Unlinkability beim Vorweisen einer E-ID

Challenge Owner
Jonas Niestroj

Challenge Participants
Nicolin Dora
Christian Ulbrich
Abidin Vejseli

Herausforderungen

- Anonymität im Internet gewährleisten
- Datensammlungen präventiv verhindern

Unsere Challenge

- Mögliche Ansätze studieren
  - BBS (Boneh, Boyen, and Shacham)
  - Zwischen Layer
  - EU-Lösung
  - Klassische asymmetrische Crypto

Ergebnisse

- BBS – Knacknuss Hardware Support
- EU–Lösung – Neue Herausforderungen
- Zwischen Layer – SPOF
- Klassische asymmetrische Crypto - Pubilc Key (Trackbar)
- PoC Aufgebaut mit dem BBS-Ansatz