Supporting Incremental Authorization after SSI-based Authentication

Ilayda Cansin Koc

Master Thesis Final 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

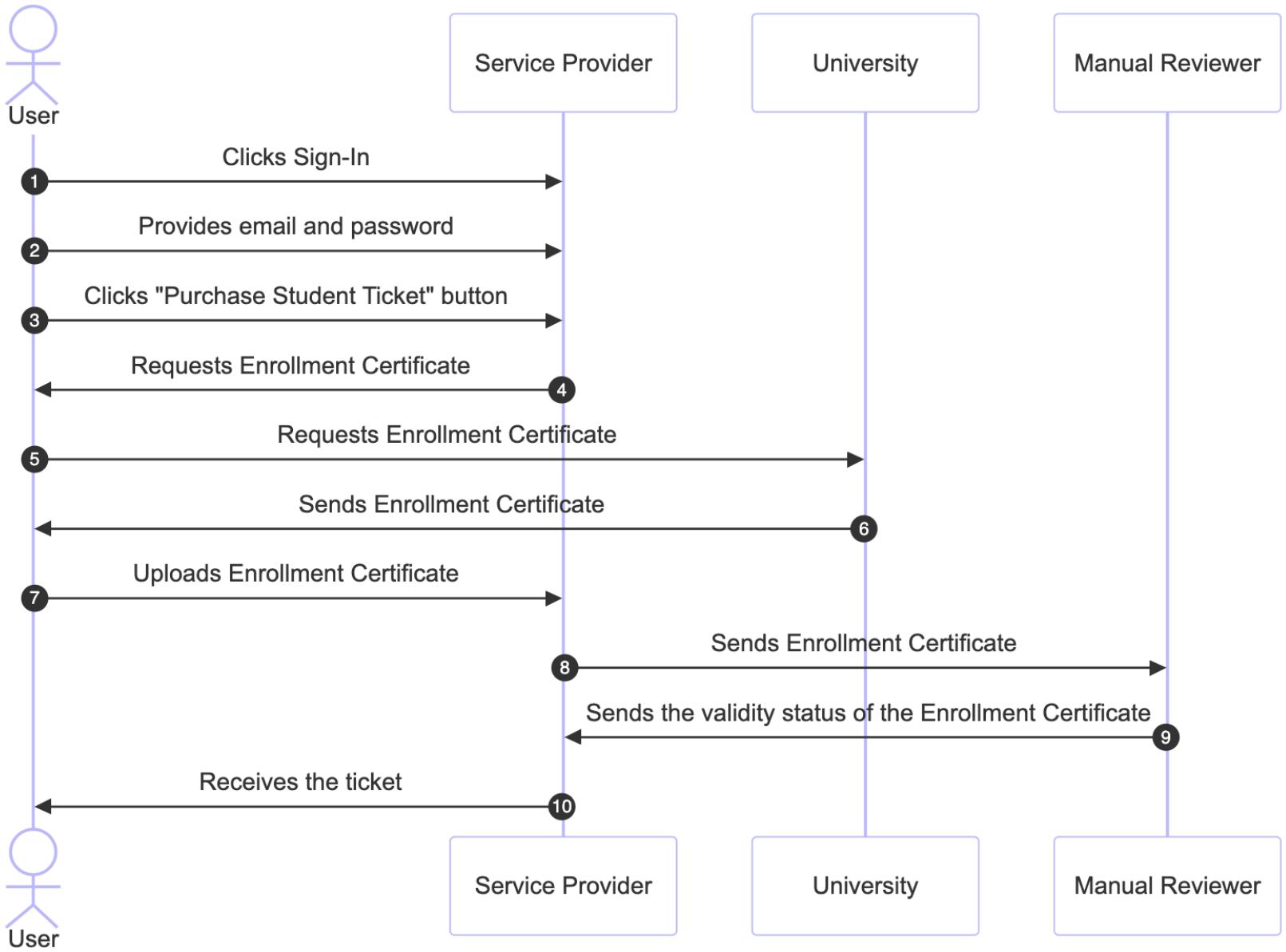
Motivation & Problem Statement
- The Status Quo
- Self-Sovereign Identity
- SSI-to-OIDC Bridge

