

# Towards a Decentralized Single Sign-On with Keycloak and Yivi

*Master Thesis Presentation*

Student: Sara Vahdati Pour

Supervisors: Dr. Greg Alpar  
Dr. Bram Westerbaan

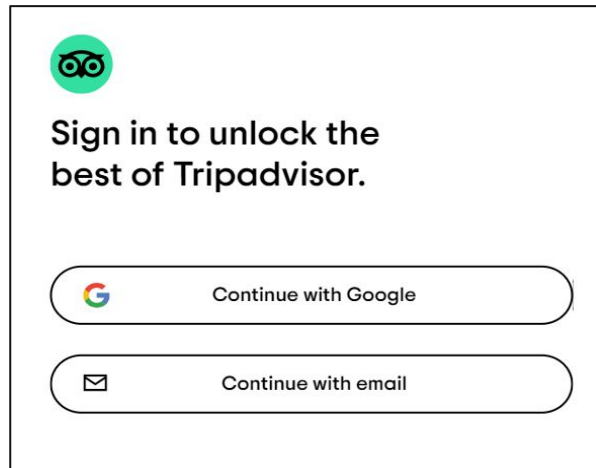
# Contents

1. SSO on the Web: Privacy Challenges and Risks
2. Digital Identity Privacy-Enhancing Designs
3. Keyvi Prototype and Contributions



# 1. SSO on the Web: Privacy Challenges and Risks

→ Single Sign-On (SSO)



 Sign in with Google



## Sign in

to continue to [Tripadvisor](#)

Email or phone

[Forgot email?](#)


To continue, Google will share your name, email address, language preference, and profile picture with Tripadvisor. Before using this app, you can review Tripadvisor's [privacy policy](#) and [terms of service](#).

[Create account](#)

[Next](#)


# 1. SSO on the Web: Privacy Challenges and Risks

→ Single Sign-On (SSO)

 Sign in with Google



## Sign in to Tripadvisor

 `serena@tripadvisor@googlemail.com`

By continuing, Google will share your name, email address, language preference and profile picture with Tripadvisor. See Tripadvisor's [privacy policy](#) and [Terms of Service](#).

You can manage Sign in with Google in your [Google Account](#).

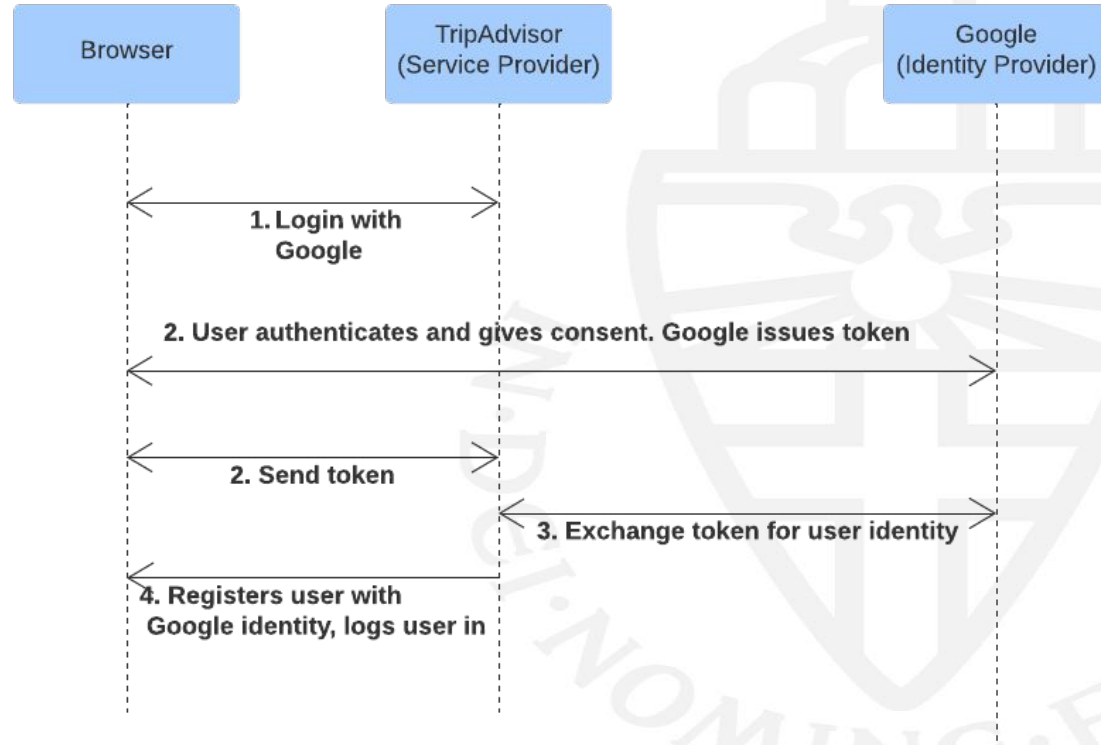
**Consent**

Cancel

Continue

# 1. SSO on the Web: Privacy Challenges and Risks

→ Single Sign-On (SSO)




# 1. SSO on the Web: Privacy Challenges and Risks

- Single Sign-On (SSO)
- **Digital Identity**

 Sign in with Google



## Sign in to Tripadvisor

 sarovar.datipour@googlemail.com

**Identifier**

**Attributes**

By continuing, Google will share your name, email address, language preference and profile picture with Tripadvisor. See Tripadvisor's [privacy policy](#) and [Terms of Service](#).

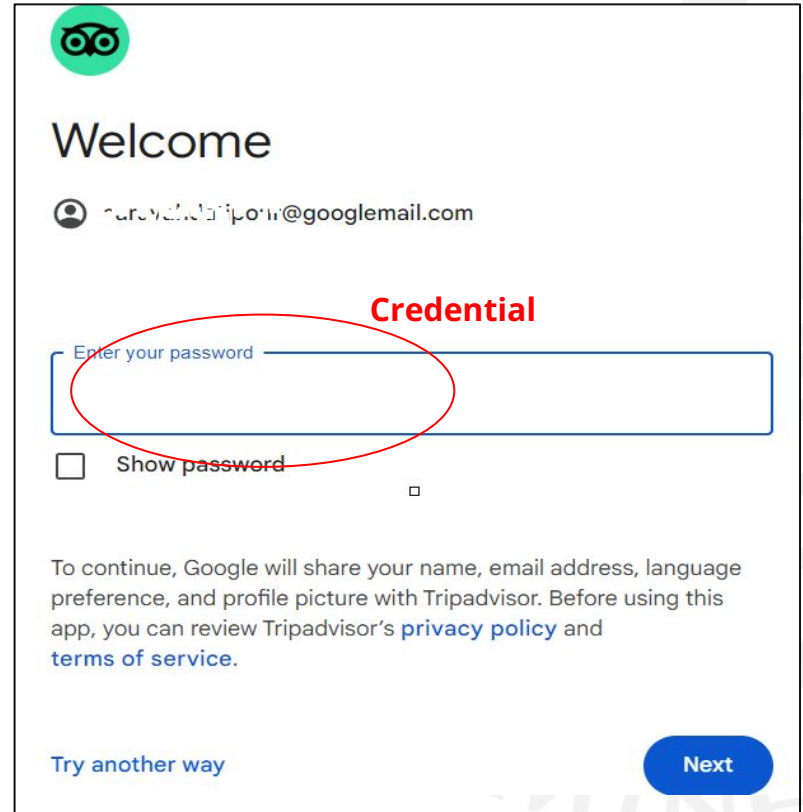
You can manage Sign in with Google in your [Google Account](#).


