Design and Implementation of a Decentralized Trusted Issuer Registry for Self-Sovereign Identity

Michael Schmidmaier

16.10.2023, Kick-off 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
2. Problem Statement
3. Research Questions
4. Methodology
5. Timeline

© sebis

Are you in control of your digital identity?

- We all have only one real identity -> but many online accounts
- Identity providers have full control over your online identity
- You have limited control over your identity
- Today: low interoperability & portability, limited data protection, …

© sebis

Self-Sovereign Identity (SSI)

A rather new approach on digital identity where users have full control over their identity without relying on a third party [1]

© sebis

Gaia-X [2]

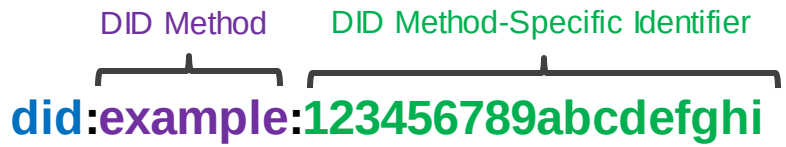
- A large European project, currently 377 members [3]
- Goal: a federated, self-sovereign and secure data infrastructure built on common standards and interfaces
- Gaia-X won't run the infrastructure, but build its standards

- Source of requirements for my thesis

© sebis

Decentralized Identifiers [4]

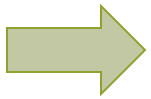
- A W3C standard for identifying subjects without relying on a central organization
- Today: Username, email address, phone number, etc...



did:ethr:0xc530503a148babcaca6…

did:web:tum.de

…



```
// DID-Document
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security
/suites/ed25519-2020/v1"
  ],
  "id":
"did:example:123456789abcdefghi",
  authentication": [{
    "id":
"did:example:123456789abcdefghi#key
s-1",
    "type":
"Ed25519VerificationKey2020",
    "controller":
"did:example:123456789abcdefghi",
    "publicKeyMultibase":
"zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwn
Zn6z3wXmqPV"
  }]
}
```


© sebis

Verifiable Credentials [5]

- A W3C standard for subjects making claims about subjects that can be cryptographically verified
- Example: Company A claims that person B is an employee at A

…


```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials
/examples/v1"
  ],
  "id": "http://example.edu/credentials/1872",
  "type": ["VerifiableCredential",
"AlumniCredential"],
  "issuer": "https://example.edu/issuers/565049",
  "issuanceDate": "2023-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "alumniOf": {
      "id":
"did:example:c276e12ec21ebfeb1f712ebc6f1",
      "name": [{
        "value": "Example University",
        "lang": "en"
      }]
    }
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2023-06-18T21:19:10Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://example.edu
/issuers/565049#key-1",
    "jws": "eyJhbGci...dBBPM"
  }
}
```

