/2022/12/14/rebooting-trust-management-in-x-road (visited on 29 October 2024). Nordic Institute for Interoperability Solutions (NIIS), 2022.

[132] Mariia Bakhtina et al. *Review of Key Management Mechanisms*. 2024. DOI: 10.5281/zenodo.10886209.

[133] Ron Ross, Mark Winstead, and Michael McEvilley. *NIST SP 800-160. Engineering Trustworthy Secure Systems*. National Institute of Standards & Technology, 2022.

[134] Jingwei Huang, Mamadou D. Seck, and Adrian Gheorghe. “Towards trustworthy smart cyber-physical-social systems in the era of Internet of Things”. In: *SoSE*. IEEE, 2016, pp. 1–6. DOI: 10.1109/SYSOSE.2016.7542961.

[135] David Temoshok et al. *NIST SP 800-63-4. Digital Identity Guidelines (Public Draft of Revision 4)*. National Institute of Standards & Technology, 2024.

[136] Kim Cameron. “The laws of identity”. In: *Microsoft Corp* 12 (2005), pp. 8–11.

[137] Loganathan Parthipan et al. “DRoT: A Decentralised Root of Trust for Trusted Networks”. In: *Information and Communications Security*. Ed. by Ding Wang et al. Singapore: Springer Nature Singapore, 2023, pp. 683–701. ISBN: 978-981-99-7356-9.

[138] World Wide Web Consortium (W3C). *Verifiable Credentials Data Model v1.1*. Available at https://www.w3.org/TR/vc-data-model (visited on 29 October 2024). 2022.

[139] IBM. *What is the OSI model?* Available at https://www.ibm.com/think/topics/osi-model (visited on 29 October 2024). 2024.

[140] Phillip J Windley. *Learning Digital Identity: Design, Deploy, and Manage Identity Architectures*. O’Reilly Media, Incorporated, 2023.

[141] Adam J. Slagell and Rafael Bonilla. “PKI Scalability Issues”. In: *CoRR* cs.CR/0409018 (2004), pp. 1–23.

[142] Sharon Boeyen et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 5280. 2008. DOI: 10.17487/RFC5280.

[143] Vivek Nair and Dawn Song. “Decentralizing Custodial Wallets with MFKDF”. In: *IEEE ICBC 2023*. 2023, pp. 1–9. DOI: 10.1109/ICBC56567.2023.10174998.

[144] Poulami Das et al. “The Exact Security of BIP32 Wallets”. In: *CCS 2021*. Virtual Event, Republic of Korea: ACM, 2021, pp. 1020–1042. ISBN: 9781450384544.

[145] Carolyn Guthoff et al. “Perceptions of Distributed Ledger Technology Key Management – An Interview Study with Finance Professionals”. In: *IEEE SP 2023*. 2023, pp. 588–605.

[146] Reza Soltani, Uyen Trang Nguyen, and Aijun An. “Decentralized and Privacy-Preserving Key Management Model”. In: *ISNCC 2020*. 2020, pp. 1–7.

[147] Syh-Yuan Tan and Swee-Huay Heng. “New Identity-Based Identification and Signature Schemes in the Standard Model”. In: *ARES 2023*. Benevento, Italy: ACM, 2023. DOI: 10.1145/3600160.3604999.

[148] Don Johnson, Alfred Menezes, and Scott A. Vanstone. “The Elliptic Curve Digital Signature Algorithm (ECDSA)”. In: *Int. J. Inf. Sec.* 1.1 (2001), pp. 36–63.

[149] Chun-I Fan et al. “Secure Hierarchical Bitcoin Wallet Scheme against Privilege Escalation Attacks”. In: *Int. J. Inf. Secur.* 19.3 (2020), pp. 245–255. ISSN: 1615-5262. DOI: 10.1007/s10207-019-00476-5.

[150] Elaine Barker. *NIST SP 800-57. Recommendation for Key Management*. 2016.

[151] Vivek Nair and Dawn Song. “Multi-Factor Key Derivation Function (MFKDF) for Fast, Flexible, Secure, & Practical Key Management”. en. In: (2023).

[152] Chelsea Komlo and Ian Goldberg. “FROST: Flexible Round-Optimized Schnorr Threshold Signatures”. In: *Selected Areas in Cryptography*. Cham: Springer, 2021, pp. 34–65. ISBN: 978-3-030-81652-0.

[153] Pieter Wuille. *BIP 0032. Hierarchical Deterministic Wallets*. Available at https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki (visited on 29 October 2024).

[154] Nabil Alkeilani Alkadri et al. “Deterministic Wallets in a Quantum World”. In: *CCS 2020*. Virtual Event, USA: ACM, 2020, pp. 1017–1031. ISBN: 9781450370899. DOI: 10.1145/3372297.3423361.

[155] Victor Shoup. “Practical Threshold Signatures”. In: *Advances in Cryptology – EUROCRYPT 2000*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 207–220. ISBN: 978-3-540-45539-4.

[156] Vid Kersic et al. “Orchestrating Digital Wallets for On- and Off-Chain Decentralized Identity Management”. In: *IEEE Access* 11 (2023), pp. 78135–78151. DOI: 10.1109/ACCESS.2023.3299047.

[157] Mariia Bakhtina, Raimundas Matulevicius, and Lukas Malina. *Report on Empirical Study of Information Security and Privacy Management in Intelligent Transportation Systems*. 2024. DOI: 10.5281/zenodo.10960046.

[158] Barbara Kitchenham and Stuart Charters. *Guidelines for performing Systematic Literature Reviews in Software Engineering*. Tech. rep. EBSE-2007-01. 2007.

[159] Ricard Borges and Francesc Sebé. “An Efficient Privacy-Preserving Pay-by-Phone System for Regulated Parking Areas”. en. In: *International Journal of Information Security* 20.5 (Oct. 2021), pp. 715–727. ISSN: 1615-5270. DOI: 10.1007/s10207-020-00527-2.

[160] Muhammad Khalid et al. “From Smart Parking Towards Autonomous Valet Parking: A Survey, Challenges and Future Works”. In: *Journal of Network and Computer Applications* 175 (2021), p. 102935. ISSN: 1084-8045. DOI: 10.1016/j.jnca.2020.102935.

[161] Ricard Garra, Santi Martínez, and Francesc Sebé. “A Privacy-Preserving Pay-by-Phone Parking System”. In: *IEEE Transactions on Vehicular Technology* 66.7 (2017), pp. 5697–5706. ISSN: 1939-9359. DOI: 10.1109/TVT.2016.2634785.

[162] Petr Dzurenda et al. “Privacy-Preserving Online Parking Based on Smart Contracts”. In: *Proceedings of the 16th International Conference on Availability, Reliability and Security*. ARES ’21. Vienna, Austria: ACM, 2021. ISBN: 9781450390514. DOI: 10.1145/3465481.3470058.

[163] Ioannis Chatzigiannakis, Andrea Vitaletti, and Apostolos Pyrgelis. “A Privacy-Preserving Smart Parking System Using an IoT Elliptic Curve Based Security Platform”. In: *Computer Communications* 89-90 (2016), pp. 165–177. ISSN: 0140-3664. DOI: 10.1016/j.comcom.2016.03.014.

[164] Fadi Al-Turjman, Hadi Zahmatkesh, and Ramiz Shahroze. “An Overview of Security and Privacy in Smart Cities’ IoT Communications”. In: *Transactions on Emerging Telecommunications Technologies* 33.3 (2022), e3677. ISSN: 2161-3915. DOI: 10.1002/ett.3677.

[165] Petr Dzurenda et al. “Privacy-Preserving Solution for Vehicle Parking Services Complying with EU Legislation”. In: *PeerJ Computer Science* 8 (2022), e1165. DOI: 10.7717/PEERJ-CS.1165.

[166] Sara Ramezanian et al. “Lightweight Privacy-Preserving Ride-Sharing Protocols for Autonomous Cars”. In: *Proceedings of the 6th ACM Computer Science in Cars Symposium*. CSCS ’22. ACM, 2022, 11:1–11:11. ISBN: 9781450397865. DOI: 10.1145/3568160.3570234.

[167] Wendong Chen et al. “A Review of Research on Privacy Protection of Internet of Vehicles Based on Blockchain”. In: *Journal of Sensor and Actuator Networks* 11.4 (2022). ISSN: 2224-2708. DOI: 10.3390/jsan11040086.

[168] Zhendong Wang et al. “Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey”. In: *Sustainability* 14.19 (2022). ISSN: 20711050. DOI: 10.3390/su141912409.

[169] N Sathyanarayana. “A Survey on Vehicle Detection and Classification for Electronic Toll Collection Applications”. In: *Distributed Computing and Optimization Techniques: Select Proceedings of ICDCOT 2021*. Springer Nature Singapore, 2022, pp. 101–110. ISBN: 978-981-19-2281-7. DOI: 10.1007/978-981-19-2281-7_10.

[170] Ricard Borges, Francesc Sebé, and Magda Valls. “An Anonymous and Unlinkable Electronic Toll Collection System”. In: *International Journal of Information Security* 21.5 (2022), pp. 1151–1162. DOI: 10.1007/s10207-022-00604-8.

[171] Supriya Sutar et al. “Security Based Electronic Toll Collection Using NFC and Android Application”. In: *International Journal of Scientific and Research Publications* 5 (4 2015).

[172] Mariia Bakhtina, Raimundas Matulevicius, and Lukas Malina. *Supplementary Material for Empirical Study of Information Security and Privacy Management in Intelligent Transportation Systems in Estonia and South Moravia*. Apr. 2024. DOI: 10.5281/zenodo.10960351.

[173] Edward Curry. "Real-time Linked Dataspaces: A Data Platform for Intelligent Systems Within Internet of Things-Based Smart Environments". In: *Real-time Linked Dataspaces: Enabling Data Ecosystems for Intelligent Systems*. Cham: Springer International Publishing, 2020, pp. 3–14. ISBN: 978-3-030-29665-0. DOI: 10.1007/978-3-030-29665-0_1.

[174] Aintzane Mosteiro-Sanchez et al. "End to End secure data exchange in value chains with dynamic policy updates". In: *Future Generation Computer Systems* 158 (2024), pp. 333–345. ISSN: 0167-739X. DOI: 10.1016/j.future.2024.04.053.

[175] *Preparatory work in view of the procurement of an open source cloud-to-edge middleware platform*. Tech. rep. European Commission, 2022.

[176] Mariia Bakhtina. *FISP-ProCOP: User Guide*. 2025. DOI: 10.5281/zenodo.14923440.

[177] International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 27002: 2022, Information security, cybersecurity and privacy protection — Information security controls*. 2022.

[178] Steven Alter. "Six work system lenses for describing, analyzing, or evaluating important aspects of is security". In: *International Journal of Systems and Society (IJSS)* 4.2 (2017), pp. 69–82.

[179] Moufida Sadok, Steven Alter, and Peter Bednar. "It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs". In: *Information & Computer Security* 28.3 (Jan. 2020), pp. 467–483.

[180] Bruce Silver and Bruce Richard. *BPMN method and style*. Vol. 2. Cody-Cassidy Press Aptos, 2009.

[181] Raimundas Matulevičius et al. "A Method for Managing GDPR Compliance in Business Processes". In: *Advanced Information Systems Engineering*. Ed. by Nicolas Herbaut and Marcello La Rosa. Cham: Springer International Publishing, 2020, pp. 100–112. ISBN: 978-3-030-58135-0. DOI: 10.1007/978-3-030-58135-0_9.

[182] Anastasiya V. Soldatova et al. "Customer Loyalty Management in the Context of Digital Transformation of Business". In: *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*. 2021, pp. 907–910. DOI: 10.1109/ITQMIS53292.2021.9642759.

[183] Ioannis Krontiris et al. "Autonomous Vehicles: Data Protection and Ethical Considerations". In: *Proceedings of the 4th ACM Computer Science in Cars Symposium*. CSCS '20. Feldkirchen, Germany: Association for

Computing Machinery, 2020. ISBN: 9781450376211. DOI: 10.1145/3385958.3430481.

[184] Mariia Bakhtina. "Securing Passenger's Data in Autonomous Vehicles". Master's Thesis. University of Tartu, Institute of Computer Science, 2021.

[185] University of Tartu. *Autonomous Driving Lab*. Available at https://adl.cs.ut.ee/ (visited on 29 October 2024).

[186] Whitney Quesenbery and Whitney Interactive Design. "Dimensions of usability: Defining the conversation, driving the process". In: *UPA 2003 Conference*. 2003, pp. 23–27.

[187] Petr Dzurenda et al. "Privacy-preserving solution for vehicle parking services complying with EU legislation". In: *PeerJ Comput. Sci.* 8 (2022), e1165. DOI: 10.7717/peerj-cs.1165.

[188] Sander Truu. "Tool-Supported Privacy Analysis of Smart Parking". Bachelor's Thesis. University of Tartu, Institute of Computer Science, 2024.

[189] Damiano Torre et al. "An AI-assisted Approach for Checking the Completeness of Privacy Policies Against GDPR". In: *2020 IEEE 28th International Requirements Engineering Conference (RE)*. 2020, pp. 136–146. DOI: 10.1109/RE48521.2020.00025.

[190] GDPR.EU. *GDPR checklist for data controllers*. Available at https://gdpr.eu/checklist/ (visited on 29 October 2024).

[191] Marlon Dumas, Luciano García-Bañuelos, and Peeter Laud. "Disclosure Analysis of SQL Workflows". In: *Graphical Models for Security*. Ed. by George Cybenko, David Pym, and Barbara Fila. Cham: Springer International Publishing, 2019, pp. 51–70. ISBN: 978-3-030-15465-3. DOI: 10.1007/978-3-030-15465-3_4.

