A Method for Information Security and Privacy Management in Smart Solutions

Mariia Bakhtina

Junior Research Fellow in Information Security, PhD student

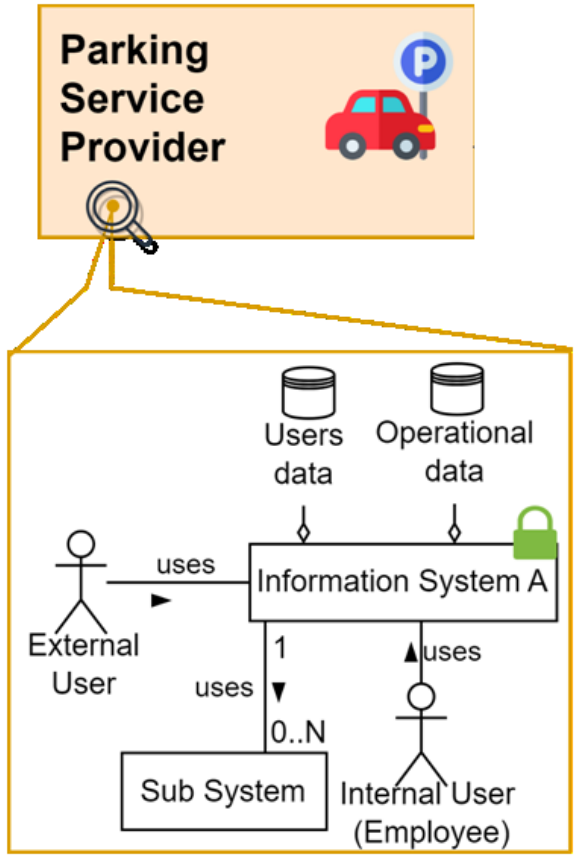
About Me

- BSc in System Analysis,
  - National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Ukraine (2014 – 2018)
- Junior AX Developer,
  - SMART Business, Ukraine (2018 – 2019)
- MA in Innovation and Technology Management,
  - University of Tartu, Estonia (2019 – 2021)
- PhD in Computer Science,
  - University of Tartu, Estonia (2021 – Present)

PhD research project

“A Method for Information Security and Privacy Management in Smart Solutions”

Smart Parking Solution



Transport Administration Agency

Parking enforcement agency

Motivation Scenario

An expert group aims to update the business processes and systems
to ensure information security and privacy
of a collaborative data exchange
as a part of a smart solution (e.g., smart parking).

The expert group consists of:

- a data protection officer (DPO),
- a chief information security officer (CISO),
- a business analyst,
- a security architect

How to support an expert group

in ensuring information security and privacy

of cross-organisational data exchange

for a smart solution?

Open Problems

Frameworks and models for information security and privacy are **too abstract** and aim to guide info. sec. mgmt activities, not depict the state

- Objective 1: develop a framework for information security and privacy management to enable defining the static current state

High-level requirements guiding the need for **privacy analysis** and assurance w.r.t. GDPR & ISO/IEC 27001

