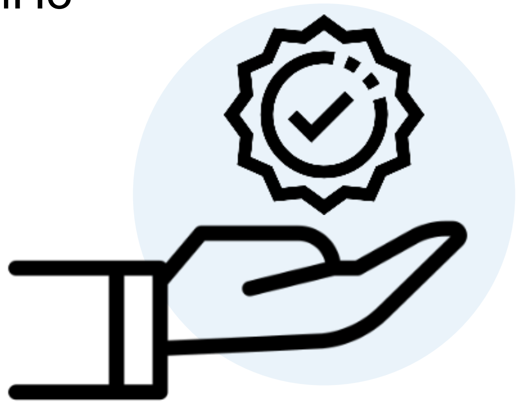
Requirements Engineering, User Workflows, and Prototypes

Digital Credentials for Higher Education Institutions – DiBiHo



2nd International Stakeholder Dialogue, May 4th 2022

Dr. Matthias Gottlieb, Alexander Mühle

SPONSORED BY THE

Federal Ministry
of Education
and Research

Ref. No. M534800

Icons: Pixelmeetup, Good Ware

Motivation

Digital Credentials should improve our current credential systems.
Therefore, they have to maintain and expand the properties of paper-based credentials

Paper-based Credentials

- ☑ Verifiable
- ☑ Fully controlled by holder

Digital Credentials

- ☑ Verifiable
- ☑ Fully controlled by holder
- ☑ Automatically processable

DiBiHo Project Summary

Consortium

HPI Hasso Plattner Institut
Digital Engineering • Universität Potsdam

DAAD

Project Goal

Exploration of a **trusted, distributed,** and **internationally interoperable infrastructure standard** for issuing, storing, presenting, and verifying **digital academic credentials** in a **national and international context** for **German Higher Education Institutions**.

Project Period

11/2020 – 12/2022

Funding

Federal Ministry
of Education
and Research

Ref. No.: M534800

Contact

Matthias Gottlieb (Project Manager, TUM)

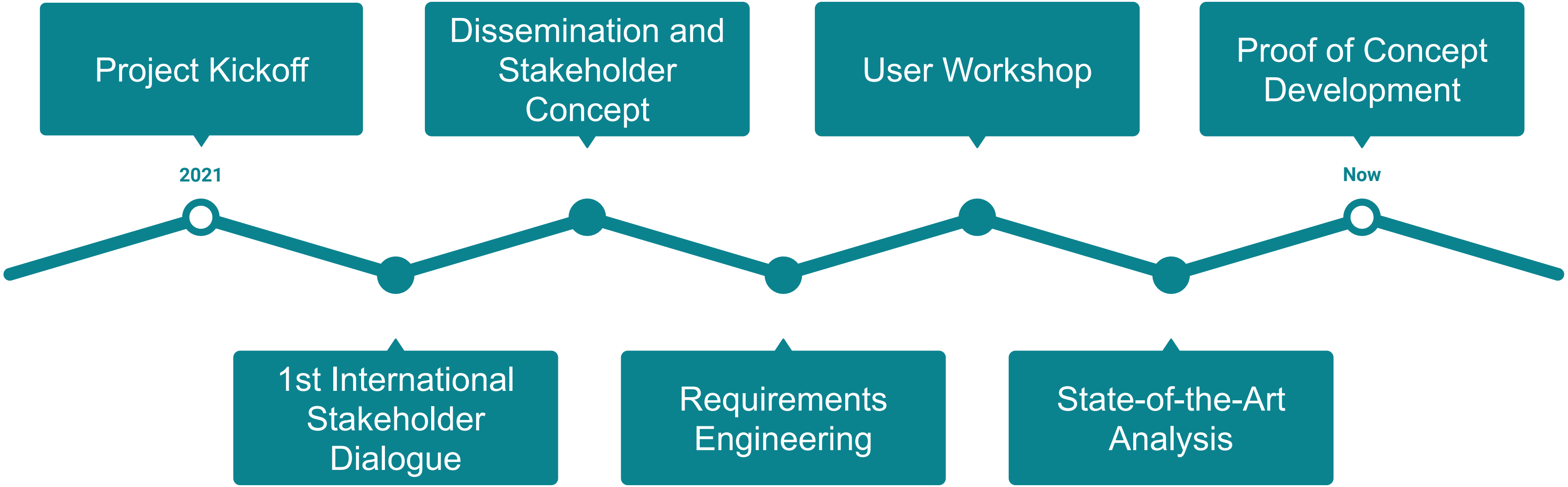
Alexander Mühle (Lead HPI Team)

Kathleen Clancy (Lead DAAD Team)

