

Transforming a Digital University Degree Issuance Process Towards Self-Sovereign Identity

Carsten Sehlke, October 10th, 2022, Master's Thesis

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

Introduction

Problem Statement

Research Questions

Results

Future Work

Motivation: Verifiable Credentials

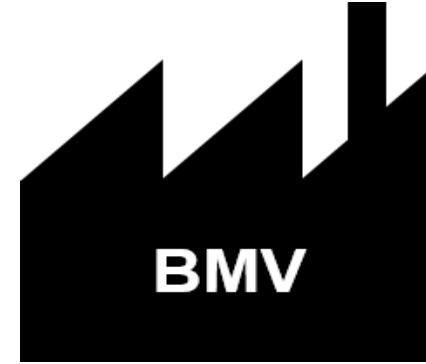


Erika Mustermann

- Just finished university
- Applies for a job online

Wants to:

- Present her university degree digitally



BMV

- Offers a job on website

Wants to:

- Verify the university degree
- Automate processes to reduce costs

Image source: [Personalausweis Führerschein](#)

For more information visit [What is a Verifiable Credential](#) [What is Self-Sovereign Identity \(SSI\)](#)

Motivation: Verifiable Credentials

Physical World



- ✓ Verifiably created by an authority
- ✓ Holder has full control (SSI)
- ✓ Integrity verifiable by everyone
- ✗ Automatically processable

Image source: [Personalausweis Führerschein](#)

For more information visit [What is a Verifiable Credential What is Self-Sovereign Identity \(SSI\)](#)

Motivation: Verifiable Credentials

Physical World



Digital World



- ✓ Verifiably created by an authority
- ✓ Holder has full control (SSI)
- ✓ Integrity verifiable by everyone
- ✗ Automatically processable

Image source: [Personalausweis Führerschein](#)

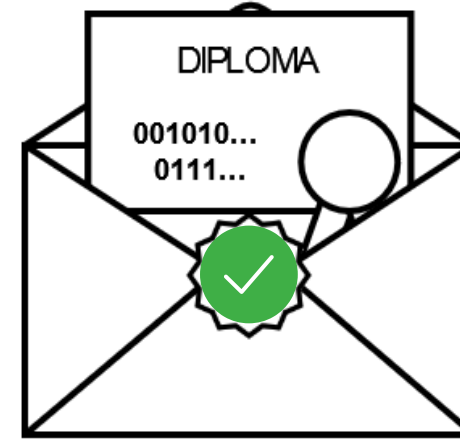
For more information visit [What is a Verifiable Credential What is Self-Sovereign Identity \(SSI\)](#)

Motivation: Verifiable Credentials

Physical World



Digital World (Verifiable Credential)



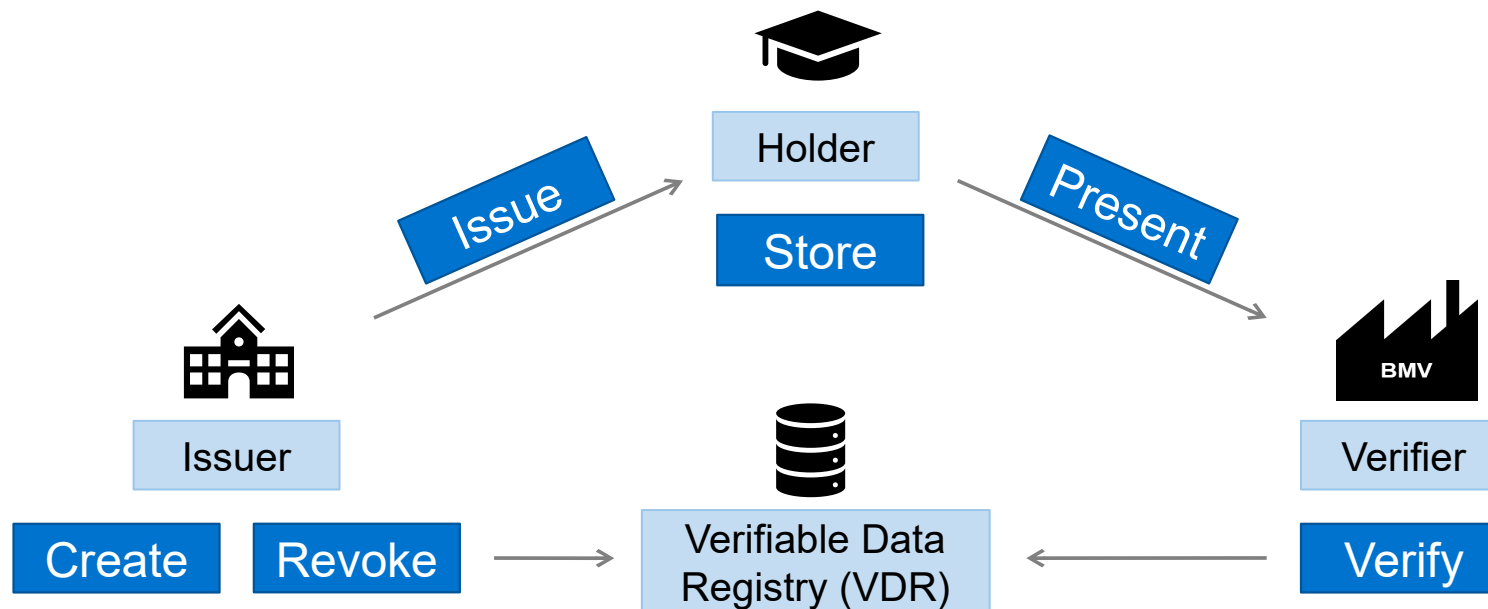
- | | | |
|---|------------------------------------|---|
| ✓ | Verifiably created by an authority | ✓ |
| ✓ | Holder has full control (SSI) | ✓ |
| ✓ | Integrity verifiable by everyone | ✓ |
| ✗ | Automatically processable | ✓ |

Image source: [Personalausweis Führerschein](#)

For more information visit [What is a Verifiable Credential What is Self-Sovereign Identity \(SSI\)](#)

