Digitale Souveränität für den Nutzer

Selbstbestimmte Identitäten im Kontext der Landeshauptstadt Dresden

Prof. Jürgen Anke, Robert Schröder

DIV-Konferenz, 08.11.2021

IDEAL

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Dresden.

Überblick / Agenda

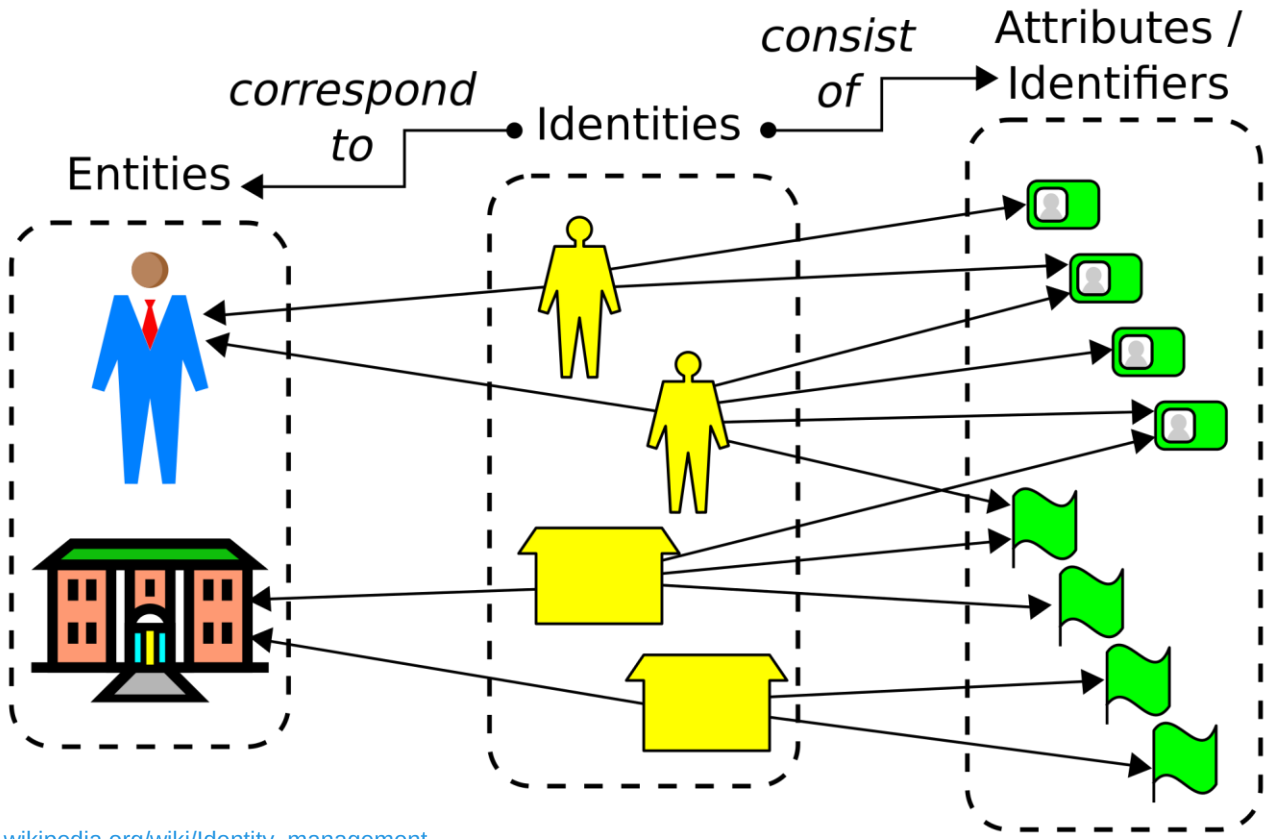
- Ausgangssituation
  - Vertrauen und Identitäten
  - Ansätze zum Management digitaler Identitäten
- Self-Sovereign Identity
  - Standardisierung digitaler Nachweise
  - Technische Grundlagen
- Das Schaufensterprojekt „ID-Ideal“
  - Ziele & Struktur
  - Lösungsansatz
  - Anwendungsszenarien
- Ausblick

Vertrauen (nicht nur) im digitalen Raum

- Der Ablauf einer Interaktion wird vom **Vertrauen** der beteiligten Akteure zueinander bestimmt
- Reale Welt: **Nachweis** der Vertrauenswürdigkeit durch äußerlichen Eindruck / Verhalten oder durch Dokumente von vertrauenswürdigen Herausgebern
- Anforderung an Grad der Vertrauenswürdigkeit hängt von **Bedeutung** der Interaktion ab:
  - Zeitung kaufen
  - Reiseauskunft bekommen
  - Reisepass beantragen
  - Bankkonto eröffnen
  - Netflix-Abo abschließen

Was ist eine Identität?

Eine **Identität** ist eine Menge von Attributen anhand derer sich Personen oder Objekte eindeutig beschreiben lassen.
Real: Fingerabdruck, Irismerkmale, Name, Adresse, Größe, …
Digital: Nutzername, Passwort, Token, biometrische Daten



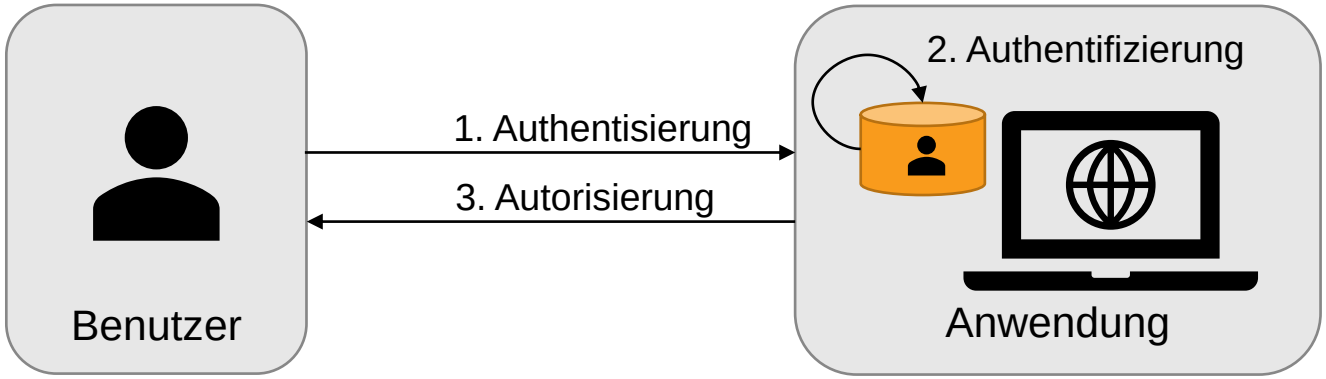
https://en.wikipedia.org/wiki/Identity_management

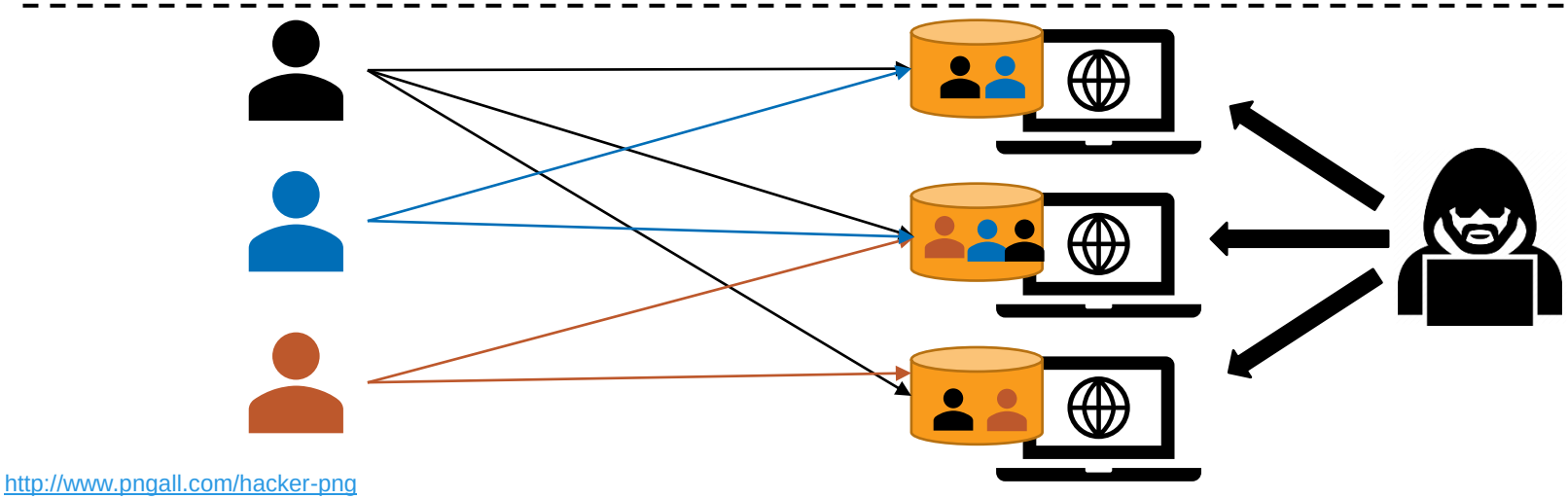
Management digitaler Identitäten

Vergleich grundlegender Ansätze.

