Self-sovereign Identity

Ideologie, Paradigma, Standards und aktuelle Entwicklungen

Christoph Menzer
Fakultät CB | BCCM

30. September 2020

HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

Inhalt

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Digitale Identität

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

> *Eine digitale Identität ist eine Sammlung elektronischer Daten zur Charakterisierung eines Internetnutzers mit einer physischen Identität.*

Daten, die zu einer digitalen Identität gehören, sind z.B.:

- Nutzername
- E-Mail-Adresse
- Wohnanschrift
- Kontonummer
- Passwort

(Tietz u. a. 2017, S. 13)

Digitale Identität

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

- jene Daten werden als Attribute bezeichnet
- ein physischer Nutzer kann sich im Internet mit vielen verschiedenen digitalen Identitäten bewegen (anderer Nutzername, andere E-Mail usw.)
- es gibt verschiedene Rollen, z.B. „privat“, „staatlich“und „geschäftlich“

Authentifizierung

- Bindung an den jeweiligen physischen Nutzer muss sichergestellt werden
- die Überprüfung findet in Form eines Anmeldeprozesses (Login) statt
- der Nutzer muss beweisen, dass er Besitzer einer digitalen Identität ist, d.h., er muss sich *authentifizieren*
- Passwörter, PIN, Fingerabdruck, Gesichtserkennung, Chipkarten usw.

(Tietz u. a. 2017, S. 13)

Digitale Identität

Ansätze des Identitätsmanagements I

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

- isoliertes Identitätsmanagement
  - jeder Dienst verwaltet seine Nutzer selbst
  - am weitesten im Internet verbreitet
- zentralisiertes Identitätsmanagement
  - zentrale Einheit, die Nutzer verwaltet und Anmeldeprofile speichert, die andere Einheiten abrufen können
  - auch als Identitätsprovider (IdP) bezeichnet
  - z.B. Social-Logins, LDAP, Active Directory

(Tietz u. a. 2017, S. 13)

Digitale Identität

Ansätze des Identitätsmanagements II

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

- dezentralisiertes Identitätsmanagement
  - mehrere Identitätsprovider, die benutzt werden können
  - der Dienst muss den Identitätsprovider im Vorfeld nicht kennen (Auflösung durch URL), jedoch auf seine Aussage vertrauen
  - z.B. OpenID
- föderiertes (federated) Identitätsmanagement
  - Föderation bzw. einen Vertrauenskreis (Circle of Trust) von Diensten und Identitätsprovidern, die gegenseitig ihren Identitätsinformationen vertrauen
  - z.B. WS-Federation, Kantara Initiative

(Tietz u. a. 2017, S. 13)

Self-sovereign Identity

Definition, Prinzipien, Ideologie

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

- Self-sovereign Identity (SSI, dt. Selbst-souveräne Identität)
- Modell für digitale Identitäten, bei dem der Nutzer einer Identität in die Lage versetzt wird, alle Handlungen und Informationen bezüglich seiner Identität selbst zu verwalten
- Über eine genaue Definition, was SSI ausmacht, herrscht noch kein Konsens
- Einen ersten allgemeingültigen Definitionsversuch unter Aufstellung von zehn Prinzipien, die diese auszeichnen, gibt Christopher Allen in seinem Blogpost „The Path to Self-Sovereign Identity“ (Allen 2016)

Prinzipien nach Allen (2016) I

Existence (Existenz) jeder Nutzer hat eine unabhängige Existenz, d.h eine SSI basiert auf einer realen/physischen Persönlichkeit und kann nicht ausschließlich in der digitalen Welt existieren.

Control (Kontrolle) jeder Nutzer sollte die alleinige Kontrolle über seine Identität haben.

Access (Zugriff) der Nutzer sollte zu jeder Zeit uneingeschränkten Zugriff zu seinen Daten haben. Das heißt allerdings nicht, dass der Nutzer seine Daten jederzeit bearbeiten kann.

Transparency (Transparenz) die Algorithmen, über die Identitäten verwaltet werden, müssen frei und quelloffen und weitestgehend unabhängig von speziellen Systemarchitekturen sein. Ähnliches gilt für die Netzwerke, die zur Identitätsverwaltung genutzt werden.

Prinzipien nach Allen (2016) II

Persistence (Persistenz) Identitäten sollten für immer, oder wenigstens so lange, wie der Nutzer es wünscht, gültig sein.

Portability (Portabilität) Identitäten sollten nicht an ein bestimmtes Netzwerk gebunden sein.

Interoperability (Interoperabilität) Identitäten sollten wenn möglich überall, d.h. über Landesgrenzen und Grenzen digitaler Systeme hinweg, nutzbar sein.

Consent (Zustimmung) jede Freigabe von persönlichen Informationen gegenüber Dritten erfordert die Zustimmung des Nutzers.

Prinzipien nach Allen (2016) III

Minimalization (Minimalismus) es sollte möglich sein, nur Informationen freizugeben, die unbedingt notwendig sind. Typisches Beispiel ist der Nachweis eines bestimmten Alters. Wenn nur gefragt ist, ob man älter als 18 Jahre alt ist, sollte auch nur diese Information zur Verfügung gestellt werden und nicht etwa das genaue Alter oder gar das Geburtsdatum.

Protection (Schutz) die Freiheiten und Rechte eines Nutzers wiegen höher als die Interessen des Identitätsnetzwerkes und sollten geschützt werden.

Self-sovereign Identity

Definition, Prinzipien, Ideologie

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

- weiterer Ansatz: „A Technology-Free Definition of Self-Sovereign Identity“ von Andrieu (2016)
- Blockchain Bundesverband (Kai Wagner u. a. 2018, S. 5):

  We use the terminology of SSI, as an identity model that allows an individual or entity to have sole control of their digital identity expressed through the use of one or more decentralised identifiers or “DIDs.”

  ...

Self-sovereign Identity

Standards und Initiativen

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

- W3C Working Draft: *Decentralized Identifiers (DIDs) v1.0* (2019)
- Draft Community Group Report: *Decentralized Identifier Resolution (DID Resolution) v0.2* (2019)
- W3C Recommendation: *Verifiable Credentials Data Model 1.0* (2019)

- Decentralized Identity Foundation (DIF)
- Internet Identity Workshop (IIW)
- Rebooting Web-of-Trust (RWOT) Design Workshop
- SSI Meetup
- International Organization for Standardization (ISO)
- ID2020 Alliance
- Blockchain-Bundesverband

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Decentralized Identifiers (DIDs)

Decentralized Identifiers (DIDs)

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

> *Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, „self-sovereign“ digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority.*