DiBiHo: Digital Credentials for Higher Education Institutions

Project goal: Proof of concept for whole Credential Life-Cycle



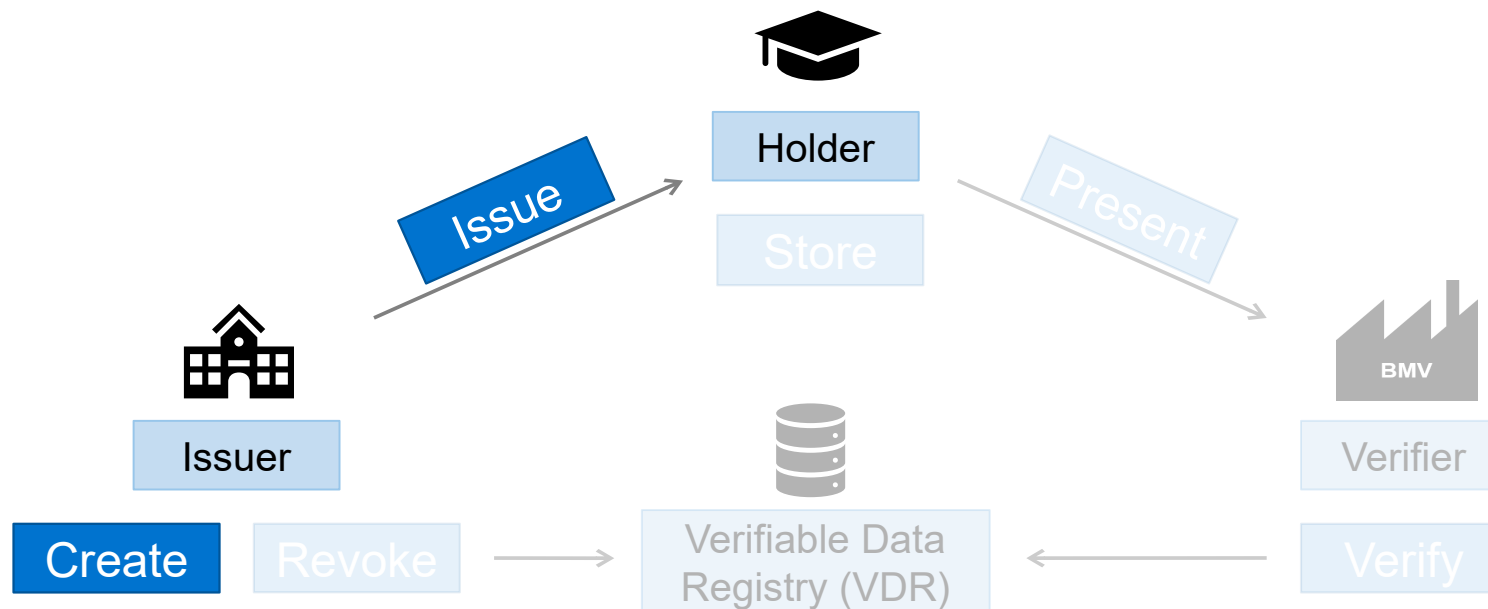
Self-Sovereign Identity (SSI)

- Holder has full control over his (identity) data
- No centralized data storage
- Privacy first approach

For more information visit [DiBiHo What is Self-Sovereign Identity \(SSI\)](#)

DiBiHo: Digital Credentials for Higher Education Institutions

Project goal: Proof of concept for whole Credential Life-Cycle



Self-Sovereign Identity (SSI)

- Holder has full control over his (identity) data
- No centralized data storage
- Privacy first approach

For more information visit [DiBiHo What is Self-Sovereign Identity \(SSI\)](#)

Introduction

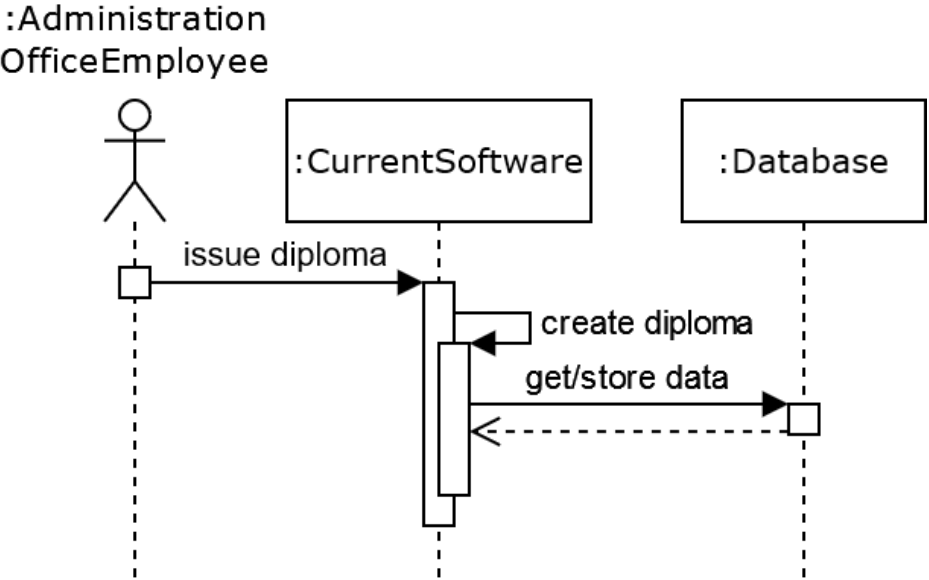
Problem Statement

Research Questions

Results

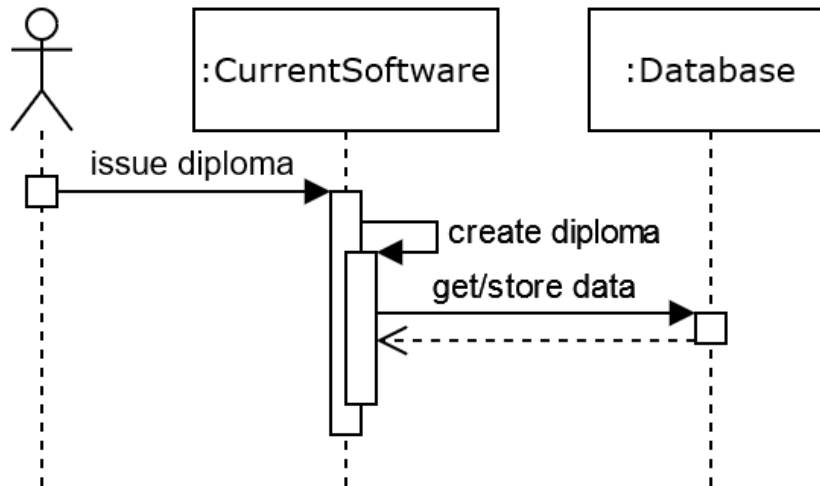
Future Work

Problem Statement: Create Verifiable Credentials



Problem Statement: Create Verifiable Credentials

:Administration
OfficeEmployee

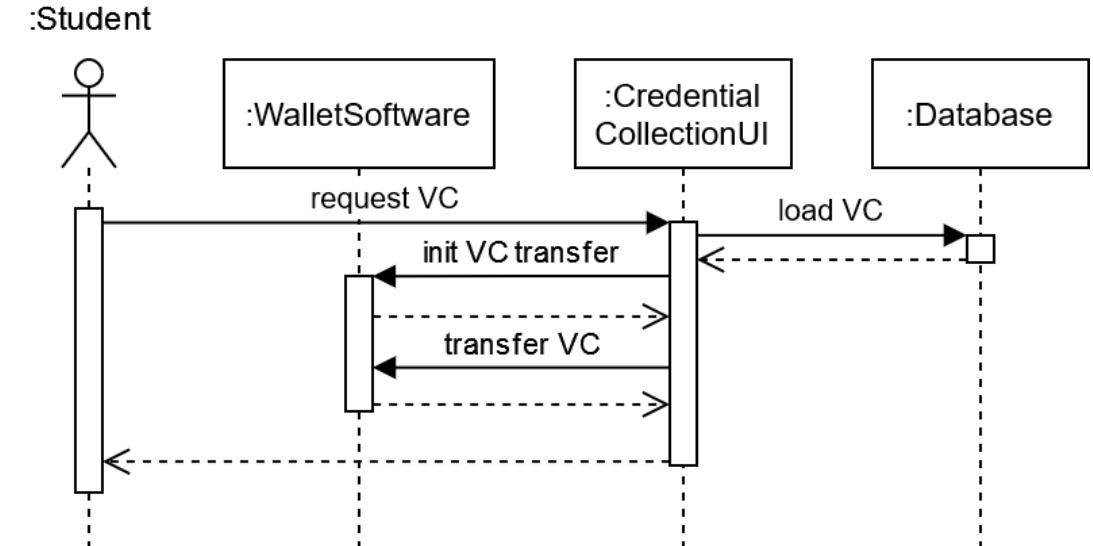


How to trigger the VC creation?