ID-Managementansätze: Isoliert / Zentralisiert

- Isoliert: ein Account pro Onlineangebot
- Beispiele: z.B. Lufthansa, Teilauto, OTTO, Telekom, …

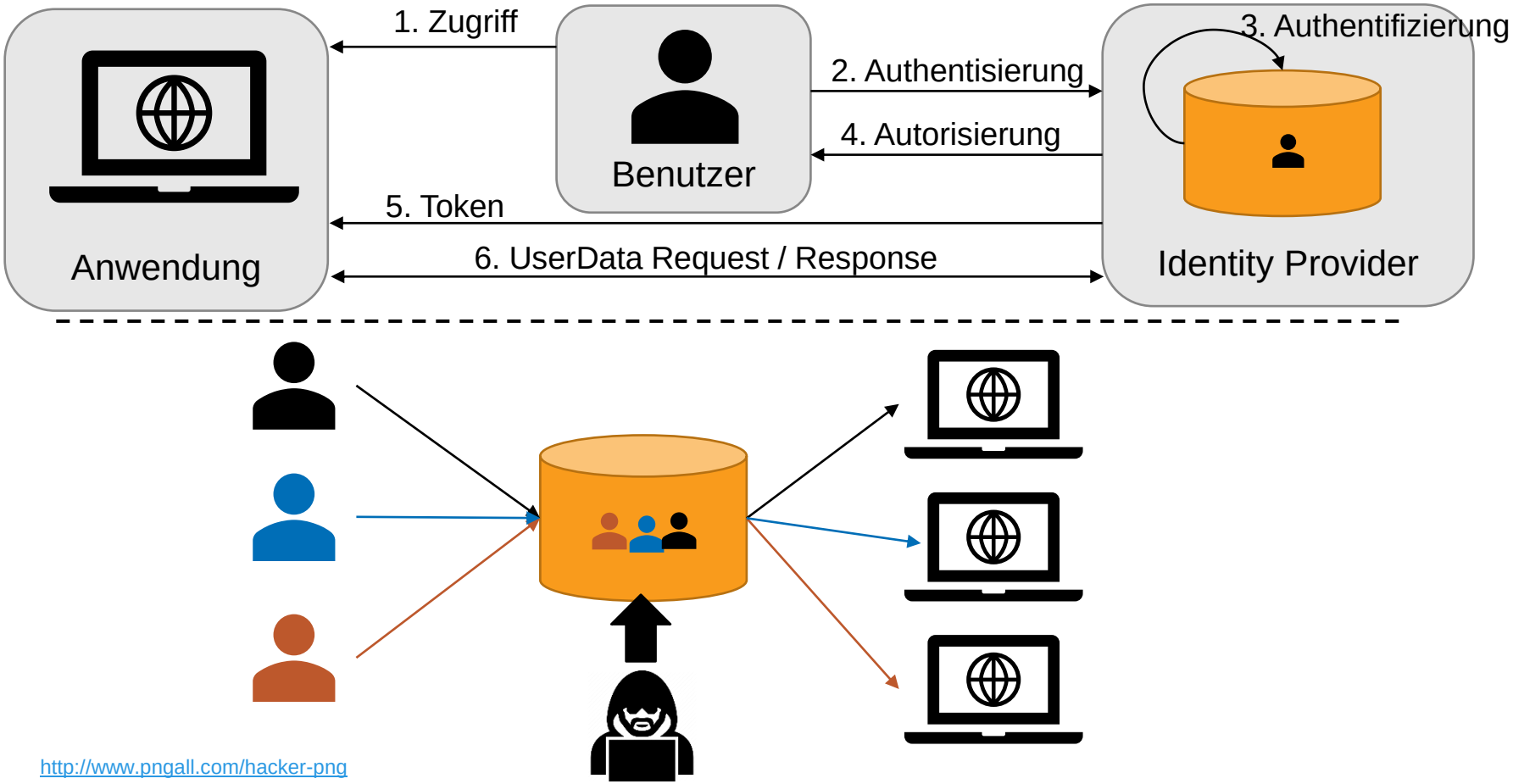




http://www.pngall.com/hacker-png

ID-Managementansätze: Föderiert

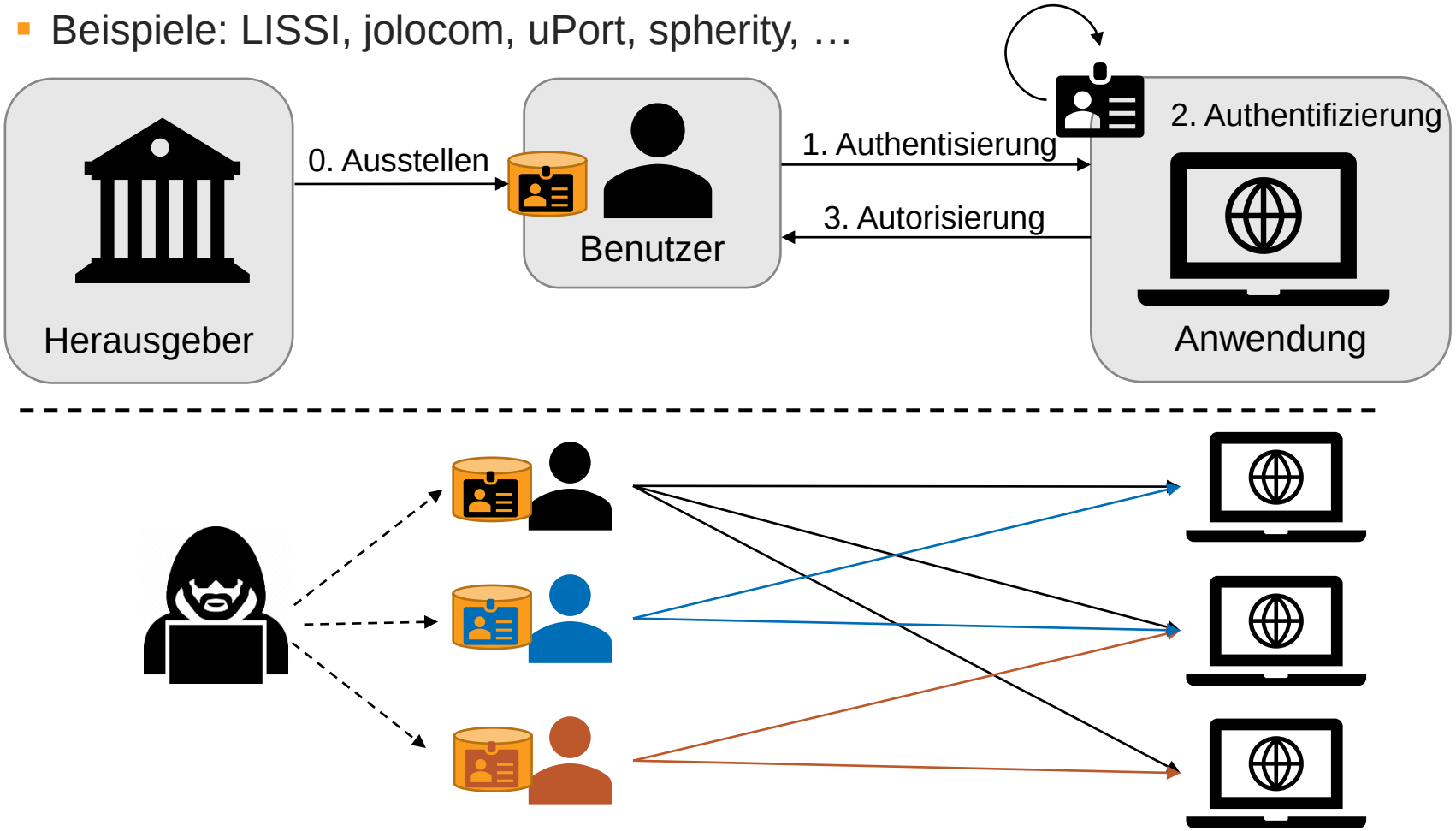
- Föderiert – ein Account pro Identity Provider
- Beispiele: Social Logins (Google, Facebook, …), Microsoft, verimi



http://www.pngall.com/hacker-png

ID-Managementansätze: Self-sovereign

- Self-Sovereign Identity – eine Wallet pro Benutzer
- Beispiele: LISSI, jolocom, uPort, spherity, …

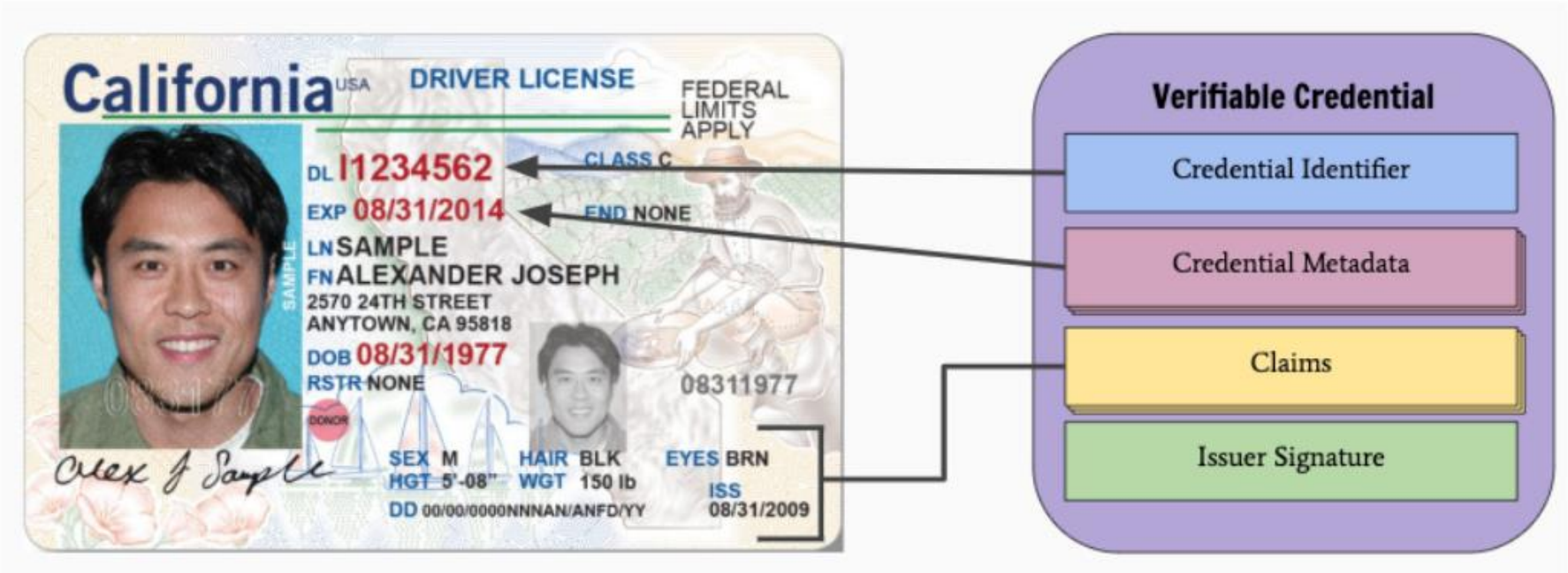


http://www.pngall.com/hacker-png

Self-Sovereign Identity

Standardisierter Austausch digitaler Nachweise.