[192] Rafael Accorsi, Andreas Lehmann, and Niels Lohmann. "Information leak detection in business process models: Theory, application, and tool support". In: *Information Systems* 47 (2015), pp. 244–257. ISSN: 0306-4379. DOI: https://doi.org/10.1016/j.is.2013.12.006.

[193] Nordic Institute for Interoperability Solutions. *X-Road WORLD MAP*. Available at https://x-road.global/xroad-world-map (visited on 29 October 2024).

[194] Nordic Institute for Interoperability Solutions (NIIS). *X-Road Academy*. Available at https://x-road.thinkific.com/ (visited on 29 October 2024). 2020.

[195] Fredrik Milani. *Digital business analysis*. Springer, 2019. DOI: 10.1007/978-3-030-05719-0.

[196] IIBA. *BABOK: A Guide to the Business Analysis Body of Knowledge*. v. 3. International Institute of Business Analysis, 2015. ISBN: 9781927584026.

[197] Nordic Institute for Interoperability Solutions (NIIS). *X-Road Documentation*. Available at https://github.com/nordic-institute/X-Road/tree/develop/doc (visited on 29 October 2024).

[198] Nordic Institute for Interoperability Solutions (NIIS). *X-Road Resources*. Available at https://x-road.global/xroad-library (visited on 29 October 2024).

[199] *Nordic Institute for Interoperability Solutions (NIIS)*. Available at https://www.niis.org/ (visited on 29 October 2024).

[200] Pinky Bai et al. "Self-Sovereignty Identity Management Model for Smart Healthcare System". In: *Sensors* 22.13 (2022). ISSN: 1424-8220. DOI: 10.3390/s22134714.

[201] Abylay Satybaldy, Mariusz Nowostawski, and Jørgen Ellingsen. "Self-Sovereign Identity Systems". In: *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers*. Ed. by Michael Friedewald et al. Cham: Springer International Publishing, 2020, pp. 447–461. ISBN: 978-3-030-42504-3. DOI: 10.1007/978-3-030-42504-3_28.

[202] Anhtuan Le, Gregory Epiphaniou, and Carsten Maple. "A comparative cyber risk analysis between federated and self-sovereign identity management systems". In: *Data & Policy* 5 (2023), e38. DOI: 10.1017/dap.2023.41.

[203] Verizon. *DBIR 2021 Data Breach Investigations Report*. Available at https://www.verizon.com/business/resources/reports/dbir/ (visited on 29 October 2024). 2021.

[204] Jean-Claude Laprie. *Dependability: basic concepts and terminology*. Vol. 5. Dependable Computing and Fault-Tolerant Systems. Springer, 1992, pp. 3–245. ISBN: 3-211-82296-8.

[205] Georgy Ishmaev. "Sovereignty, privacy, and ethics in blockchain-based identity management systems". In: *Ethics and Information Technology* 23.3 (2021), pp. 239–252.

[206] Tim Hobson et al. "Trustchain–trustworthy decentralised public key infrastructure for digital credentials". In: (2023).

[207] Paolo Giorgini et al. "Requirements engineering for trust management: model, methodology, and reasoning". In: *International Journal of Information Security* 5.4 (2006), pp. 257–274.

[208] Petteri Kivimäki. *Resisting Failure*. Available at https://www.niis.org/blog/2020/11/20/resisting-failure (visited on 29 October 2024). 2020.

[209] Digicert. *Understanding OCSP Times and What They Mean for You*. Available at https://www.digicert.com/blog/ocsp-times-and-what-they-mean-for-you (visited on 29 October 2024). 2015.

[210] Mohammed Shuaib et al. "Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison". In: *Mobile Information Systems* 2022 (2022), pp. 1–17. DOI: 10.1155/2022/8930472.

[211] Sovrin Foundation. *Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust*. White Paper. 2018.

[212] Andrew Tobin. *Sovrin: What Goes on the Ledger?* White Paper. Evernym, 2018.

[213] World Wide Web Consortium (W3C). *Peer DID Method Specification*. Available at https://www.w3.org/TR/did-spec-registries/#did-methods (visited on 29 October 2024). 2022.

[214] Georgy Ishmaev. "Sovereignty, privacy, and ethics in blockchain-based identity management systems". In: *Ethics Inf. Technol.* 23.3 (2021), pp. 239–252.

[215] Kin Long Leung. "Decentralized Public Key Infrastructure for X-Road". Master's Thesis. University of Tartu, Institute of Computer Science, 2023.

[216] Michael Lodder and Daniel Hardman. *Sovrin DID Method Specification*. Available at https://sovrin-foundation.github.io/sovrin/spec/did-method-spec-template.html (visited on 29 October 2024).

[217] The Hyperledger Foundation. *Hyperledger Aries Cloud Agent Python*. Available at https://github.com/hyperledger/aries-cloudagent-python(visited on 29 October 2024).

[218] NIIS. *X-ROAD®*. Available at https://x-road.global/ (visited on 29 October 2024).

[219] *Gaia-X: A Federated Secure Data Infrastructure*. Available at https://gaia-x.eu/ (visited on 29 October 2024).

[220] Verizon Business. *2023 Data Breach Investigations Report*. en. Available at https://www.verizon.com/business/resources/reports/dbir/ (visited on 29 October 2024). 2023.

[221] Christoph Buck et al. "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust". In: *Computers & Security* 110 (2021), p. 102436. ISSN: 0167-4048.

[222] Walid Fdhila, Nicholas Stifter, and Aljosha Judmayer. "Challenges and Opportunities of Blockchain for Auditable Processes in the Healthcare Sector". In: *BPM 2022 Blockchain, RPA and CEE Forum*. Cham: Springer International Publishing, 2022, pp. 68–83. ISBN: 978-3-031-16168-1. DOI: 10.1007/978-3-031-16168-1_5.

[223] European Union Agency for Cybersecurity et al. *Digital Identity: Leveraging the SSI Concept to Build Trust*. Publications Office of the European Union, 2022. DOI: 10.2824/8646.

[224] Jianwei Liu et al. "An analysis of digital identity management systems-a two-mapping view". In: *BRAINS*. IEEE, 2020, pp. 92–96.

[225] Andreas Grüner, Alexander Mühle, and Christoph Meinel. "An Integration Architecture to Enable Service Providers for Self-sovereign Identity". In: *NCA*. IEEE, 2019, pp. 1–5. DOI: 10.1109/NCA.2019.8935015.

[226] Aaliya Sarfaraz, Ripon K. Chakrabortty, and Daryl L. Essam. “AccessChain: An access control framework to protect data access in blockchain enabled supply chain”. In: *FGCS* 148 (2023), pp. 380–394. ISSN: 0167-739X. DOI: 10.1016/j.future.2023.06.009.

[227] Andreas Abraham et al. “Privacy-Preserving eID Derivation to Self-Sovereign Identity Systems with Offline Revocation”. In: *IEEE TrustCom 2021*. 2021, pp. 506–513.

[228] Muhammad Ajmal Azad et al. “Verify and trust: A multidimensional survey of zero-trust security in the age of IoT”. In: *Internet of Things* 27 (2024), p. 101227. ISSN: 2542-6605. DOI: https://doi.org/10.1016/j.iot.2024.101227.

[229] Binanda Sengupta and Anantharaman Lakshminarayanan. “DistriTrust: Distributed and low-latency access validation in zero-trust architecture”. In: *Journal of Information Security and Applications* 63 (2021), p. 103023. ISSN: 2214-2126. DOI: 10.1016/j.jisa.2021.103023.

[230] Lampis Alevizos, Vinh Thong Ta, and Max Hashem Eiza. “Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review”. In: *SECURITY AND PRIVACY* 5.1 (2022), e191. DOI: 10.1002/spy2.191.

[231] Jana Glöckler et al. “A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity”. In: *Business & Information Systems Engineering* (2023).

Appendix A. COMPONENTS OF THE PROPOSED METHOD

Table 15: Components of the method for information security and privacy management in smart solutions

Concept	Procedure	Notation
Business Goal	Identified by the requirements and goals of the smart solution	In plain text as Goals or Requirements
Business Process	Using documentation and tacit knowledge, the business analyst creates the BPMN models to depict the key collaborative processes within the smart solution. The models might be extended or annotated based on the input from DPO, CISO, and Security architect to depict their domain knowledge during any stage of the framework.	BPMN, PE-BPMN, in plain text within FISP-ProCOP matrix
Actors Relationship	Describes dependencies and trust between actors involved in a smart solution. Using documentation and tacit knowledge, the business analyst creates the i* models to depict the dependencies (including trust) between smart solution entities.	i*, trust model, in plain text within FISP-ProCOP matrix
System Component	Using documentation and tacit knowledge, the security architect creates the models to depict the system components involved in the collaborative processes within the smart solution. The models might be extended or annotated based on the input from DPO, CISO, and a business analyst to depict their domain knowledge during any stage of the framework.	Class diagram, Conceptual Architecture model, Component diagram, in plain text within FISP-ProCOP matrix
Data Object	Using documentation and undocumented knowledge, the expert group defines the data objects during the first step of the method. The data object should be depicted as a static class diagram to depict the types of information used in the smart solution and the relationships between them. Additionally, the data objects' transformation and usage throughout the smart solution processes should be depicted through BPMN models. The dependencies among actors and system components on the data objects are depicted in i* model or in plain text.	BPMN, Class diagram, i*, in plain text within FISP-ProCOP matrix
Data Flow	Describes how the data objects are manipulated and transferred between system components and actors. Depicted as a part of InfoSec & privacy mgmt aspects, business processes, system architecture, and actor relationships	BPMN, Class diagram, Conceptual architecture model, i*, in plain text within FISP-ProCOP matrix
Security Criteria	Identified for the exchanged data in the collaborative processes by understanding the importance of such data objects.	in plain text within FISP-ProCOP matrix
Privacy Objective	Identified for the personal data objects used in the smart solution with respect to the trust model	in plain text within FISP-ProCOP matrix

The UML class diagram in Figure 38 depicts components of the FISP-ProCOP attributes and maps them with the key concepts operated within the proposed method for information security and privacy management in smart solutions. Yellow objects highlight the method input, green – key method concepts, and purple – possible concepts representations used as intermediate data objects in the method.

Table 16 depicts the data model for the proposed method for information security and privacy management in smart solutions, reflecting dependencies between data objects created through the thesis contributions usage by the expert group.