Research Questions and Results
- Requirements Engineering
- Implementation

Live Demo

Evaluation & Future Work
- Attack Tree Analysis
- Usability Tests
- Future Work

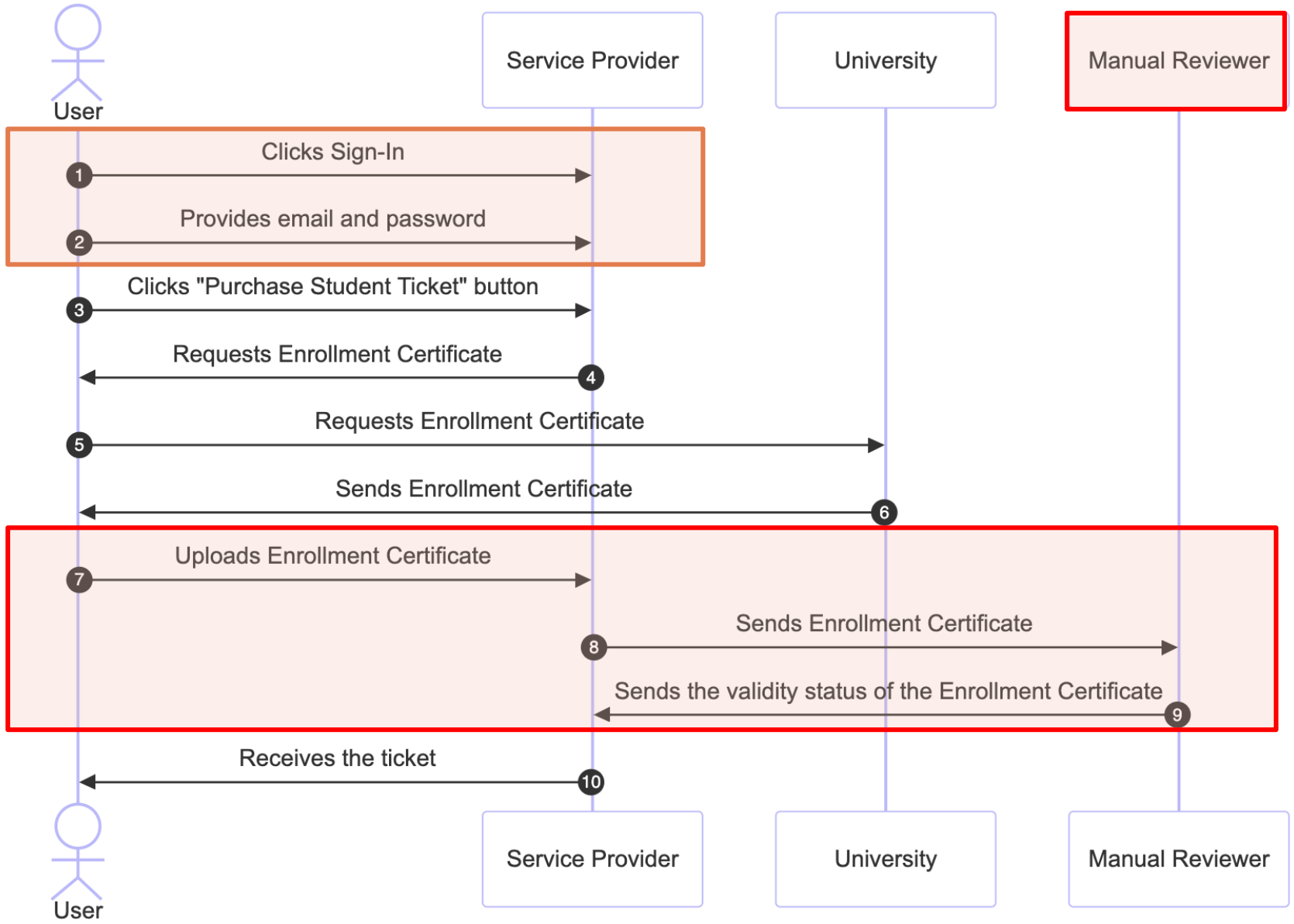
The Status Quo



Problems with The Status Quo

The first problem

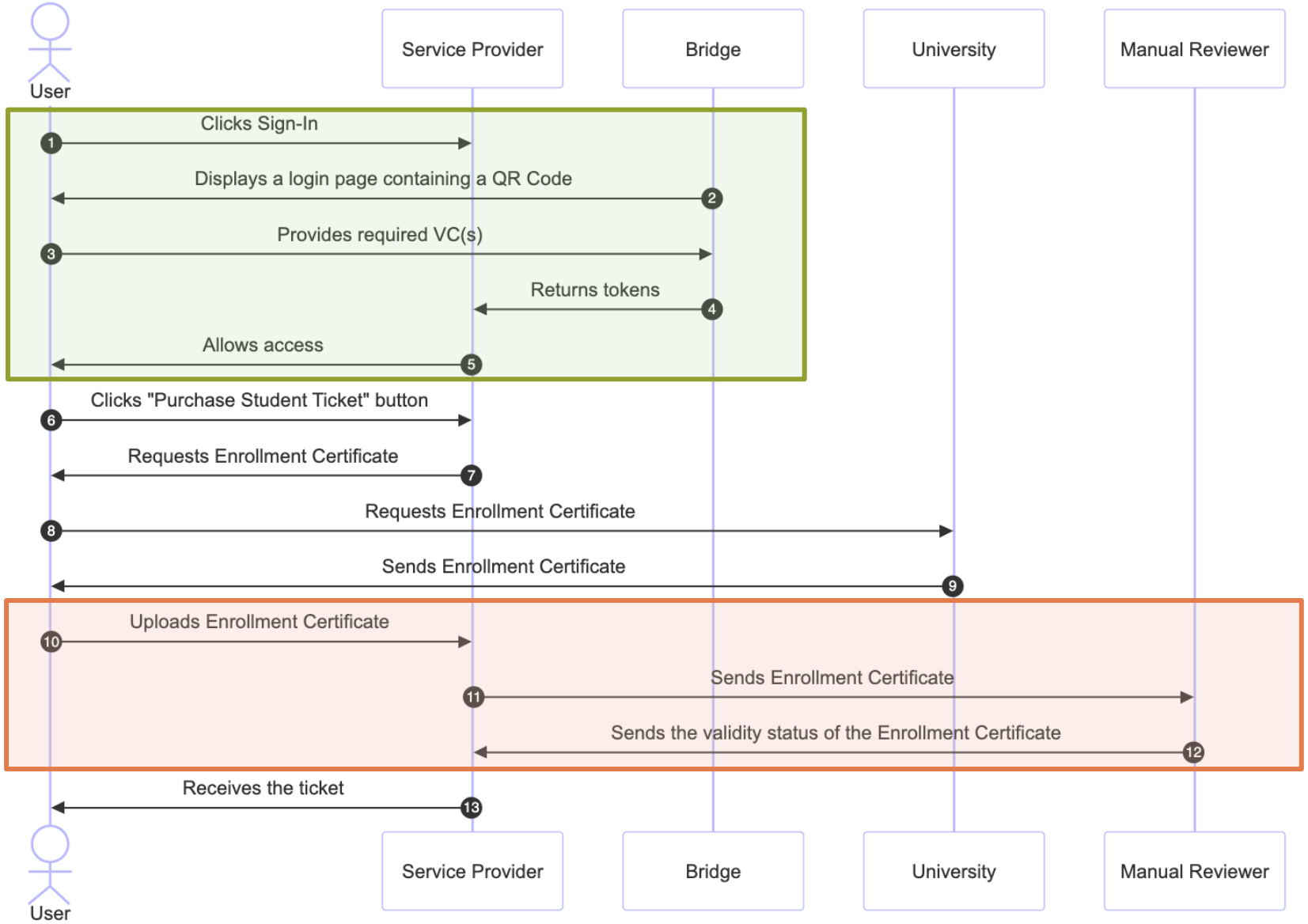
The second problem



How do we make it fully SSI?