Website

www.dibiho.de

Project Timeline



2021

Project Kickoff

1st International Stakeholder Dialogue

Dissemination and Stakeholder Concept

Requirements Engineering

User Workshop

State-of-the-Art Analysis

Proof of Concept Development

Now

Requirements

Spanning 3 Use Cases

- MOOC
- Diploma
- Scholarship

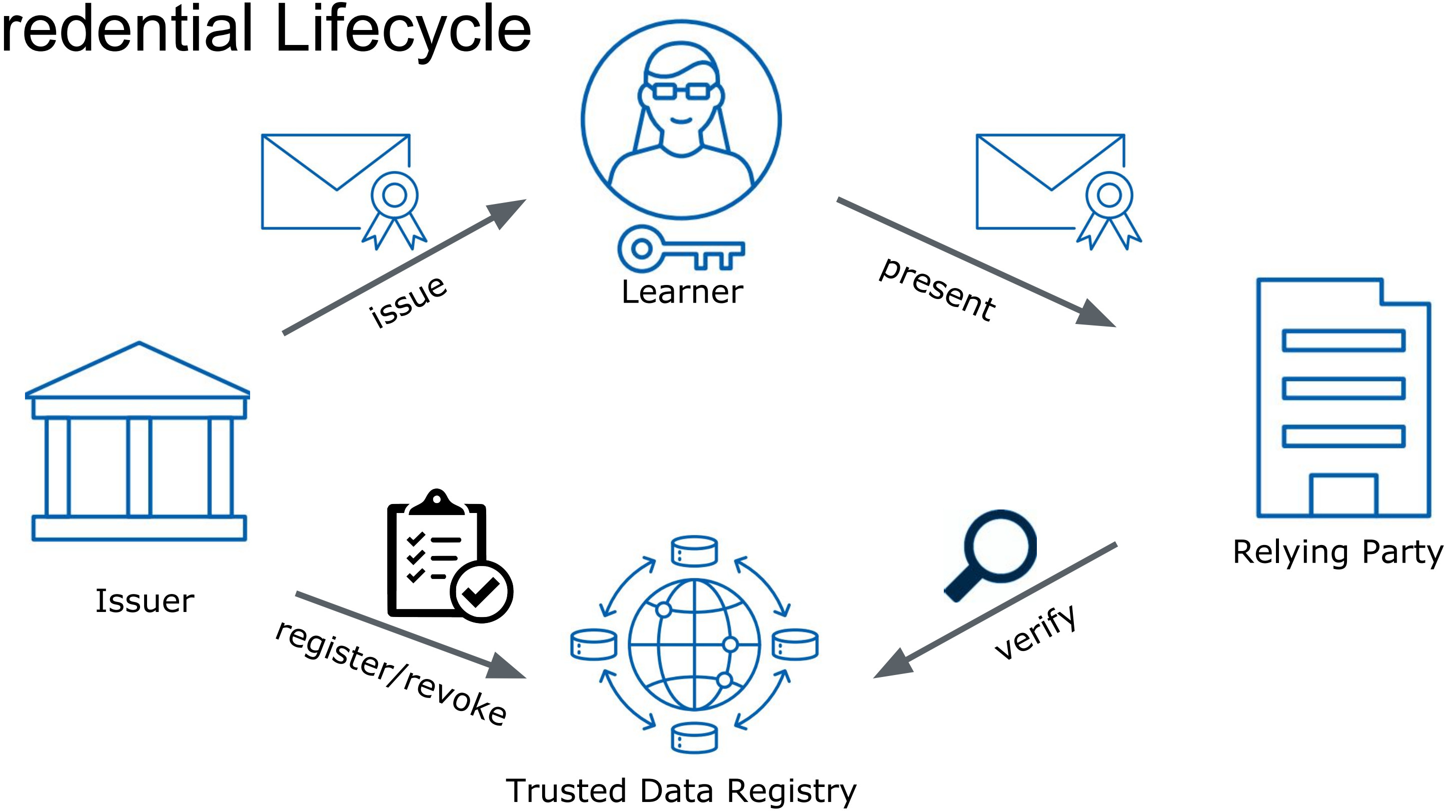
46
Functional Requirements

10
Non-Functional Requirements

Based on user stories informed by expert interviews. Enriched with comments and origin tracing.

Dive into the full report here

Credential Lifecycle



What do we issue?

> *„Digital Identity as a **set of claims** made by one digital subject about itself or another digital subject"*
>
> \- Kim Cameron

- Different claims can be issued by different institutions
- Primary goal for our institutions
  - Diploma, records of achievements and scholarships
- Secondary goal to enable the primary goal
  - Identity attributes of the learner

What do we issue?