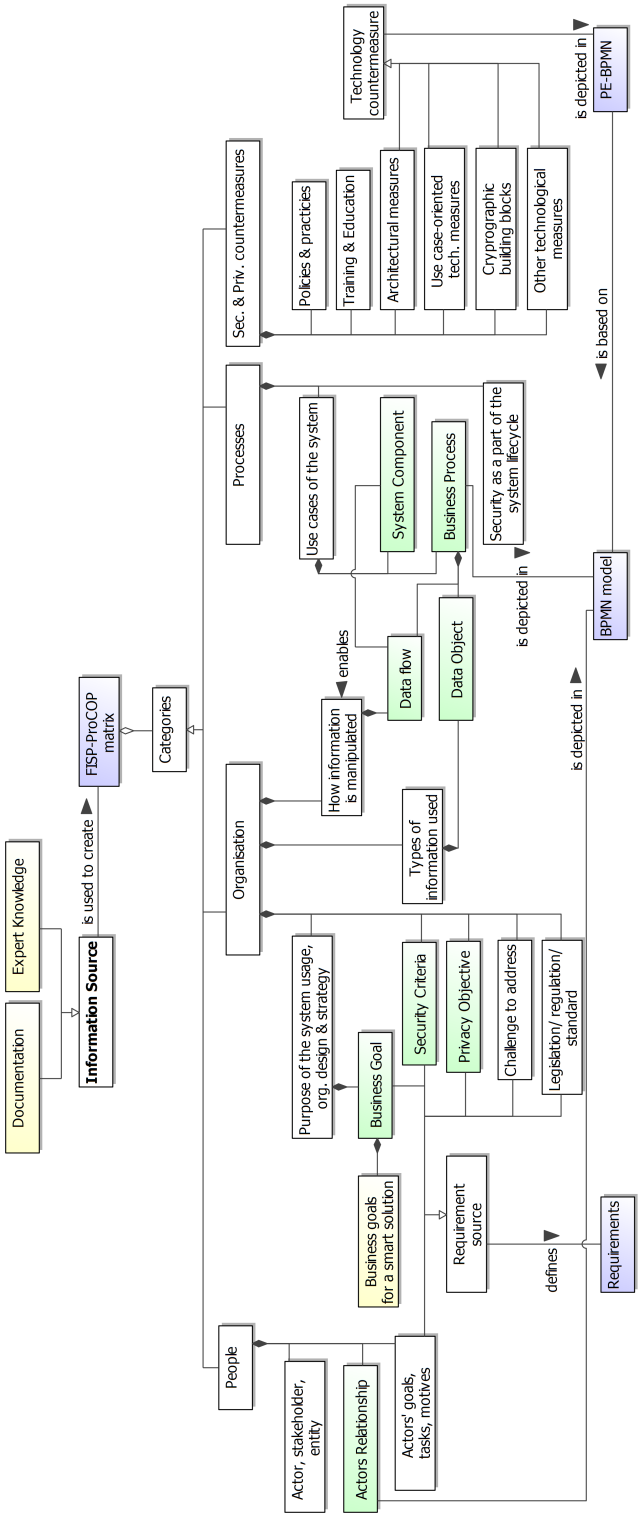


Figure 38: FISP-ProCOP attributes data model

Table 16: The proposed method data model

Contr. #.step	Step executor	DO ID	Data object (DO)	Form	Data object attributes	Other sources	Create based on other DO	Source in FISP-ProCOP
C1	All	1	Business goals for a smart solution	Textual description				
		2	Documentation	Oranisational policies, rulebook, reports; System documentation; other written documents				
		3	Expert knowledge	Unwritten knowledge or informal documents, draft, notes, etc.				
		4	FISP-ProCOP matrix	Table			1, 2, 3	
		5	Requirements	Textual description			4	
C2.1	DPO, BA, Security Architect	6	User input	Selections in DPO tool UI	Roles assignment		4, 5	PA, PR
					Personal Data Objects			OI
					Processing tasks			OI, PrU, CP, CT
					Purpose of processing & consent			PA, PR, OI, OC
					Processing system and technical measures			CP, CT, PrL,PrU
		7	Business process	BPMN model	Actors		4, 5	PA
					Tasks			PA, PR, PrU, CT, CE
					Data Objects			OI
					Data Flow			OI, PR, PrU, CT
		8	Compliance	UML class diagram	Violation explanation	DPO tool	6, 7	
		9	General process improvements	BPMN model, textual description	Actors	Added based on the Compliance issues and Business process by DPO, BA or Security Architect	7, 8	
					Tasks			
					Data Objects			
					Data Flow			
C2.2	CISO, BA, Security Architect	10	Business process	PE-BPMN model	Business process (as a BPMN model)		7	
					Communication protection	Added based on the compliance issues by Security Architect		CT
					PET-Task (optionally, with Computation script)			CT
		11	Privacy disclosure results	Table	Actor	Pleak tool	10	
					Data Object			
					Data visibility to actors			
		12	BPMN leak-when results	Table	Data Object	Pleak tool	10	
					Dependent Data Object			
					Leakage condition			
C.2.3	All	13	GDPR-compliant privacy-assured business process	BPMN model, PE-BPMN model	Business process (as a BPMN model)		7, 9	
					Compliance issues (non-vialation expalantions)		8	
					Privacy disclosure results		11	
					BPMN leak-when results		12	
C3.1 C4.1	BA	14	Actors, resources, objectives	Textual description	Actors		4	PA, PR
					Exchange data resources			OI
					Objective of actors			PR, PrU
					Trust assumptions			PR
C3.2 C4.2	BA, Security Architect	15	IdM system 1 model	BPMN model	Actors, actors relationship, exchanges data objects, data flow, actors tasks, system components, system tasks, technologies		4	PA, PR, OI, CP, CT
				Class diagram				
				Sequence diagram				
				(Conceptual) system architecture model				
				i* dependency model				
				Component diagram				
C3.4 C4.4	BA, Security Architect	16	IdM system 2 model	BPMN model	Actors, actors relationship, exchanges data objects, data flow, actors tasks, system components, system tasks, technologies	Designed based on external system documentation, guidelines, standards, etc. by Security Architect, CISO and BA	4	PA, PR, OI
				Class diagram				
				Sequence diagram				
				(Conceptal) system architecture model				
				i* dependency model				
				Component diagram				
C3.3, C3.5 C4.3, C4.5	BA, Security Architect	17	Assessment model	Table				
C3.6 C4.6	All	18	Assessment results	Table		External publications, reports, system evaluations	4, 15, 16, 17	

Appendix B. FISP-PROCOP ARTEFACTS

B.1. FISP-ProCOP Desription

Table 18 depicts the FISP-ProCOP matrix with the guiding questions in the last column. These questions should be used by the expert group to identify inconsistencies in information security and privacy management across the matrix attributes.

Table 17: FISP-ProCOP matrix for a ride-hailing company

Dimension	Category	Attribute	#	Cross-validation questions between attributes (#)
P. People	PA. Actors	Actors, stakeholders, entities	1	I. Did you include the actors (1) who provide the security measures (13, 14, 15, 16)? II. Did you include all the actors (1) involved in business processes (18) for the end-users within the smart system?
		Goals, tasks, motives	2	III. Which of the actors (1) is fully trusted to share the information (7) with?
	PR. Relationships	Relationships and dependencies between actors	3	IV. Did you depict the relationships (3) between all the actors (users, stakeholders, service providers) (1) including the ones outside of smart system scope?
O. Organisation	OS. Strategy	Purpose for the system usage, org. design & strategy	4	V. Does the mentioned system purpose consider the interests (2) of the actors (1)? VI. Does the number of active end-users pose a challenge (5) to the smart system? VII. Is the level of your organisation's involvement in the smart system lifecycle reflected in the policies & practices (11) used for the partners? VIII. Do you mention owners of the systems your organisation use as actors (1)? IX. Do you mention owners of the systems your smart system has integrations with as actors (1)?
		Challenges to address	5	X. Can the mentioned challenges be solved by using the respective standards (6)? XI. Are the mentioned challenges addressed by any measures in (11, 12, 13, 14, 15, 16)?
	OC. Formal Constraints	Legislation, regulation, standard	6	XII. Do the legislations, regulations, and standards (6) include sector-specific (4) regulations and standards w.r.t. the system purposes?
	OI. Information Involved	Type of information used	7	XIII. Who from (1) is the origin or provider of this information? How do you verify the origin?
		How the information is manipulated	8	XIV. Does the infromation manipulation by actors in (1) directly correspond to their goals in (2)? XV. Do the manipulation operations (8) over the information (7) correspond to the system purpose (4)?
		Security criteria	9	XVI. Can the dependencies (3) between actors (1) violate security criteria (9)? XVII. Do the defined security criteria (9) consider the all the requirements for the information types (7) w.r.t. legislations and standards (6)?
		Privacy objectives	10	XVIII. Did you define the rules of PII (8) visibility (10) for all the actors (1)? XIX. Can the dependencies (3) between actors (1) violate privacy criteria (10)? XX. Do the defined security criteria (9) consider the all the requirements for the information types (7) w.r.t. legislations and standards (6)?
C. Sec. & Privacy Countermeasures	CP. Policies & Practices	Policies & practices	11	XXI. Are the policies & practices (11) include all the mandatory ones from regulations and standards (6)?
	CE. Training & Education	Training & education	12	XXII. Do you have training & education (12) measures for all the actors in (1) (users, stakeholders, external entities)? XXIII. Do the training & education (12) include all the mandatory ones from regulations and standards (6)?
	CT. Technology	Architectural measures	13	XXIV. Do the architectural measures (13) include all the mandatory ones from regulations and standards (6)?
		Use case-oriented technological measures	14	XXV. Do the use case-oriented measures (14) include all the mandatory ones from regulations and standards (6)?
		Cryptographic building blocks	15	XXVI. Do the used cryptographic measures (15) include all the mandatory ones from regulations and standards (6)?
		Others technological measures	16	XXVII. Do the other technological measures (15) include all the mandatory ones from regulations and standards (6)?
Pr. Processes	PrL. System Lifecycle	Security as a part of the system lifecycle	17	XXVIII. Does the system lifecycle (17) include all the mandatory activities, practices, etc. from the followed regulations and standards (6)?
	PrU. Usage of the System	Use cases of the system as a part of the business processes	18	XXIX. Do the specified business processes cover the data exchange (8) of all the information types (7) with all the actors (1)?

Table 18 depicts an example of the FISP-ProCOP matrix for a ride-hailing company[22].

Table 18: FISP-ProCOP matrix for a ride-hailing company

Dimension	Category	#	Attribute	Attribute instances	
P. People	PA. Actors	1	Actors, stakeholders, entities	Users: driver, car owners; Service providers: AWS, Paypal, Payment system provider; Other stakeholders: Trusted Authority, City government, Local taxi firms	
		2	Goals, tasks, motives	user, service provider, IaaS	
	PR. Relationships	3	Relationships and dependencies between actors	TA is governed by a city government	
O. Organisation	OS. Strategy	4	Purpose for the system usage, org. design & strategy	Objective: ride-hailing in the cities; Active end-user: 1,001 — 10,000; Involvement in the system lifecycle: We have a development team that is fully responsible for the system, its support and development; Number of integrations: 1-2	
		5	Challenges to address	interoperability, availability	
	OC. Formal Constraints	6	Legislation, regulation, standard	European Union directive 2010/40/EU (7 July 2010) (a.k.a. ITS Directive), NIS2 directive, Předpis 181/2014 Sb. (zákon o kybernetické bezpečnosti), ISO/IEC 27001, No, not certified	
	OI. Information Involved	7	Type of information used	Car plates	Driver ID
		8	How the information is manipulated	Car plates are shared with Driver and City governement	we save DriverID for checking the eligibility of driving
		9	Security criteria	Confidentiality, Integrity	Confidentiality, Integrity
		10	Privacy objectives	Not a PII	Controller: We are; Processor: PLT; Can be shared with: PLT & City government
C. Sec. & Privacy Counter measures	CP. Policies & Practices	11	Policies & practices	Policies & Practices: NIST CSF, Security Development Lifecycle; Principles: Least privilege, Data minimisation; Knowledge management practices: System documentation, Unwritten rules followed by the teams	Coordination of policies with partners: auditing
	CE. Training & Education	12	Training & education	Trainings for user: Introducing the privacy policy during the first-time onboarding to the system; Trainings for employees: we don't have	
	CT. Technology	13	Architectural measures	Architecture: Public Key Infrastructure (PKI); Managing identities of partners: access control & logging	
		14	Use case-oriented technological measures	Payment-related measures: Card-based payment	Document creation-related measures: usual document
		15	Cryptographic building blocks	Classical cryptograhy: RSA digital signature; Post-quantum cryptography: No	
		16	Others technological measures	IAM: Role-based access control; Secure communication: Not applicable; Other: firewall	
Pr. Processes	PrL. System Lifecycle	17	Security as a part of the system lifecycle	Principles of system development and support: Security testing, Separation of development, test and production environments; Security monitoring: Vulnerability scanner	
	PrU. Usage of the System	18	Use cases of the system as a part of the business processes	Ride fulfilment, gas fill-in; car service	

[22]The spreadsheet can be accessed here: `https://doi.org/10.5281/zenodo.14923440`.

Table 19: FISP-ProCOP matrix for a ride-hailing company

#	Cross-validation questions between attributes	Explanation for validation failure	Validation result
1	I. Are the mentioned actors (1) include the providers of the security measures (13, 14, 15, 16)?		Yes
	II. Are the mentioned actors (1)include all the parties involved in business processes (18) for the end-users within the smart system?	Our employees participate in car services, but are not included as actors	No
2	III. Are all the actors (1) trusted to share the information (7) with for their purposes (2)?		Yes
3	IV. Did you depict the relationships (3) between all the actors (users, stakeholders, service providers) (1) including the ones outside of smart system scope?		Yes
4	V. Does the mentioned system purpose consider the interests (2) of the actors (1)?		Yes
	VI. If the number of active end-users poses a challenge to the smart system, is it mentioned in as a challenge (5)?		Yes
	VII. Is the level of your organisation's involvement in the smart system lifecycle reflected in the policies & practices (11) used for the partners?		Yes
	IX. Do you mention owners of the systems your smart system has integrations with as actors (1)?	We didn't mention the integration with payment system providers	No
5	X. Can the mentioned challenges be solved by using the respective standards (6)?		Yes
	XI. Are the mentioned challenges addressed by any measures in (11, 12, 13, 14, 15, 16)?		Yes
6	XII. Do the legislations, regulations, and standards (6) include sector-specific (4) regulations and standards w.r.t. the system purposes, sector and location of your partners (1)?	ITS directive is mandatory for transportation but is not mentioned; We operate in EU and collect Driver's info, therefore GDPR is relevant, but isn't mentioned	No
7	XIII. Who from (1) is the origin or provider of this information? Do the measures in (13, 14, 15, 16) verify the origin?	yes, RSA signature	Yes
8	XV. Do the manipulation operations (8) over the information (7) correspond to the system purpose (4)?		Yes
9	XVI. Are there no dependencies (3) between actors that may violate security criteria (9)?		Yes
	XVII. Do the defined security criteria (9) consider all the requirements for the information types (7) w.r.t. legislations and standards (6)?		Yes
10	XVIII. Did you define the rules of PII (8) visibility (10) for all the actors (1)?	We didn't specify the need of protecting DriverID from access by AWS or Payment system provider	No
	XIX. Do the dependencies (3) between actors (1) not violate privacy criteria (10)?		Yes
	XX. Do the defined roles (10) consider all the requirements for the information types (7) w.r.t. legislations and standards (6)?		Yes
11	XXI. Are the policies & practices (11) include all the mandatory ones from regulations and standards (6)?		Yes
12	XXII. Do you have training & education (12) measures for all the actors in (1) (users, stakeholders, external entities)?		Yes
	XXIII. Do the training & education (12) include all the mandatory ones from regulations and standards (6) and policies (11)?	Trainings for employees are absent but are required by the followed NIST CSF	No
13	XXIV. Do the architectural measures (13) include all the mandatory ones from regulations and standards (6) and policies (11)?		Yes
14	XXV. Do the use case-oriented measures (14) include all the mandatory ones from regulations and standards (6) and policies (11)?		Yes
15	XXVI. Do the used cryptographic measures (15) include all the mandatory ones from regulations and standards (6) and policies (11)?	ISO 27001 encourages considering emerging threats like quantum computing. Thus, having threat of "harvest now, decrypt later", we should start using post-quantum cryptography in the upcomming years	No
16	XXVII. Do the other technological measures (15) include all the mandatory ones from regulations and standards (6)?		Yes
17	XXVIII. Does the system lifecycle (17) include all the mandatory activities, practices, etc. from the followed regulations and standards (6)?	Threat modelling is a part of Sec. Dev-t Lifecycle but is not mentioned here	No
18	XXIX. Do the specified business processes cover the data exchange (8) of all the information types with all the actors (1)?		Yes

Table 20 provides the mapping of the components of FISP-ProCOP with the clauses of the ISO/IEC 27001 standard [27].

