UNIVERSITY OF TARTU

MUNI Masaryk University

The Power of Many: Securing Organisational Identity Through Distributed Key Management

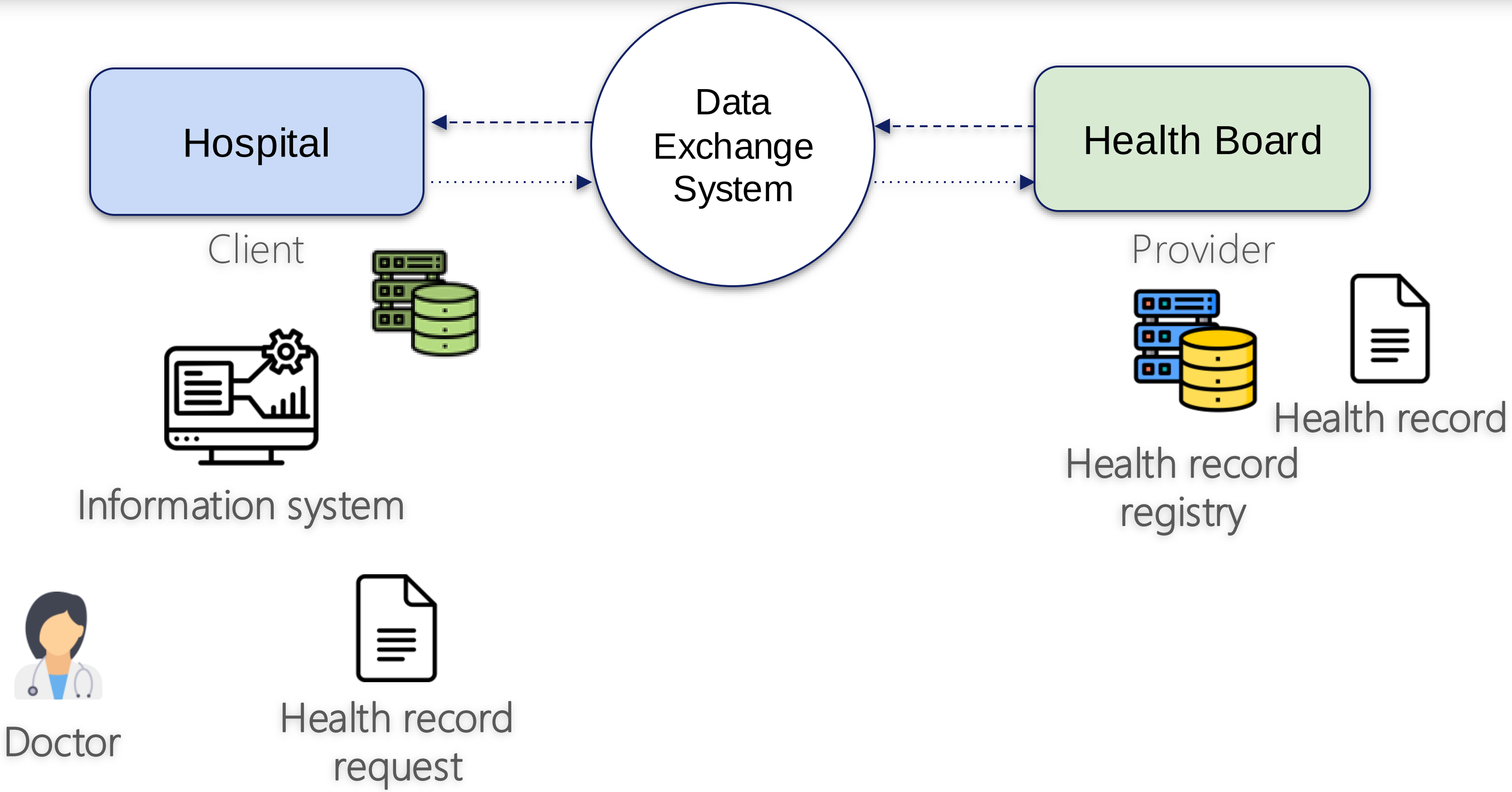
Mariia Bakhtina[1], Jan Kvapil[2],
Petr Švenda[2], and Raimundas Matulevičius[1]