- Create based on the diploma data
- Sign
- Log onto the Verifiable Data Registry (VDR)
- Store

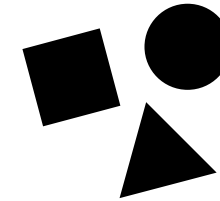
Problem Statement: Student Collects Verifiable Credentials

- Offers an interface for transferring VCs
- Supports multiple transfer protocols



Which format for the data?

- Interoperable
- Compatible with other systems



Outline



Introduction

Problem Statement

Research Questions

Results

Future Work

RQ1: What implementation-specific **requirements** emerge from the process-specific ones for transforming the **local student information system**?

RQ2: What is the **current state of the art for issuing** digitally verifiable credentials to clients?

- Transfer protocols
- Wallet software

RQ3: What **data** in the student information system CAMPUSonline is **relevant**, **where** is it **located**, and **how** can it be **accessed**?

RQ4: What does it need to develop a module for the existing student information systems **CAMPUSonline to issue verifiable credentials?**

- Hardware
- Software
- Configuration changes (firewall/network)
- Distribute VCs

RQ5: To what extent does the implemented solution enable the automated issuance process of university degrees as verifiable credentials?

- Limitations

Outline



Introduction

Problem Statement

Research Questions

Results

Future Work

RQ1: What implementation-specific requirements emerge from the process-specific ones for transforming the local student information system?

1) CAMPUSonline compatibility

2) Data privacy and protection during verifiable credential creating and transfer

3) Invisible to administration office employee to avoid increasing their workload

RQ2: What is the current state of the art for issuing digitally verifiable credentials to clients?



Learner Credential Wallet –
Digital Credentials Consortium



Enmeshed –
j&s-soft



Blockcerts Wallet –
Hyland Credentials



VC Wallet –
Crossword Cybersecurity



Trinsic Wallet –
Trinsic



Indisi Wallet –
CRUBN



Ana Wallet –
Tykn



Microsoft Authenticator –
Microsoft



Consent Wallet –
Infoeaze

Image source: [Google Play Store Tykn](#)

RQ3: What data in the student information system CAMPUSonline is relevant, where is it located, and how can it be accessed?

