CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

UNIVERSITY OF TARTU
1632

MUNI Masaryk University

A Decentralised Public Key Infrastructure for X-Road

Mariia Bakhtina[1], Kin Long Leung[1], Raimundas Matulevičius[1], Ahmed Awad[1], and Petr Švenda[2]

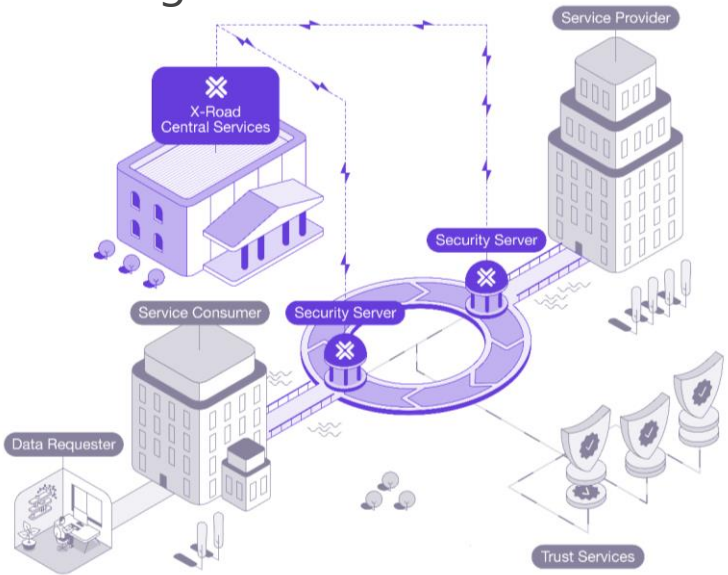
[1] University of Tartu, Tartu, Estonia
[2] Masaryk University, Brno, Czech Republic

The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29 - September 01, 2023, Benevento, Italy

Case description

X-Road© is a centrally managed distributed data exchange system that provides unified and secure data exchange between organisations

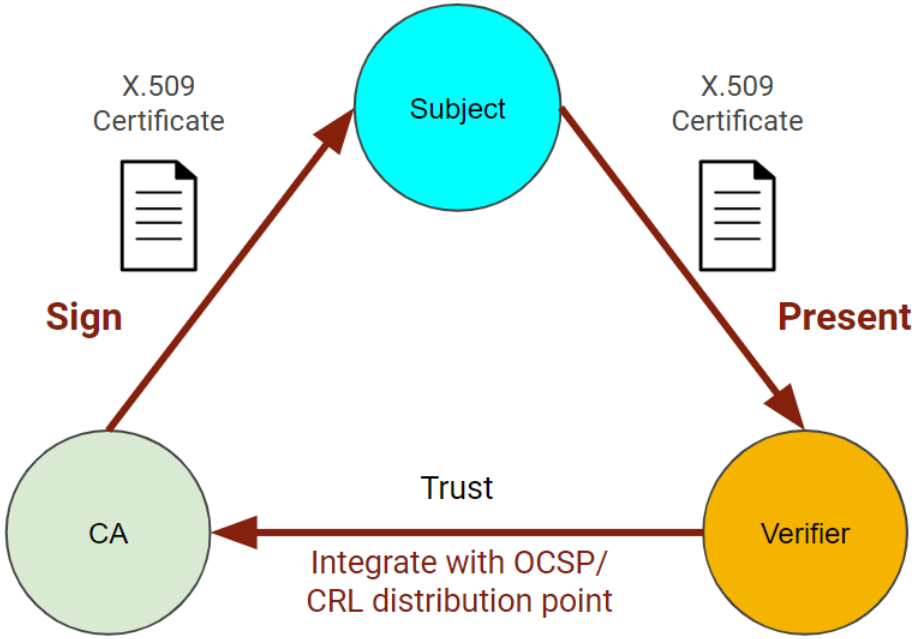
- What is trust? Credentials?
  - Centralised root of trust (PKI X.509, i.e. PKIX)



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

Motivation

- PKIX requires (manual) identity verification for certificate issuance
- PKIX is prone to the threat of DoS and to a single point of failure



PKI with X.509

Motivation

- Rise of Self-Sovereign identity brings new standards & technologies
  - DID
  - VC / VP

did:ethr:0x03fdd57adec3d438ea237fe46

Decentralised Identifier (DID) created without the help of centralised authorities

```
{
  "@context": [ "https://www.w3.org/ns/did/v1" ]
  "id": "did:ethr:0x03fdd57adec3d438ea237fe46",
  "authentication": [{
    "id": "did:ethr:0x03fdd57adec3d438ea237fe46#keys-1",
    "type": "Ed25519VerificationKey2020",
    "publicKeyMultibase":
       "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

DID document on distributed ledger

Motivation

- Rise of Self-Sovereign Identity brings new standards & technologies
  - DID
  - VC / VP

