

TeleTrust-Konferenz

Berlin, 29.06.2023

**Das EU-Digital Wallet - der Schlüssel für (rechts)sichere
dezentrale Identitäten in Europa? SSI zwischen ARF, eIDAS
2.0 und Large Scale Pilots**

Steffen Schwalm, msg security advisors, c/o EWC

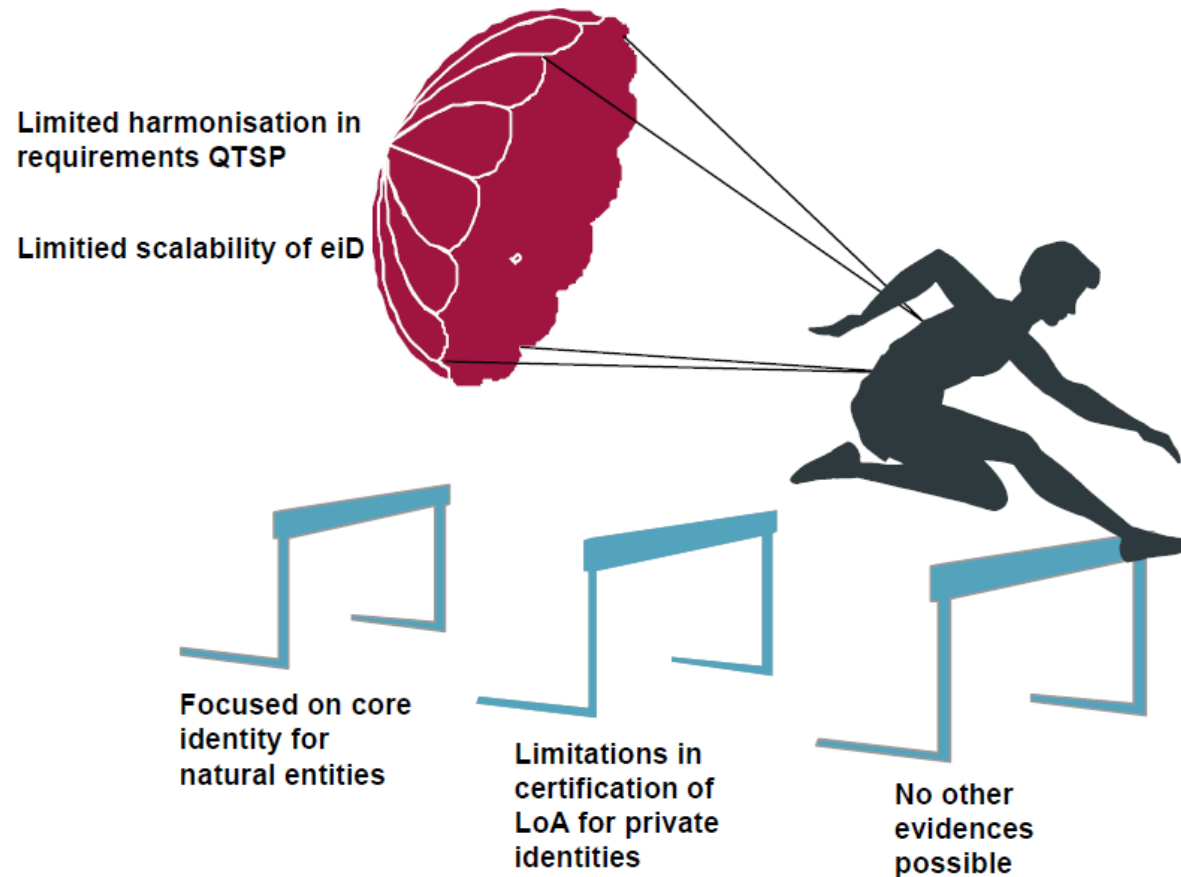
1. Status quo eIDAS 1.0 und Grenzen von SSI

2. EUDIW between ARF and Large Scale Pilots – Anforderungen und UseCases

3. Challenges und offene Punkte in ARF und LSP

4. Outlook

Der enge Fokus von eIDAS 1.0 auf die Kernidentität sowie mangelnde Harmonisierung der Anforderungen an QTSP führte zu starker Fragmentierung des Marktes und Wettbewerbsnachteilen



Impact in Germany and Europe

Missverhältnis von Security und Useability führte zu limitierter Nutzung eID in D