Solved by SSI-to-OIDC bridge

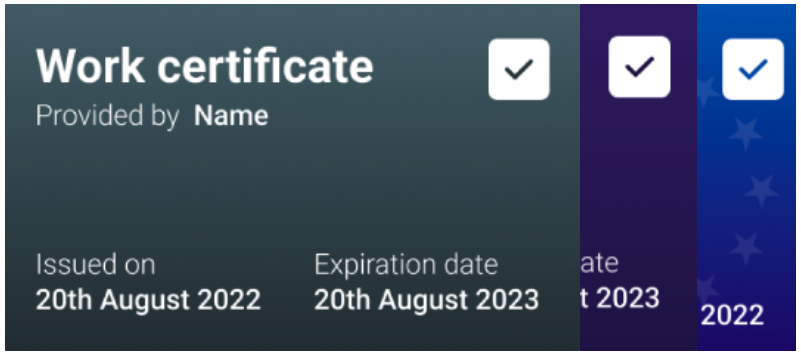
Thesis



Self-Sovereign Identity

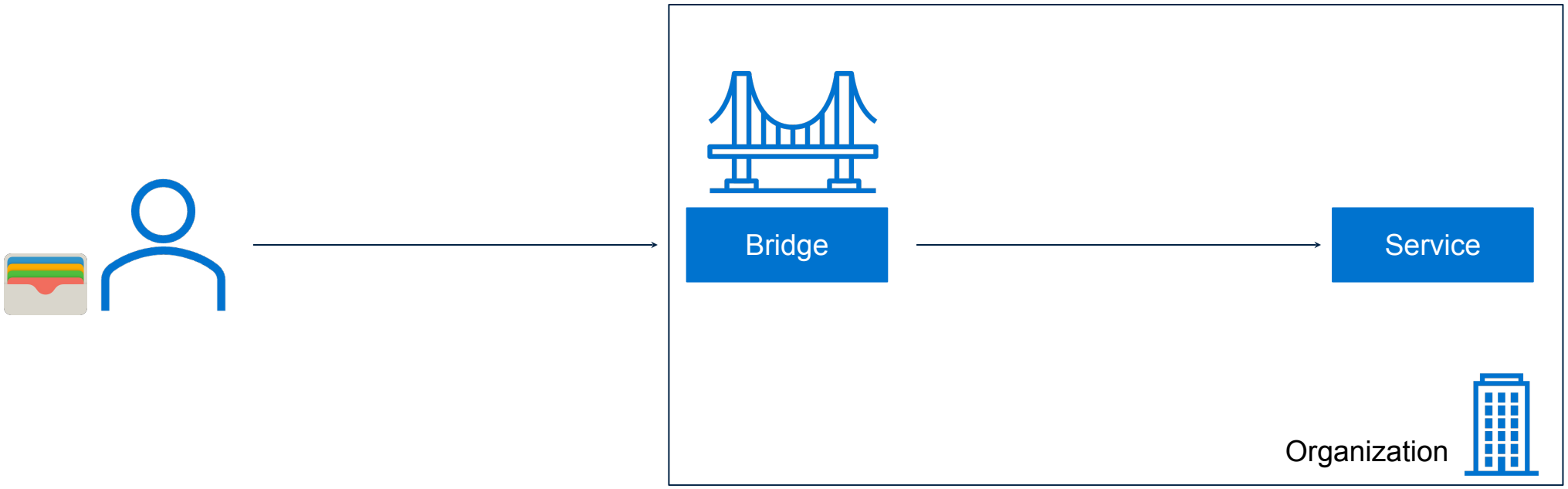
- A promising principle to decentralize and de-risk the identity management.
- Use of Verifiable Credentials (VCs) as a representation of the same information that a physical credential represents.


```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "id": "http://example.com/credentials/4643",
  "type": [
    "VerifiableCredential"
  ],
  "issuer": "https://example.com/issuers/14",
  "issuanceDate": "2018-02-24T05:28:04Z",
  "credentialSubject": {
    "id": "did:example:abcdef1234567",
    "name": "Jane Doe",
    "email": "jane.doe@gmail.com"
  },
  "proof": {
    "type": "Ed25519Signature2020",
    "created": "2022-02-25T14:58:43Z",
    "verificationMethod": "https://example.edu/issuers/14#keys-1",
    "proofPurpose": "assertionMethod",
    "proofValue": "zyrpmzxPy2fDzqv9Pgr4XBzX2rys1FDuLNkYRVmhXuyype8fB44qNX
  }
}
```

SSI-to-OIDC Bridge

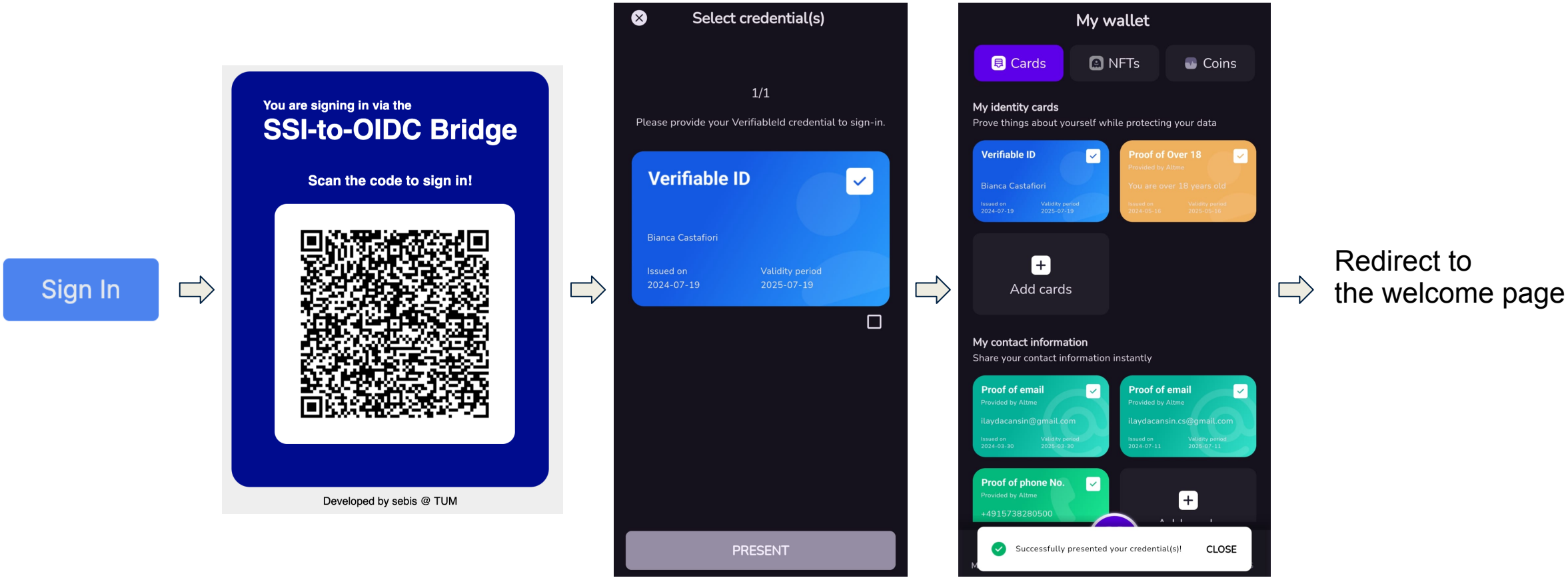
- Adoption of SSI requires expert knowledge, and resource to fully implement such a solution.
- SSI-to-OIDC Bridge fills in this gap by providing a universal solution as an OIDC provider.



https://github.com/GAIA-X4PLC-AAD/ssi-to-oidc-bridge

How can organizations adopt SSI?