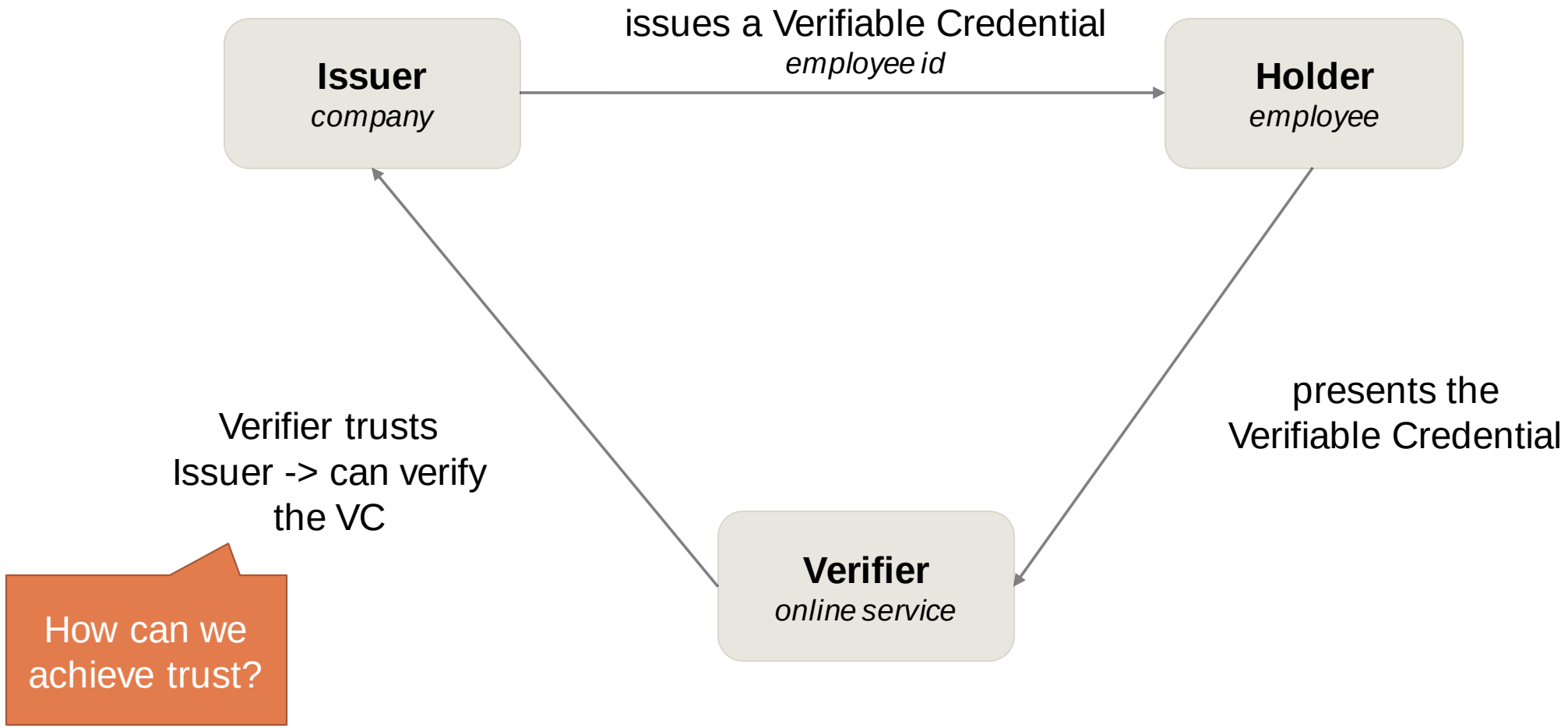

Verifiable Credential

- Metadata (e.g., Issuer DID)
- Claim(s)
- Proof(s)

© sebis

Problem Statement [5]

