Supporting Incremental Authorization after SSI-based Authentication

Ilayda Cansin Koc

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

Motivation
- The general problem with identity management models
- How can one easily adopt SSI?
- Why the bridge?

Problem Statement
- The Status Quo
- Problems with the status quo approach
- How to mitigate problems associated with the status quo approach?

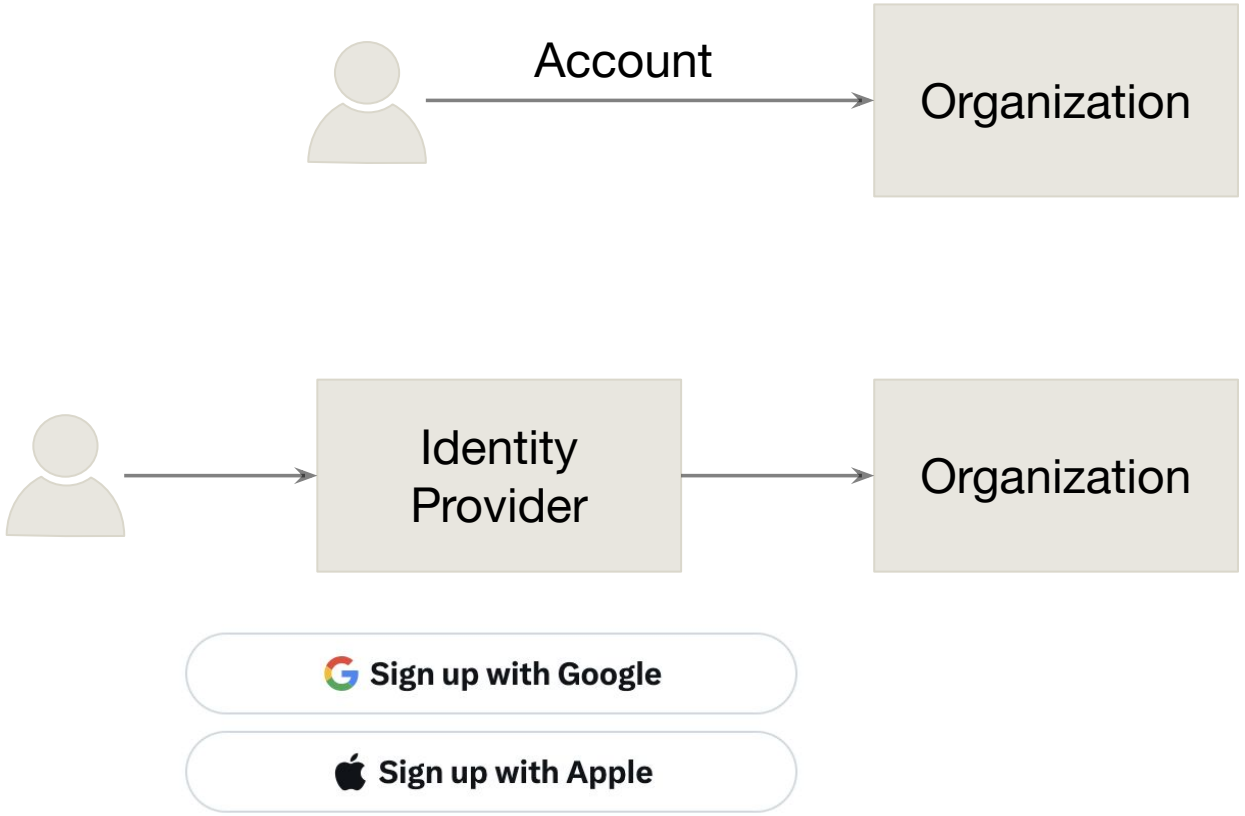
Possible Solutions
- Functional and Non-functional requirements
- Presenting a different credential
- DIDComm
- Extension to SSI-to-OIDC Bridge

Next steps
- Research Questions
- Timeline

Questions

The general problem with mostly used identity management models

- Centralized/Federated identity management is used in a big portion on the Internet.
- Attractive hacker targets
- User activity can be monitored
- Single point of failure
- Such limitations introduced the concept of SSI.



Images based on A. Preukschat, “Self-Sovereign Identity”.

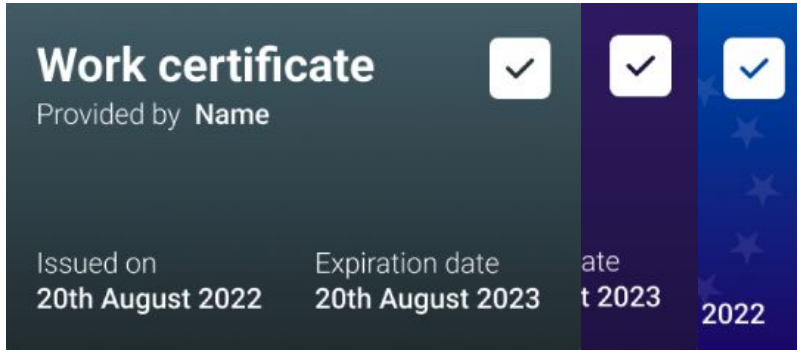
How can one easily adopt SSI?

SSI in short:

- A promising principle to decentralize and de-risk identity management.
- Use of verifiable credentials instead username, password or an account in an identity provider.

How can organizations adopt SSI?