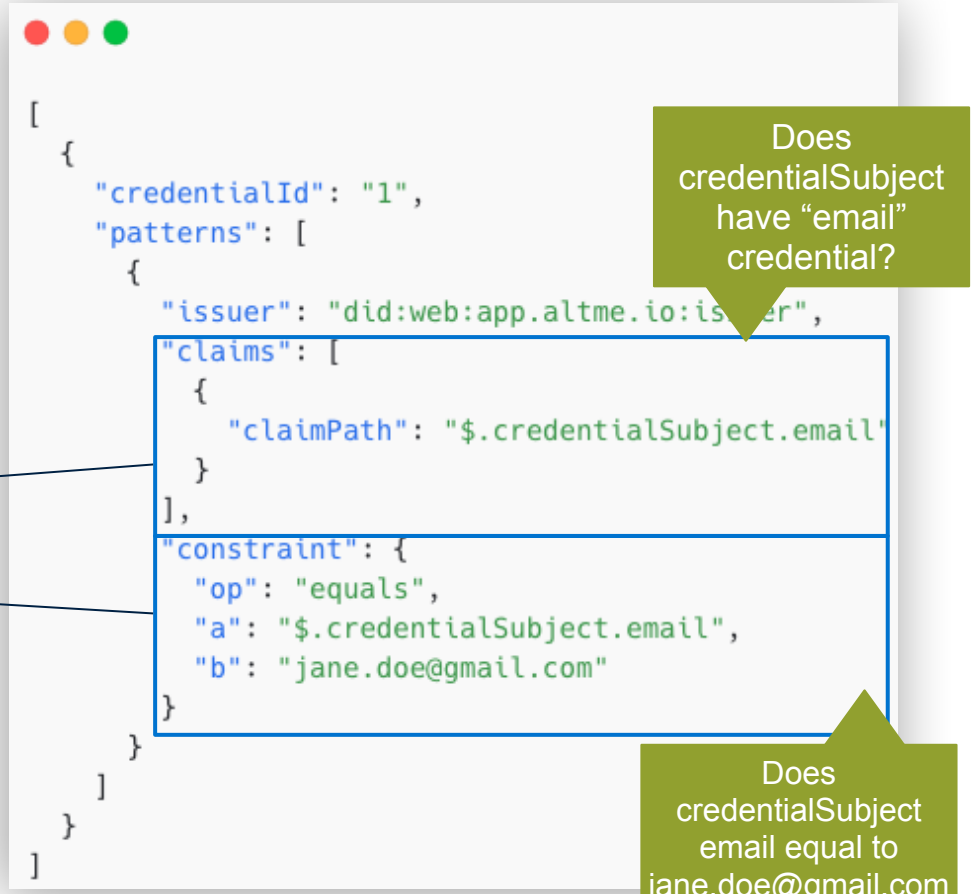
- SSI-to-OIDC bridge as an identity provider in an organization.
- Users authenticate through the bridge to access a specific service of the organization.



SSI-to-OIDC Bridge

- To authenticate and authorize users, the bridge uses policy files.
- These file is used to determine which claims to expect and from which issuer.

Submitted VC



Policy file

SSI-to-OIDC Bridge

The VC with type “VerifiableId” must contain “firstName” claim

The VC with type “EnrollmentCertificate” must contain “email” claim

These both VCs should have the same credentialSubject.id

```
[
  {
    credentialId: "1",
    type: "VerifiableId",
    patterns: [
      {
        issuer: "did:web:app.altme.io:issuer",
        claims: [
          {
            claimPath: "$.credentialSubject.firstName",
          },
        ],
      },
    ],
  },
  {
    credentialId: "2",
    type: "EnrollmentCertificate",
    patterns: [
      {
        issuer: "did:key:z6MkuY5iCnPkoNw4KSxvc8ae9krvaNECGYUSoCGXaJmc32tD",
        claims: [
          {
            claimPath: "$.credentialSubject.email",
          },
        ],
        constraint: {
          op: "equals",
          a: "$2.credentialSubject.id",
          b: "$1.credentialSubject.id",
        },
      },
    ],
  },
];
```

Quick Recap

- We want to solve the problem associated with the incremental authorization processes.
- To do that, we want to improve the SSI-to-OIDC bridge.

Outline

Motivation & Problem Statement
- The Status Quo
- Self-Sovereign Identity
- SSI-to-OIDC Bridge

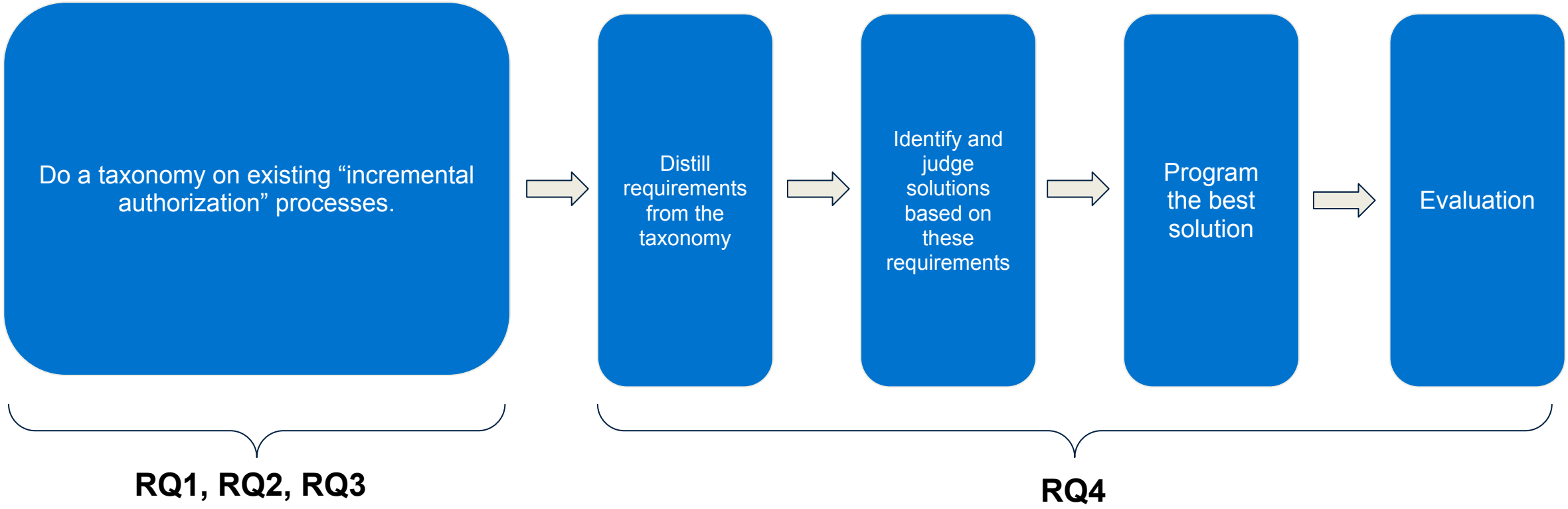
Research Questions and Results
- Requirements Engineering
- Implementation

Live Demo

Evaluation & Future Work
- Attack Tree Analysis
- Usability Tests
- Future Work

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 incremental authorization procedure?
4. How can incremental authorization work on top of an OIDC sign-in that uses Verifiable Credentials as its ground truth?



Requirements Engineering

Non-functional Requirements

1. An intuitive user interface for easy and quick user interaction.
2. Compatible with universal SSI wallets.
3. Allow cross-device flow, enabling interaction through various devices.
4. Should respond under a minute for authorization requests.

Functional Requirements

1. Support incremental authorization processes uses universally issued attestations.
2. Function regardless of any service-mandated update frequency.
3. Return a QR Code string to start credential exchange flow.
4. Return extracted claims and authorization response to the service.

