Lehrstuhl für
Rechtsinformatik
Universität des Saarlandes

Technische Aspekte datenschutzgerechter digitaler Identitäten

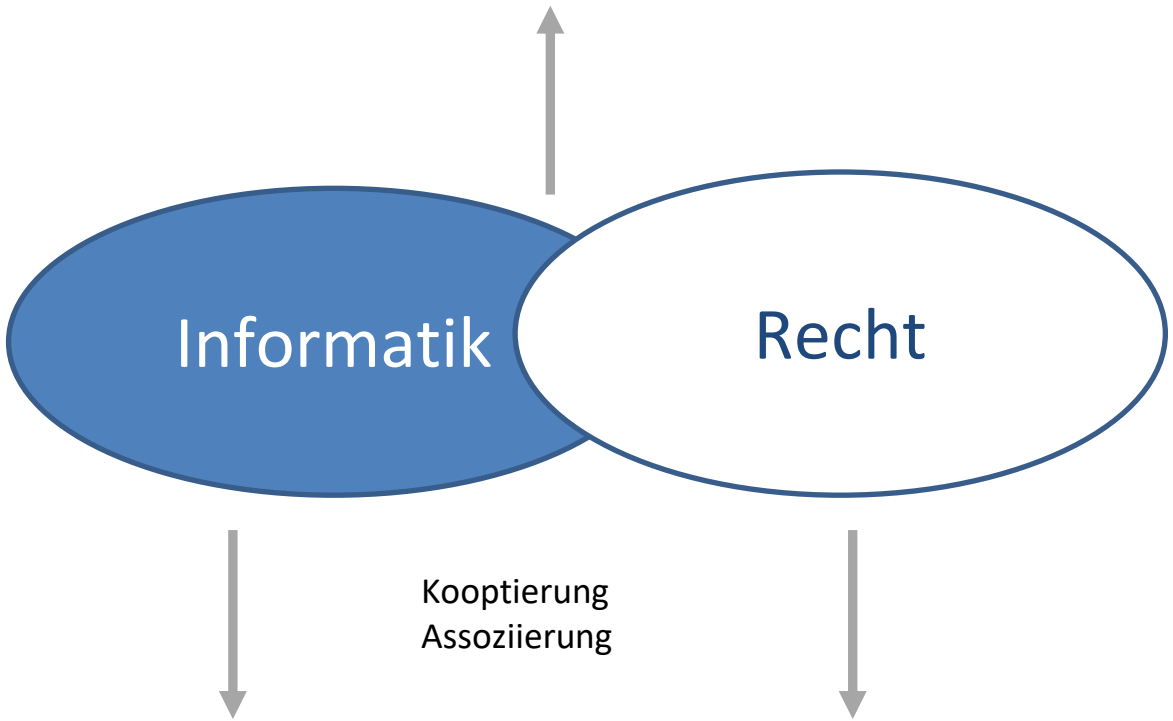
Christoph Sorge

Der Lehrstuhl in Kürze

RECHTSWISSENSCHAFTLICHE FAKULTÄT
UNIVERSITÄT DES SAARLANDES

ZRD Zentrum für Recht und Digitalisierung Saarbrücken

INSTITUT FÜR RECHTSINFORMATIK
UNIVERSITÄT DES SAARLANDES



SIC Saarland Informatics Campus

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

- Drittmittelstarker und großer Lehrstuhl, besetzt mit einem Informatiker
- Schwerpunkte
  - Datenschutz durch Technik (Privacy Enhancing Technologies)
  - Informationsrechtliche Fragestellungen an der Schnittstelle zur IT-Sicherheit
  - IT für Justiz und Verwaltung
  - IT-Forensik
  - Maschinelles Lernen auf juristischen Texten

Der Lehrstuhl in Kürze

- Drittmittelstarker und großer Lehrstuhl, besetzt mit einem Informatiker
- Schwerpunkte
  - Datenschutz durch Technik (Privacy Enhancing Technologies)
  - Informationsrechtliche Fragestellungen an der Schnittstelle zur IT-Sicherheit
  - IT für Justiz und Verwaltung
  - IT-Forensik
  - Maschinelles Lernen auf juristischen Texten