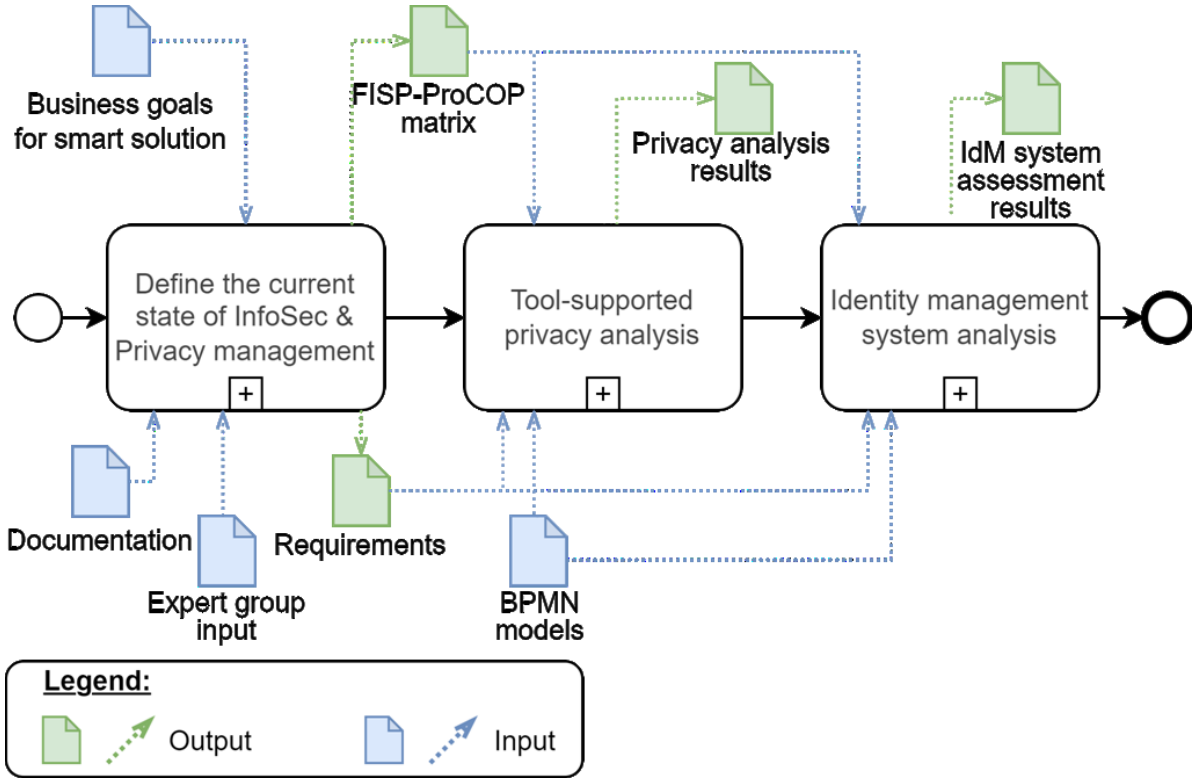
- Objective 2: develop a method for privacy analysis of collaborative business processes to enable defining and fulfilling local data protection regulations

Emerging **alternative trust and identity models** are not researched for the organisational context

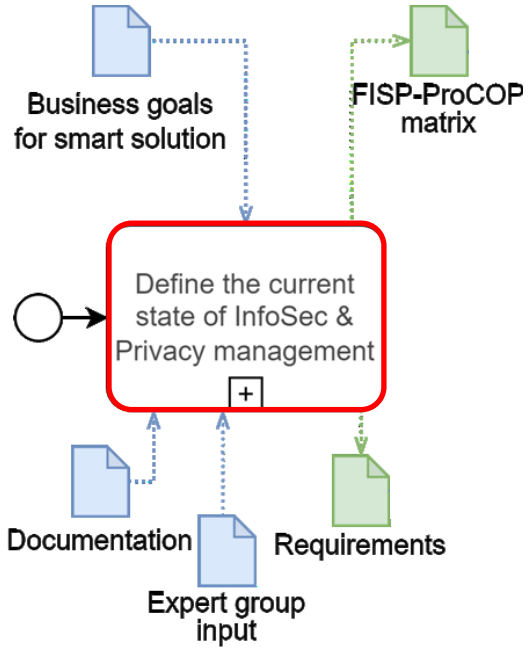
- Objective 3: develop a method for trust and identity model selection

Results (1/4)

The final method for information security and privacy management of cross-organisational collaboration



Results (2/4)


Business goals for smart solution
FISP-ProCOP matrix
Define the current state of InfoSec & Privacy management
+
Documentation
Expert group input
Requirements

Results (2/4): FISP-ProCOP

Step 1

Framework for Information Security and Privacy Management -- *FISP-ProCOP* -- for depicting the static view of information security and privacy management in organisations

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

The usability of FISP-ProCOP has been validated with respect to:

- a tool for current InfoSec & Privacy management state definition
- a tool for cross-validating the usage of measures within the organisation
- a tool for comparing InfoSec & Privacy management states

[1] Mariia Bakhtina, Raimundas Matulevičius, and Lukaš Malina. "*Information Security and Privacy Management in Intelligent Transportation Systems*".