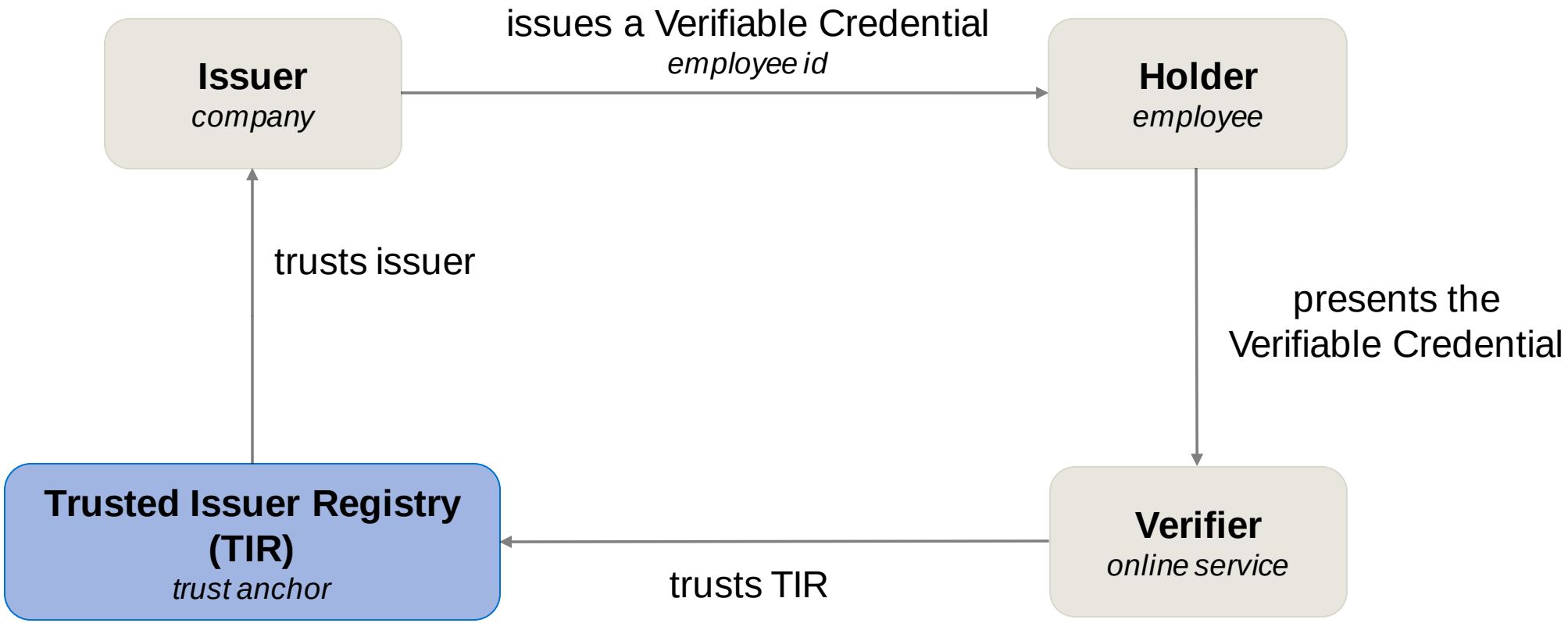
example



© sebis

Problem Statement [5]

example



© sebis

Problem Statement

Trusted Issuer Registry (TIR)

- There exist already some Trusted Issuer Registry designs
- But: they all have several drawbacks

- Centralization vs Decentralization
- Authentication and/or Authorization?
- Scalability
- Security

[6]

```
// DCC Issuer Registry MVP
{
  "meta": {
    "created":
"2020-12-02T02:32:16+0000",
