# Warum die Diskussion zur E-ID nicht technologisch sein sollte

Winterkongress 2022 - Digitale Gesellschaft

# Agenda

- Ein paar Worte zu mir
- Die (komplizierte) Diskussion
- Für was braucht es eine eID
- Was für IDs gibt es bereits
- Was sind Herausforderungen
- Was für Lösungsansätze gibt es
- Welche Lösung scheint sinnhaft

# Florian Forster

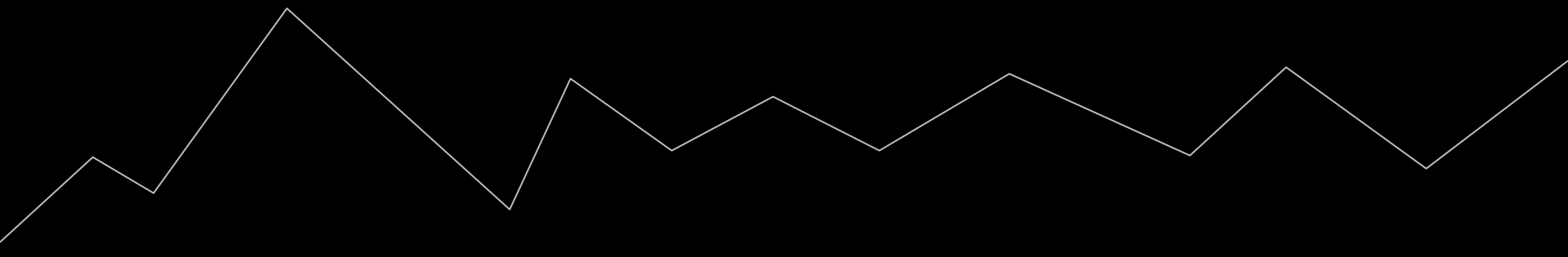
- Gründer & Partner eines Open Source IAM Herstellers
- IAM Architekt
- Ehemals Leiter Fachgruppe IAM vom Verein eCH
- Mitglied OpenID Foundation
- Ein bisschen Infosec nerd ;-)

# Bereit?

# Triggerwarnung:

**Enthält (viel) persönliche Meinungen**

# Die (komplizierte) Diskussion



# Wo klemmt es?

- Was soll die eID leisten
- Was ist mit dem Datenschutz
- Was ist mit der Sicherheit
- Wie einfach ist die Lösung
- Ausländische Anerkennung
- Einflüsse von Lobbies
- Legale Risiken (Haftung)
- Viel Halbwissen
- Technologie (Alb)Träume
- Inklusion von von allen Personen

# Für was braucht es eine eID?

## Oder auch nicht!

# Anwendungsfälle

- eGovernment
- Als Login für “alles”
- Altersnachweis beim Konsum
- Sammlung von Nachweisen

# Funktionalitäten

- Authentifizieren
- Identifizieren
- Nachweisen
- Signieren
- Verschlüsseln

# Frage

—

- Ist der zweck **primär** die Identifikation?
- Oder brauchen wir ein Ökosystem?