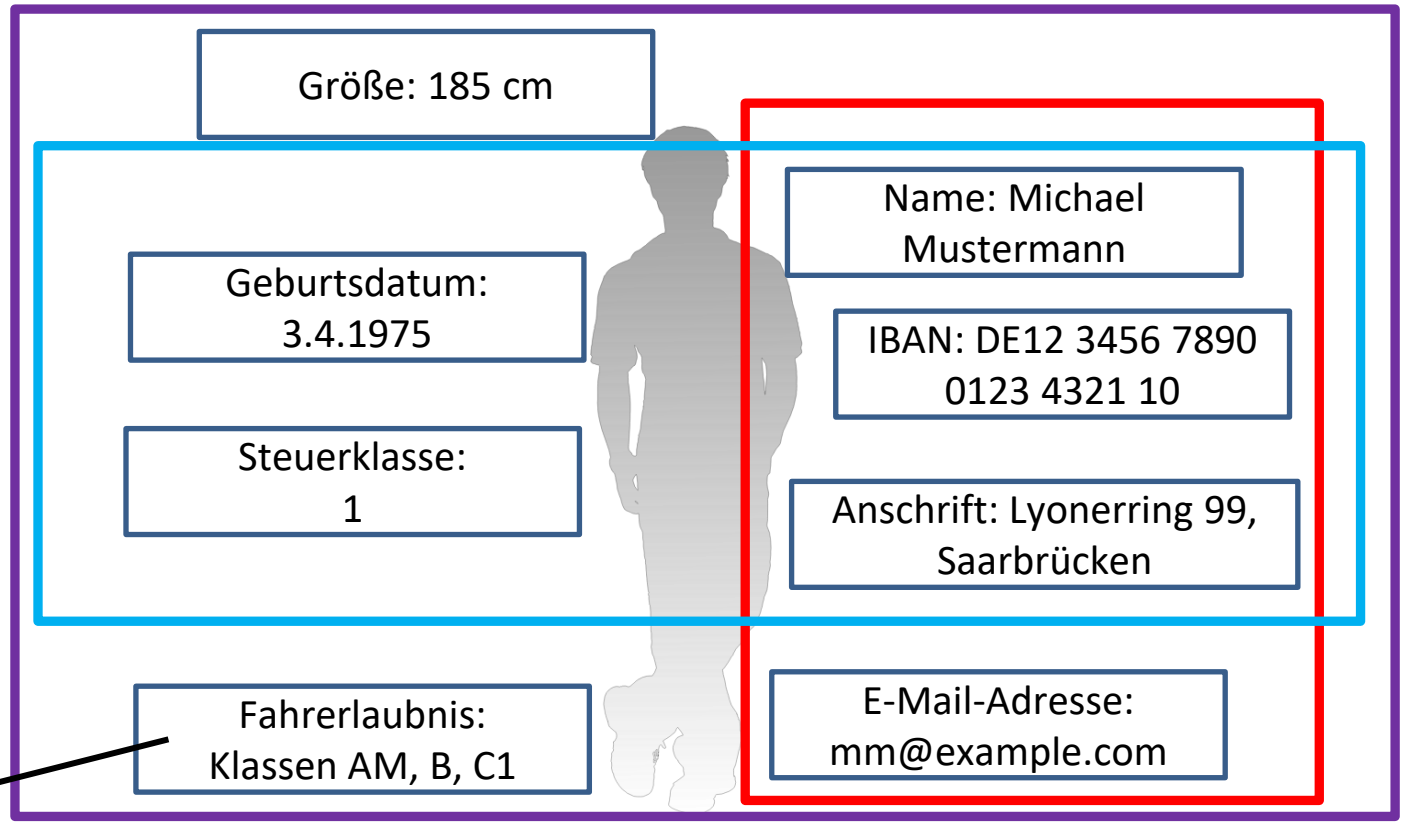
Der Lehrstuhl: Einbettung und Kooperationen

Themen

- Grundbegriffe Identitätsmanagement
- Kryptographie für den Datenschutz
- Elektronischer Personalausweis und Smart eID
- Blockchain und SSI