    "updated": "2022-05-25T12:40:00+0000"
  },
  "registry": {
     "did:example:1234": {
        "name": "Example University",
        "location": "San Diego, CA, USA",
        "url": "https://www.example.edu"
     },
     "did:web:tum.de": {
        "name": "Technical University
Munich",
        "location": "Munich, Germany",
        "url": "https:/www.tum.de"
     }
  }
}
```

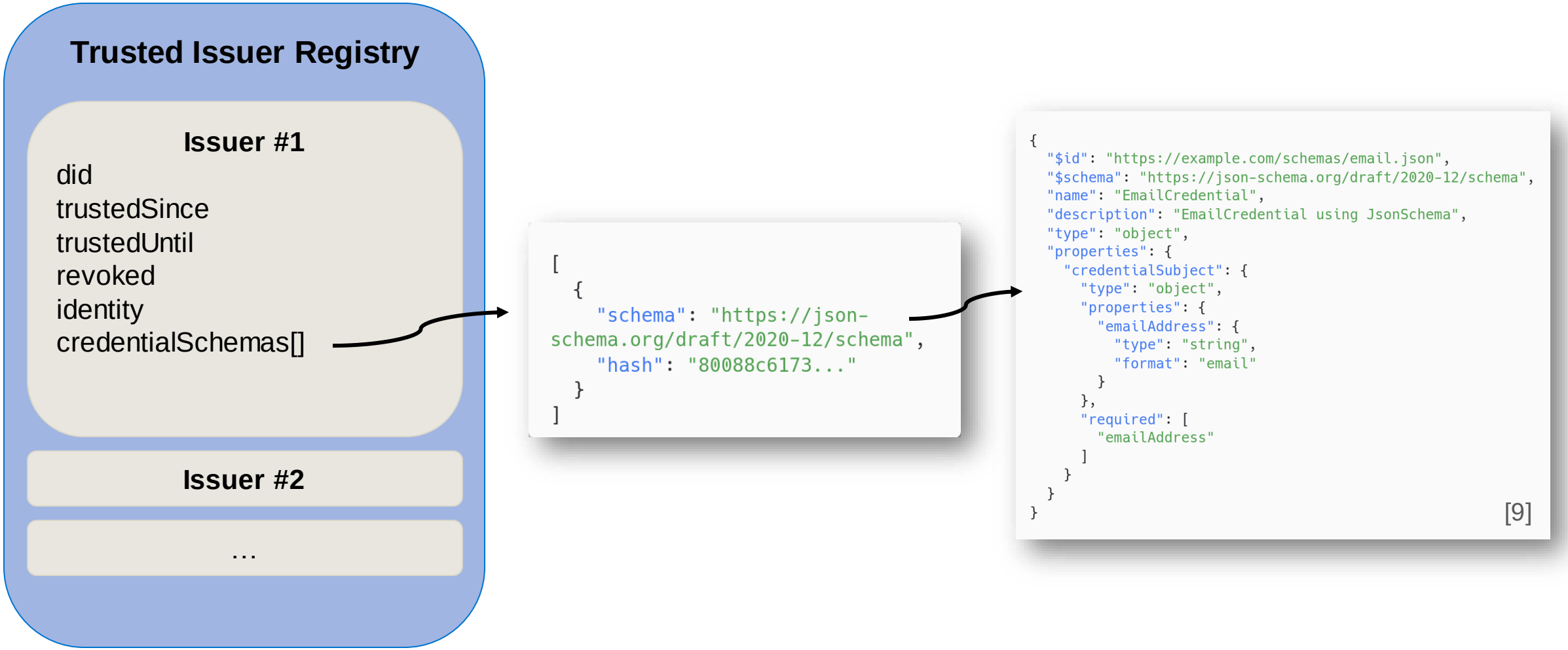
TRAIN
Jeyakumar,
Chadwick, Kubach [7]

