Zero-Trust Architecture for Legal Entities

Erwin Nieuwlaar

26-04-2023

TUDelft

KVK

Thesis Committee and supervisors:
Dr. ir. J.A. Pouwelse, TU Delft
Dr. C. Lofi, TU Delft
Dr. J. Ubacht, TU Delft
ir. J. Fleuren, KVK

Overview

- Introduction - Context
- Problem Statement – The why
- Architecture – The theoretical how
- Design – The practical how
- Performance Analysis – The feasibility
- Conclusion – Sum up and main takeaways
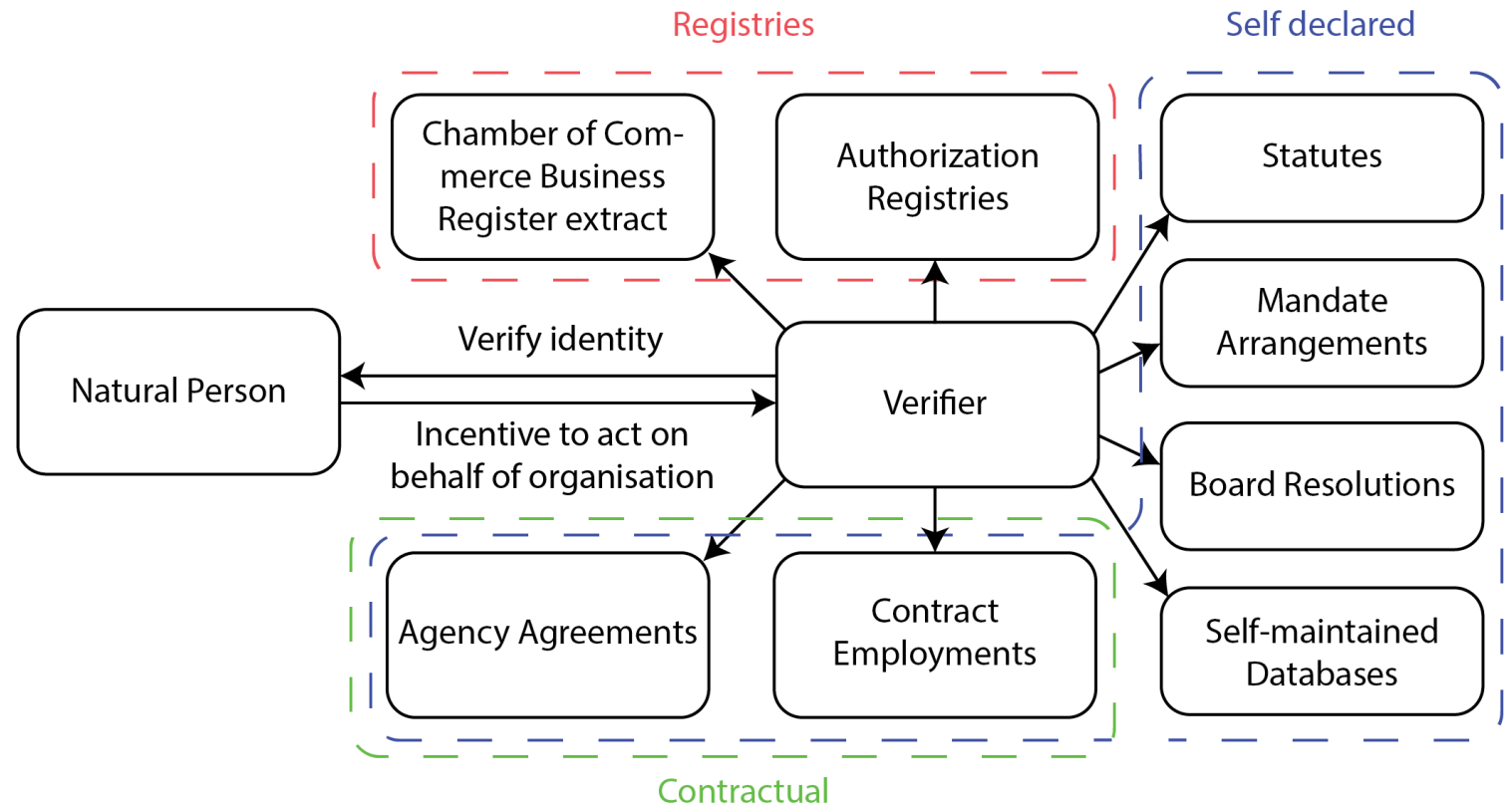- Future research – How to proceed

Introduction

- CISA Zero-Trust

- European Digital Identity
    - Architecture Reference Framework
    - eIDAS 2.0

- Binding Natural Person and Legal Entity
    - Power of Attorney (PoA)
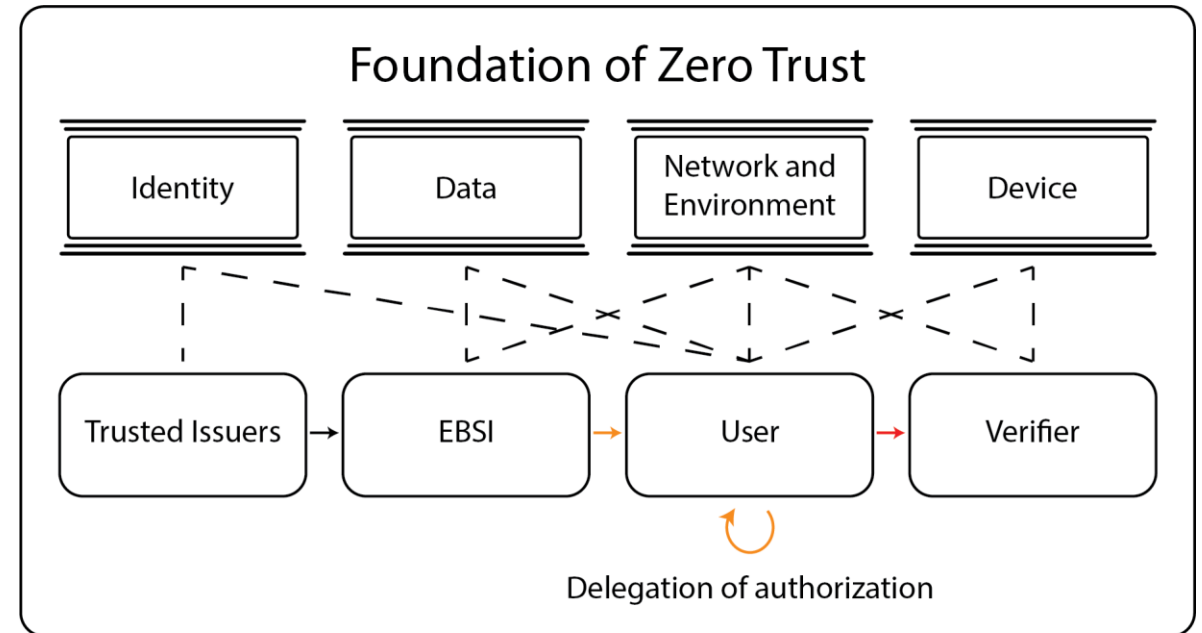   - KVK Extract
    - eHerkenning