# Was für (e)IDs gibt es bereits?

—

- SuisseID
- SwissID
- Switch
- TrustID
- eIDAS*
- …

# Was sind die Herausforderungen?

# Herausforderungen

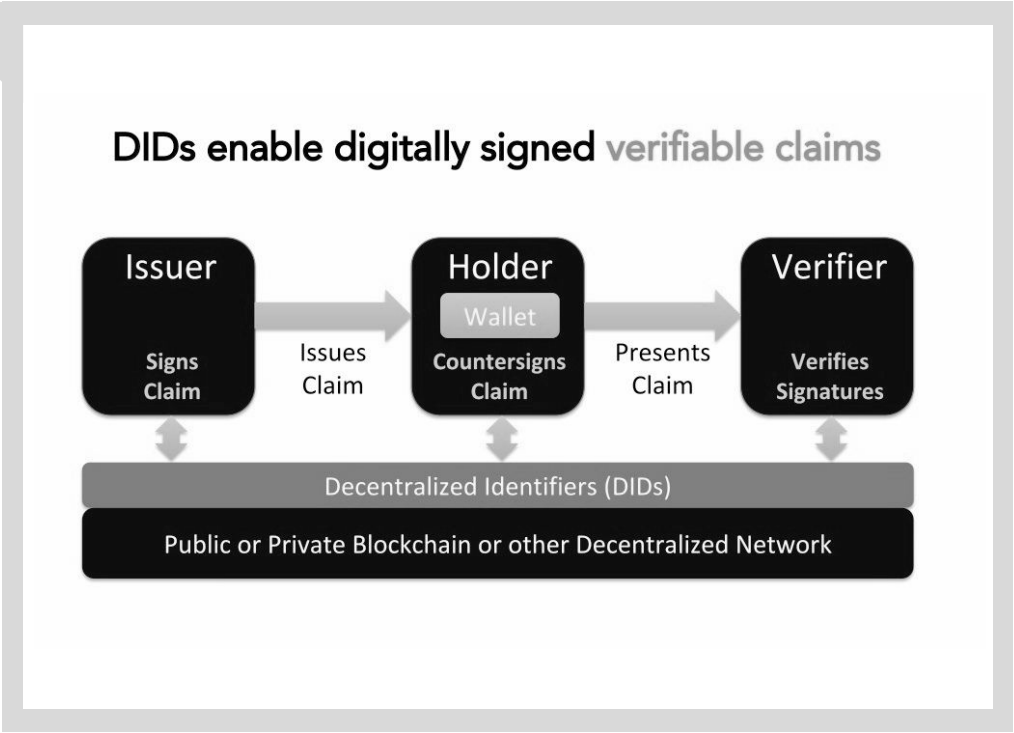
- Haftung
- Privacy
- Security
- Ease-of-use
- Ease-of-integration
- Akzeptanz (Marktverbreitung)

# Lösungsansätze & Technologien

# Verifiable Credentials (VC) & Decentralized identifiers (DID)

- Junge Technologie(n)
- Data Loss von Proofs ein Problem
- Grundlage teils SSI Implementierungen
- Verteilte Revokation ist nicht einfach

# VC & DID


DIDs enable digitally signed verifiable claims
Issuer
Signs Claim
Issues Claim
Holder
Wallet
Countersigns Claim
Presents Claim
Verifier
Verifies Signatures
Decentralized Identifiers (DIDs)
Public or Private Blockchain or other Decentralized Network

# SSI mit DLT (Blockchain)

- Recht auf vergessen bei PII
- Data ownership unklar
- Post quantum crypto Angriffe
- Threat Modelle (noch) unklar
- Maturität (noch) gering
- Client (meist) nicht Mitglied der chain
- Verlust von Nachweisen und VC als Challenge

# SSI ohne DLT

- Maturität noch gering
- Privacy besser als bei PKI
- Threat Modelle (noch) unklar
- Verlust von Nachweisen und VC als Challenge

# Public Key Infrastructure (PKI)

- Mature Technologie
- Bekannte Threat Modelle
- Key distribution als Herausforderung
- Mobile Support eingeschränkt
- Privacy durchzogen (je nach Anwendung)
- Kann vor MitM schützen (mTLS)

# Identity Provider (IdP)

- Mature Technologie
- Einfache Integration
- Bekannte Threat Modelle
- Privacy als Problem (Nutzungsdaten)
- Schutz vor Impersonation schwierig (Haftungsfrage)