Cancel

Continue


# 1. SSO on the Web: Privacy Challenges and Risks

- Single Sign-On (SSO)
- **Digital Identity**





## Welcome

 maraveloustriponr@gmail.com

Enter your password **Credential**

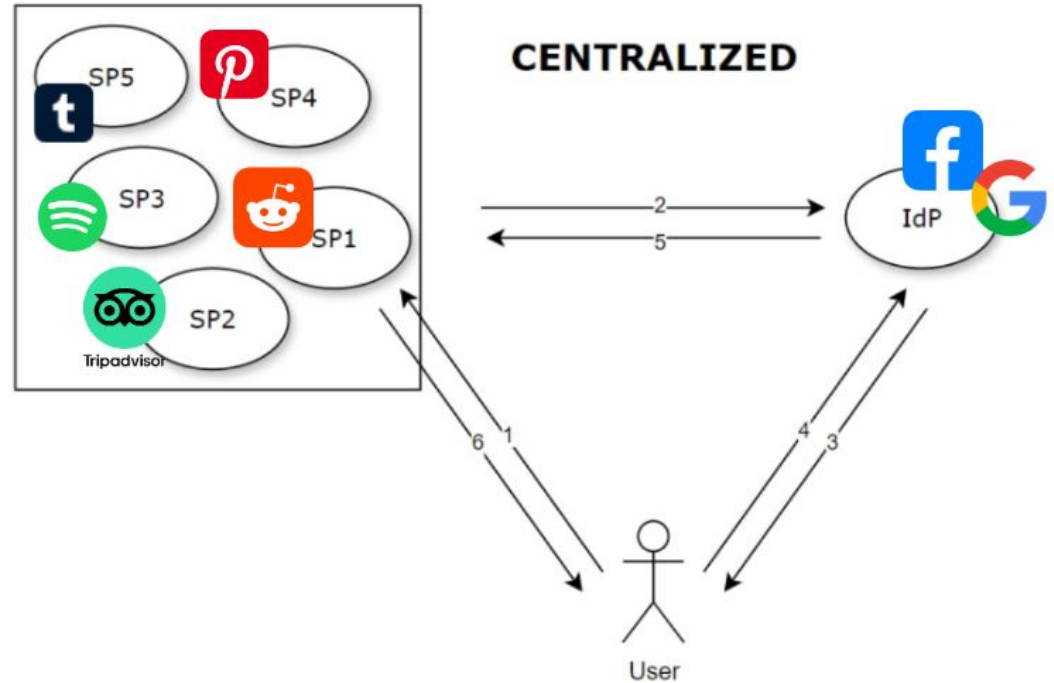
Show password

To continue, Google will share your name, email address, language preference, and profile picture with Tripadvisor. Before using this app, you can review Tripadvisor's [privacy policy](#) and [terms of service](#).

[Try another way](#) **Next**

# 1. SSO on the Web: Privacy Challenges and Risks

- Single Sign-On (SSO)
- Digital Identity
- **Web SSO is Centralized**





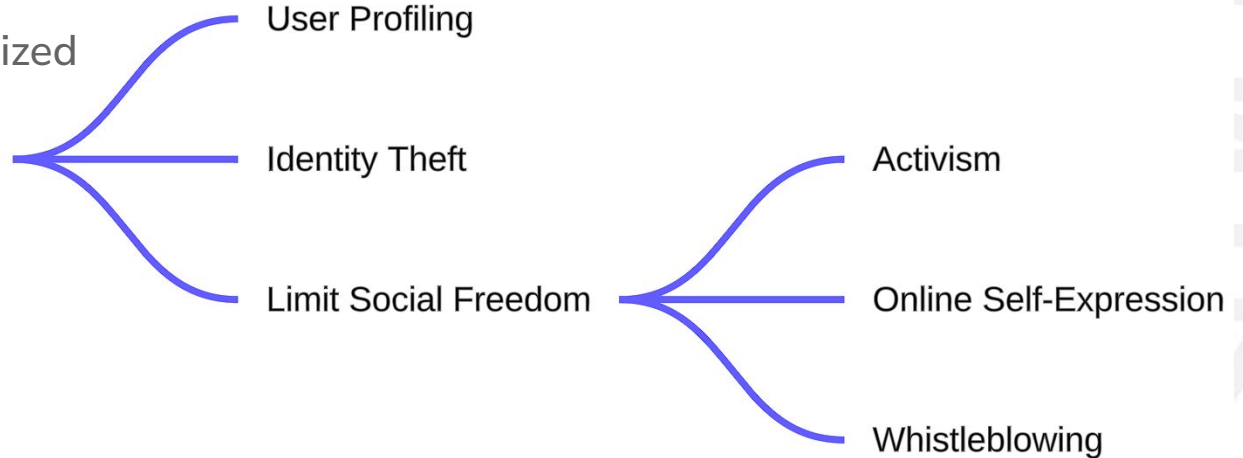
# 1. SSO on the Web: Privacy Challenges and Risks

- Single Sign-On (SSO)
- Digital Identity
- Web SSO is Centralized
- **Privacy Challenges**

Privacy Property	Lack of Property
Undetectability	IdP detects authentication to SP
Unlinkability	IdP links authentication on SPs
Confidentiality	IdP knows what attributes were shared

# 1. SSO on the Web: Privacy Challenges and Risks

- Single Sign-On (SSO)
- Digital Identity
- Web SSO is Centralized
- Privacy Challenges
- **Privacy Risks**



# 1. SSO on the Web: Privacy Challenges and Risks

- Single Sign-On (SSO)
- Digital Identity
- Web SSO is Centralized
- Privacy Challenges
- Privacy Risks