- Requires expert knowledge, and resource to fully implement such a solution.
- There are tools that exists to make adoption easier.
  - SSI-to-OIDC bridge




```
{
   "@context": [
      "https://www.w3.org/ns/credentials/v2",
      "https://www.w3.org/ns/credentials/examples/v2",
      "https://w3id.org/security/suites/ed25519-2020/v1"
   ],
   "id": "http://university.example/credentials/3732",
   "type": [
      "VerifiableCredential",
      "ExampleDegreeCredential"
   ],
   "issuer": "https://university.example/issuers/565049",
   "validFrom": "2010-01-01T00:00:00Z",
   "credentialSubject": {
      "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
      "degree": {
        "type": "ExampleBachelorDegree",
        "name": "Bachelor of Science and Arts"
      }
   },
   "proof": {
      "type": "Ed25519Signature2020",
      "created": "2024-01-13T14:39:26Z",
      "verificationMethod": "https://university.example/issuers/565049#key,
      "proofPurpose": "assertionMethod",
      "proofValue": "
         z3FME68PHxPXLkDWY54FeE2ckhq5xicaUwPNPoPL5gubTeuWBg3Fq9wW
         ZwnTL2hVMMJfwRChKeznxfyfot5RohnvP"
   }
}
```

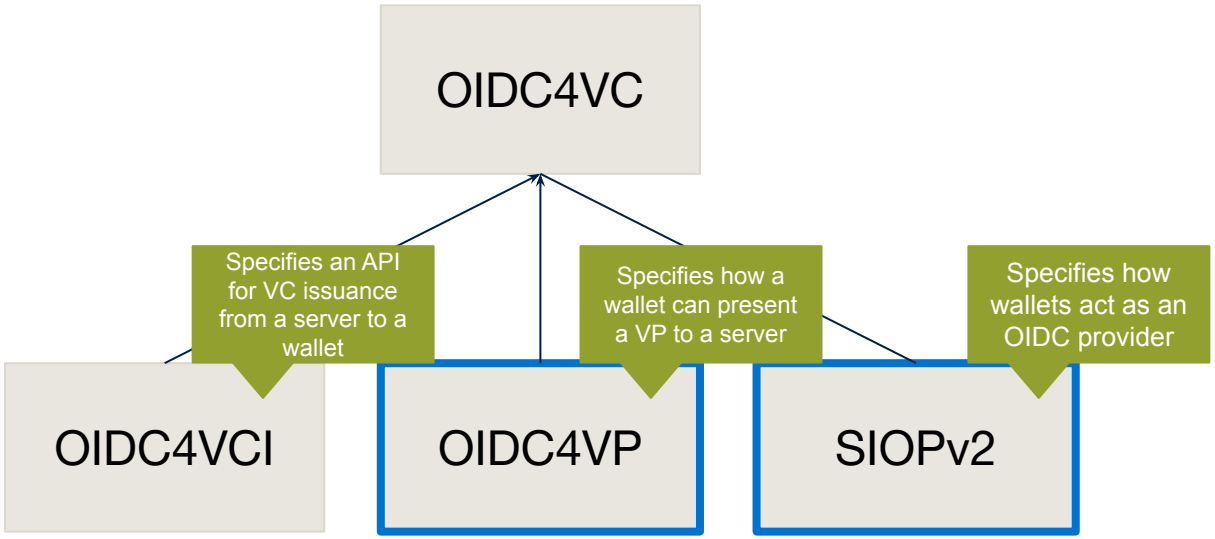

https://talao.co/sandbox/playground

Why the bridge?

- Supports SSI-based sign ins for services that support OIDC.
- Rely on OIDC4VC standards.
- Simple language to define policies to handle claims in a VC.
- **Open source, a global solution, simple to configure.**

```
[{
  "credentialID": "expected_credential_for_name",
  "patterns": [{
    "issuer": "did:example:123",
    "claims": [{
        "claimPath": "$.credentialSubject.e_mail",
        "newPath": "$.email",
        "token": "id_token"
    }]
  },
  {
    "issuer": "did:example:456",
    "claims": [{
        "claimPath": "$.credentialSubject.email",
        "token": "id_token"
    }]
  }]
}]
```

Login Policy Example



https://openid.net/sg/openid4vc/

Outline

Motivation
- The general problem with identity management models
- How can one easily adopt SSI?
- Why the bridge?

Problem Statement
- The Status Quo
- Problems with the status quo approach
- How to mitigate problems associated with the status quo approach?