Table 20: Mapping FISP-ProCOP with the clauses in ISO/IEC 27001

FISP-ProCOP			ISO/IEC 27001 clauses																											
Dimension	**Category**	**#**	**4.1**	**4.2**	**4.3**	**4.4**	**5.1**	**5.2**	**5.3**	**6.1 .1**	**6.1 .2**	**6.1 .3**	**6.2**	**6.3**	**7.1**	**7.2**	**7.3**	**7.4**	**7.5 .1**	**7.5 .2**	**7.5 .3**	**8.1**	**8.2**	**8.3**	**9.1**	**9.2 .1**	**9.2 .2**	**9.3 .1**	**9.3 .2**	**9.3 .3**	**10.1**	**10.2**
P. People	**PA.** Actors	1		a																											
		2		b																											
	PR. Relationships	3		b																											
O. Organisation	**OS.** Strategy	4	●				a, b	a																							
		5	●																												
	OC. Formal Constraints	6		●																											
	OI. Information Involved	7											○																		
		8		●																											
		9		c				b					○																		
		10		c																											
C. Sec. & Privacy Countermeasures	**CP.** Policies & Practices	11						e, f, g	○	○	○	○		○					●	○	a	●	○	○	○	○	○	○	○	○	○
	CE. Training & Education	12						f				○b					●	●													
	CT. Technology	13										○b																			
		14										○b																			
		15										○b																			
		16										○b																			
Pr. Processes	**PrL.** System Lifecycle	17		c	●					●	○	○	○							○				○	○	○	○	○	○	○	○
	PrU. Usage of the System	18		c																		●									

● - the clause is covered by the marked FISP-ProCOP attribute

○ - the clause is covered not explicitly by the marked FISP-ProCOP attribute

- the clause is covered by some attributes

- the clause is covered not explicitly by some attributes

- the clause is not covered by any attributes

B.2. Study 2: FISP-ProCOP Validation

Table 21 contains the questions from the questionnaire used in Study 2 for FISP-ProCOP validation.

Table 21: Study 2 - Questionnaire (shortened) [26]

General questions about the company
1.1. What is your organization's name?
1.2. What is your position/role in the organization?
1.3. Where does your company primarily operate?
1.4. For which purposes does your company use IT system(s)?
1.5. Would you call the system used in your company "an intelligent transportation system"?
1.6. In which area does your company primarily operate?
1.7. How many active end-users does your digital solution have in the selected region?
Section "Organization"
2.1. What is the main objective of your ITS?
2.2. How much is your company involved in the lifecycle of your ITS?
2.3. How much has your system changed during the last 5 years?
2.4. With how many external systems is your system integrated?
2.5. What are the challenges you face during the usage/development/support of your ITS?
2.6. What kind of information is used within your ITS?
2.7. Which security or privacy-related legislation and/or regulations affect your ITS?
2.8. Which cyber/information security standard(s) does your organization follow?
Section "Security and Privacy measures. Part 1"
3.1. Who are the stakeholders of your products/services the ITS?
3.2. What are the practices and policies used for assuring information security and/or privacy management in your company?
3.3. How much security development is integrated into your system lifecycle?
3.4. Which information security and privacy training are established for your system users?
3.5. Which information security and privacy training are established for the employees?

Table 21 – *Continued from previous page*

Section "Security and Privacy measures. Part 2"
4.1. Which of the following architectural measures are used in your ITS?
4.2. Which technologies are used in your ITS for authentication and access control?
4.3. Which measures are used in your ITS for secure communication between parties?
4.4. Which cryptographic measures are used in your intelligent transportation system?
Section "Security and Privacy measures. Part 3: System functionality"
4.5.1. Do you have navigation/routing functionality in your ITS?
4.5.2. Which technologies are used in your ITS for navigation/routing?
4.6.1. Do you have payment functionality in your ITS?
4.6.2. Which technologies are used in your ITS for payment?
4.7.1. Do you have a location-based search in your ITS?
4.7.2. Which technologies are used in your ITS for parking slot/toll/vehicle search?
4.8.1. Do you have the functionality of pass/reservation document creation in your ITS?
4.8.2. Which technologies are used in your ITS for pass/reservation document creation?
Section "Security and Privacy measures. Other"
4.9. What are the other security- or privacy-preserving technologies used in your ITS which were not mentioned?
4.10. Do you consider employing post-quantum cryptography in the future in your ITS?
Section "Security and Privacy measures. Part 4: Processes"
5.1. Which of the following principles are used during your system development/support?
5.2. Which network security measures are used for your ITS support?
Follow-up questions about this survey
How would you assess the level of your information system security?
Which sources did you use to answer this survey?
How easy was it for you to find the information asked in this survey?

Table 22 depicts the mapping of the questionnaire with the framework's dimensions and attributes.

Table 22: Study 2 - Mapping attributes of FISP-ProCOP with the questionnaire [26].

Dimension	Category	Attribute	Questions from the questionnaire
P. People	PA. Actors	Actors, stakeholders, entities	3.1; Follow-up questions
		Goals, tasks, motives	
	PR. Relationships	Relationships and dependencies between actors	-
O. Organisation	OS. Strategy	Purpose for the system usage, org. design & strategy	2.1,
		Challenges to address	2.5
	OC. Formal Constraints	Legislation, regulation, standard	2.7-2.8
	OI. Information Involved	Type of information used	2.6
		How the information is manipulated	-
		Security criteria	-
		Privacy objectives	-
C. Sec. & Privacy Countermeasures	CP. Policies & Practices	Policies & practices	3.2-3.3, 4.1, 5.1; Follow-up questions
	CE. Training & Education	Training & education	3.4-3.5
	CT. Technology	Architectural measures	4.1
		Use case-oriented technological measures	4.2-4.3, 4.5-4.8
		Cryptographic building blocks	4.4, 4.10
		Others technological measures	4.9
Pr. Processes	PrL. System Lifecycle	Security as a part of the system lifecycle	2.2-2.3, 5.2
	PrU. Usage of the System	Use cases of the system as a part of the business processes	4.5-4.8

Appendix C. PRIVACY ANALYSIS ARTEFACTS

C.1. Study 3: Ride Fulfilment

Figure 39 depicts the instantiated GDPR model for processing task '3. Approve ride'.

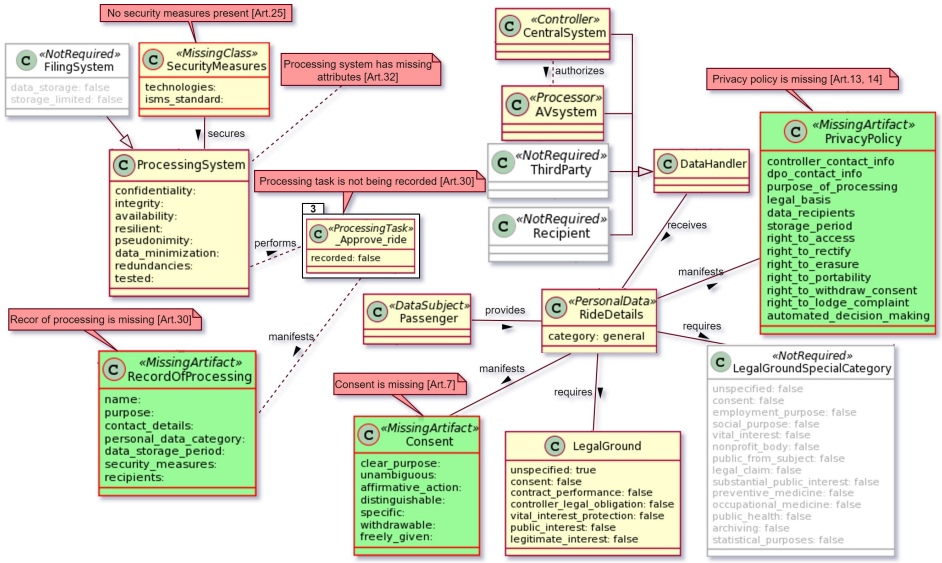


Figure 39: Study 3 - GDPR compliance check results: output of the DPO tool [59]

Figure 40 depicts the proposed general redesign aspects with the blue artefacts, and the green ones correspond to the activities where PETs need to be applied.

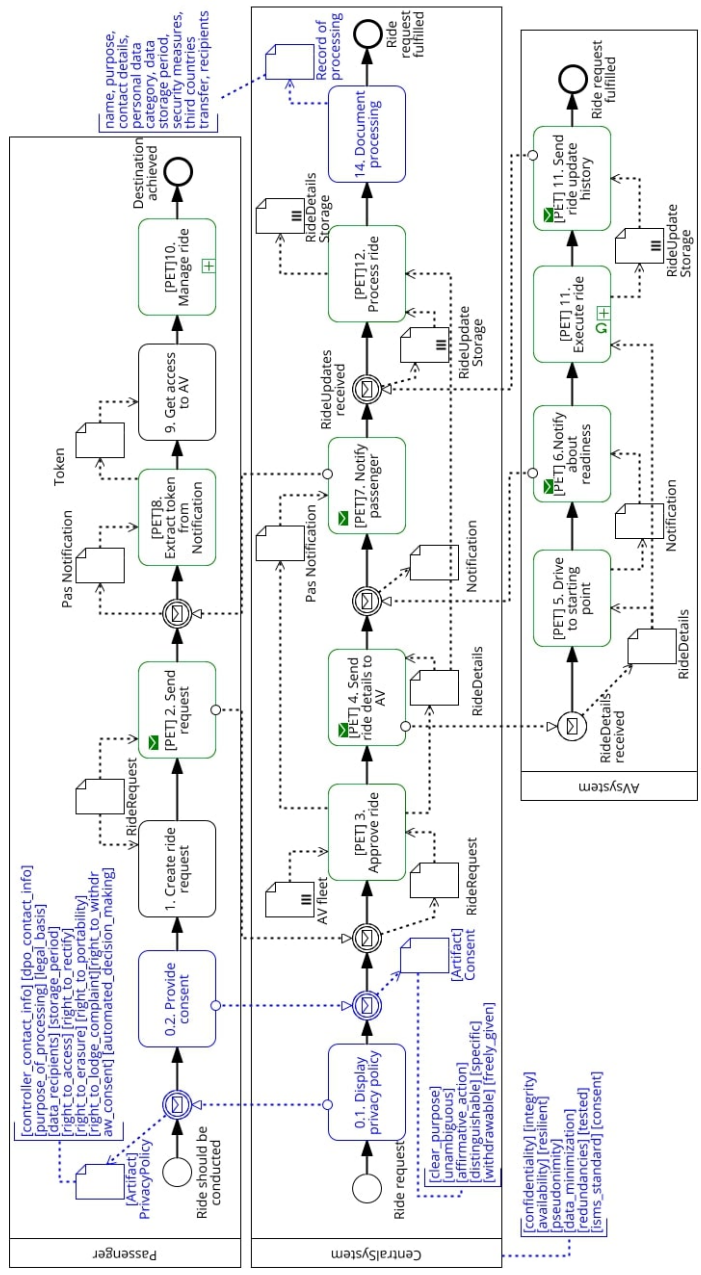


Figure 40: Study 3 - The developed GDPR-compliant business process [59]

The results of data disclosure analysis in Pleak are presented in Figure 41, and they show data artefacts visibility considering employed PETs.

#	IntermToken	EncrPas Notification, PasNotification	Encr RideDetails, RideDetails	RideDetails Storage_1, RideDetails Storage_2	Encr RideRequest, RideRequest	RideUpdate Storage, RideUpdate Storage_1, RideUpdate Storage_2	Token	privateKey_A	privateKey_B	publicKey_A	publicKey_B
AVsystem	V	V	V	-	-	V	-	O	-	-	O
CentralSystem	V	H	H	H	H	H	-	-	-	-	-
External _server	-	-	-	H	-	H	-	-	-	-	-
Passenger	-	V	-	-	O	-	V	-	O	O	-

Figure 41: Study 3 - Example of data disclosure analysis results (V - visible, O - owner, H - hidden)

C.2. Study 4: Smart Parking

The following As-Is models are used as $BPMN_1$ inputs for the proposed method:

- Register user (Figure 42);
- Request a parking permit (Figure 43a);
- Conduct payment (Figure 43b);
- Park a vehicle (Figure 44);
- Request extension (Figure 45);
- Analyse parking (Figure 46).