- Analyzed paper-based degree certificate
 - Identity Data
 - Degree Data



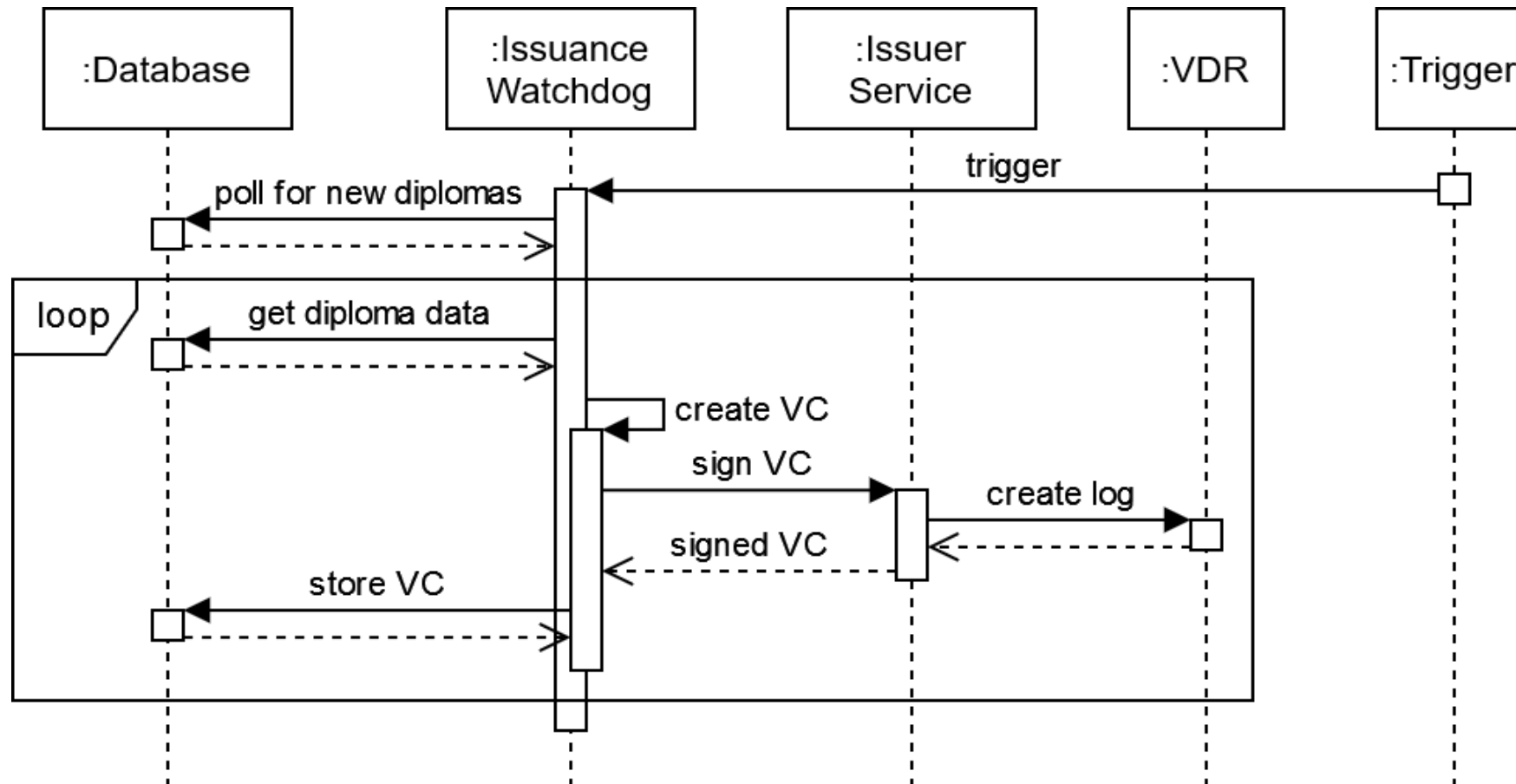
- Built CAMPUSonline database views



- Option to include current paper-based degree documents as PDF

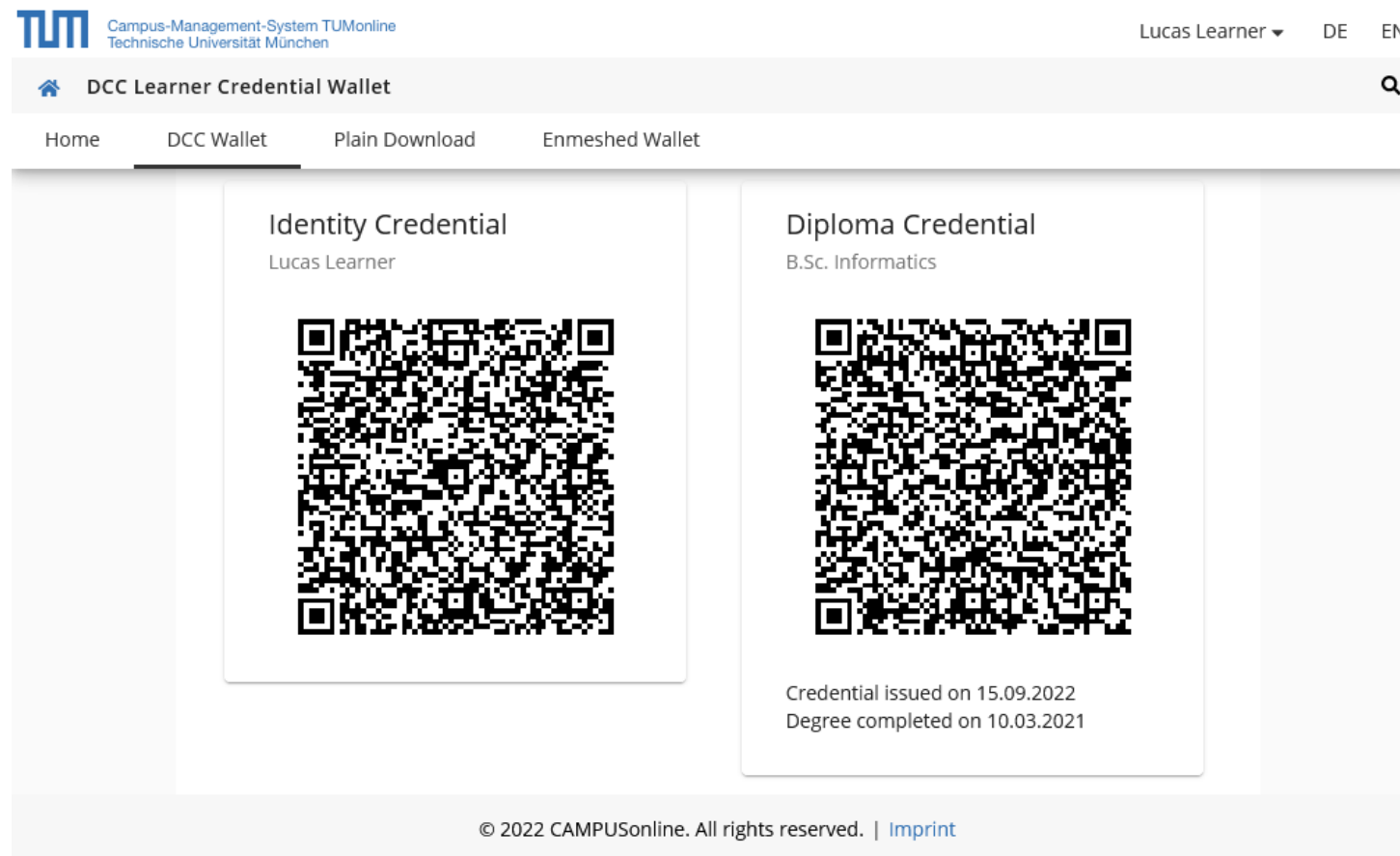
RQ4: What does it need to develop a module for the existing student information systems CAMPUSonline to issue verifiable credentials?

Issuing Verifiable Credentials:



RQ4: What does it need to develop a module for the existing student information systems CAMPUSonline to issue verifiable credentials?

Distributing Verifiable Credentials (via DCC Credential Request):

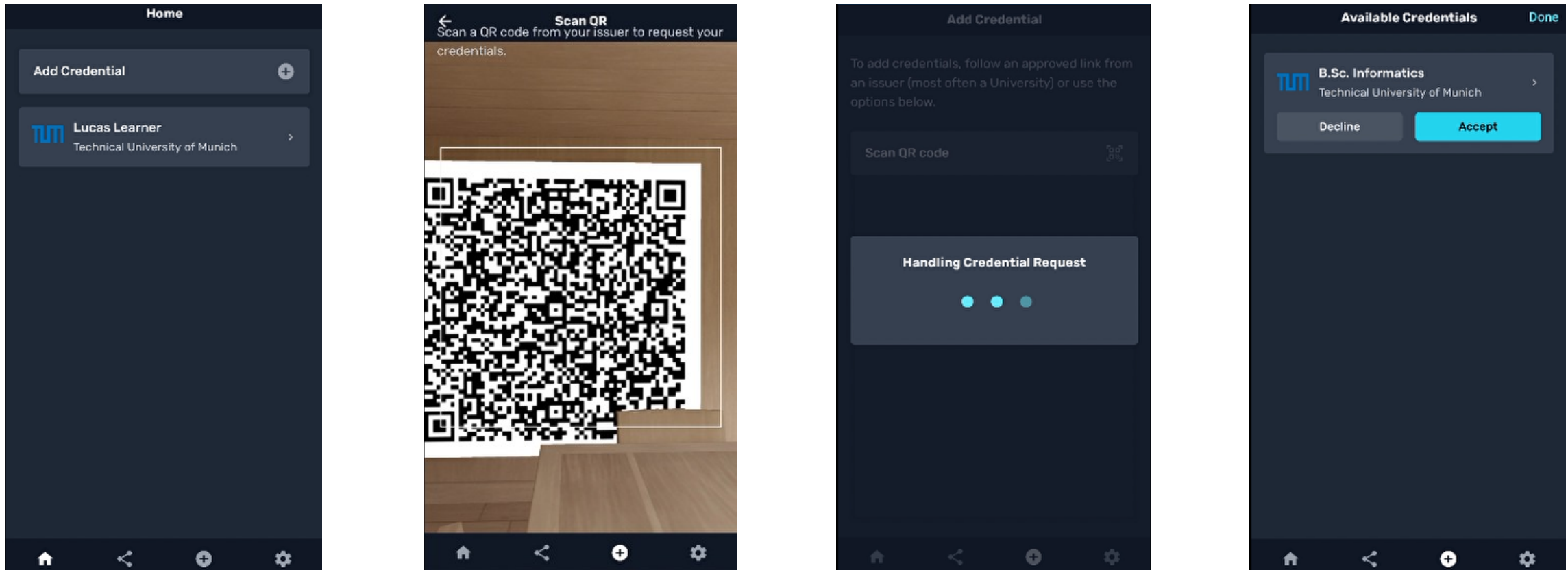


QR code:

- Request URL
- Challenge
- Further app specific information

RQ4: What does it need to develop a module for the existing student information systems CAMPUSonline to issue verifiable credentials?

Distributing Verifiable Credentials (via DCC Credential Request):



RQ5: To what extent does the implemented solution enable the automated issuance process of university degrees as verifiable credentials?

- CAMPUSonline compatibility
- Data privacy and protection
- Invisible to administration office employee



Additionally:

- 100% ELMO/ELM compatible
(European standards for learner data exchange)



RQ5: To what extent does the implemented solution enable the automated issuance process of university degrees as verifiable credentials?

Credential Creation:

- Enrollment process not adapted
 - students cannot provide their public key material (DID)
- VCs creation based on a timewise trigger vs. instant creation
 - VC creation date is off

Credential Distribution:

- VC wallet support limited
- „Golden Standard“ takeout solution missing

RQ5: To what extent does the implemented solution enable the automated issuance process of university degrees as verifiable credentials?

Overall:

- Not production-ready
→ proof of concept
- Not deployed to the CAMPUSonline infrastructure
→ ongoing security audit

Outline



Introduction

Problem Statement

Research Questions

Results

Future Work

Future Work

- Eliminate limitations from RQ5
→ Production-ready implementation
- Improve existing wallet software and transfer mechanisms
→ Further standardization
- Update to verifiable credential v2
- **Spread the word about verifiable credentials**



B.Sc.