Implementation

- Two implementation examples:
  - Dynamic Bridge Endpoint (DBE) Approach
  - OIDC Scopes (OIDS) Approach
- Focus on **re-using the bridge** as much as possible.

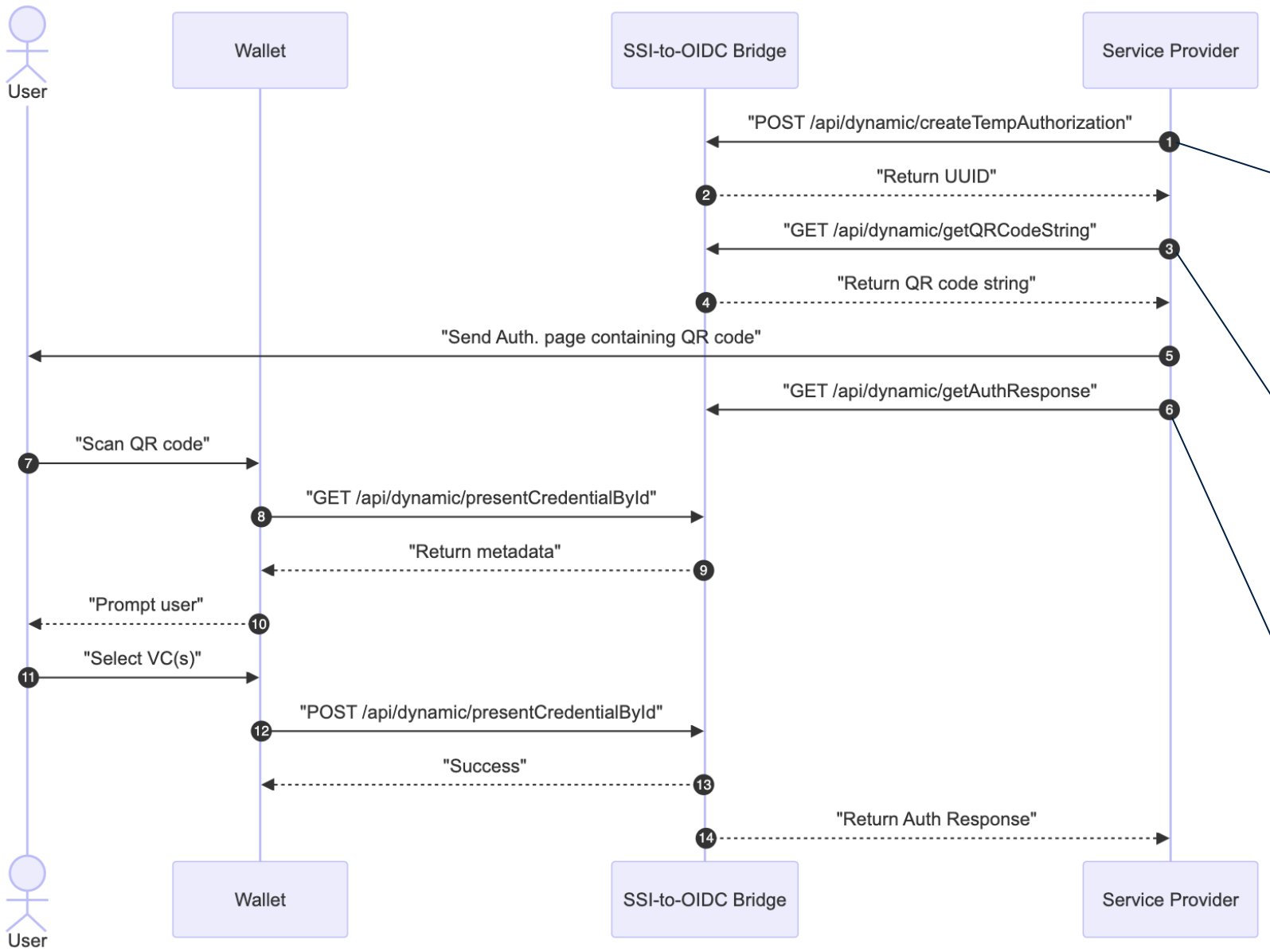
DBE Approach

- Set of endpoints introduced to enable credential exchange flow on demand.
- Specify authorization policy in these requests.

OIDS Approach

- Predefined set of policies on the bridge.
- Indicate with the scope value which policy you want to apply.

DBE Approach



Endpoint to define which authorization policy will be used for the incremental authorization.

"I want to perform an authorization using this policy file"

Endpoint to retrieve QR code string to render in the service provider's frontend.

"I need a QR code string to start credential exchange flow"

Endpoint to retrieve authorization status and claims in the credentials.

"I need to know if authorization is successful or not, and the claims returned"

