Zentrale vs. dezentrale PKI für SSI / eIDAS 2.0 – welche Ansätze brauchen wir für nutzerfreundliche wie sichere digitale Identitäten?

Tutorial auf der Omnisecure 2023

Berlin, 24. Mai 2023

Dr. Dominik Deimel, comuny

Steffen Schwalm msg system AG

.msg

comuny
Empowering Personal Data

Wie müssen technische Architekturen gestaltet werden, um Regulatorik, Anspruch der Usecases und technische Möglichkeiten zusammenzubringen?

- Compliant zum ARF
- Flexibel, um neben eIDAS 2.0 auch branchenspezifische Vorgaben zu erfüllen (z.B. Payment, Travel, Health, Government)
- Offen für die Nutzung durch natürliche wie juristische Personen (mobile Wallet, Cloud Wallet)

- Offen in der Attribute Gestaltung, um vielfältige Anwendungsfälle zu ermöglichen
- Flexibel, denn wir werden eine sanfte Migration hin zu eIDAS 2.0 erleben
- Button up statt Top down gedacht, um digitales Prozessdesign in Entwicklung regulatorischer Vorgaben zu integrieren

.msg

COMUNY
Empowering Personal Data

Wie lassen sich die Anforderungen des Architecture Reference Framework zur EU ID Wallet für den breiten Ausbau digitaler Identitäten nutzen?

- Mitgliedsstaaten auch private Wallets zulassen (gegen Vorgaben ARF durch eine CAB zertifiziert)
- Mitgliedsstaaten ihr EUDIW an jeden EU-Bürger herausgeben können
- Neben Type 1, vor allem auch Type 2 möglich ist (EAA)
- Ergebnisse der LSP hinsichtlich Anwendung + Interoperabilität berücksichtigt werden

- Neue, offene Standards fordern aber Migrationsweg zulassen
- ARF als technische Leitlinie für alle Wallet-basierte Ansätze im Identitätsmanagement ansehen
- Bandbreite des Vertrauensniveaus in unterschiedlichsten Anwendungsfällen berücksichtigen

.msg

COMUNY
Empowering Personal Data

Haben etablierte zentrale PKI bzw. neue dezentrale PKI (wie z.B. Blockchain basierte Ansätze) die gleiche Berechtigung bei der Umsetzung digitaler Identitäten in Europa?

- Ja, solange Zertifizierungen für EUDIW, (qualifizierte) Vertrauensdienste erfolgreich nachgewiesen werden
- Ja, da dezentrale PKI nicht zwingend DLT bedeutet
- Ja, da Privacy durch GDPR & Relying Party bestimmt wird, wesentlich ist Erfüllung regulatorischer Vorgaben im Anwendungsfall (Banking, Public etc.)

- Ja, wenn Mehrwert von dezentraler PKI gegenüber etablierter Trust Standards nachgewiesen werden kann
- Ja, wenn hierdurch am Ende Privacy und Selbstbestimmung wirklich umgesetzt werden
- Ja, wenn Zugang und Anpassung bei Verwendung dezentraler PKI für die Akteure im digitalen Ökosystem einfach umsetzbar wird

.msg

COMUNY
Empowering Personal Data

Vielen Dank für Ihre Aufmerksamkeit !

Steffen Schwalm
Principal Business Consultant
msg security advisors
Mail: steffen.schwalm@msg.group
Mobil: +49 162 280 64 72

Dr. Dominik Deimel
CEO / Gründer
comuny GmbH
Mail: dominik.deimel@comuny.de
Mobil: +49 160 5858 447

Empowering Personal Data