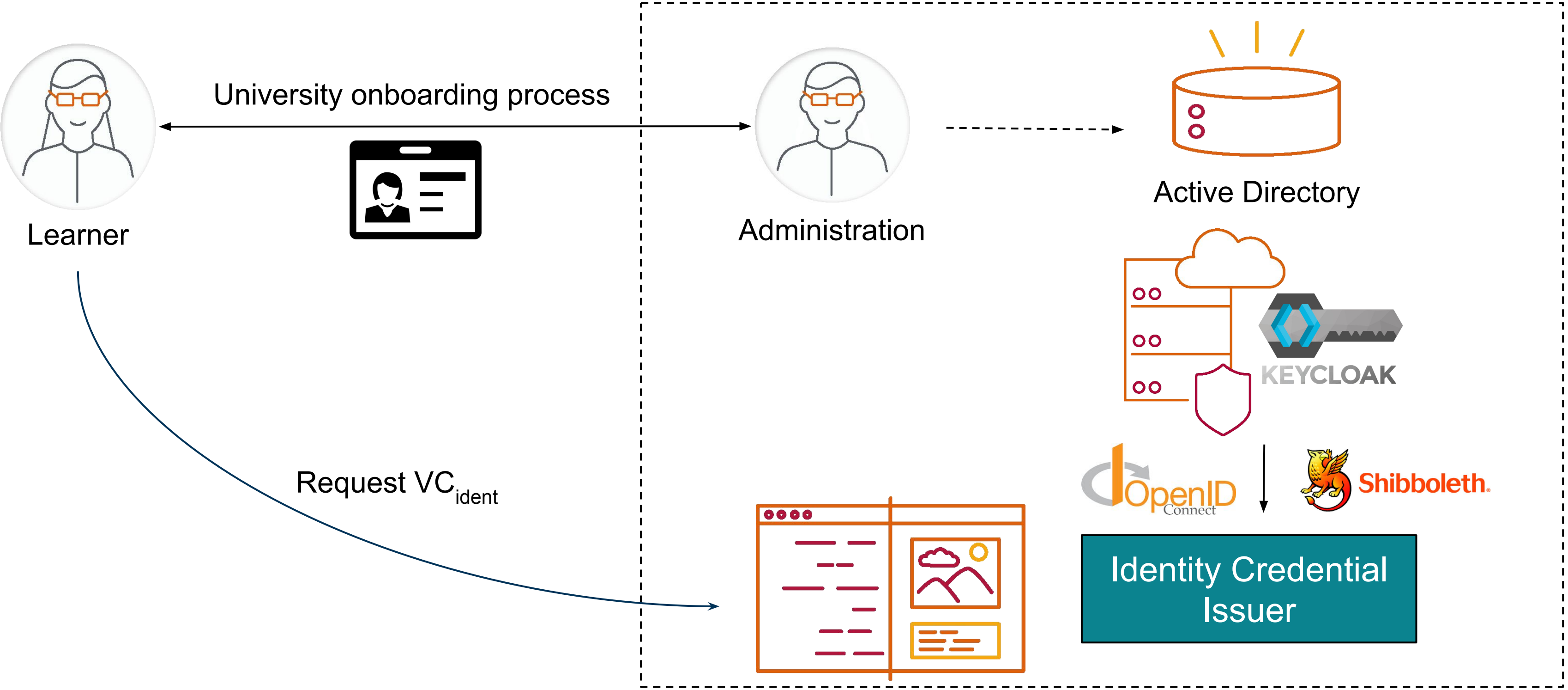
VC

- Verifiable Credential (VC) as standardised by W3C
- Different contexts definable
- I.e. credential attesting to learning achievements

VC_{ident}

- VC identifying the learner
- Needs to be linked to other VCs **if** real life identity is required by relying party

Where do we get (trusted) data from?



Where do we get (trusted) data from?

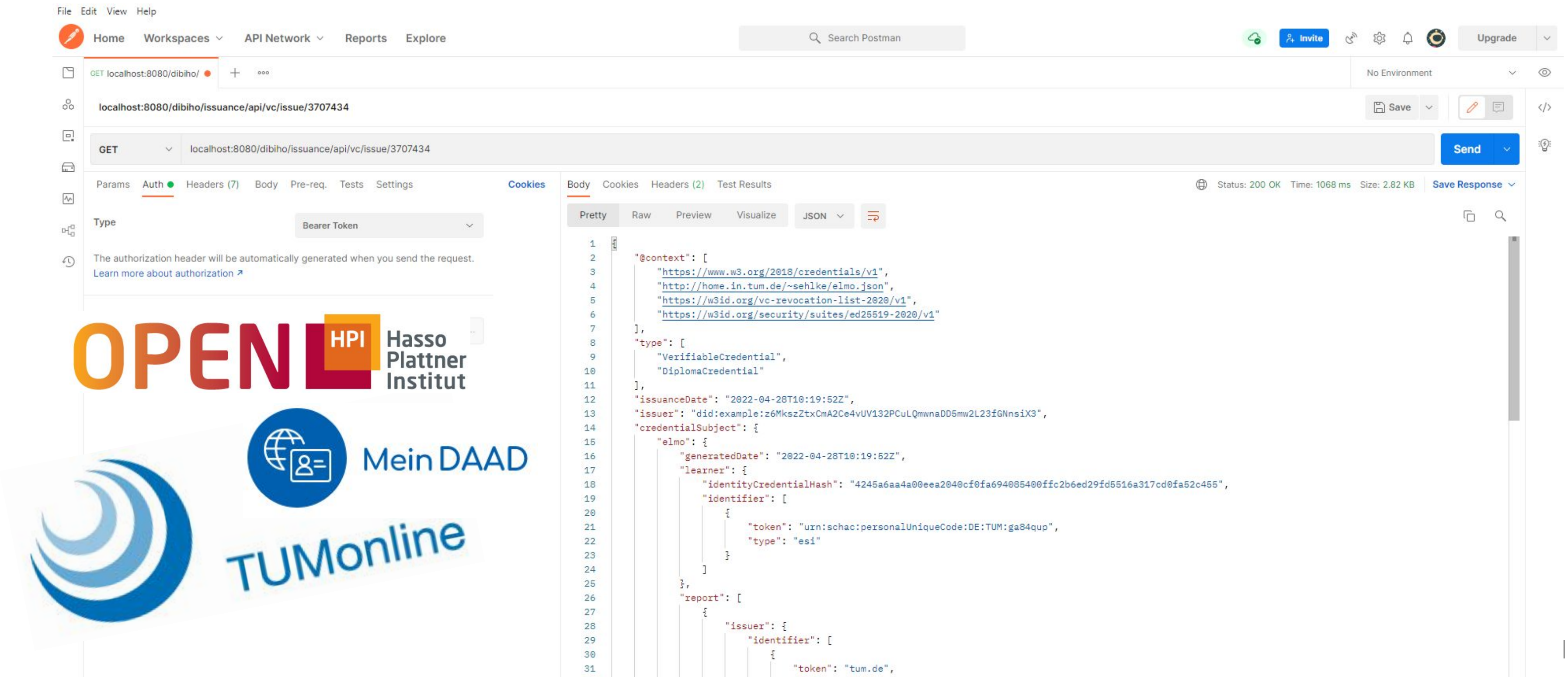
DiBiHo-3

As a learner, I want to manage (request, present, delete, recover, store) my credentials in a usable and secure way, so that I have full control over my data, can access it at all times, can use the system and have trust in the system.