FISP-ProCOP

Validation:

- Literature review of measures (24 papers) -> Targeted state (To-Be)
- Survey of organisations (15 organisations) -> Current state (As-Is)

[1] Mariia Bakhtina, Raimundas Matulevičius, and Lukaš Malina. "*Information Security and Privacy Management in Intelligent Transportation Systems*".

FISP-ProCOP

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							

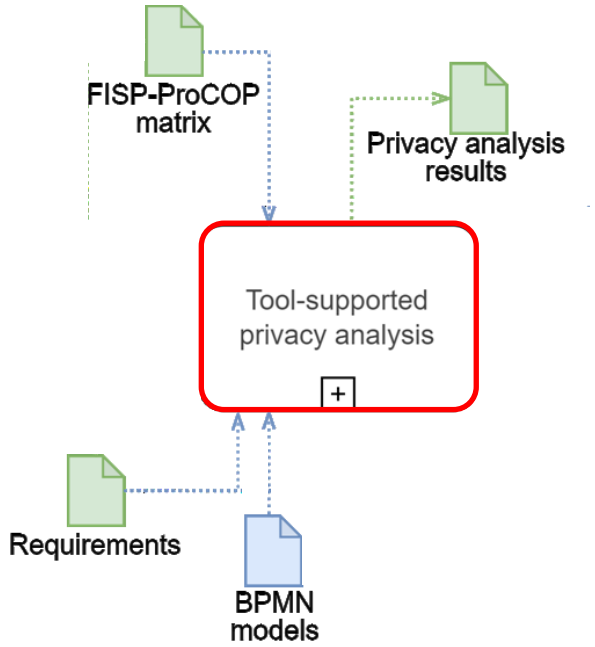
Cell colour mapping: 0 | 3 | 6 | 14 (by number of supporting responses)

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

- a tool for cross-validating the usage of measures within the organisation
- a tool for comparing InfoSec & Privacy management states - As-Is vs To-Be (e.g., from standard)

[1] Mariia Bakhtina, Raimundas Matulevičius, and Lukaš Malina. "*Information Security and Privacy Management in Intelligent Transportation Systems*".

Results (3/4)

