

TeleTrust-Konferenz

Berlin, 29.06.2023

Technische Eckpunkte der European Digital Identity Wallet (EUDIW) gemäß ARF

Dr. Torsten Lodderstedt, Tuconic

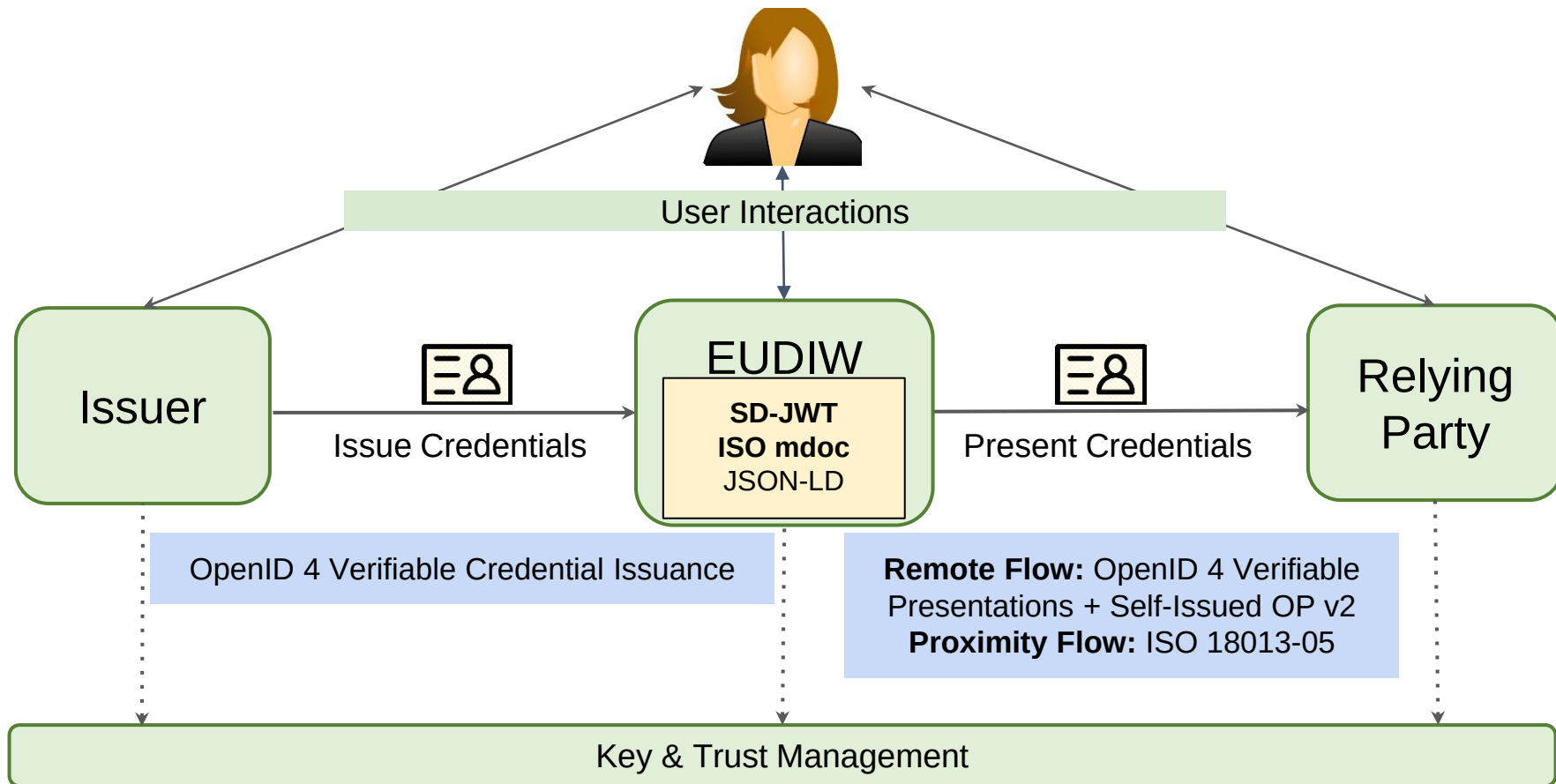
Was ist das ARF?

“The purpose of the document is to provide all the specifications needed to develop an interoperable EUDI Wallet Solution based on common standards and practices.”*

- Das ARF wird von Vertretern der Mitgliedstaaten und der Kommission entwickelt (Expert Group).
- Liegt aktuell in Version 1.1.0 vor

*<https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework>

Überblick



OpenID 4 Verifiable Credentials (OID4VC)

- Protokollfamilie für Wallet-basierte Anwendungen
 - Ausstellung und Präsentation von Credentials
 - Pseudonyme Authentifizierung mittels RP-spezifischem Schlüsselmaterial
- Sowohl auf demselben als auch zwischen unterschiedlichen Geräten
- Basiert auf OAuth2 (und dem Erfahrungsschatz von OpenID Connect)
- Multi-Format-Support (alle ARF-Formate können transportiert werden)
- Entwicklung bei der OpenID Foundation
- Spezifikationen, Issues und Pull Requests unter <https://openid.net/openid4vc>



Selective Disclosure for JWTs (SD-JWT)

- Weiterentwicklung von JSON Web Tokens (JWT) für selektive Weitergabe von Attributen
- Unterstützt etablierte Signatur-Algorithmen, wie ECDSA, damit ist Hardware-Binding möglich
- Unterstützt JAdES (z.B. long term validation)
- Einfach zu benutzen, breiter Open Source Library Support
- Entwicklung bei der IETF (OAuth WG)
- Spec, Issues und Pull Requests unter <https://github.com/oauth-libs/selective-disclosure-jwt>



ISO 18013-05

- ISO Standard für digitalen Führerschein
- Protokoll, Datenformat (mdoc) und Schema (mDL)
- Protokollnachrichten und Datenformat basieren auf CBOR (binäres Encoding)
- mdoc Format
 - unterstützt Selective Disclosure
 - unterstützt etablierte Signatur-Algorithmen, wie ECDSA, damit ist Hardware-Binding möglich
- Protokoll
 - Derzeit einziger verfügbarer Standard für Credential-Übertragung über Nahfeldkommunikation (NFC, BLW, Wi-fi Aware)
 - Datenübertragung Verbindungsaufbau über Nahfeldkommunikation auch über Server des Ausstellers möglich (Server Retrieval)
- Offizielle Publikation: <https://www.iso.org/standard/69084.html>



Technologies

Credential Format / Protocols	OpenID for Verifiable Credentials (Remote Flow)	ISO 18013-5 (Proximity Flow)
Selective Disclosure JWTs (SD-JWT)	○	×
ISO mdoc (ISO 18013-5)	○	○

- Person Identification Data (PID) müssen in beiden Formaten ausgestellt werden

Was muss noch ergänzt werden?

- Trust Model
- Schlüsselerwaltung
- Widerruf von Credentials
- Juristische Personen
- ...

Vielen Dank!