Beispiel

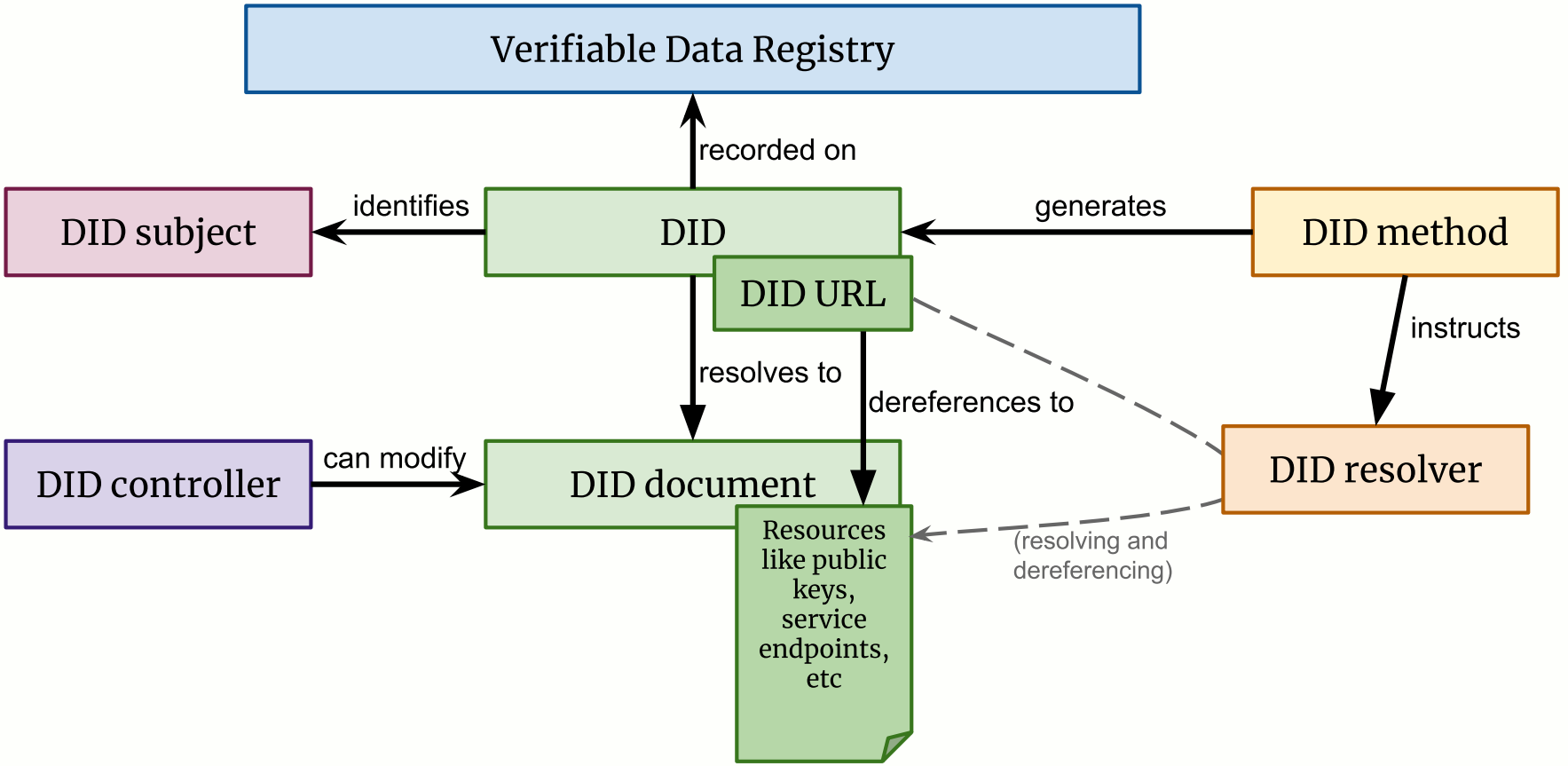
did:example:123456789abcdefghi

- eine DID besteht aus Schema:Methode:Identifier
- an eine DID ist ein DID Document gebunden
- DID enthält aufgrund der Methode bereits Routing-Informationen, damit ist sie an eine bestimmte *Verifiable Data Registry* gebunden
- Ähnlichkeit zur E-Mail-Adresse: 123456789abcdefghi@example.did
- in vielen DID-Methoden enthält der DID-Suffix kryptografisches Material (z.B. den Hash eines Öffentlichen Schlüssels)

(*Decentralized Identifiers (DIDs) v1.0* 2019)

Decentralized Identifiers (DIDs)

Architektur



(*Decentralized Identifiers (DIDs) v1.0* 2019)

Decentralized Identifiers (DIDs)

DID-Document

*A DID document is the resource that is **associated with** a decentralized identifier (DID). DID documents typically express **verification methods** (such as public keys) and **services** that can be used to interact with a DID controller.*

- Context
- Subject
- Public Keys
- Authentication
- Authorization and Delegation
- Service Endpoints
- Created
- Updated
- Proof
- Extensibility

(*Decentralized Identifiers (DIDs) v1.0* 2019)

Decentralized Identifiers (DIDs)

DID-Document

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

Das DID-Document sollte/darf keine persönlichen Informationen (personally identifiable information, PII) enthalten!

Decentralized Identifiers (DIDs)

DID-Method

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

Schemas

- Die Methodenspezifikation muss genau ein bestimmtes DID-Schema definieren
- sie muss durch genau einen Methodennamen identifiziert werden können
- die DID-Methodenspezifikation für das spezifische DID-Schema muss angeben, wie die methodenspezifische ID-Komponente einer DID zu erzeugen ist
- dafür bedarf es keines zentralen Registrierungsdienstes

Operationen

- Erstellen (create)
- Abrufen (read/verify)
- Aktualisieren (update)
- Deaktivieren (deactivate)

(*Decentralized Identifiers (DIDs) v1.0* 2019)

Decentralized Identifiers (DIDs)

DID-Method

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

*A DID method specification **MUST define exactly one method-specific DID scheme**, identified by exactly one method name. For more information, see the method-name rule in Section § 5.1 Generic DID Syntax.*

*The DID method specification for the method-specific DID scheme **MUST specify how to generate the method-specific-id** component of a DID.*

*The method-specific-id value MUST be able to be generated **without** the use of a **centralized registry service**.*

(*Decentralized Identifiers (DIDs) v1.0* 2019)

Decentralized Identifiers (DIDs)

DID-Method

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

- der Methodenname sollte eindeutig sein
- keine zentrale Behörde für die Zuweisung oder Genehmigung von DID-Methodennamen
- Die W3C Credentials Community Group führt eine nicht autorisierende Liste bekannter DID-Methodennamen
- mehr als 70 solcher Methoden bisher gelistet

Decentralized Identifiers (DIDs)

DID-Method

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

DID Method Registry

A registry for Decentralized Identifier Methods

Draft Community Group Report 17 January 2020

Latest editor's draft:
https://w3c-ccg.github.io/did-method-registry/

Editors:
Manu Sporny (Digital Bazaar)
Drummond Reed (Evernym)

Author:
Credentials Community Group (W3C)

Participate:
GitHub w3c-ccg/did-method-registry
File a bug
Commit history
Pull requests

(*DID Method Registry* 2019)

Decentralized Identifiers (DIDs)