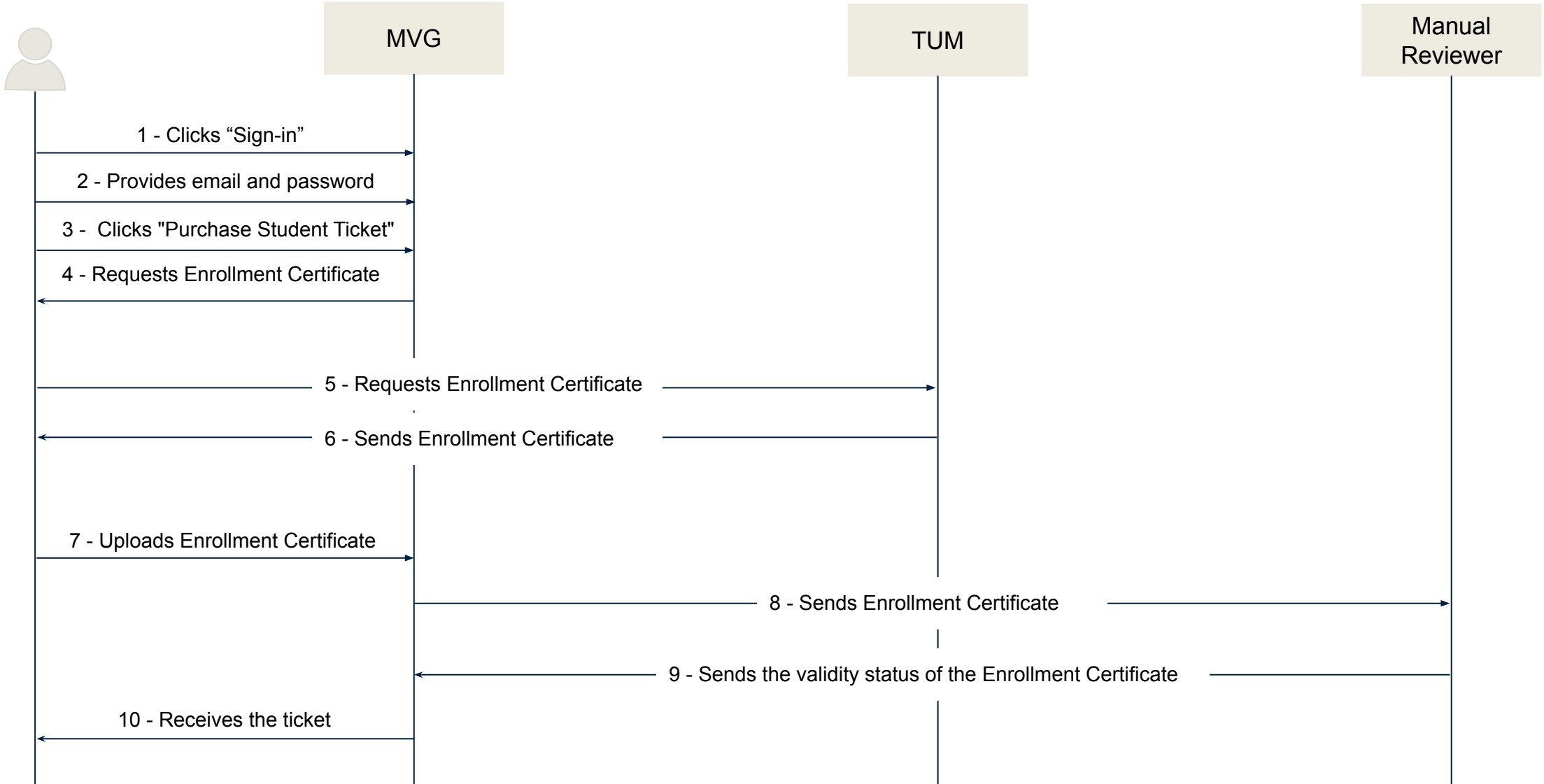
Possible Solutions
- Functional and Non-functional requirements
- Presenting a different credential
- DIDComm
- Extension to SSI-to-OIDC Bridge