## Data allegedly stolen from 560 million Ticketmaster users

30 May 2024

By Brandon Drenon, BBC News

Share ↗

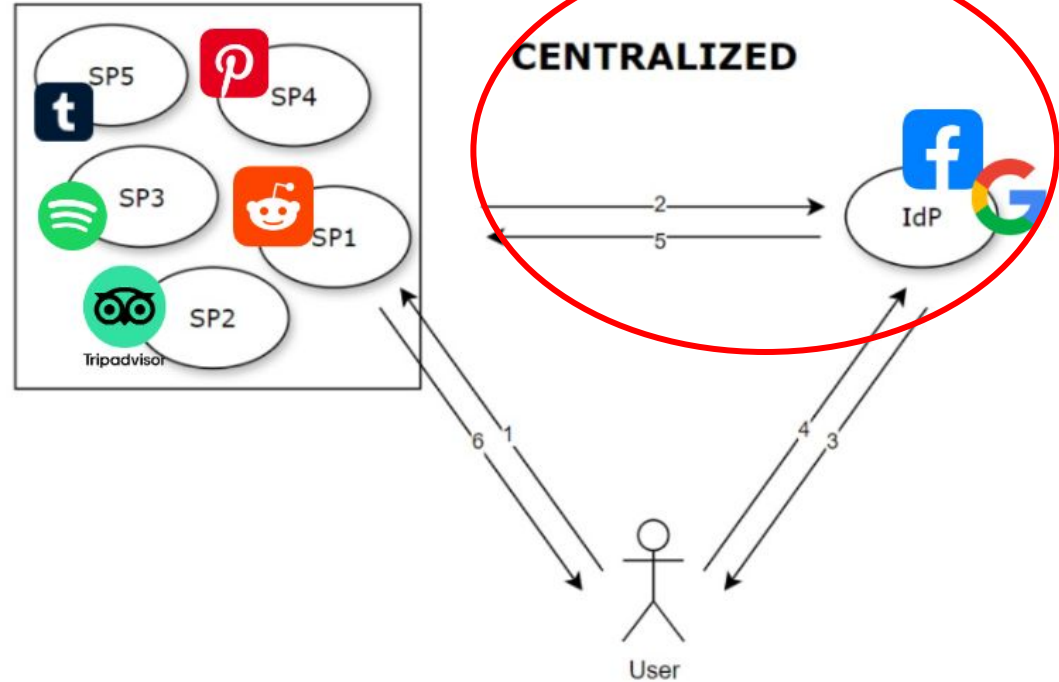
12-12-2020 | NEWS

## Every employee's worst nightmare, getting outed on Glassdoor, could become a reality

You leave a bad review of your former employer. Now the former employer is asking the court to unmask you.

# 1. SSO on the Web: Privacy Challenges and Risks

- Single Sign-On (SSO)
- Digital Identity
- Web SSO is Centralized
- Privacy Challenges
- Privacy Risks
- **Why?**



# 1. SSO on the Web: Privacy Challenges and Risks

- Single Sign-On (SSO)
- Digital Identity
- Web SSO is Centralized
- Privacy Challenges
- Privacy Risks
- Why?
- **Threat Model**

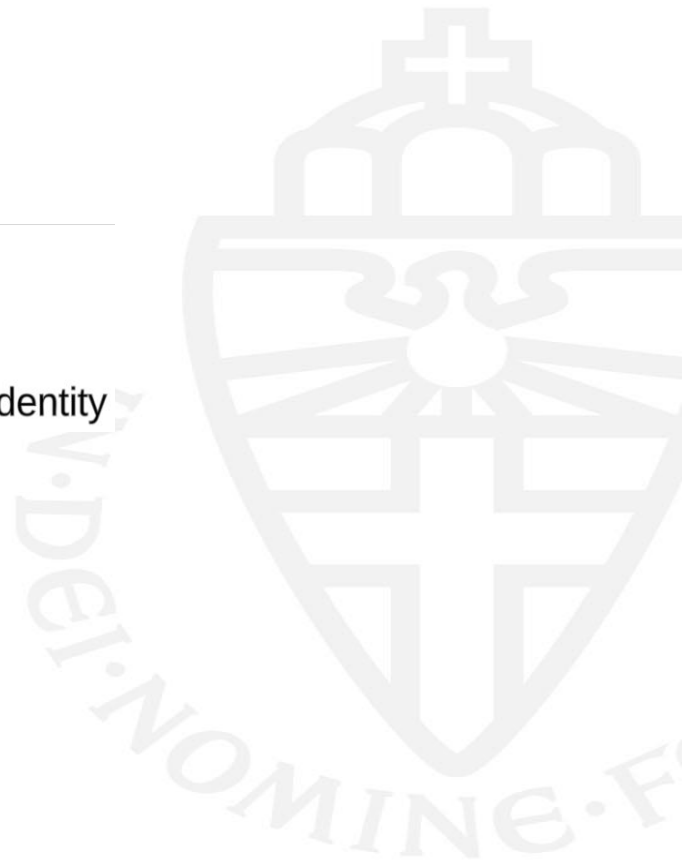
Threat Models	Privacy Consideration
Honest IdP	Can suffer data breaches
Honest-but-curious IdP	Can link users' activities
Malicious IdP	Can impersonate users on SPs