DID-Resolution

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

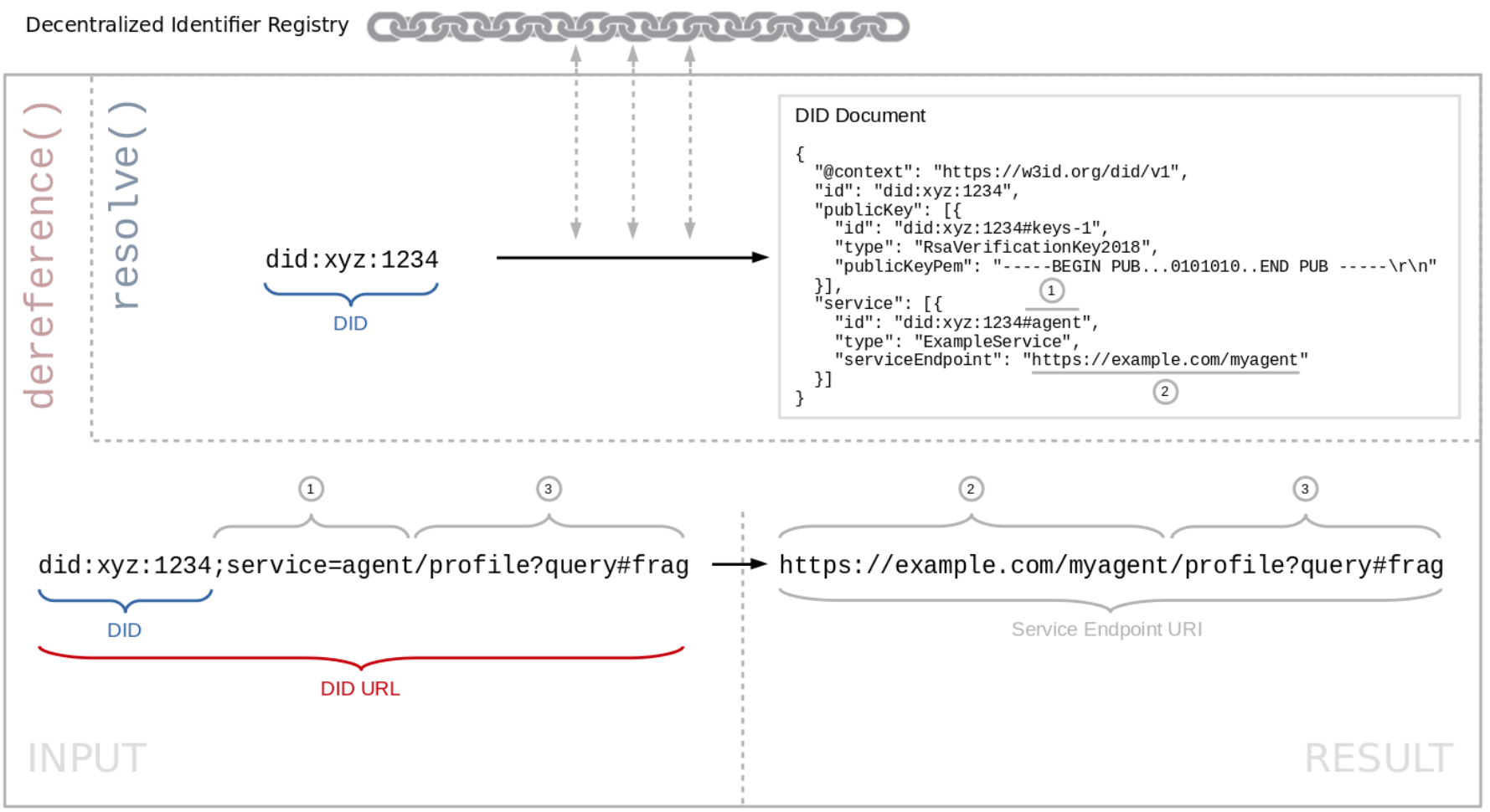
*DIDs **resolve** to DID Documents – simple documents that describe **how to use** that specific DID.*

- Auflösen von DIDs und Dereferenzierung von DID-URLs
- DID-Resolution ist der Prozess zur Erlangung eines DID-Dokuments für einen bestimmten DID
- DID-URL-Dereferenzierung ist der Prozess des Abrufs einer Repräsentation einer Ressource für eine bestimmte DID-URL
- Die Algorithmen müssen von einem konformen DID-Resolver implementiert werden.

(*Decentralized Identifier Resolution (DID Resolution) v0.2* 2019)

Decentralized Identifiers (DIDs)

DID Resolution



(*Decentralized Identifier Resolution (DID Resolution) v0.2* 2019)

Decentralized Identifiers (DIDs)

DID Resolution

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

Self-sovereign identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating user autonomy. To accomplish this, a self-sovereign identity must be transportable; ***it can't be locked down to one site or locale****.*

- Christopher Allen -

(vgl. Kai Wagner u. a. 2018)

Decentralized Identifiers (DIDs)

DID Resolution

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

Self-sovereign identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating user autonomy. To accomplish this, a self-sovereign identity must be transportable; ***it can't be locked down to one site or locale****.*

- Christopher Allen -

(vgl. Kai Wagner u. a. 2018)

Widerspruch?

Decentralized Identifiers (DIDs)

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Was „verankert“ die Verifiable Data Registry eigentlich?

- sie stellt in erster Linie die Verbindung zwischen Identifier und Öffentlichen Schlüssel(n) her
- vgl. Zertifikat (z.B. x.509, PGP) und DID-Document

Wozu brauche ich das?

- die Öffentlichen Schlüssel für einen Identifier können sich im Laufe der Zeit ändern (Verlust, Diebstahl etc.)
- z.T. werden verschiedene Öffentliche Schlüssel für Signaturen und/oder zur Verschlüsselung benötigt
- nützliche Erweiterungen: z.B. Service Endpoints

Exkurs: ECDSA

- für Blockchains, die den *Elliptic Curve Digital Signature Algorithm (ECDSA)* verwenden, gilt: Transaktionen haben kein from-Feld, da sich der Öffentliche Schlüssel aus der Signatur berechnen lässt

Signature Prefix Value (v) und Public Key Recovery I

- Signatur besteht aus r (x-Koordinate) und s (Signatur)
- aus r können wir zwei Punkte auf der Kurve R und R' berechnen (Symmetrie zur X-Achse)
- r hat außerdem ein multiplikatives Inverses r^{-1}
- wir ermitteln weiterhin z, was das n-niedrigste Bit des Hashes der Nachricht ist, wobei n die Ordnung der Kurve ist

(Antonopoulos und Wood 2018, S. 120 ff.)

Exkurs: ECDSA

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

Signature Prefix Value (v) und Public Key Recovery II

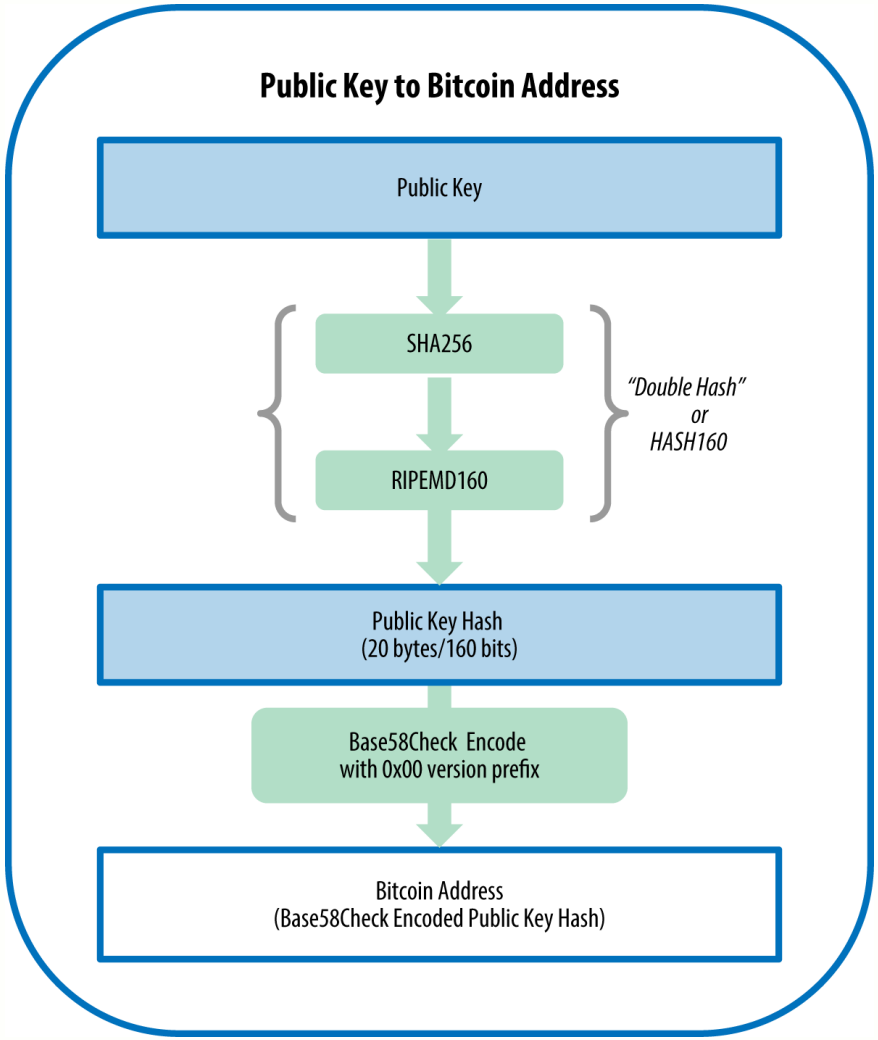
- die möglichen Schlüssel berechnen sich dann aus