Next steps
- Research Questions
- Timeline

Questions

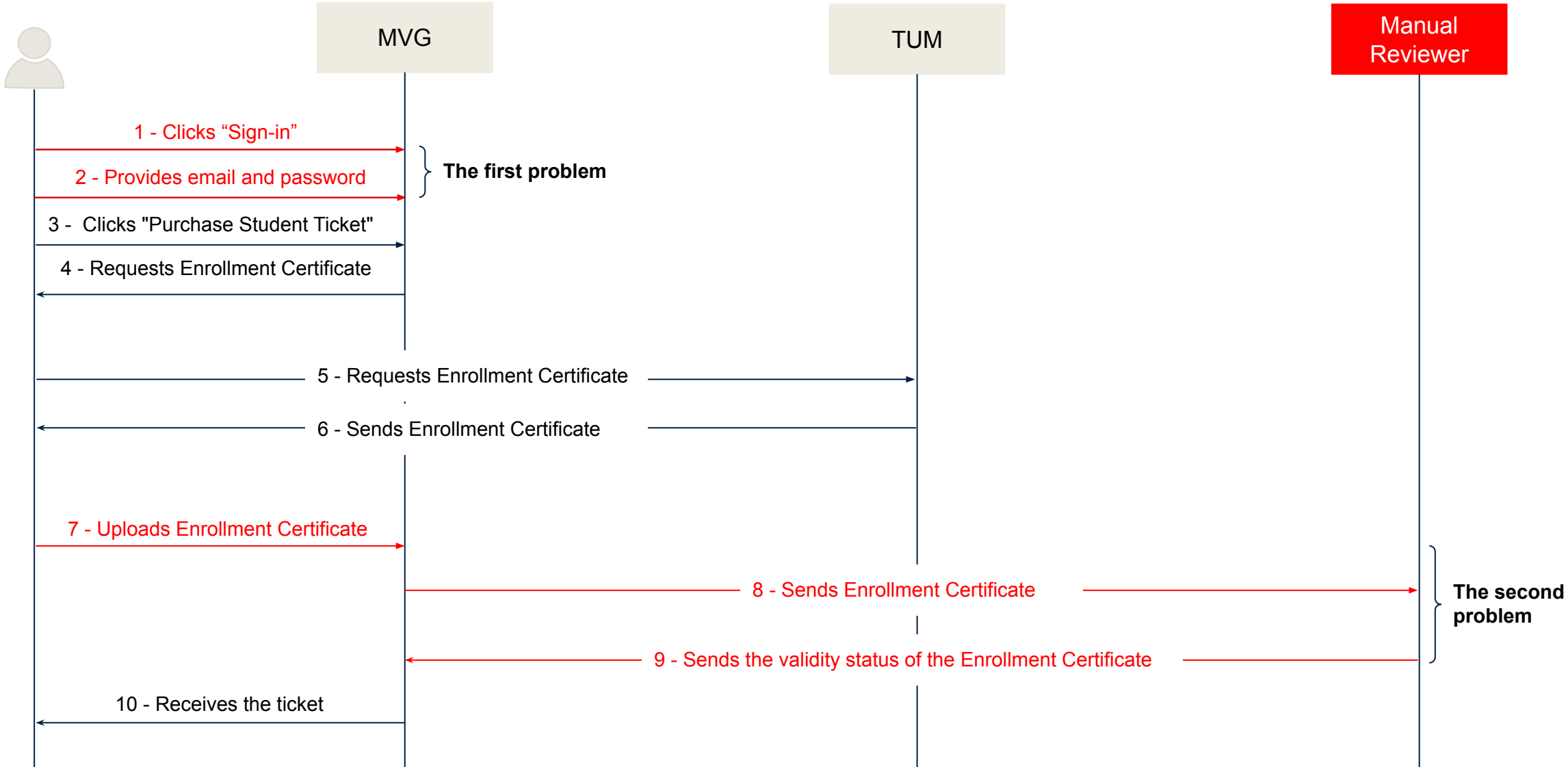
The Status Quo

- Imagine Alice, a student at TUM, wants to purchase a student ticket from MVG.



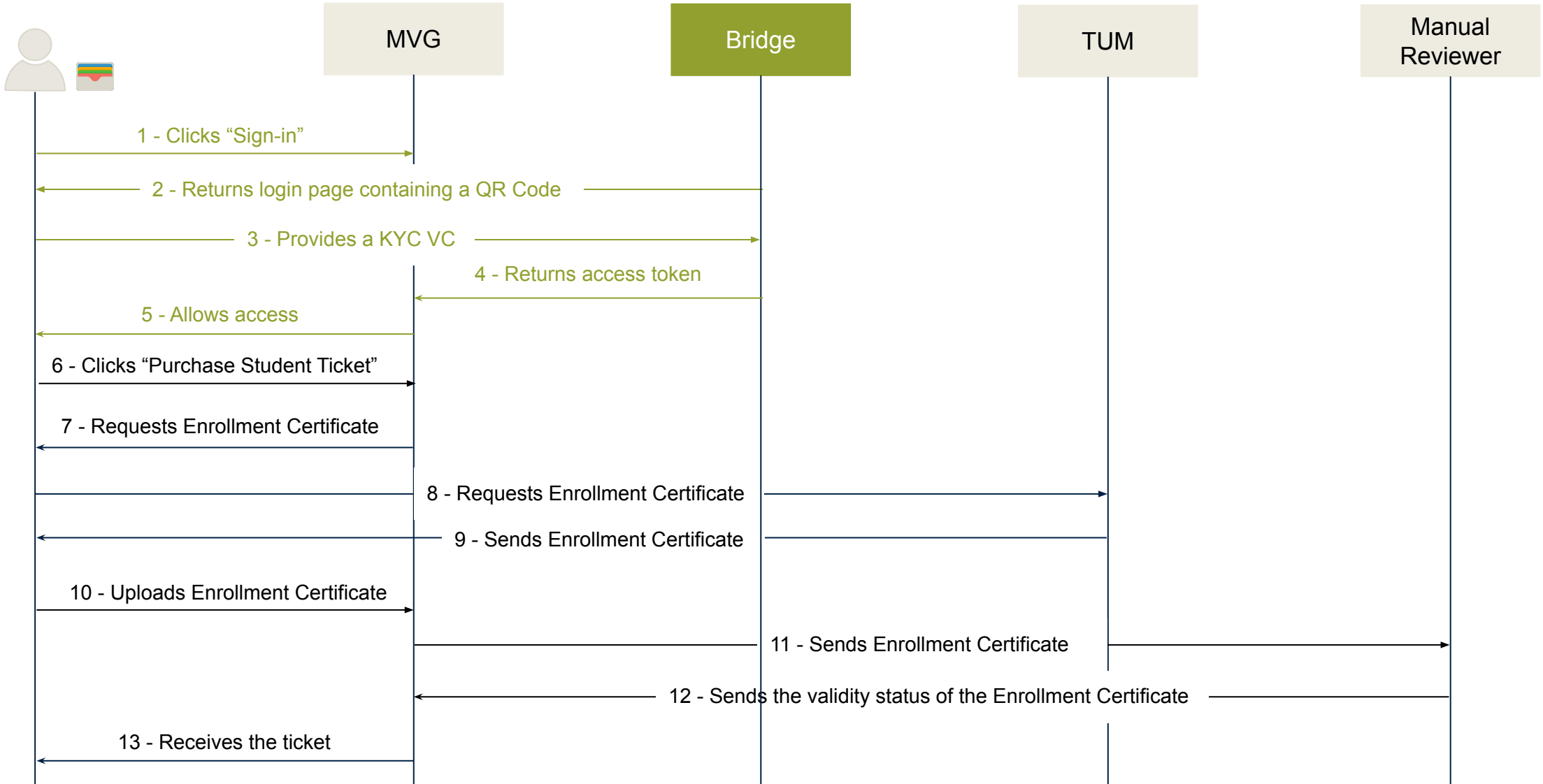
Problems with the status quo approach

- Imagine Alice, a student at TUM, wants to purchase a student ticket from MVG.