DiBiHo-56

As an identity issuer, I want to create a digital credential for a user from their existing identity data, so that I can support self-sovereign identity systems.

Where do we get (trusted) data from?



localhost:8080/dibiho/issuance/api/vc/issue/3707434

GET localhost:8080/dibiho/issuance/api/vc/issue/3707434

Type: Bearer Token

The authorization header will be automatically generated when you send the request.
Learn more about authorization ↗

Status: 200 OK Time: 1068 ms Size: 2.82 KB

```
{
    "@context": [
        "https://www.w3.org/2018/credentials/v1",
        "http://home.in.tum.de/~sehlke/elmo.json",
        "https://w3id.org/vc-revocation-list-2020/v1",
        "https://w3id.org/security/suites/ed25519-2020/v1"
    ],
    "type": [
        "VerifiableCredential",
        "DiplomaCredential"
    ],
    "issuanceDate": "2022-04-28T10:19:52Z",
    "issuer": "did:example:z6MkszZtxCmA2Ce4vUV132PCuLQmwnaDD5mw2L23fGNnsiX3",
    "credentialSubject": {
        "elmo": {
            "generatedDate": "2022-04-28T10:19:52Z",
            "learner": {
                "identityCredentialHash": "4245a6aa4a00eea2040cf0fa694085400ffc2b6ed29fd5516a317cd0fa52c455",
                "identifier": [
                    {
                        "token": "urn:schac:personalUniqueCode:DE:TUM:ga84qup",
                        "type": "esi"
                    }
                ]
            },
            "report": [
                {
                    "issuer": {
                        "identifier": [
                            {
                                "token": "tum.de",
```

How is the issuance process triggered?

In favor of interoperability, we limit assumptions about the system that our Issuer Service is integrated into. Thus, every institution has full control over how exactly issuance is triggered.

Push Principle

The **(student information) system triggers issuance**. The learner is notified to collect his new credential.

Example: DiBiHo Diploma at TUM

vs.

Pull Principle

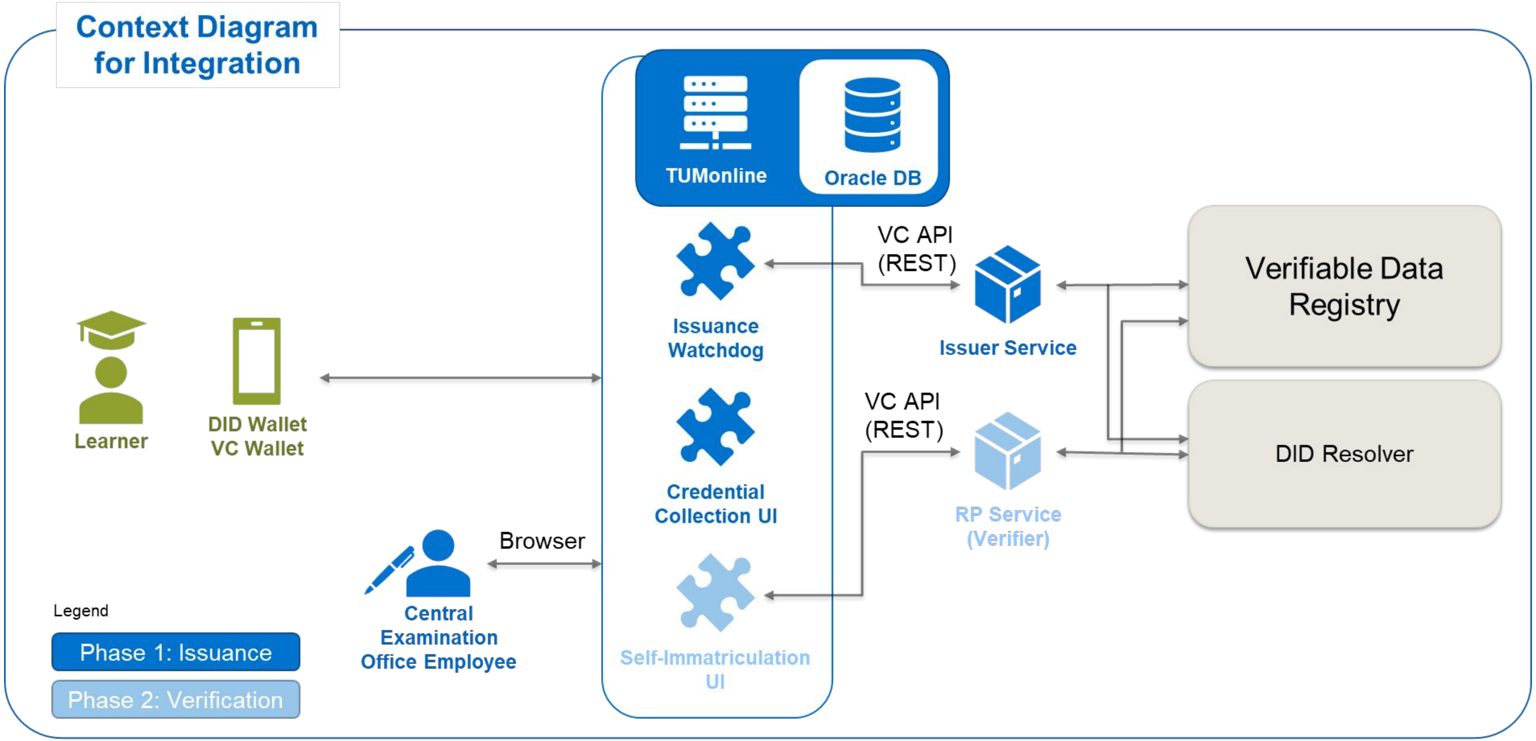
The **student triggers issuance**. Enables the option to document learner consent.