ebsi European Blockchain [8]

...

© sebis

Potential Solutions - Authorization

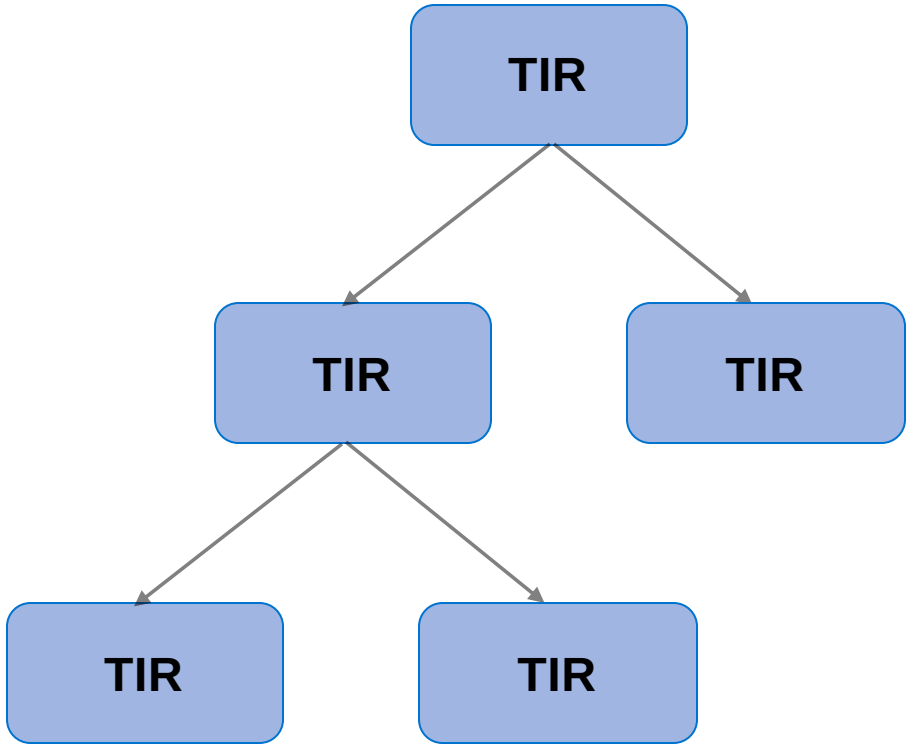


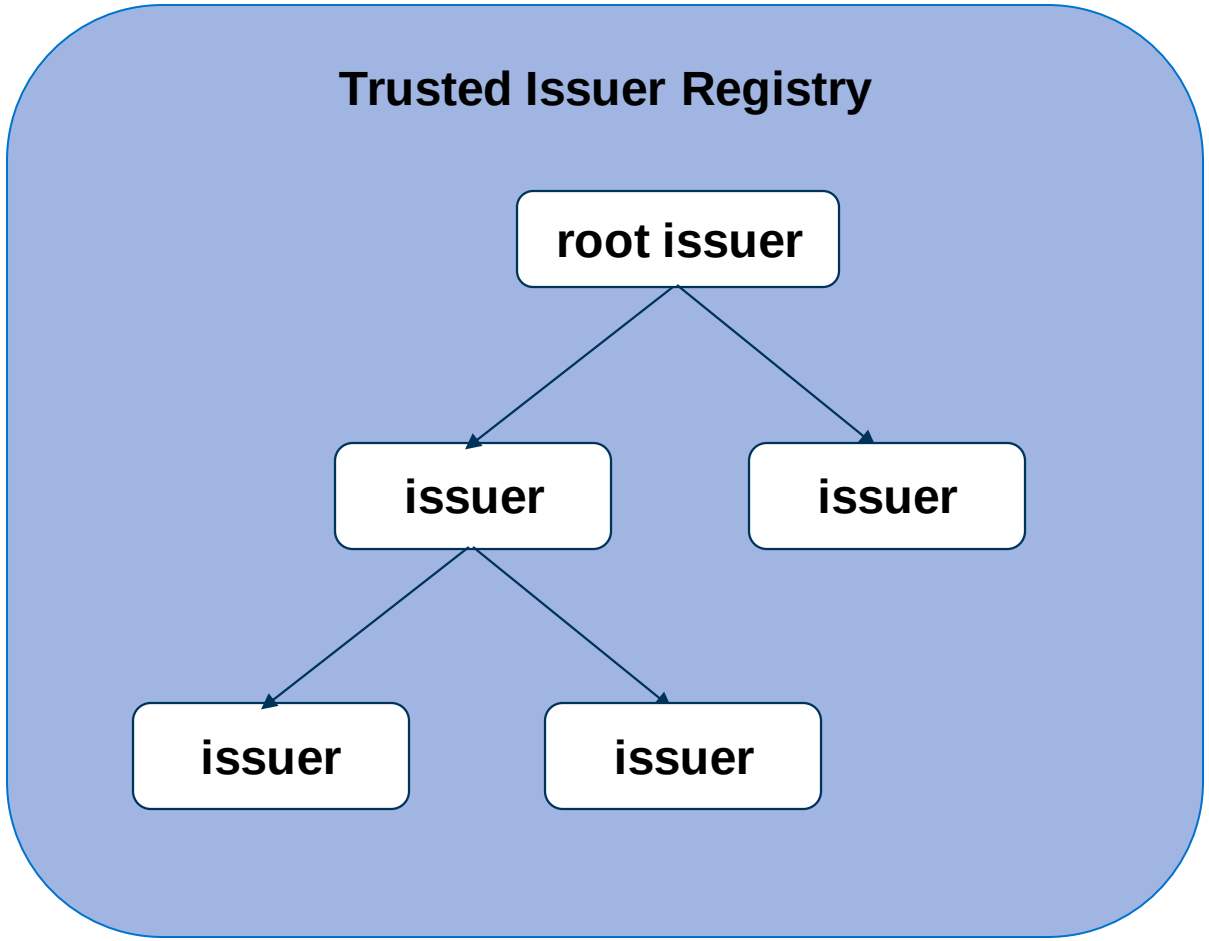
[9]

© sebis

Potential Solutions - Scalability

- Hierarchy of registries
- Hierarchy of issuers
- ...





© sebis

Research Questions

RQ1: What are the advantages and disadvantages of existing centralized and decentralized Trusted Issuer Registry designs?