Outline

Motivation & Problem Statement

- The Status Quo
- Self-Sovereign Identity
- SSI-to-OIDC Bridge

Research Questions and Results

- Requirements Engineering
- Implementation

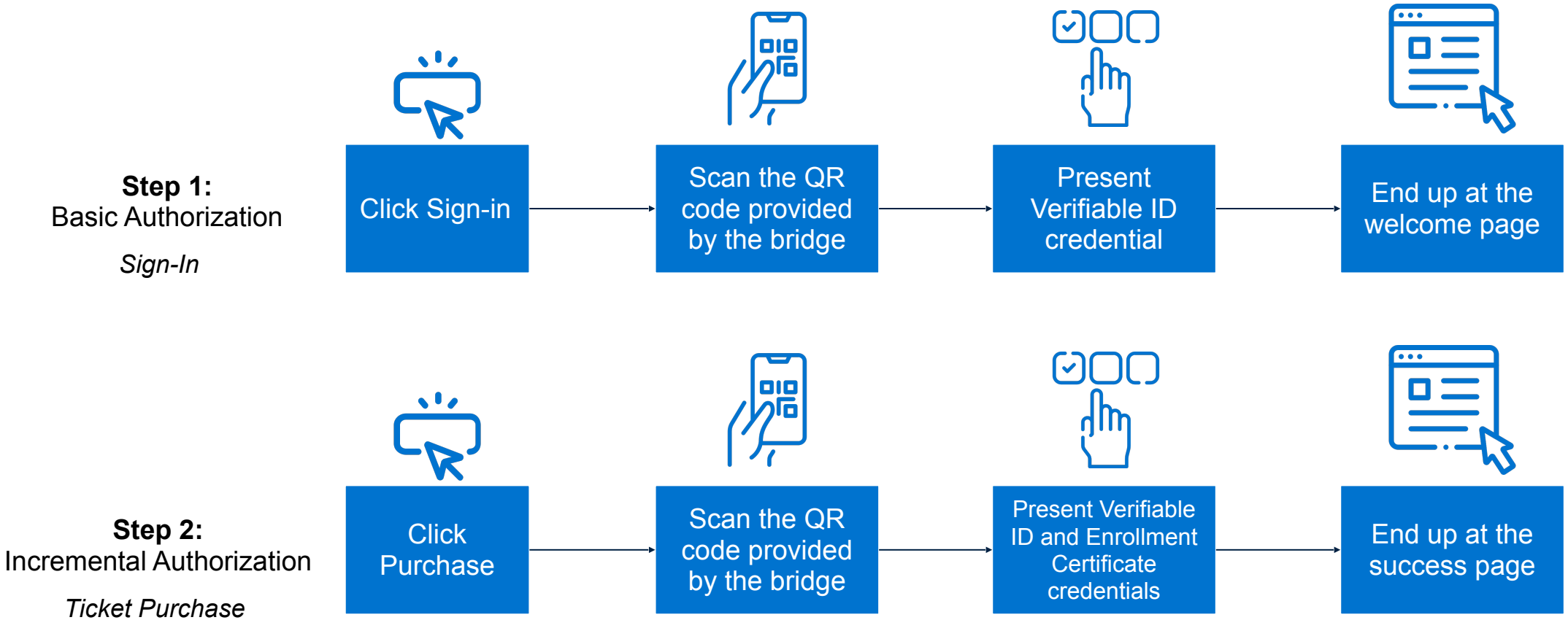
Live Demo

Evaluation & Future Work

- Attack Tree Analysis
- Usability Tests
- Future Work

Live Demo

- Student Ticket Purchase scenario
- Mock Ticket Provider Application as service provider



Outline

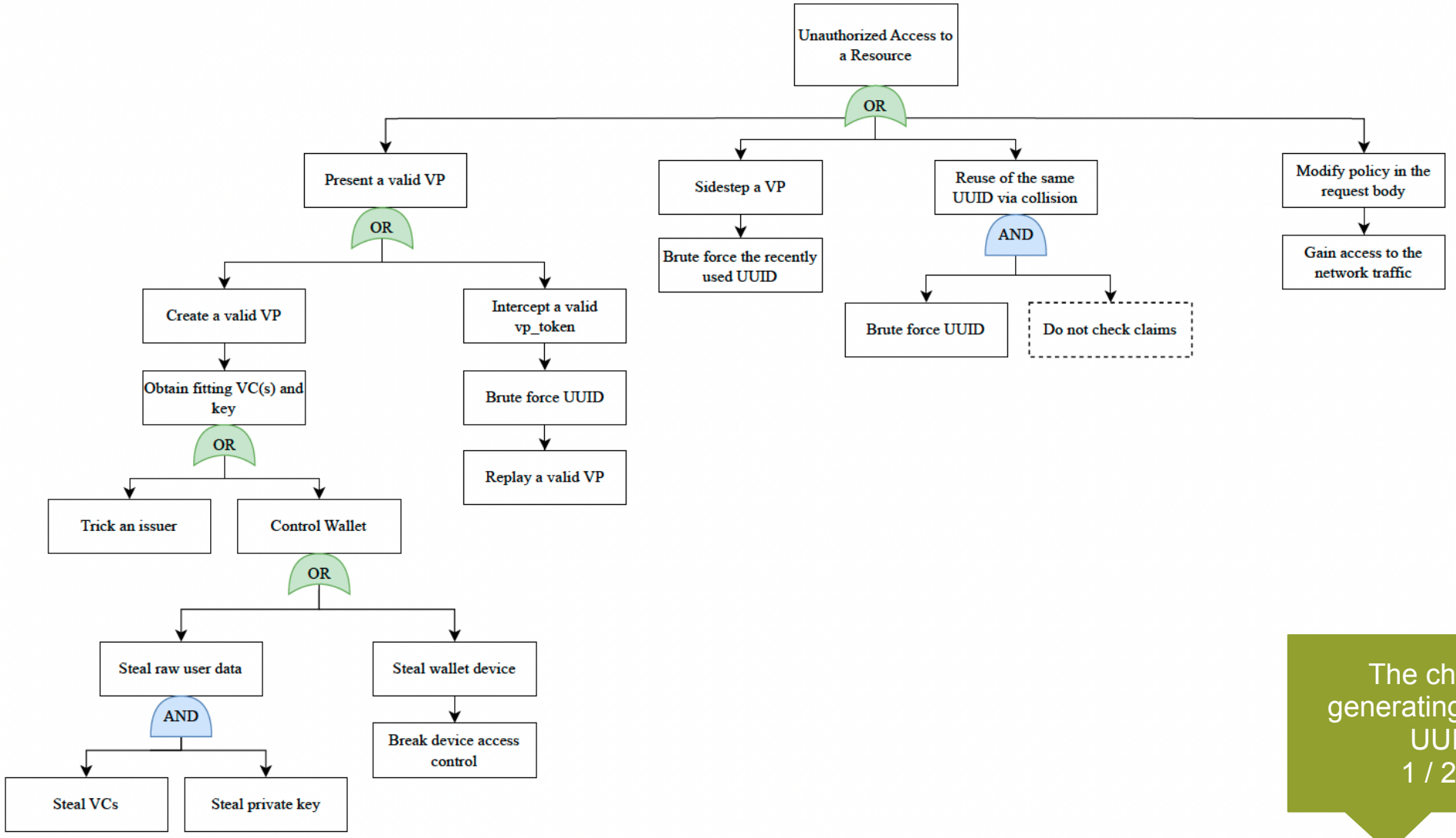
Motivation & Problem Statement
- The Status Quo
- Self-Sovereign Identity
- SSI-to-OIDC Bridge