Example: DiBiHo MOOC at HPI

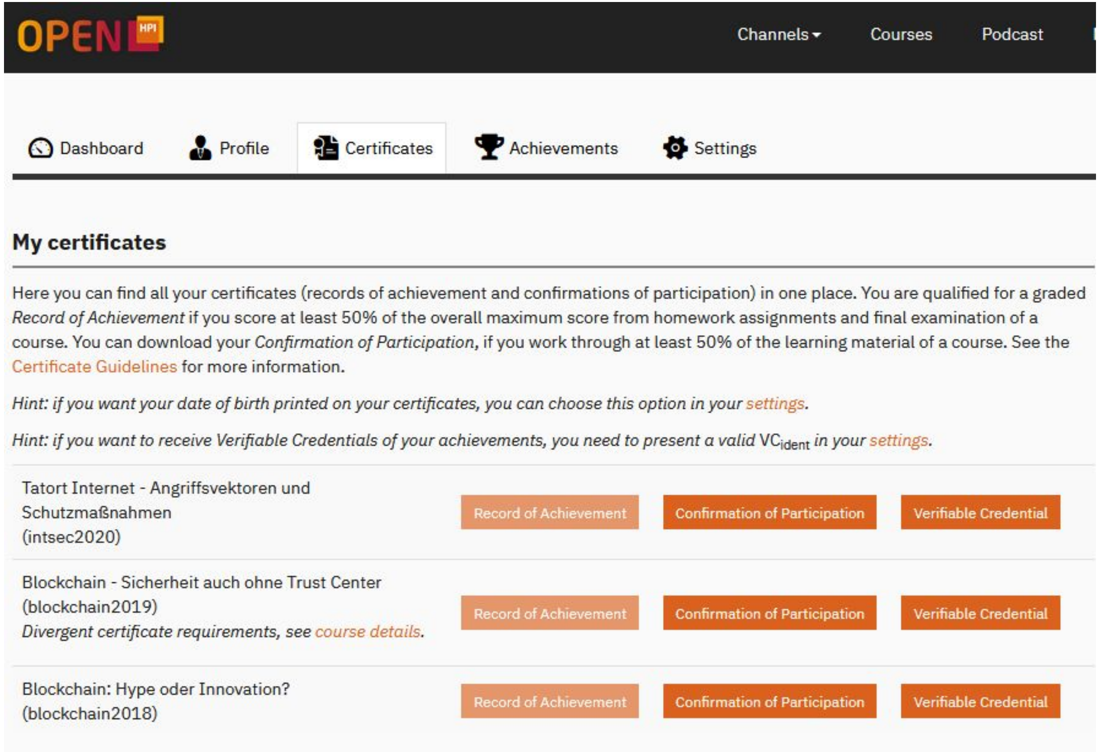
Some factors to consider when choosing:

- type(s) of education credentials to be issued
- type and make of system used as data source
- existing identity management

How is the issuance process triggered? (cont.)



How is the issuance process triggered? (cont.)



My certificates

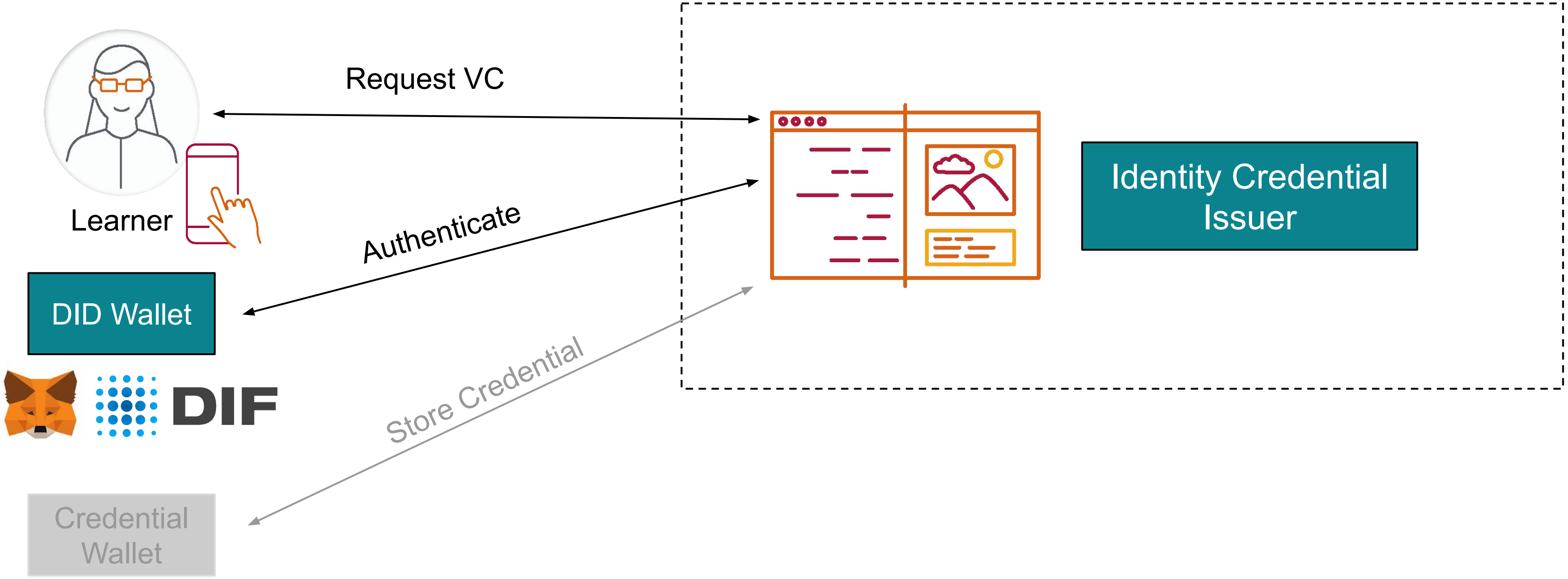
Here you can find all your certificates (records of achievement and confirmations of participation) in one place. You are qualified for a graded *Record of Achievement* if you score at least 50% of the overall maximum score from homework assignments and final examination of a course. You can download your *Confirmation of Participation*, if you work through at least 50% of the learning material of a course. See the Certificate Guidelines for more information.