Problem Statement

- Current Situation
- Non-portable
- Not cross-border
- Expensive

Architecture

- Trusted Issuer
- European Blockchain Infrastructure Services (EBSI)
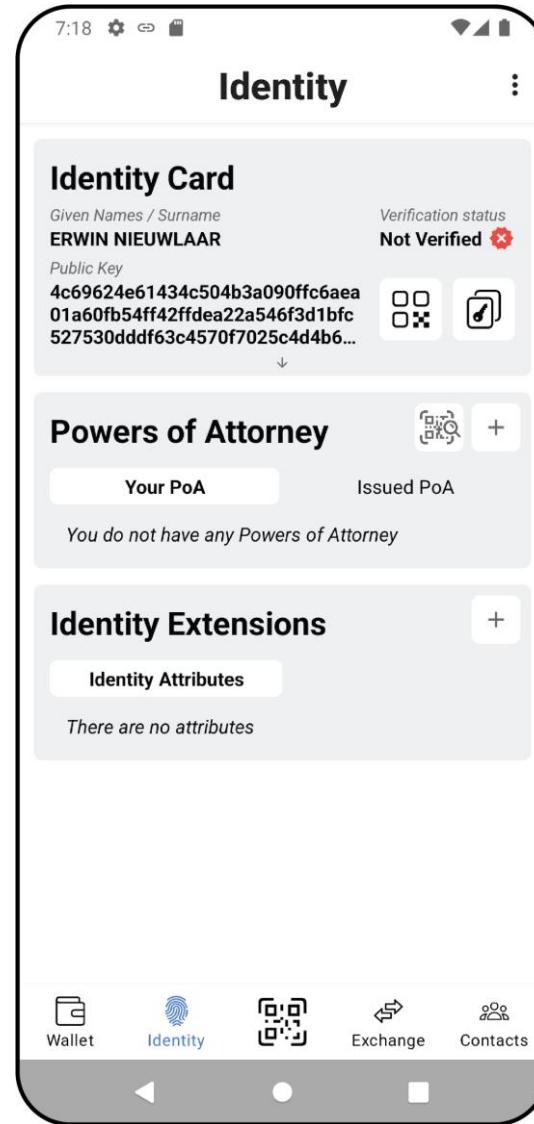- Users
- Verifiers

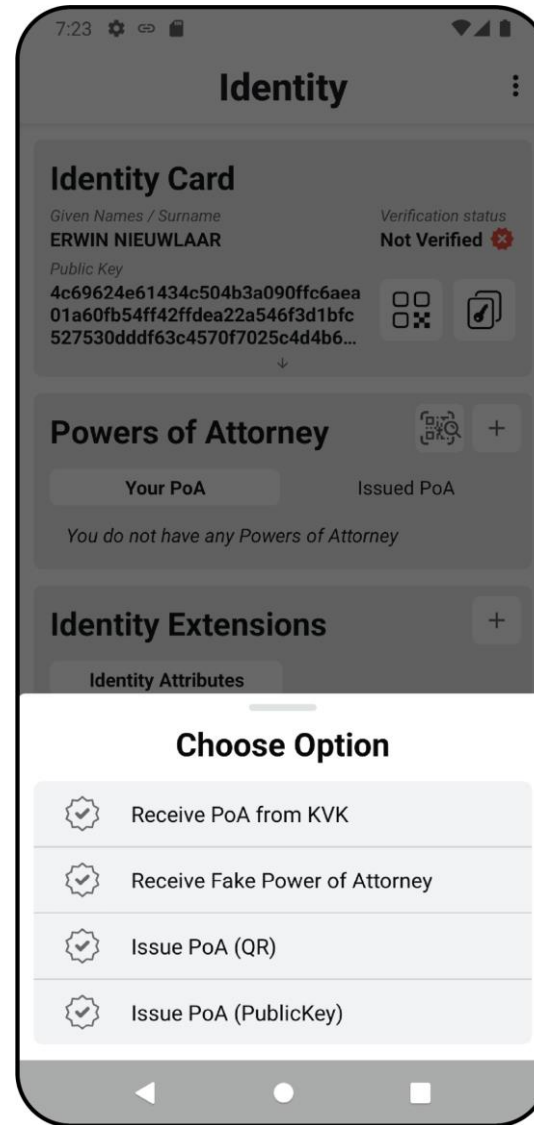Foundation of Zero Trust

Identity | Data | Network and Environment | Device

Trusted Issuers → EBSI → User → Verifier

Delegation of authorization

— — Includes
——→ Trusted
——→ Trusted or untrusted (privacy-trust trade off)
——→ Untrusted