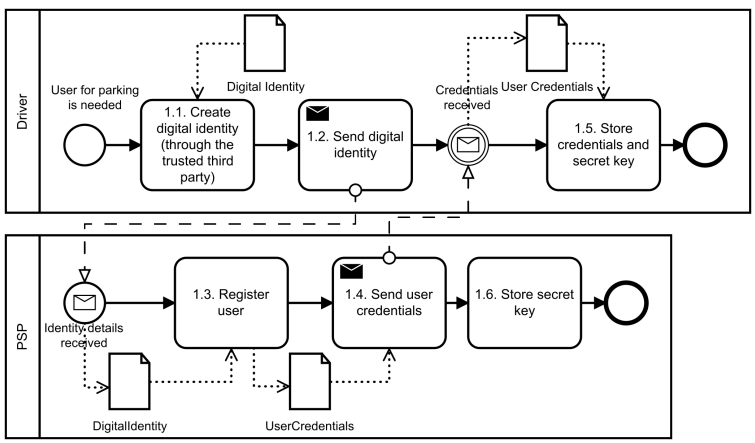
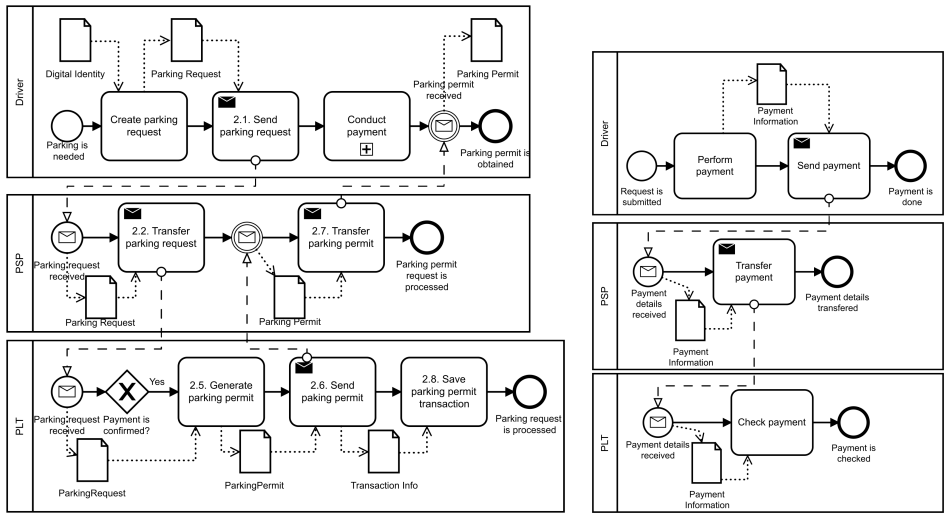


Figure 42: Study 4 - Register user As-Is sub-process (adapted from [188, 187]



(a) Study 4 - Request permit (b) Study 4 - Conduct payment

Figure 43: Study 4 - Request permit and Conduct payment As-Is sub-processes (adapted from [188, 187])

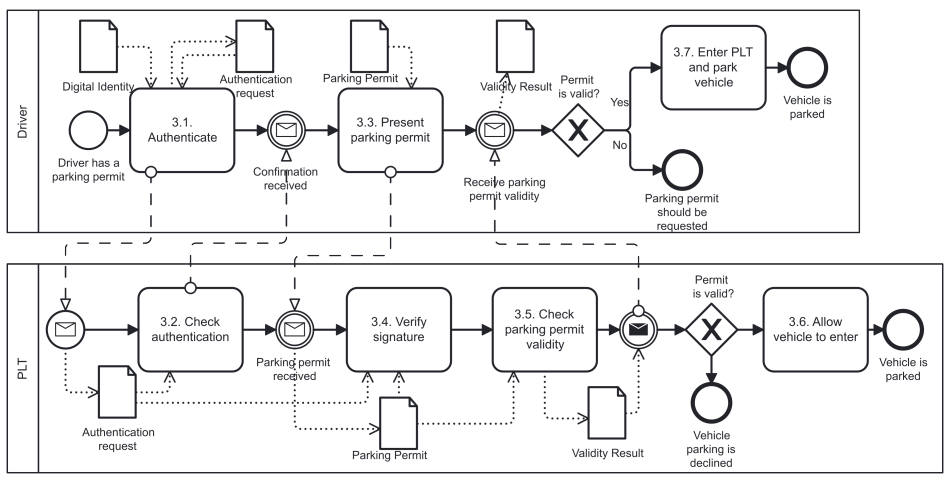


Figure 44: Study 4 - Park a vehicle As-Is sub-process (adapted from [188, 187]

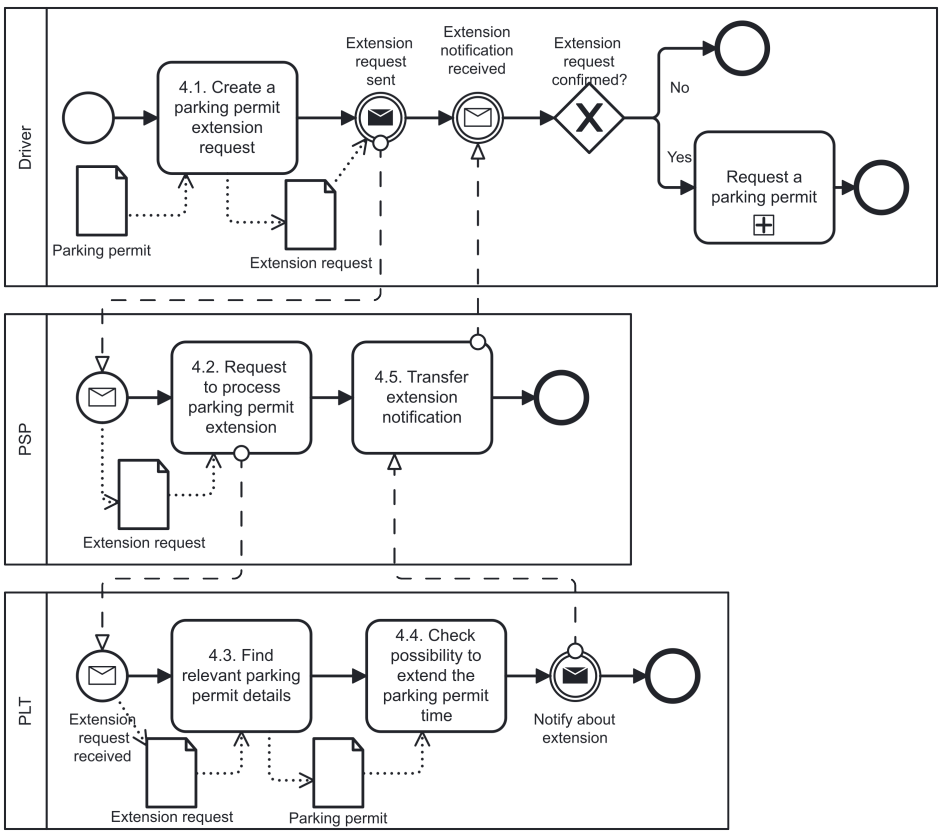


Figure 45: Study 4 - Request extension As-Is sub-process (adapted from [188, 187]

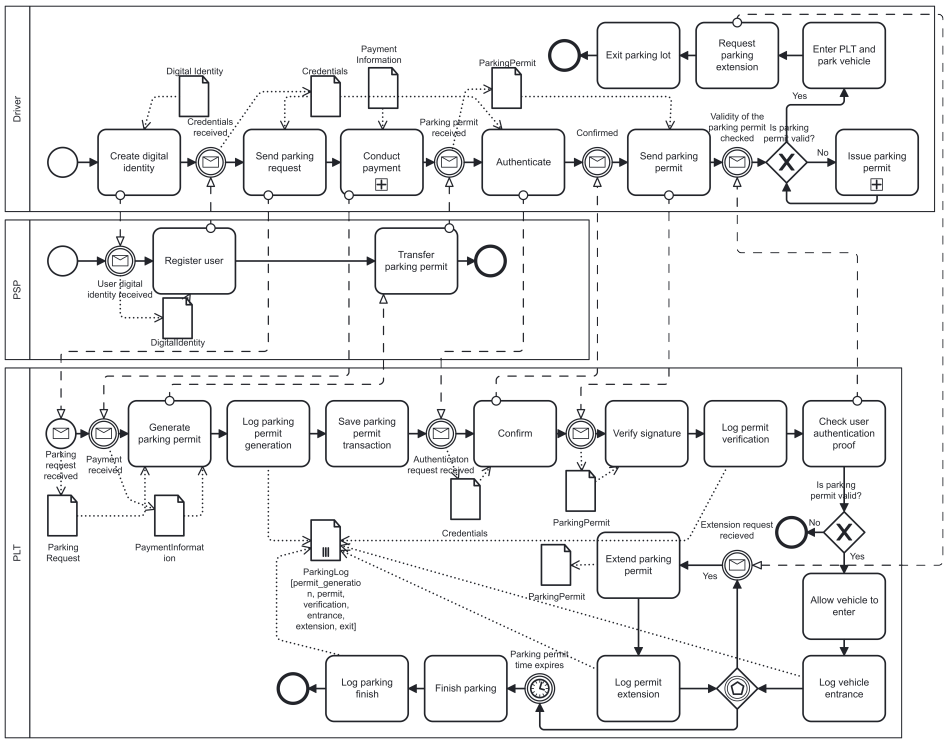


Figure 46: Study 4 - Analyse parking As-Is sub-process (adapted from [188, 187]

Table 23 depicts the exact inputs used in the DPO Tool for each sub-process in order to conduct GDPR compliance analysis.

Sub-Process	**Data subject**	**Controller**	**Processor**	**Processing task**	**Personal Data object**
Register User	Driver	PSP	PSP	Process Digital Identity	Digital Identity
Request a parking permit	Driver	PSP	PLT	Transfer parking permit (representing the delegated Generate parking permit)	Parking Request (based on Digital Identity)
Conduct Payment	Driver	PSP	PLT	Transfer payment (representing the delegated Check payment)	Payment Information

Table 23: DPO Tool Inputs for the Sub-Processes

Figure 47 depicts the instantiated GDPR model for processing task 'Transfer parking permit' in the Request permit As-Is sub-process.

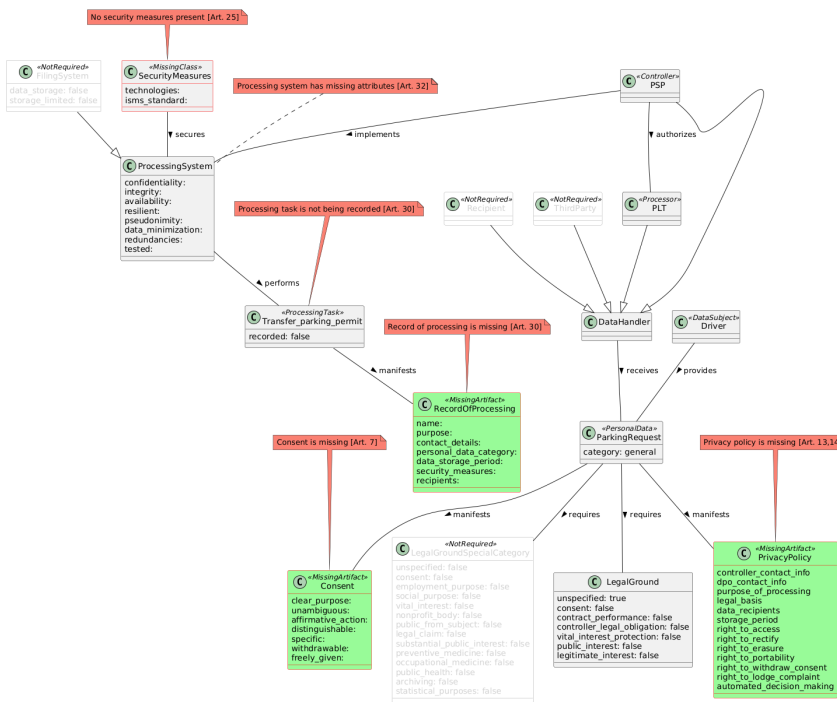


Figure 47: Study 4 - GDPR compliance check results for Request permit As-Is sub-process (adapted from [188])

Figure 48 depicts the Request permit To-Be sub-process extended with PKI encryption and GDPR-required process aspects.

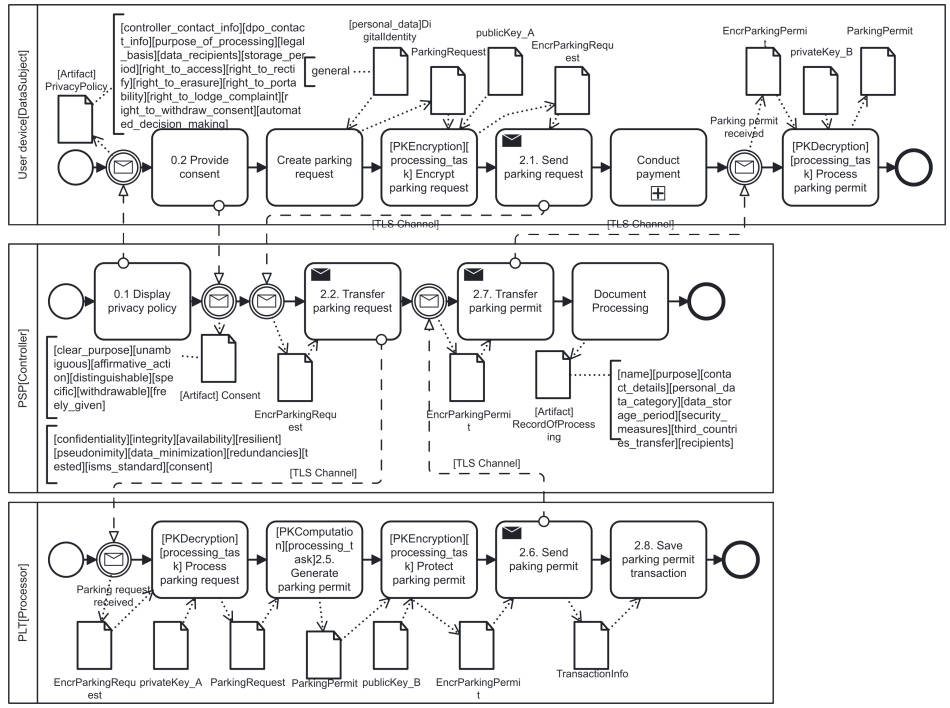


Figure 48: Study 4 - Request permit To-Be sub-process (adapted from [188])

The results of data disclosure analysis in Pleak are presented in Figure 49, and they show data artefacts visibility considering employed PETs of Request permit To-Be sub-process.

#	DigitalId	EncrParkingPermit, ParkingPermit	EncrParkingRequest, ParkingRequest	TransactionInfo	privateKey_A	privateKey_B	publicKey_A	publicKey_B
Driver	O	V	V	-	-	O	O	-
PLT	-	V	V	V	O	-	-	O
PSP	-	H	H	-	-	-	-	-

Figure 49: Study 4 - Data disclosure analysis results for Request permit To-Be sub-process (V - visible, O - owner, H - hidden)

Figure 50 depicts the instantiated GDPR model for processing task ‘Protect parking permit’ in the Request permit To-Be sub-process.