Hint: if you want your date of birth printed on your certificates, you can choose this option in your settings.

Hint: if you want to receive Verifiable Credentials of your achievements, you need to present a valid VC_{ident} in your settings.

Tatort Internet - Angriffsvektoren und Schutzmaßnahmen (intsec2020)	Record of Achievement	Confirmation of Participation	Verifiable Credential
Blockchain - Sicherheit auch ohne Trust Center (blockchain2019) *Divergent certificate requirements, see course details.*	Record of Achievement	Confirmation of Participation	Verifiable Credential
Blockchain: Hype oder Innovation? (blockchain2018)	Record of Achievement	Confirmation of Participation	Verifiable Credential

How does the learner interact?



Request VC

Learner

Authenticate

DID Wallet

Store Credential

Credential Wallet

Identity Credential Issuer

How does the learner interact?

DiBiHo-4

As a learner, I want to tie my identifier to my reallife identity, so that I can identify myself.

DiBiHo-101

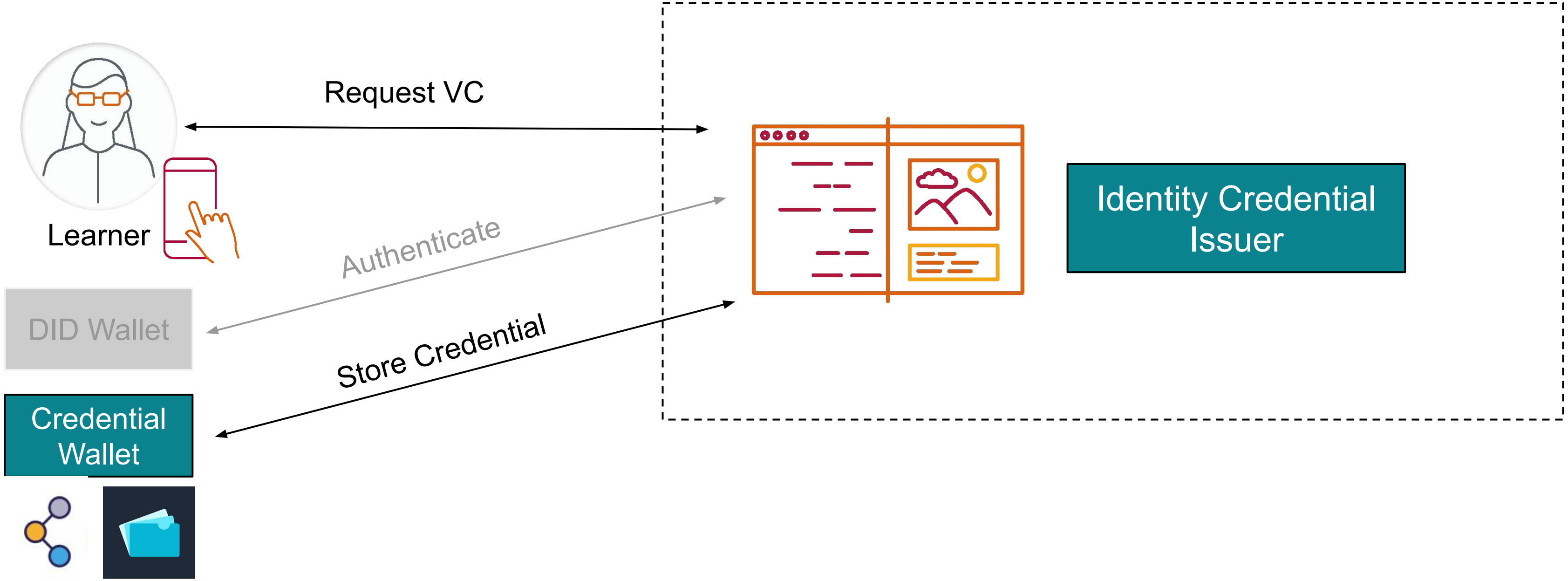
As an issuer who is a university, I want to authenticate a learner at the time of enrollment and establish a known identifier for that student, so that I can be sure that subsequently issued credentials are securely bound to that natural person and cannot be passed on.

User consent and non-repudiation

DiBiHo-2

As a learner I want to authorize an issuer to create new credentials for me and store them in a trusted data registry [...].

How does the learner interact?



Where do we store the Credential?

- Download and self-management
- Credential wallets that communicate via QR codes
    - Transmit credential encoded in QR code
        - CBOR-LD encoding
        - i.e. Learner Credential Wallet
    - Transmit information on how to retrieve credential
        - i.e. enmeshed

Where do we store the Credential?