Architecture

- Power of Attorney (PoA)
- Trusted Issuer
- European Blockchain Infrastructure Services (EBSI)
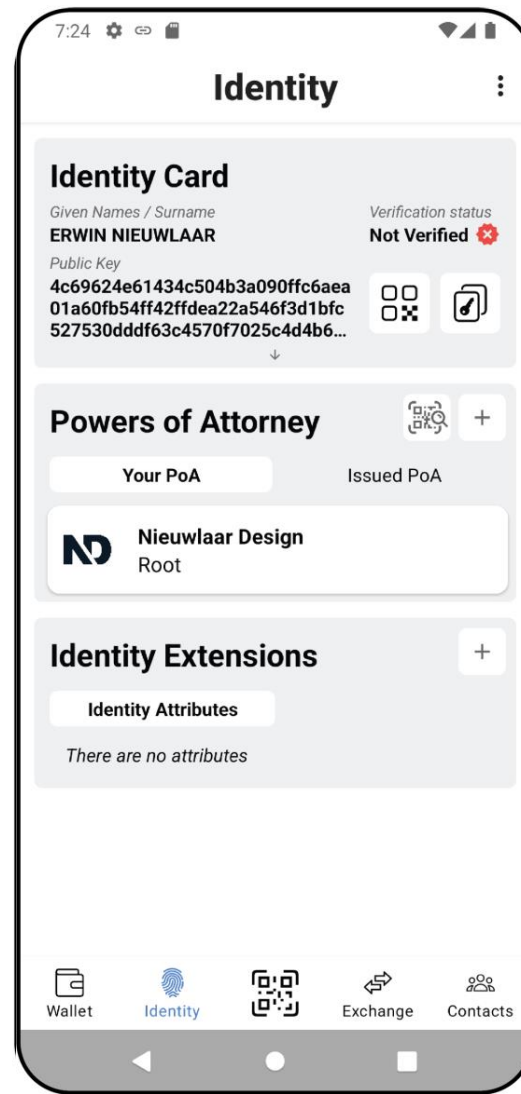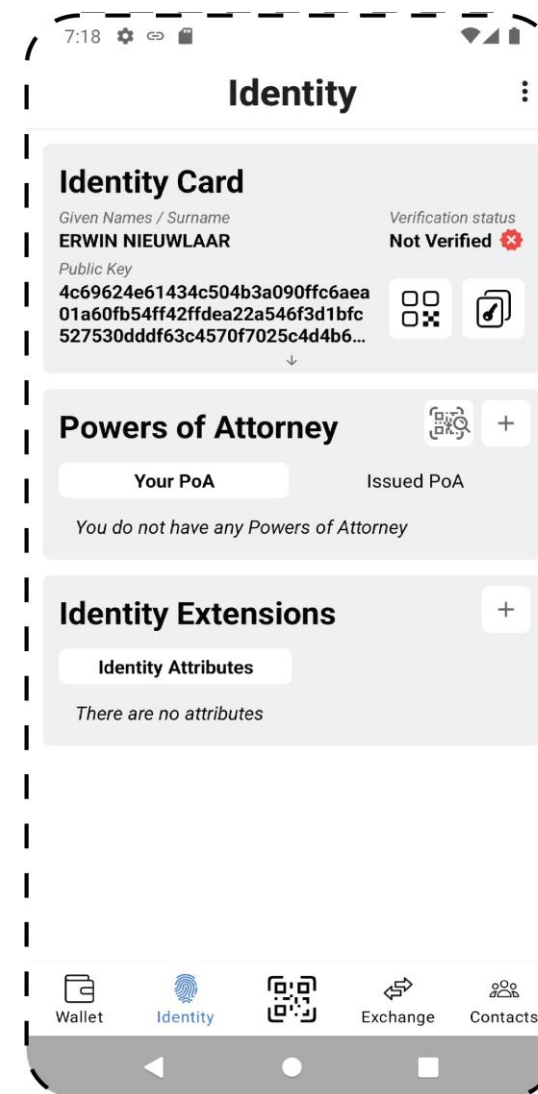- Users
- Verifiers
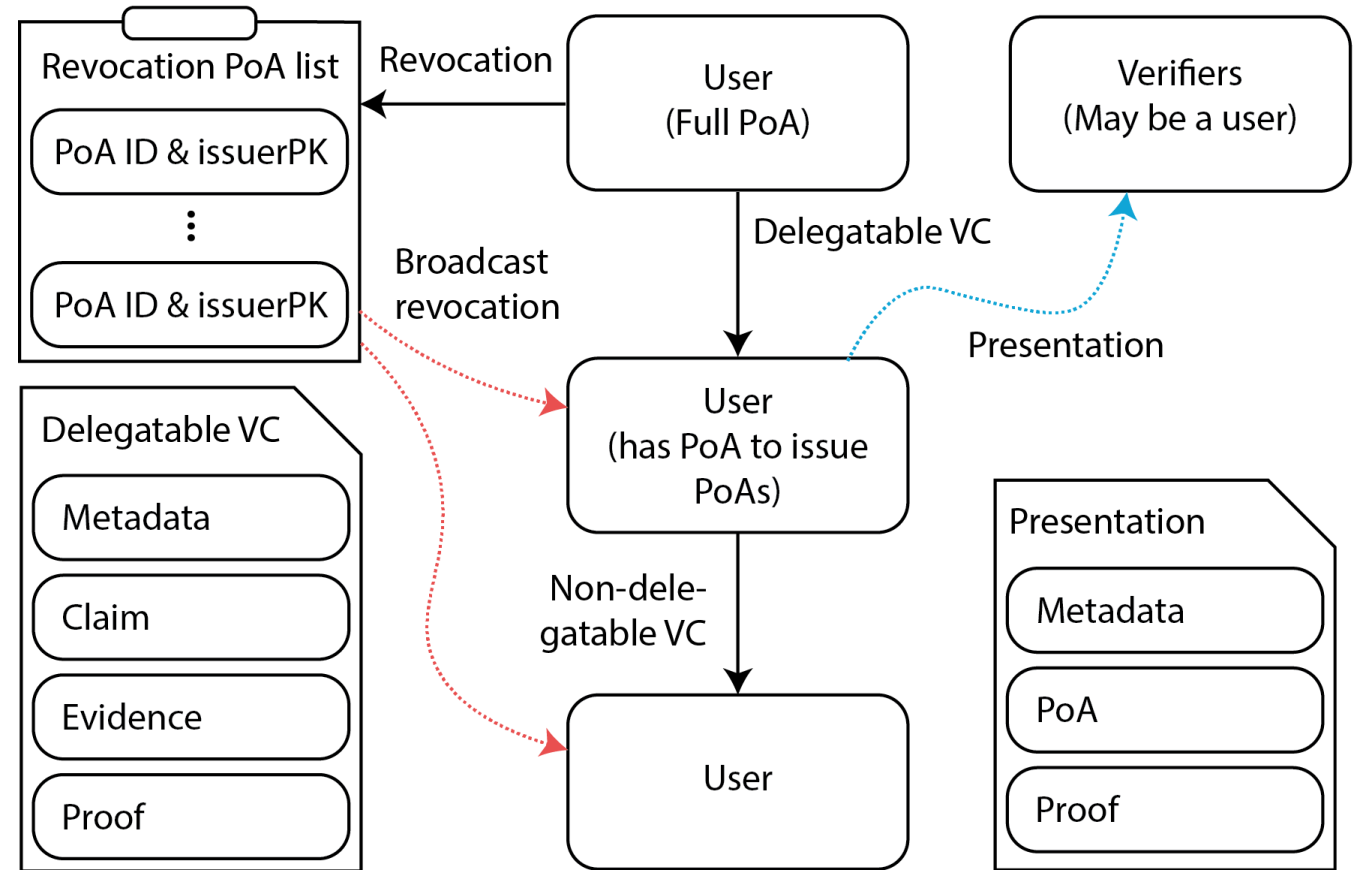
Design