Carsten Sehlke

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

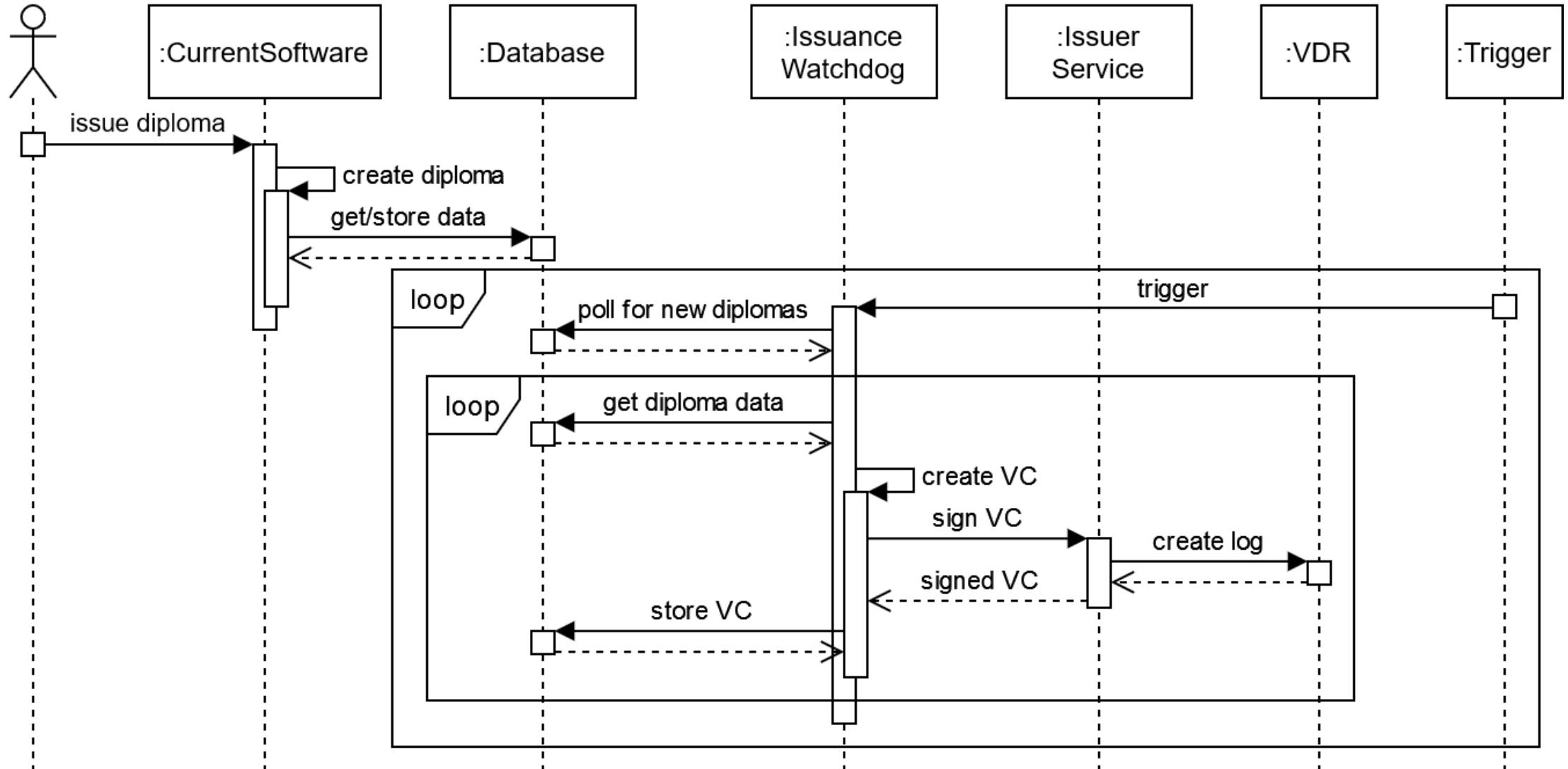
Boltzmannstraße 3
85748 Garching bei München