## 2. Digital Identity Privacy-Enhancing Designs

→ Main solution categories

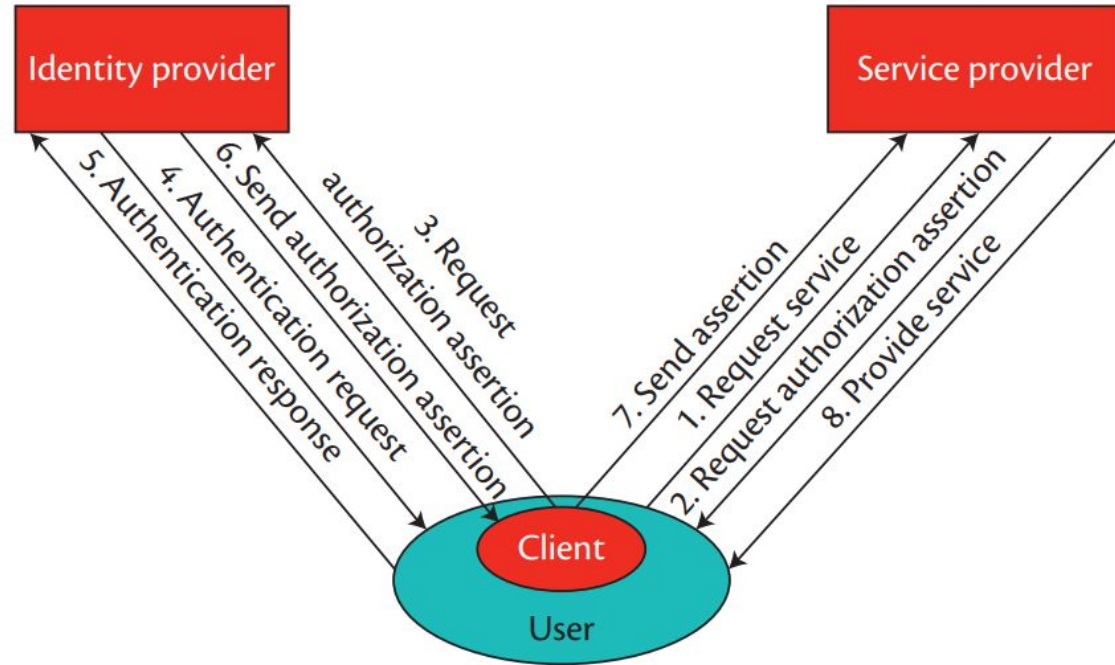
Active Client

Decentralized Identity



## 2. Digital Identity Privacy-Enhancing Designs

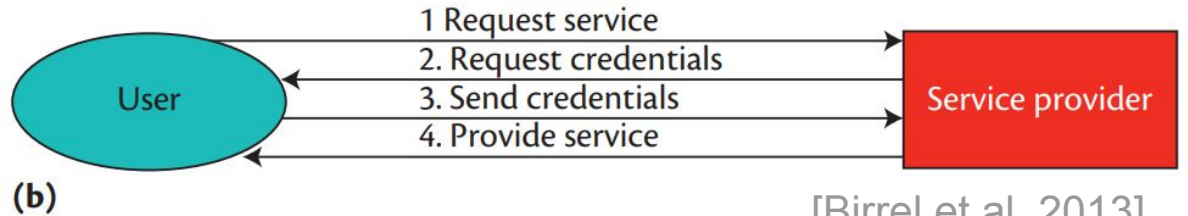
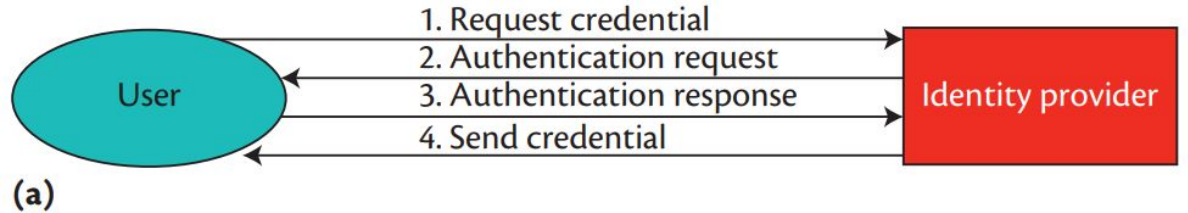
- Main solution categories
- **Active Client**



[Birrel et al. 2013]

## 2. Digital Identity Privacy-Enhancing Designs

- Main solution categories
- Active Client
- **Decentralized Identity**



[Birrel et al. 2013]



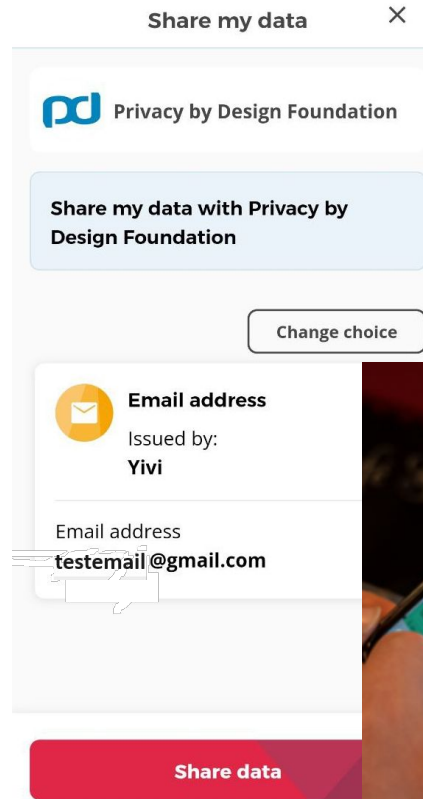
## 2. Digital Identity Privacy-Enhancing Designs

- Main solution categories
- Active Client
- Decentralized Identity
- **Differences**

Design Type	Privacy Property	Threat Model
Active Client	Unlinkability	Honest-but-curious
Decentralized Identity	Undetectability, Unlikability, Confidentiality	Malicious

## 2. Digital Identity Privacy-Enhancing Designs

- Main solution categories
- Active Client
- Decentralized Identity
- Differences
- **Decentralized Identity: Yivi**



yivi



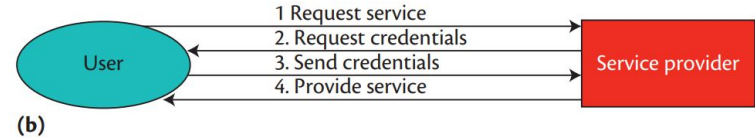
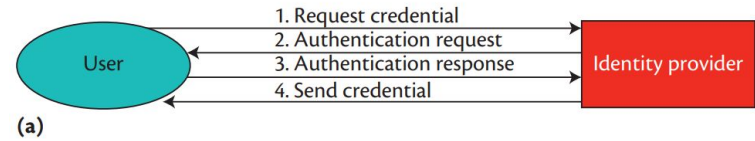
## 2. Digital Identity Privacy-Enhancing Designs

- Main solution categories
- Active Client
- Decentralized Identity
- Differences
- **Decentralized Identity: Yivi**

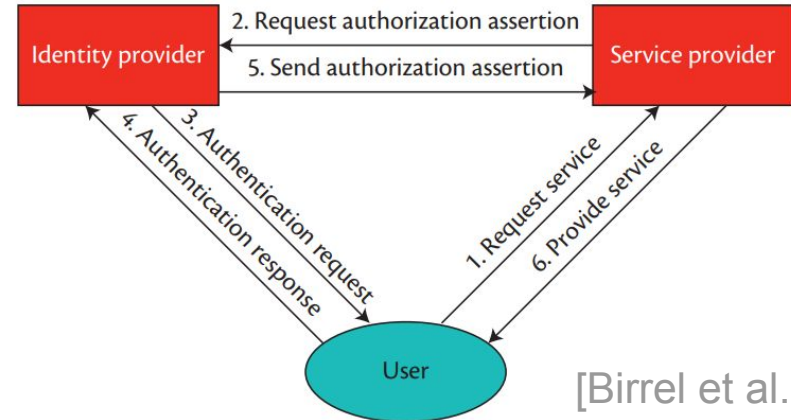
Yivi Features	Privacy Property
Selective Disclosure of Attributes	Confidentiality
Zero-Knowledge Proof	Unlinkability
Decentralized Identity	Undetectability