Design

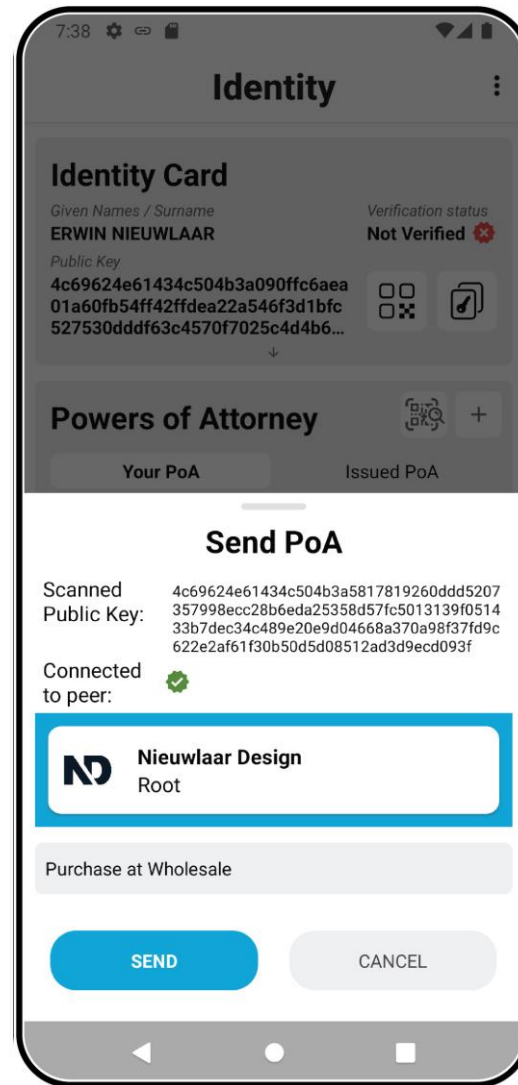# Design
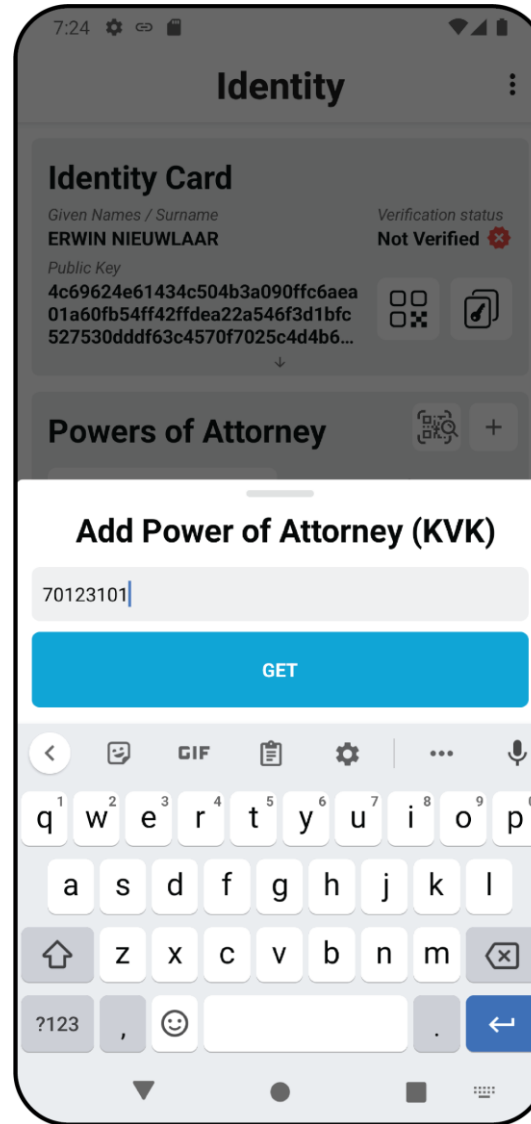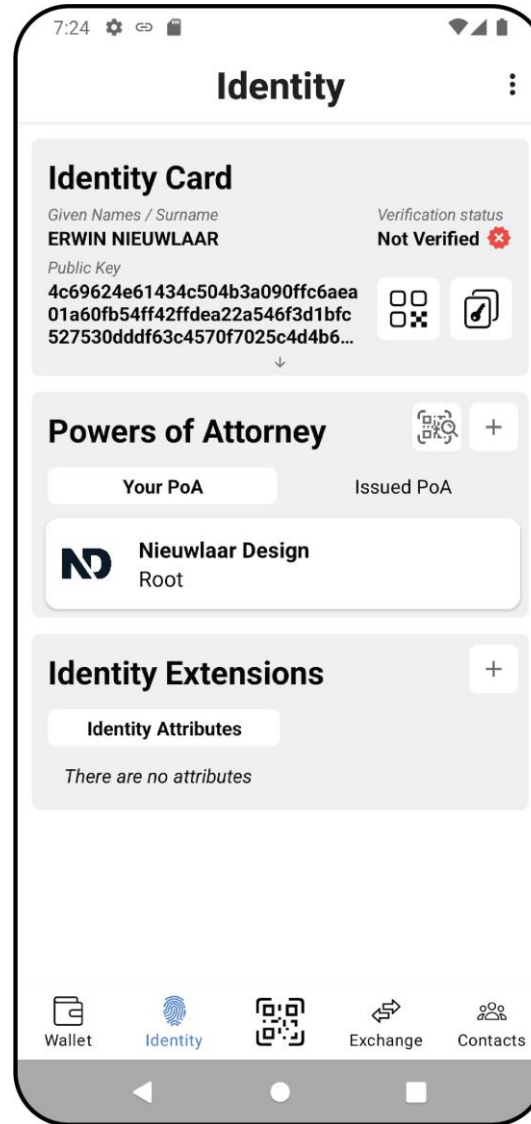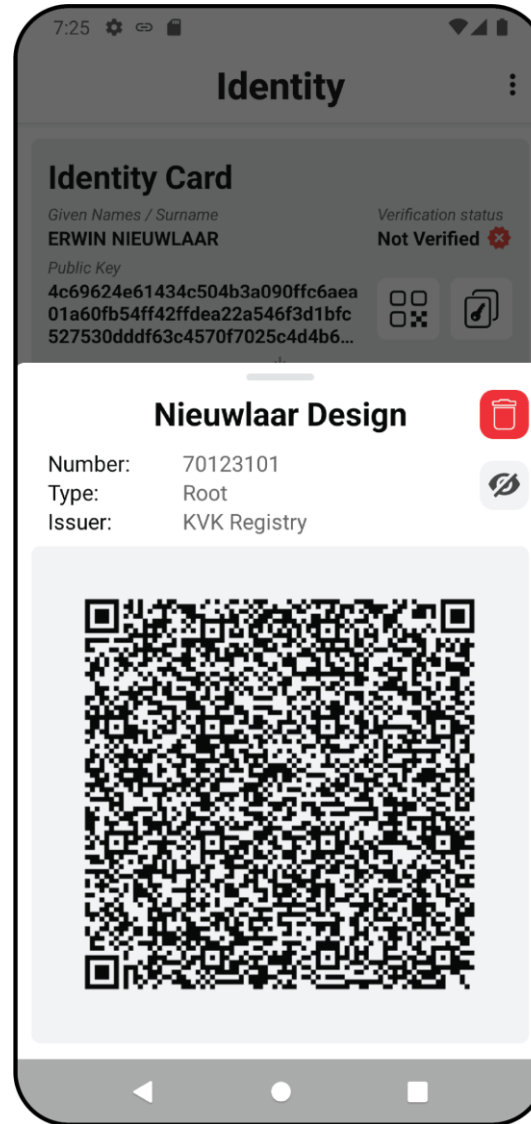
Design