Carsten.Sehlke@tum.de
www.matthes.in.tum.de



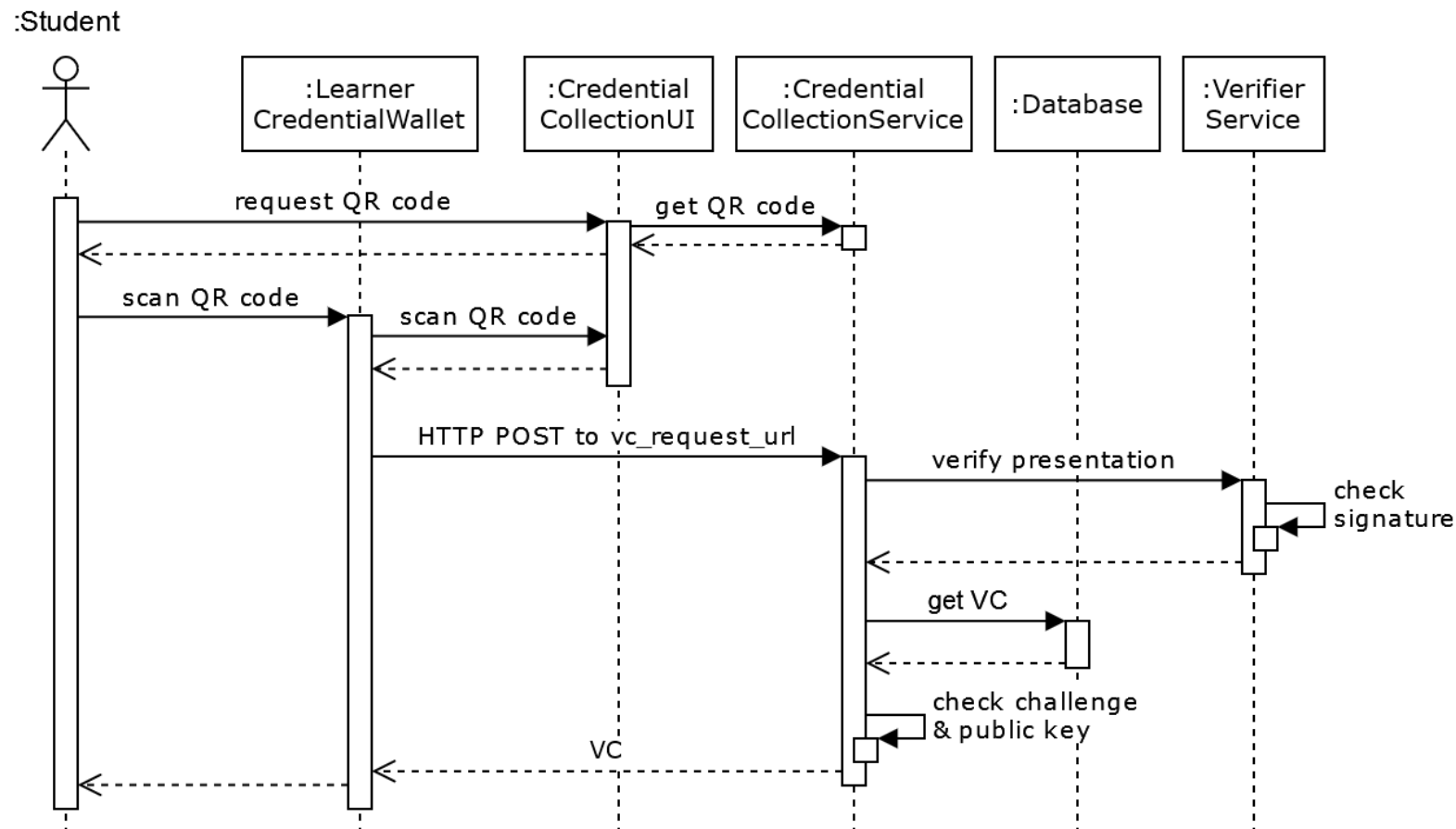
Issuance Watchdog

:Administration
OfficeEmployee

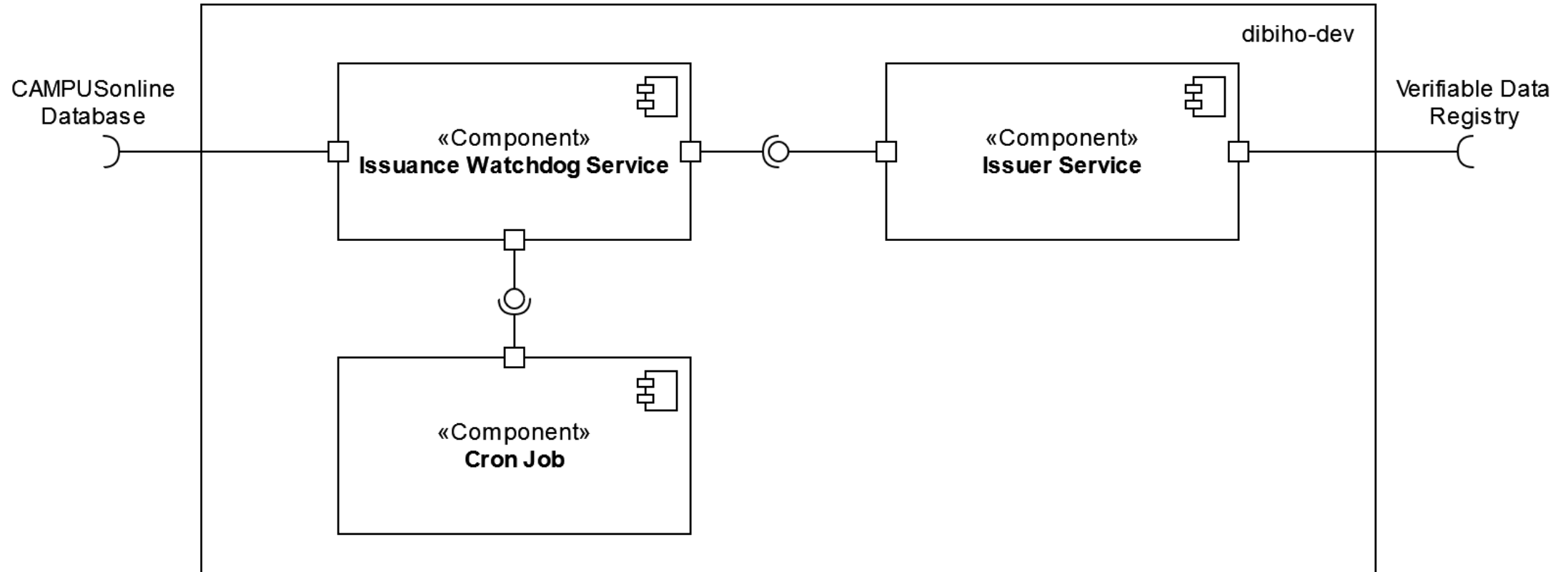


RQ4: What does it need to develop a module for the existing student information systems CAMPUSonline to issue verifiable credentials?

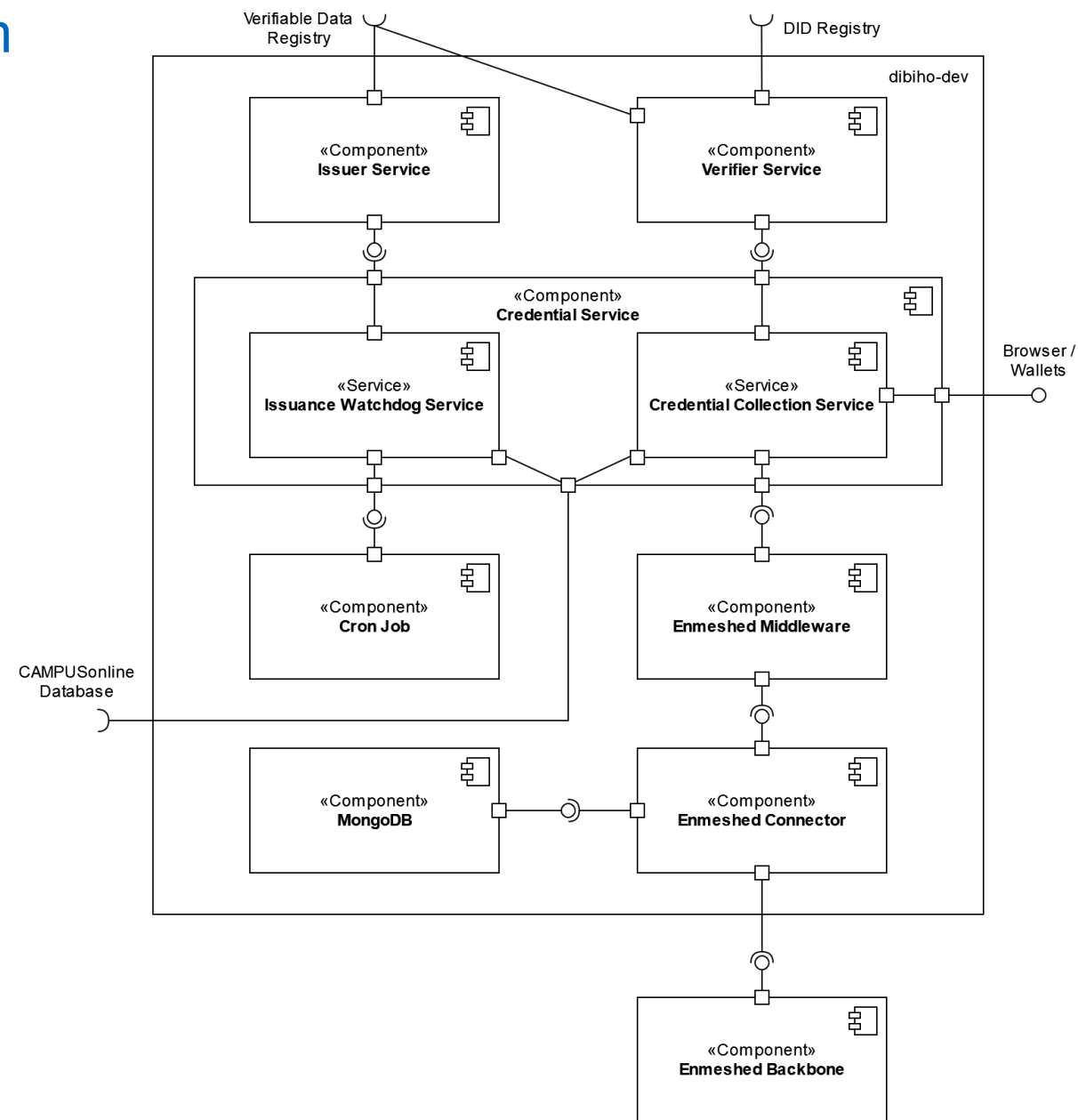
Distributing Verifiable Credentials (via DCC Credential Request):