Verifiable Credential

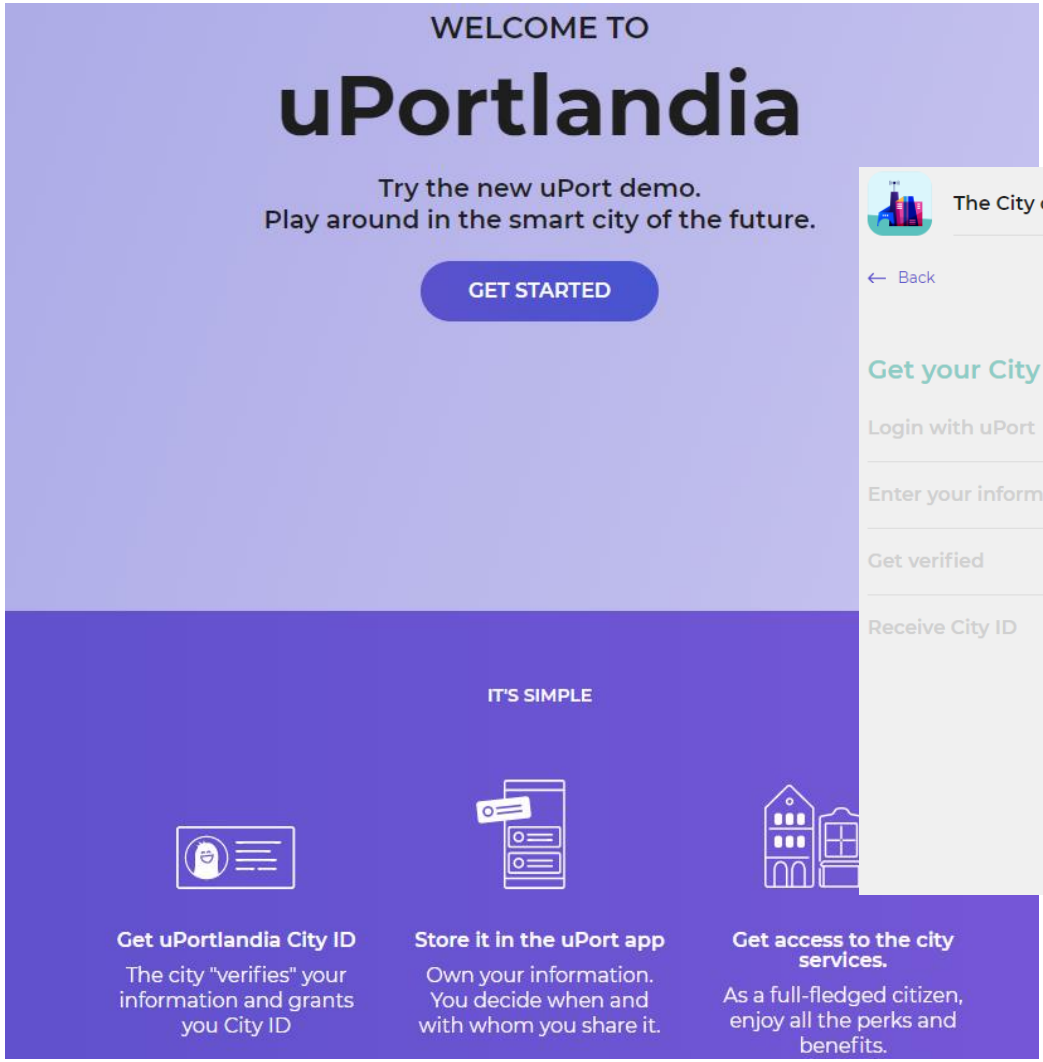


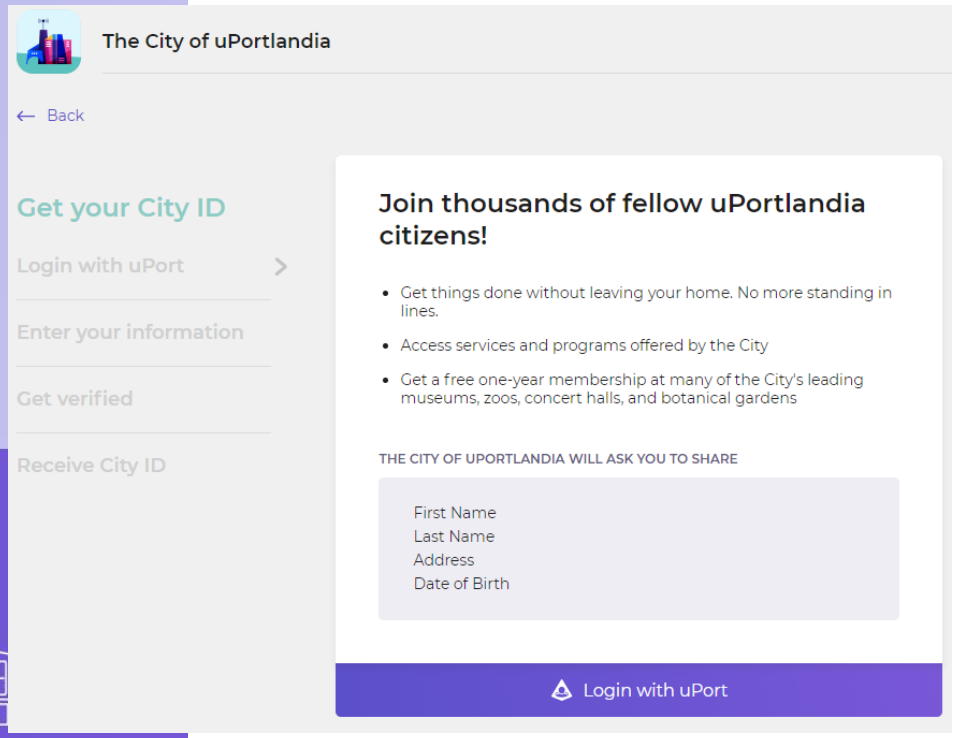
[PR20], S. 27

Digitale Nachweise in SSI: „Verifiable Credentials“

- VCs sind das digitale Äquivalent zu Urkunden bzw. Ausweisen und stellen eine kryptografisch gesicherte Aussage über ein Subjekt dar, die von einer autorisierten Stelle bestätigt wird, z.B.
  - Markus Meier ist Student an der HTW Dresden
  - Laura Lehmann ist Geschäftsführerin der DigiConsult GmbH
  - Emil Ehrlich hat eine DVB Monatskarte
- VCs werden von Dienstanbietern ausgegeben und von den Inhabern in einer digitalen Brieftasche („Wallet“) gespeichert.
- Inhaber können diese VCs nutzen, um daten-minimale kryptografisch prüfbare Bestätigungen („Proofs“) bei Online-Services für weitere Vorgänge präsentieren, z.B.
  - Laura Lehmann beantragt Fördermittel bei der SAB
  - Markus Meier erhält Studentenrabatt im Fitnessstudio
  - Emil Ehrlich leiht ein NextBike Fahrrad