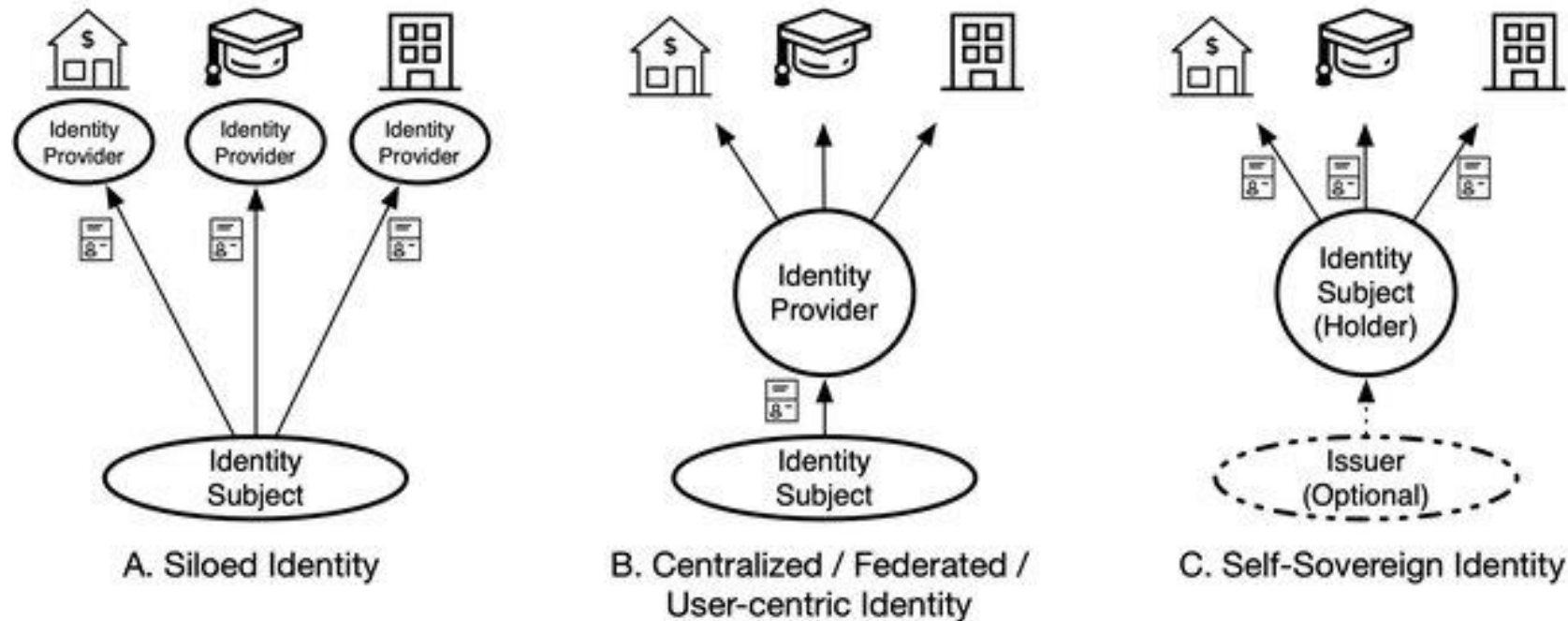
Heterogene Anforderungen an QTSP führte zu Wettbewerbsnachteilen und mangelnder Nutzung

Europ. Standards fördern Interoperabilität und Nutzung

TrustList ermöglichte Transparenz und nachweisliches Vertrauen für Vendors und Nutzer

Fokus auf Kernidentitäten beschränkte voll-digitale Transaktionen

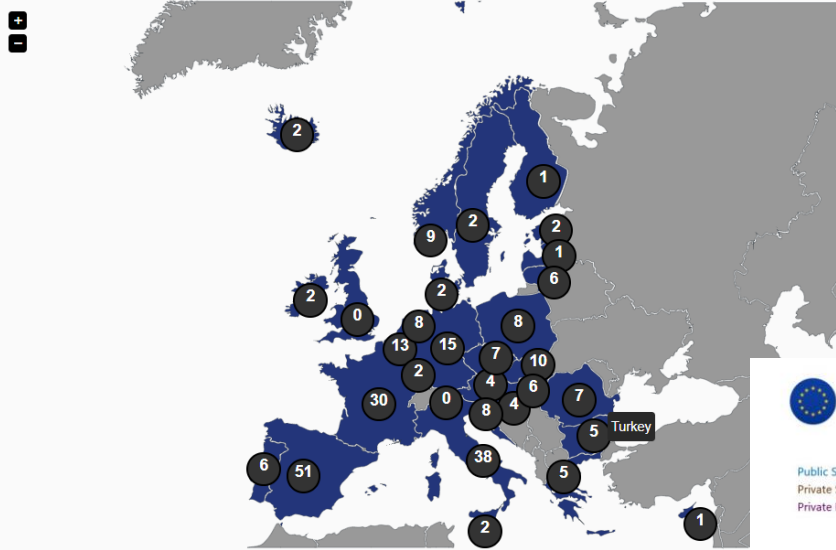
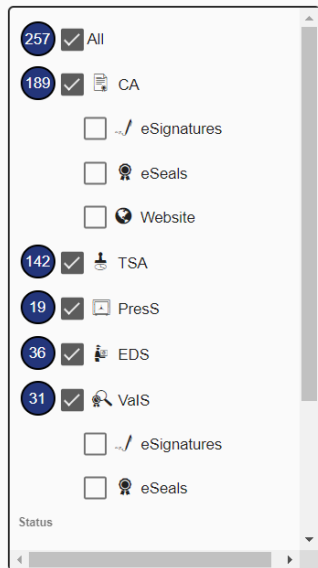
There's no trust by default or self-declaration – die Grenzen des aktuellen SSI-Approaches



Source: H. Yildiz et. al.: "Connecting Self-Sovereign identity with federated and User-Centric identities via SAML integration," in 2021 IEEE Symposium on Computers and Communications (ISCC) (IEEE ISCC 2021), Sep. 2021

Wenn es keine vertrauenswürdigen Dritten gibt, der nachweislich sichere PID, Wallet, Attestations ausstellt – woher kommt Legal Trust?