Design

Design

Device 1

Device 2

Design

Device 1

Device 2

Design

Device 1

Device 2

Design

Device 1

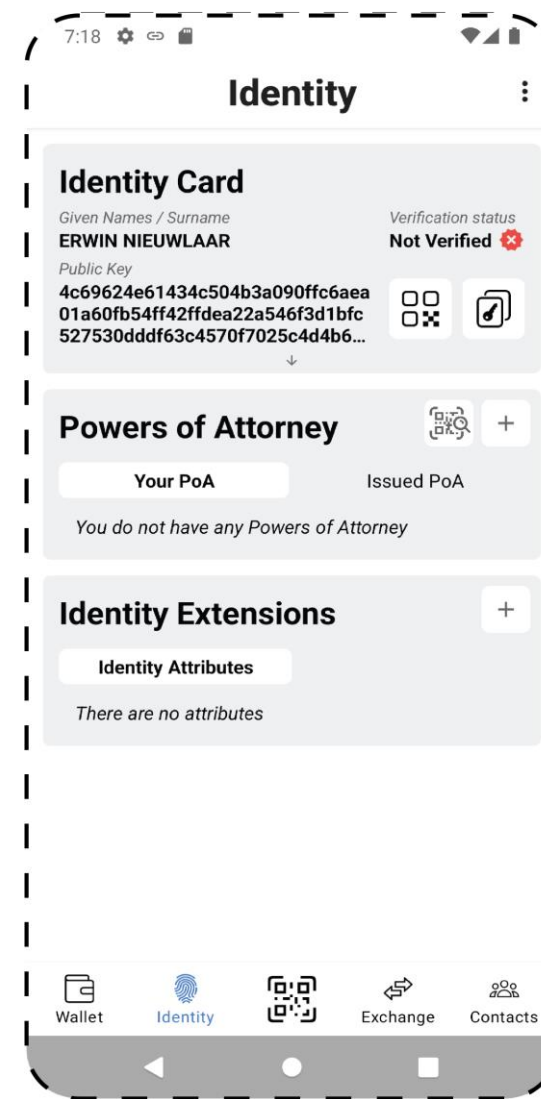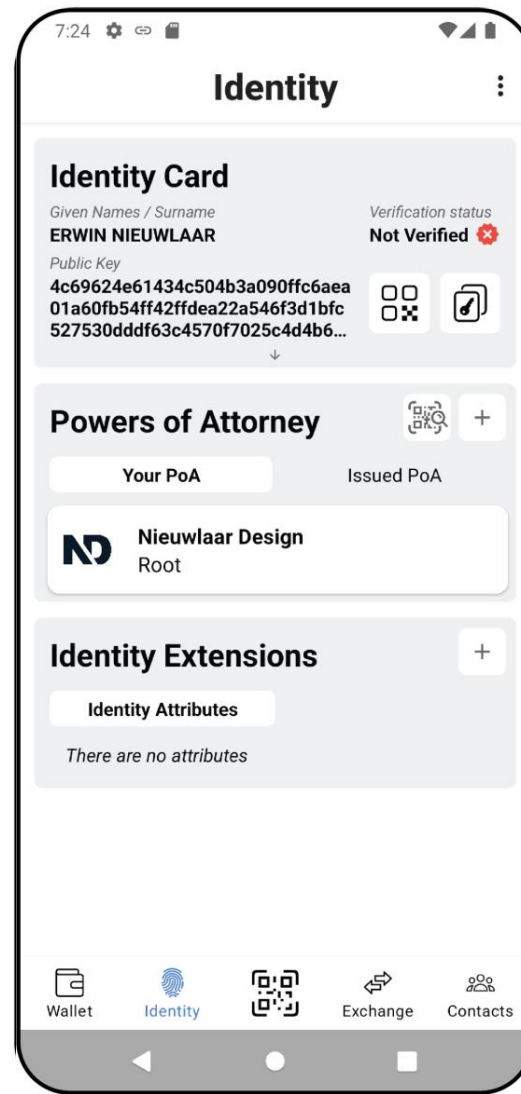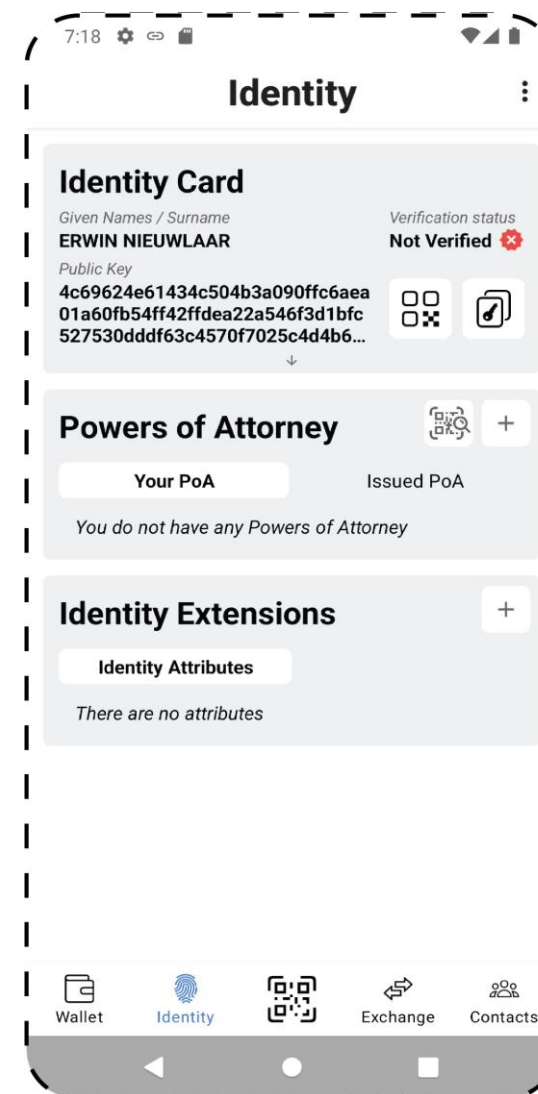