[1] University of Tartu, Tartu, Estonia
[2] Masaryk University, Brno, Czech Republic

36th International Conference on Advanced Information Systems Engineering (CAiSE 2024), Limassol, Cyprus, June 03-07, 2024

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Motivation



Hospital

Data Exchange System

Health Board

Client

Provider

Information system

Health record registry

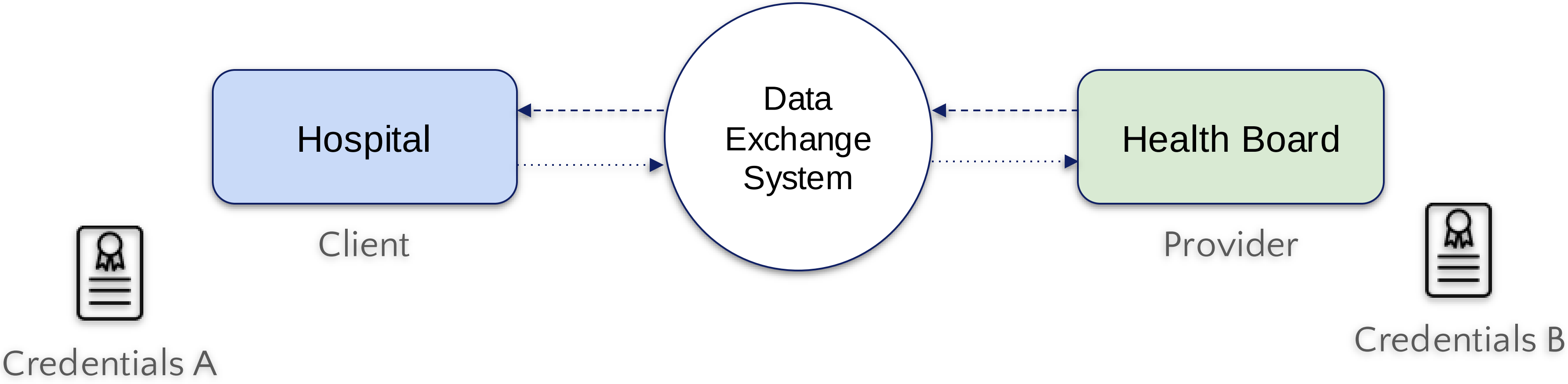
Health record

Doctor

Health record request

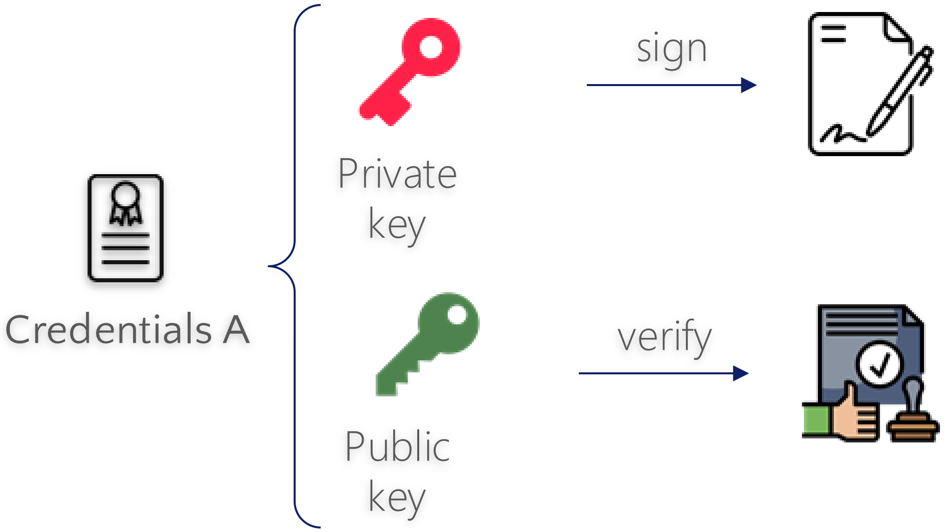
Motivation

- **Organisational Digital Identity** defines an organisation and its attributes for other entities through credentials
- **Credentials** — certificates based on Public Key Infrastructure