(qualifizierte) Vertrauensdienste werden europaweit eingesetzt – ihre Integration ins eIDAS 2.0 Ökosystem ist essentiell für den Erfolg des EUDIW

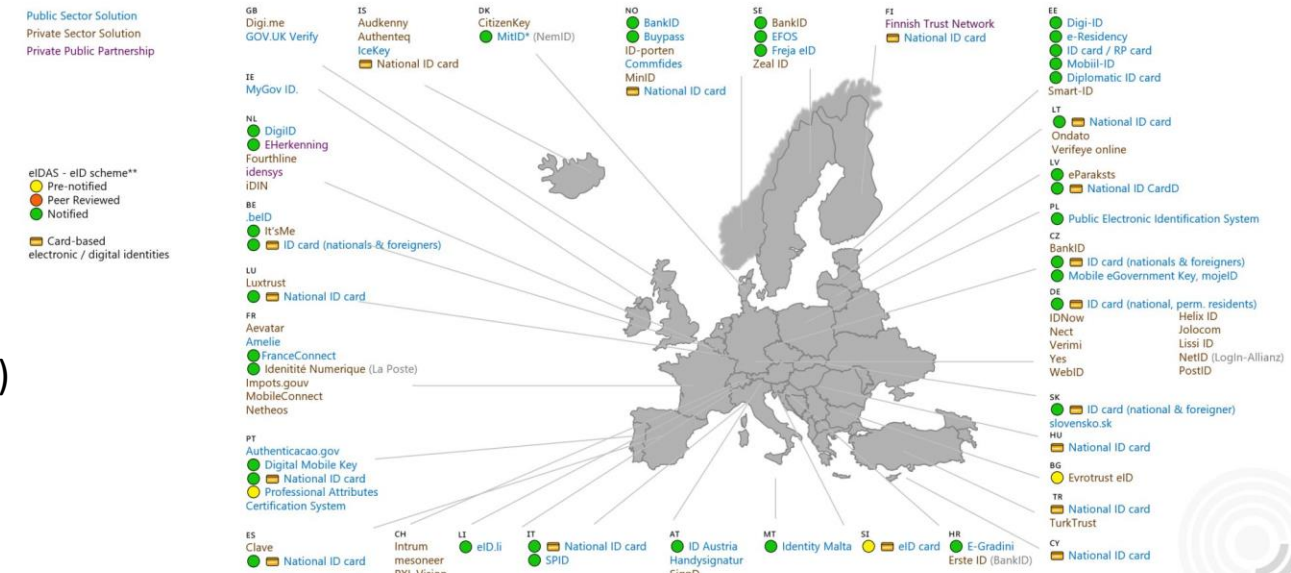


- > 250 (Q)TSP in Europe
- All Trust Services provided
- Especially QES/Qseal widely used
- Adoption and interoperability by eIDAS 2.0 needed for wide utilization of EUDIW

Source: goeIDAS e.V. c/o ecsec GmbH

- Notified eID in nearly all member states
- Further eID Means established and widely used
- Adopted by several regulations (AML, Health, Insurance etc.)
- Adoption and interoperability by eIDAS 2.0 needed for wide utilization of EUDIW

Landscape Remote ID Proofing & Digital Identity



Last update: February 6, 2023 © Joerg Lenz Namirial ; Information provided without guarantee for accuracy and completeness of data displayed; for clarity reasons organizations are only listed in their home / main country
 * Source: Namirial Research and European Commission - eID User Community: Overview of (pre-)notified eID schemes (i.e. those that can be used across national borders thanks to their integration with the eIDAS network) <http://bit.ly/eIDASchemes-eIDAS>

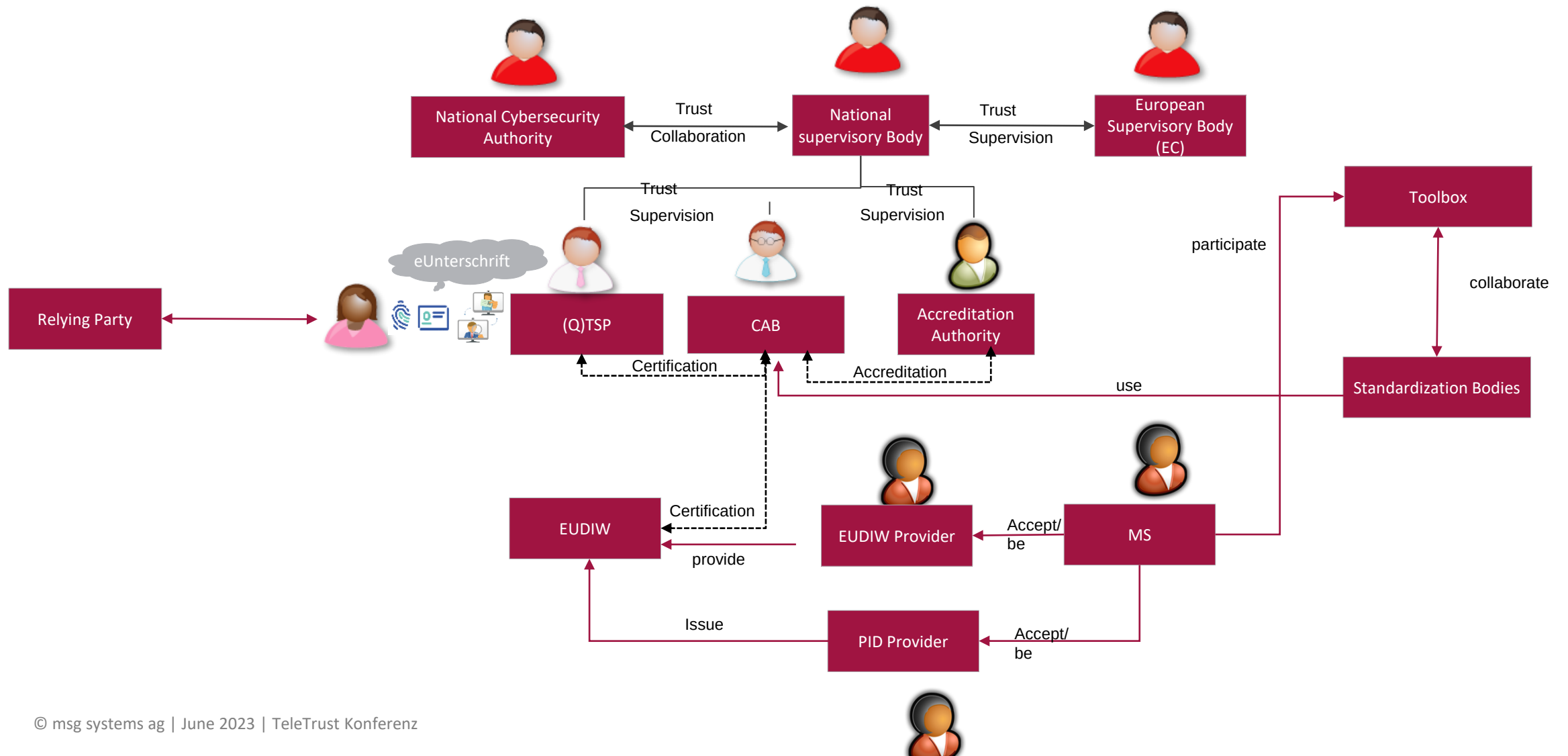
1. Status quo eIDAS 1.0 und Grenzen von SSI

