Verification of Digital Credentials Supporting Self-Sovereign Identity for Higher Education Institutions

Pascal Herrmann, June 13th 2022 – Master's Thesis Kick-Off

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
wwwmatthes.in.tum.de

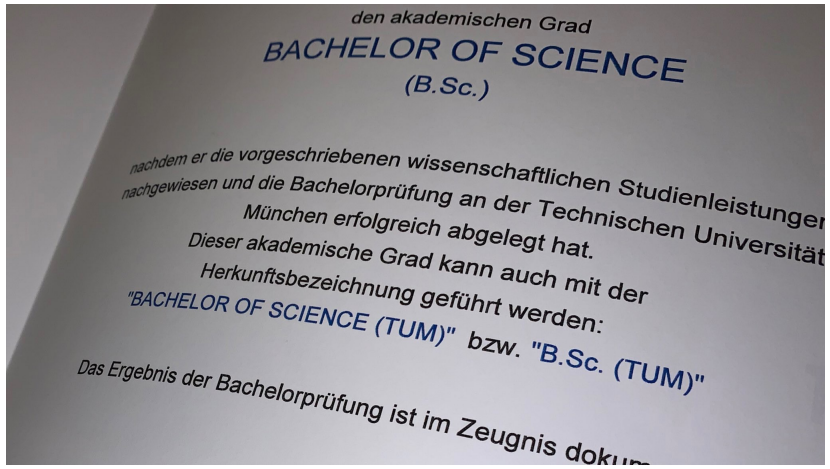
Outline

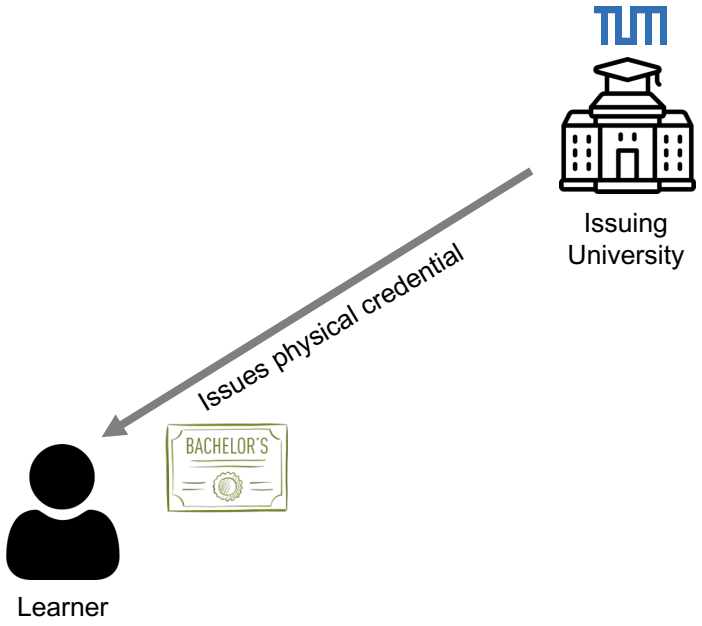
1. Motivation and Introduction
2. Problem Statement
3. Research Questions & Methodology
4. Timeline & Current Status

© sebis

Motivation

Typically, Higher Education Credentials are issued to students as **physical paper documents**.



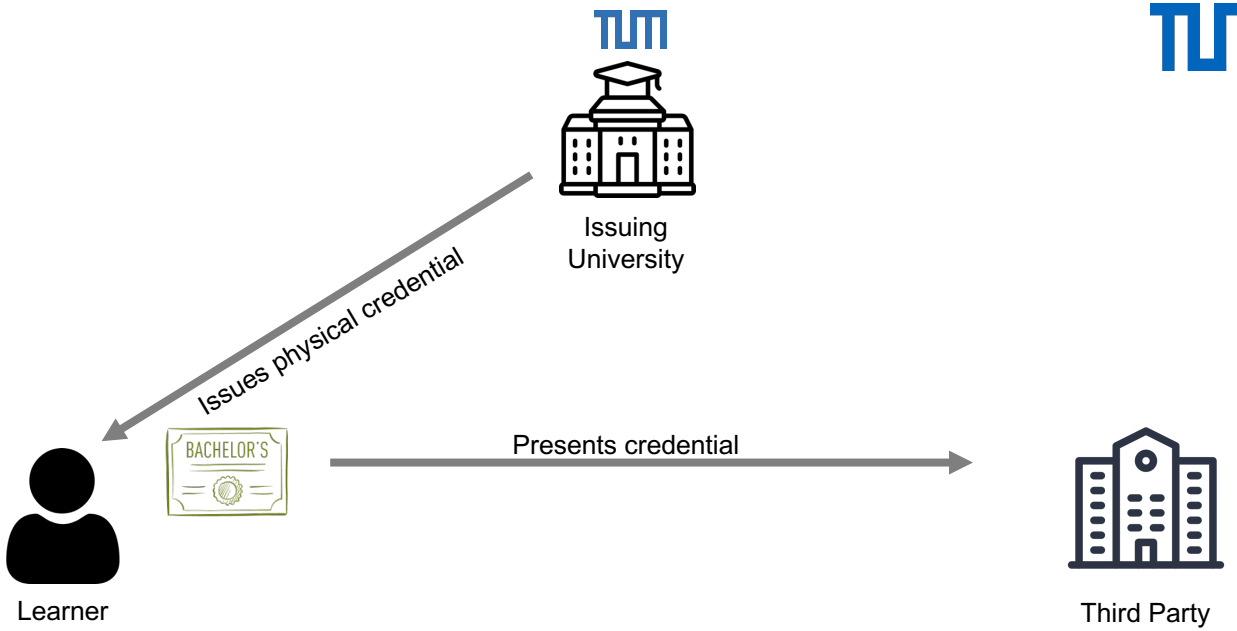


© sebis

Motivation

Typically, Higher Education Credentials are issued to students as **physical paper documents**.

These documents are required for several important purposes.