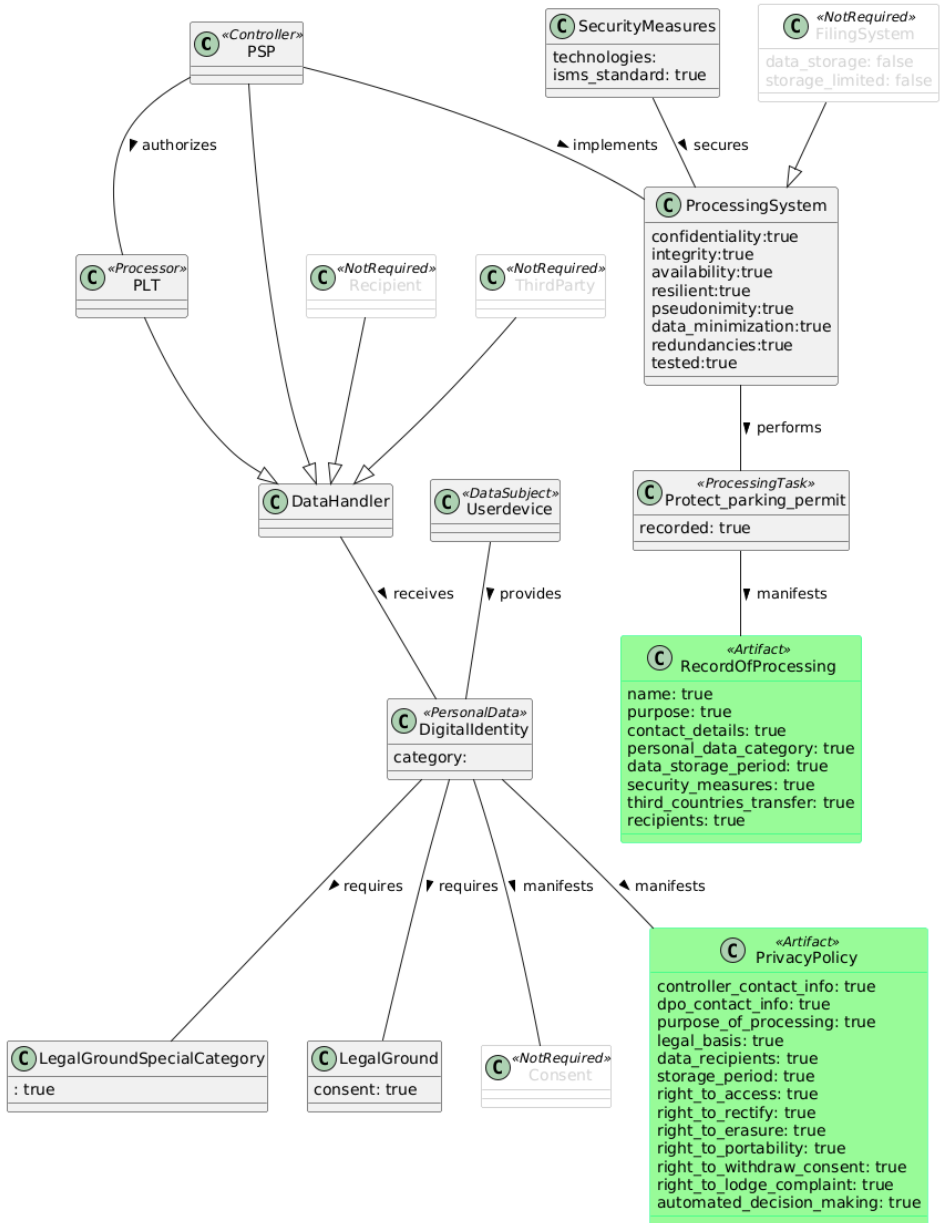


Figure 50: Study 4 - GDPR compliance check results for Request permit To-Be sub-process (adapted from [188])

Appendix D. IDM SYSTEM ANALYSIS ARTEFACTS

This appendix contains additional models created during the development and evaluation of Contribution 3 and Contribution 4.

D.1. PKI-based IdM System in X-Road

Figure 51 depicts a process of a new Member onboarding in the form of a BPMN model.

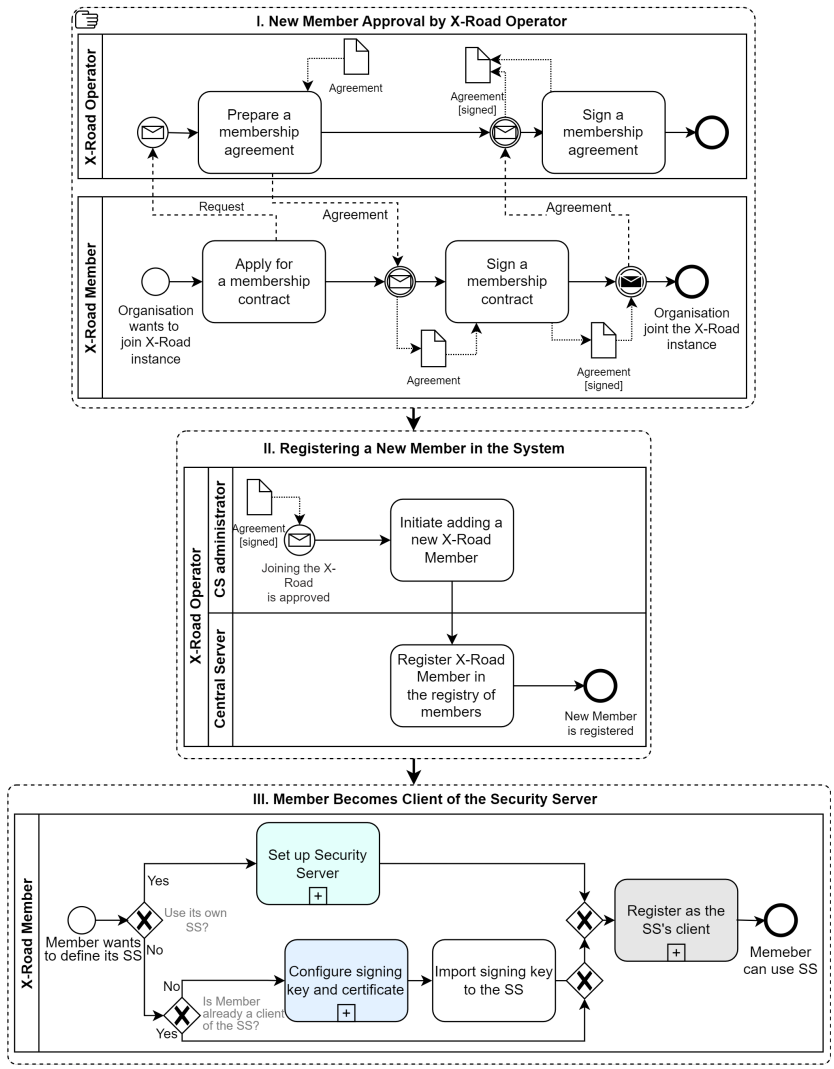


Figure 51: Process of Member Onboarding

The sub-processes of onboarding are presented in detail further. Figure 52 describes the processes of setting up a new Security Server.

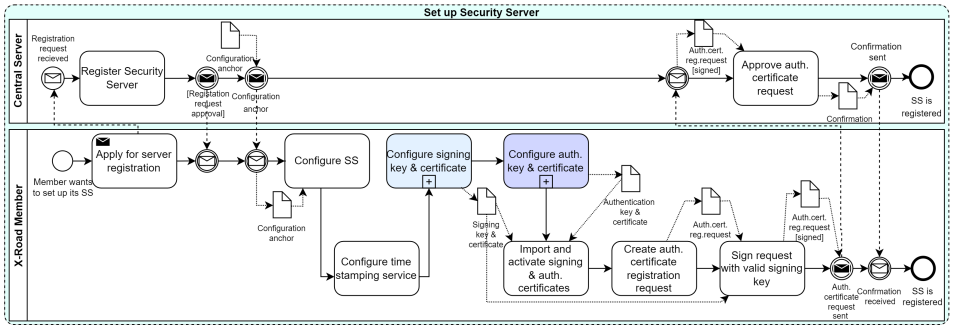


Figure 52: Process of setting up a Security Server [131]

Figure 53 and 54 describe the procedure of obtaining signing and authentication certificates by the respective identities.

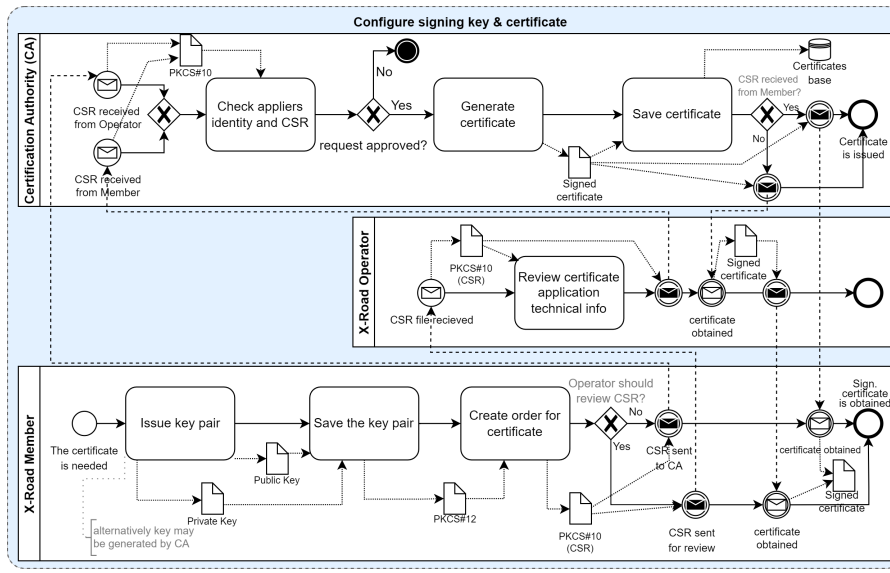


Figure 53: Process of configuring a signing key and certificate [131]

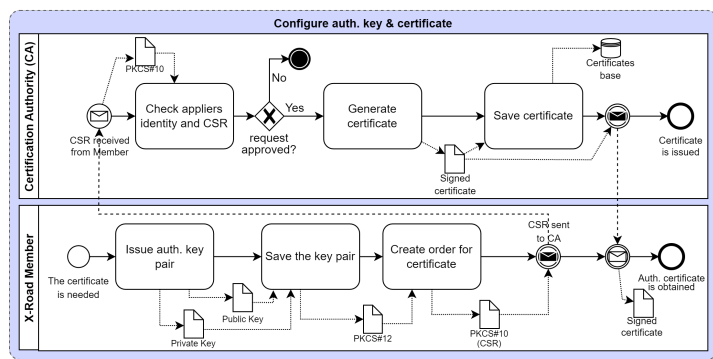


Figure 54: Process of configuring an authentication key and certificate

Figure 55 concludes the Member's onboarding by becoming a client of the selected Security Server.

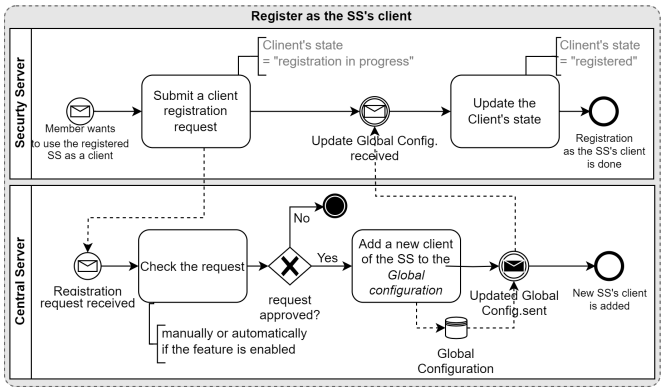


Figure 55: Process of registering as a Security Server client

D.2. DPKI-based IdM System in X-Road

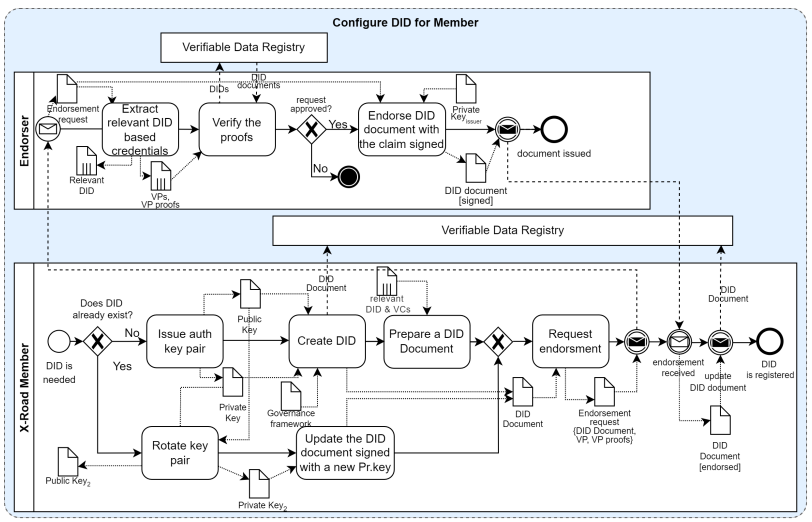


Figure 56: Process of configuring a DID for a Member

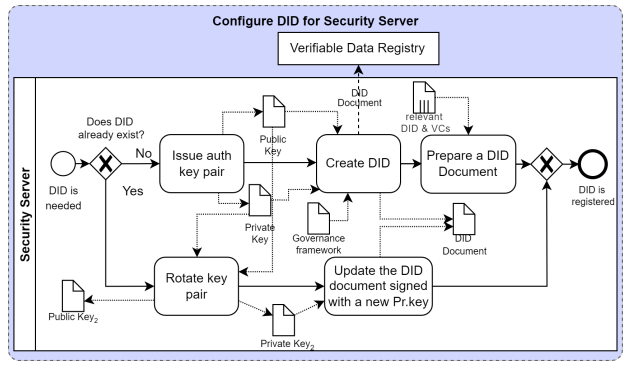
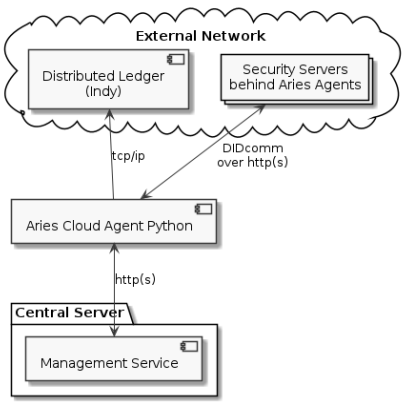
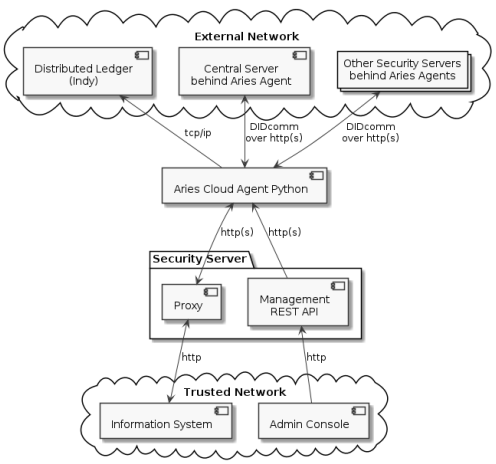