Identitäten und Identitätsmanagement

- Terminologie uneinheitlich – guter Ausgangspunkt aber:
  Pfitzmann/Hansen (2010), *A terminology for talking about privacy by data minimization*



Vollständige Identität

(Partielle) Identität Finanzamt, Pseudonym = Steuernummer 123/334/5678

Ein *Attribut*

Partielle Identität Online-Shop, Pseudonym = Kundennummer 98765

Allgemein: Eine Identität = Teilmenge der Attributwerte einer Person, die diese Person in einer Menge von Personen ausreichend identifiziert

Bild: https://openclipart.org/detail/181150/shadow-of-person-standing-leg-cross-and-put-hands-in-the-pockets

Herausforderungen Identitätsmanagement

- Unverkettbarkeit / Unverknüpfbarkeit: Zusammenhang zweier „Dinge“ kann durch Unbefugte (Angreifer) nicht mit ausreichender Gewissheit bestimmt werden

- Beispiel: Unverknüpfbarkeit

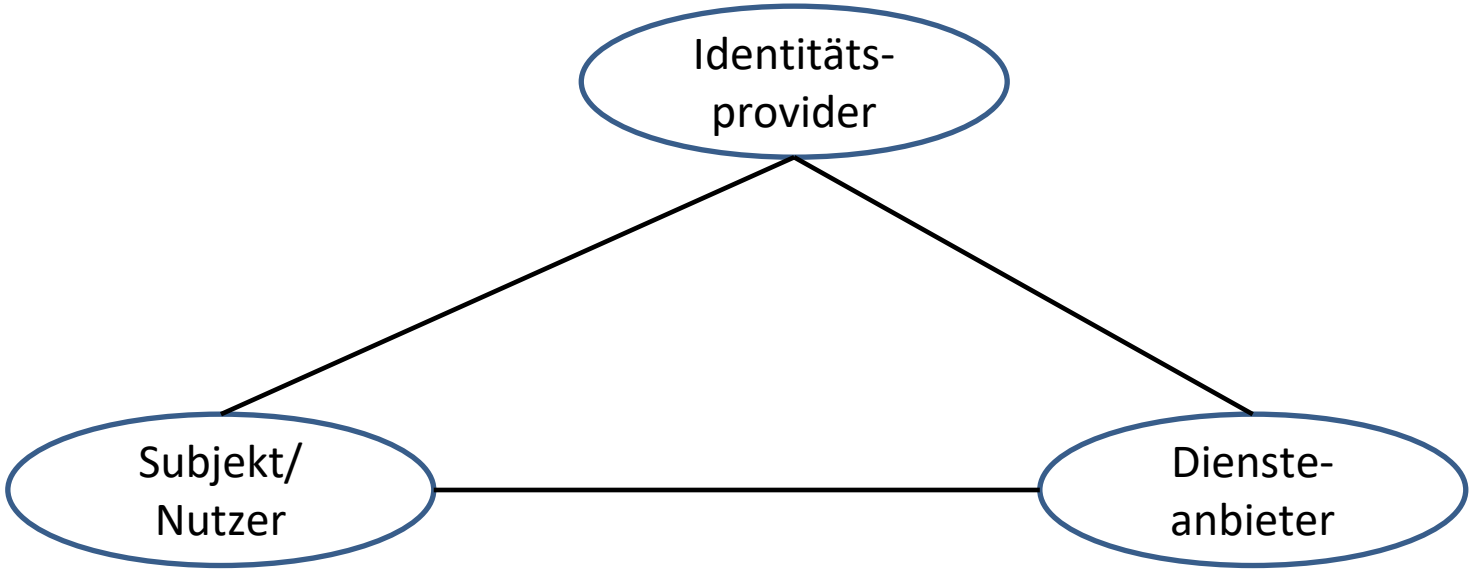
  – der Anmeldungen bei verschiedenen Online-Diensten (durch: Werbetreibende, die bei beiden Online-Diensten Anzeigen schalten; durch die Online-Dienste selbst, die ihre Daten zusammenlegen; …)

  – der Interaktionen mit verschiedenen Behörden (Gegenbeispiel: Architektur des Registermodernisierungsgesetzes)