2. EUDIW between ARF and Large Scale Pilots – Anforderungen und UseCases

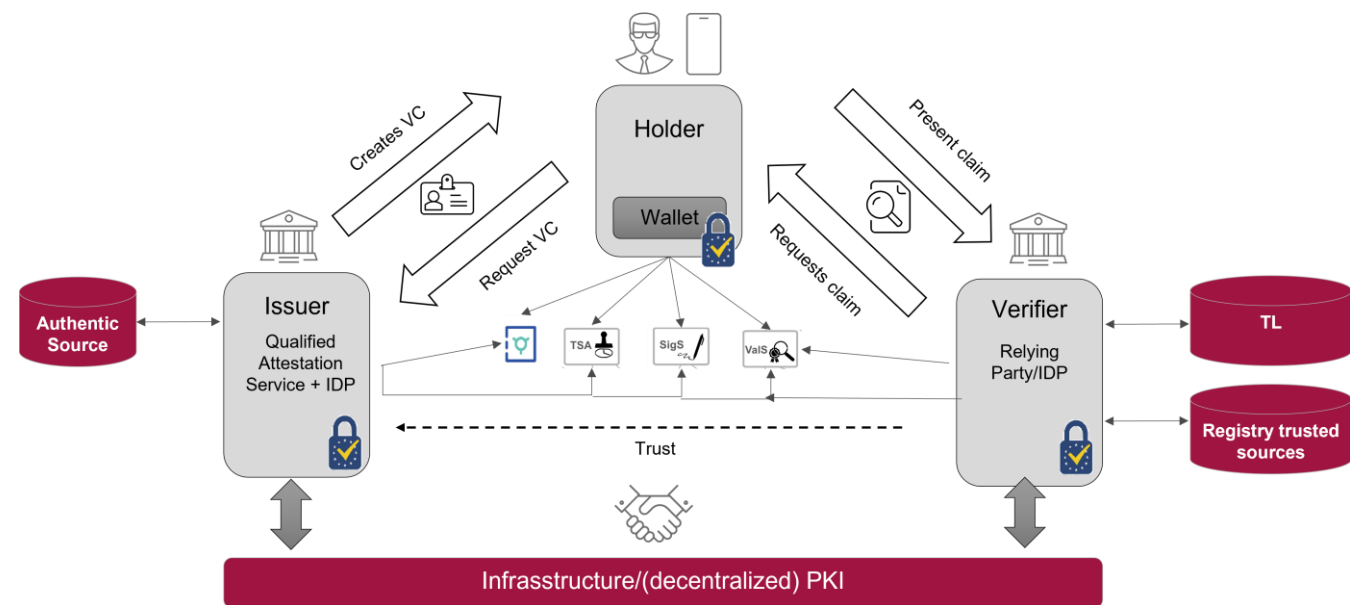
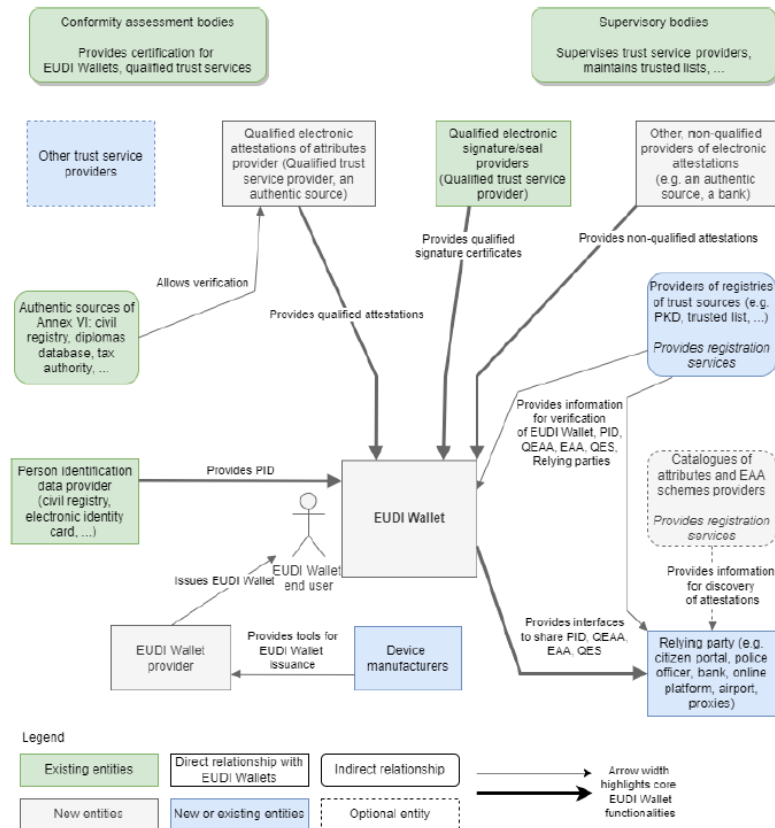
3. Challenges und offene Punkte in ARF und LSP