Employment

Further Education

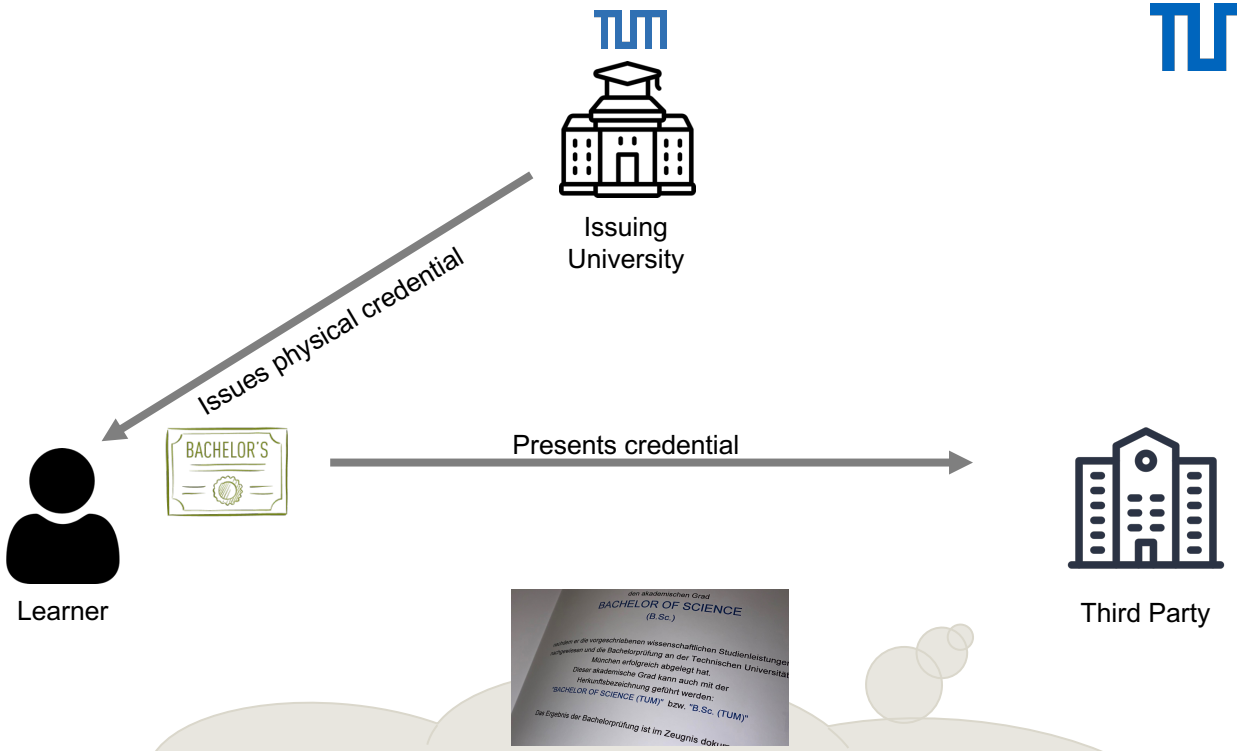
Immigration

© sebis

Motivation

Typically, Higher Education Credentials are issued to students as **physical paper documents**.

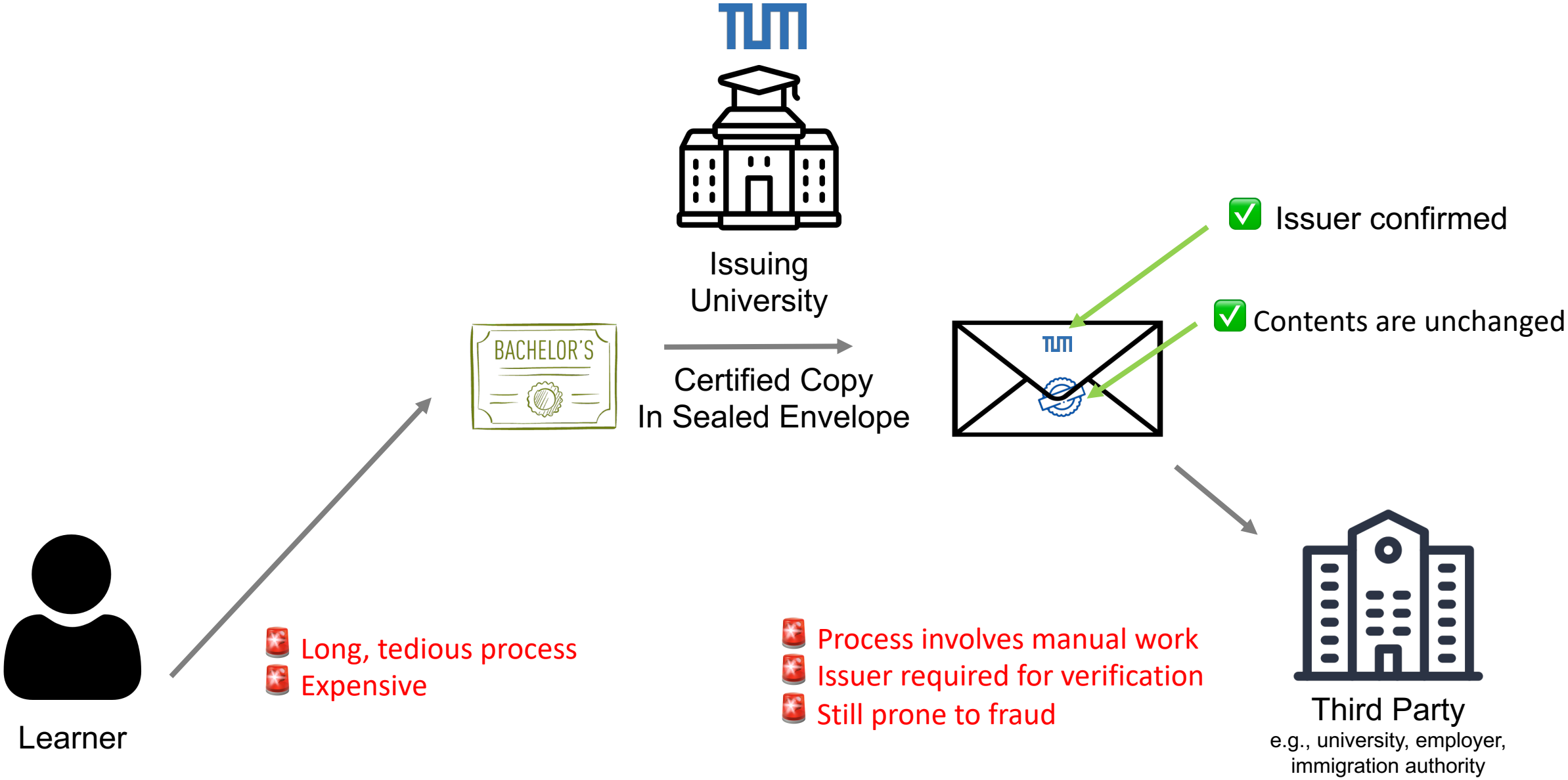
These documents are required for several important purposes.



