How to Wisely Identify Natural Subjects in Verifiable Credentials

Evan Christopher, 26.06.2023, Bachelor's Thesis Kickoff Presentation

Chair of Software Engineering for Business Information Systems (sebis)
Department of Computer Science
School of Computation, Information and Technology (CIT)
Technical University of Munich (TUM)
wwwmatthes.in.tum.de

Outline

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

Motivation – Self-Sovereign Identity (SSI)

Self-Sovereign Identity

Having authority and control over your own identity, without a centralised trusted party.

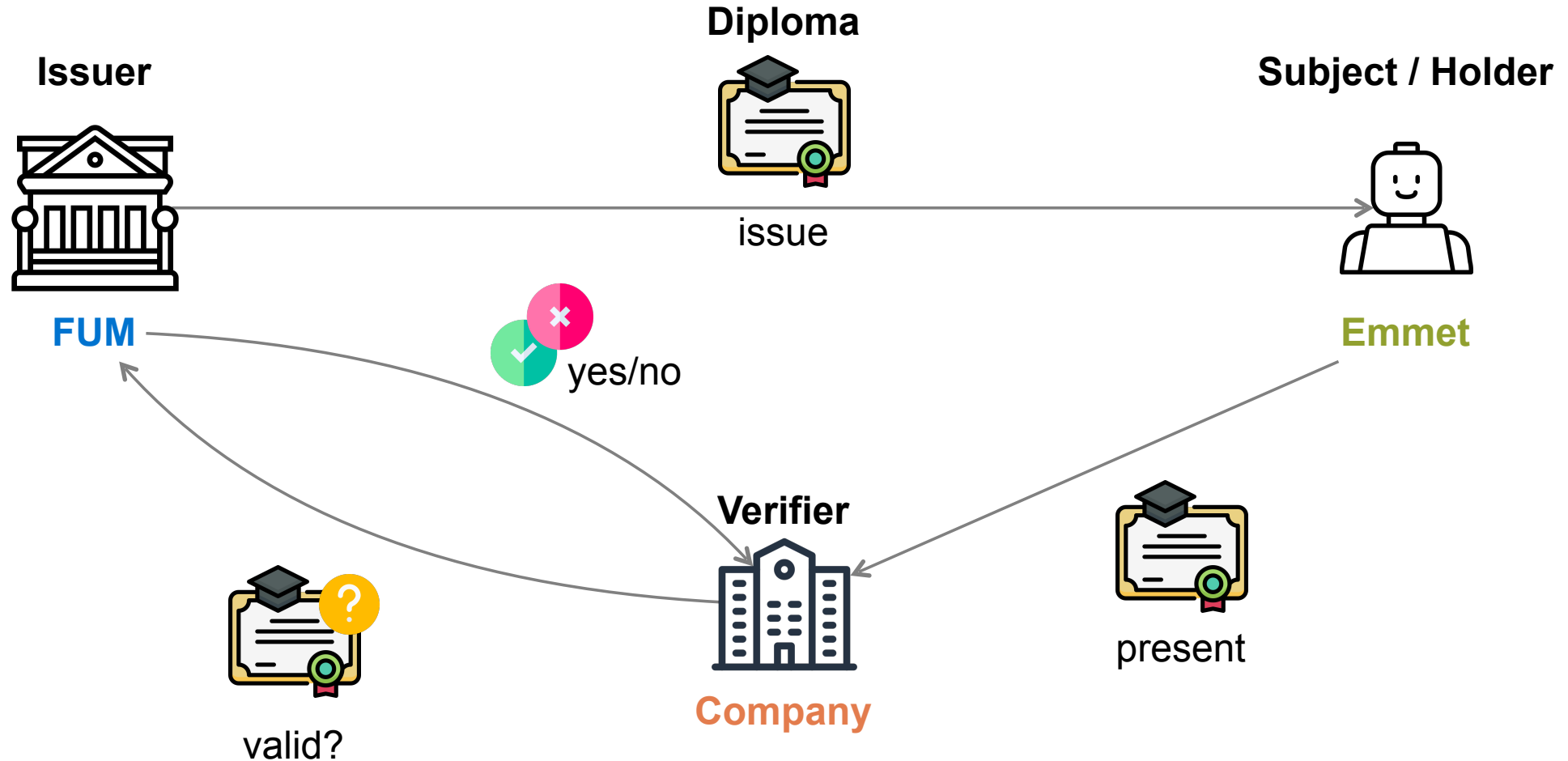| Verifiable Credentials	Decentralised Identifiers