$$K_1 = r^{-1}(sR - zG) \text{ und } K_2 = r^{-1}(sR' - zG)$$

- G ist der Generator-Punkt der Kurve
- um nicht jedes Mal ausprobieren zu müssen, wurde zusätzlich zur Signatur der Prefix v eingeführt
  - wenn v gerade ist, dann ist R korrekt
  - wenn v ungerade ist, dann ist R' korrekt

(Antonopoulos und Wood 2018, S. 120 ff.)

Exkurs: Bitcoin-Adressen



- Bitcoin- oder ähnliche Adressen sind grundlegend ebenfalls Identifier

(Antonopoulos 2015, S. 72)

Decentralized Identifiers (DIDs)

Authentifizierung

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

- dieser Mechanismus lässt sich prinzipiell auch ohne eine Verifiable Data Registry zur Authentifizierung nutzen

Problem

- der Zusammenhang zwischen Öffentlichem Schlüssel und Identifier ist fix

Lösungen

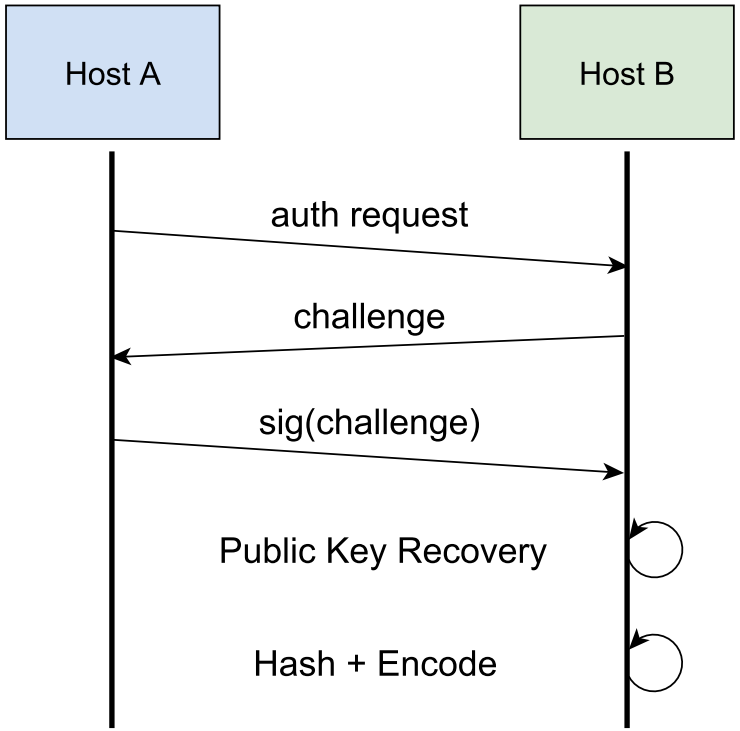
- sehr geschickt: BTCR-Methode (*BTCR DID Method* 2019)
- sehr flexibel: ETHR-Methode / *ERC-1056* (2018)
- 2nd-Layer: Sidetree
- ohne Blockchain: Key Event Receipt Infrastructure (KERI, Smith 2019), Peer-DID (*Peer DID Method Specification* 2020)
- u.v.m.

Decentralized Identifiers (DIDs)

Authentifizierung

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

- einfache Authentifizierung mit Bitcoin- oder ähnlichen Adressen/Identifiern (u.a. DIDAuth)



Problem

- nicht resistent gegenüber *Men-in-the-Middle*-Angriffen

Lösungen

- DIDComm / DID Exchange (Aries RFC 0434, Aries RFC 0023)
- TLS (ungünstig)
- Challenge verschlüsseln (Auth-Request + PubKey)
- andere Kanalsicherungen, z.B. mit Diffie-Hellman-Schlüsselaustausch o.ä.

Verifiable Credentials

Verifiable Credentials

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

*A verifiable credential can represent all of the same information that a **physical credential** represents. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts.*

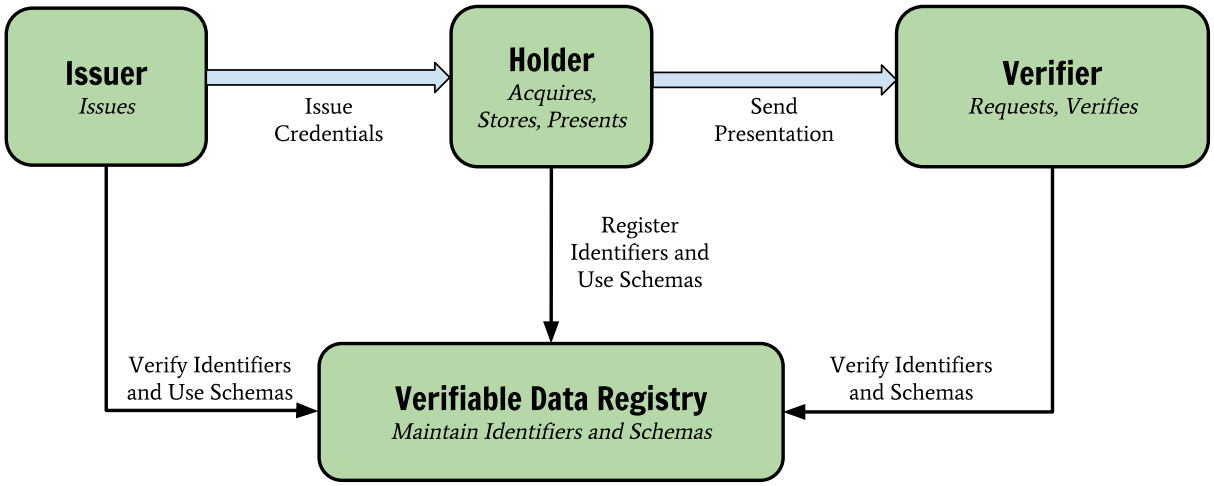
*Holders of verifiable credentials can generate **verifiable presentations** and then share these verifiable presentations with verifiers to prove they possess verifiable credentials with certain characteristics.*

(*Verifiable Credentials Data Model 1.0* 2019)