The verification of these documents is challenging!

© sebis

Example: Verification of Physical Education Credentials



© sebis

Vision: Verifiable Digital Credentials

Students obtain a **digital, verifiable credential** at graduation.

MyDegrees

Bachelor's Degree


```
{
  "issuer": "did:ipid:z6MkqVmUBC49F98kv ···  12zms",
  "credential": {
    "learner": "did:ethr:0x759871343297 ···  ffa5b",
    "degreeType": "Bachelor of Science",
    "major": "Informatics",
    "grade": "1.3"
     ⋮
  },
  "signature": "z2hMLrKN5x6m1i9DRctPNSL ···  X19bHn"
}
```


Self-Sovereign Identity:
✅ prove identity of issuer & learner

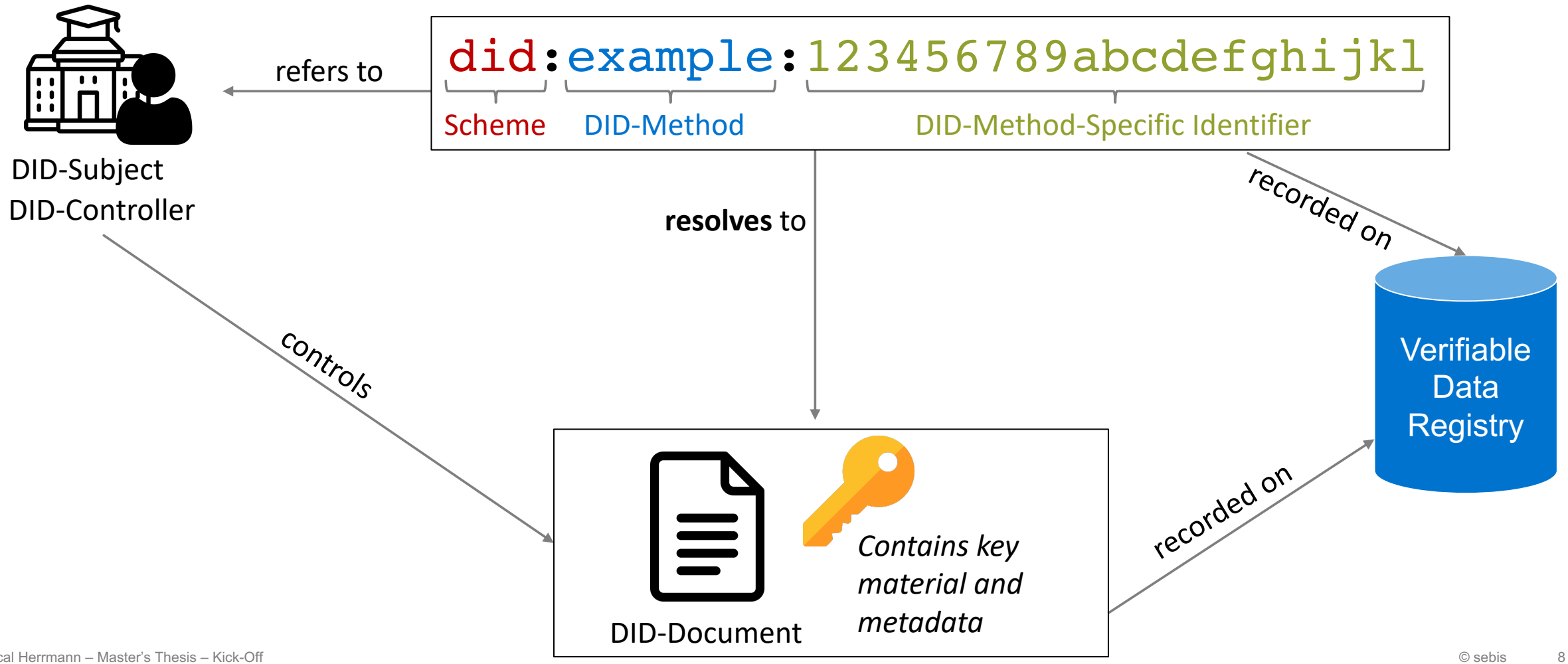
Cryptographic Signature:
✅ contents remain unchanged

The digital credential can be verified by relying parties
- ✅ Without involvement of the issuer
- ✅ In an efficient, automated way

© sebis

Self Sovereign Identities

Decentralized Identifiers (DIDs) resolve to DID-Documents that contain key material and metadata which can be used to authenticate DID subjects



© sebis

Outline

1. Motivation and Introduction
2. Problem Statement
3. Research Questions & Methodology
4. Timeline & Current Status

© sebis

DiBiHo

- A collaboration of

Deutscher Akademischer Austauschdienst
German Academic Exchange Service

- In close cooperation with the

Goal: Proof of Concept for verifiable, digital credentials for higher education institutions