4. Outlook

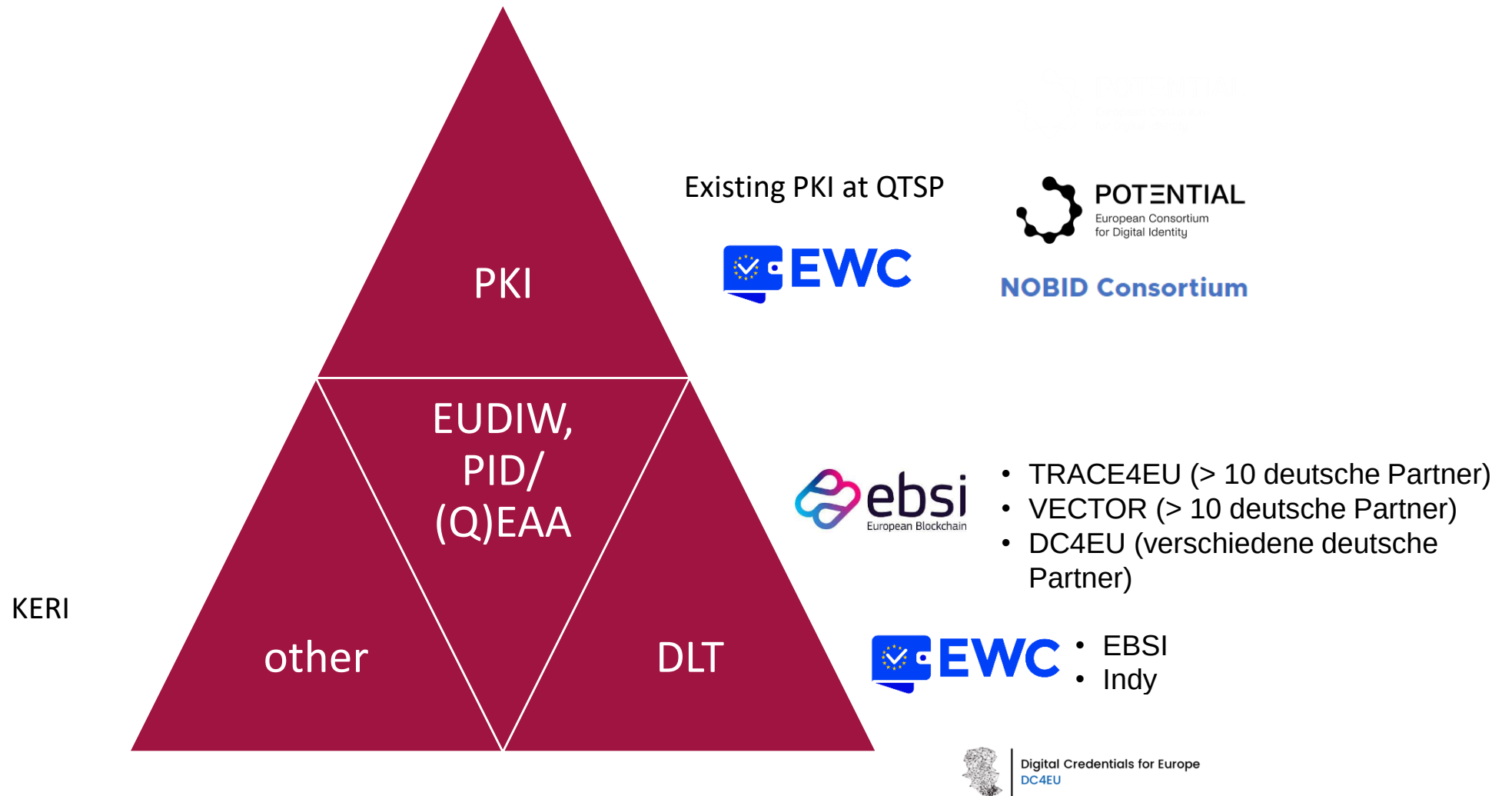
Trust Model and interaction in a nutshell