Research Questions and Results
- Requirements Engineering
- Implementation

Live Demo

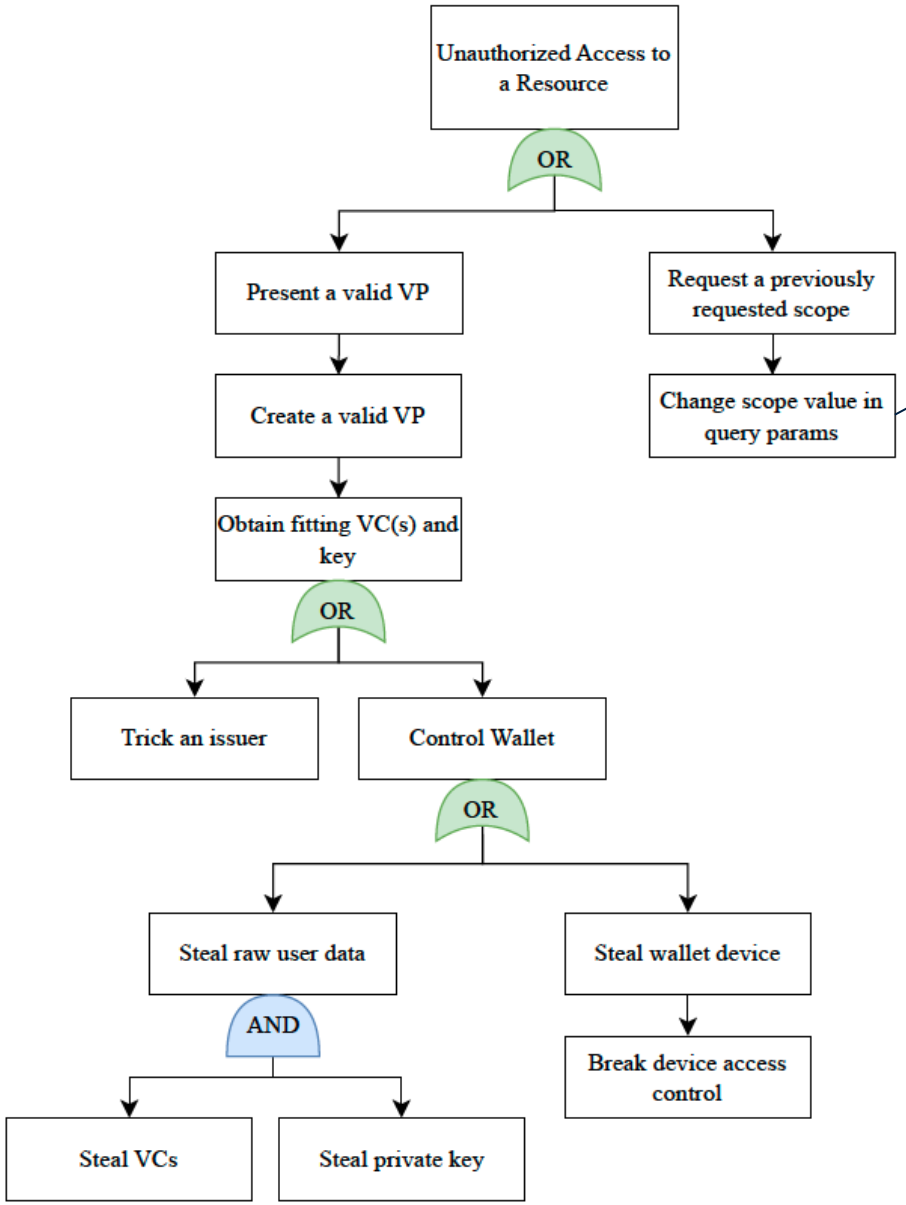
Evaluation & Future Work
- Attack Tree Analysis
- Usability Tests
- Future Work

Evaluation - DBE Attack Tree Analysis



The chance of generating a specific UUID is
1 / 2^128

Evaluation - OIDS - Attack Tree Analysis



An incremental authorization request

https://www.example.com/auth/authorize?
client_id=<client_id>....
&**scope=openid%20student**

Mandatory scope value to perform basic authentication

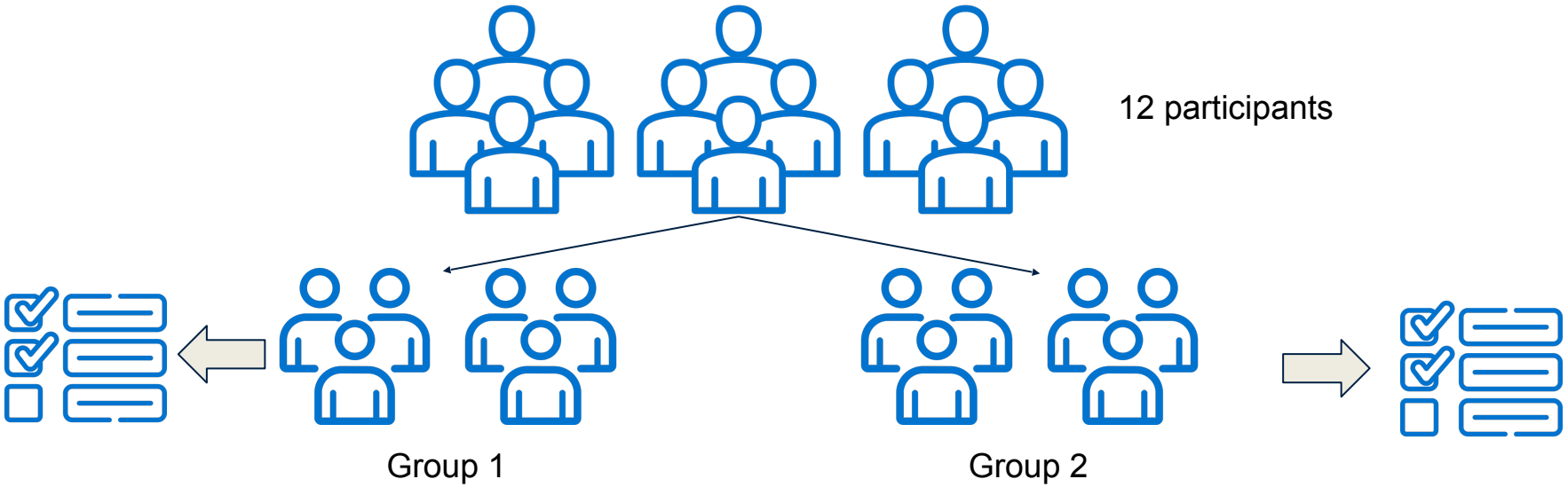
Scope value that represents an incremental auth policy to be applied

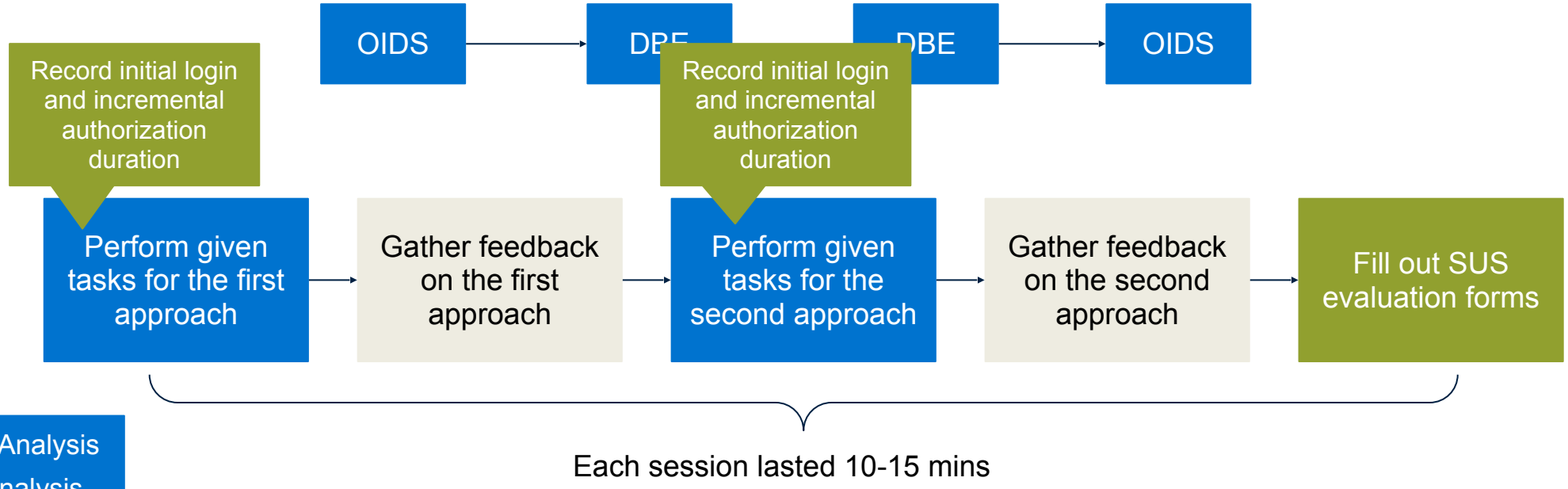
Manually edit the scope values

https://www.example.com/auth/authorize?
client_id=<client_id>....
&**scope=openid**

Unauthorized Access

Evaluation - Usability Analysis





Evaluation - Usability Analysis Quantitative Results

For Group 1

An improvement by 2.59 seconds

For Group 2

A deterioration by 0.58 seconds.