Figure 57: Process of configuring a DID for a Member



(a) Central Server in DPKI PoC [215]



(b) Security Server in DPKI PoC [215]

Figure 58: Components and interfaces of the modified DPKI-based PoC X-Road

ACKNOWLEDGEMENTS

First and foremost, I extend my gratitude to my supervisor, Raimundas Matulevičius, for his unwavering support and guidance throughout our five-year collaboration. I am truly fortunate to have had Raimundas's mentorship from the time of my master's research until the completion of my PhD. He provided the perfect balance of being strict and humorous, giving flexibility and direction, allowing me to explore my own research interests while keeping me on track. I am deeply grateful for his belief in me, his constructive criticism, and his insistence on publication deadlines, which pushed me to strive for excellence and not to lose focus.

I am grateful to the external reviewers, Siv Hilde Houmb and Manfred A. Jeusfeld, and the internal reviewer, Mohamad Gharib, for taking the time to read my thesis and provide constructive feedback. Their comments helped me ensure the consistency of the thesis and challenged me to strengthen my work.

I would like to thank my co-authors Jan, Petr, Petteri, Ahmed, and Lukaš and my supervisees Jason and Sander for their contribution to my research and nice collaboration experience. I am grateful to Mari Seeba, Tarmo Oja and all the members of the InfoSec team for their insightful feedback, thought-provoking discussions, and fresh perspectives, which enhanced my critical thinking skills throughout my research career. I am grateful to all my colleagues at the Institute of Computer Science for the interesting conversations and inspiring stories shared in the Delta corridors. Their stories of successes and failures helped me not to give up and stay motivated throughout the journey.

I would like to thank Taavi, Novin, Mari-Liis, Marharyta, Slava and all the other PhD events co-organisers for making the events together. These events were a way of self-expression and made the PhD studies period easier thanks to having the purpose of strengthening the ICS community.

A special thanks to my friends Kateryna and Marharyta, who were constant companions during the ups and downs of our PhD experiences. Their friendly shoulder support and understanding were invaluable.

I am grateful for the many travels, conversations and events I had over PhD study years. I would like to acknowledge Petr Švenda, Vashek Matyáš and Lukaš Malina for their warm hospitality during my visits to Masaryk University and Brno University of Technology in Brno, Czechia.

On a personal note, I would like to thank my parents, grandparents, and brother Ivan for their unwavering support and encouragement. I am eternally grateful to my life partner, Stanislav, for his love, patience, and belief in me. And of course, I thank him for supplying me with a daily dose of high-quality TV series, movies and jokes, which were so much needed for my mental health.

Finally, I want to acknowledge the supportive role of music in my research life. The soothing sounds of Ludovico Einaudi and the calming melodies of rainforest bird songs helped me stay focused and calm during dark Estonian winters throughout these years.

Note on the use of tools in the writing of this thesis. I acknowledge the use of Large Language Models (LLMs) for text rephrasing and grammar correction during the thesis manuscript preparation. The following tools were used in the writing process of this thesis: ChatGPT (models 3.5 and 4)[23], Gemini[24], and Grammarly[25].

The degree study has been financially supported by the European Union under Grant Agreement No. 101087529.

[23] `https://chatgpt.com/`
[24] `https://gemini.google.com/`
[25] `https://app.grammarly.com/`

SISUKOKKUVÕTE

Infoturbe ja privaatsuse haldamise meetod nutilahendustes

Tänapäeval on kodanike jaoks nutisüsteemide arendamine hoogustunud. Sellised nutisüsteemid on tavaliselt lisatud juba olemasolevatele eraldiseisvatele infosüsteemidele, millel on eelseadistatud turva- ja privaatsuse meetmed. Ometi peaks organisatsioon süsteemi integreerimisel väliste süsteemidega tagama turvalisuse uues kontekstis. Sel põhjusel peaks organisatsioon kontrollima, kas uuenenud äriprotsess, andmevood ja turvameetmed vastavad uue nutisüsteemi lahenduse turva- ja privaatsusnõuetele. Eeldame, et selle ülesande jaoks peaks organisatsioon kokku panema ajutise ekspertgrupi, et analüüsida muutusi, mis põhinevad uutel süsteemi koostöösuhetel.

Olemasolevad infoturbe- ja privaatsusraamistikud on peamiselt keskendunud turvalisuse tagamiseks kõrgtaseme haldustegevusele. Siiski ei keskendu nad organisatsiooniülese koostöö mõjule. Seetõttu võtsime siinse lõputöös eesmärgiks uurida, milline on sellise koostöö mõju infoturbele ja privaatsusele. Täpsemalt keskendusime tehniliste ja organisatsiooniliste meetmete valimisele, mis aitaksid tagada turvalise andmevahetuse väliste üksustega. Käesolevas lõputöös käsitleti peamise uurimisküsimusena: kuidas toetada ekspertgruppi nutilahenduse organisatsiooniülese koostöö mõju infoturbe ja privaatsuse hindamisel?

Peamisele uurimisküsimusele vastamiseks kasutasime disainiteaduslikku uurimismeetodit. Uurimistöö tulemusena valmis meetod infoturbe ja privaatsuse haldamiseks nutikates lahendustes. Meetod koosneb kolmest astmest, millest igaüks esindab käesoleva väitekirja eraldi tööpanust.

Tööpanus 1. Olemasolevad infoturbe- ja privaatsusraamistikud ning -mudelid keskenduvad sageli kõrgtaseme turbehaldusele või konkreetsetele turvameetmetele. Kuigi on olemas arvukalt suuniseid ja standardeid, puuduvad neil sageli juhised praktiliseks rakendamiseks. Selle probleemi lahendamiseks töötasime välja FISP-ProCOP raamistiku infoturbe ja privaatsuse haldamiseks. FISP-ProCOP on maatriksipõhine raamistik, mida saab kasutada mudeli või mallina organisatsiooni infoturbe ja privaatsuse haldamise hindamiseks. Raamistik keskendub neljale võtmedimensioonile: protsessid, meetmed, organisatsioon ja inimesed. Iga dimensioon sisaldab kategooriaid ja atribuute, mida saab kohandada konkreetsetele nutisüsteemi kontekstidele. Raamistikku valideerisime kahe juhtumiuuringuga liikluse nutisüsteemide valdkonnas.

Tööpanus 2. Privaatsuse tagamise tõendamiseks töötasime välja tööriistadega toetatud meetodi, mis kasutab ELi andmekaitse regulatsiooni nõuetele vastavaid ja privaatsust edendavaid tehnoloogilisi analüüsi vahendeid. See meetod aitab tuvastada privaatsuse rikkumisi ning annab soovitusi minimaalsetele protsessi ja süsteemi kohandusvajadustele. Eeldades, et ekspertgrupp on määratlenud äriprotsessi mudelid, kasutab meetod avatud lähtekoodiga tööriistu nagu DPO ja Pleak, et analüüsida privaatsusnõudeid ja hinnata tehnoloogia privaatsuskaitse efektiiv-

sust. Me valideerisime meetodit kahe liikluse nutisüsteemi juhtumiuuringu abil: autonoomne sõidukipõhine sõidujagamissüsteem ja nutikas parkimislahendus.

Tööpanus 3 ja 4. Et aidata organisatsioonidel mõista usaldusmudelite mõju turvalisusele ja privaatsusele organisatsiooniülestes nutilahendustes, töötasime välja kaks identiteedihaldussüsteemi kujundust. Kujundusi hinnatakse IdM-süsteemi kvaliteedi hindamise mudeliga, mis põhineb Cameroni digitaalse identiteedi seadustel ning keskendub turvalisusele, kontrollile, kasutatavusele ja hooldatavusele. Välja töötatud disainilahendused võimaldavad nutikaid süsteeme, mis on lubatud X-tee andmevahetussüsteemiga. Kujunduste hindamisel selgus, et optimaalne usaldus- ja identiteedimudeli valik sõltub konkreetsetest organisatsioonilistest eesmärkidest ja soovitud süsteemi omadustest. Igal läbi vaadatud usaldusmudelil – detsentraliseeritud ja hajutatudmudelil – on oma eelised ja puudused. Detsentraliseeritud mudel on osutunud organisatsioonide jaoks ebapraktiliseks infrastruktuuri ja juhtimise keerukuse tõttu. Praktilisem alternatiiv täielikult tsentraliseeritud PKI-põhisele süsteemile on hajutatud usaldusega tsentraliseeritud IdM, mis pakub tasakaalu detsentraliseerimise, usalduse minimeerimise ja vähenenud keerukuse vahel.

Kokkuvõtvalt võib öelda, et kirjeldatud meetod aitab andmekaitseametnikke, infoturbeametnikke, ärianalüütikuid ja turvaarhitekte turvalisuse ja privaatsuse tagamise koordineerimisel. See uurimus annab organisatsioonidele võimaluse tugevdada turvalisust, kaitsta tundlikke andmeid ja järgida õiguslike regulatsioonide vastavust.

CURRICULUM VITAE

Personal data

Name:	Mariia Bakhtina
Date of Birth:	19.06.1997
Citizenship:	Ukraine
E-mail:	mariia.bakhtina@ut.ee
ORCID:	0000-0002-0940-9713

Education

2021–2025	PhD in Computer Science, University of Tartu, Estonia
2019–2021	MA in Innovation and Technology Management (*cum laude*), University of Tartu, Estonia
2014–2018	BSc in System Analysis, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Ukraine

Employment

2021–2025	Junior Research Fellow in Information Security, University of Tartu, Estonia
2018–2019	Junior AX Developer, SMART Business, Ukraine

Teaching

Spring 2022-2024	Principles of Secure Software Design (teaching assistant)
Spring 2022	Human-Computer Interaction (teaching assistant)
Fall 2021-2023	Requirements Engineering (teaching assistant)

Scientific work

Main fields of interest:

- information security management
- identity management
- information systems

ELULOOKIRJELDUS

Isikuandmed

Nimi:	Mariia Bakhtina
Sünniaeg:	19.06.1997
Kodakondsus:	Ukraina
E-post:	mariia.bakhtina@ut.ee
ORCID:	0000-0002-0940-9713

Haridus

2021–2025	PhD informaatikas, Tartu Ülikool, Eesti
2019–2021	MA innovatsiooni ja tehnoloogia juhtimises (*cum laude*), Tartu Ülikool, Eesti
2014–2018	BSc süsteemianalüüsis, Ukraina Riiklik Tehnikaülikool "Igor Sikorsky Kiiev Polütehniline Instituut", Ukraina

Teenistuskäik

2021–2025	Infoturbe nooremteadur, Tartu Ülikool, Eesti
2018–2019	Noorem AX arendaja, SMART Business, Ukraina

Õppetöö

Kevad 2022-2024	Turvalise tarkvaradisaini põhimõtted (õppeassistent)
Kevad 2022	Inimese ja arvuti interaktsioon (õppeassistent)
Sügis 2021-2023	Nõuete analüüs (õppeassistent)

Teadustegevus

Peamised uurimisvaldkonnad:

- infoturbe juhtimine
- identiteedihaldus
- infosüsteemid

DISSERTATIONES INFORMATICAE PREVIOUSLY PUBLISHED IN DISSERTATIONES MATHEMATICAE UNIVERSITATIS TARTUENSIS

19. **Helger Lipmaa.** Secure and efficient time-stamping systems. Tartu, 1999, 56 p.
22. **Kaili Müürisep.** Eesti keele arvutigrammatika: süntaks. Tartu, 2000, 107 lk.
23. **Varmo Vene.** Categorical programming with inductive and coinductive types. Tartu, 2000, 116 p.
24. **Olga Sokratova.** Ω-rings, their flat and projective acts with some applications. Tartu, 2000, 120 p.
27. **Tiina Puolakainen.** Eesti keele arvutigrammatika: morfoloogiline ühestamine. Tartu, 2001, 138 lk.
29. **Jan Villemson.** Size-efficient interval time stamps. Tartu, 2002, 82 p.
45. **Kristo Heero.** Path planning and learning strategies for mobile robots in dynamic partially unknown environments. Tartu 2006, 123 p.
49. **Härmel Nestra.** Iteratively defined transfinite trace semantics and program slicing with respect to them. Tartu 2006, 116 p.
53. **Marina Issakova.** Solving of linear equations, linear inequalities and systems of linear equations in interactive learning environment. Tartu 2007, 170 p.
55. **Kaarel Kaljurand.** Attempto controlled English as a Semantic Web language. Tartu 2007, 162 p.
56. **Mart Anton.** Mechanical modeling of IPMC actuators at large deformations. Tartu 2008, 123 p.
59. **Reimo Palm.** Numerical Comparison of Regularization Algorithms for Solving Ill-Posed Problems. Tartu 2010, 105 p.
61. **Jüri Reimand.** Functional analysis of gene lists, networks and regulatory systems. Tartu 2010, 153 p.
62. **Ahti Peder.** Superpositional Graphs and Finding the Description of Structure by Counting Method. Tartu 2010, 87 p.
64. **Vesal Vojdani.** Static Data Race Analysis of Heap-Manipulating C Programs. Tartu 2010, 137 p.
66. **Mark Fišel.** Optimizing Statistical Machine Translation via Input Modification. Tartu 2011, 104 p.
67. **Margus Niitsoo**. Black-box Oracle Separation Techniques with Applications in Time-stamping. Tartu 2011, 174 p.
71. **Siim Karus.** Maintainability of XML Transformations. Tartu 2011, 142 p.
72. **Margus Treumuth.** A Framework for Asynchronous Dialogue Systems: Concepts, Issues and Design Aspects. Tartu 2011, 95 p.
73. **Dmitri Lepp.** Solving simplification problems in the domain of exponents, monomials and polynomials in interactive learning environment T-algebra. Tartu 2011, 202 p.