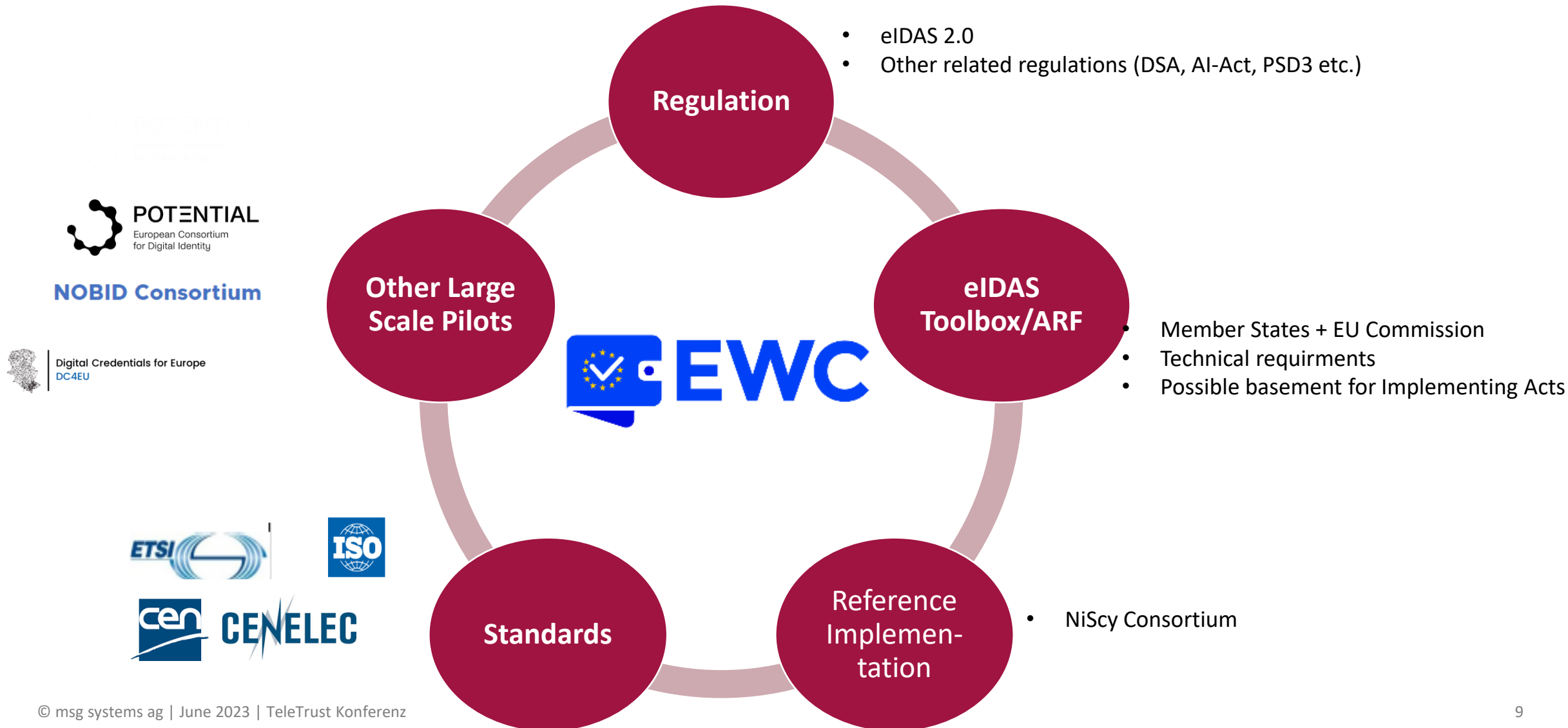
eIDAS 2.0 enables ermöglicht vertrauenswürdige dezentrale digitale Identitäten durch Integration von SSI ins eIDAS Ökosystem



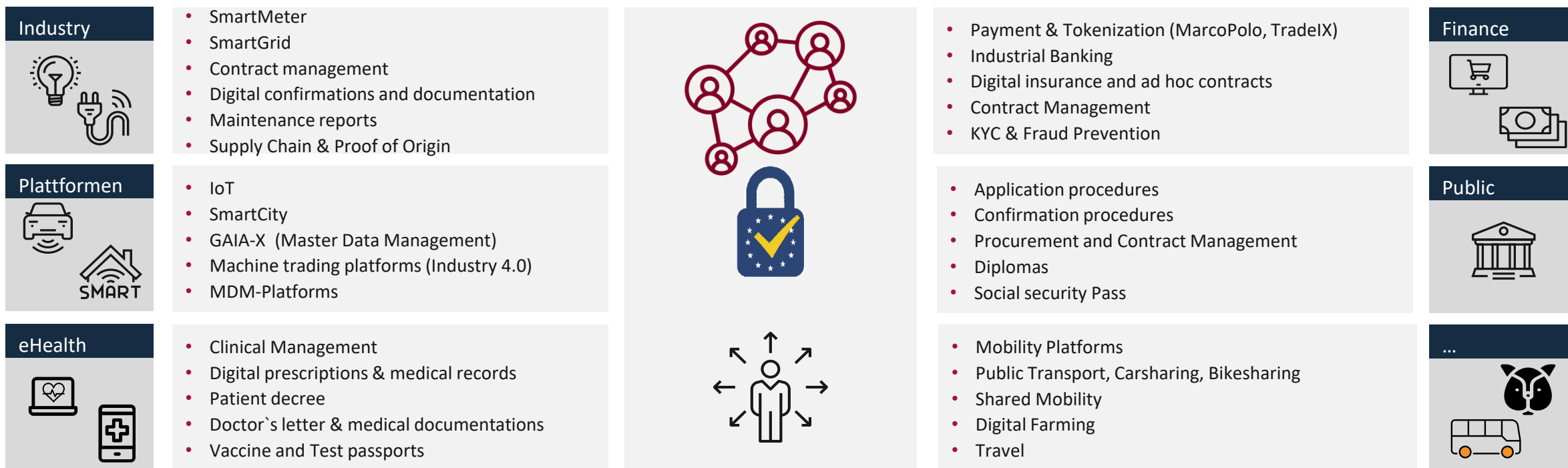
Das ARF beinhaltet de facto keine Verbote hinsichtlich der Infrastruktur für EUDIW, PID oder qualified attestations of attributes – wann ermöglicht Deutschland sichere DLT-Nutzung?