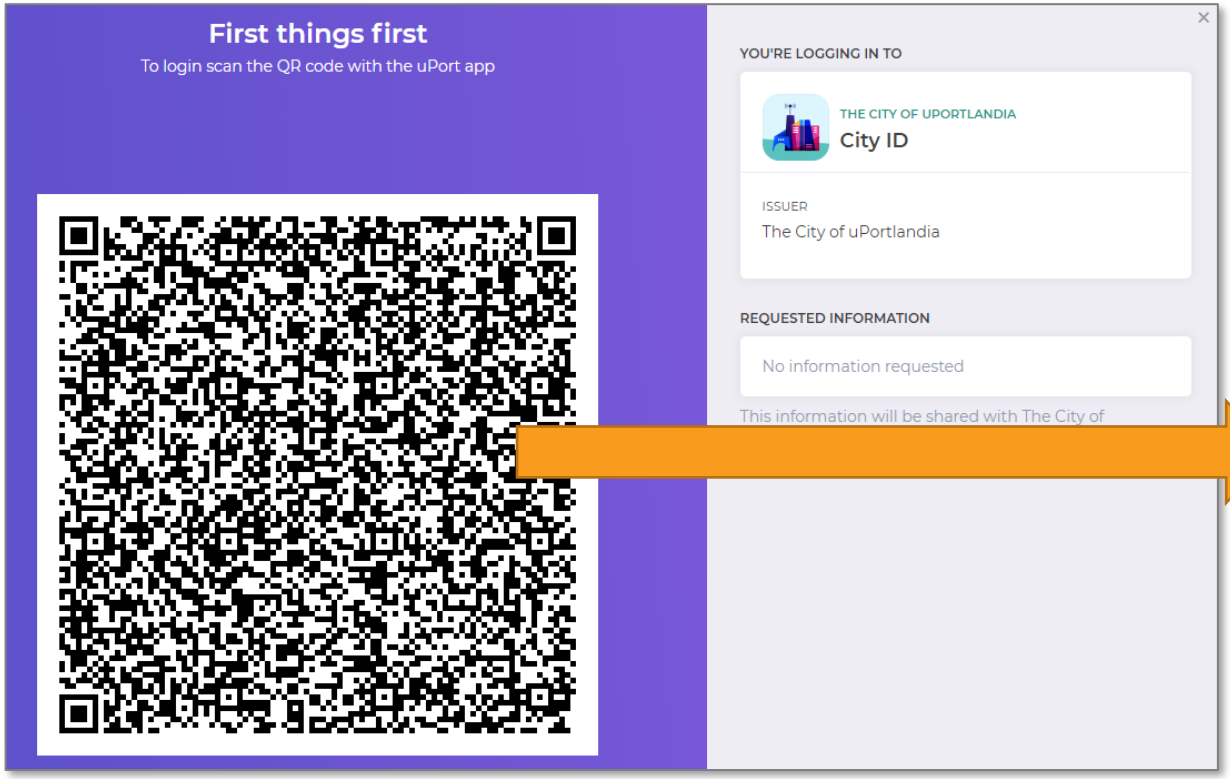
SSI-Demo zum Ausprobieren

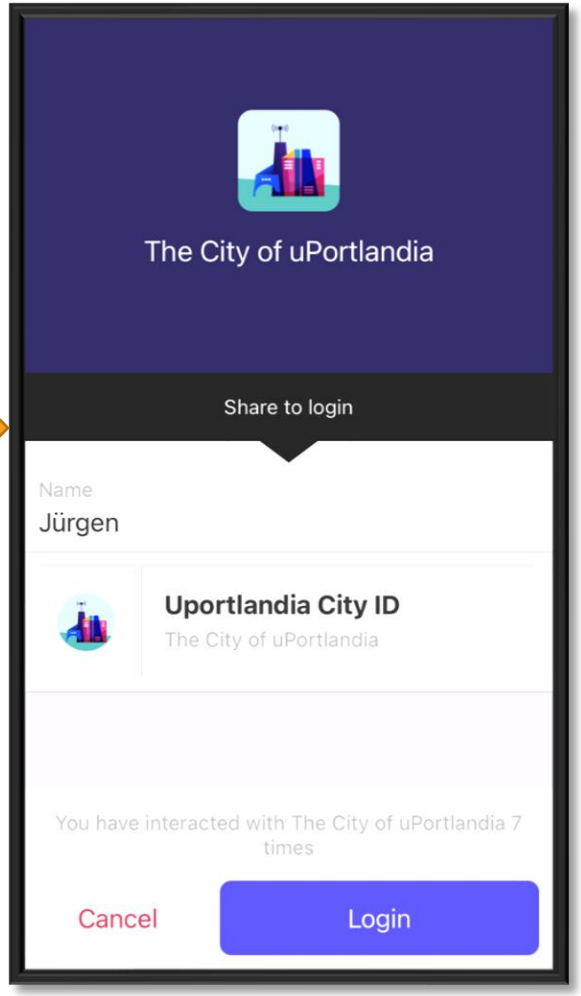




https://uportlandia.uport.me/

Authentifizierung per QR-Code starten





Verwendete Digitale Nachweise in uPortlandia

THE CITY OF UPORTLANDIA

City ID

4 credentials included

Identify yourself with one click. Get a digital City ID. Enjoy quick, seamless, and often free access to many city services.

YOU'LL BE ASKED TO SHARE

First Name
Last Name
Address
Date of Birth

GET CITY ID

THE UNIVERSITY OF UPORTLANDIA

Diploma

4 credentials included

Get a verified digital copy of your diploma. Share it easily at you next job interview or while applying to post graduate program.

YOU'LL BE ASKED TO SHARE

City ID

GET DIPLOMA

DREAM JOB LLC.

Employment Verification

3 credentials included

Share confirmation of your employment easily. No more collecting stacks of documents to apply for a mortgage or sign a lease.

YOU'LL BE ASKED TO SHARE

City ID
Diploma

GET EMPLOYMENT VERIFICATION

PEOPLE CARE INSURANCE LLC.

Insurance Coverage

3 credentials included

Share your insurance information easily at your doctor's office, pharmacy or at any emergency.

YOU'LL BE ASKED TO SHARE

City ID
Employment Verification

GET INSURANCE COVERAGE

YOUR HEALTH MEDICAL CENTER

Prescription Drug

1 credential included

No more waiting for the doctor to call your pharmacy. Share your drug prescription at any drug store, any time.

YOU'LL BE ASKED TO SHARE

City ID
Insurance Coverage
Diploma

GET PRESCRIPTION DRUG

UPORTLANDIA CITY TRANSIT

Monthly Bus Ticket

1 credential included

Are you a uPortlandia citizen? Alumni of The uPortlandia University? Get your monthly bus ticket for free and enjoy the city transportation!