Verifiable Credentials

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Rollen



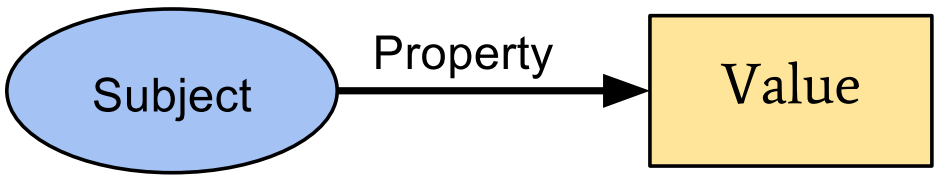
- Subject
- Holder/Owner
- Issuer
- Verifier
- Verifiable Data Registry

(*Verifiable Credentials Data Model 1.0* 2019)

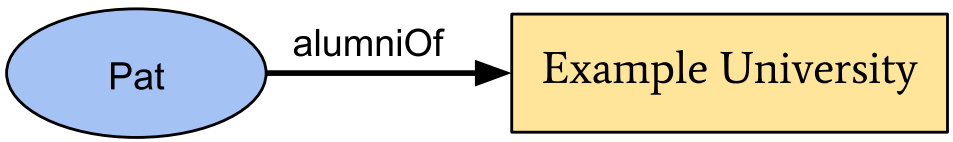
Verifiable Credentials

Claims

A claim is a statement about a subject. A subject is a thing about which claims can be made. Claims are expressed using subject-property-value relationships.



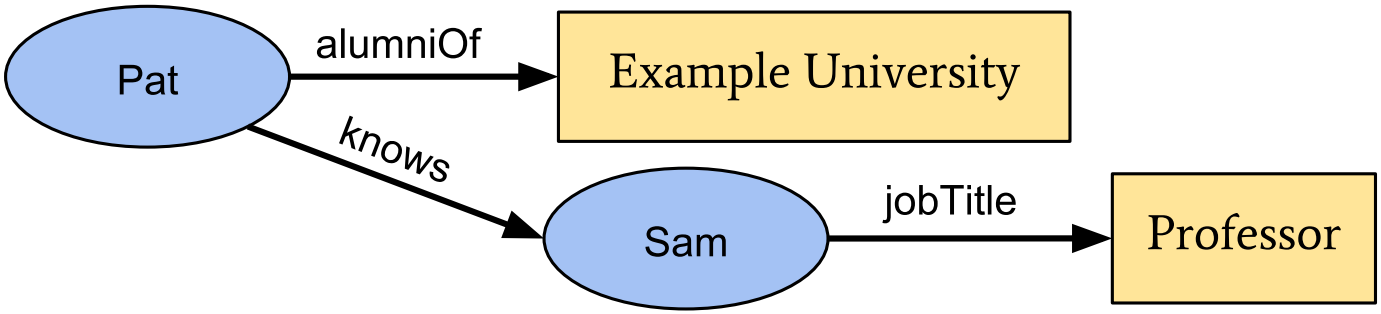
Beispiel



(*Verifiable Credentials Data Model 1.0* 2019)

Verifiable Credentials

Claims



(*Verifiable Credentials Data Model 1.0* 2019)

Verifiable Credentials

Claims

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

Beispiel

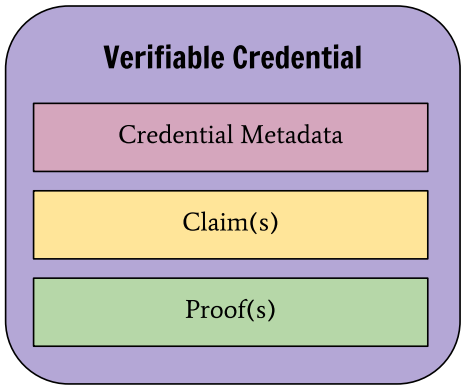
```
"alumniOf": {
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
      "name": [{
        "value": "Example University",
        "lang": "en"
      }, {
        "value": "Exemple d'Université",
        "lang": "fr"
      }]
    }
```

Verifiable Credentials

Credentials

A credential is a set of one or more claims made by the same entity.

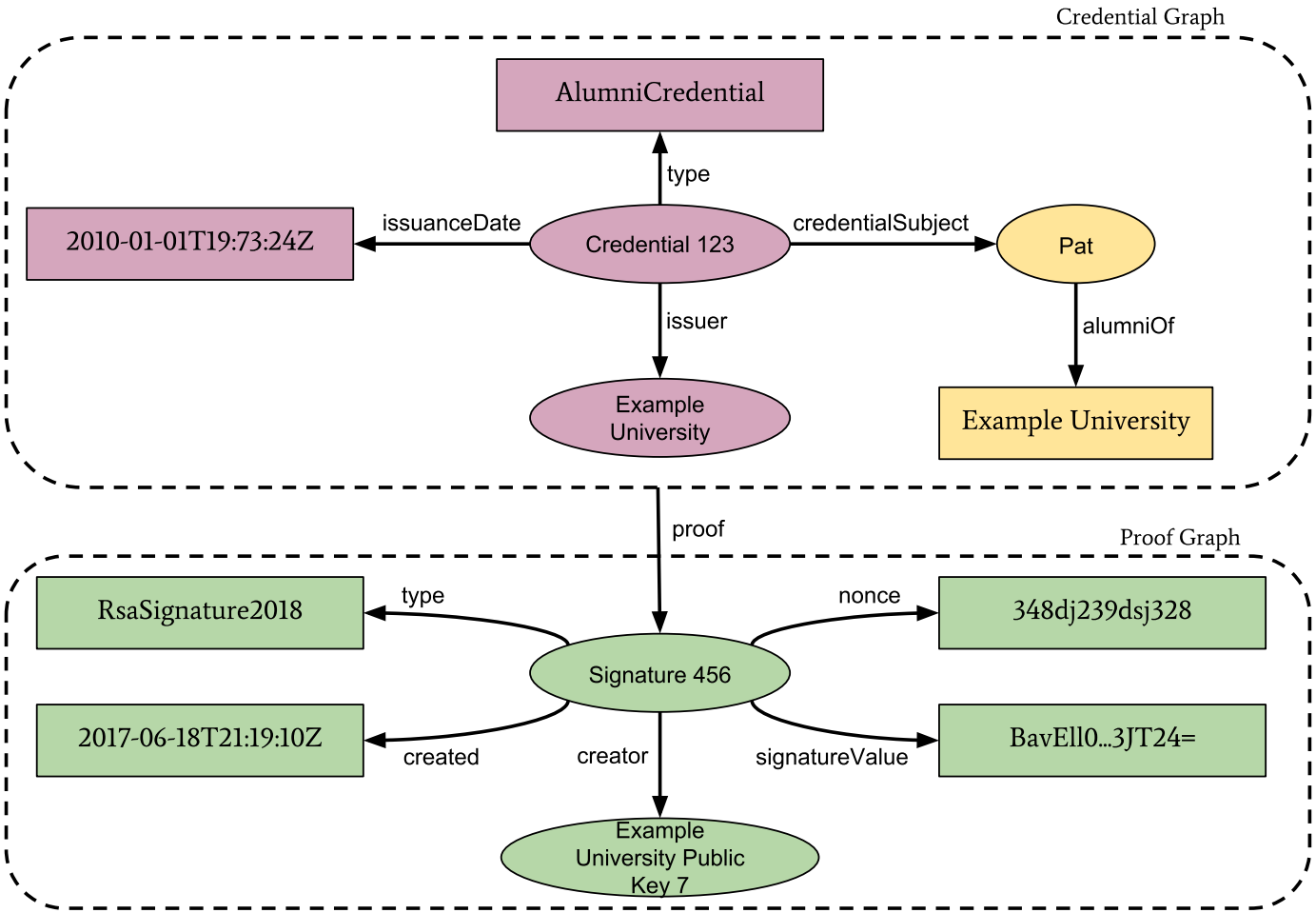
- kann auch einen Identifikator und Metadaten zur Beschreibung der Eigenschaften enthalten:
  - Ablaufdatum und -zeit
  - ein repräsentatives Bild
  - einen öffentlichen Schlüssel für Verifizierungszwecke
  - den Widerrufsmechanismus
- Metadaten können ebenfalls vom Issuer signiert sein
- manipulationssichere Claims und Metadaten, die kryptografisch belegen, wer sie ausgestellt hat