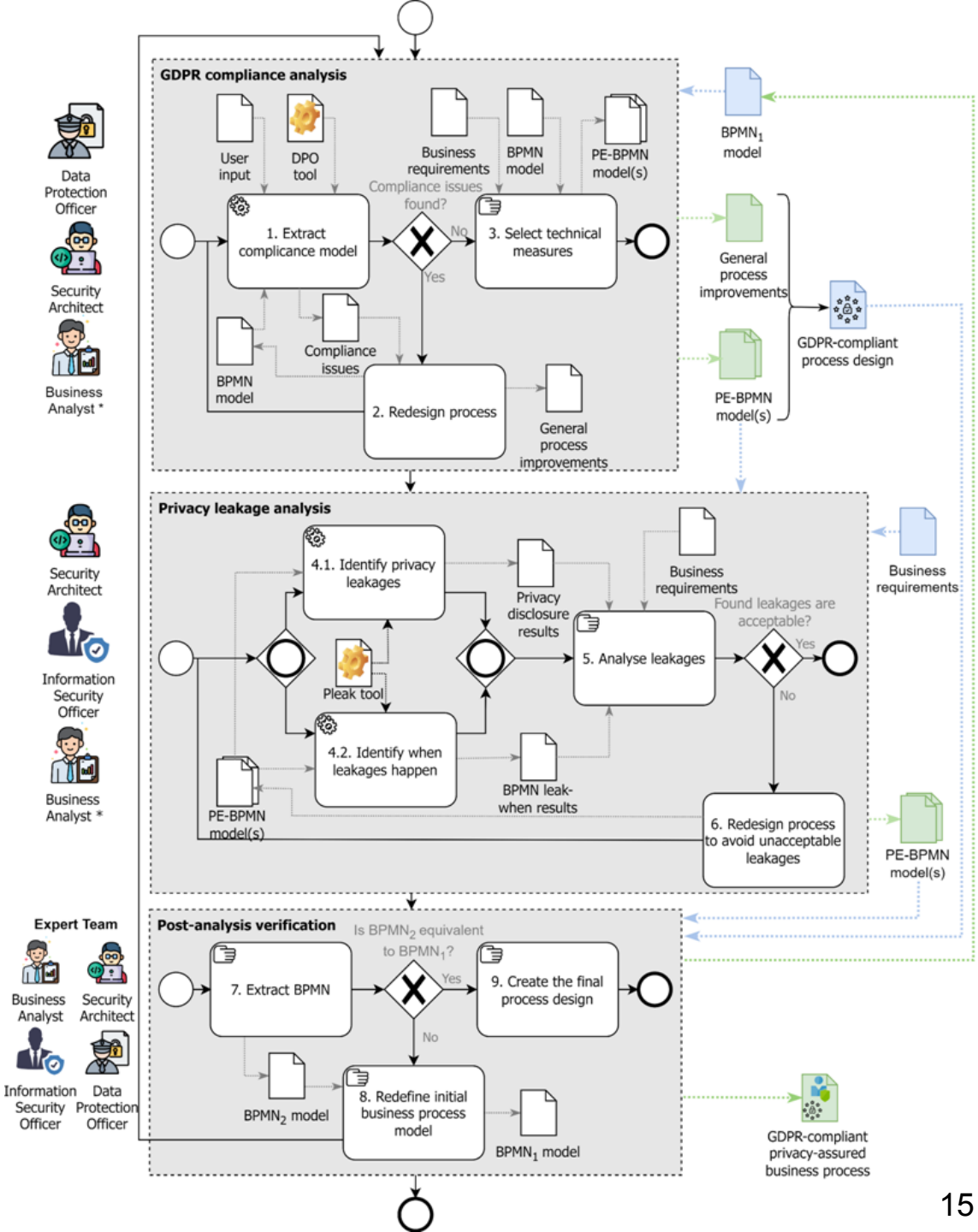

FISP-ProCOP matrix
Privacy analysis results
Tool-supported privacy analysis
Requirements
BPMN models

Results (3/4)

Step 2

The *tool-supported privacy analysis method* proved to:

- support the elicitation of requirements to the information system to comply with GDPR
- support the selection of technical measures for privacy assurance



[2] Mariia Bakhtina, Raimundas Matulevičius, and Mari Seeba. "Tool-supported method for privacy analysis of a business process model".
[6] Sander Truu. 2024. "Tool-Supported Privacy Analysis of Smart Parking". BSc thesis.