Just a concept? **No!**

Motivation – Self-Sovereign Identity (SSI)

Job Application using Diploma

Diploma

Issuer

Subject / Holder

FUM

issue

Emmet

yes/no

Verifier

valid?

present

Company

Motivation – Self-Sovereign Identity (SSI)

Job Application using Diploma

Diploma Verification

❌ Manual work

❌ Issuer required

❌ Prone to fraud

alleviated by

Self-Sovereign Identity ←

Who is the diploma for?

FUM

With this diploma the
Fictional University of Munich
awards
Mr.
Emmet
Born Ocenia, April 10 1984
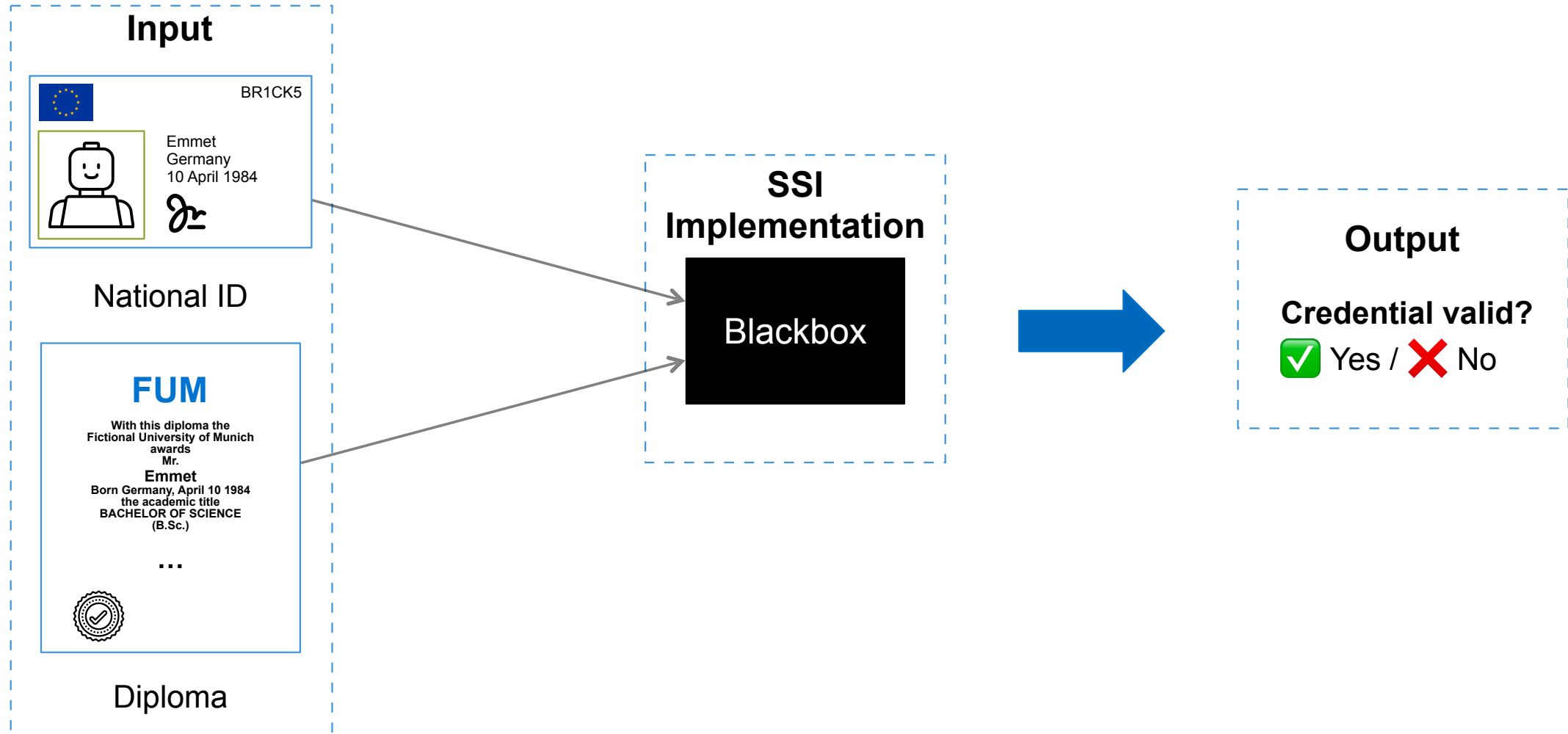the academic title
BACHELOR OF SCIENCE
(B.Sc.)