Issuance Watchdog



Component Diagram



Verifiable (Identity) Credential

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://dibiho.org/contexts/elmoLearner",
    "https://w3id.org/vc-revocation-list-2020/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "type": [ "VerifiableCredential", "IdentityCredential", "ElmoIdentityCredential" ],
  "issuanceDate": "2022-08-04T16:03:20Z",
  "issuer": {
    "name": "Technical University of Munich",
    "url": "https://www.tum.de",
    "image": "https://dibiho.org/resources/img/TUM_logo-440x236.png",
    "id": "did:web:dibiho.org:TUM.Test"
  },
  "credentialSubject": {
    "id": "did:web:dibiho.org:Lucas.Learner",
    "hasCredential": {
      "name": "Lucas Learner",
      "description": "Identity credential for Lucas Learner"
    },
    "elmo": {
      "givenNames": "Lucas",
      "familyName": "Learner",
      "gender": 1,
      "bday": "2000-05-10T00:00:00Z",
      "placeOfBirth": "Bamberg",
      "birthName": "Lucas Learner"
    }
  },
  "expirationDate": "2102-08-04T16:03:20Z",
  "id": "https://dibiho.org/credentials/709",
```

```
  "credentialStatus": {
    "id": "https://dibiho.org/credentials/status/1#709",
    "type": "RevocationList2020Status",
    "revocationListIndex": 709,
    "revocationListCredential": "https://dibiho.org/credentials/status/1"
  },
  "proof": {
    "type": "Ed25519Signature2020",
    "created": "2022-09-07T13:21:43.750Z",
    "verificationMethod": "did:web:dibiho.org:TUM.Test#key",
    "proofPurpose": "assertionMethod",
    "proofValue": "z5o1Y7aNcSWnKwKo3UPxhRFTThWwhEPY66uAVGygsWTZd2Hx5aX8G3eU5hUHs5N7r8B5nS3e2ZqauonjAXTTL6UW9x"
  }
}
```

Verifiable (Degree) Credential

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://dibiho.org/contexts/elmoDiploma",
    "https://w3id.org/vc-revocation-list-2020/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "type": [ "VerifiableCredential", "DiplomaCredential", "ElmoDiplomaCredential" ],
  "issuanceDate": "2022-08-04T17:21:33Z",
  "issuer": {...},
  "credentialSubject": {
    "id": "did:web:dibiho.org:Lucas.Learner",
    "hasCredential": {
      "name": "B.Sc. Informatics",
      "description": "Awarded the academic title Bachelor of Science (B.Sc.) after completing the Informatics program at the Technical University of Munich."
    }
  },
  "elmo": {
    "generatedDate": "2022-08-04T17:21:33Z",
    "learner": {
      "identityCredentialHash": "d6fe2002e674d36f2cd90ce531bb9c89394a0352e43c2ecf23740b0c2090db87",
      "identifier": [{
        "token": "urn:mace:terena.org:schac:personalUniqueCode:de:tum.de:Matrikelnumm er:00001811",
        "type": "esi"
      }]
    }
  },
  "report": [{
    "issuer": {...},
    "issueDate": "2021-03-10T00:00:00Z",
    "learningOpportunitySpecification": [{
      "title": [{ "token": "Informatics", "lang": "EN" }],

```

```

"specifies": {
  "learningOpportunityInstance": {
    "date": "2021-03-10T00:00:00Z",
    "status": "passed",
    "gradingSchemeLocalId": "73c814a3",
    "resultLabel": "1.6",
    "credit": { "scheme": "ects", "value": 180 }
  }
},
"identifier": [...],
"type": ["Degree Programme"],
"description": [
  "Bachelor of Science", "B.Sc.", "Signed by: Prof. Dr. Hans Michael Gerndt",
  "Signed by: Prof. Dr. Thomas F. Hofmann"
],
"hasPart": [{
  "learningOpportunitySpecification": {
    "title": [{ "token": "Bachelor's Thesis", "lang": "EN" }],
    "specifies": {
      "learningOpportunityInstance": {
        "start": "2020-11-11T00:00:00Z",
        "date": "2021-01-14T00:00:00Z",
        "status": "passed",
        "gradingSchemeLocalId": "f6615bde",
        "resultLabel": "1.2",
        "credit": { "scheme": "ects", "value": 12 },
        "languageOfInstruction": ["DE"]
      }
    }
  },
  "identifier": [...],
  "type": ["Course"],
  "description": [{
    "token": "Potential analysis for Big Data in production", "lang": "EN"
  }]
}]
},
}]

```

Verifiable (Degree) Credential (2)

```

    "gradingScheme": [{
      "localId": "73c814a3",
      "description": [{
        "token": "Bachelor Examination\n\nGrade\tShort Name\tDescription\n\n1.6\tG 1,60\tpassed with merit",
        "lang": "EN"
      }]
    }],
    {
      "localId": "f6615bde",
      "description": [{
        "token": "Bachelor's Thesis\n\nGrade\tShort Name\tDescription\n\n1.2\t1,2\tvery good",
        "lang": "EN"
      }]
    }
  ],
  "expirationDate": "2102-08-04T17:21:33Z",
  "id": "https://dibiho.org/credentials/747",
  "credentialStatus": {
    "id": "https://dibiho.org/credentials/status/1#747",
    "type": "RevocationList2020Status",
    "revocationListIndex": 747,
    "revocationListCredential": "https://dibiho.org/credentials/status/1"
  },
  "proof": {
    "type": "Ed25519Signature2020",
    "created": "2022-09-07T13:27:58.408Z",
    "verificationMethod": "did:web:dibiho.org:TUM.Test#key",
    "proofPurpose": "assertionMethod",
    "proofValue": "z5JGdE4JAajAepePdMVmS7EK3dtLb7suN6VTdWdKR5Jcx6kNnW55RpbigEVUk8WYAnMbGmbEvbh7MZnQymHM6wws"
  }
}

```

ELMO Document



```
<elmo
  xmlns="https://github.com/emrex-eu/elmo-schemas/tree/v1"
  xmlns:xml="http://www.w3.org/XML/1998/namespace"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="https://github.com/emrex-eu/elmo-schemas/tree/v1 schema.xsd"
>
  <generatedDate>2022-08-04T17:21:33Z</generatedDate>
  <learner>
    <identifier type="esi">urn:mace:terena.org:schac:personalUniqueCode:de:tum.de:Matrikeln
      ummer:00001811</identifier>
    <givenNames>Lucas</givenNames>
    <familyName>Learner</familyName>
    <bday>2000-05-10Z</bday>
    <placeOfBirth>Bamberg</placeOfBirth>
    <birthName>Lucas Learner</birthName>
    <gender>1</gender>
  </learner>
  <report>
    <issuer> ... </issuer>
    <learningOpportunitySpecification>
      <identifier type="local">4713587</identifier>
      <title xml:lang="EN">Informatics</title>
      <type>Degree Programme</type>
      <description>Bachelor of Science</description>
      <description>B.Sc.</description>
      <description>Signed by: Prof. Dr. Hans Michael Gerndt</description>
      <description>Signed by: Prof. Dr. Thomas F. Hofmann</description>
      <specifies>
        <learningOpportunityInstance>
          <date>2021-03-10Z</date>
          <status>passed</status>
          <gradingSchemeLocalId>73c814a3</gradingSchemeLocalId>
          <resultLabel>1.6</resultLabel>
          <credit>
            <scheme>ects</scheme>
            <value>180</value>
          </credit>
        </learningOpportunityInstance>
      </specifies>
    </learningOpportunitySpecification>
  </report>
</elmo>
```