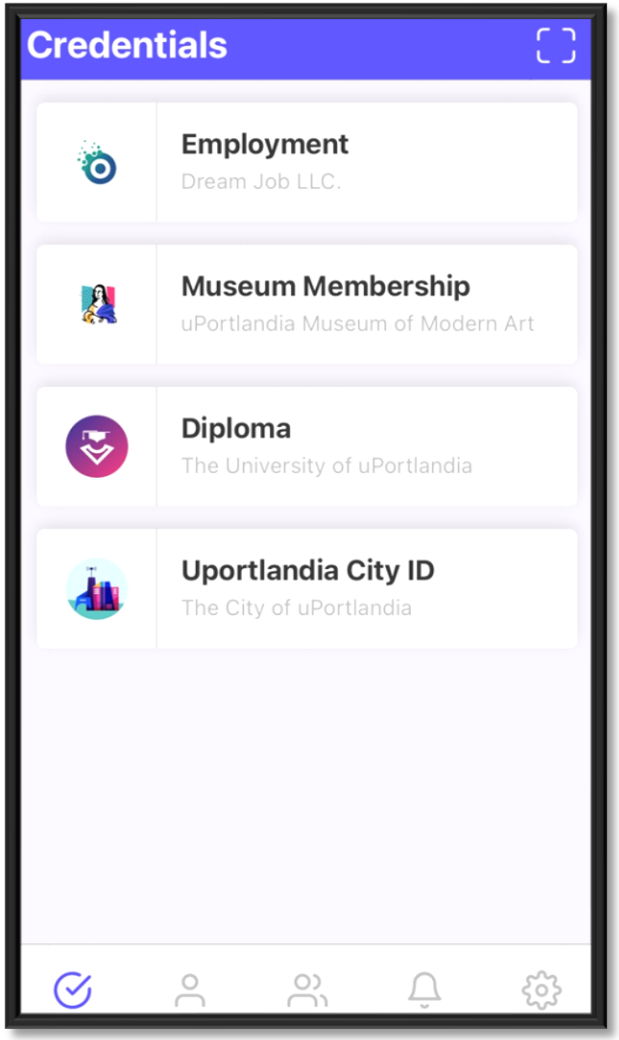
YOU'LL BE ASKED TO SHARE

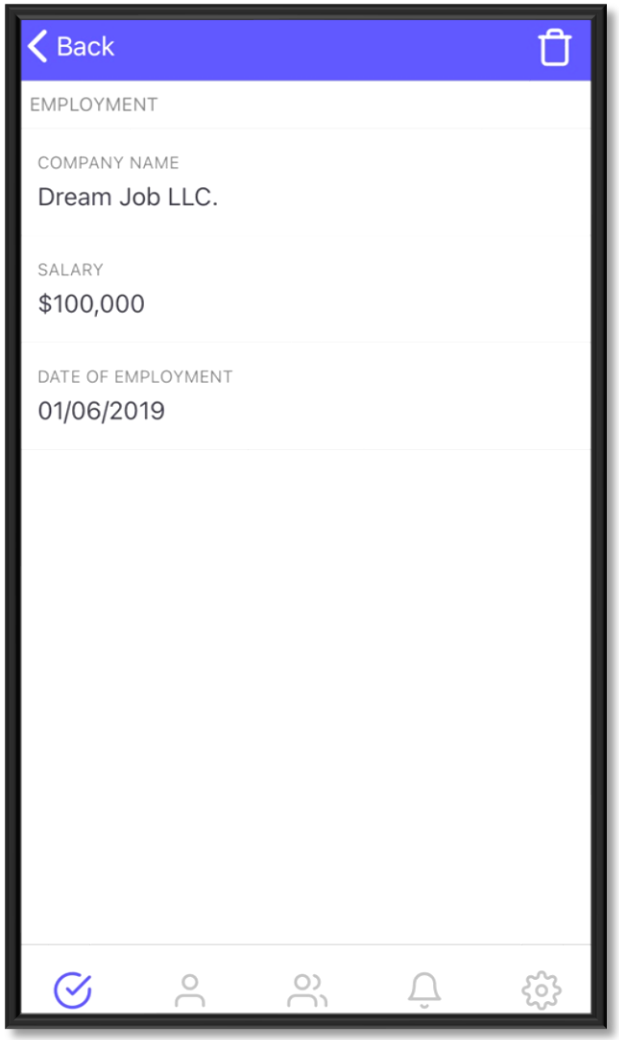
City ID
Diploma

GET MONTHLY BUS TICKET

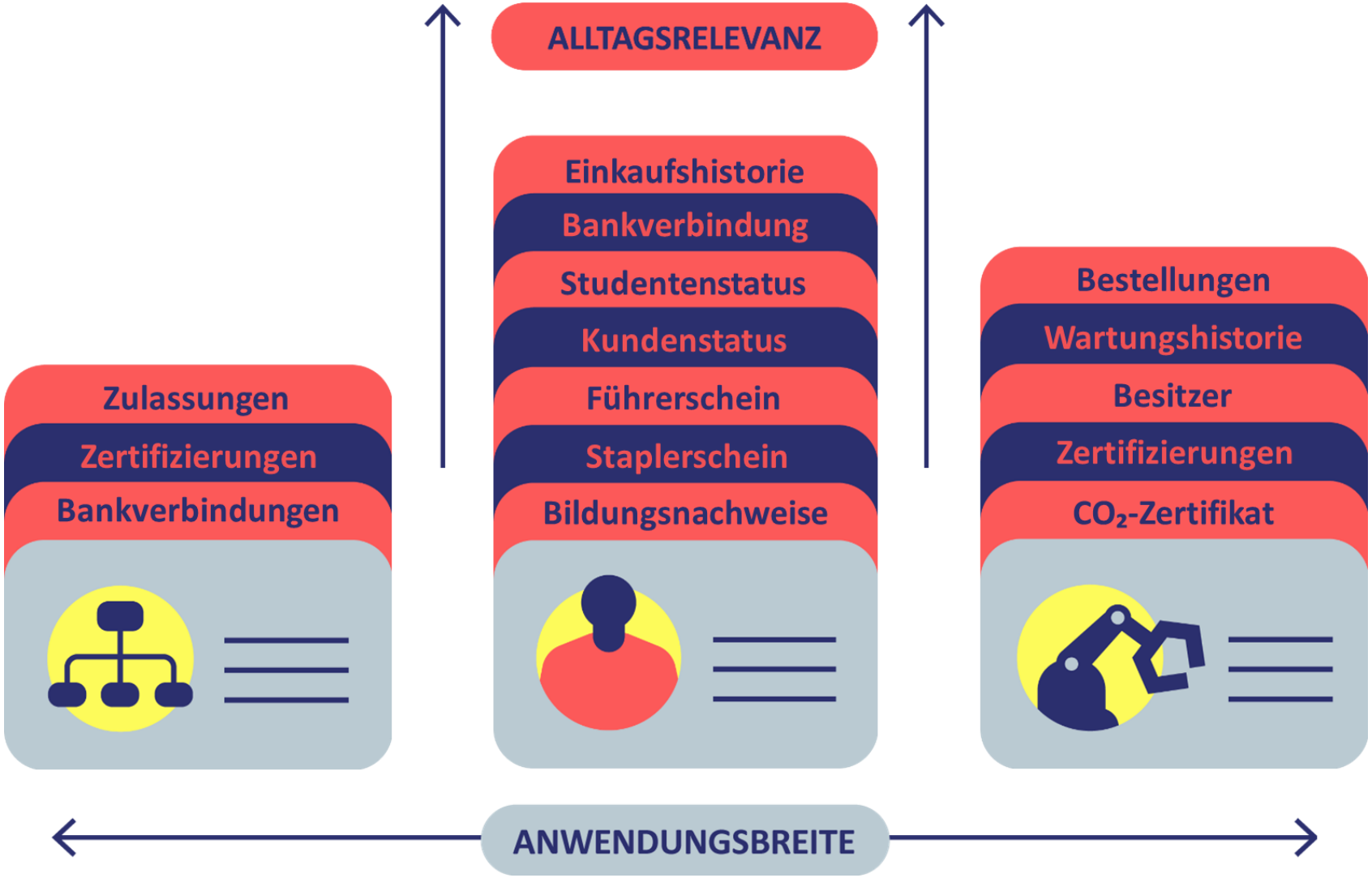
https://uportlandia.uport.me/

Anzeige von Credentials in der Wallet



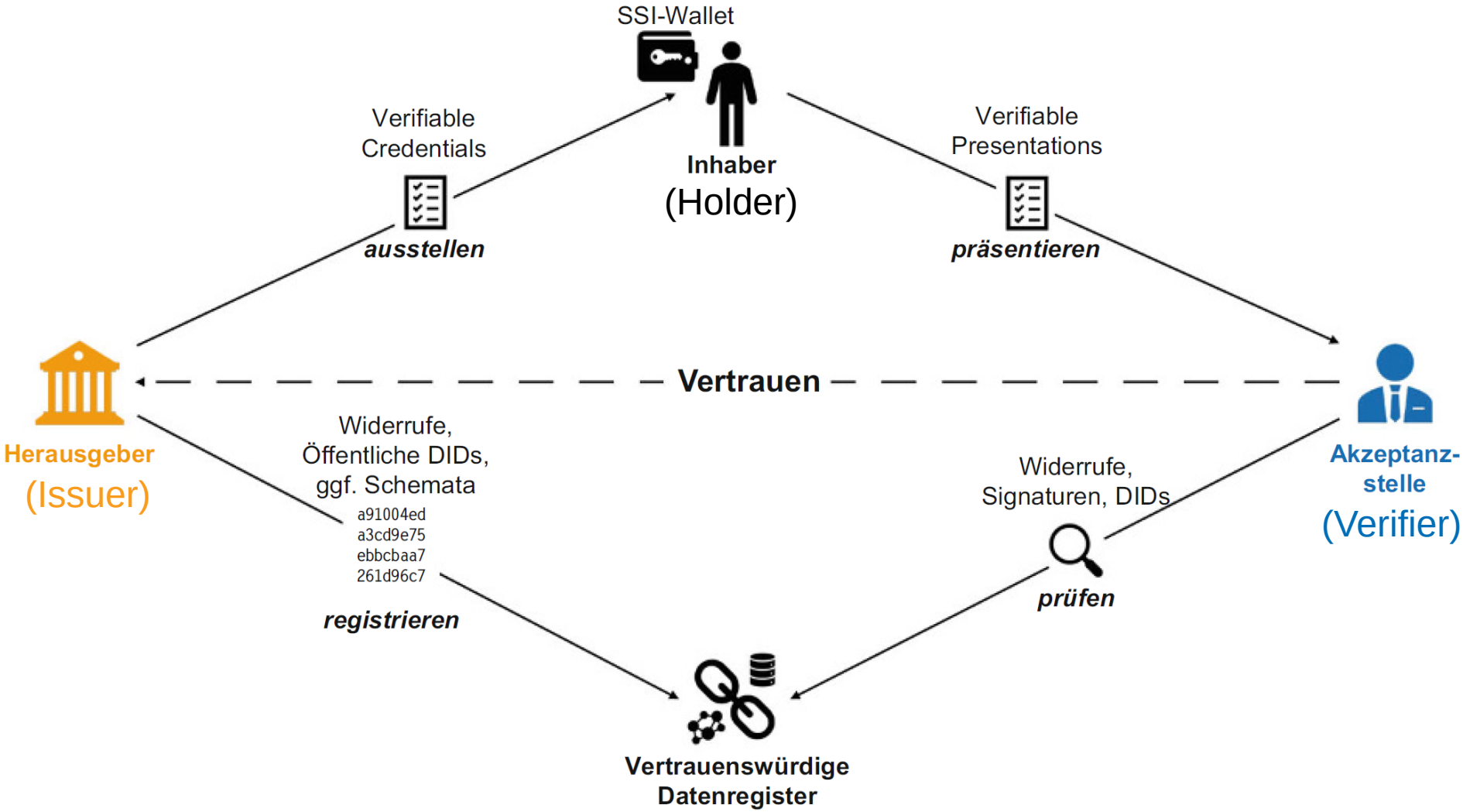


Vielfalt digitaler Nachweise



Technische Grundlagen von SSI

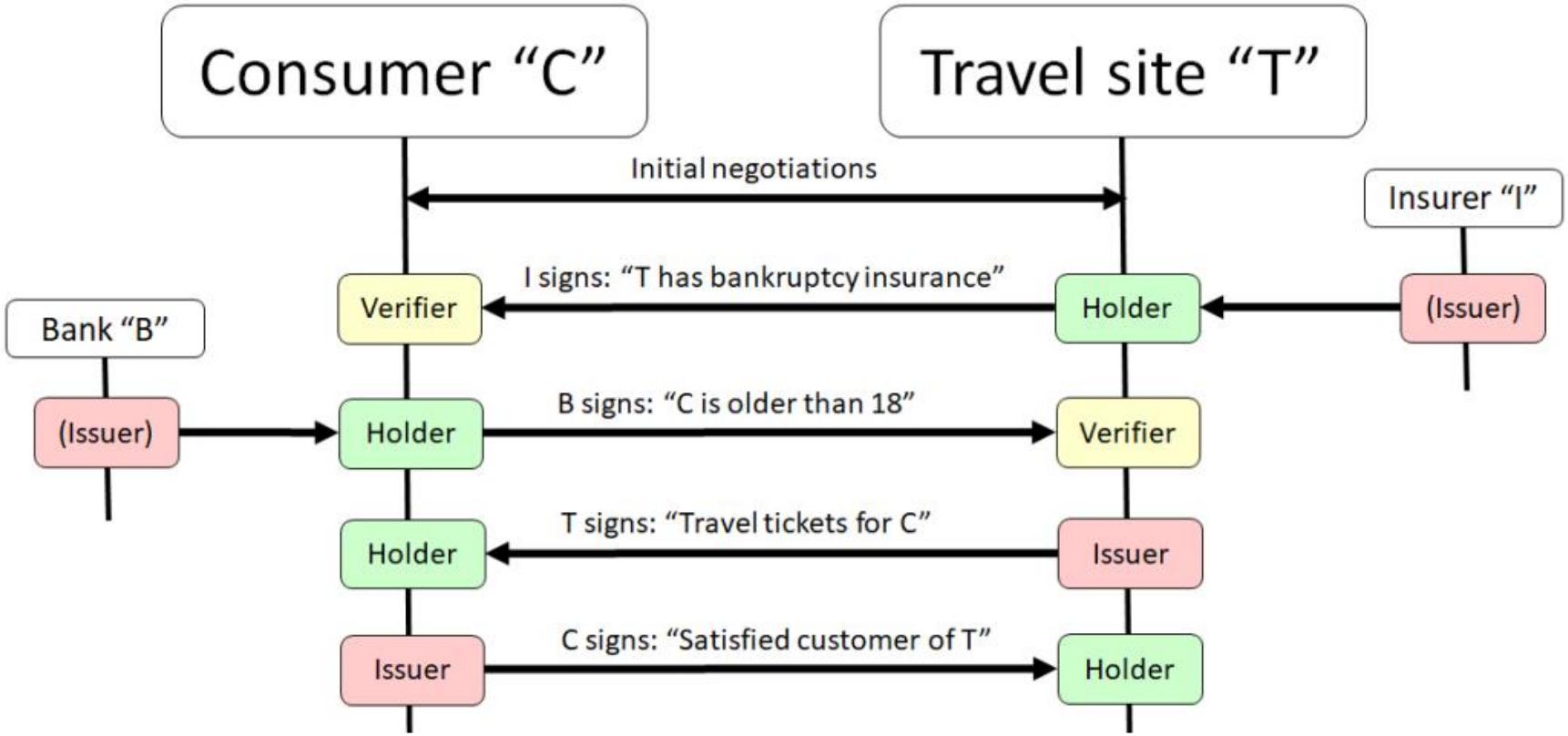
SSI-Interaktionsschema und Rollen



[ER+21]