…
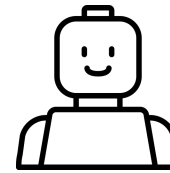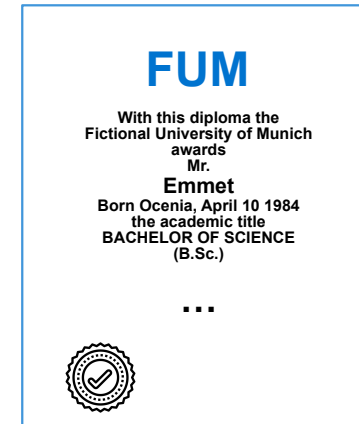
PII contained:

- Name
- Birthdate
- Place of birth
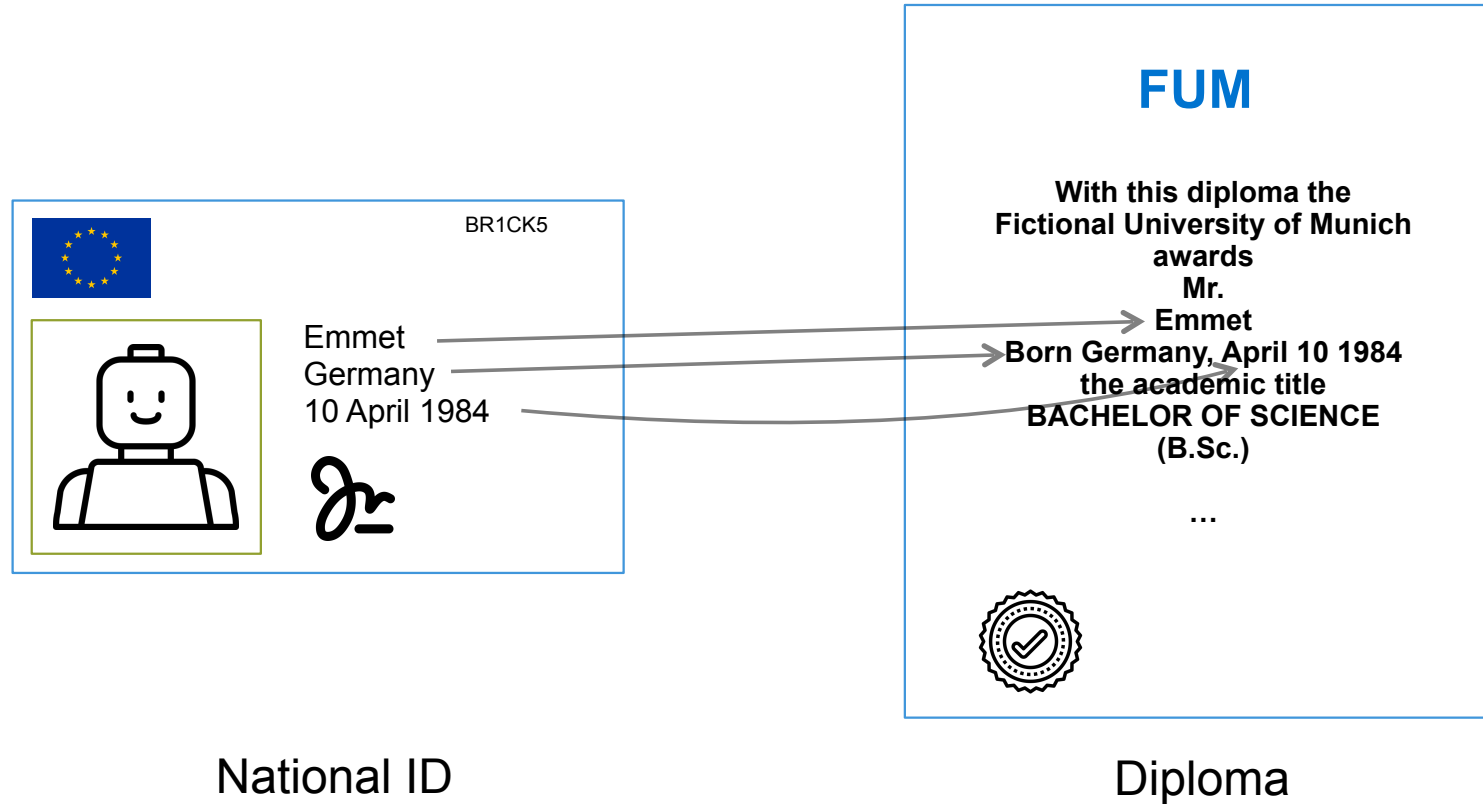
How is the diploma (credential) linked to Emmet (its subject)?
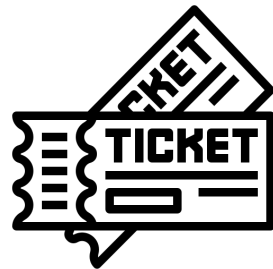
?

Problem Statement – Vision

Problem Statement – Solution(?)

Credential (Attributes) mapping?   ❌ **Limit automation**

National ID

Diploma

Motivation – Self-Sovereign Identity (SSI)