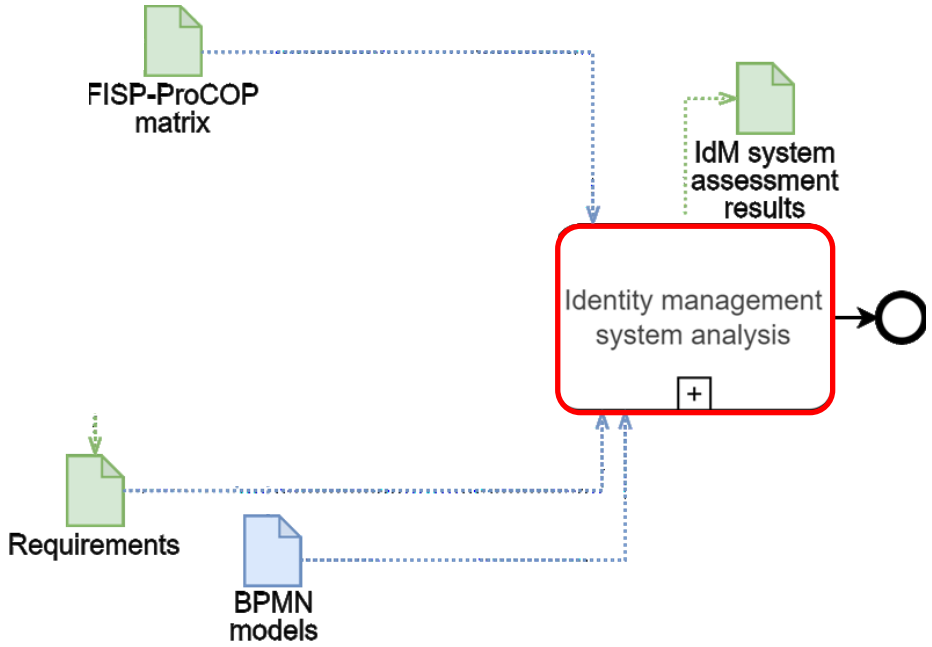
Tool-supported privacy analysis

Validation:

- Scenario 1: Autonomous Vehicle usage for ride-hailing
- Scenario 2: Smart parking

[2] Mariia Bakhtina, Raimundas Matulevičius, and Mari Seeba. “Tool-supported method for privacy analysis of a business process model”.
[6] Sander Truu. 2024. “Tool-Supported Privacy Analysis of Smart Parking”. BSc thesis.

Results (4/4)


FISP-ProCOP matrix
IdM system assessment results
Identity management system analysis
+
Requirements
BPMN models

Results (4/4)

Step 3

Comparison of 3 identity management models in the selected data exchange systems

- The selection of trust and identity models is defined by the business objectives and the required IdM system qualities