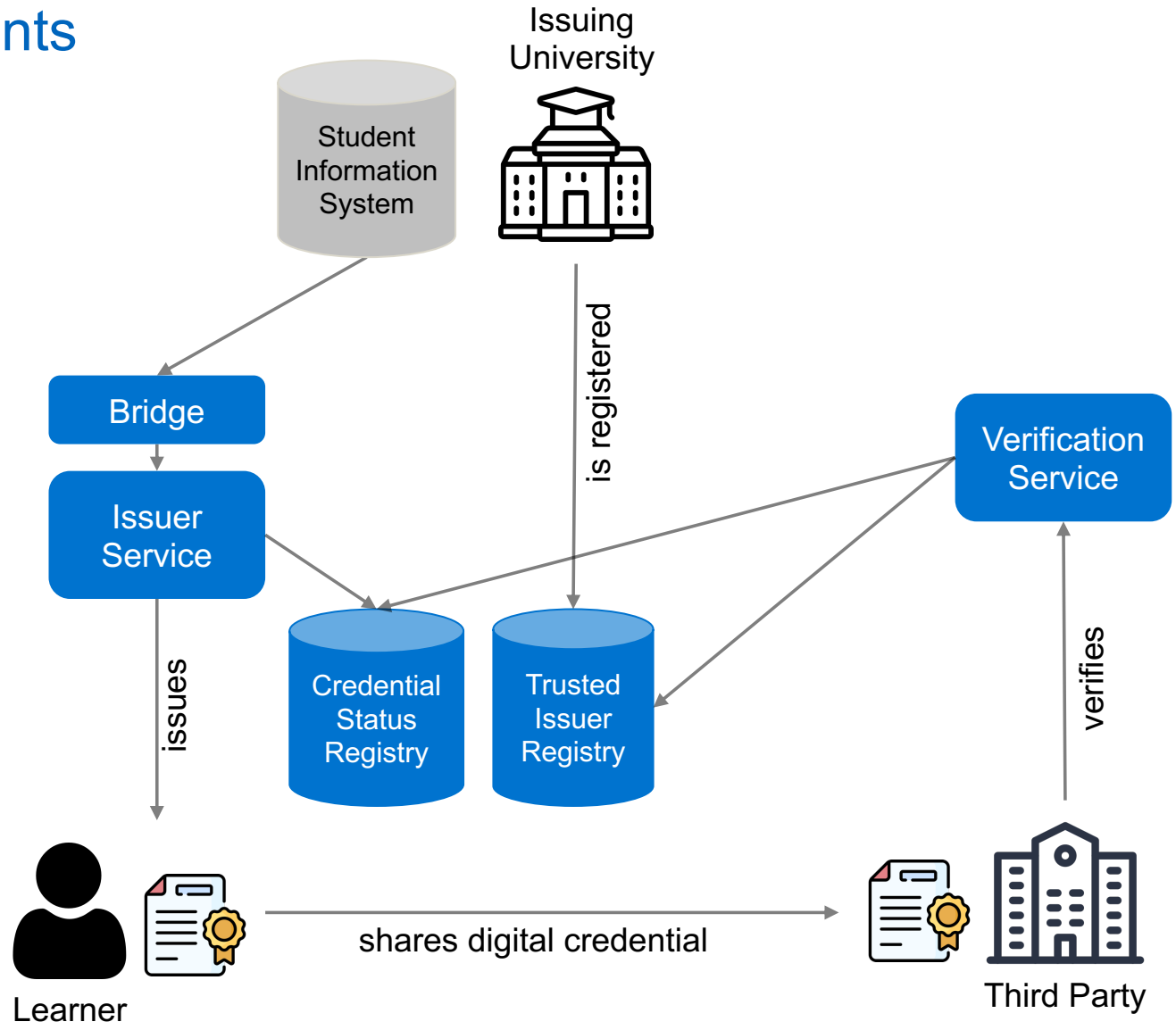
https://www.dibiho.de/

© sebis

DiBiHo Components

Open-Source Reference Implementations

Consortium-Maintained Registries

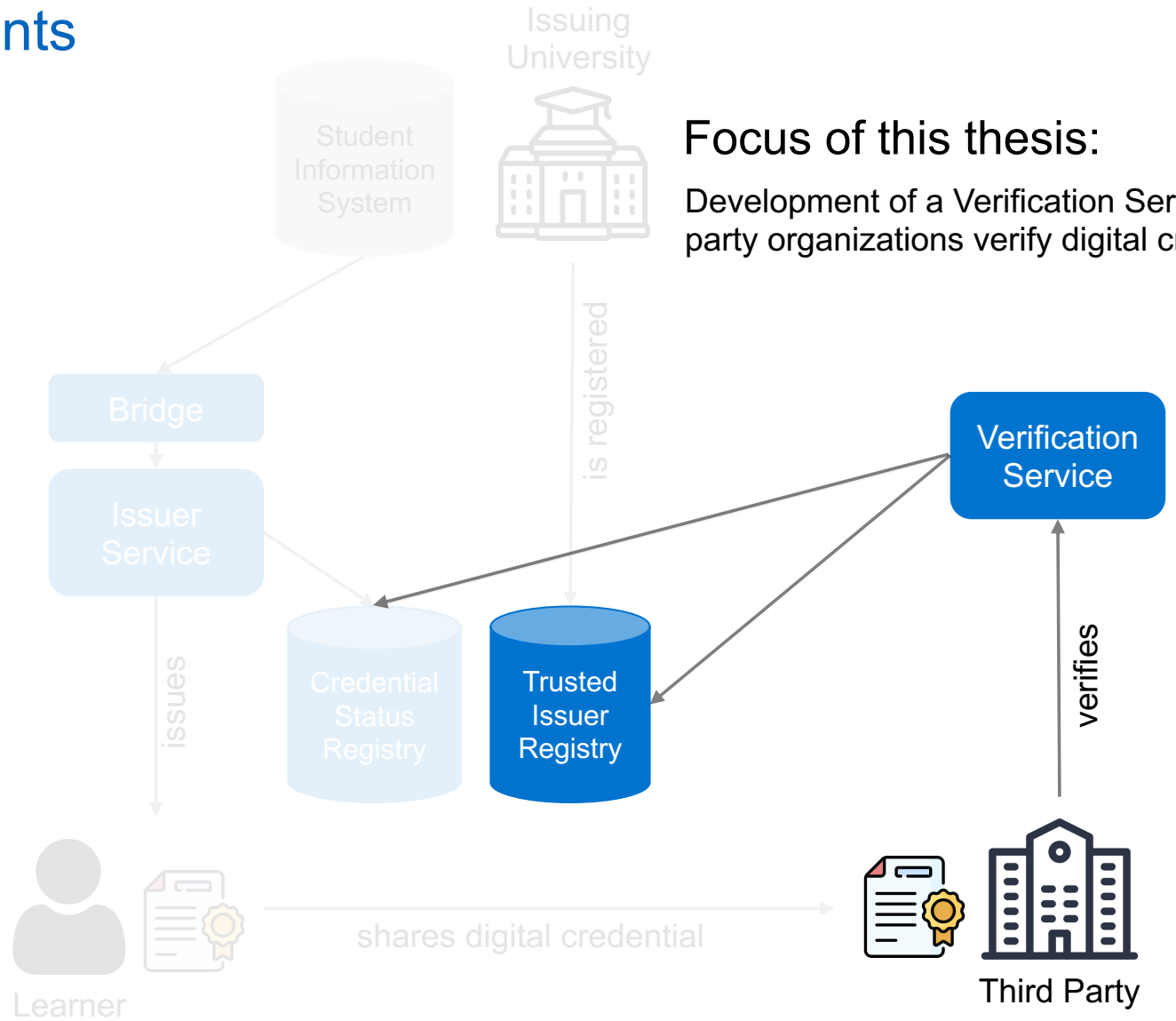


© sebis

DiBiHo Components

Open-Source Reference Implementations

Consortium-Maintained Registries



Focus of this thesis:

Development of a Verification Service component, which lets third-party organizations verify digital credentials.