(*Verifiable Credentials Data Model 1.0* 2019)

Verifiable Credentials

Credentials



(*Verifiable Credentials Data Model 1.0* 2019)

Verifiable Credentials

Credentials

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Beispiel

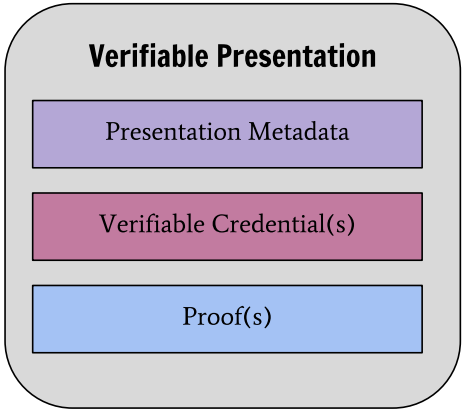
```
{
  "issuer": "https://example.edu/issuers/565049",

  "credentialSubject": {

    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

    "alumniOf": {
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
      "name": [{
        "value": "Example University",
        "lang": "en"
      }, {
        "value": "Exemple d'Université",
        "lang": "fr"
      }]
    }
  },
  "proof": {
  ...
  }
}
```

Verifiable Credentials

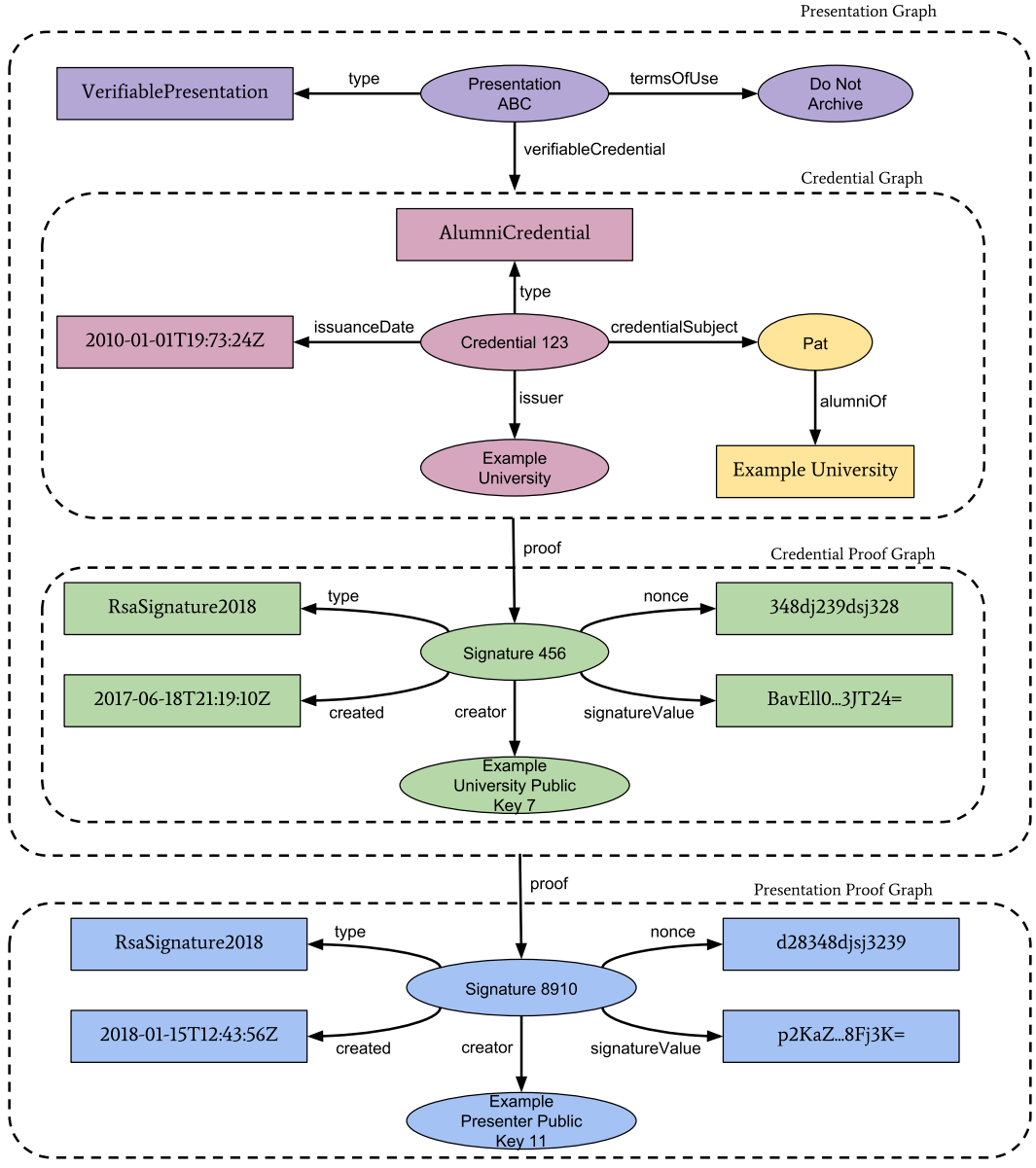
Presentations

A verifiable presentation expresses data from one or more verifiable credentials, and is packaged in such a way that the authorship of the data is verifiable.

- die Daten in einer Präsentation beziehen sich oft auf dasselbe Subjekt, können aber von mehreren Ausstellern ausgegeben worden sein
- die Aggregation dieser Informationen drückt typischerweise einen Aspekt einer Person, Organisation oder Einheit aus
- auch Präsentationen mit mehreren Credentials über verschiedene Subjekte sind möglich



(*Verifiable Credentials Data Model 1.0* 2019)



(*Verifiable Credentials Data Model 1.0* 2019)

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

Beispiel I

```
{
  "type": "VerifiablePresentation",

  "verifiableCredential": [{

    "issuer": "https://example.edu/issuers/565049",

    "credentialSubject": {

      "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",

      "alumniOf": {
        "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
        "name": [{
          "value": "Example University",
          "lang": "en"
        },
```