## 2. Digital Identity Privacy-Enhancing Designs

- Main solution categories
- Active Client
- Decentralized Identity
- Differences
- Decentralized Identity: Yivi
- **Obstacle: No SSO Support**



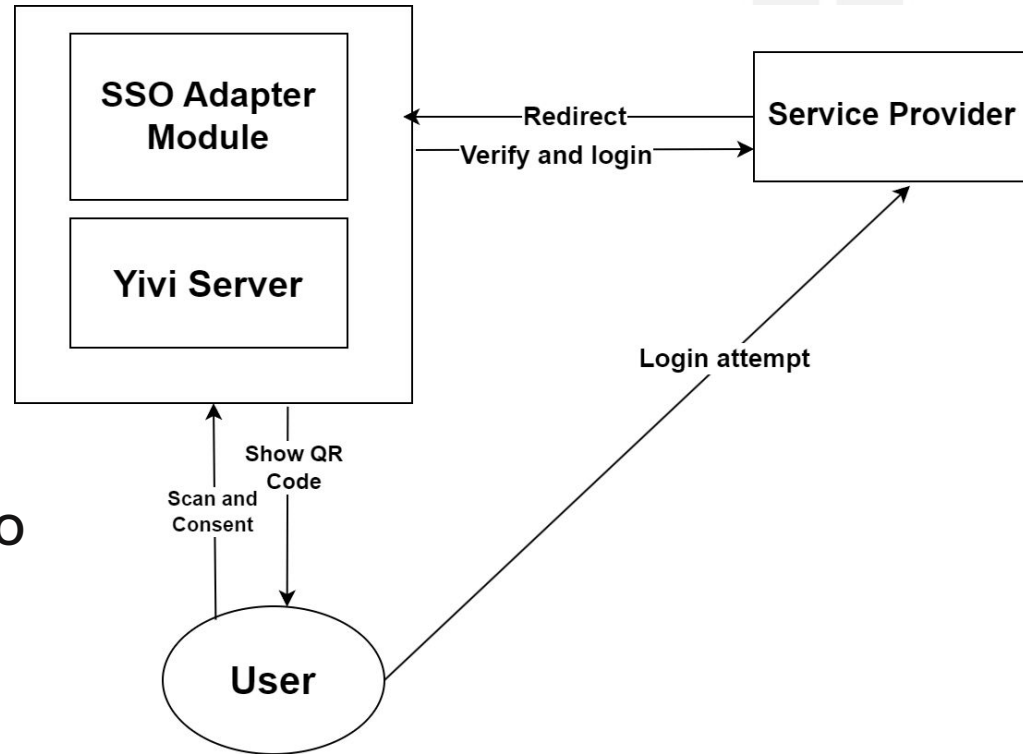
### Architecturally Different!



[Birrel et al. 2013]

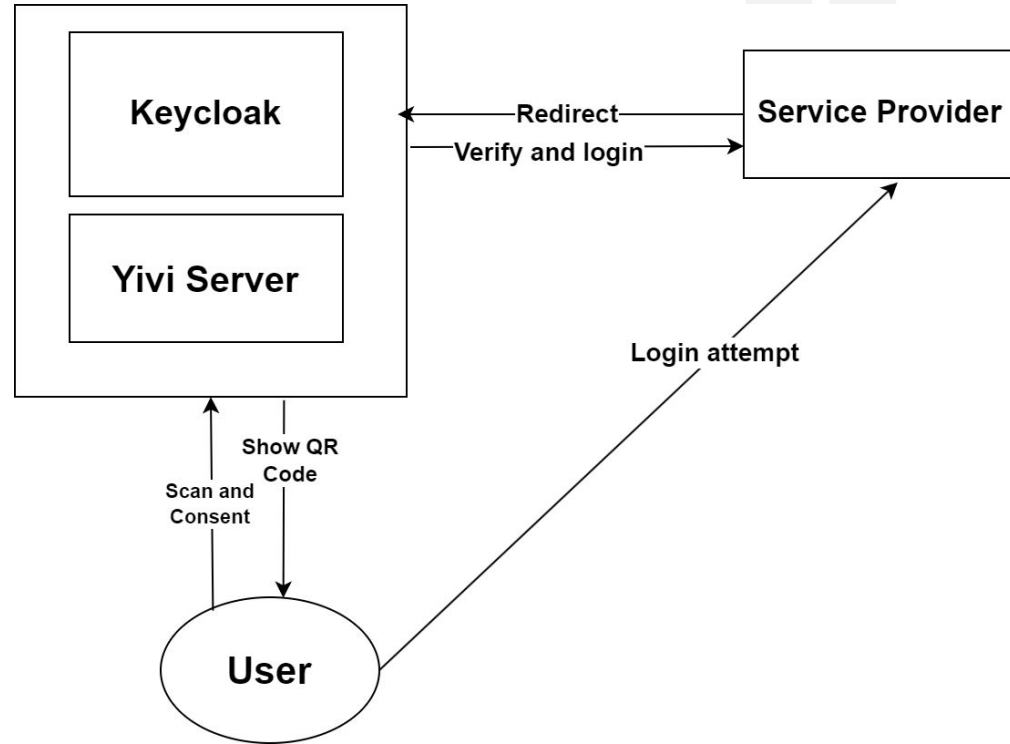
## 2. Digital Identity Privacy-Enhancing Designs

- Main solution categories
- Active Client
- Decentralized Identity
- Differences
- Decentralized Identity: Yivi
- Obstacle: No SSO Support
- **Approach: Integrate Yivi into a SSO**