Organisational Digital Identity

Public Key Infrastructure preserves integrity and authenticity of the data through signing the message



Credentials A

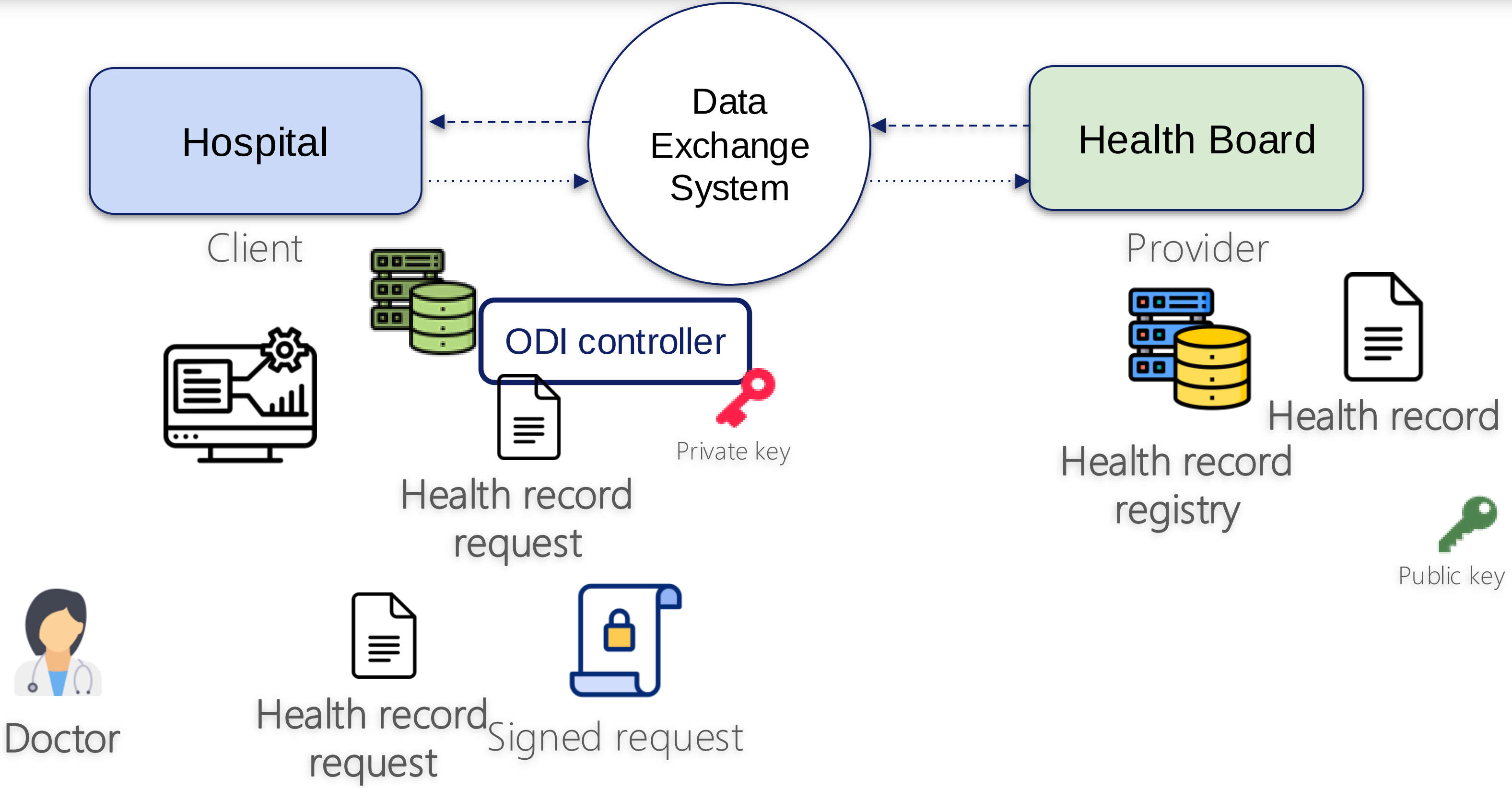
Private key

sign

Public key

verify

Organisational Digital Identity



Hospital

Client

Data Exchange System

Health Board

Provider

ODI controller

Private key

Health record request

Health record

Health record registry

Public key

Doctor

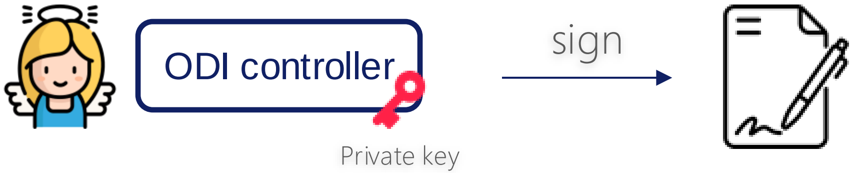
Health record request

Signed request

Problem Statement

Who controls private key? Do we trust this entity?

Custodian — administrator, system component, third-party controller

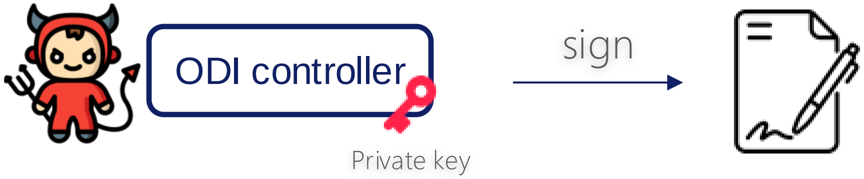


Centralised control over an organisation's private key is a threat to message authenticity and integrity

Problem Statement

Who controls private key? Do we trust this entity?

Custodian — administrator, system component, third-party controller



Centralised control over an organisation's private key is a threat to message authenticity and integrity

Problem Statement

Do we need to have a fully trusted ODI controller?

Zero Trust strategy:

eliminate implicit trust – verify instead

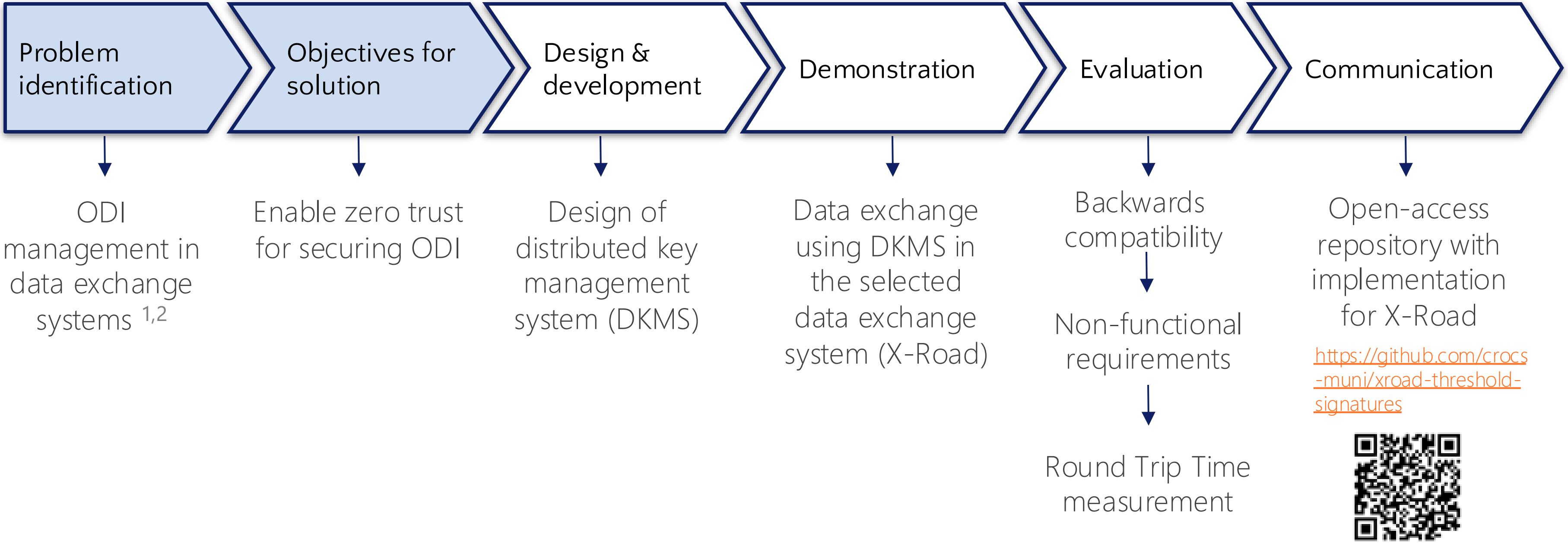
Research Question

How to secure organisational identity

through key management mechanisms

for achieving zero trust?

Design Science Research Method



Problem identification → ODI management in data exchange systems [1,2]

Objectives for solution → Enable zero trust for securing ODI

Design & development → Design of distributed key management system (DKMS)

Demonstration → Data exchange using DKMS in the selected data exchange system (X-Road)

Evaluation → Backwards compatibility → Non-functional requirements → Round Trip Time measurement

Communication → Open-access repository with implementation for X-Road

https://github.com/crocs-muni/xroad-threshold-signatures

[1] Bakhtina et al. “On the Shift to Decentralised Identity Management in Distributed Data Exchange Systems”, SAC’23

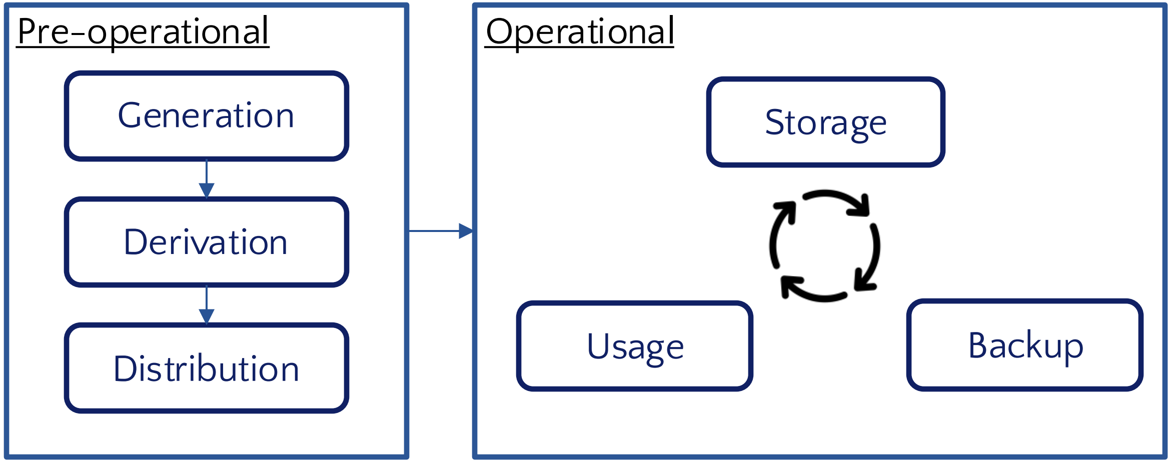
[2] Bakhtina et al. “A Decentralised Public Key Infrastructure for X-Road”, SP2I @ ARES’23