Rollen der Akteure in einem Buchungsprozess

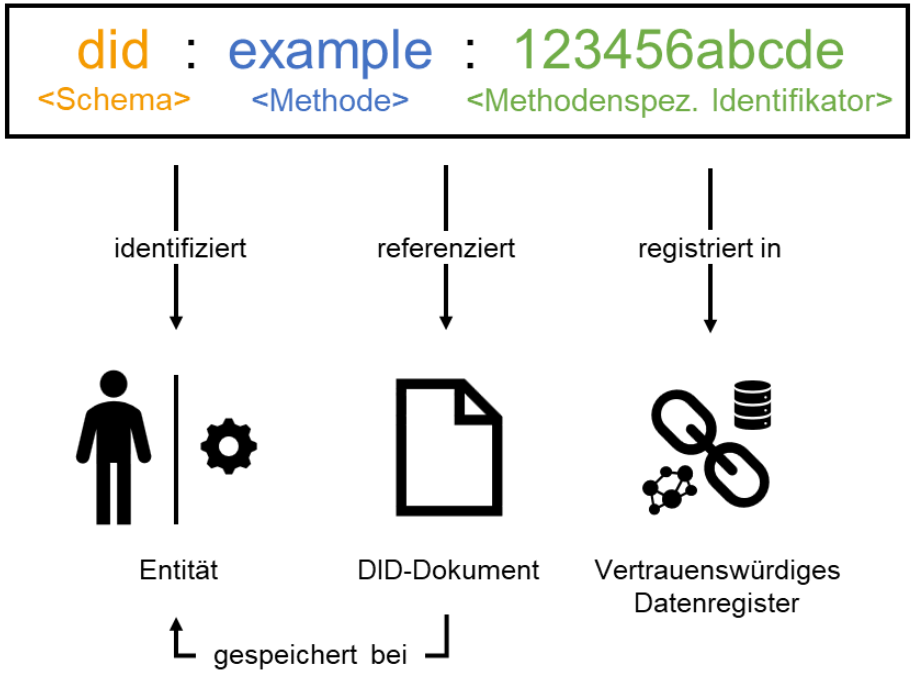
Die meisten Interaktionen sind ein Austausch von Credentials → Akteure haben je nach Prozessschritt eine anderen Rolle



[PR20], S. 30

Decentralized Identifier (DID)

- W3C Standard, entspricht URI-Schema
- Dient als Identifikator für Entitäten (Person, Organisation, Objekt)
- Wird vom Besitzer der Entität angelegt, **unterliegt keiner zentralen Kontrolle**
- URL verweist auf DID Document mit Informationen zu kryptografischen Prüfmethoden und Services
- Aktuell 112 Methoden für den Umgang mit DIDs in Entwicklung
- Hinterlegung in Register nur für Auffindbarkeit bzw. Prüfbarkeit notwendig

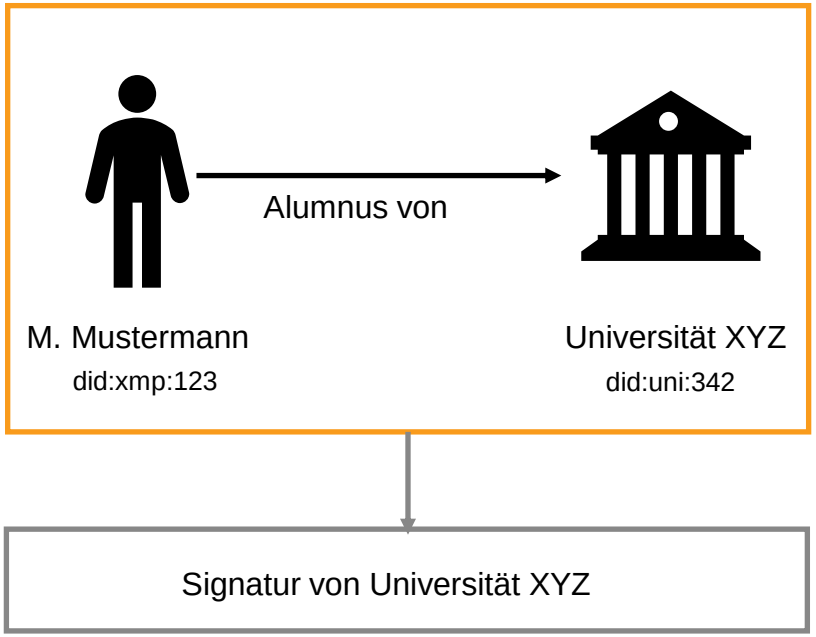


https://www.w3.org/TR/did-core/ ; https://w3c.github.io/did-spec-registries/#did-methods

Verifiable Credential

- Verifiable Credentials sind ein W3C-Standard für ein Format zur Darstellung kryptografisch gesicherter Aussagen über ein Subjekt
- Subjekt und Herausgeber werden durch DIDs referenziert
- Verifizierung des Vorgelegten Credentials ohne Kontakt zum Herausgeber möglich

Behauptung

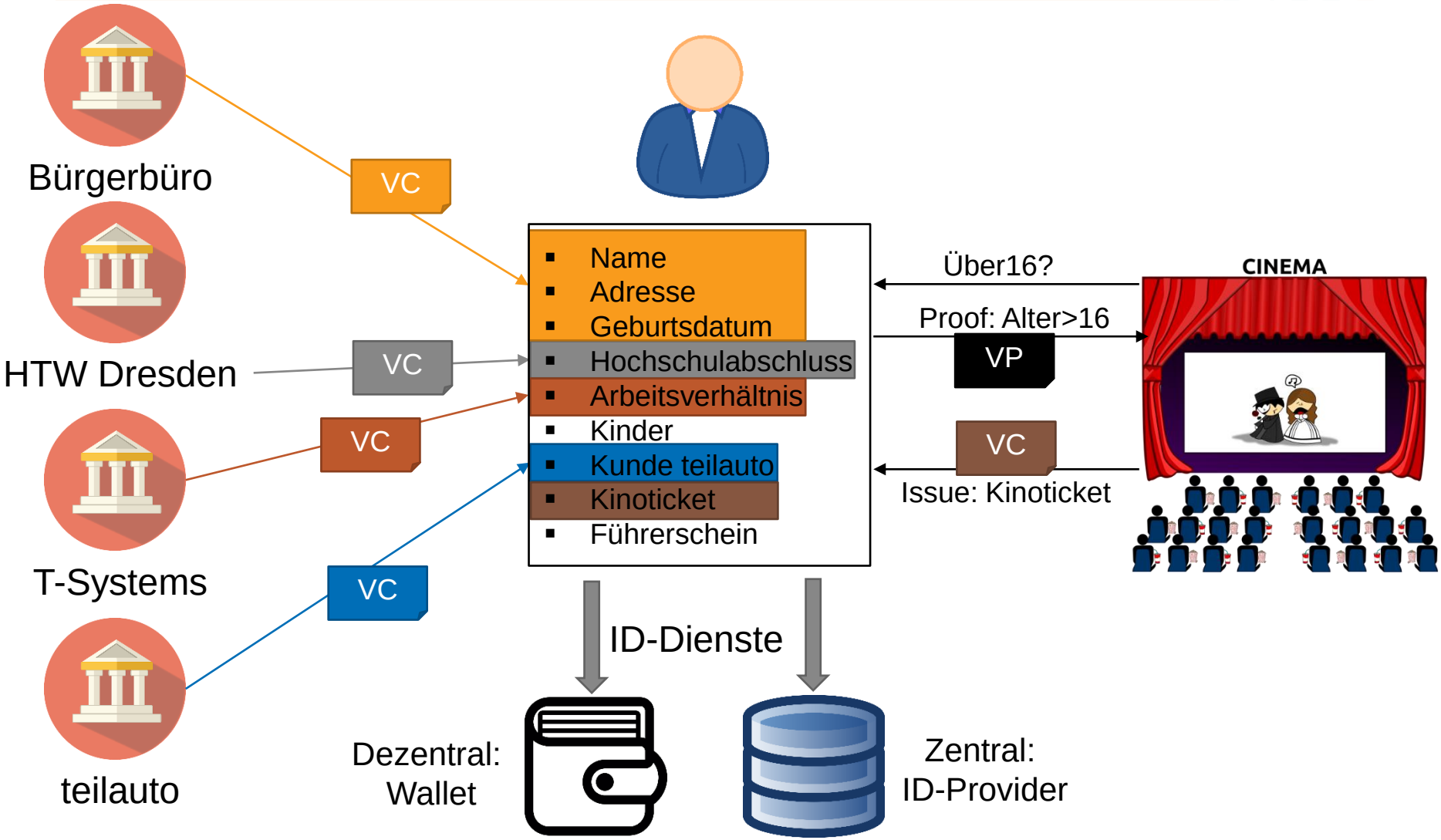


Beweis

https://www.w3.org/TR/vc-data-model/


```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://htwexample.edu/credentials/1234",
  "type": ["VerifiableCredential", "AlumniCredential"],
  "issuer": "https://example.edu/hochschulen/sachsen/12345",
  "issuanceDate": "2020-01-01T19:73:24Z",
  "credentialSubject": {
    "id": "did:xmp:123",
    "alumniOf": {
      "id": "did:uni342",
      "name": "Universität XYZ"
    }
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2017-06-18T21:19:10Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://example.edu/issuers/keys/1",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmF...PAYuNzVBAh4vGHSrQyHUdBBPM"
  }
}
```

Verwaltung digitaler Nachweise mit SSI



Interoperable ID-Dienste durch ein Trust Framework

Das Projekt „ID-Ideal“
(BMWi-Schaufenster „Sichere Digitale Identitäten“)

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Was soll ID-Ideal leisten?

Vision: Rechtssicherheit im digitalen Raum durch einfach nutzbare digitale Identitäten.

Mission: *Entwicklung*, *Anwendung* und *Verbreitung* eines Rahmenwerks für sichere digitale Identitäten von Personen, Organisationen und Objekten.