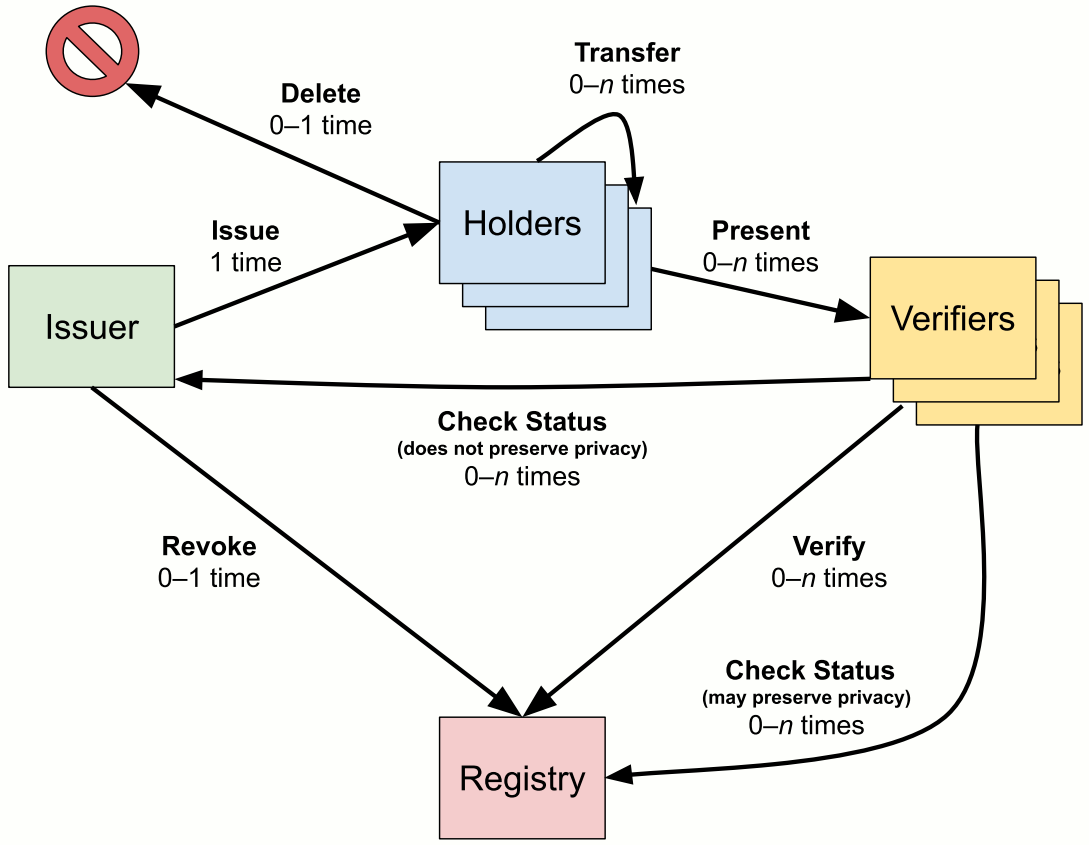
HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

Beispiel II

```
          {
            "value": "Exemple d'Université",
            "lang": "fr"
          }]
        }
      },
      "proof": {

      }
    }],

    "proof": [{

    }]
}
```

Verifiable Credentials

Lebenszyklus



(*Verifiable Credentials Data Model 1.0* 2019)

Verifiable Credentials

Lebenszyklus

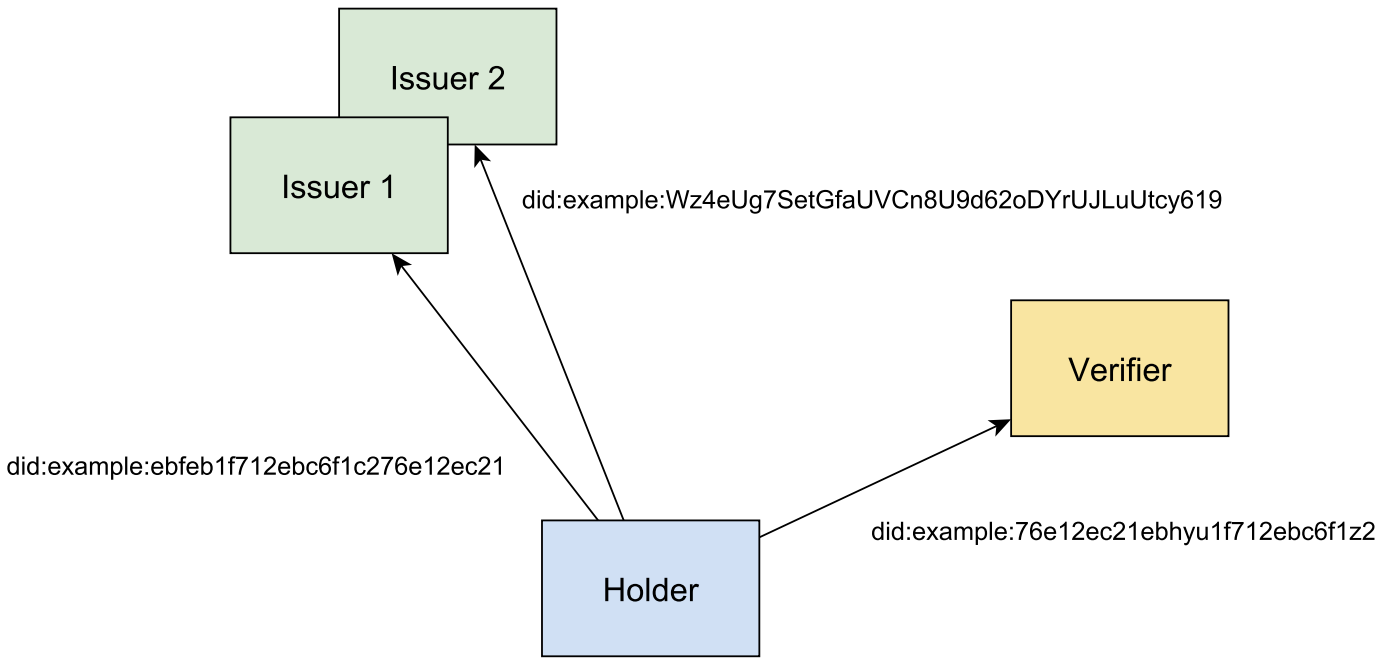
HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

- ein Issuer stellt einem Holder ein Verifiable Credential aus. Die Ausstellung erfolgt immer vor allen anderen Aktionen, die ein Credential betreffen
- ein Holder kann einen oder mehrere seiner Credentials auf einen anderen Inhaber übertragen
- ein Inhaber legt einen oder mehrere seiner Credentials einem Verifier vor, optional innerhalb einer Verifiable Presentation
- ein Verifier überprüft die Authentizität der vorgelegten Presentation und der Credentials. Dazu sollte auch die Überprüfung des Status für den Widerruf der Credentials gehören.
- ein Issuer könnte ein Credential widerrufen
- ein Inhaber kann ein Credential löschen.