© sebis

Outline

1. Motivation and Introduction
2. Problem Statement
3. Research Questions & Methodology
4. Timeline & Current Status

© sebis

Research Question 1

RQ1: What is an effective validity check for verifiable credentials?

- What checks must be performed and in what order?
- What data must be fetched?
- What error states are possible? How should they be communicated?

Artifact:

Functioning implementation that can verify digital credentials created in accordance to the needs of higher education institutions

Methodology:

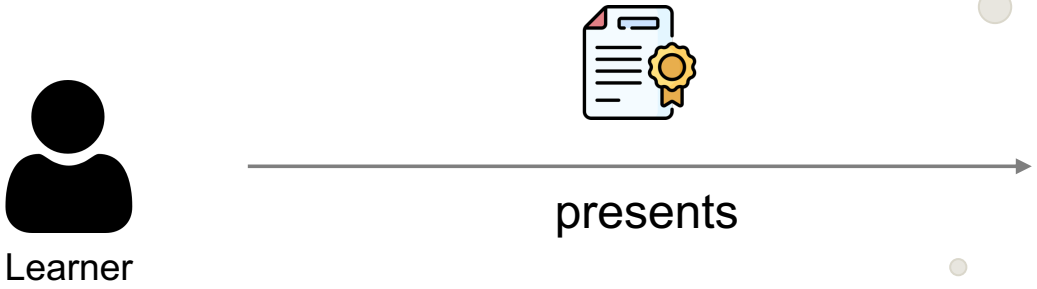
- Requirements Analysis
- Literature Research
- Scrum
- Test Driven Development

© sebis

Is the **issuer** a **trusted university?**

Has the credential been **revoked**?

Is the content **unchanged**?

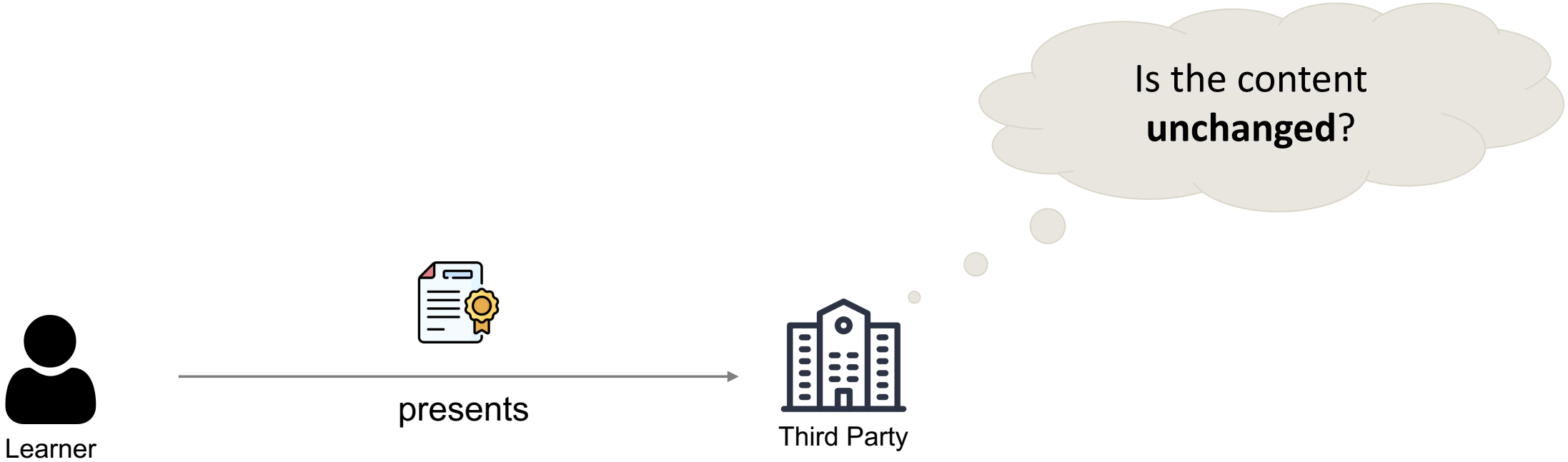


Is the credential **expired**?

… ?