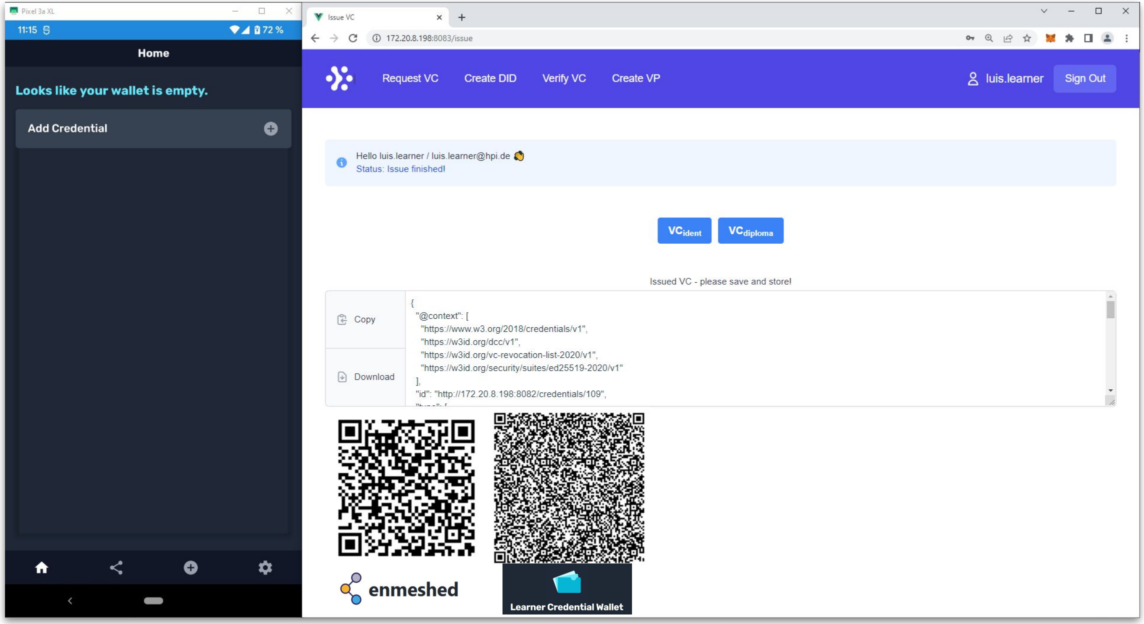
DiBiHo-8

As a learner, I want to choose my storage location, so that I can switch to the storage best suiting my needs of accessibility, privacy, security.

DiBiHo-50

As a learner, I want to have all information related to me available in my wallet, so that I have full control.

Where do we store the Credential?



Looks like your wallet is empty.

Add Credential

Hello luis.learner / luis.learner@hpi.de 👏
Status: Issue finished!

Issued VC - please save and store!

```
{
 "@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://w3id.org/dcc/v1",
  "https://w3id.org/vc-revocation-list-2020/v1",
  "https://w3id.org/security/suites/ed25519-2020/v1"
 ],
 "id": "http://172.20.8.198:8082/credentials/109",
```

DiBiHo-8

As a learner, I want to choose my storage location, so that I can switch to the storage best suiting my needs of accessibility, privacy, security.

DiBiHo-50

As a learner, I want to have all information related to me available in my wallet, so that I have full control.

HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

DAAD

TUM

How are the credentials verified?

The verifier has access to several data sources:

Verifiable Credential

- credential that is verified
- could be VC or Verifiable Presentation (VP)

DID Registry/Registries

- depending on supported DID methods
- provide cryptographic keys and metadata
- e.g., Ethereum, IPFS, Web Server

Verifiable Data Registry

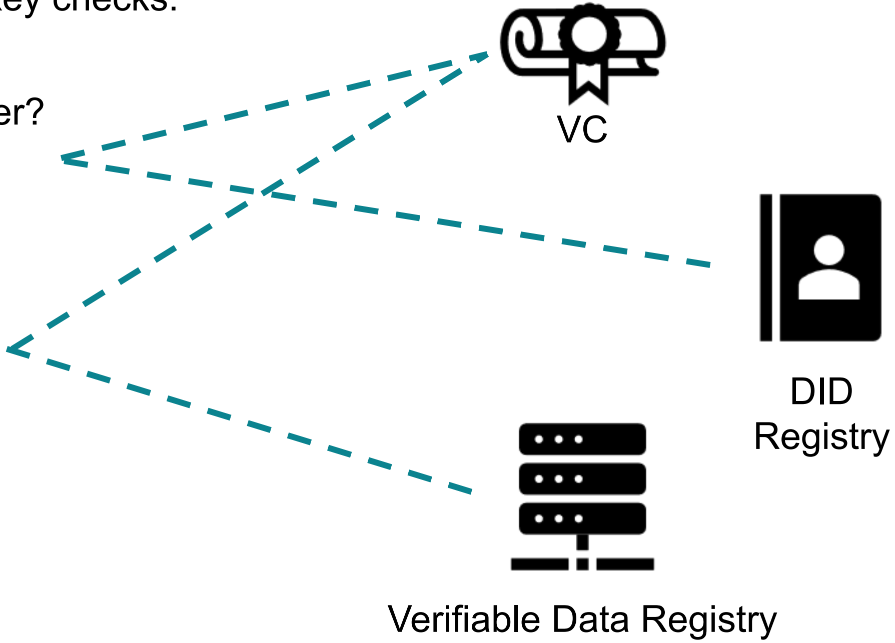
- required to provide revocation information
- can additionally provide issuance logs
- underlying infrastructure is still being discussed

How are the credentials verified? (cont.)

The verifier uses the data available for selected key checks:

Is the credential created by the claimed issuer?
Is the credential unchanged since issuance?
(Is the credential requested by the subject?)

Is the credential still not revoked?