TLUTI

Verifiable Credentials (VCs)
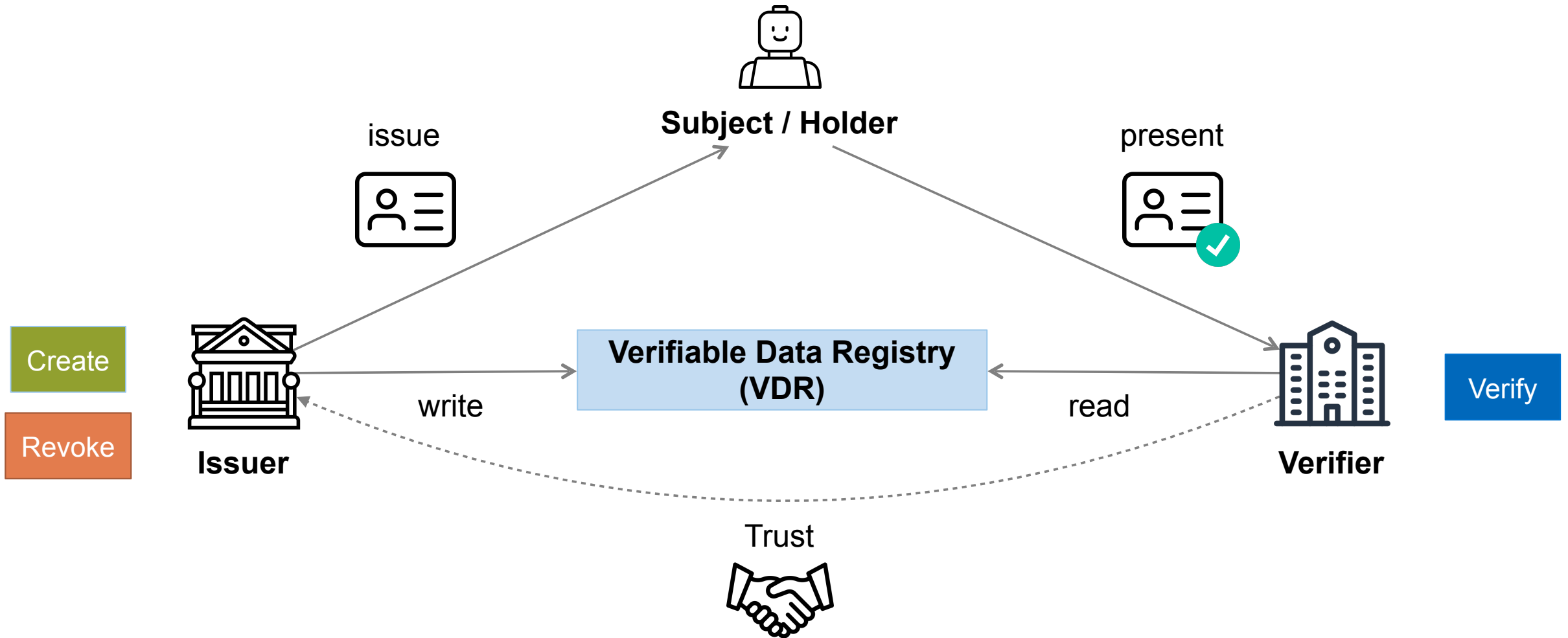

Credentials

```
{
    "@context": [
        "https://www.w3.org/2018/credentials/v1",
        "https://www.w3.org/2018/credentials/
        examples/v1"
    ],
    "type": ["VerifiableCredential"],
    "issuer": "https://example.com/issuers/14",
    "issuanceDate": "2023-04-30T12:34:56Z",
    "expirationDate": "2028-04-30T12:34:56Z",
    "credentialSubject": {
        "name": "Erika",
        "familyName": "Mustermann"
    } …..
}
```

Digital Verifiable Credentials

Motivation – Self-Sovereign Identity (SSI)

Verifiable Credentials Lifecycle

Subject / Holder

issue

present

Create

Revoke

Issuer

write

Verifiable Data Registry
(VDR)

read

Verify

Verifier

Trust

Motivation – Self-Sovereign Identity (SSI)

Decentralised Identifiers (DIDs)