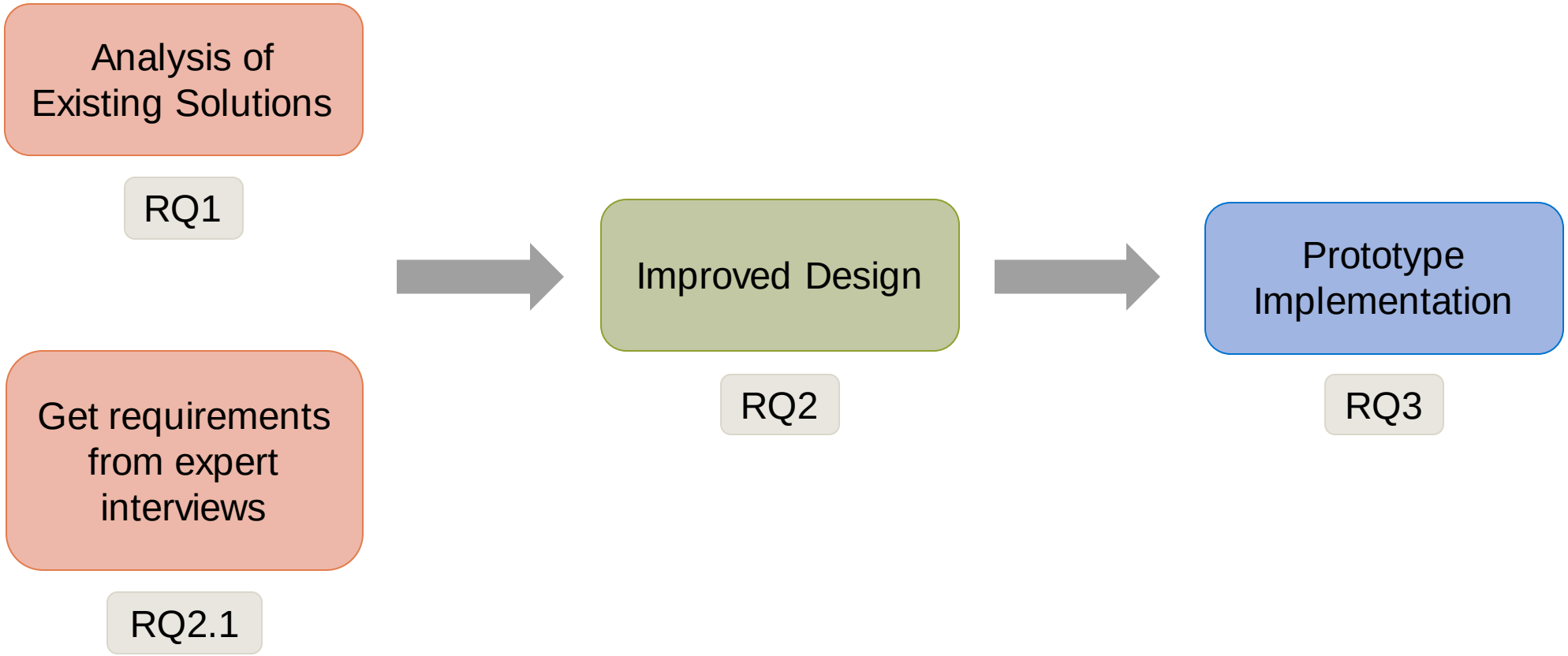
RQ2: How can a general-purpose Trusted Issuer Registry be designed to meet the needs of Self-Sovereign Identity in Gaia-X ecosystems and address the drawbacks of existing solutions?

- **RQ2.1:** What are the requirements for a Trusted Issuer Registry in Gaia-X ecosystems?
- **RQ2.2:** What specific functionalities should a Trusted Issuer Registry provide in Gaia-X ecosystems?
- **RQ2.3:** What is a suitable technical infrastructure for a Trusted Issuer Registry?
- **RQ2.4:** How can scalable governance be achieved?