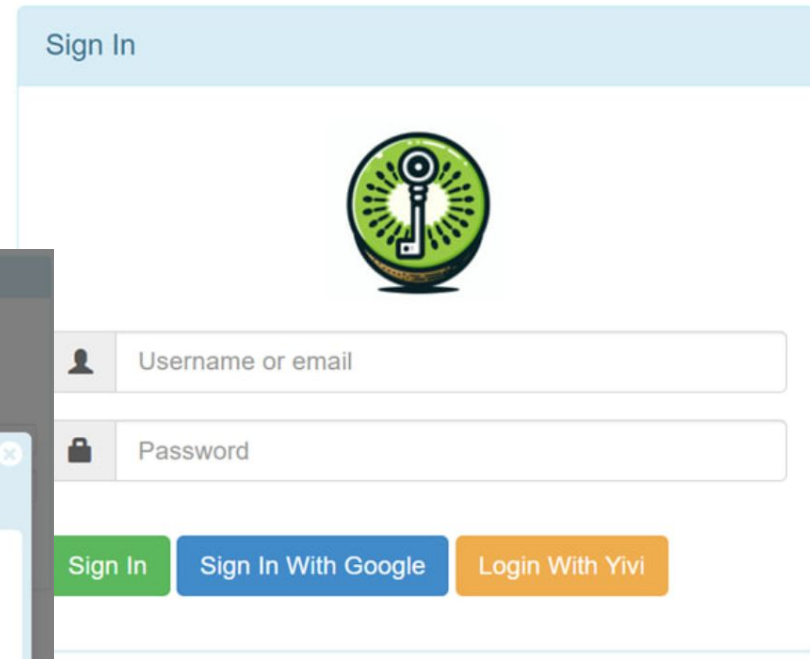
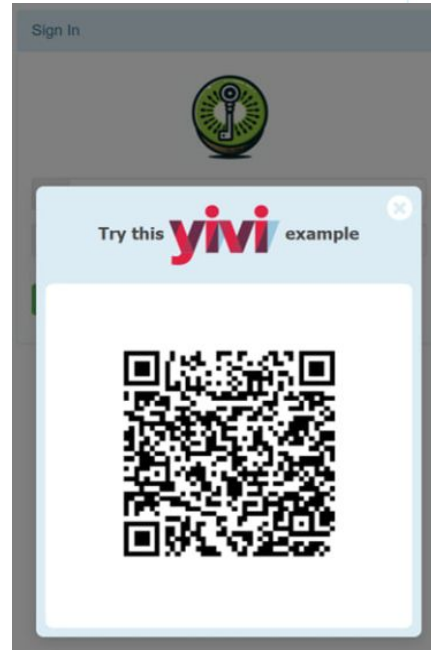
## 2. Digital Identity Privacy-Enhancing Designs

- Main solution categories
- Active Client
- Decentralized Identity
- Differences
- Decentralized Identity: Yivi
- Obstacle: No SSO Support
- Approach: Integrate Yivi into a SSO
- **Keycloak: Open-source and Free**



### 3. Keyvi Prototype and Contributions

→ Keyvi: Keycloak with Yivi



### 3. Keyvi Prototype and Contributions

→ Keyvi: Keycloak with Yivi

→ **Demo:**

1. Mastodon micro-blogging
2. Wordpress webshop





### 3. Keyvi Prototype and Contributions

Demo Time!



### 3. Keyvi Prototype and Contributions

- Keyvi: Keycloak with Yivi
- Demo
- **Contributions**

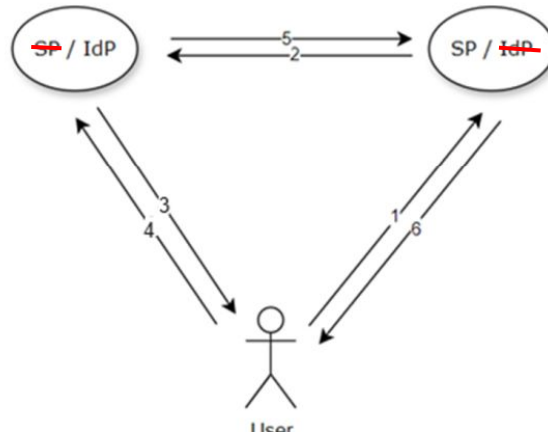
To researchers

Proof of Concept : Web SSO that is Decentralized is possible  
With the current free open source software

Opening up discussion for Federated Decentralized SSO

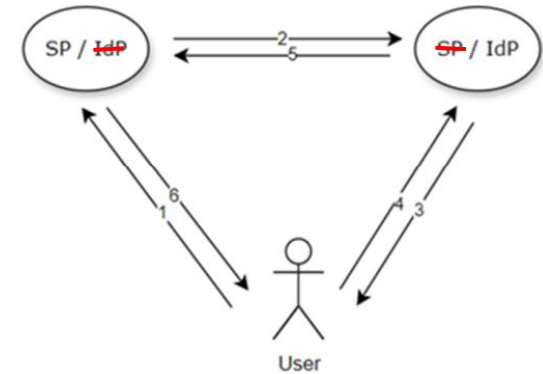
### 3. Keyvi Prototype and Contributions