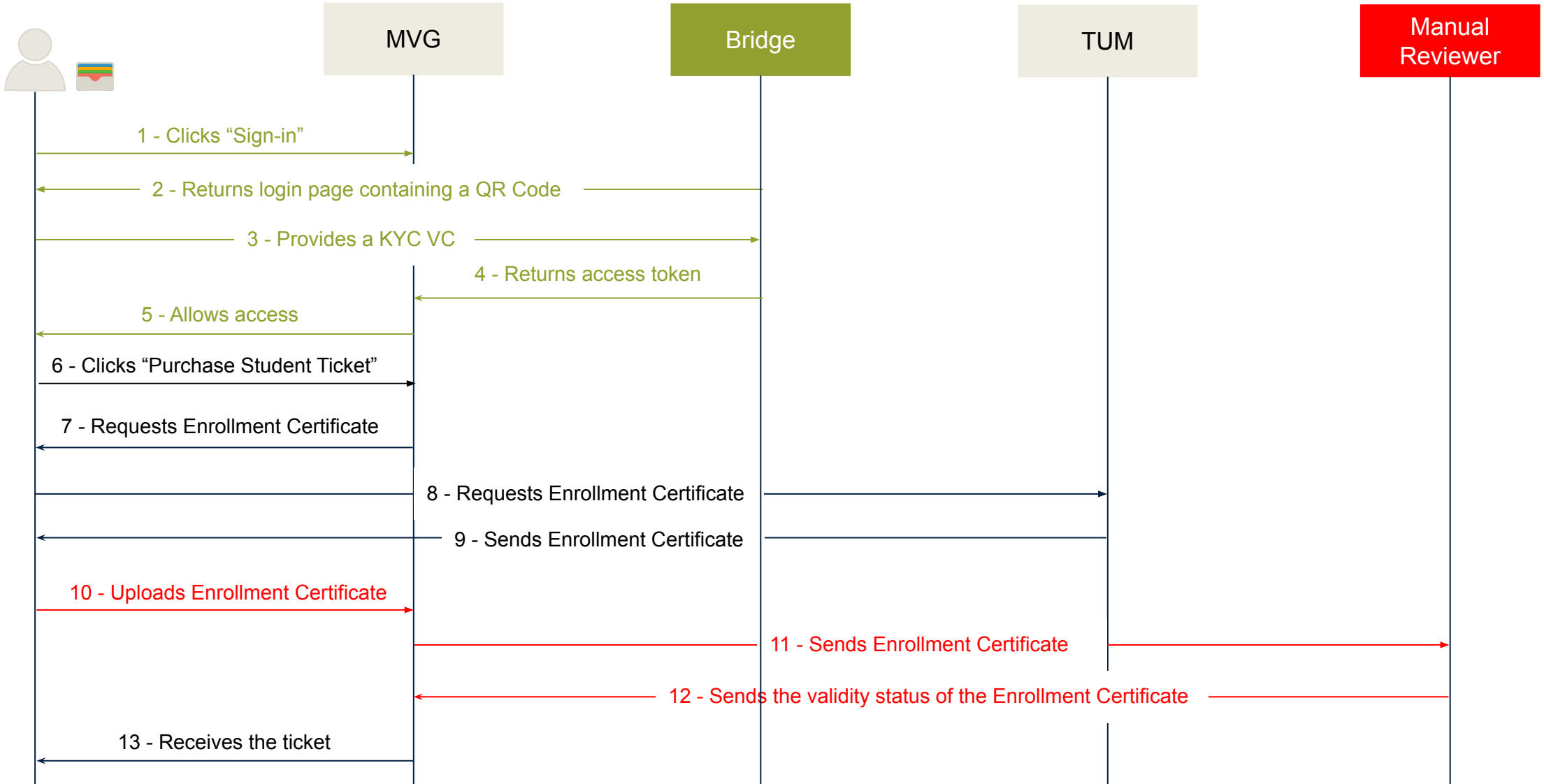
How to mitigate the first problem?

- Use the bridge.



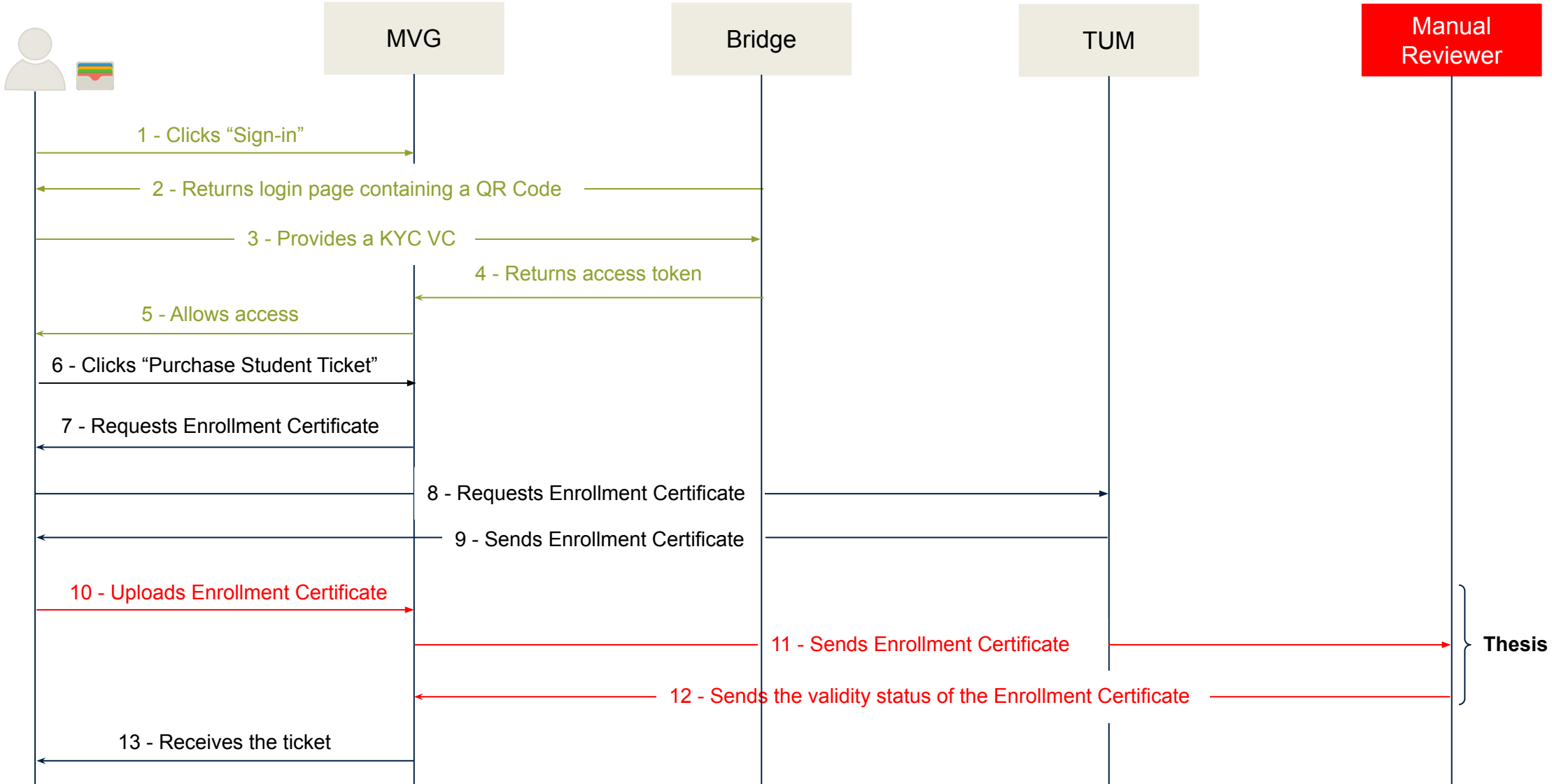
How to mitigate the first problem?