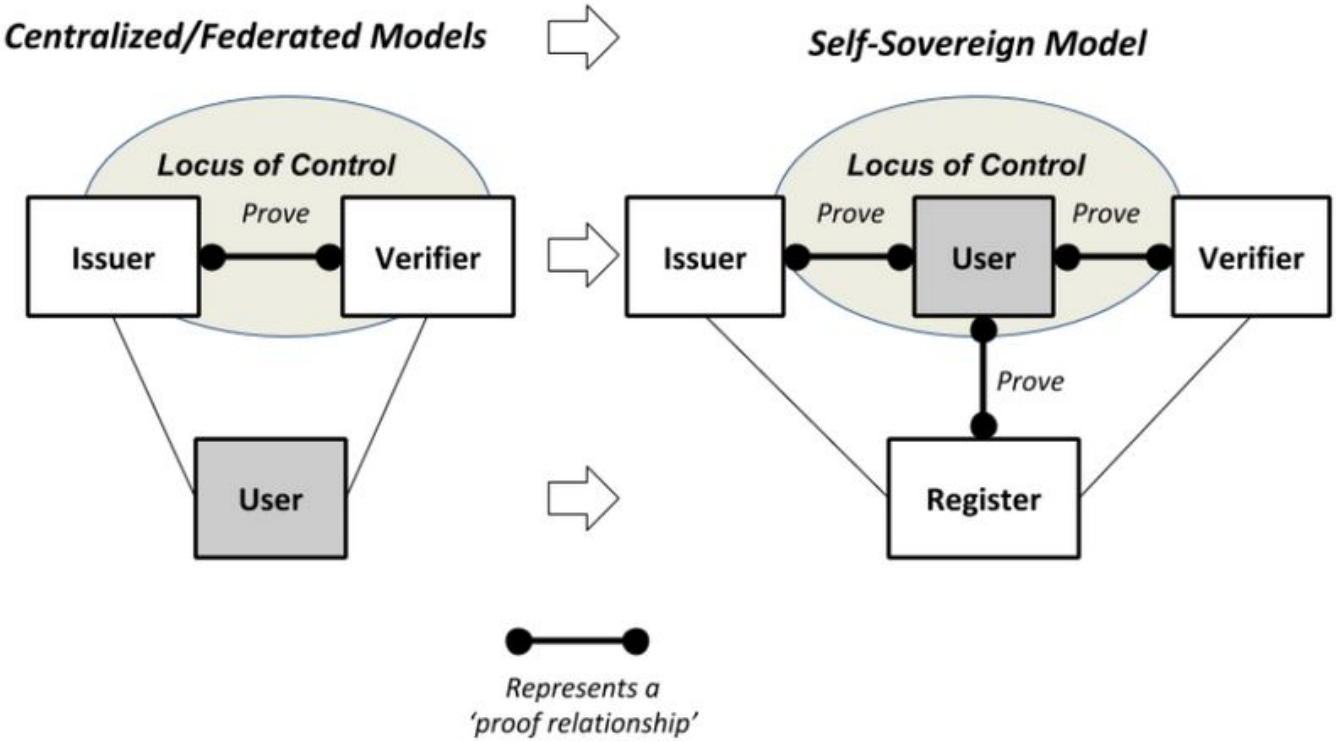
# Wallet vs. Server Architektur

**Wallet (Dezentral)**

- Ease-of-use noch unklar
- Potentiell “bessere” Privacy
- Security Platform abhängig
- Schutz vor Phishing unklar zzt.
- Technologien
  - SSI
  - SIOP
  - PKI

**Server (Zentral)**

- Bekannte Ease-of-use
- Privacy als grosse Herausforderung
- Impersonation als Herausforderung
- “Kann” vor Phishing schützen
- Technologie
  - Federation Protokolle




Old Model versus New Model

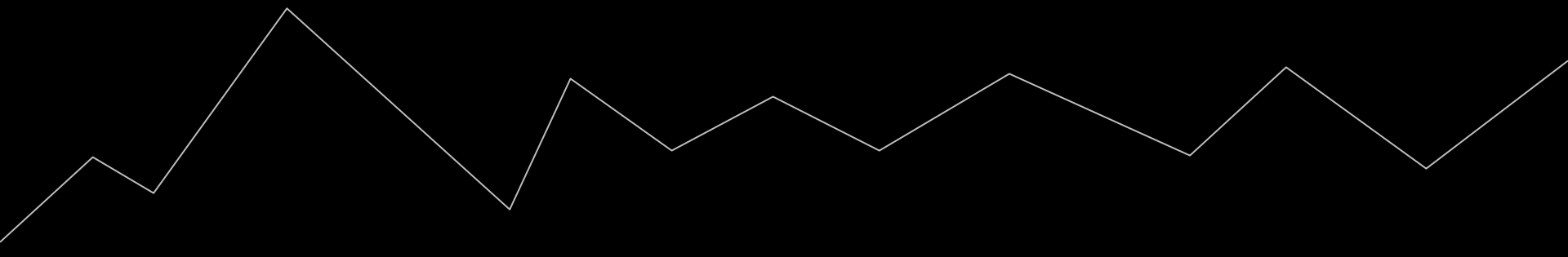
# Hybrid I
## Wallet und (Cloud) Backup

- Self-recovery bei Verlust oder Defekt des Wallets
  - Erhöhung der Angriffsfläche durch mehr Teilnehmer

## Hybrid II
### Wallet und Datenträger

- Self-recovery bei Verlust/Defekt des Wallets möglich
- Reduktion der aktiven Angriffsfläche mit Offline Datenträger

# Welche Lösung scheint sinnhaft?



# Kombination Ausweise (PKI) mit einem Wallet

- Self Enrollment mit Ausweis
- Hohe LoA mit dem Ausweis als Authenticator
- Tiefe LoA mit lokaler Biometrie oder Pin
- Vorerst verzicht auf VC / DID
- Reine Nutzung als Personen Identifikationsmittel

Phishing verbleibt ein Problem.
Besonders bei Nutzung über mehrere Geräte (Zum Beispiel mit QR-Code)

# Warum die Diskussion zur E-ID nicht technologisch sein sollte

Weil die Anforderungen unklar sind!

# Fragen?