```
{
  "@context":
["https://www.w3.org/2018/credentials/v1"],
  "type":
["VerifiableCredential","UniversityDegreeCredential"],
  "issuer": "did:btcr:x705-jznz-q3nl-srs",
  "credentialSubject": {
    “id”: "did:ethr:0x03fdd57adec3d438ea237fe46",
    "degree": {
      "name": "Bachelor of Science and Arts",
      "college": "College of Engineering"
    }
  },
  // credential-holder binding, revocation status
  "proof": { … }
}
```

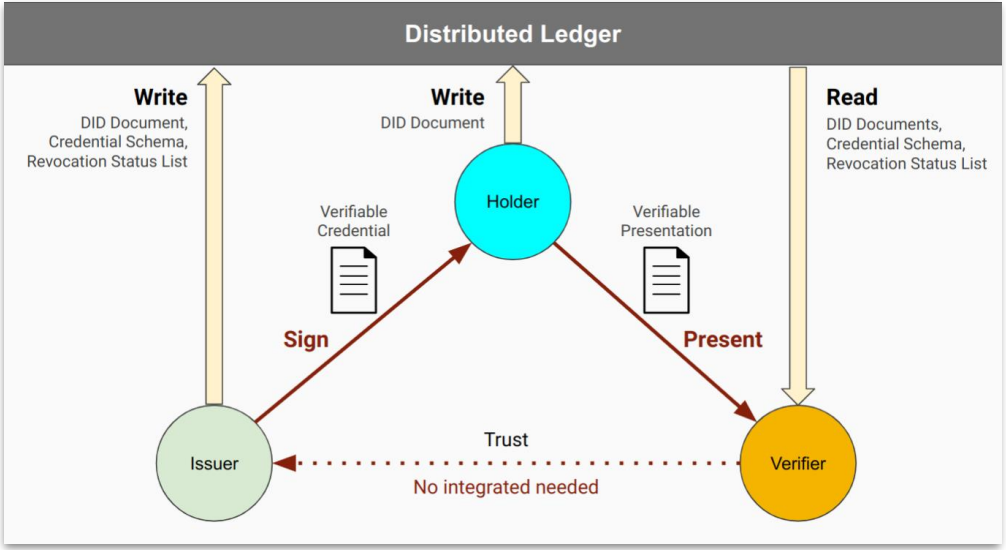
Verifiable Credential (VC) – a tamper-evident credential that has authorship and can be cryptographically verified,
+ can be presented in a form of **Verifiable Presentation (VP)**

Motivation

Self-Sovereign Identity (SSI) was primarily developed for physical entities

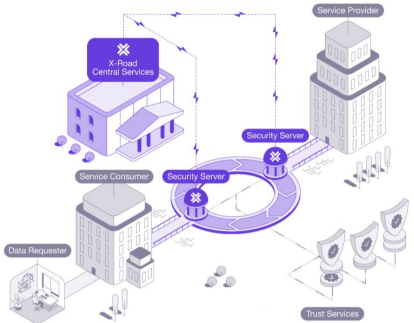
How about organisational identity?

Can DPKI be enable organisational identity management?