- Use the bridge.
- **The problem:** The bridge does not support anything after a login.



How do we make it fully SSI?

- Eliminate the manual reviewer.
- Ask for a digital document, VC, instead of documents like pdf.



Outline

Motivation
- The general problem with identity management models
- How can one easily adopt SSI?
- Why the bridge?

Problem Statement
- The Status Quo
- Problems with the status quo approach
- How to mitigate problems associated with the status quo approach?

Possible Solutions
- Functional and Non-functional requirements
- Presenting a different credential
- DIDComm
- Extension to SSI-to-OIDC Bridge

Next steps
- Research Questions
- Timeline

Questions

Functional and Non-functional requirements

Non-functional requirements:

- It should integrate with the bridge.
- It should not compromise SSI principles, security and privacy considerations.
- Simple to administrate (e.g. no need for additional server hosted)
- Simple user experience
- It should be interoperable.

Functional requirements:

- A service provider should be able to request additional VCs after login.

Presenting a different credential

- One possible solution is to perform login again with a different credential.

- **Login 1:**
  - Login with KYC credentials.
  - Request for an Enrollment Certificate credential to purchase a student ticket.
  - Logout.

- **Login 2:**
  - Login with Enrollment Certificate credential.
  - Purchase ticket using the information in the credential.

- This may introduce additional overhead for the verifier.
- There needs to be done a DID matching system to make sure the user data is not lost when the second login is performed.
- Bad user experience.

DIDComm

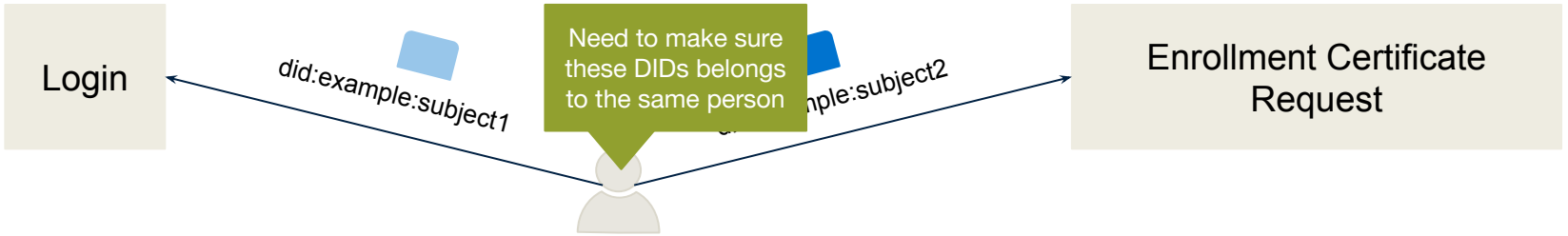
A standard that creates libraries and design patterns for two or more DID-controlling entities.

Considerations

- Search for a DIDComm protocol that enables communication between the wallet and the verifier. (WACI DIDComm - Presentation)
- Search for wallets that support DIDComm.