Peffers, Ken, et al. "A design science research methodology for information systems research." *Journal of management information systems* 24.3 (2007): 45-77

Key Management Mechanisms

Review of key management mechanisms

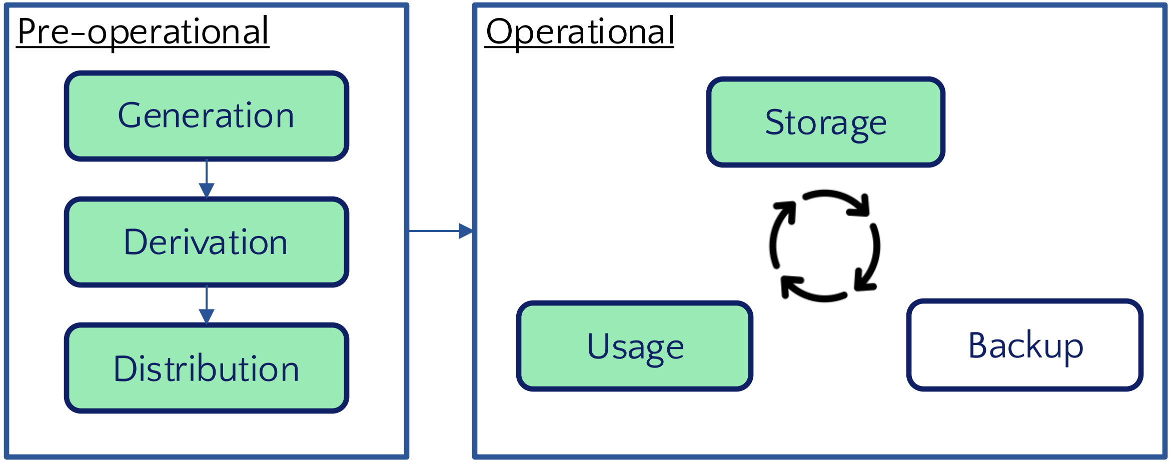
- Stages
- Affected non-functional system characteristics



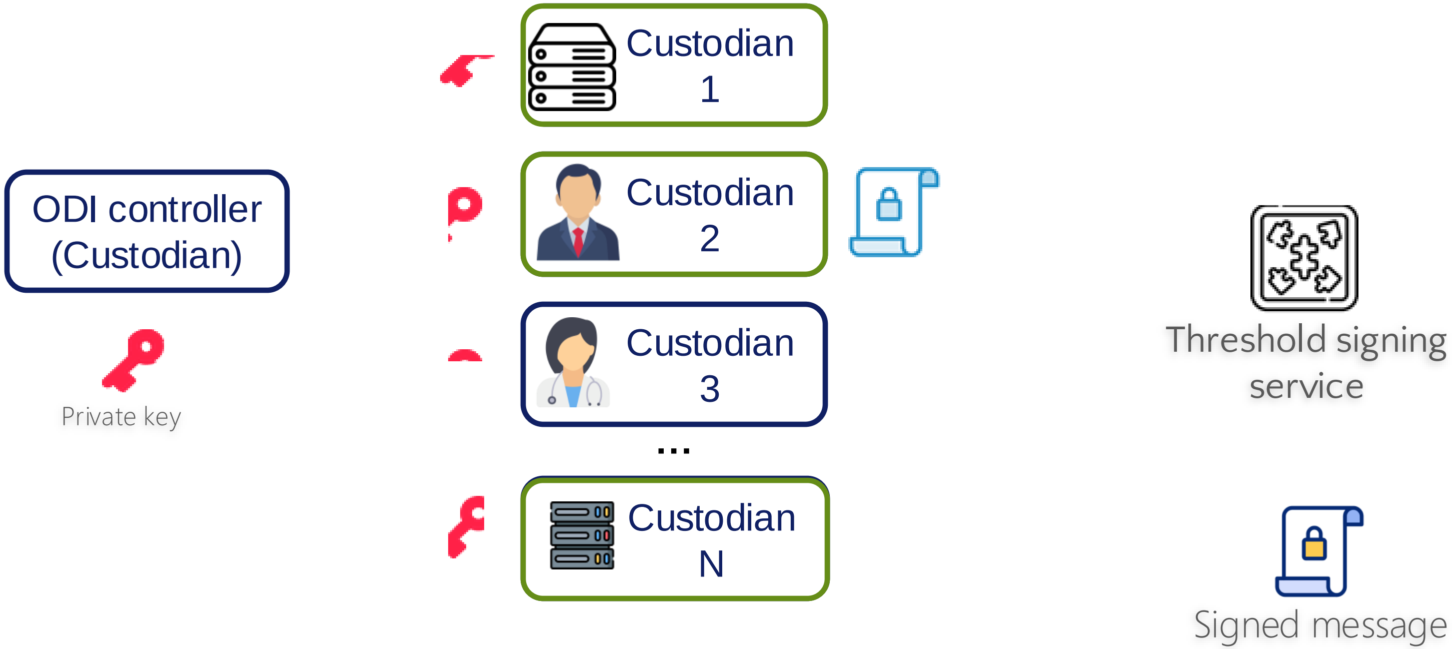
Distributed Key Management System (DKMS)