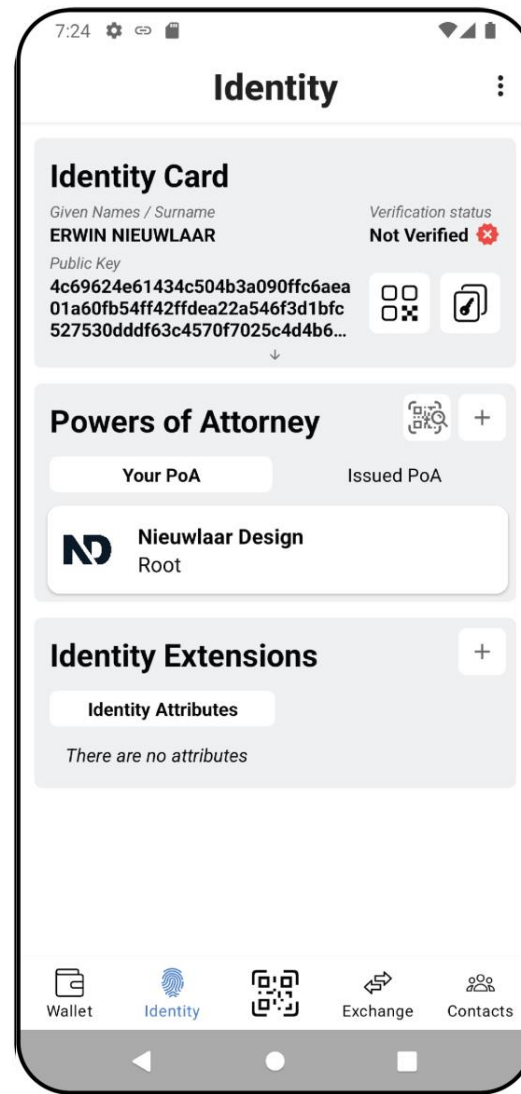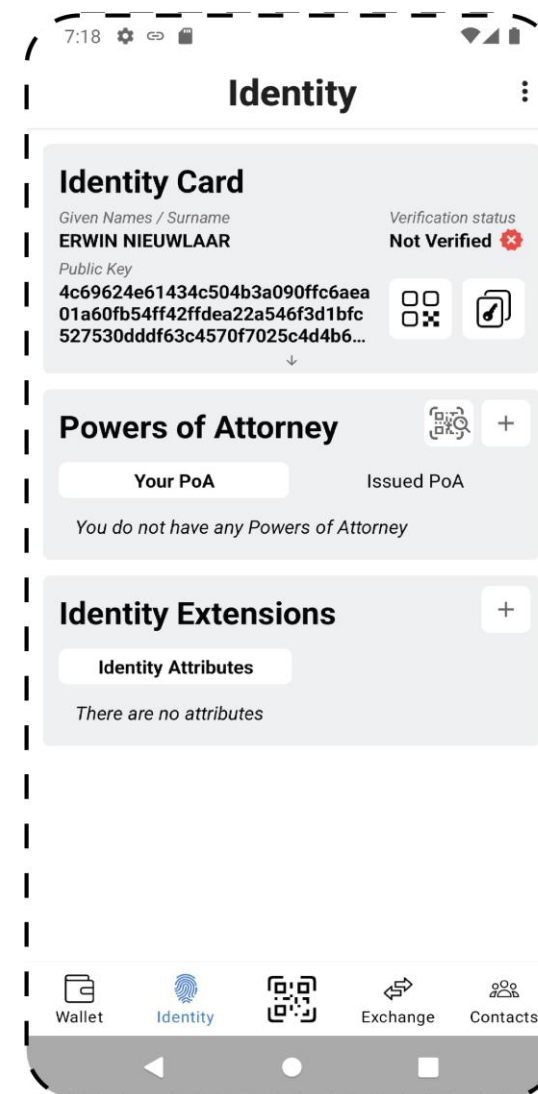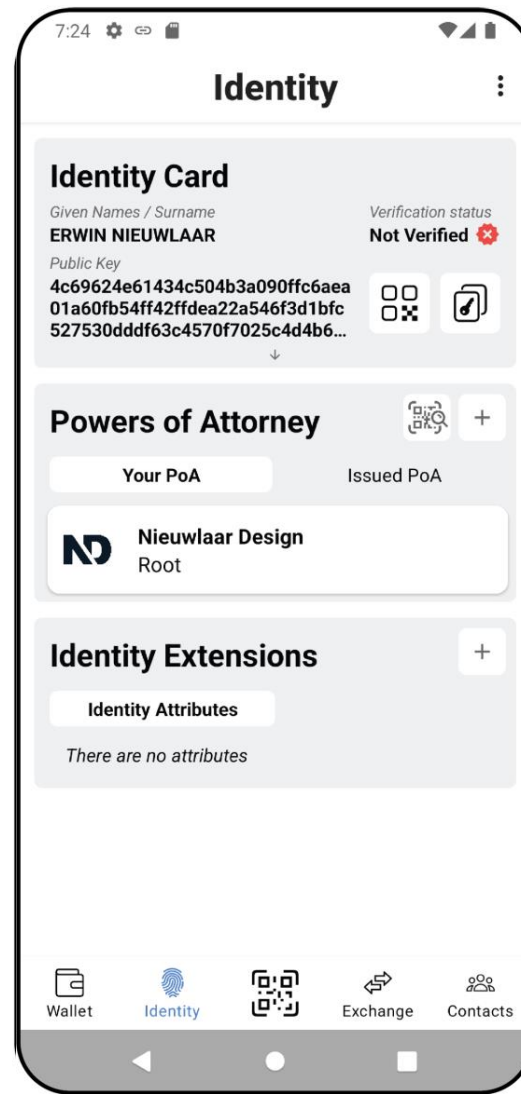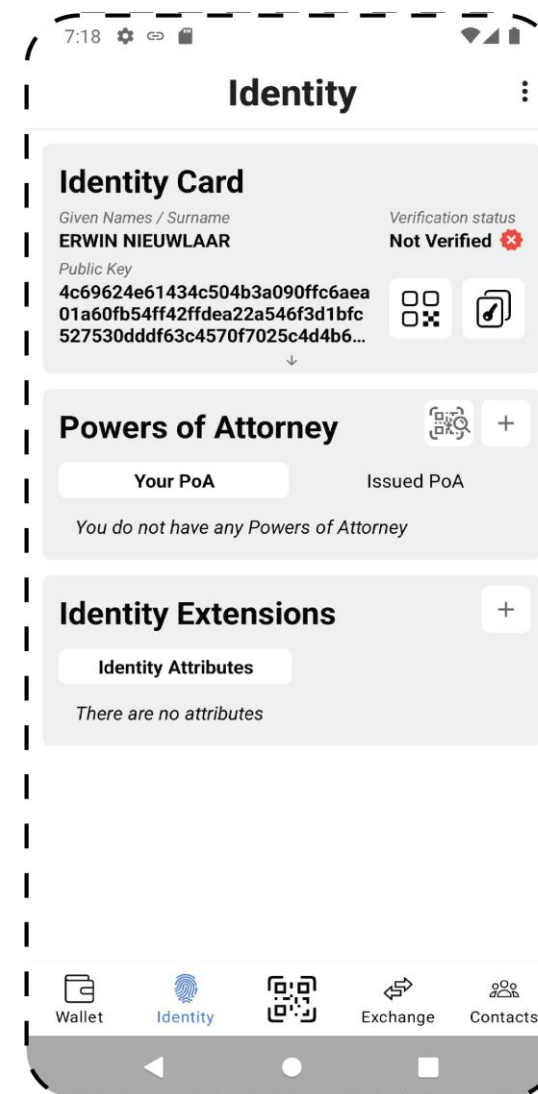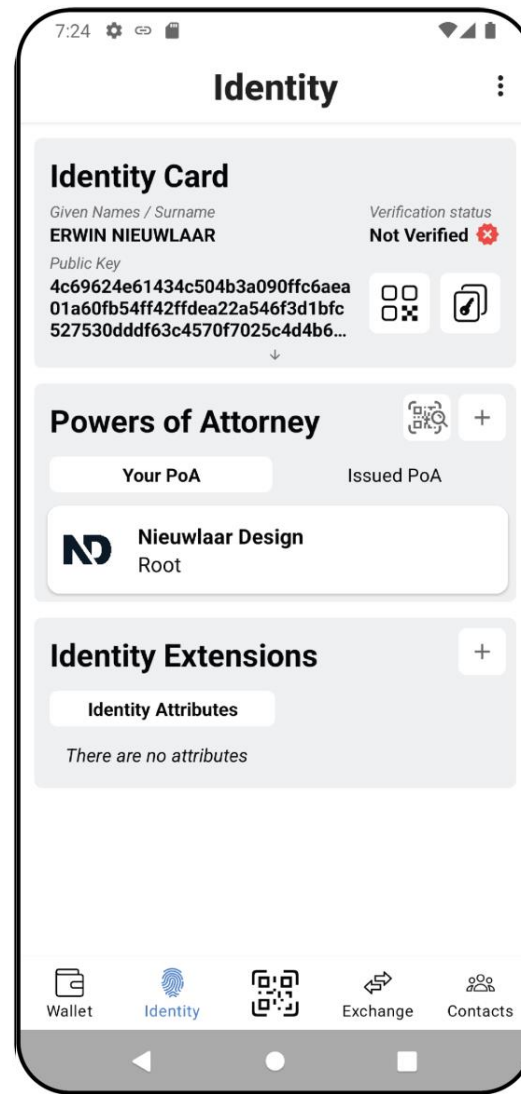