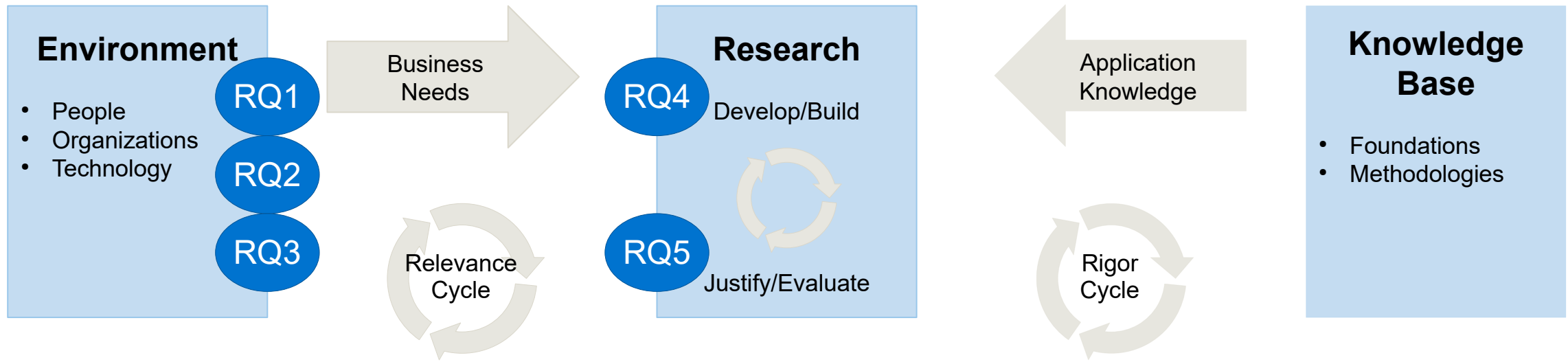
```
</learningOpportunityInstance>
</specifies>
<hasPart>
  <learningOpportunitySpecification>
    <identifier type="local">207366</identifier>
    <title xml:lang="EN">Bachelor's Thesis</title>
    <type>Course</type>
    <description xml:lang="EN">Potential analysis for Big Data in production
    </description>
    <specifies>
      <learningOpportunityInstance>
        <start>2020-11-11Z</start>
        <date>2021-01-14Z</date>
        <status>passed</status>
        <gradingSchemeLocalId>f6615bde</gradingSchemeLocalId>
        <resultLabel>1.2</resultLabel>
        <credit>
          <scheme>ects</scheme>
          <value>12</value>
        </credit>
        <languageOfInstruction>DE</languageOfInstruction>
      </learningOpportunityInstance>
    </specifies>
  </learningOpportunitySpecification>
</hasPart>
</learningOpportunitySpecification>
<issueDate>2021-03-10T00:00:00Z</issueDate>
<gradingScheme localId="73c814a3">
  <description xml:lang="EN">Bachelor Examination

  Grade  Short Name  Description

  1.6    G    1,60  passed with merit</description>
</gradingScheme>
<gradingScheme localId="f6615bde">
  <description xml:lang="EN">Bachelor's Thesis

  Grade  Short Name  Description

  1.2    1,2    very good</description>
</gradingScheme>
</report>
</elmo>
```



Hevner et al. "Design Science in Information Systems Research." In: *Management Information Systems Quarterly* 28(Mar. 2004), pp. 75–105.

Motivation: Verifiable Credentials

Physical World



- ✓ Verifiably created by an authority
- ✓ Holder has full control (SSI)
- ✓ Integrity verifiable by everyone
- ✗ Automatically processable

Image source: [Personalausweis Führerschein](#)

For more information visit [What is a Verifiable Credential What is Self-Sovereign Identity \(SSI\)](#)

Motivation: Verifiable Credentials

Physical World



Digital World



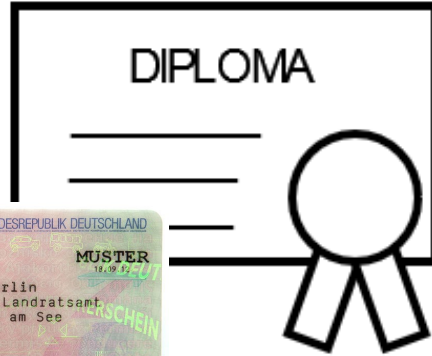
- ✓ Verifiably created by an authority
- ✓ Holder has full control (SSI)
- ✓ Integrity verifiable by everyone
- ✗ Automatically processable

Image source: [Personalausweis Führerschein](#)

For more information visit [What is a Verifiable Credential What is Self-Sovereign Identity \(SSI\)](#)

Motivation: Verifiable Credentials

Physical World



Digital World (PDF-Scan)



✓	Verifiably created by an authority	✗
✓	Holder has full control (SSI)	✓
✓	Integrity verifiable by everyone	✗
✗	Automatically processable	✗

Image source: [Personalausweis Führerschein](#)

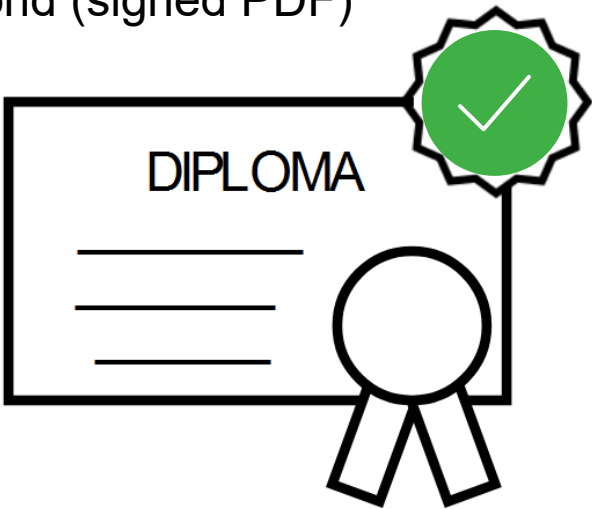
For more information visit [What is a Verifiable Credential What is Self-Sovereign Identity \(SSI\)](#)

Motivation: Verifiable Credentials

Physical World



Digital World (signed PDF)



✓	Verifiably created by an authority	✓
✓	Holder has full control (SSI)	✓
✓	Integrity verifiable by everyone	✓
✗	Automatically processable	✗

Image source: [Personalausweis Führerschein](#)

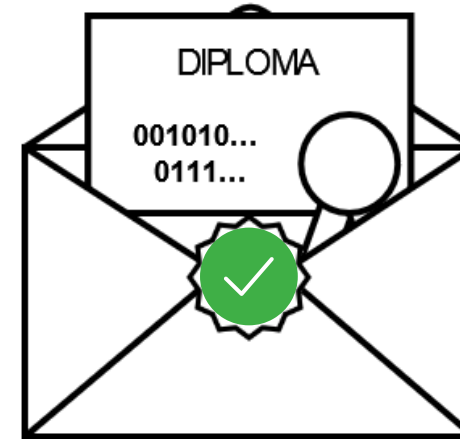
For more information visit [What is a Verifiable Credential What is Self-Sovereign Identity \(SSI\)](#)

Motivation: Verifiable Credentials

Physical World



Digital World (Verifiable Credential)



- | | | |
|---|------------------------------------|---|
| ✓ | Verifiably created by an authority | ✓ |
| ✓ | Holder has full control (SSI) | ✓ |
| ✓ | Integrity verifiable by everyone | ✓ |
| ✗ | Automatically processable | ✓ |

Image source: [Personalausweis Führerschein](#)

For more information visit [What is a Verifiable Credential What is Self-Sovereign Identity \(SSI\)](#)