Zielbild: Entstehung eines Ökosystems aus Herausgebern, Inhabern und Akzeptanzstellen, in dem Akteure

- ihre digitale Nachweise zur Schaffung von Vertrauen über die Grenzen bisher isolierter Vertrauensdomänen hinweg einsetzen und
- sie dafür aus einer Vielzahl kompatibler ID-Dienste einen auswählen, der ihren Bedürfnissen am besten entspricht.

Mit ID-Ideal leisten wir einen Beitrag zur Anregung von Innovationen und Wertschöpfung durch den Einsatz digitaler Identitäten in Wirtschaft, Verwaltung und Gesellschaft.

Lösungsansatz ID-Ideal

Vorteil für Onlinedienste: Ohne Registrierung nutzbar, Geringer Integrationsaufwand.

Vorteil für ID-Dienste: Erhöhung der Reichweite für die eigenen Nutzer.

Kommunale Dienstleister | Verwaltung / Amt24 | … | Kommerzielle Onlinedienste

Adapter | Adapter | Adapter

ID-Dienste

Erweiterung — Bürgeraccount

Erweiterung — AUTHADA App

…

Servicekonto

TrustNet Ökosystem:
Vielfalt von ID-Diensten und Akzeptanzstellen durch Interoperabilität

W3C | DIF | eIDAS | helix id | JOLOCOM | euan network

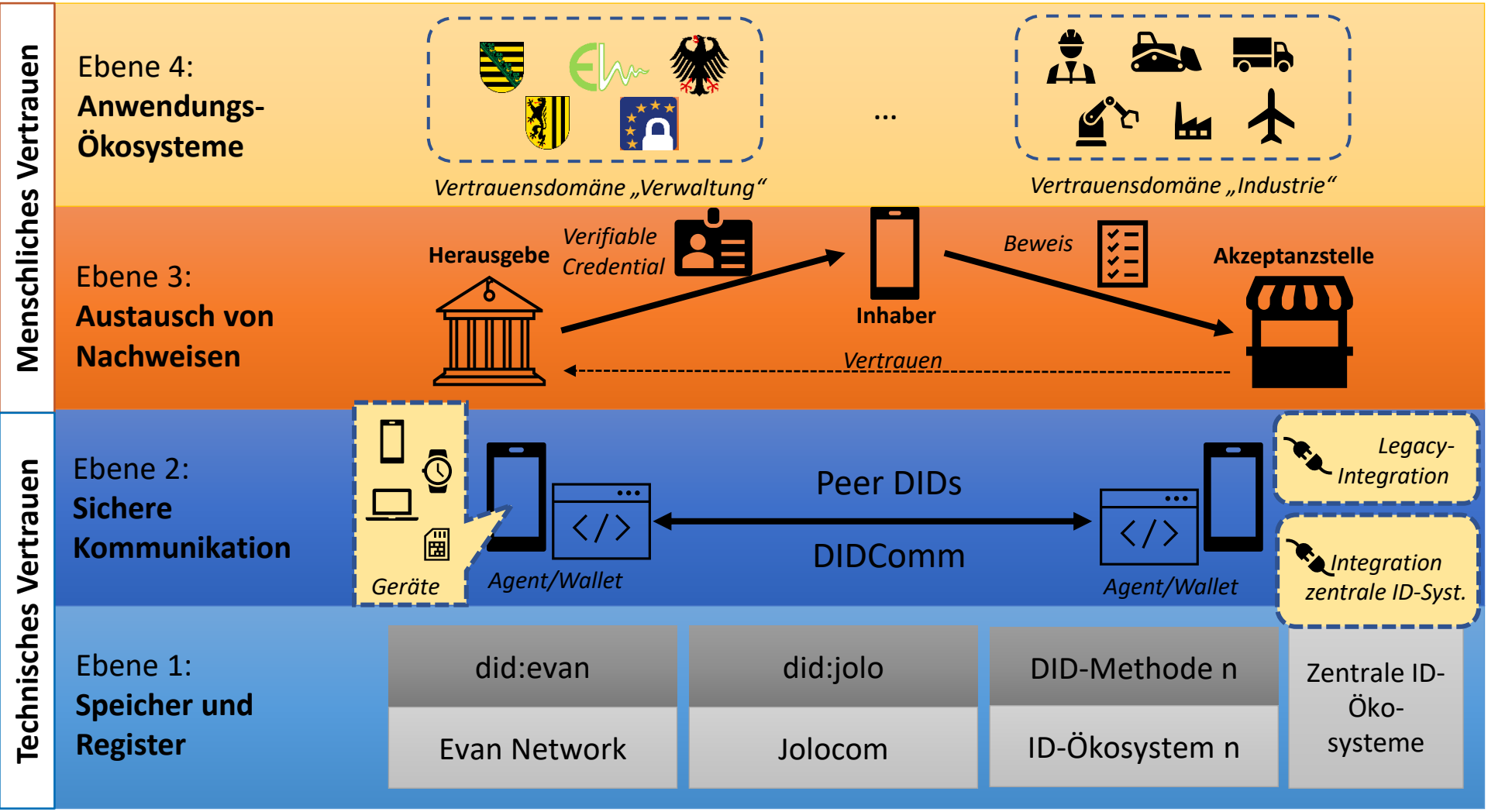
SSI-Wallets

nPA als Basisidentität

Vorteil für Nutzer: Freie Auswahl eines Dienstes, der vielfältig einsetzbar ist.