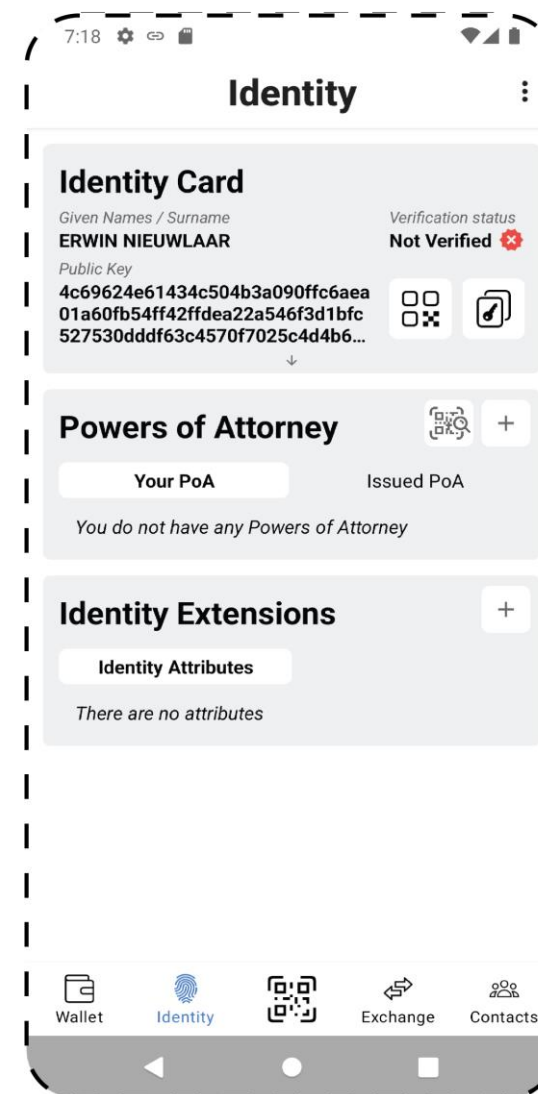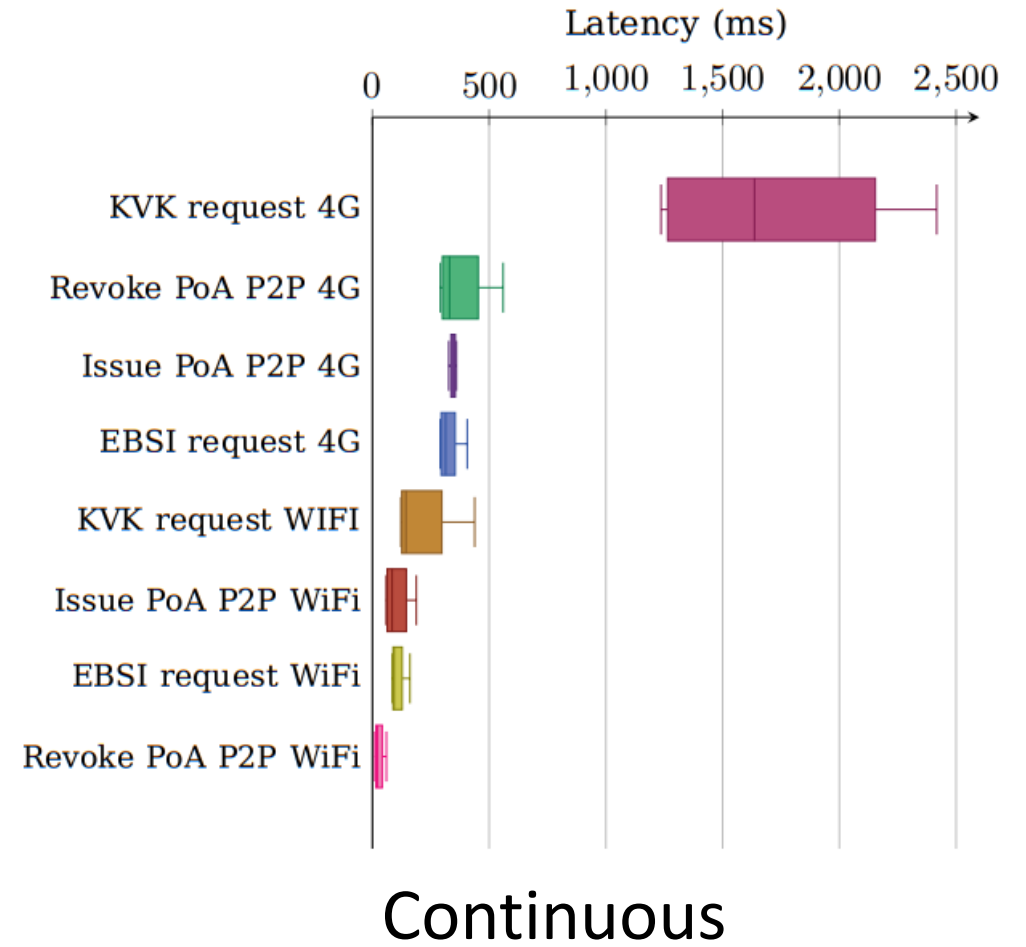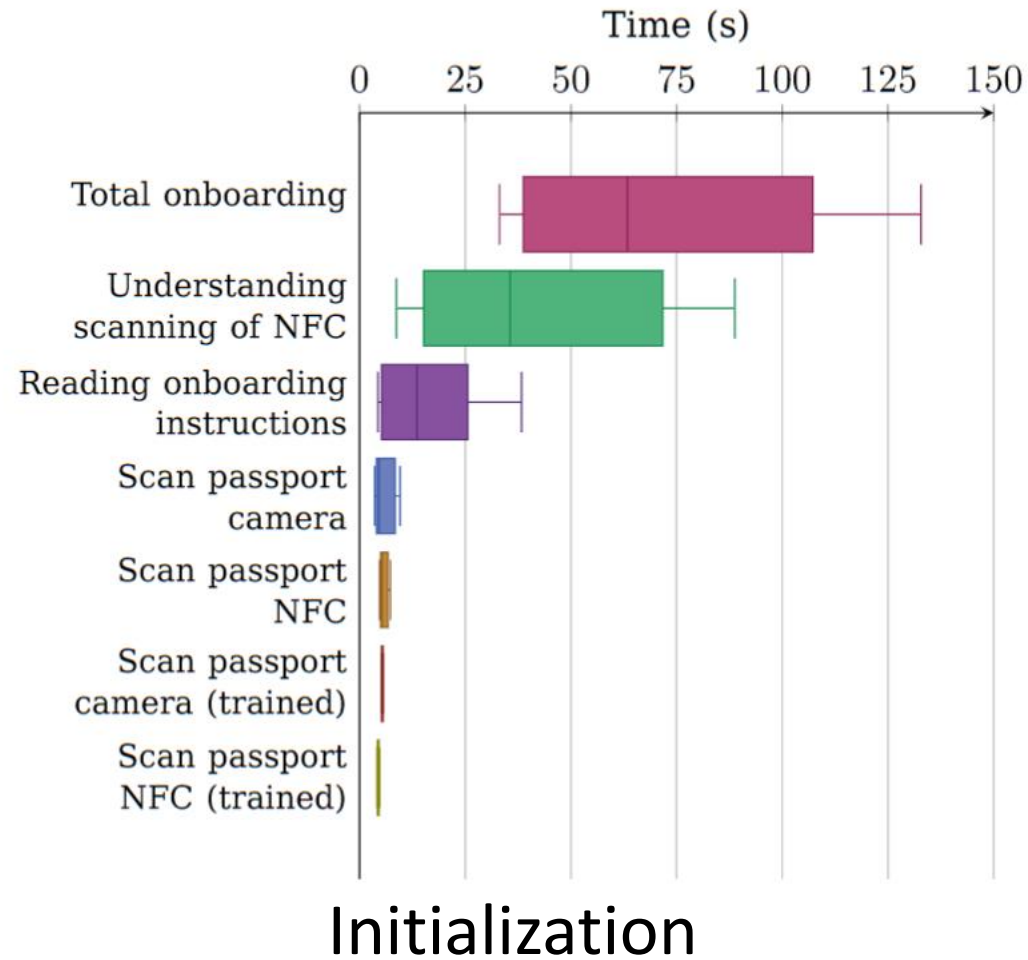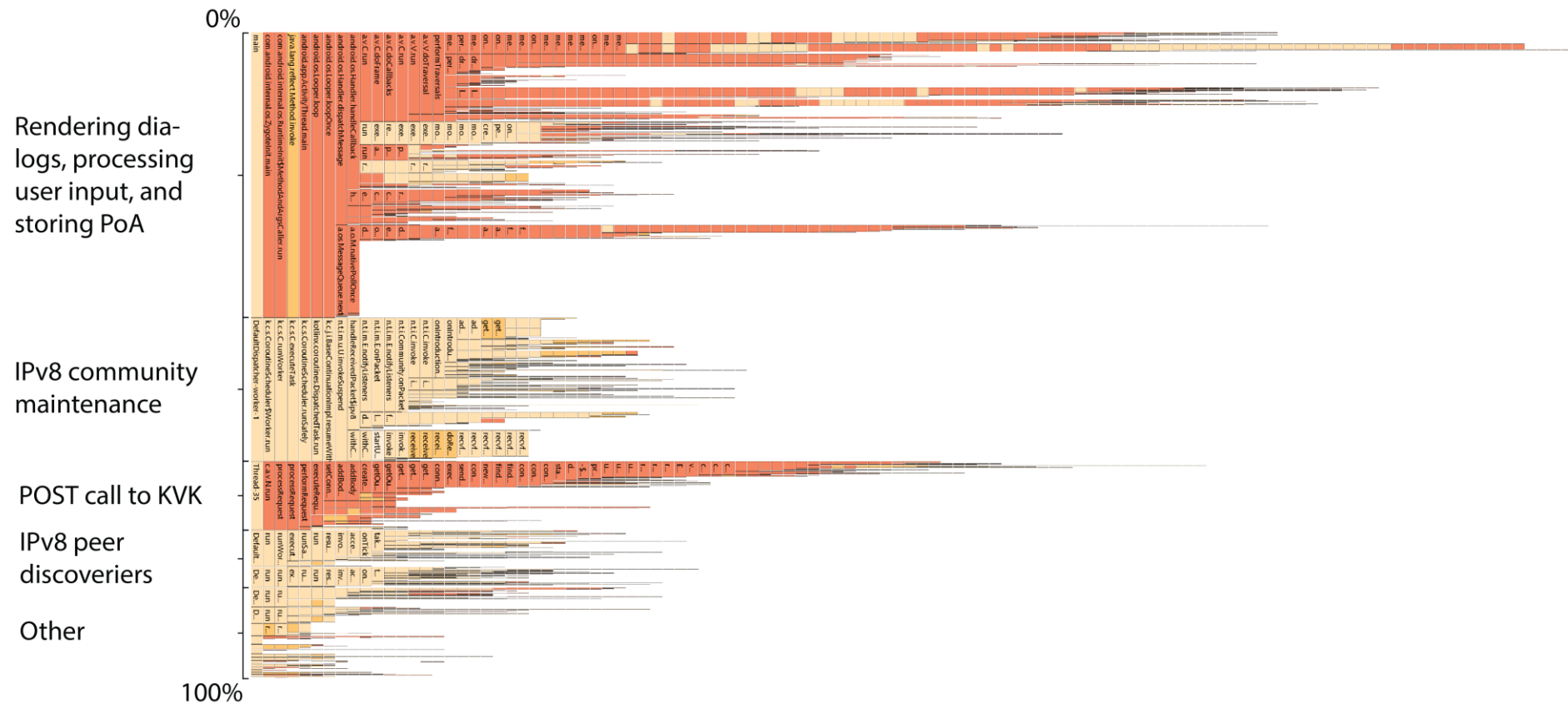Device 2

Design

Device 1

Device 2

Design

Device 1   Device 2

Performance Analysis

Initialization

Continuous

Performance Analysis

Flame chart, CPU usage (max. 35%)

Conclusion

- Scalable

- eIDAS compliant

- Cross-border (EBSI)

- W3C compliant

- Self sovereign

Future work