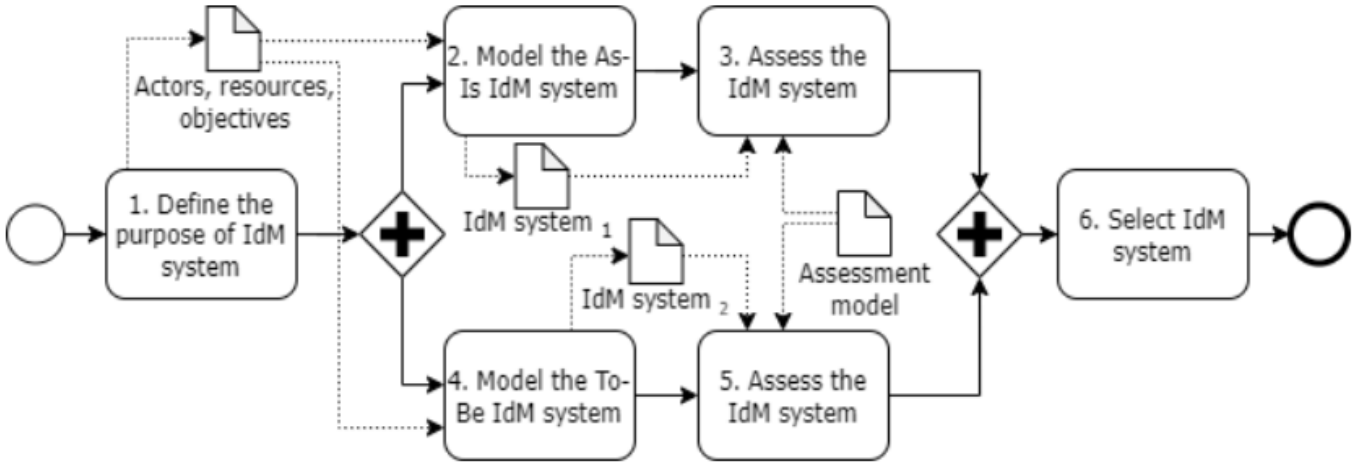


Figure 11: Method for identity management system analysis

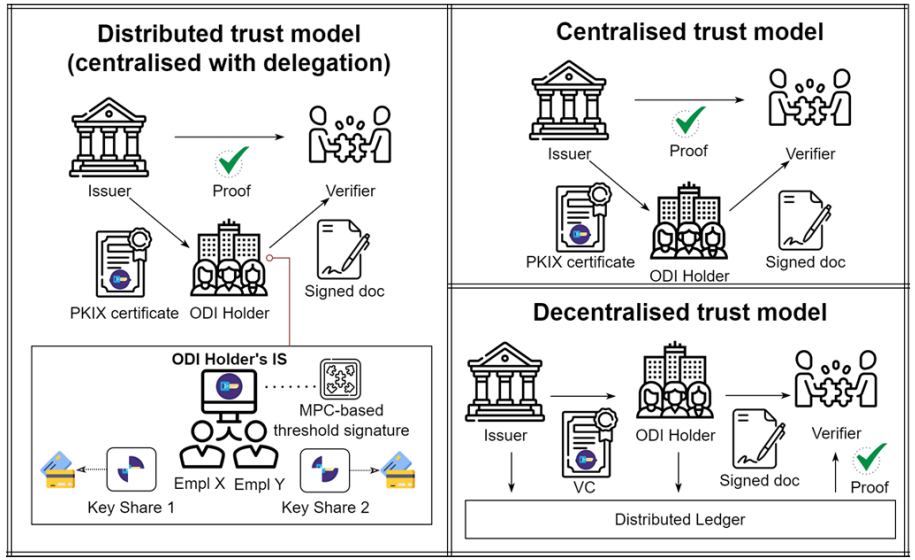
Quality criteria	Quality sub-criteria	Indicators	How to measure
Security	**Preventing insider threat**	Fact of having built in prevention mechanism	Yes / No
	Decentralisation	Decentralisation of credentials issuance/verification	Yes / No
		Decentralisation of credentials and keys management	Yes / No
	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

[3] Bakhtina et al. "On the Shift to Decentralised Identity Management in Distributed Data Exchange Systems."
[4] Mariia Bakhtina et al. "A Decentralised Public Key Infrastructure for X-Road".
[5] Mariia Bakhtina, Jan Kvapil, Petr Švenda, and Raimundas Matulevičius. "The Power of Many: Securing Organisational Identity Through Distributed Key Management".

Results (4/4)

Comparison of 3 identity management models in the selected data exchange systems (X-Road)

- All the three analysed IdM systems have its pros & cons
- DPKI-based IdM system is not feasible for the organisational context
- PKI-based IdM system with distributed key management is a more feasible alternative to DPKI-based, enabling zero trust (partial trustlessness & decentralization)