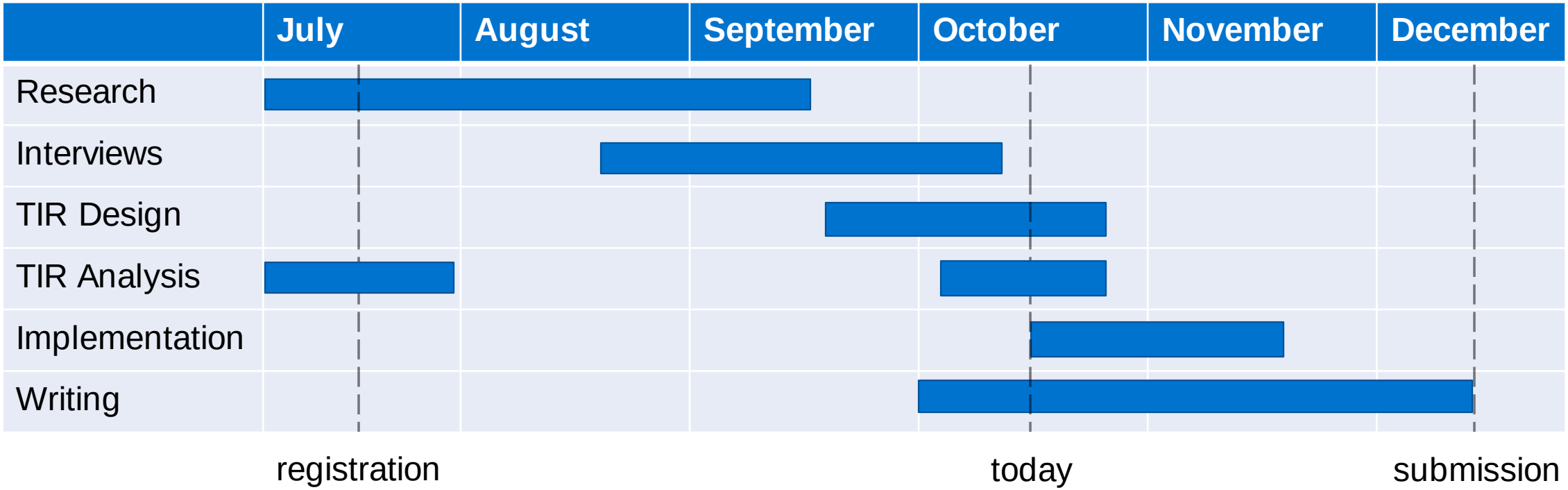
RQ3: How can the design be implemented using a concrete technology?

© sebis

Methodology



Timeline



© sebis

Michael Schmidmaier
michael.schmidmaier@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

References

- Stock photos: pexels.com
- [1] C. Allen, “The Path to Self-Sovereign Identity,” Life With Alacrity. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
- [2] “Gaia-X: A Federated Secure Data Infrastructure,” Gaia-x.eu, 2022. https://gaia-x.eu/ (accessed Oct. 13, 2023).
- [3] “Members Directory - Gaia-X: A Federated Secure Data Infrastructure,” Gaia-x.eu, 2022. https://gaia-x.eu/membership/members-directory/ (accessed Oct. 13, 2023).
- [4] M. Sabadello, M. Sporny, A. Guy, and D. Reed, “Decentralized Identifiers (DIDs) v1.0,” W3C, W3C Recommendation, Jul. 2022. [Online]. Available: https://www.w3.org/TR/2022/REC-did-core-20220719/
- [5] D. Longley, B. Zundel, K. D. Hartog, D. Burnett, G. Noble, and M. Sporny, “Verifiable Credentials Data Model v1.1,” W3C, W3C Recommendation, Mar. 2022. [Online]. Available: https://www.w3.org/TR/2022/REC-vc-data-model-20220303/
- [6] K. H. Duffy, “Issuer Registry MVP.” Accessed: Jul. 24, 2023. [Online]. Available: https://github.com/digitalcredentials/docs/blob/main/identity/issuer_registry.md
- [7] I. H. Johnson Jeyakumar, D. W. Chadwick, and M. Kubach, “A novel approach to establish trust in verifiable credential issuers in Self-sovereign identity ecosystems using TRAIN,” in *Open Identity Summit 2022*, Bonn: Gesellschaft für Informatik e.V., 2022, pp. 27–38. doi: 10.18420/OID2022_02.
- [8] “Trusted Issuers Registry API v5.” European Blockchain Services Infrastructure (EBSI). Accessed: Oct. 11, 2023. [Online]. Available: https://api-pilot.ebsi.eu/docs/apis/trusted-issuers-registry/latest
- [9] O. Steele, A. Uribe, and G. Cohen, “Verifiable credentials JSON schema specification,” W3C, W3C working draft, Oct. 2023.

© sebis