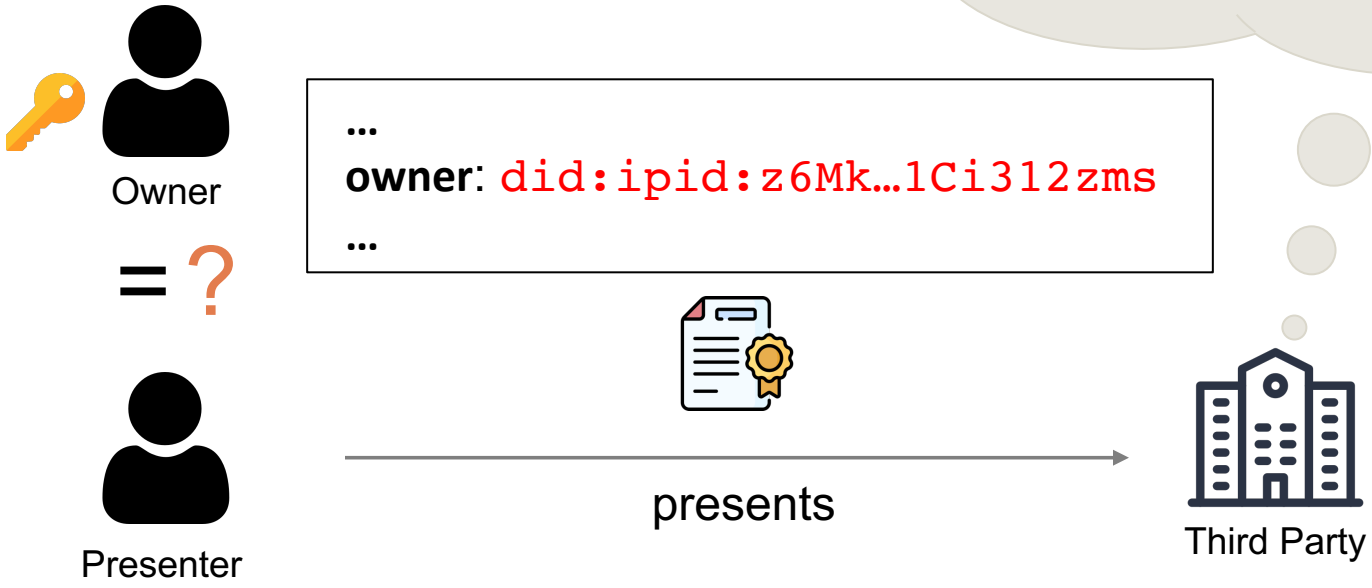
Is the person who **presents** the credential the **owner** of the credential?

© sebis



© sebis

Is the person who **presents** the credential the **owner** of the credential?



© sebis

Research Question 2

RQ2: What SSI libraries shall be used in the implementation of the Verification Service?

- Which criteria must SSI libraries fulfill to be well-suited for this use case?
- What SSI libraries exist and how do they fulfill these criteria?

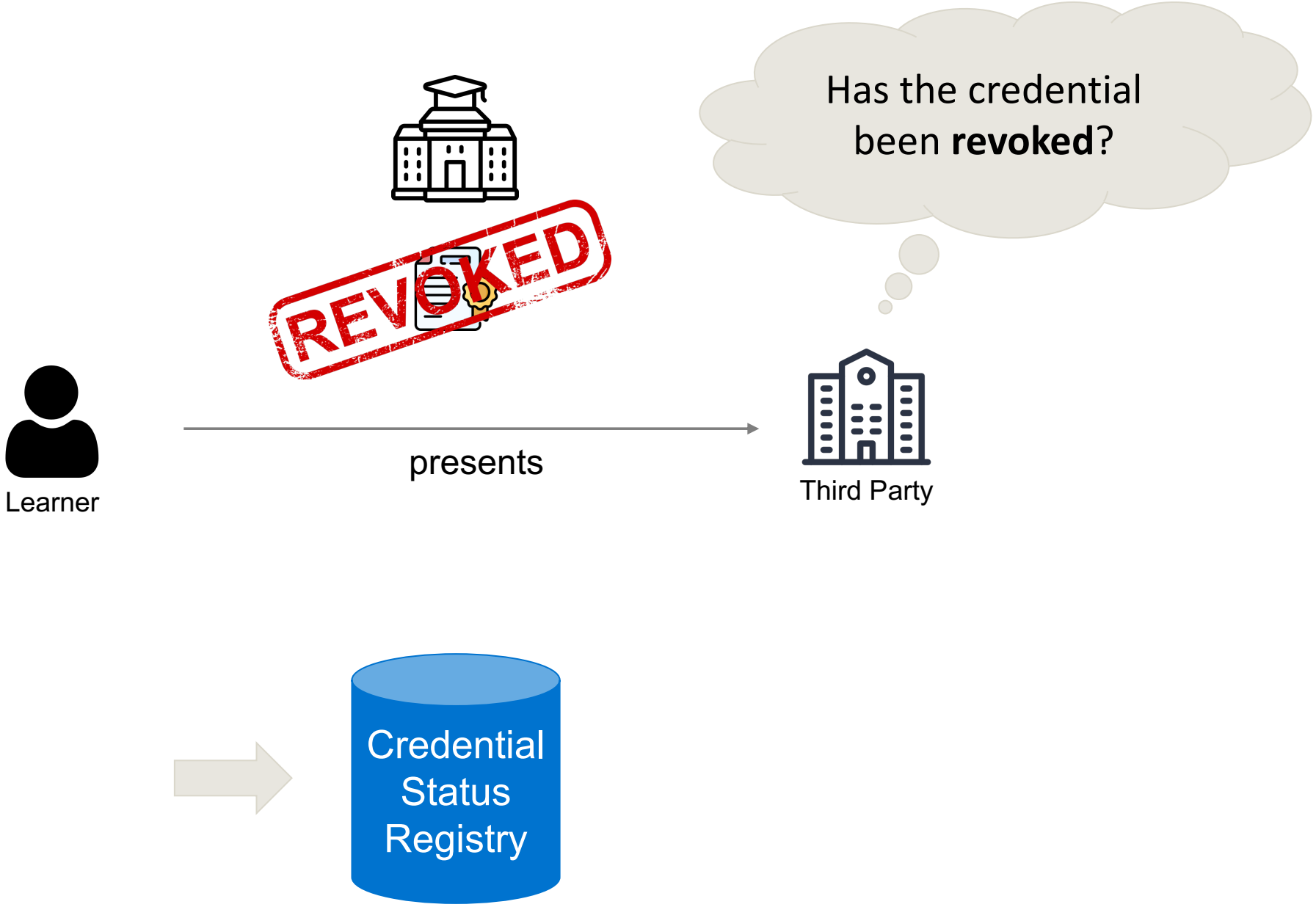
Artifact:

- Criteria Catalog
- Set of frameworks rated according to these criteria

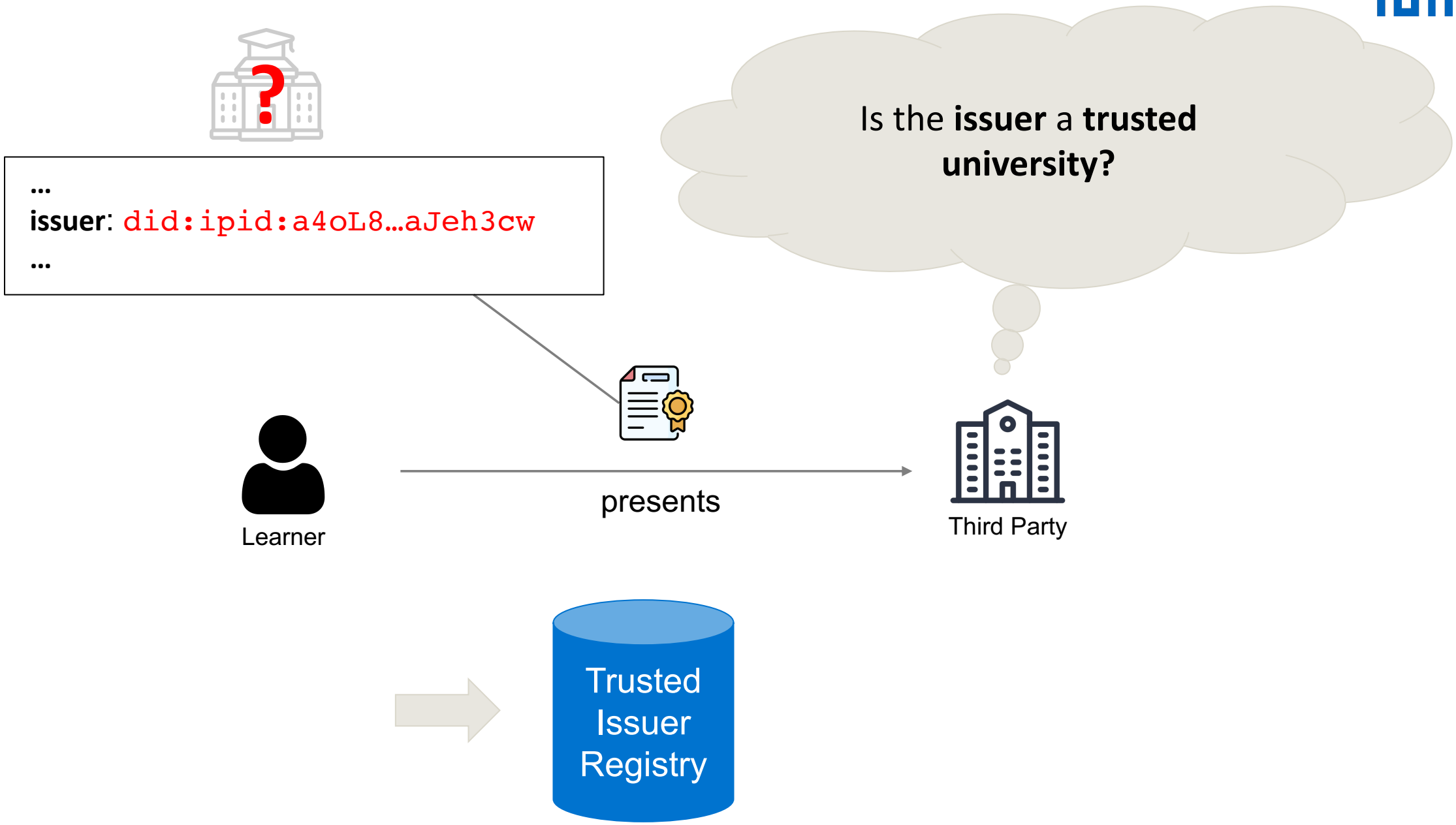
Methodology:

- Requirements Analysis
- Literature Research

© sebis


Has the credential been **revoked**?
REVOKED
Learner
presents
Third Party
Credential Status Registry

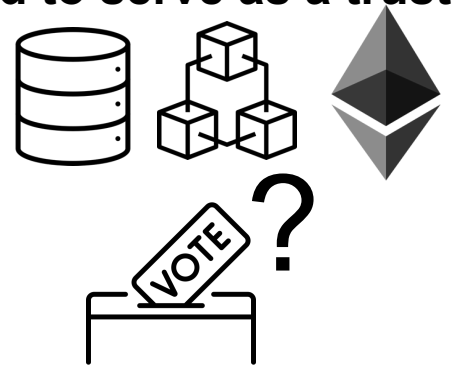
© sebis


...
issuer: did:ipid:a4oL8…aJeh3cw
...
Is the issuer a trusted university?
Learner
presents
Third Party
Trusted Issuer Registry

© sebis

Research Question 3

RQ3: How can a Trusted Issuer Registry be designed and implemented to serve as a trust-anchor for verifying issuers of digital credentials?



- Which type of infrastructure is suited?
- What information must be stored?
- How can new issuers be added while maintaining high level of trust?
- How can the Trusted Issuer Registry be implemented?

Artifact:

- Architecture and Implementation of Trusted Issuer Registry

Methodology:

- Literature Research
- Proof of Concept Development

© sebis

Overview: Verification Checks

Verifiable Credential

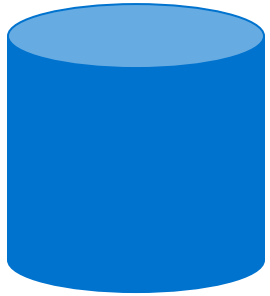
Credential to be verified
Shared/Uploaded by Learner

- Check whether the credential is **expired**
- Check whether **format/syntax** is correct
- …?

DID Registry/Registries

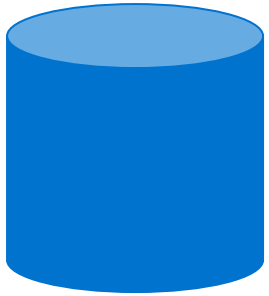
Depend on supported DID methods
Provide cryptographic keys/metadata
e.g. Ethereum, IPFS, Web Server

- Resolve Issuer DID/ **Resolver** Learner DID to obtain **Key Material**
- Verify whether issuer **signature** is valid
- Check if credential provider can **authenticate as credential subject**?
- …?



Credential Status Registry

- Check whether credential has been **issued**
- And **not revoked**
- …?