  – der Anmeldungen beim gleichen Online-Dienst (durch den Online-Dienst selbst)

Klassisches Dreieck des nutzerbasierten Identitätsmanagements

• Speichert Identitäten (Attributwerte und Pseudonyme) des Nutzers
• Führt Authentifizierung des Nutzers durch; übermittelt Pseudonym und ggf. benötigte Attributwerte an Diensteanbieter



• Benötigt lediglich Authentifizierungsdaten für Identitätsprovider

• Erbringt nach durch Identitätsprovider bestätigter Authentifizierung Dienst für den Nutzer
• Muss selbst keine personenbezogenen Daten speichern

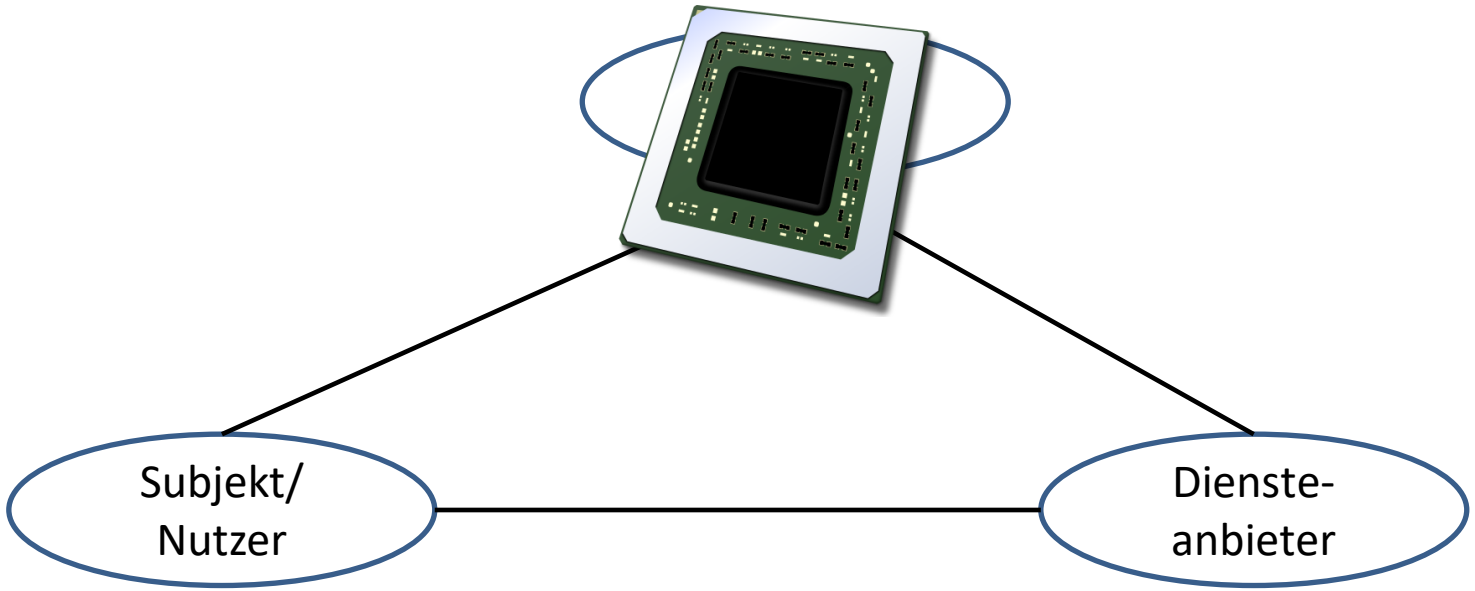
Herausforderungen Identitätsmanagement: Attributpreisgabe

- Unproblematisch: Wer ein Attribut für eine Person überprüft hat, bestätigt die Verknüpfung zwischen Attribut und Identität (repräsentiert durch einen Identifikator, z.B. ein Pseudonym) – z.B. mit qualifiziertem elektronischen Siegel
  - Beispiel: Führerscheinstelle kann bestätigen, dass Michael Mustermann eine Fahrerlaubnis der Klassen AM, B und C1 erworben hat