Die Interaktion von Regulierung, Toolbox, Reference Implementierung, Standardisierung und Large Scale Pilots ermöglicht Etablierung nutzerfreundlicher wie interoperabler Lösungen fürs EUDIW



Attestation of Attributes complements digital identities with the necessary evidences



How to ensure burden of proof and documentation requirements for retention periods of 30, 60 or more years?

1. Status quo eIDAS 1.0 und Grenzen von SSI

2. EUDIW between ARF and Large Scale Pilots – Anforderungen und UseCases

3. Challenges und offene Punkte in ARF und LSP

4. Outlook

Gaps und Issues

- Fokus auf ISO mDL und mDoc in Referenz-implementierung (und Diskussionspapier des BMI) limitiert Anwendungsfälle
- Konkreter Ausstellungsprozess PID & QEAA unklar
- SD-JWT & W3C entwickeln sich auseinander, mit potenziell kritischer Auswirkung auf Anwendbarkeit W3C Data Model

Security und Data Sovereignty

- Datensouveränität mit nichteurop. Hardware?
- Massentauglichkeit von PID im Secure Element
- Anforderungen an HSM für Schlüsselerzeugung und Korrelation mit QTSP
- Sicherheitsanforderungen an EUDIW, QEAA und Zertifizierung

Marktfähigkeit und Nutzbarkeit

- Integration notifizierter eID und eIDAS Nodes
- Abbildung Organisationsidentitäten und Wallet für Organisationen
- Auswahl authentic sources
- Integration bestehender QTSP

Trust Services and Signatures

- Integration bestehender QTSP
- Integration bestehender Formate, Standards und kryptographischer Vorgaben
- Erzeugung und Prüfung
- Referenzierung NIS2

DLT and Standardisierung

- Reinstate Section 11
- Fokus auf EBSI anstatt Indy/Aries
- Integration ETSI/CEN
- Ensure long term verifiability

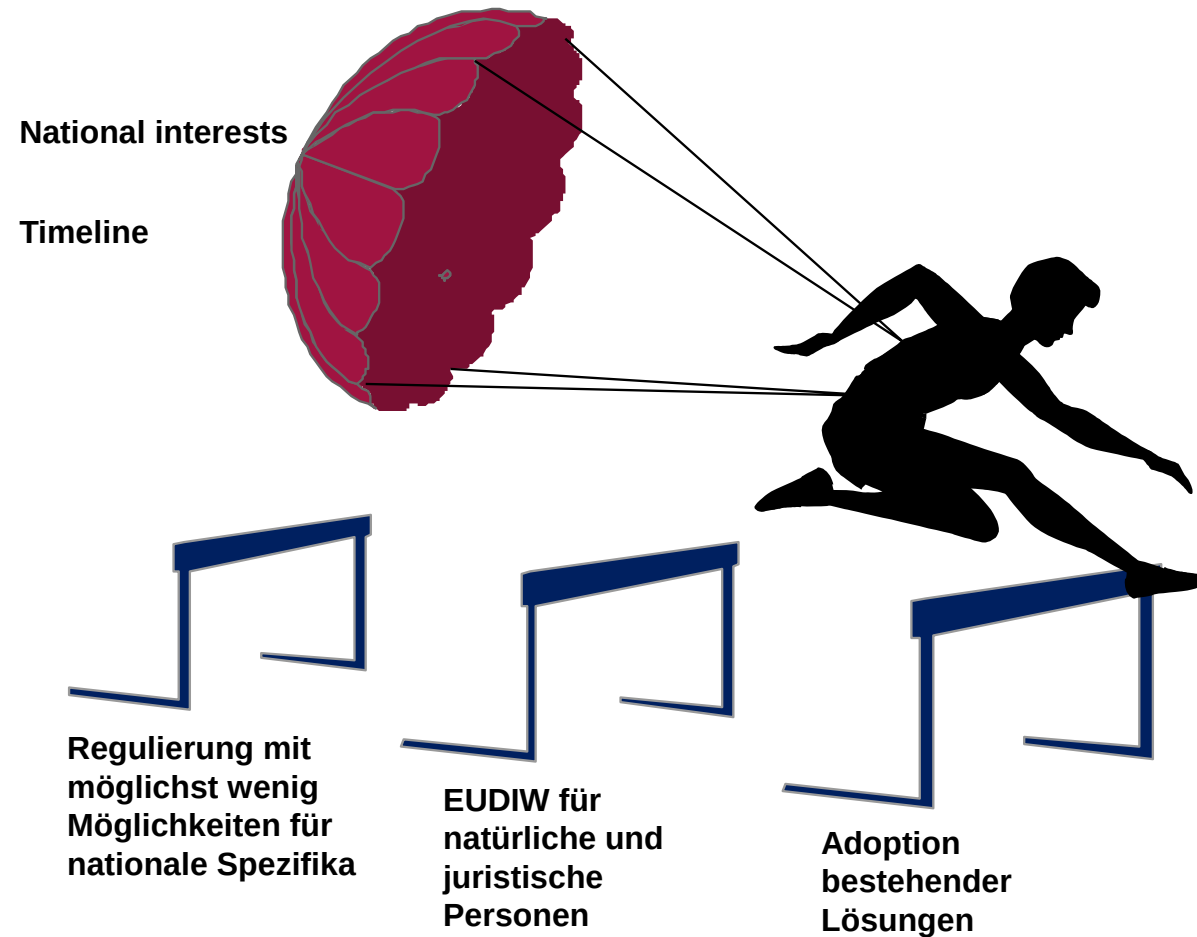
1. Status quo eIDAS 1.0 und Grenzen von SSI