Research Questions
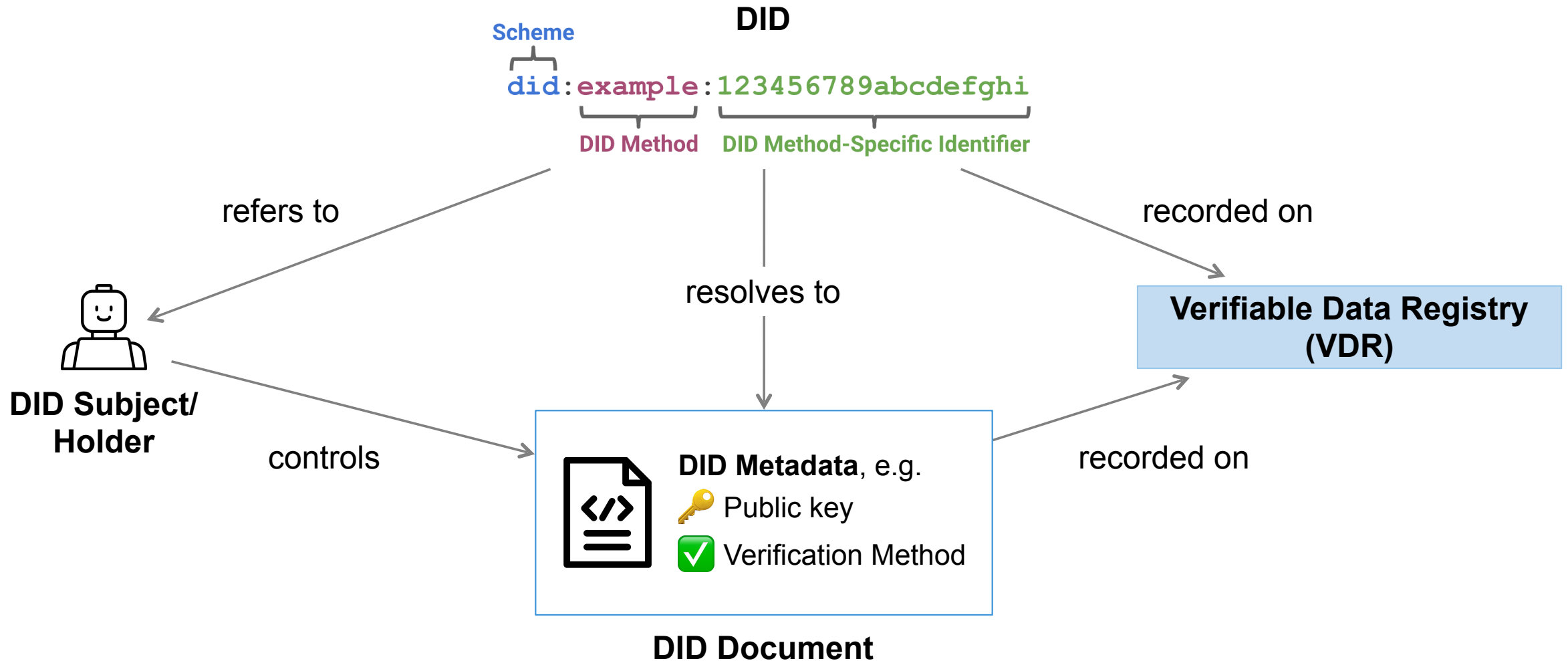
RQ1 What are the existing solutions and proposals for including identifying information in VCs?

    A. How are identifying information included in VCs from these existing solutions?

    B. How do the existing approaches compare?

Comparative survey

RQ2 How can updates to identifying information be handled in VCs?

    A. What are the actively used update mechanisms for VCs?

    B. What are the existing methods for propagating changes in VCs when identifying information is updated?

RQ3 What is the most effective method to include identifying information in Verifiable Credentials?

Design/ implement

    A. How can we ensure the method is adaptable for identity changes?

    B. How can we confirm multiple presented VCs belong to the same natural person?

Methodology and Current Status

Comparative survey

1. (Adapted) Multivocal Literature Review [1]

- Find existing approaches from white and grey literature

2. Nickerson et al. [2]

- Create a taxonomy to differentiate existing approaches

- (Combination of) **Keywords used for literature search:**
  - *Verifiable Credentials, Digital credentials, Digital Identity, Decentralised Identity, Identity Management, Self-sovereign identity, Know your customer, Proof of personhood, Personal identifying information, Biometrics, Credential updates, Credential metadata, Credential transfer, Credential linking, Micro-credentials, and Attribute-based Credentials.*
- **Databases/Tools**
  - IEEE, Scholar, elicit.org
- **Initial inclusion Criteria**
  - English-language papers between April 2016 – June 2023
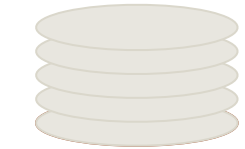 - Read through abstract

[1] Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Information and software technology, 106, 101-121.