- Schwierig: Nachweis, dass einer Person ein oder mehrere bestimmte Attribute bestätigt wurden, ohne gleichzeitige Preisgabe weiterer Informationen (volle Identität oder auch nur einzelne nicht benötigte Attribute)
  - Beispiel: Nachweis des Besitzes einer Fahrerlaubnis ohne Offenlegung des Namens Michael Mustermann
  - Naive Ansätze ermöglichen Nachweis einzelner Attribute, erlauben aber Nutzern, ihre Attribute weiterzugeben bzw. Attribute unterschiedlicher Nutzer zusammenzuführen („Nutzer Nr. 4711 hat eine Fahrerlaubnis“ und „Nutzer Nr. 1234 wohnt in Saarbrücken“ zu „Nutzer Nr. 4711 hat eine Fahrerlaubnis und wohnt in Saarbrücken“)

Klassisches Dreieck des nutzerbasierten Identitätsmanagements – mit Hardware

• Vertrauenswürdiges „intelligentes“ Endgerät (z.B. Chipkarte, Personalausweis) – Echtheit wird ggü. Diensteanbieter nachgewiesen
• Speichert Identitäten (Attributwerte und Pseudonyme) des Nutzers, generiert Pseudonyme bei Bedarf neu



• Benötigt lediglich Authentifizierungsdaten für Identitätsprovider

• Erbringt nach durch Identitätsprovider bestätigter Authentifizierung Dienst für den Nutzer
• Muss selbst keine personenbezogenen Daten speichern

Bild: https://openclipart.org/detail/100267/cpu-central-processing-unit

Restricted Identification beim Personalausweis

- Ziel der Restricted Identification: Generierung eines „bereichsspezifischen Identifikators“ – Identifikator, unter dem eine Person in einem Bereich *wieder*erkannt werden kann
  - Auch ohne Kenntnis der vollständigen Identität des Ausweisinhabers
  - Bereich: z.B. Steuerbehörden, einzelner Betreiber einer Website
  - Bereichsspezifischer Identifikator eines Bereichs nicht aus bereichsspezifischen Identifikatoren anderer Bereiche ableitbar

  →Tracking einer Person über verschiedene Bereiche nicht möglich

- Rekonstruktion der „bereichsspezifischen Identität“ bei Sperrung durch Zusammenarbeit verschiedener Stellen möglich

- Weitere Funktionalitäten: Altersverifikation ohne Offenlegung des Geburtsdatums, Wohnortverifikation in unterschiedlichen Granularitäten etc.

- Einbettung in eIDAS-Architektur

Kryptographie für den Datenschutz

- Anonyme Berechtigungsnachweise
  - Nachweis, einer Gruppe anzugehören, ohne weitere Informationen über die eigene Identität preiszugeben
- Gruppen- und Ringsignaturen
  - Zusätzlich Möglichkeit, ein Dokument als Mitglied einer Gruppe zu signieren, ohne weitere Informationen über die eigene Identität preiszugeben
  - Funktionales Äquivalent (gemeinsamer privater Schlüssel) beim elektronischen Personalausweis
- Attributbasierte Kryptographie
  - Möglichkeit, Zuordnung von Attributkombinationen nachzuweisen, ohne weitere Informationen über die eigene Identität preiszugeben

Weitere Schritte: Mobiltelefon

- Schleppende Verbreitung der eID-Funktion des Personalausweises
  - Henne/Ei (Anwendungen – Nutzer mit freigeschalteter eID-Funktion)
  - zunächst problematische Usability, Sicherheitsprobleme der ersten Ausweis-App und schlechte Presse
  - zunächst Notwendigkeit zur Beschaffung eines Kartenlesers
- Heute: Smartphone als Kartenleser
- „Morgen“: Secure Element – sichere Hardware im Smartphone übernimmt Funktion des Personalausweises für eID (Smart-eID-Gesetz)
  - Nur einmalig Übertragung der Attribute an das Secure Element
  - Funktionen dann im Prinzip wie im Personalausweis selbst möglich

