StudentVC X.509 Architecture with DIDs and Verifiable Credentials

PKI Infrastructure

Public Components:
- Root CA Certificate
- Intermediate CA Certificate
- University End-Entity Certs

Private: Certificate Private Keys

Verification Paths

Public Components:
- DID-based Verification
- X.509-based Verification
- Dual-Path Verification
- Certificate Revocation Lists

DID Infrastructure

Public Components:
- DID Identifiers
- DID Documents with X.509 Certificate Chains

Private: Verification Methods

Educational Institutions
- TU Berlin — did:web:edu:tu.berlin
- FU Berlin — did:web:edu:fu-berlin.de

Verifiable Credentials

Private: Certificate Private Keys
- TU/FU Berlin Credentials with X.509 certificate chains
- BBS+ Selective Disclosure — Privacy-preserving presentations
- Revocation Registry

Recipients
- Students, Employees, Alumni
- Student Wallet — Mobile app for credential storage and management

Private: Private Keys

OpenID Protocols

Private Component:
- OID4VC Issuance

Public Components:
- OID4VP Verification

Oprates · Issues · Stores · Manages · Uses for issuance · Uses for presentation

Public Data

Private Data