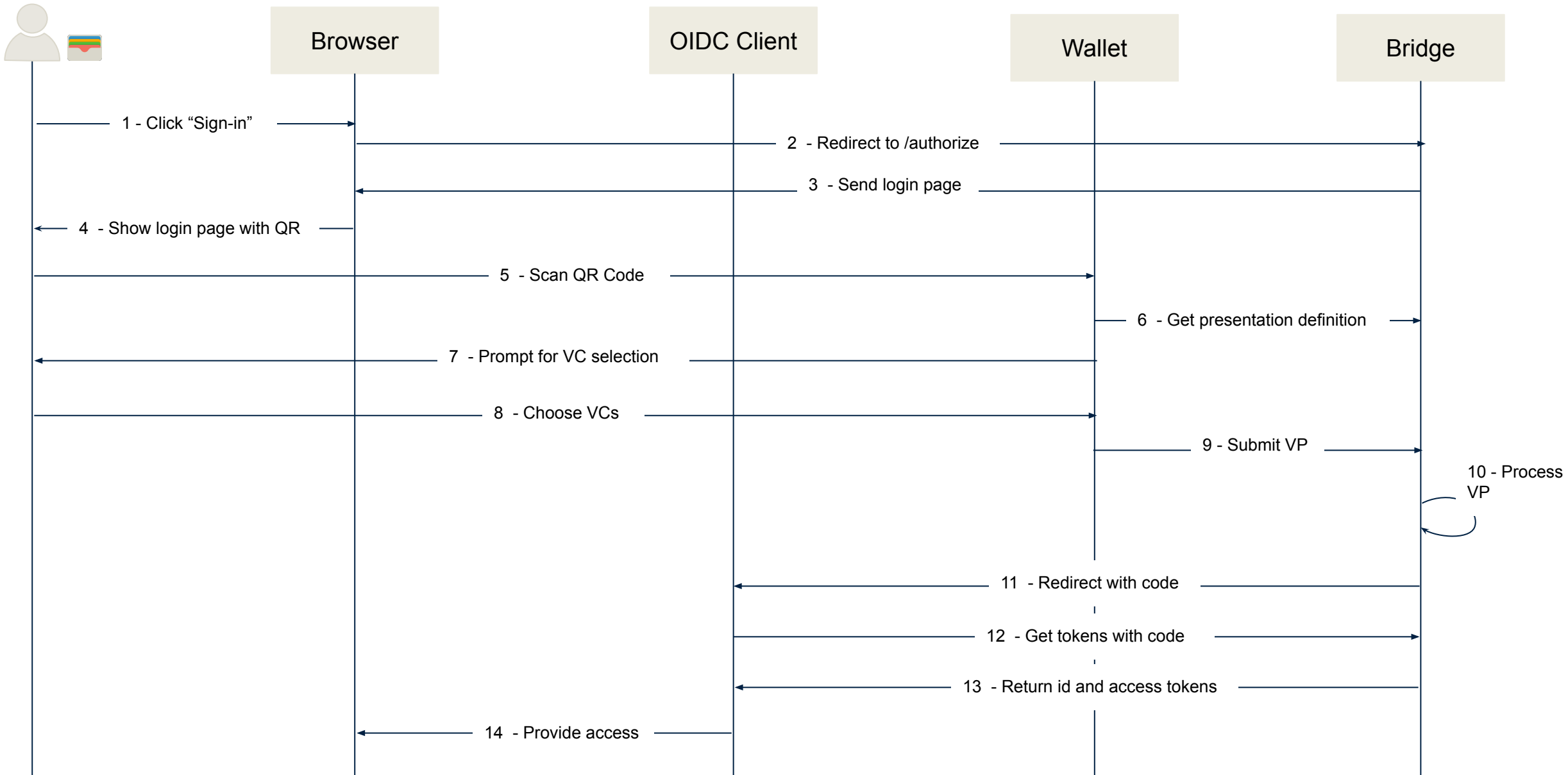
Not a good approach because

- The problem of ensuring the DIDs belong to the same person that performed the login.
- The service provider would have the responsibility to implement mechanism to check the validity of a VP.
  - e.g., DID resolution, verification of a VP, revocation status controls



Solution: Reuse the functionality in the bridge instead.

SSI-to-OIDC bridge



An Extension to the Bridge

An extension to extend functionality of the bridge.

Considerations

- A software module that can be used by any organization:
  - Must be interoperable.
- Re-use the bridge as much as possible.

A good candidate for solution to our problem.

Outline

Motivation
- The general problem with identity management models
- How can one easily adopt SSI?
- How do you get on demand data?

Problem Statement
- A Status Quo Approach
- Bridge Integration & Current Limitations

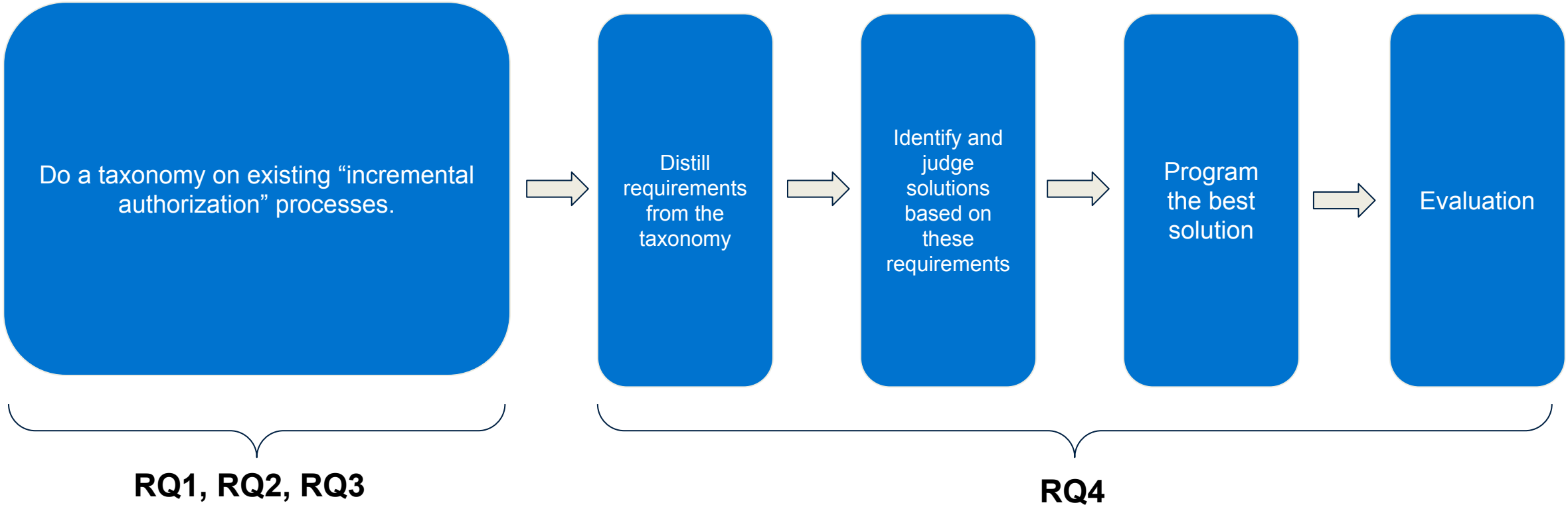
Possible Solutions
- Presenting a different credential
- DIDComm
- Extension to SSI-to-OIDC Bridge