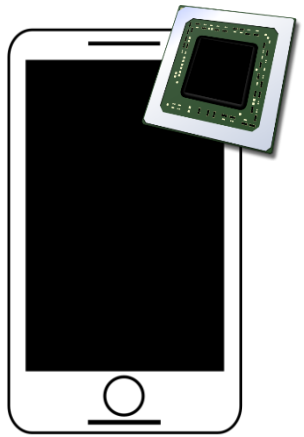


Bild: https://openclipart.org/detail/276127/smartphone-tablet-black-and-white-free-clipart-icon

Weitere Schritte: SSI (Self-sovereign identity)

- Fortschreibung des nutzerzentrierten Identitätsmanagements, Fokus auf Dezentralisierung und eigener Kontrolle der Nutzer (kein zentraler Identitätsprovider notwendig)
  - Verschiedene Initiativen
  - z.B. Standardisierung durch W3C
  - European Self-Sovereign Identity Framework mit Blick auf eIDAS- und DSGVO-Konformität
  - Lektüreempfehlung und Quelle:
    Digital Identity, Leveraging the Self-Sovereignty [sic!] Identity (SSI) Concept to Build Trust, ENISA-Bericht, Januar 2022 sowie Ferdous et al., *In Search of Self-Sovereign-Identity Leveraging Blockchain Technology*, IEEE Access 7, S. 103059-103079, 2019.