- Keyvi: Keycloak with Yivi
- Demo
- **Contributions**



**FEDERATED**

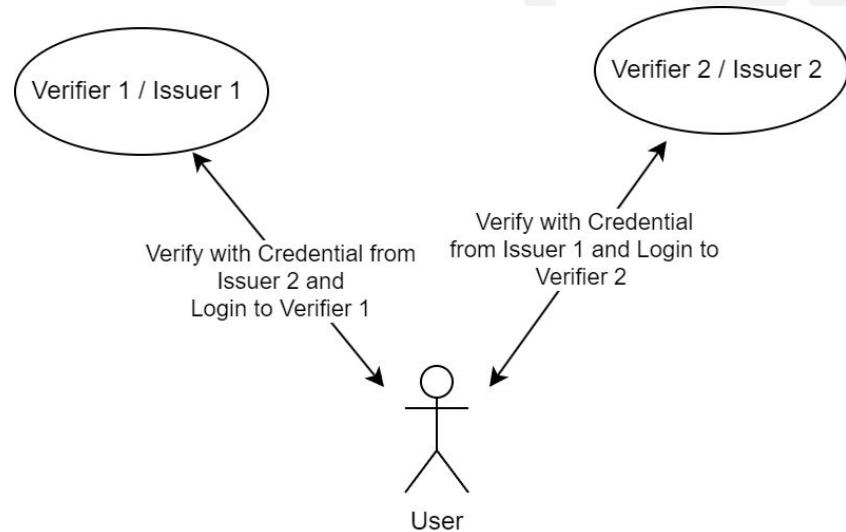
OR



### 3. Keyvi Prototype and Contributions

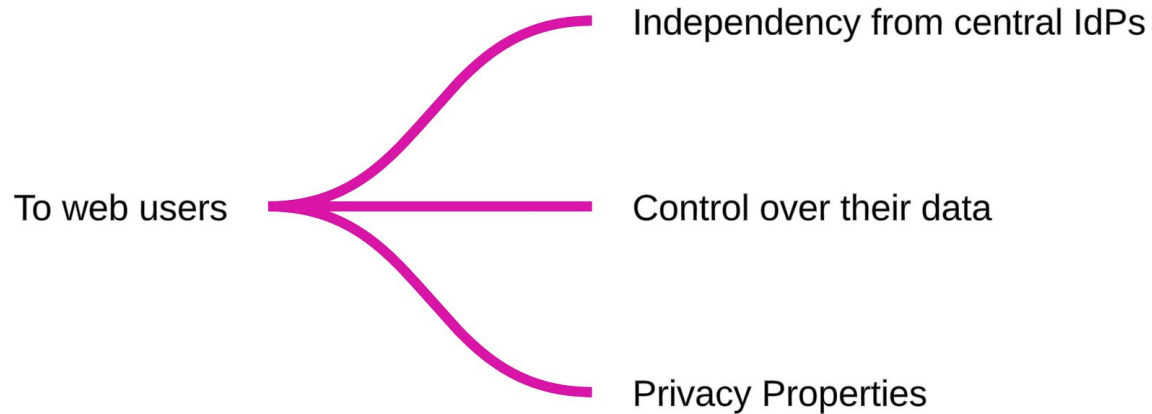
- Keyvi: Keycloak with Yivi
- Demo
- **Contributions**

#### Decentralized and Federated



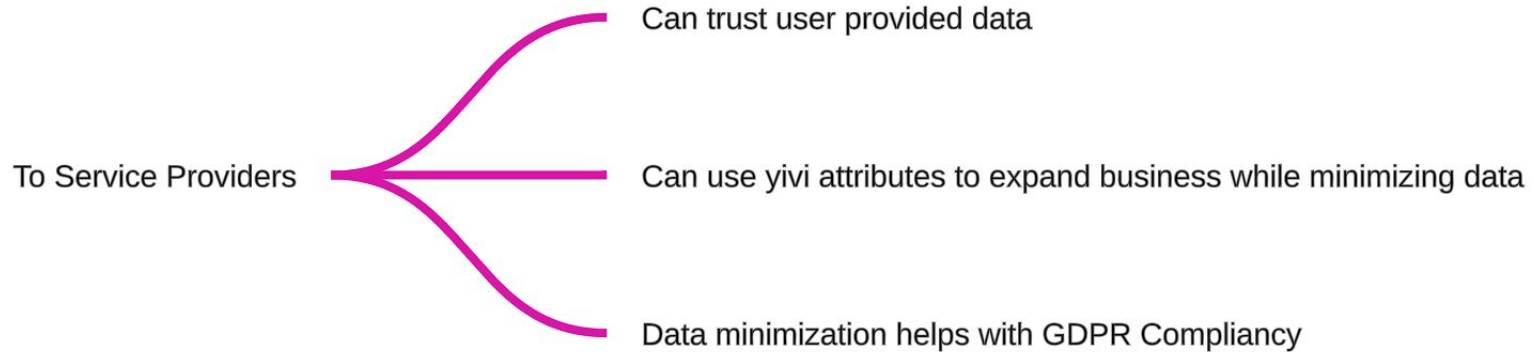
### 3. Keyvi Prototype and Contributions

- Keyvi: Keycloak with Yivi
- Demo
- **Contributions**



### 3. Keyvi Prototype and Contributions

- Keyvi: Keycloak with Yivi
- Demo
- **Contributions**



### 3. Keyvi Prototype and Contributions

- Keyvi: Keycloak with Yivi
- Demo
- **Contributions**

Example benefit of trustworthy Identity: **Limit catfishing on services**



### 3. Keyvi Prototype and Contributions

- Keyvi: Keycloak with Yivi
- Demo
- Contributions
- **Considerations**

- Greedy SPs asking for sensitive data (e.g BSN)
- Learning curve in developing Keycloak server
- Feasibility study needed
- Implementation of Single Sign-Out needed