Verifiable Credentials

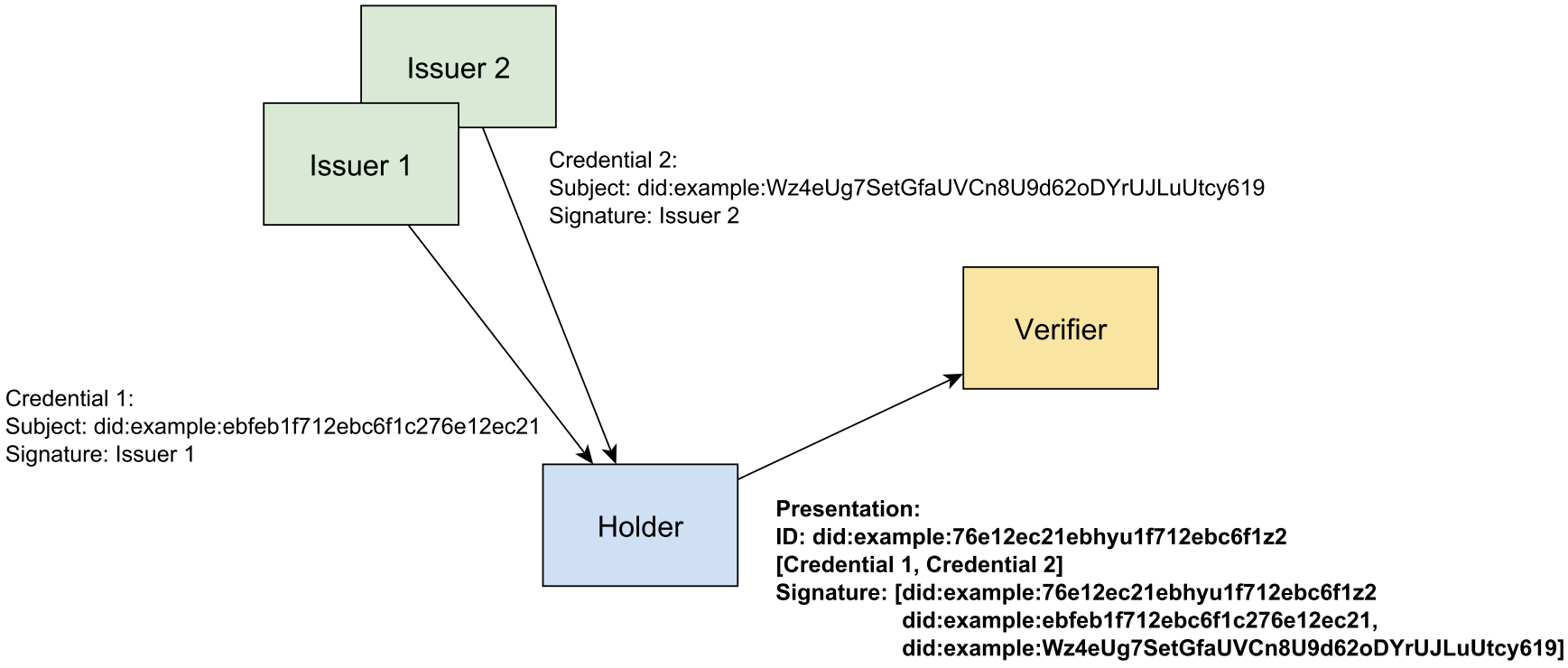
Anti-Korrelation

- Credentials könnten für unterschiedliche DIDs ausgestellt werden
- Nachweis der Eigentümerschaft durch mehrere Signaturen/Self-issued-Credentials in der Presentation (Pairwise DIDs)
- verhindert Korrelation nur gegenüber den Issuern, aber nicht in jedem Fall gegenüber den Verifiern



Verifiable Credentials

Anti-Korrelation



- DID könnte nun als URI/URL eines jeweiligen Credentials gesehen und zum Eigentümer aufgelöst werden (Service Endpoints evtl. nützlich)

Zusammenfassung

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES

- Benutzer können ihre digitale Identität nicht kontrollieren. Im besten Fall kontrollieren sie ihre Geräte/Software, und diese kontrollieren die digitale Identität
- eine digitale Identität besteht aus einem Identifier und verifizierbaren Eigenschaften
  - der Identifier wird durch einen Decentralized Identifier (DID) dargestellt
  - Eigenschaften werden durch Verifiable Credentials (VCs) ausgedrückt
- einmal offengelegte Informationen (in VCs) können nicht entzogen oder zurückgezogen werden
- öffentlich zugänglich müssen sein:
  - letzte Rotation/Änderung von Schlüsseln
  - Widerrufslisten/Zertifikatssperrlisten (Revocation Lists) von Credentials
  - Credential-Schemas und deren Semantik

Vielen Dank

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Was fehlt...

- Decentralized Key Management Systems (DKMS; z.B. Secret-Sharing, Multisig etc.)
- Vertrauensmodelle/Trust-Frameworks
- Herstellung von Vertrauen in die Anwendersoftware
- Bereitstellung von Revocation Lists
- Bereitstellung von Credential-Schemas und deren Semantik
- sichere Speicherung von Credentials (lokal, Hubs, Backups usw.)
- CL-Signaturen und Zero-Knowledge-Proofs

Was bleibt...

- Vielen Dank für Ihre Aufmerksamkeit
- Bei Fehlern, Anmerkungen oder Kritik: kommen Sie gern auf mich zu

Vielen Dank

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Christoph Menzer
Projektmitarbeiter

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät CB| BCCM

T +49 (0) 3727 58-1175
F +49 (0) 3727 58-21175

menzer@hs-mittweida.de
https://blockchain.hs-mittweida.de/

Haus 6 | Grunert de Jácome Bau | Raum 6.04.23
Technikumplatz 17| 09648 Mittweida

Literatur I

Allen, Christopher (25. Apr. 2016). *The Path to Self-Sovereign Identity*. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html (besucht am 27. 04. 2020).

Andrieu, Joe (Okt. 2016). *A Technology-Free Definition of Self-Sovereign Identity*. URL: https://github.com/WebOfTrustInfo/rwot3-sf/blob/master/topics-and-advance-readings/a-technology-free-definition-of-self-sovereign-identity.pdf (besucht am 27. 09. 2020).

Antonopoulos, Andreas M. (2015). *Mastering Bitcoin*. First edition. Sebastopol CA: O'Reilly. 272 S. ISBN: 978-1-4493-7404-4 978-1-4919-0260-8.

Antonopoulos, Andreas M. und Gavin A. Wood (4. Dez. 2018). *Mastering Ethereum: Building Smart Contracts and DApps*. 1. Aufl. Farnham: O'Reilly UK Ltd. 384 S. ISBN: 978-1-4919-7194-9.

Literatur II

BTCR DID Method (8. Aug. 2019). URL: https://w3c-ccg.github.io/didm-btcr/ (besucht am 14. 07. 2020).

Decentralized Identifier Resolution (DID Resolution) v0.2 (2019). URL: https://w3c-ccg.github.io/did-resolution/ (besucht am 03. 12. 2019).

Decentralized Identifiers (DIDs) v1.0 (2019). URL: https://w3c.github.io/did-core/ (besucht am 12. 11. 2019).

DID Method Registry (2019). URL: https://w3c-ccg.github.io/did-method-registry/ (besucht am 13. 11. 2019).

Literatur III

ERC-1056 (3. Mai 2018). *ERC: Lightweight Identity · Issue #1056 · Ethereum/EIPs*. URL: https://github.com/ethereum/EIPs/issues/1056 (besucht am 04. 06. 2020).

Kai Wagner u. a. (23. Okt. 2018). *Self-Sovereign Identity*. URL: https://www.bundesblock.de/wp-content/uploads/2019/01/ssi-paper.pdf (besucht am 15. 10. 2019).

Peer DID Method Specification (2020). URL: https://identity.foundation/peer-did-method-spec/ (besucht am 29. 09. 2020).

Smith, Samuel (3. Juli 2019). *Key Event Receipt Infrastructure (KERI)*.

Literatur IV

Tietz, Christian u. a. (2017). *Management digitaler Identitäten: aktueller Status und zukünftige Trends*. Technische Berichte des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam 114. Potsdam: Universitätsverlag Potsdam. 66 S. ISBN: 978-3-86956-395-4.

Verifiable Credentials Data Model 1.0 (2019). URL: https://www.w3.org/TR/vc-data-model/ (besucht am 04. 12. 2019).