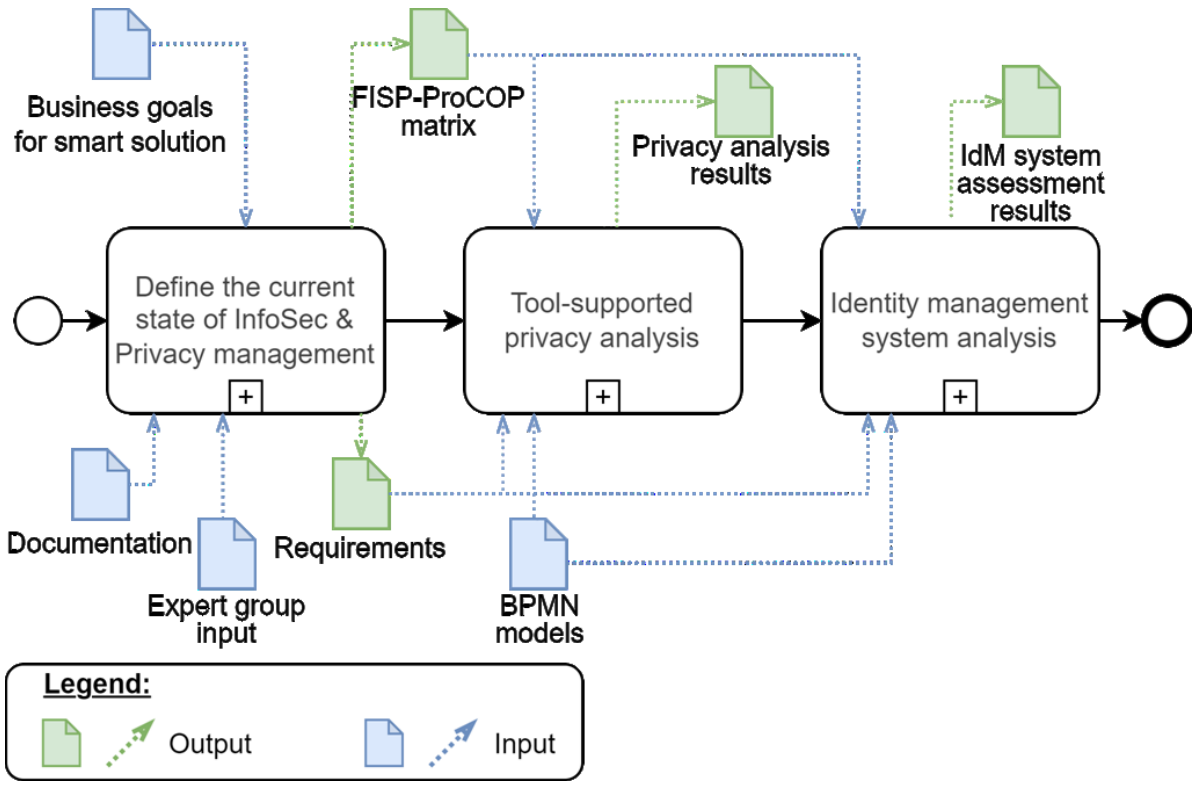


Quality criteria	Quality sub-criteria	Indicators	How to measure	Measurement					
				PKI	DPKI	DPKI vs PKI		DKMS	DKMS vs PKI
Security	Preventing insider threat	Fact of having built in prevention mechanism	Yes / No	No	No	=	+	Yes	+
	Decentralisation	Decentralisation of credentials issuance/verification	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* / sec *	-
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	+
Maintain-ability	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	=-

[3] Bakhtina et al. "On the Shift to Decentralised Identity Management in Distributed Data Exchange Systems."
[4] Mariia Bakhtina et al. "A Decentralised Public Key Infrastructure for X-Road".
[5] Mariia Bakhtina, Jan Kvapil, Petr Švenda, and Raimundas Matulevičius. "The Power of Many: Securing Organisational Identity Through Distributed Key Management".

Main contribution

A method for information security and privacy management of cross-organisational collaboration



Future Work

- Development of a supplementary tool for analysing data extracted through FISP-ProCOP
- Extension of privacy analysis method with commercial tools
- Extension of the GDPR reference model and the update of the used compliance analysis tool
- The guideline/decision tree for the identity management model selection

Thank you for attention!

Mariia Bakhtina
bakhtina@ut.ee

Information Security Research Group
https://infosec.cs.ut.ee/

Funded by the European Union

Funded by the European Union
under Grant Agreement No. 101087529.

Credits: the used icons are from www.flaticon.com

References

[1] Mariia Bakhtina, Raimundas Matulevičius, and Lukaš Malina. "*Information Security and Privacy Management in Intelligent Transportation Systems*". In: CSIMQ 38 (2024), pp. 100–131, DOI: 10.7250/csimq.2024-38.04

[2] Mariia Bakhtina, Raimundas Matulevičius, and Mari Seeba. "*Tool-supported method for privacy analysis of a business process model*". In: JISA 76 (2023), p. 103525, DOI: 10.1016/j.jisa.2023.103525

[3] Bakhtina et al. "*On the Shift to Decentralised Identity Management in Distributed Data Exchange Systems*." Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing. 2023. doi:10.1145/3555776.3577678

[4] Mariia Bakhtina et al. "*A Decentralised Public Key Infrastructure for X-Road*". In: Proceedings of the 18th International Conference on Availability, Reliability and Security. 2023. DOI: 10.1145/3600160.3605092

[5] 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. DOI: 10.1007/978-3-031-61057-8_28

[6] Sander Truu. 2024. "*Tool-Supported Privacy Analysis of Smart Parking*". BSc thesis. University of Tartu

[7] Mariia Bakhtina. "*Towards More Secure and Data Protective Intelligent Infrastructure Systems*". CAiSE (Doctoral Consortium). 2023.

Table 11: 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	Describe types of information used in the smart solution	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