How are the credentials verified? (cont.)

There are two more complicated checks, which we consider essential:

Is the issuer a trusted issuer?

- it is not and never will be feasible to know every HEI
- is there one list of trusted issuers, or does everyone keep their own?
- who would be trusted to keep that list?
- rather an issue of governance, then technology

Design Outstanding

Is the issuance auditable?

- makes it harder for rogue employees (or institutions) to cause damage undetected
- comparable to Certificate Transparency for TLS

How are the credentials verified? (cont.)

DiBiHo-1

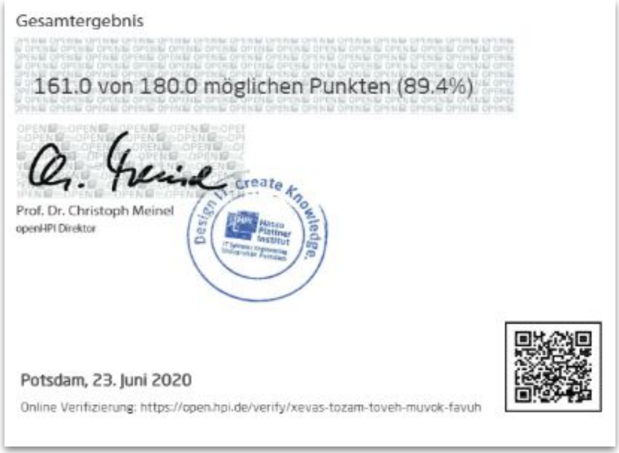
As a learner, I want to authorize relying parties to receive and verify my credentials so that I don't need to send them a certified copy of the original.

DiBiHo-13

As a relying party, I want to verify a credential, so that I can be sure that the contents of a presented credential are trustworthy.

How are the credentials presented?

- Option 1
  - A visual representation (PDF) of the achievement that is verified afterwards
  - How many will *actually* verify what they have already seen?
  - Visual representation easily changeable and insecure if not specifically checked



Gesamtergebnis

161.0 von 180.0 möglichen Punkten (89.4%)

Prof. Dr. Christoph Meinel
openHPI Direktor

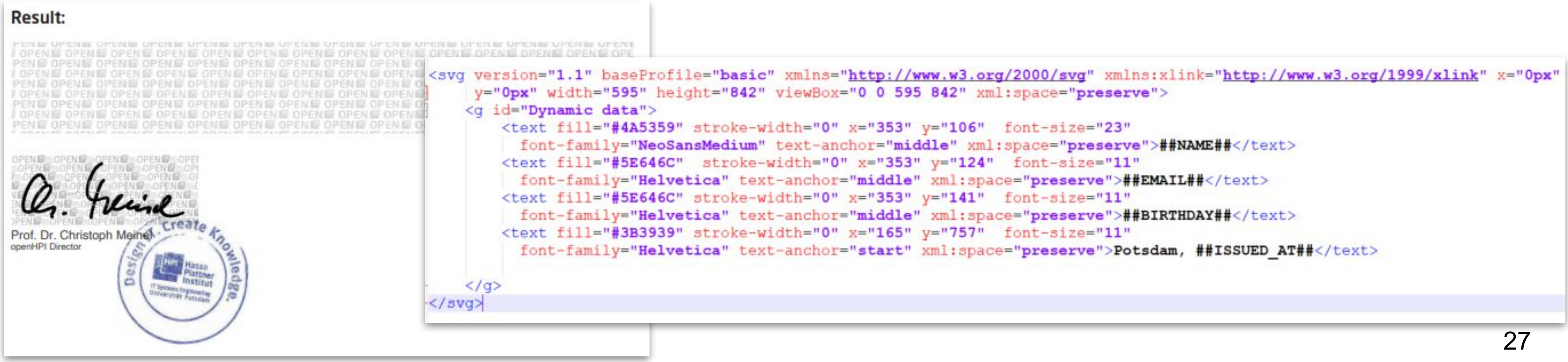
Design IT. Create Knowledge.
HPI Hasso Plattner Institut
IT Systems Engineering
Universität Potsdam

Potsdam, 23. Juni 2020

Online Verifizierung: https://open.hpi.de/verify/xevas-tozam-toveh-muvok-favuh

How are the credentials presented?

- Option 2
  - A machine readable and verifiable representation (VC) of the achievement
  - Visualisation rendered on demand using data included in the VC
  - Only one source of information for both machine readable and visual representation
  - PDF template and layout file used in combination with VC to create representation



Result:

Prof. Dr. Christoph Meinel
openHPI Director

```
<svg version="1.1" baseProfile="basic" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px"
   y="0px" width="595" height="842" viewBox="0 0 595 842" xml:space="preserve">
  <g id="Dynamic data">
      <text fill="#4A5359" stroke-width="0" x="353" y="106"  font-size="23"
        font-family="NeoSansMedium" text-anchor="middle" xml:space="preserve">##NAME##</text>
      <text fill="#5E646C"  stroke-width="0" x="353" y="124"  font-size="11"
        font-family="Helvetica" text-anchor="middle" xml:space="preserve">##EMAIL##</text>
      <text fill="#5E646C" stroke-width="0" x="353" y="141"  font-size="11"
        font-family="Helvetica" text-anchor="middle" xml:space="preserve">##BIRTHDAY##</text>
      <text fill="#3B3939" stroke-width="0" x="165" y="757"  font-size="11"
        font-family="Helvetica" text-anchor="start" xml:space="preserve">Potsdam, ##ISSUED_AT##</text>

  </g>
</svg>
```

Thank you for your attention

Join our mailing list.

Get the full report.