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
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

TUM  HPI Hasso Plattner Institut  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

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

- Project Kickoff
- Dissemination and Stakeholder Concept
- User Workshop
- Proof of Concept Development

- 1st International Stakeholder Dialogue
- Requirements Engineering
- State-of-the-Art Analysis
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

Issuer

Learner

Relying Party

Trusted Data Registry

issue

present

register/revoke

verify
What do we issue?

● 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

„Digital Identity as a set of claims made by one digital subject about itself or another digital subject“
- Kim Cameron
What do we issue?

<table>
<thead>
<tr>
<th>VC</th>
<th>W3C®</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Verifiable Credential (VC) as standardised by W3C</td>
</tr>
<tr>
<td></td>
<td>• Different contexts definable</td>
</tr>
<tr>
<td></td>
<td>• I.e. credential attesting to learning achievements</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VC_{ident}</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• VC identifying the learner</td>
</tr>
<tr>
<td></td>
<td>• Needs to be linked to other VCs if real life identity is required by relying party</td>
</tr>
</tbody>
</table>
Where do we get (trusted) data from?

- **Learner**
  - University onboarding process

- **Administration**
  - Active Directory

- **Identity Credential Issuer**
  - Keycloak
  - Shibboleth
  - OpenID Connect
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?
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*

### 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.)
How does the learner interact?

Learner

Request VC

Authenticate

Identity Credential Issuer

DID Wallet

Credential Wallet

Store Credential
How does the learner interact?

**DiBiHo-4**
As a learner, I want to tie my identifier to my real-life 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

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?

- Request VC
- Authenticate
- Store Credential

Learner

DID Wallet

Credential Wallet

Identity Credential Issuer
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?

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.
How are the credentials verified?

The verifier has access to several data sources:

<table>
<thead>
<tr>
<th>Source</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifiable Credential</td>
<td>• credential that is verified</td>
</tr>
<tr>
<td></td>
<td>• could be VC or Verifiable Presentation (VP)</td>
</tr>
<tr>
<td>DID Registry/Registries</td>
<td>• depending on supported DID methods</td>
</tr>
<tr>
<td></td>
<td>• provide cryptographic keys and metadata</td>
</tr>
<tr>
<td></td>
<td>• e.g., Ethereum, IPFS, Web Server</td>
</tr>
<tr>
<td>Verifiable Data Registry</td>
<td>• required to provide revocation information</td>
</tr>
<tr>
<td></td>
<td>• can additionally provide issuance logs</td>
</tr>
<tr>
<td></td>
<td>• underlying infrastructure is still being discussed</td>
</tr>
</tbody>
</table>
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?

VC

DID Registry

Verifiable Data Registry
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

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.)

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.

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
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
Thank you for your attention

Join our mailing list.

Get the full report.