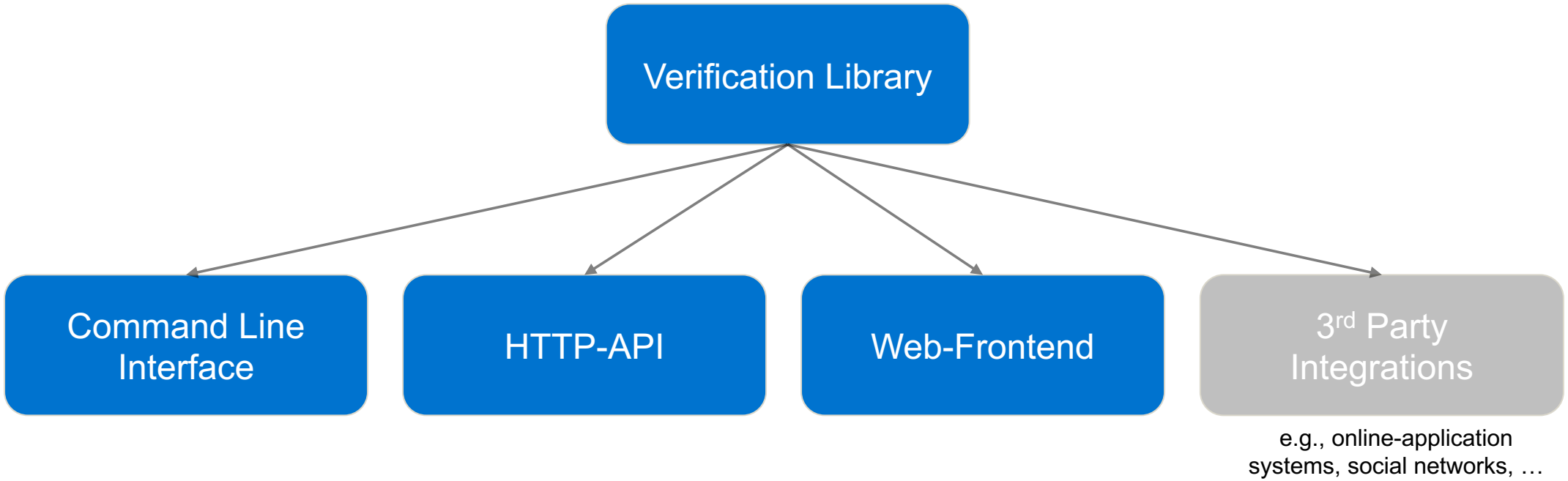


Trusted Issuer Registry

- Check whether the issuer is (still?) a **trusted organization**
- …?

© sebis

Goal: Implementation of Verification Library



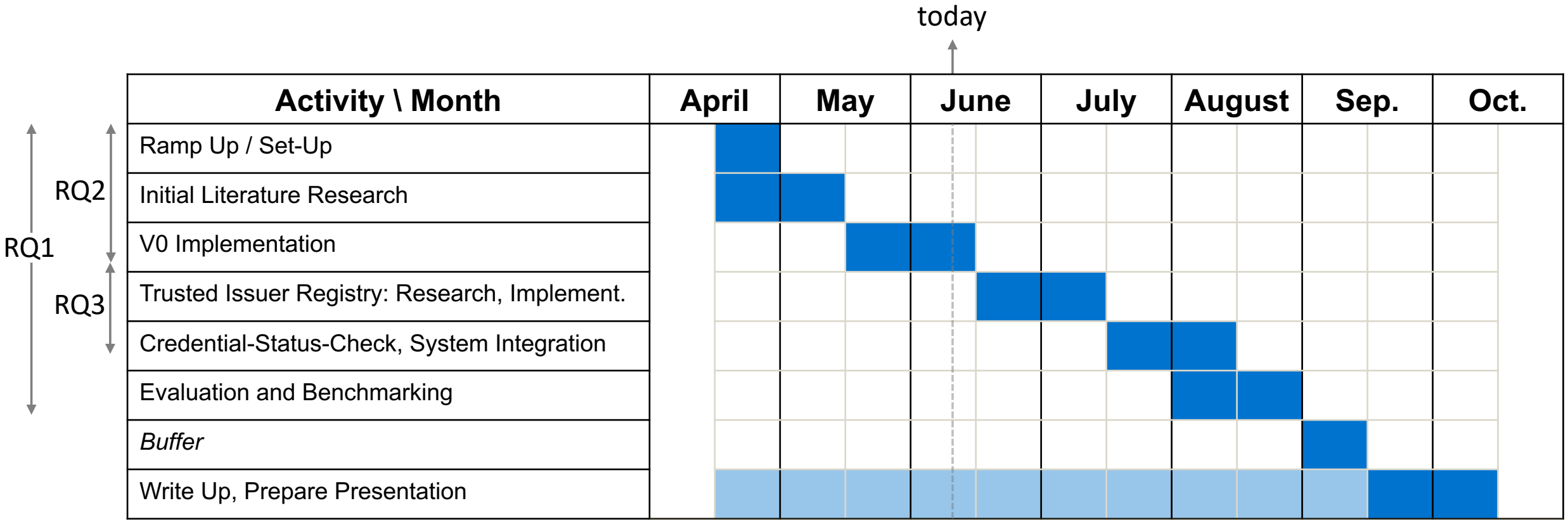
© sebis

Outline

1. Motivation and Introduction
2. Problem Statement
3. Research Questions & Methodology
4. Timeline & Current Status

© sebis

Timeline & Current Status



Current Status:

- Evaluated and assessed several SSI-Frameworks
- Set up DID-Resolving and Dereferencing for did:key, did:web, did:ethr, did:iota
- Set up Signature Verification, supporting EC and EdDSA verification methods
- Currently working on V0-Version of Verification Service (focus on DID-Resolving and Signature Verification)

© sebis

References

Digital Credentials Consortium (2020): Building the digital credential infrastructure for the future, https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf

Hans Pongratz, Matthias Gottlieb, Christoph Meinel, et al. (2022): DiBiHo: Digitale Bildungsnachweise für Hochschulen, https://www.it.tum.de/it/dibiho/

W3C (2021): Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations, https://www.w3.org/TR/did-core/

W3C (2022): Verifiable Credentials Data Model v1.1, https://www.w3.org/TR/vc-data-model/

Icons: https://www.flaticon.com/

© sebis

B.Sc.

Pascal Herrmann
pascal.herrmann@tum.de

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289.17132
Fax +49.89.289.17136

matthes@in.tum.de
wwwmatthes.in.tum.de