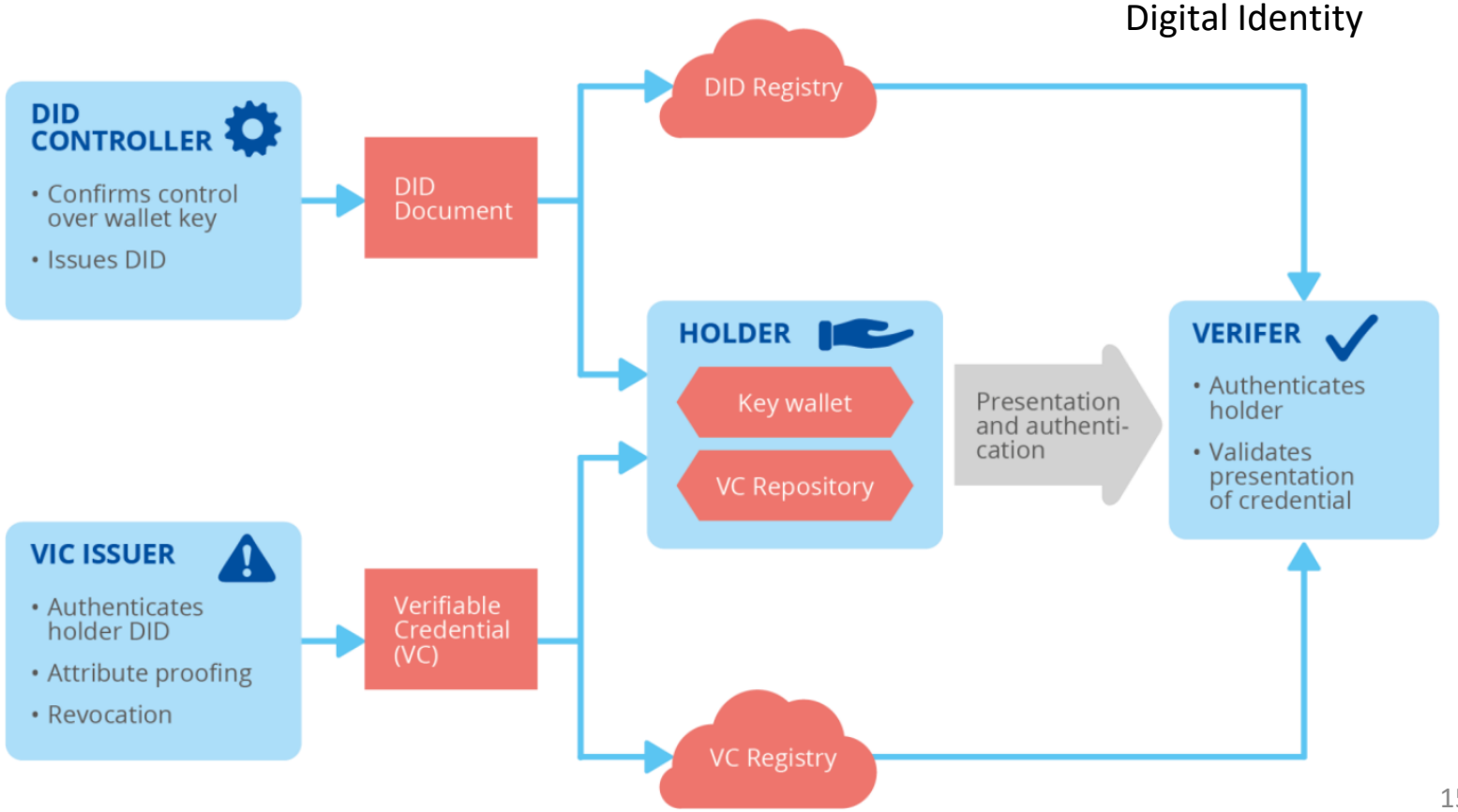
SSI: Konzepte

- Decentralised Identifier (DID) – Identifikator für eine Entität (insb. Person)
  - DID document: Enthält Verifikationsinformationen, auffindbar über ein DID register
  - DID controller (ggf. Nutzer selbst): Stellt DID und DID document aus

- Verifiable credential (VC): Durch einen Aussteller getroffene Aussage über Subjekte, deren Integrität mit kryptographischen Methoden überprüft werden kann
  - Identifikation der Subjekte insb. über DID

- Kontrolle über Preisgabe von VCs beim Nutzer

Bild: ENISA-Bericht Digital Identity



SSI: Bemerkungen

- Positiv zu bewerten: Bemühen um standardisierten Weg zum selbstbestimmten Umgang mit Identitätsattributen und deren Nachweis – ohne zentralen Identitätsprovider in jeder Interaktion
  - Zudem: Hohe Flexibilität für technische Umsetzungen in einzelnen Teilschritten
  - Kombination mit bestehenden Ansätzen denkbar

- Grenzen beachten
  - Ausstellung von Verifiable Credentials – immer noch vertrauenswürdige Stellen benötigt
  - Anonymität: Keine neuen Lösungen etwa für den anonymen Nachweis beliebiger Attributkombinationen (z.B. Fahrerlaubnis und Wohnort ohne Namen)

- Konkrete, „massentaugliche“ Ausprägung noch zu finden – bis auf weiteres bleibt die Daseinsberechtigung auch für eID-Lösungen ohne SSI

Und Blockchain?

- Blockchains als *konzeptionell* dezentrale Systeme zur Unterstützung von dezentralem Identitätsmanagement grundsätzlich denkbar
  - Persistente, unveränderliche und nachvollziehbare Speicherung von Daten des Identitätsmanagement-Systems, somit einfache Umsetzung etwa von Widerrufslösungen
  - Aber auch: Hohe Komplexität, Aufwand für Schutz von Metadaten
- Keine Vorteile bei Überprüfung von Attributen (Verifiable Credentials) per se
- Blockchain-Einsatz nicht überbewerten – Realisierung von SSI auch gänzlich ohne Blockchain möglich

Fazit

- Umfangreicher Werkzeugkasten der Informatik für datenschutzgerechte Identifizierung und Authentifizierung in den unterschiedlichsten Anwendungsfällen steht bereit
  - Sehr guter Stand aus technischer Sicht bereits mit der Einführung der eID-Funktion des Personalausweises (2010) bzw. nach der Überwindung von „Kinderkrankheiten“ in dessen Umfeld erreicht
- In der Praxis oft Tradeoff zwischen einfacher Benutzbarkeit auf Anwenderseite, Umsetzungsaufwand auf Anbieterseite und Sicherheitsniveau – durch technischen Fortschritt aber allmählich weniger Kompromisse notwendig
- Umsetzung von eID-Lösungen sollte aus Identifizierung und Lösung technischer Probleme bestehen, nicht aus Suche nach Problemen für interessante Lösungen
- Tatsächliche Durchsetzungsfähigkeit wesentlich als Ergebnis von Marktmacht (im weitesten Sinne) und Standardisierungserfolgen

Fragen?

Kontakt:

Christoph Sorge
Universität des Saarlandes,
Lehrstuhl für Rechtsinformatik

christoph.sorge@uni-saarland.de