DPKI with SSI technologies

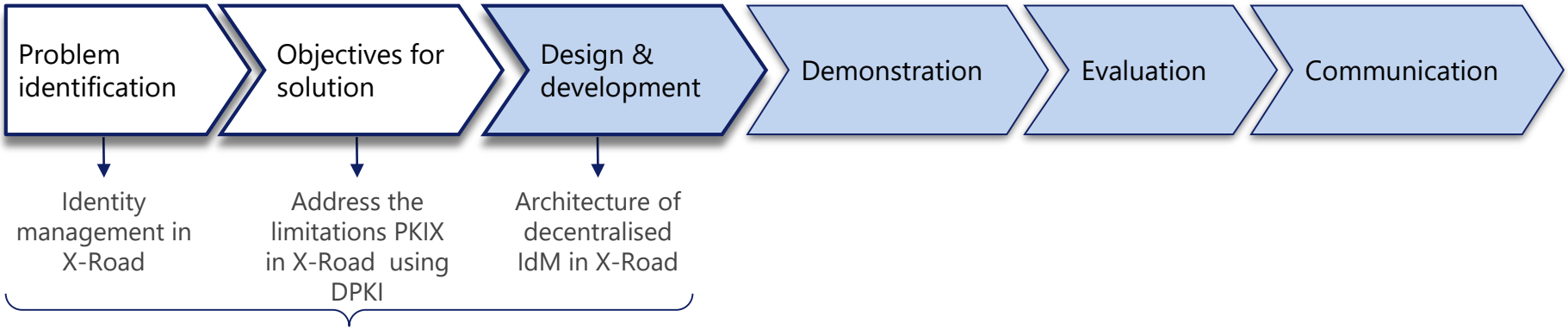
+



Research Question

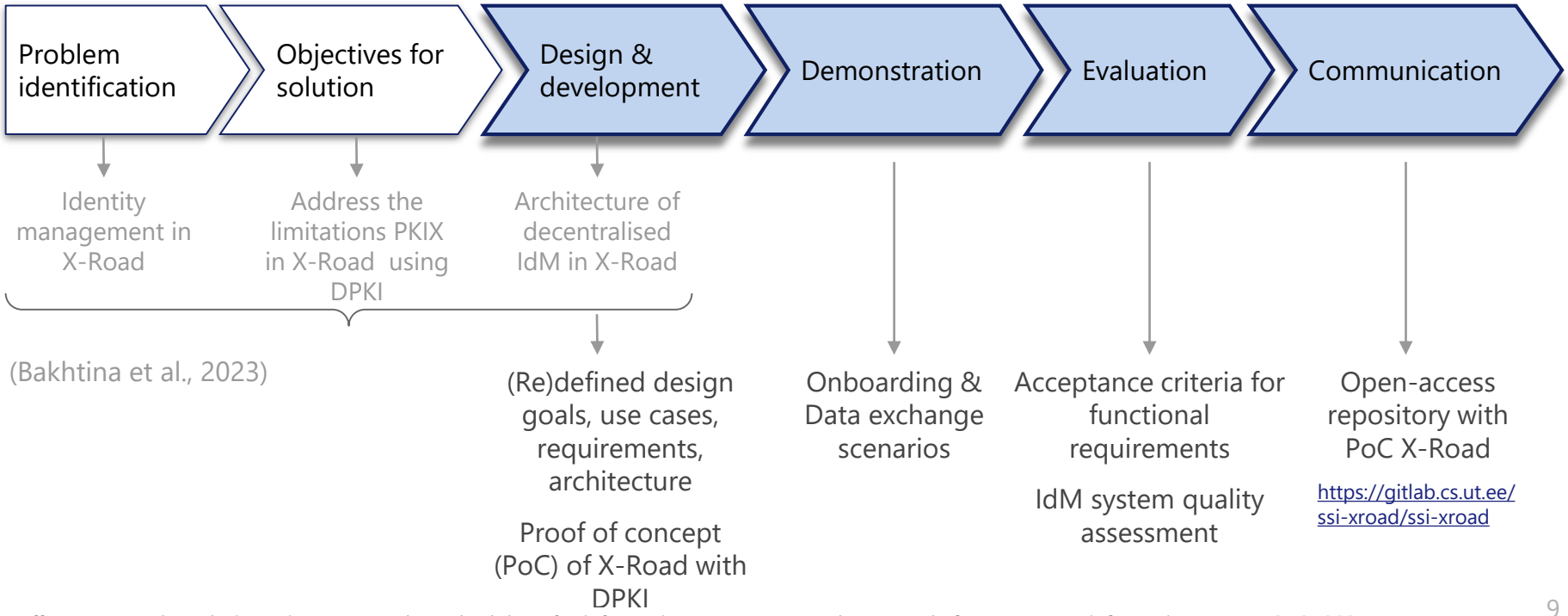
How to establish trust between information systems using a decentralised public key infrastructure in X-Road?

Design Science Research Method



(Bakhtina et al., 2023)

Design Science Research Method



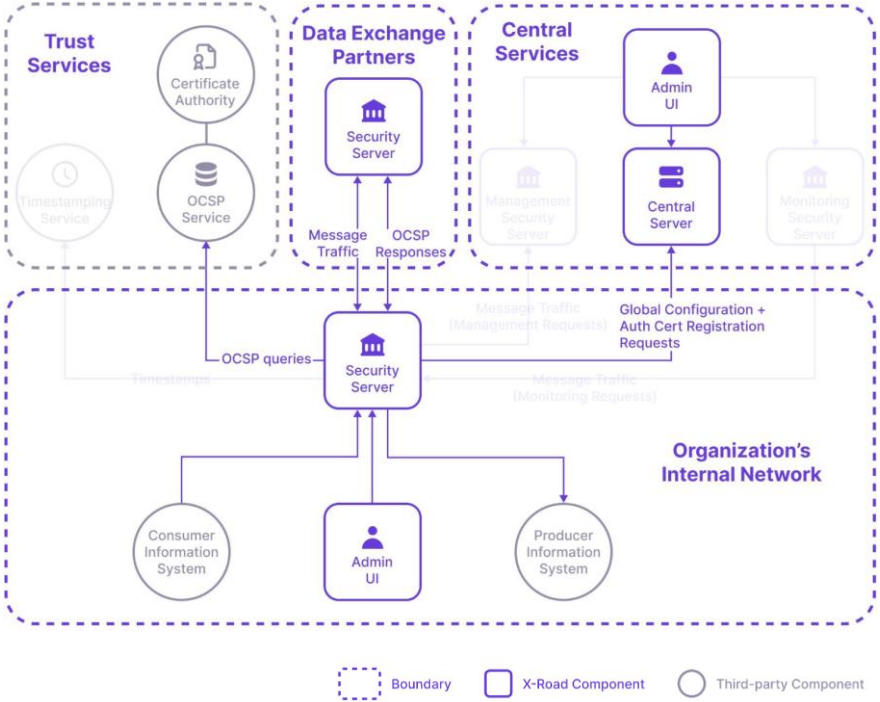
Peffers, Ken, et al. "A design science research methodology for information systems research." *Journal of management information systems* 24.3 (2007): 45-77.

Design

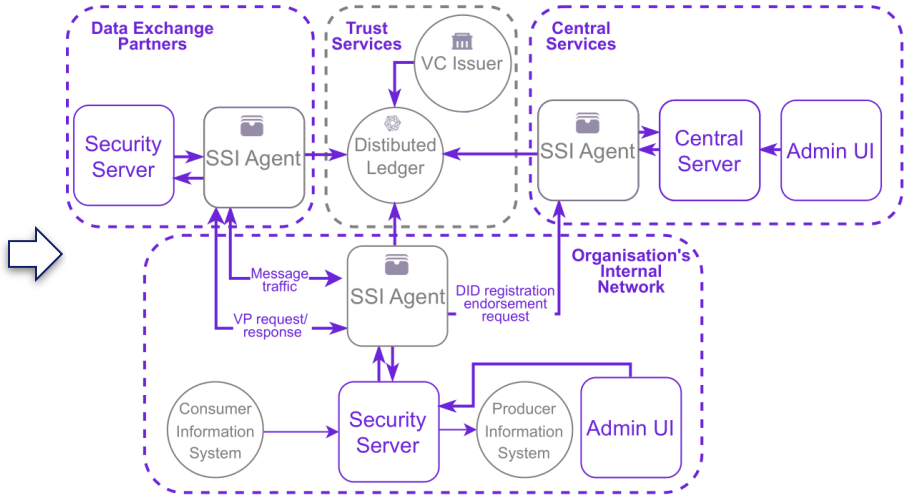
Design goals:

1. Increase the degree of decentralisation
2. Provide a more granular access control mechanism
3. Support automated member onboarding

Design

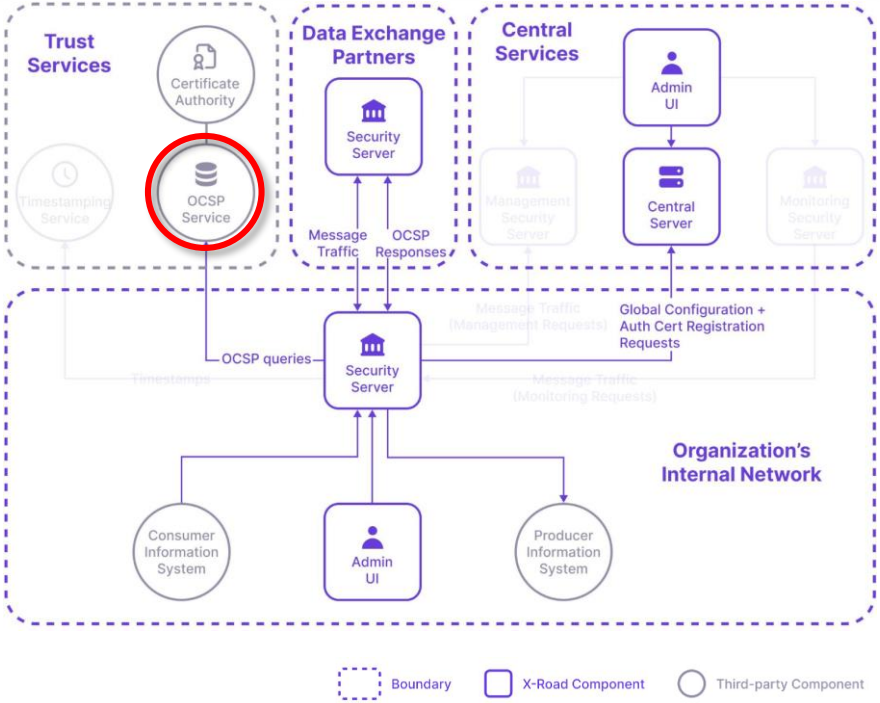


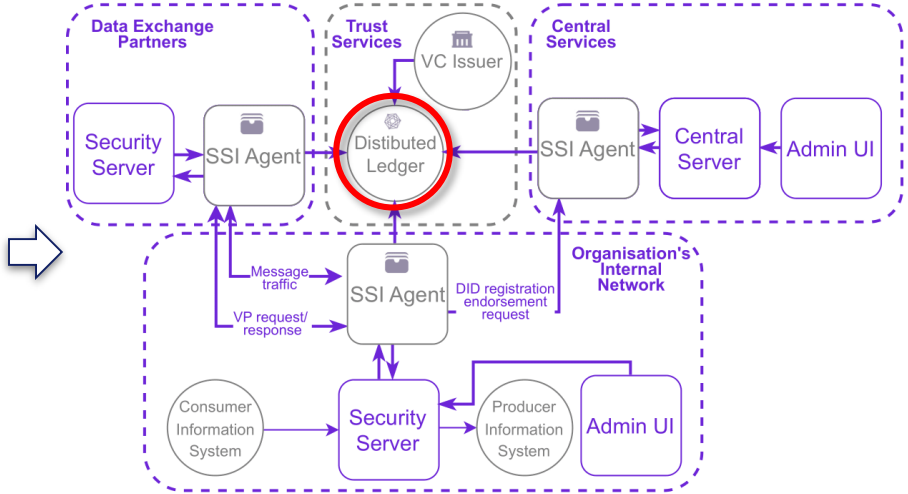
X-Road Original Architecture