[2] Nickerson, R., Varshney, U. & Muntermann, J. A method for taxonomy development and its application in information systems. Eur J Inf Syst 22, 336–359 (2013). https://doi.org/10.1057/ejis.2012.26
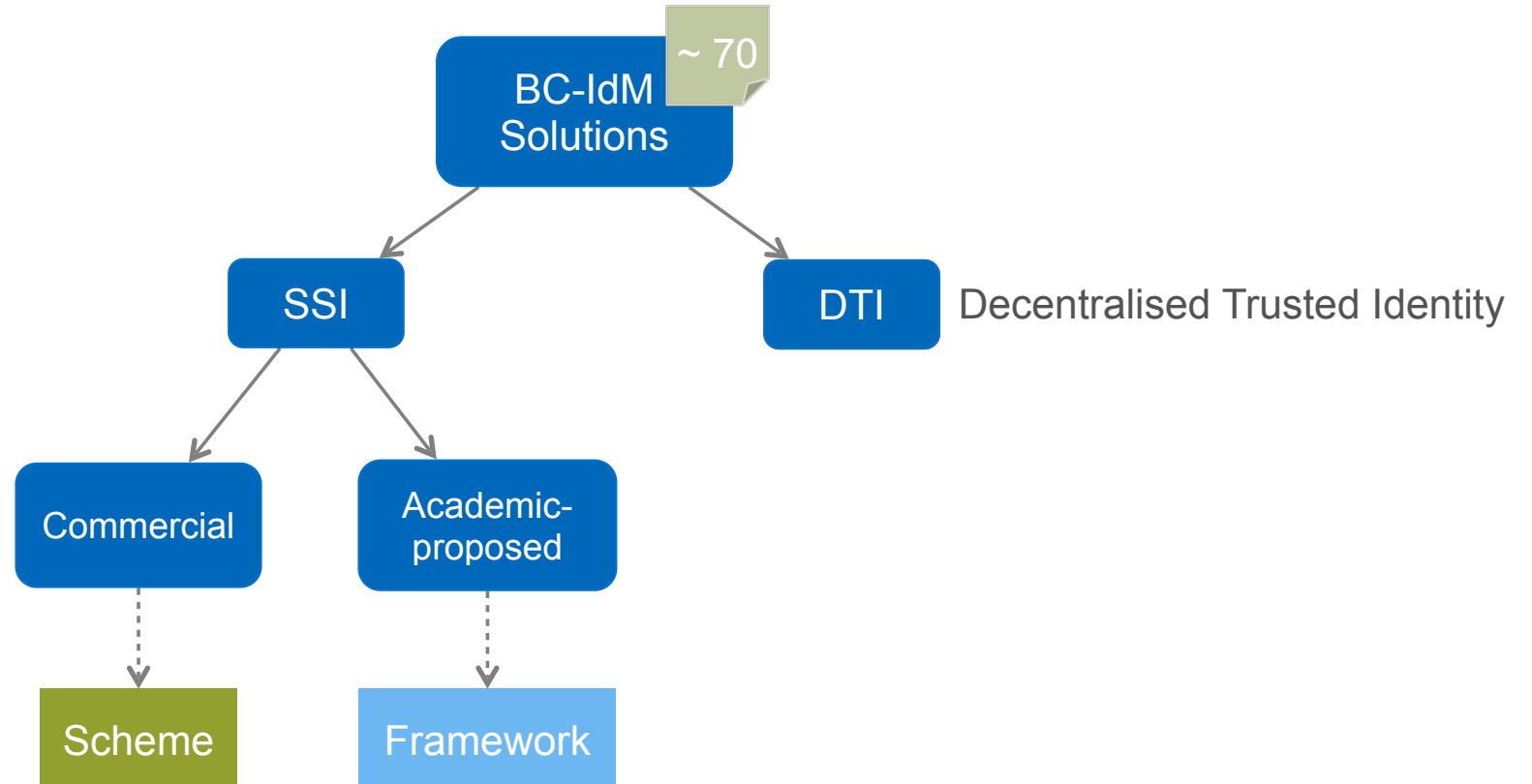
Methodology and Current Status