2. EUDIW between ARF and Large Scale Pilots – Anforderungen und UseCases

3. Challenges und offene Punkte in ARF und LSP

4. Outlook

Die Lösung der Herausforderungen ist wesentliche Voraussetzung für eine ganzheitliche Europäische Digitale Identität



Impact in Germany and Europe

ganzheitliche Europäische Digitale Identität

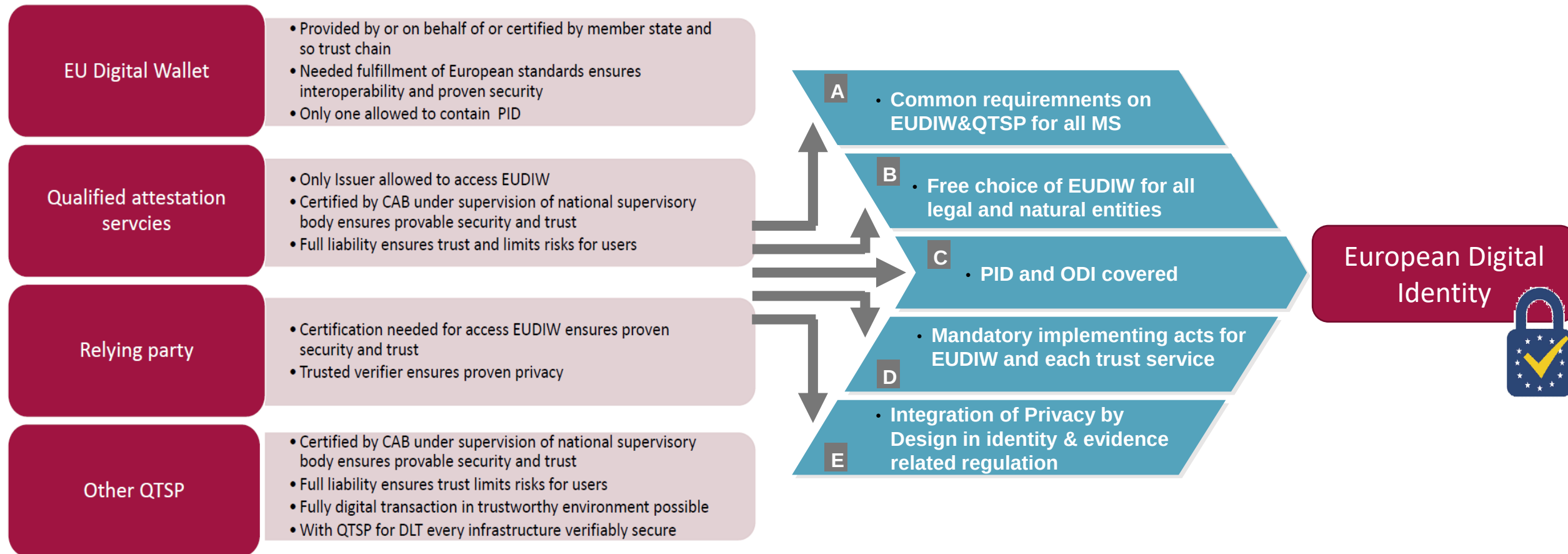
Europe-Wide utilization and worldwide adoption

European standards für prüfbare Sicherheit und nachweisliche Interoperabilität

Trustworthy decentralization for natural and legal entities despite the infrastructures

Sustainable digitization through European digital identity, attestations and trust services

eIDAS 2.0 will lead to inclusive European Digital Identity if it's regulated and designed as European regulation and technical framework.





Contact Information

Steffen Schwalm

Principal Business Consultant/Senior Manager

Digital Identity & Trust

Convenor ISO Tc 46 Sc 11 JWG 1

Expert ISO, CEN/CENELEC, ETSI

Co-Coordination (Technical Focus & Exploitation) EWC

Co-Coordination (Technical Focus & Exploitation) TRACE4EU

Expert (Technical Focus & Exploitation) VECTOR

msg systems ag

Amelia-Mary-Earhart-Straße 14

D-60549 Frankfurt am Main

Mobile +49 162 280 64 72

E-Mail: steffen.schwalm@msg.group

<http://www.msg.group>