X-Road with DPKI PoC Architecture

Design

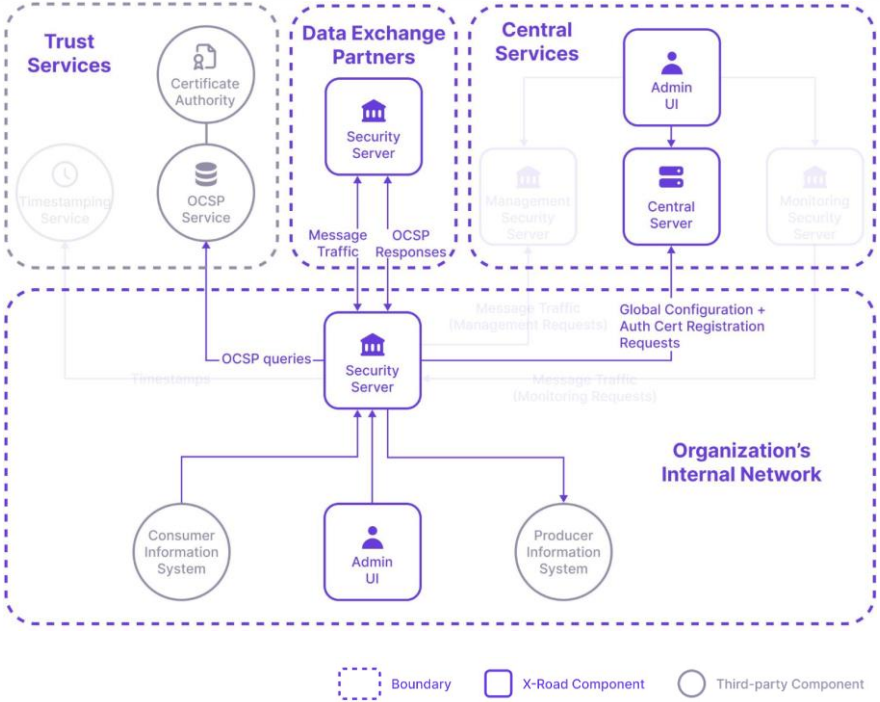


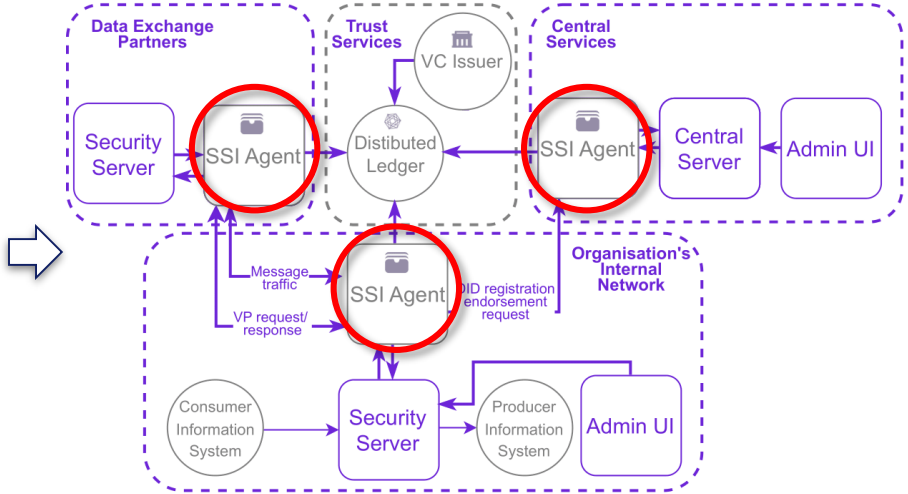


X-Road Original Architecture

X-Road with DPKI PoC Architecture

Design





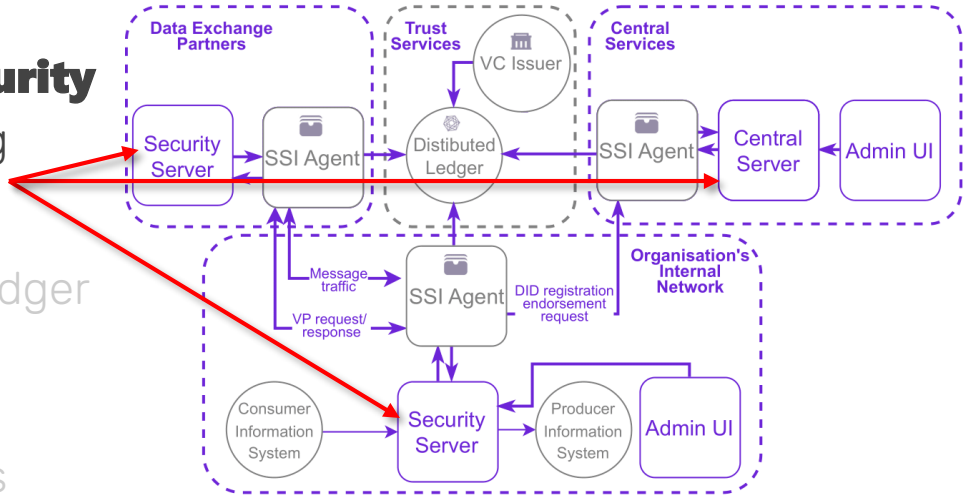
X-Road Original Architecture

X-Road with DPKI PoC Architecture

Implementation

Implemented **instance of X-Road Security Server and Central server,** integrating with:

- **Hyperledger Indy** as distributed ledger
- **Hyperledger Aries Cloud Agent Python** as SSI agent
- **AnonCreds** as verifiable credentials implementation
- **Aries Protocols** for secure connection, credential exchanges



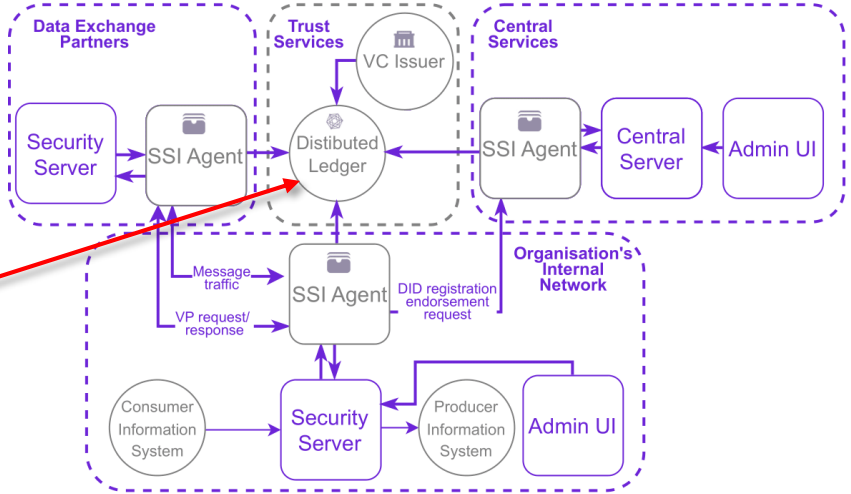
https://gitlab.cs.ut.ee/ssi-xroad/ssi-xroad

X-Road with DPKI PoC Architecture

Implementation

Implemented **instance of X-Road Security Server and Central server,** integrating with:

- **Hyperledger Indy** as distributed ledger
- **Hyperledger Aries Cloud Agent Python** as SSI agent
- **AnonCreds** as verifiable credentials implementation
- **Aries Protocols** for secure connection, credential exchanges



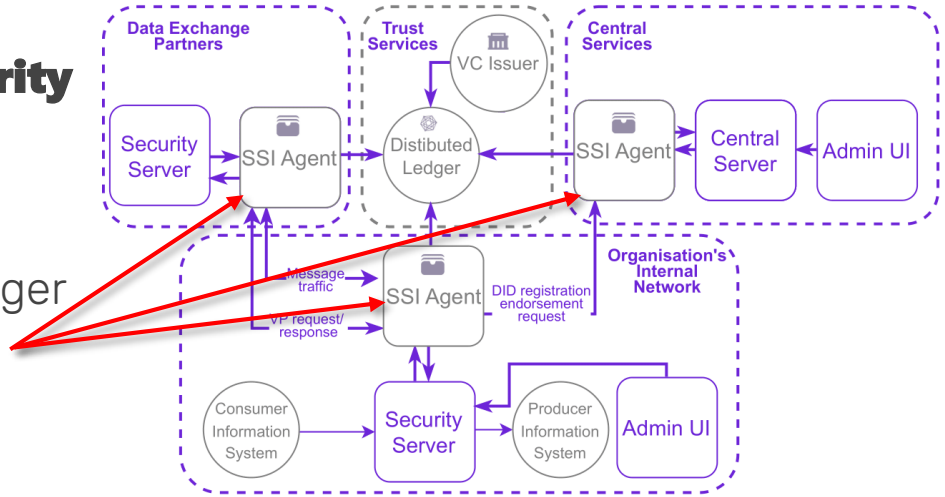
https://gitlab.cs.ut.ee/ssi-xroad/ssi-xroad

X-Road with DPKI PoC Architecture

Implementation

Implemented **instance of X-Road Security Server and Central server,** integrating with:

- **Hyperledger Indy** as distributed ledger
- **Hyperledger Aries Cloud Agent Python** as SSI agent
- **AnonCreds** as verifiable credentials implementation
- **Aries Protocols** for secure connection, credential exchanges



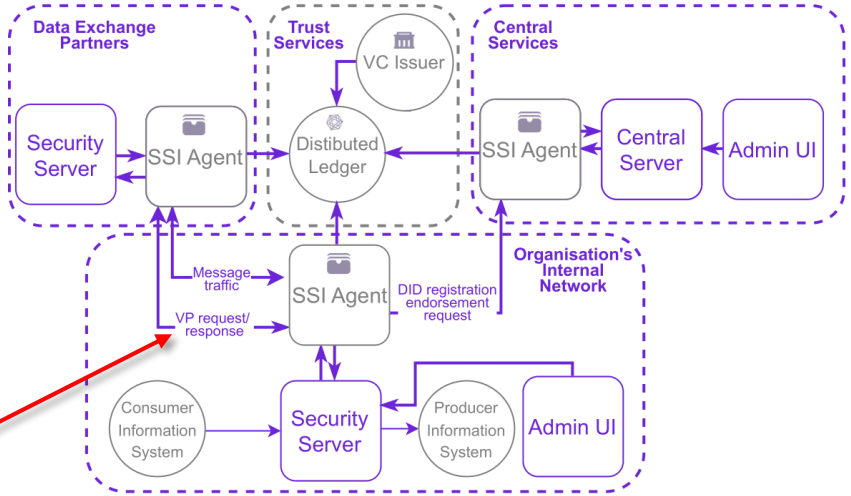
https://gitlab.cs.ut.ee/ssi-xroad/ssi-xroad

X-Road with DPKI PoC Architecture

Implementation

Implemented **instance of X-Road Security Server and Central server,** integrating with:

- **Hyperledger Indy** as distributed ledger
- **Hyperledger Aries Cloud Agent Python** as SSI agent
- **AnonCreds** as verifiable credentials implementation
- **Aries Protocols** for secure connection, credential exchanges



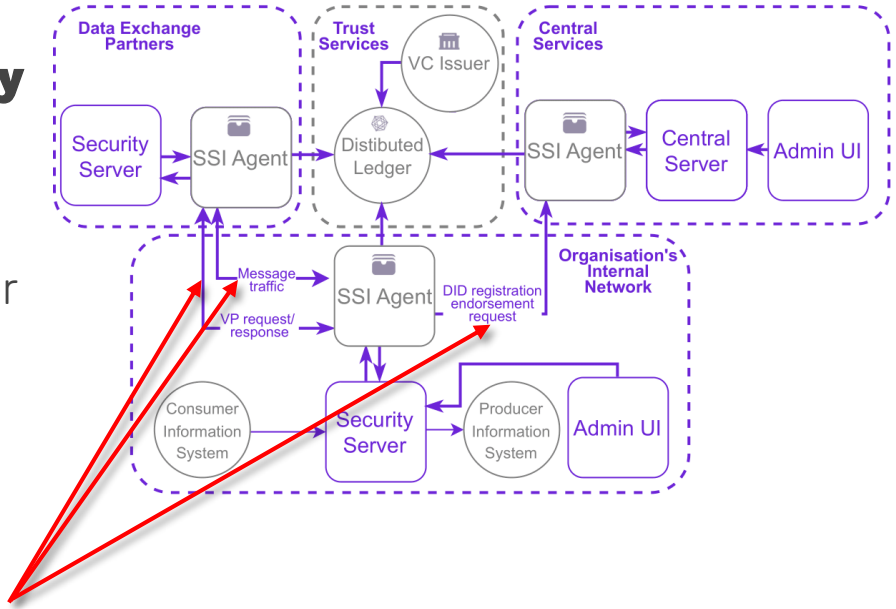
https://gitlab.cs.ut.ee/ssi-xroad/ssi-xroad

X-Road with DPKI PoC Architecture

Implementation

Implemented **instance of X-Road Security Server and Central server,** integrating with:

- **Hyperledger Indy** as distributed ledger
- **Hyperledger Aries Cloud Agent Python** as SSI agent
- **AnonCreds** as verifiable credentials implementation
- **Aries Protocols** for secure connection, credential exchanges



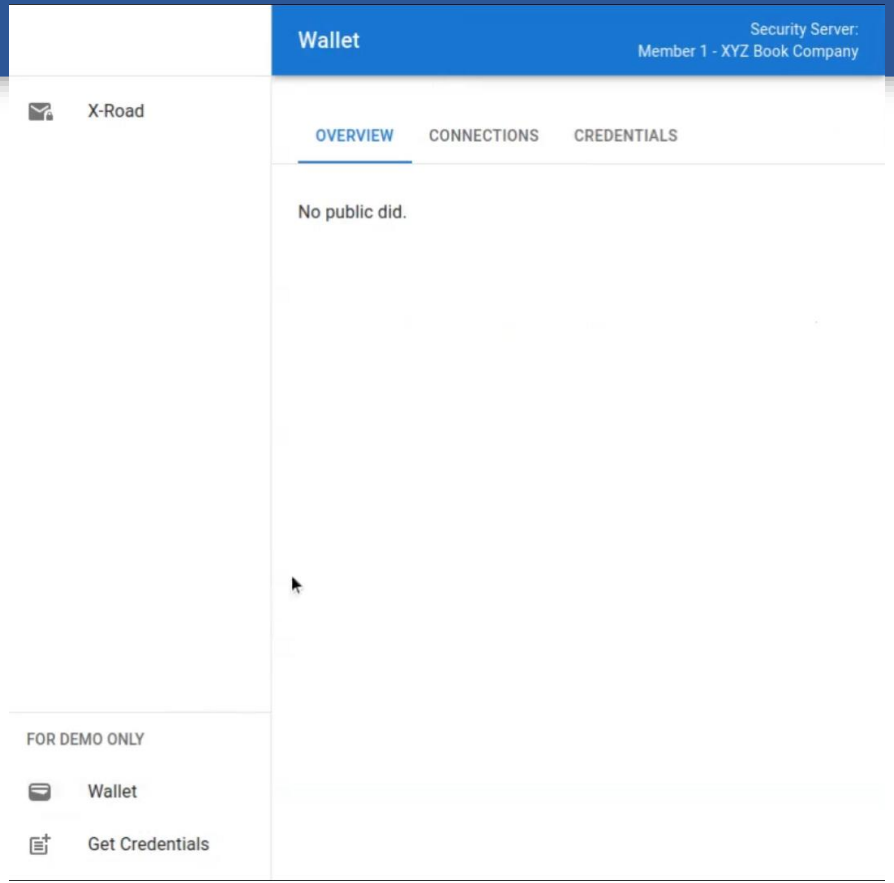
https://gitlab.cs.ut.ee/ssi-xroad/ssi-xroad

X-Road with DPKI PoC Architecture

Demonstration: Member Onboarding