Comparative survey – Literature review

- **Initial Results**

~ **90** Papers

10 Survey papers

BC-IdM Solutions ~ 70

SSI

DTI — Decentralised Trusted Identity

Commercial

Academic-proposed

Scheme

Framework

M. R. Ahmed, A. K. M. M. Islam, S. Shatabda and S. Islam, "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," in IEEE Access, vol. 10, pp. 113436-113481, 2022, doi: 10.1109/ ACCESS.2022.3216643.

Timeline

	May	June	July	August	September	October
Research						
Survey						
Design						
Prototype						
Evaluation						
Writing						

Registration Date
May 15

Today
June 26

Submission Date
October 15
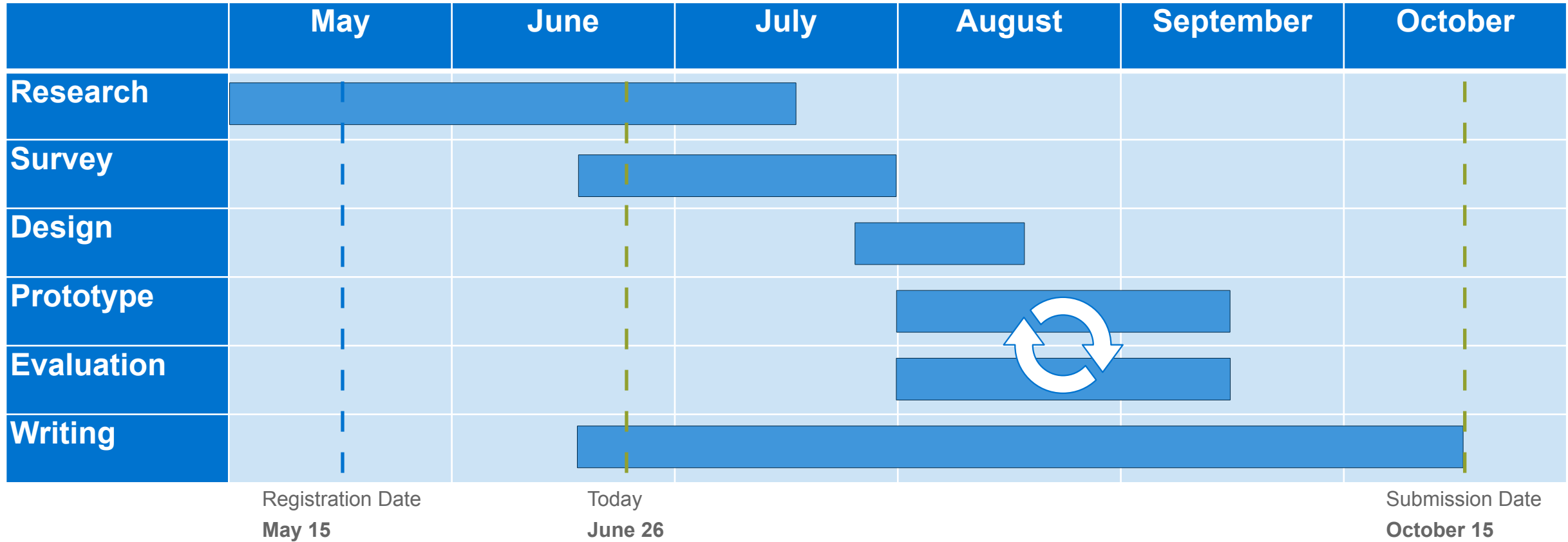
Evan Christopher

evan.christopher@tum.de

Technical University of Munich (TUM)

TUM School of CIT
Department of Computer Science (CS)
Chair of Software Engineering for Business
Information Systems (sebis)

Boltzmannstraße 3

85748 Garching bei München

wwwmatthes.in.tum.de