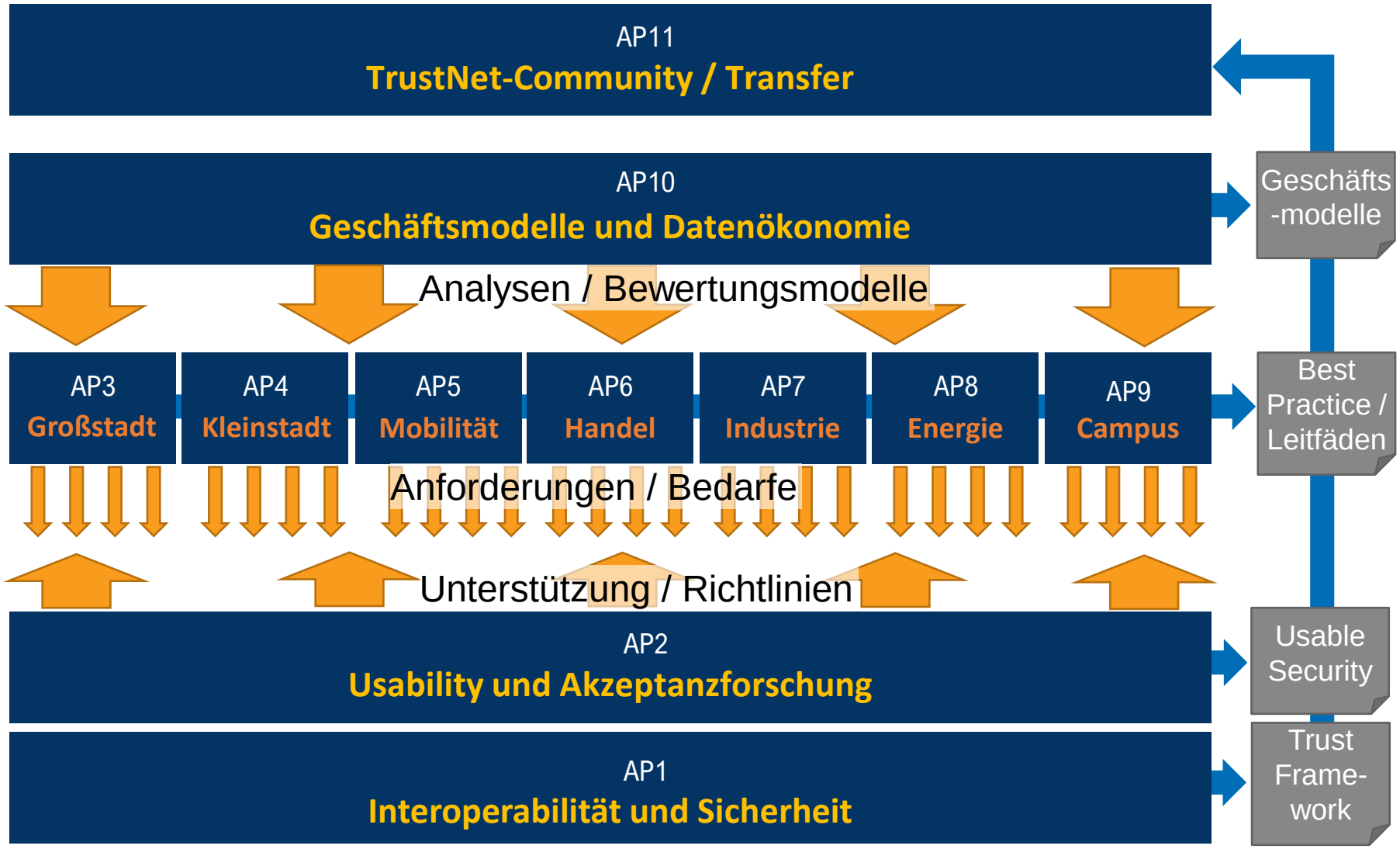
Besucher | Bürger | Unternehmen

Referenzarchitektur nach dem „Trust over IP“ Stack

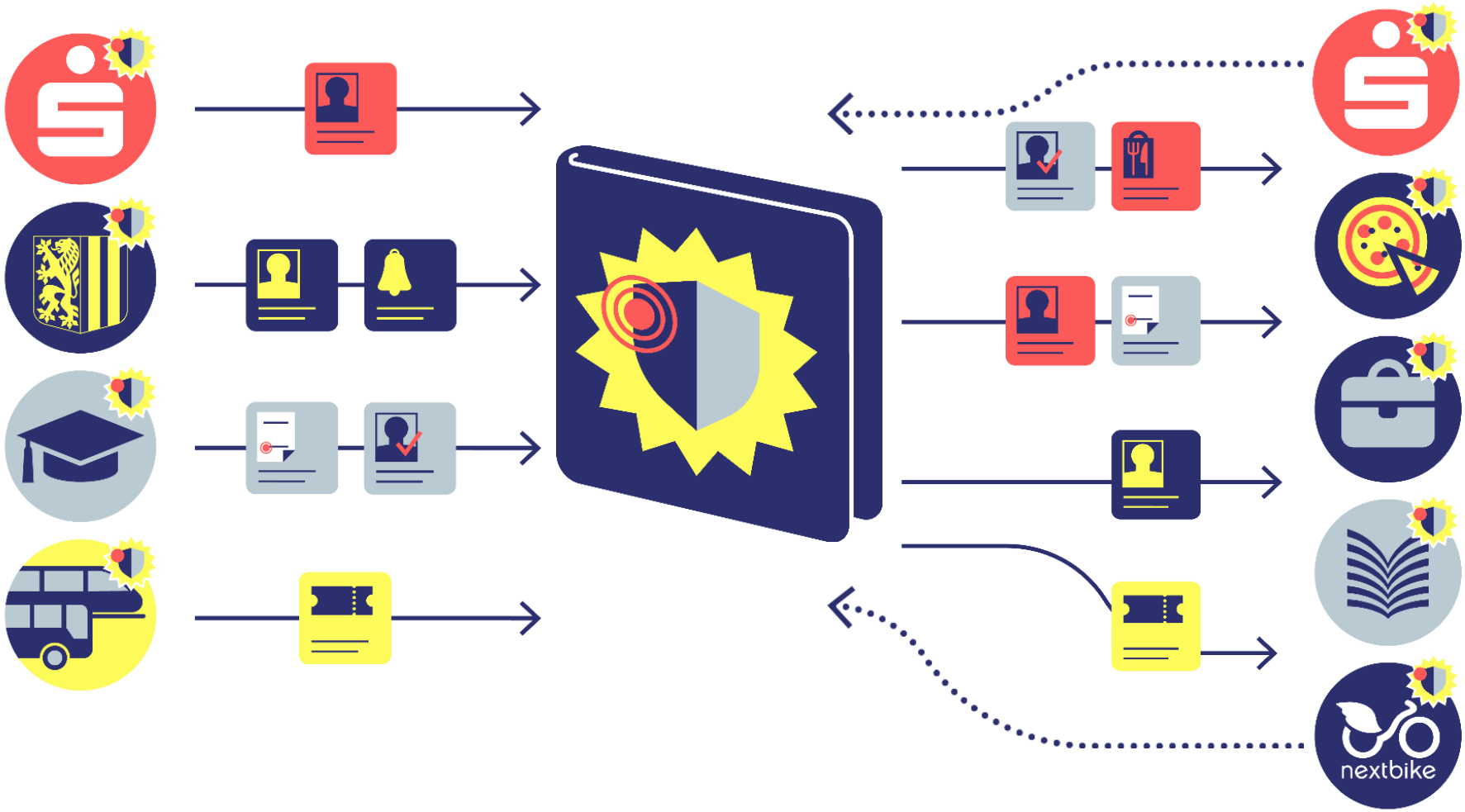


Siehe auch https://trustoverip.org/ und https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0289-toip-stack

Zusammenarbeit im Projekt



Ziel: Universelle Nutzung interoperabler Identitäten



Welche Szenarien werden im Kontext einer Großstadt umgesetzt?

- Beispiel Landeshauptstadt Dresden.

Offene Fragen / Diskussion

https://commons.wikimedia.org/wiki/File:Oliver_Tacke_-_Diskussion.png (CC-BY-SA)

Themen für die Diskussion

Resilienz

- Ausfall / Manipulation von Identity Providern beeinträchtigen Nutzer nicht
- Weniger direkte Verbindungen zwischen Backend-Systemen zur Bestimmung von Nutzer-Eigenschaften erforderlich

Souveränität

- Globale Identity Provider (Google, Facebook, …) verlieren an Macht gegenüber Nutzer
- Transparenz und Kontrolle des Umfangs bereitgestellter Daten und ihrer Empfänger

Neuorganisation des Datenmanagements

- Ad-Hoc Kundenbeziehungen statt vorgeschalteter Registrierung
- Speicherung von Nutzerdaten beim Service Provider nicht mehr erforderlich → Vereinfachung von GDPR-Compliance und Verbesserung Datenqualität

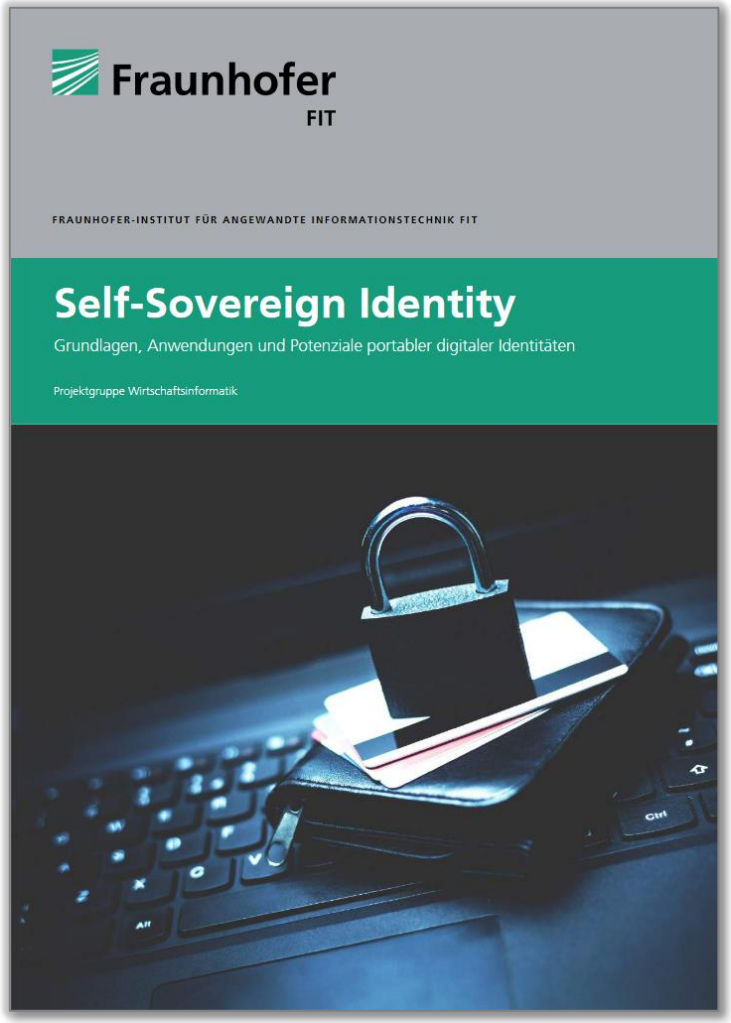
Vielen Dank für ihre Aufmerksamkeit!

Prof. Dr.-Ing. Jürgen Anke

HTW Dresden
Professur für Softwaretechnologie und Informationssysteme
Fakultät Informatik/Mathematik
Friedrich-List-Platz 1
01069 Dresden

Email: juergen.anke@htw-dresden.de

Informationen für den Einstieg



https://www.fim-rc.de/wp-content/uploads/2021/06/Fraunhofer-FIT_SSI_Whitepaper.pdf

Open Access

HMD (2021) 58:247–270
https://doi.org/10.1365/s40702-021-00711-5

SCHWERPUNKT

Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten

Tobias Ehrlich · Daniel Richter · Michael Meisel · Jürgen Anke

Eingegangen: 30. November 2020 / Angenommen: 4. Februar 2021 / Online publiziert: 22. Februar 2021

Zusammenfassung In diesem Beitrag werden die Rolle digitaler Identitäten für eine funktionierende digitale Wirtschaft thematisiert und Anforderungen an das Management digitaler Identitäten abgeleitet. Bislang hat sich kein Ansatz für das Management digitaler Identitäten in der Breite etabliert, was zu einer Fragmentierung der ID-Landschaft sowie einer Vielzahl von Benutzerkonten für den Anwender führt. Mangels Standards ist zudem die Interoperabilität von digitalen Identitäten eingeschränkt. Dies führt zu einer Reihe von Problemen, die den effizienten und sicheren Umgang mit digitalen Identitäten behindern. Abhilfe verspricht das Konzept der Self-Sovereign Identities (SSI) und den damit verbundenen Standards „Verifiable Credentials“ und „Decentralized Identifiers“. Sie erlauben den flexiblen Austausch von manipulationssicheren digitalen Nachweisen zwischen Benutzern und Systemen und bilden damit die Grundlage für den Aufbau von Vertrauensbeziehungen im digitalen Raum. In diesem Beitrag werden das SSI-Paradigma vorgestellt und die Hürden diskutiert, die dem breitenwirksamen Einsatz dieses Konzepts entgegenstehen. Damit erhält der Leser einen kompakten Überblick verschiedener Ansätze für das Identitätsmanagement und die Potenziale selbst-souveräner Identitäten. Für die

T. Ehrlich · J. Anke (✉)
Hochschule für Technik und Wirtschaft (HTW) Dresden, Friedrich-List-Platz 1, 01069 Dresden, Deutschland
E-Mail: juergen.anke@htw-dresden.de

T. Ehrlich
E-Mail: tobias.ehrlich@htw-dresden.de

D. Richter
SAP Deutschland SE & Co. KG, Hasso-Plattner-Ring 7, 69190 Walldorf, Deutschland
E-Mail: daniel.richter@sap.com

M. Meisel
Fakultät CB, Hochschule Mittweida, Technikumplatz 17, 09648 Mittweida, Deutschland

https://link.springer.com/content/pdf/10.1365/s40702-021-00711-5.pdf

Ausgewählte Quellen

[PR20] Preukschat, A. & Reed, D. (2020): „Self-Sovereign Identity - Decentralized Digital Identity and Verifiable Credentials”, Manning Publications.

[ER+21] Ehrlich, T., Richter, D., Meisel, M., Anke, J. (2021): „Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten“, HMD – Praxis der Wirtschaftsinformatik, Band 338.

W3C „Verifiable Credentials“: https://www.w3.org/TR/vc-data-model/

W3C „Decentralized Identifiers“: https://www.w3.org/TR/did-core/