Central Server requests organisation to present a “Business Registration Credential” for onboarding, i.e. joining an X-Road instance.

DID of new X-Road member is written on ledger for discovery.

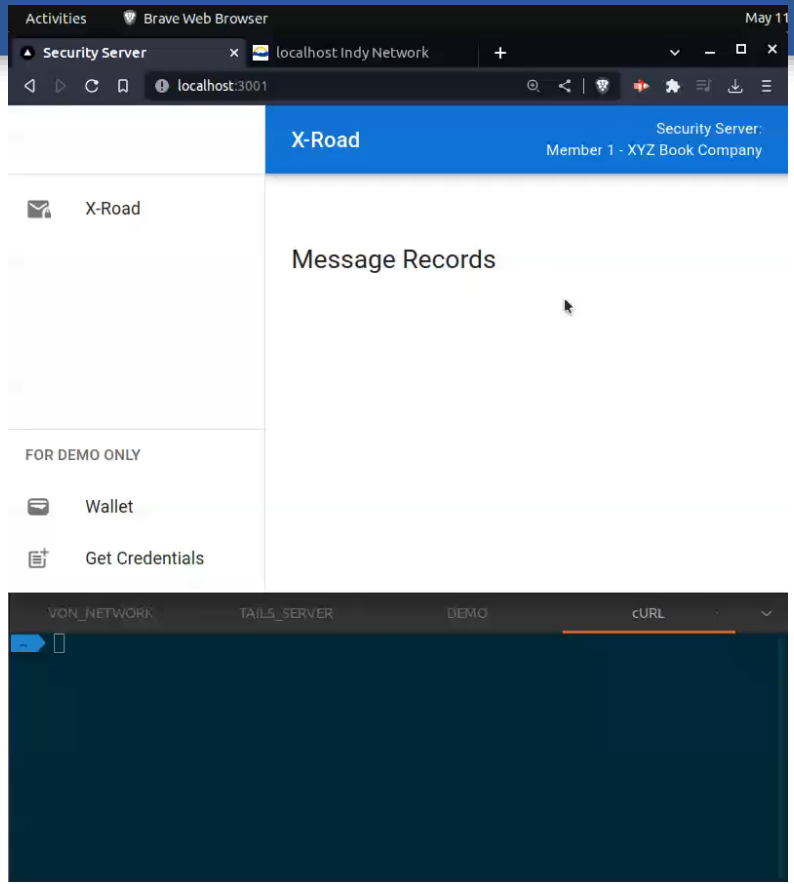


https://gitlab.cs.ut.ee/ssi-xroad/ssi-xroad

Demonstration: Message Exchange

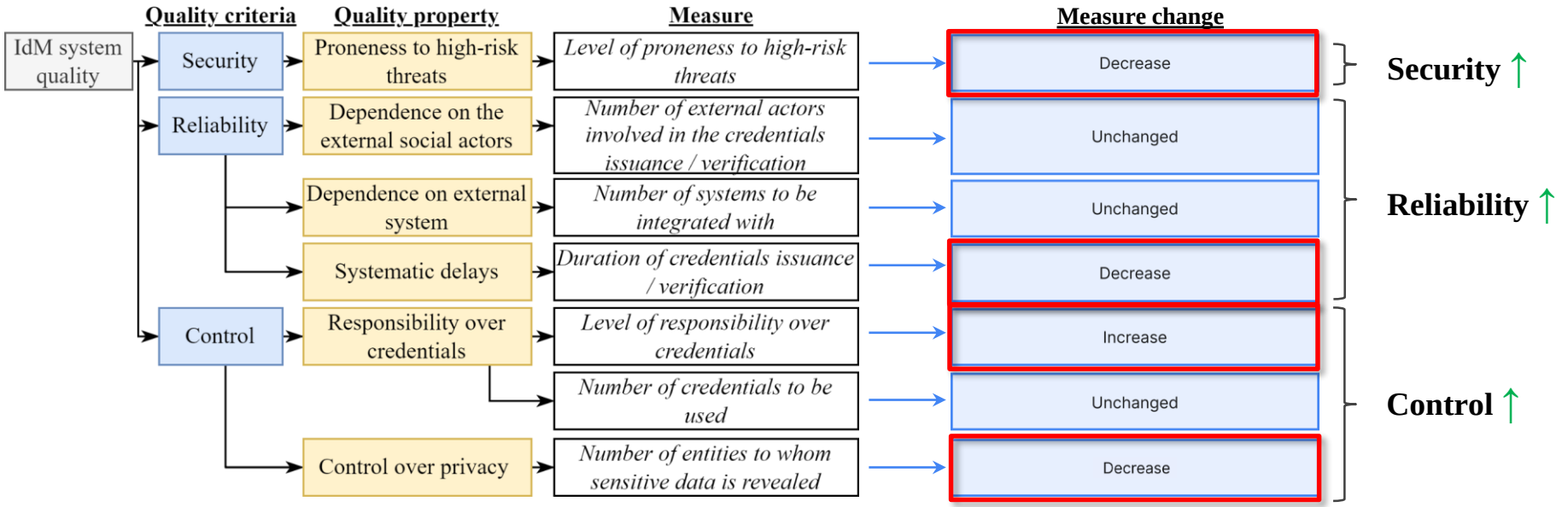
Information systems of X-Road members exchange credentials before exchanging message.

Message exchange records are signed with authentication keys in members' DID documents.



https://gitlab.cs.ut.ee/ssi-xroad/ssi-xroad

Evaluation: Change in System Quality



Identity Management System Quality Assessment Model

Evaluation

Mariia Bakhtina et al. "On the shift to decentralised identity management in distributed data exchange systems". 2023.

Conclusion

- This paper presents the **first open-access system prototype** for an **organisation's identity management** following **self-sovereign identity** principles
- The presented proof of concept proves that **DPKI helps to address** some of the **scalability issues of PKI**, improve **control over identity** and **mitigate a single point of failure** in the X-Road system

Conclusion

Limitations: The design may be biased towards the Hyperledger Indy ecosystem

Future work:

- Explore the selection of other distributed ledger-based SSI ecosystems
- Enable PKIX certificates to be VCs using the PKIX extension
- Extend the PoC with wallet management measures to strengthen access control over organisational identity

UNIVERSITY OF TARTU
1632

MUNI Masaryk University

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Thank you for attention!

Co-funded by the European Union

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.