74. **Meelis Kull.** Statistical enrichment analysis in algorithms for studying gene regulation. Tartu 2011, 151 p.
77. **Bingsheng Zhang.** Efficient cryptographic protocols for secure and private remote databases. Tartu 2011, 206 p.
78. **Reina Uba.** Merging business process models. Tartu 2011, 166 p.
79. **Uuno Puus.** Structural performance as a success factor in software development projects – Estonian experience. Tartu 2012, 106 p.
81. **Georg Singer.** Web search engines and complex information needs. Tartu 2012, 218 p.
83. **Dan Bogdanov.** Sharemind: programmable secure computations with practical applications. Tartu 2013, 191 p.
84. **Jevgeni Kabanov.** Towards a more productive Java EE ecosystem. Tartu 2013, 151 p.
87. **Margus Freudenthal.** Simpl: A toolkit for Domain-Specific Language development in enterprise information systems. Tartu, 2013, 151 p.
90. **Raivo Kolde.** Methods for re-using public gene expression data. Tartu, 2014, 121 p.
91. **Vladimir Šor.** Statistical Approach for Memory Leak Detection in Java Applications. Tartu, 2014, 155 p.
92. **Naved Ahmed.** Deriving Security Requirements from Business Process Models. Tartu, 2014, 171 p.
94. **Liina Kamm.** Privacy-preserving statistical analysis using secure multi-party computation. Tartu, 2015, 201 p.
100. **Abel Armas Cervantes.** Diagnosing Behavioral Differences between Business Process Models. Tartu, 2015, 193 p.
101. **Fredrik Milani.** On Sub-Processes, Process Variation and their Interplay: An Integrated Divide-and-Conquer Method for Modeling Business Processes with Variation. Tartu, 2015, 164 p.
102. **Huber Raul Flores Macario.** Service-Oriented and Evidence-aware Mobile Cloud Computing. Tartu, 2015, 163 p.
103. **Tauno Metsalu.** Statistical analysis of multivariate data in bioinformatics. Tartu, 2016, 197 p.
104. **Riivo Talviste.** Applying Secure Multi-party Computation in Practice. Tartu, 2016, 144 p.
108. **Siim Orasmaa.** Explorations of the Problem of Broad-coverage and General Domain Event Analysis: The Estonian Experience. Tartu, 2016, 186 p.
109. **Prastudy Mungkas Fauzi.** Efficient Non-interactive Zero-knowledge Protocols in the CRS Model. Tartu, 2017, 193 p.
110. **Pelle Jakovits.** Adapting Scientific Computing Algorithms to Distributed Computing Frameworks. Tartu, 2017, 168 p.
111. **Anna Leontjeva.** Using Generative Models to Combine Static and Sequential Features for Classification. Tartu, 2017, 167 p.
112. **Mozhgan Pourmoradnasseri.** Some Problems Related to Extensions of Polytopes. Tartu, 2017, 168 p.

113. **Jaak Randmets.** Programming Languages for Secure Multi-party Computation Application Development. Tartu, 2017, 172 p.
114. **Alisa Pankova.** Efficient Multiparty Computation Secure against Covert and Active Adversaries. Tartu, 2017, 316 p.
116. **Toomas Saarsen.** On the Structure and Use of Process Models and Their Interplay. Tartu, 2017, 123 p.
121. **Kristjan Korjus.** Analyzing EEG Data and Improving Data Partitioning for Machine Learning Algorithms. Tartu, 2017, 106 p.
122. **Eno Tõnisson.** Differences between Expected Answers and the Answers Offered by Computer Algebra Systems to School Mathematics Equations. Tartu, 2017, 195 p.

DISSERTATIONES INFORMATICAE UNIVERSITATIS TARTUENSIS

1. **Abdullah Makkeh**. Applications of Optimization in Some Complex Systems. Tartu 2018, 179 p.
2. **Riivo Kikas**. Analysis of Issue and Dependency Management in Open-Source Software Projects. Tartu 2018, 115 p.
3. **Ehsan Ebrahimi**. Post-Quantum Security in the Presence of Superposition Queries. Tartu 2018, 200 p.
4. **Ilya Verenich**. Explainable Predictive Monitoring of Temporal Measures of Business Processes. Tartu 2019, 151 p.
5. **Yauhen Yakimenka**. Failure Structures of Message-Passing Algorithms in Erasure Decoding and Compressed Sensing. Tartu 2019, 134 p.
6. **Irene Teinemaa**. Predictive and Prescriptive Monitoring of Business Process Outcomes. Tartu 2019, 196 p.
7. **Mohan Liyanage.** A Framework for Mobile Web of Things. Tartu 2019, 131 p.
8. **Toomas Krips.** Improving performance of secure real-number operations. Tartu 2019, 146 p.
9. **Vijayachitra Modhukur.** Profiling of DNA methylation patterns as biomarkers of human disease. Tartu 2019, 134 p.
10. **Elena Sügis.** Integration Methods for Heterogeneous Biological Data. Tartu 2019, 250 p.
11. **Tõnis Tasa.** Bioinformatics Approaches in Personalised Pharmacotherapy. Tartu 2019, 150 p.
12. **Sulev Reisberg.** Developing Computational Solutions for Personalized Medicine. Tartu 2019, 126 p.
13. **Huishi Yin.** Using a Kano-like Model to Facilitate Open Innovation in Requirements Engineering. Tartu 2019, 129 p.
14. **Faiz Ali Shah.** Extracting Information from App Reviews to Facilitate Software Development Activities. Tartu 2020, 149 p.
15. **Adriano Augusto**. Accurate and Efficient Discovery of Process Models from Event Logs. Tartu 2020, 194 p.
16. **Karim Baghery.** Reducing Trust and Improving Security in zk-SNARKs and Commitments. Tartu 2020, 245 p.
17. **Behzad Abdolmaleki.** On Succinct Non-Interactive Zero-Knowledge Protocols Under Weaker Trust Assumptions. Tartu 2020, 209 p.
18. **Janno Siim.** Non-Interactive Shuffle Arguments. Tartu 2020, 154 p.
19. **Ilya Kuzovkin.** Understanding Information Processing in Human Brain by Interpreting Machine Learning Models. Tartu 2020, 149 p.
20. **Orlenys López Pintado.** Collaborative Business Process Execution on the Blockchain: The Caterpillar System. Tartu 2020, 170 p.
21. **Ardi Tampuu.** Neural Networks for Analyzing Biological Data. Tartu 2020, 152 p.

22. **Madis Vasser.** Testing a Computational Theory of Brain Functioning with Virtual Reality. Tartu 2020, 106 p.
23. **Ljubov Jaanuska.** Haar Wavelet Method for Vibration Analysis of Beams and Parameter Quantification. Tartu 2021, 192 p.
24. **Arnis Parsovs.** Estonian Electronic Identity Card and its Security Challenges. Tartu 2021, 214 p.
25. **Kaido Lepik.** Inferring causality between transcriptome and complex traits. Tartu 2021, 224 p.
26. **Tauno Palts.** A Model for Assessing Computational Thinking Skills. Tartu 2021, 134 p.
27. **Liis Kolberg.** Developing and applying bioinformatics tools for gene expression data interpretation. Tartu 2021, 195 p.
28. **Dmytro Fishman.** Developing a data analysis pipeline for automated protein profiling in immunology. Tartu 2021, 155 p.
29. **Ivo Kubjas.** Algebraic Approaches to Problems Arising in Decentralized Systems. Tartu 2021, 120 p.
30. **Hina Anwar.** Towards Greener Software Engineering Using Software Analytics. Tartu 2021, 186 p.
31. **Veronika Plotnikova.** FIN-DM: A Data Mining Process for the Financial Services. Tartu 2021, 197 p.
32. **Manuel Camargo.** Automated Discovery of Business Process Simulation Models From Event Logs: A Hybrid Process Mining and Deep Learning Approach. Tartu 2021, 130 p.
33. **Volodymyr Leno.** Robotic Process Mining: Accelerating the Adoption of Robotic Process Automation. Tartu 2021, 119 p.
34. **Kristjan Krips.** Privacy and Coercion-Resistance in Voting. Tartu 2022, 173 p.
35. **Elizaveta Yankovskaya.** Quality Estimation through Attention. Tartu 2022, 115 p.
36. **Mubashar Iqbal.** Reference Framework for Managing Security Risks Using Blockchain. Tartu 2022, 203 p.
37. **Jakob Mass.** Process Management for Internet of Mobile Things. Tartu 2022, 151 p.
38. **Gamal Elkoumy.** Privacy-Enhancing Technologies for Business Process Mining. Tartu 2022, 135 p.
39. **Lidia Feklistova.** Learners of an Introductory Programming MOOC: Background Variables, Engagement Patterns and Performance. Tartu 2022, 151 p.
40. **Mohamed Ragab.** Bench-Ranking: A Prescriptive Analysis Approach for Large Knowledge Graphs Query Workloads. Tartu 2022, 158 p.
41. **Mohammad Anagreh.** Privacy-Preserving Parallel Computations for Graph Problems. Tartu 2023, 181 p.
42. **Rahul Goel.** Mining Social Well-being Using Mobile Data. Tartu 2023, 104 p.
43. **Anti Ingel.** Algorithms using information theory: classification in brain-computer interfaces and characterising reinforcement-learning agents. Tartu 2023, 142 p.

44. **Shakshi Sharma.** Fighting Misinformation in the Digital Age: A Comprehensive Strategy for Characterizing, Identifying, and Mitigating Misinformation on Online Social Media Platforms. Tartu 2023, 158 p.
45. **Kristiina Rahkema.** Quality Analysis of iOS Applications with Focus on Maintainability and Security Aspects. Tartu 2023, 182 p.
46. **Ivan Slobozhan.** Studying Online Social Media Engagement in CIS Countries during Protests, Mass Demonstrations and War. Tartu 2023, 81 p.
47. **Nurlan Kerimov.** Building a catalogue of molecular quantitative trait loci to interpret complex trait associations. Tartu 2023, 248 p.
48. **Pavlo Tertychnyi.** Machine Learning Methods for Anti-Money Laundering Monitoring. Tartu 2023, 117 p.
49. **Abasi-amefon Obot Affia.** A Framework and Teaching Approach for IoT Security Risk Management. Tartu 2023, 180 p.
50. **Raimond-Hendrik Tunnel.** Video Game Design and Development Bachelor's Curriculum for Estonia. Tartu 2024, 137 p.
51. **Ahto Salumets.** Bioinformatics analysis of various aspects in immunology. Tartu 2024, 198 p.
52. **Mohammed Abdulhameed Shaif Ali.** Deep Learning Methods for Cell Microscopy Image Analysis. Tartu 2024, 143 p.
53. **Pille Pullonen-Raudvere**. Foundations of Efficient and Secure Algorithm Development for Secure Multiparty Computation. Tartu 2024, 265 p.
54. **Marili Rõõm.** Multiple approaches to learners' success and factors affecting it in computer programming MOOCs. Tartu 2024, 170 p.
55. **Shivananda Rangappa Poojara.** Design and Orchestration of Scalable, Event-Driven Serverless Data Pipelines for Internet of Things (IoT) Applications. Tartu 2024, 172 p.
56. **Hassan Abdulgaleel Hassan Salim Eldeeb.** Empowering Machine Learning Pipelines with Automated Feature Engineering. Tartu 2024, 121 p.
57. **Muhammad Uzair.** Soft decision making for agri-food 4.0. Tartu 2024, 158 p.
58. **Kirill Milintsevich.** Estimation of Depression Level from Text: Symptom-Based Approach, External Knowledge, Dataset Validity. Tartu 2024, 130 p.
59. **Maksym Del.** Multilingual and Multi-Domain Representational Patterns Across Trpansformer-Based Models. Tartu 2024, 131 p.
60. **Kristo Raun.** Adaptive Out-of-order Handling in Streaming Conformance Checking. Tartu 2024, 118 p.
61. **Toivo Vajakas.** Towards integration of mobile network data into analyzing human mobility. Tartu 2024, 103 p.
62. **Katsiaryna Lashkevich.** Data-Driven Analysis and Optimization of Waiting Times in Business Processes. Tartu 2024, 169 p.
63. **Alejandra Duque-Torres.** Classifying, Constraining and Ranking Metamorphic Relations. Tartu 2025, 159 p.