Next steps
- Research Questions
- Timeline

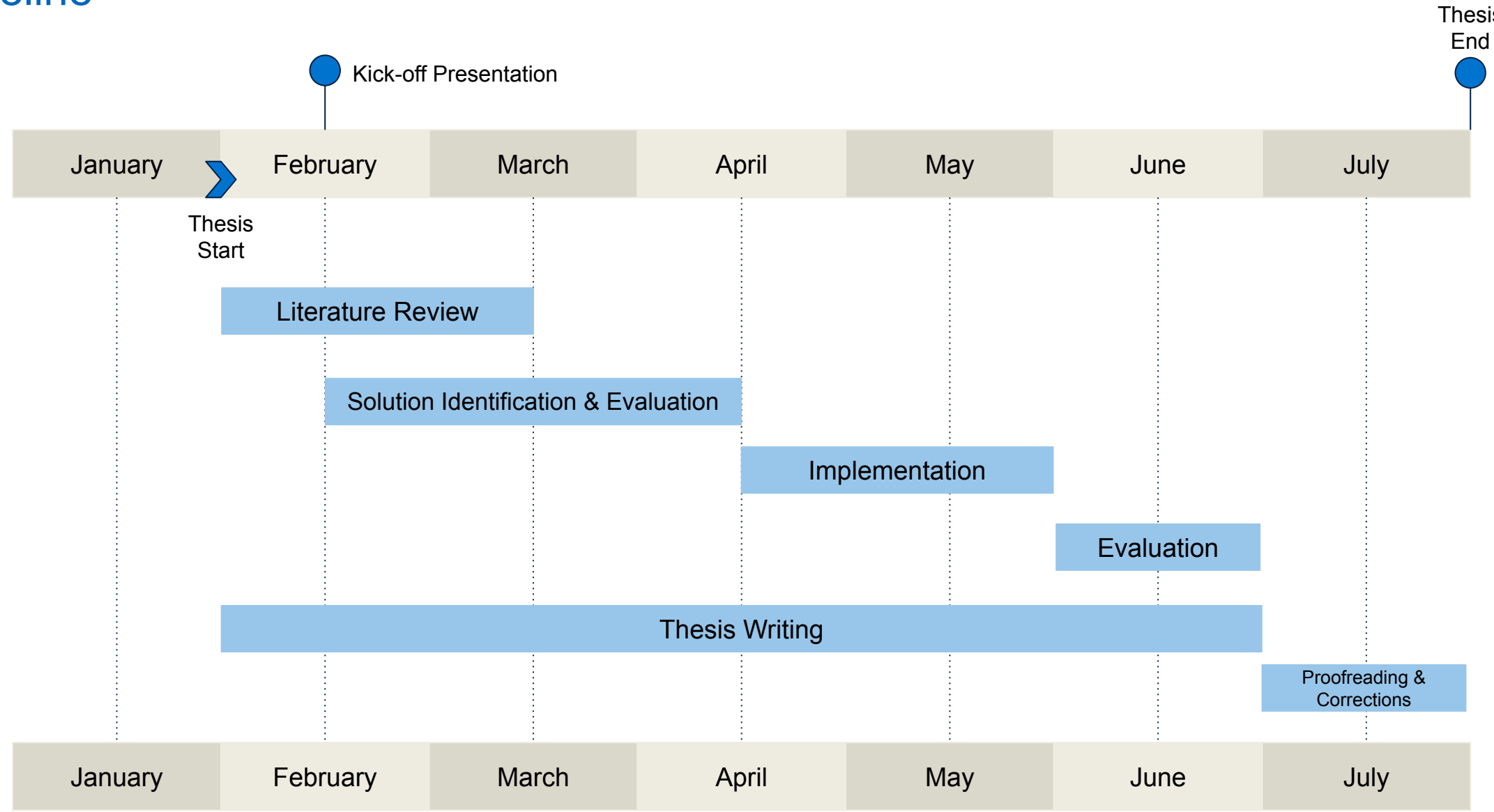
Questions

Research Questions

1. What are established ways of requesting and receiving incremental authorization data from users?
2. Which stakeholders are involved in an on-demand authorization?
3. What aspects can be used to characterize an on-demand authorization procedure?
4. How can incremental authorization work on top of an OIDC sign-in that uses Verifiable Credentials as its ground truth?



Timeline


Thesis End
Kick-off Presentation
January
February
March
April
May
June
July
Thesis Start
Literature Review
Solution Identification & Evaluation
Implementation
Evaluation
Thesis Writing
Proofreading & Corrections
January
February
March
April
May
June
July

Thank you for listening

Ilayda Cansin Koc

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

+49.89.289. 17132
matthes@in.tum.de
wwwmatthes.in.tum.de