Partial custody over ODI

- Distribution of keys among multiple semi-trusted custodians
- Threshold signature



Distributed Key Management System (DKMS)



M out of N custodians (threshold) contribute to signing

Distributed Key Management System (DKMS)

- Distribution of trust among the organisational parties – employees and IS components
- Maintaining access control in case of employee turnover
- Cryptographic enforcement of access policies

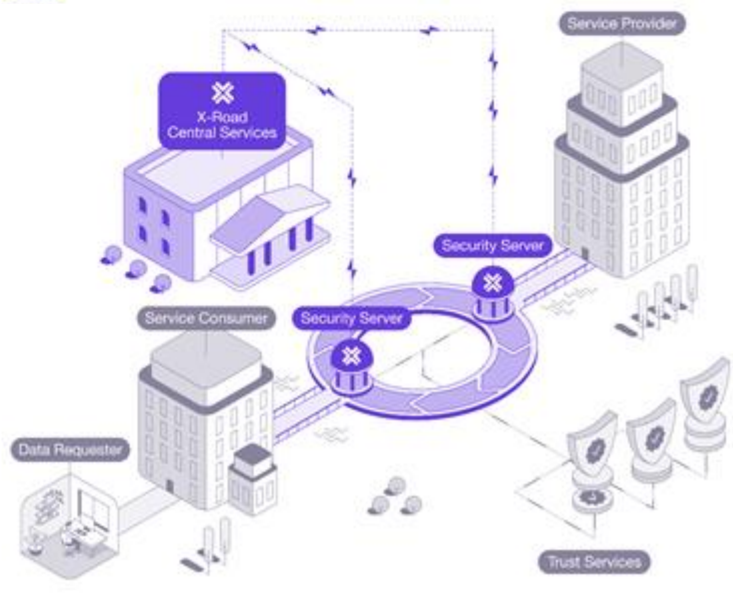
Case: X-Road Data Exchange System

Context:

- E-government infrastructure
- Private companies network

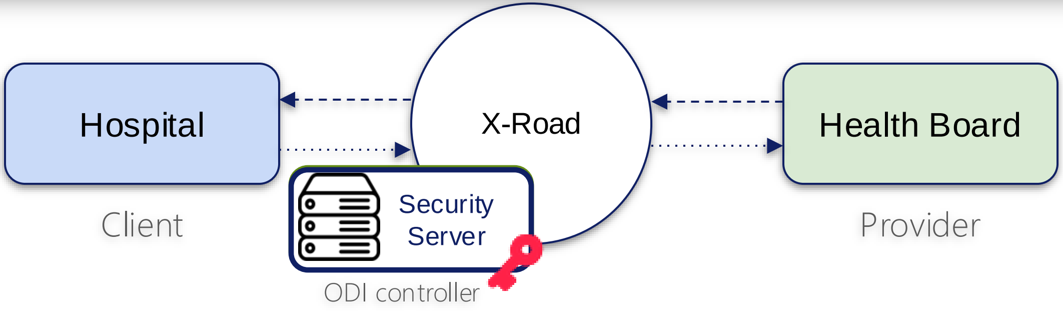
Goals:

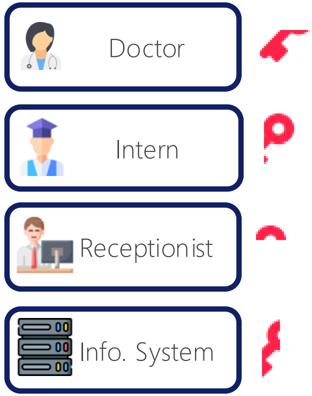
- Trustlessness
- Traceability
- Preventing privilege misuse
- Backward compatibility
- Decentralisation & Multiple users



X-Road architecture
https://x-road.global/architecture

Testing Scenario



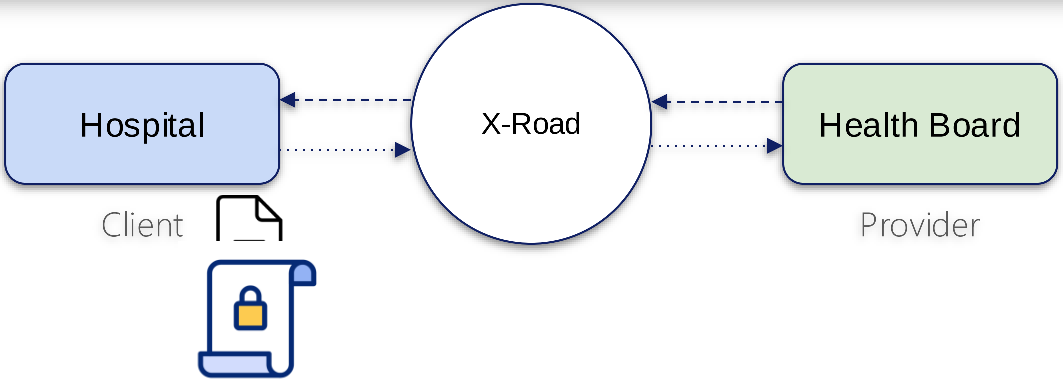


Threshold signing service

As-Is: 1 fully trusted custodian

To-Be: To 5 semi-trusted custodians
Access rule enforced: 3 out of 5

Evaluation



Round Trip Time (RTT) comparison

for Client-Provider data exchange (the Client’s signing token varies)

Client’s token:	SoftToken	SoftHSM	YubiKey 5	TPM NTC 7.2.3.1	*this work*
mean RTT	82ms	75ms	216ms	260ms	276ms
mean slowdown	1.0x	0.92x	2.65x	3.18x	3.38x

Limitations

- Performance
  - Overhead from the network and signing platform
  - (Optional) Employees's involvement is an added activity
- Legal implications
- Key lifecycle
  - Post-operational and destroyed phases are not considered

Conclusion

- a **distributed key management system (DKMS)** for achieving zero trust
- **proof-of-concept** implementation for X-Road

Future work

- Analyse the legal implications of partial custody
- Validate DKMS (running X-Road instance and other data exchange systems)

Thank you for attention!

Mariia Bakhtina
bakhtina@ut.ee

Jan Kvapil
kvapil@mail.muni.cz

Petr Švenda
svenda@fi.muni.cz

Raimundas Matulevičius
rma@ut.ee

https://chess-eu.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