Interviewee ID	Incr. Auth (OIDS)	Incr. Auth (DBE)
g1p1	30.516	27.073
g1p2	20.383	17.72
g1p3	22.572	23.913
g1p4	25.249	19.079
g1p5	24.149	23.979
g1p6	27.324	22.929
g2p1	16.536	25.513
g2p2	23.471	16.98
g2p3	23.932	27.485
g2p4	27.289	22.143
g2p5	23.93	23.073
g2p6	27.737	22.608

Incremental Authorization duration in seconds

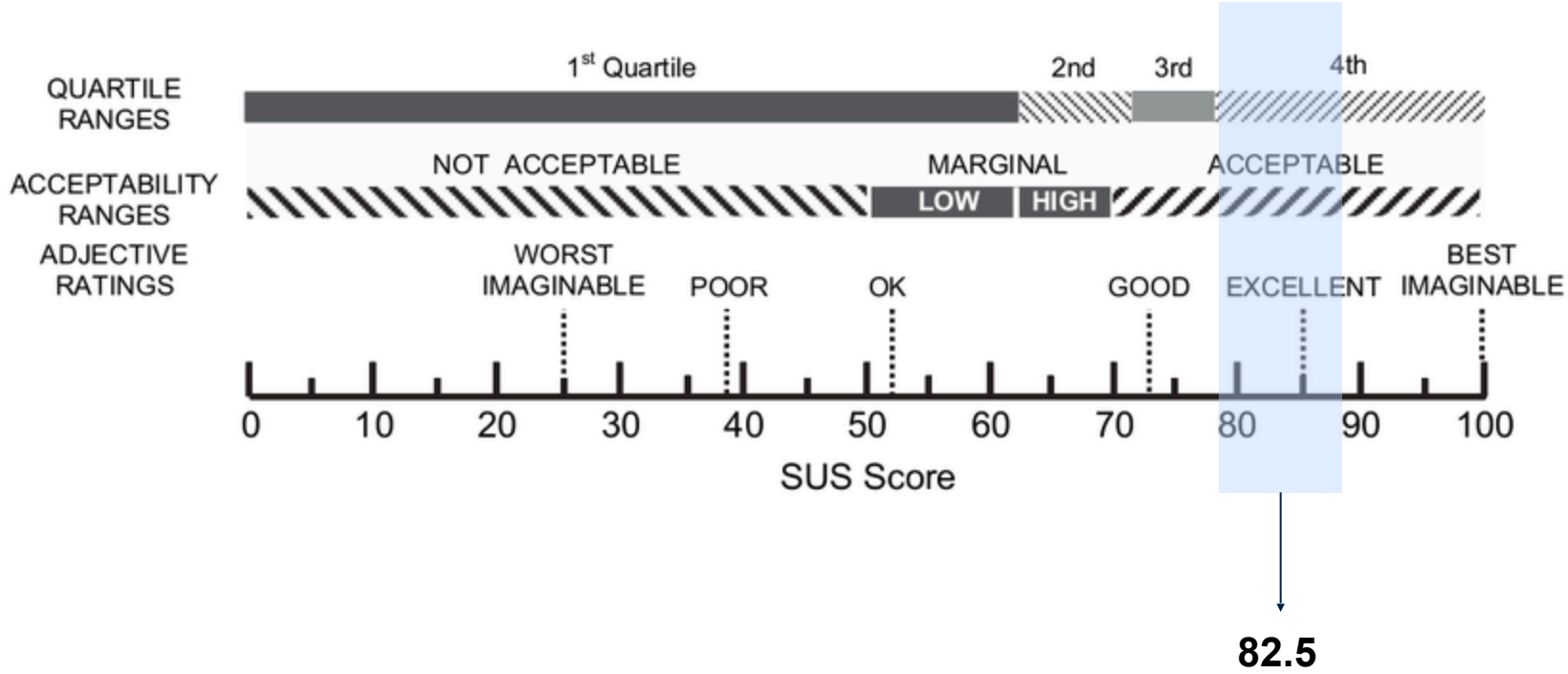
Group 1
OIDS - DBE

Group 2
DBE - OIDS

Interview Group	Incr. Auth (OIDS)	Incr. Auth (DBE)
Group 1	25.03	22.44
Group 2	23.81	22.96

Avg. Incremental Authorization duration in seconds

Evaluation - Usability Analysis Quantitative Results



Evaluation - Usability Analysis Qualitative Results

Overall Experience

"I don't need to get out my phone and scan; I can do everything on one screen, and for me, it goes faster." (g1p3)

"For other methods, I probably have to scan my student ID and be validated and verified, but everything went quiet without a lot of interaction." (g1p5)

"The only worry I have is that with the password, I can always provide it, but with the QR code, I cannot always provide the information needed if my phone has died." (g2p4)

Suggestions to improve

"The only thing I struggled with was terminology since I lacked the background information." (g2p6)

"Maybe making the wallet interface simpler and also adding clearer instructions to the app can help." (g1p3)

Future Work

- A more comprehensive user interview with more participants.
- Evaluating how intuitive is the policy language.
- A tool to simplify policy initialization.

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
www.matthes.in.tum.de

Attributions

- San francisco icons created by DinosoftLabs - Flaticon
- Compliant icons created by POD Gladiator - Flaticon
- Identity icons created by Yogi Aprelliyanto - Flaticon
- Inscription icons created by Anggara - Flaticon
- Car icons created by Freepik - Flaticon
- Phone number icons created by Tanah Basah - Flaticon
- Sell icons created by itim2101 - Flaticon
- Live icons created by berkahicon - Flaticon
- Landing page icons created by Freepik - Flaticon
- Button icons created by Prashanth Rapolu 15 - Flaticon
- Qr code icons created by afif fudin - Flaticon
- Choice icons created by Freepik - Flaticon
- Population icons created by Uniconlabs - Flaticon
- Team icons created by yut1655 - Flaticon
- List icons created by Freepik - Flaticon