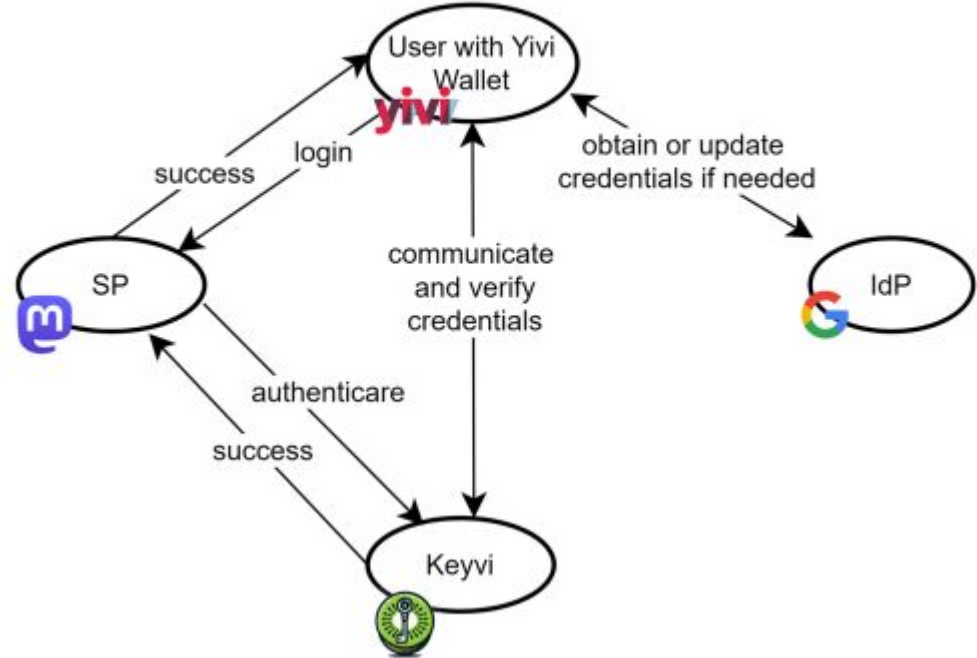


# Questions!



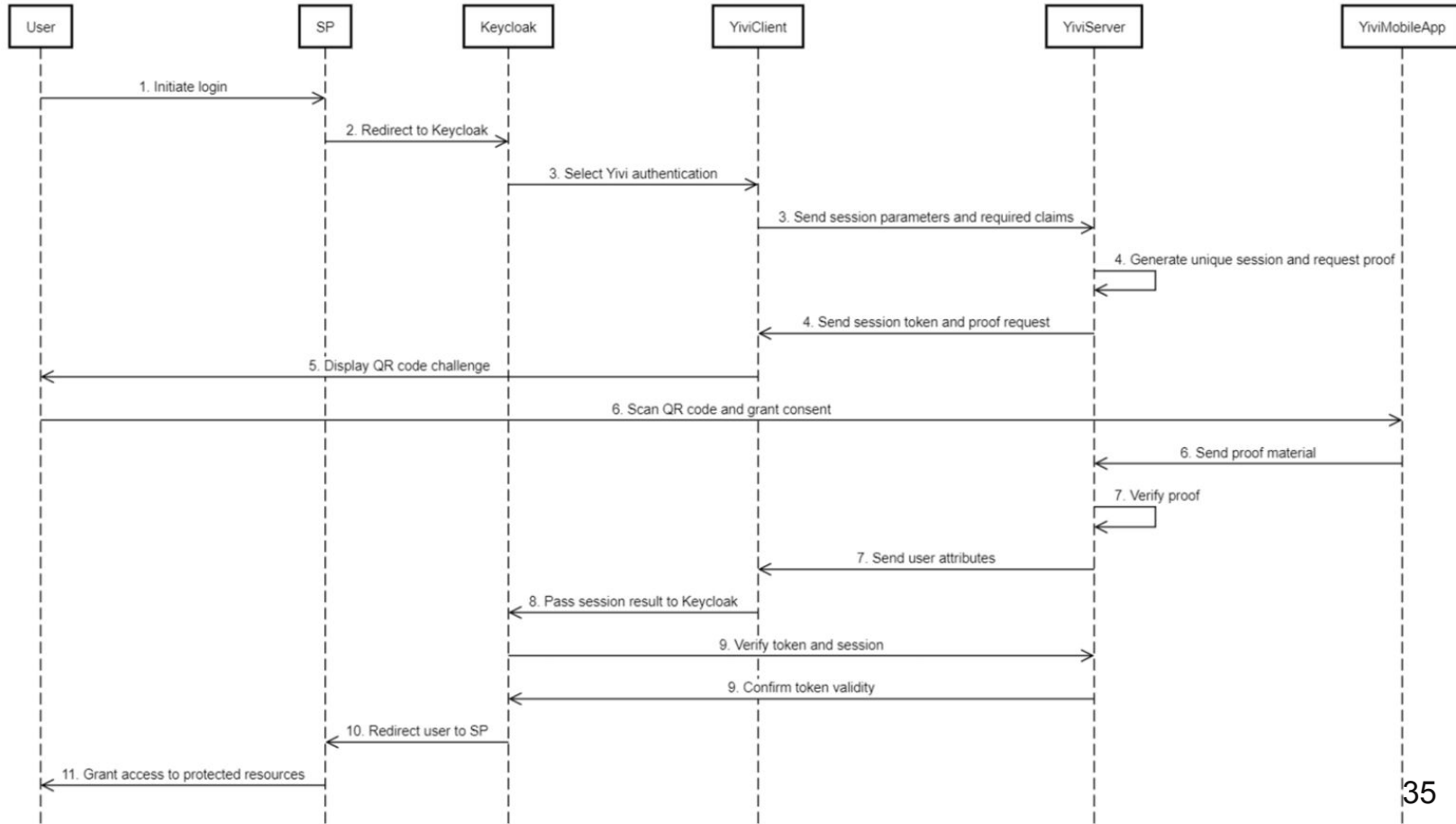
# Backup slides

- A full authentication session
- User has to acquire Yivi Credential First



# Backup slides

## Sequence Diagram of Keyvi



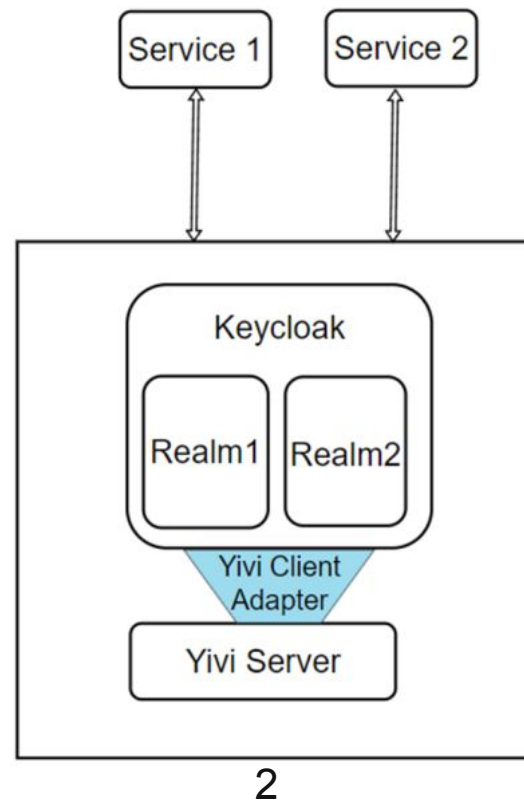
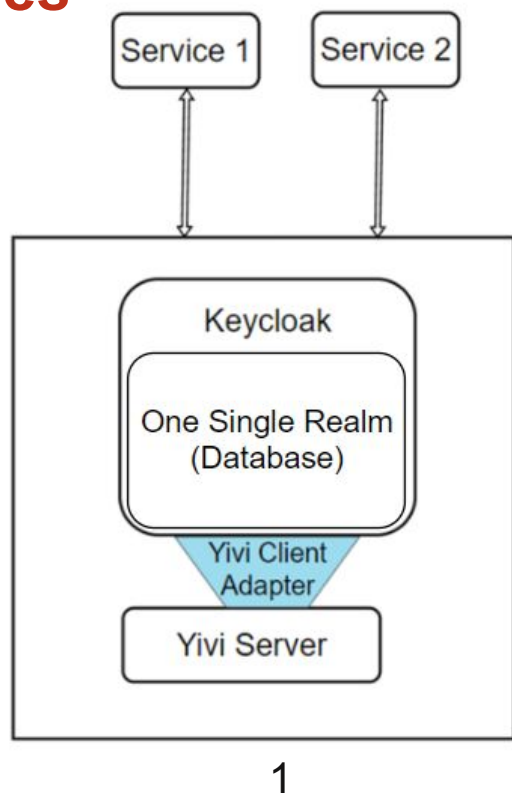
# Backup slides

- 1. Have the classic SSO experience across Different services.
- SSO to Service 1 results in *automatically* Signing in to Service 2 when a single realm is used.

OR

2. Different services of the server provider Have separate database enclaves allowing for separating user base based on use case → For *data minimization*

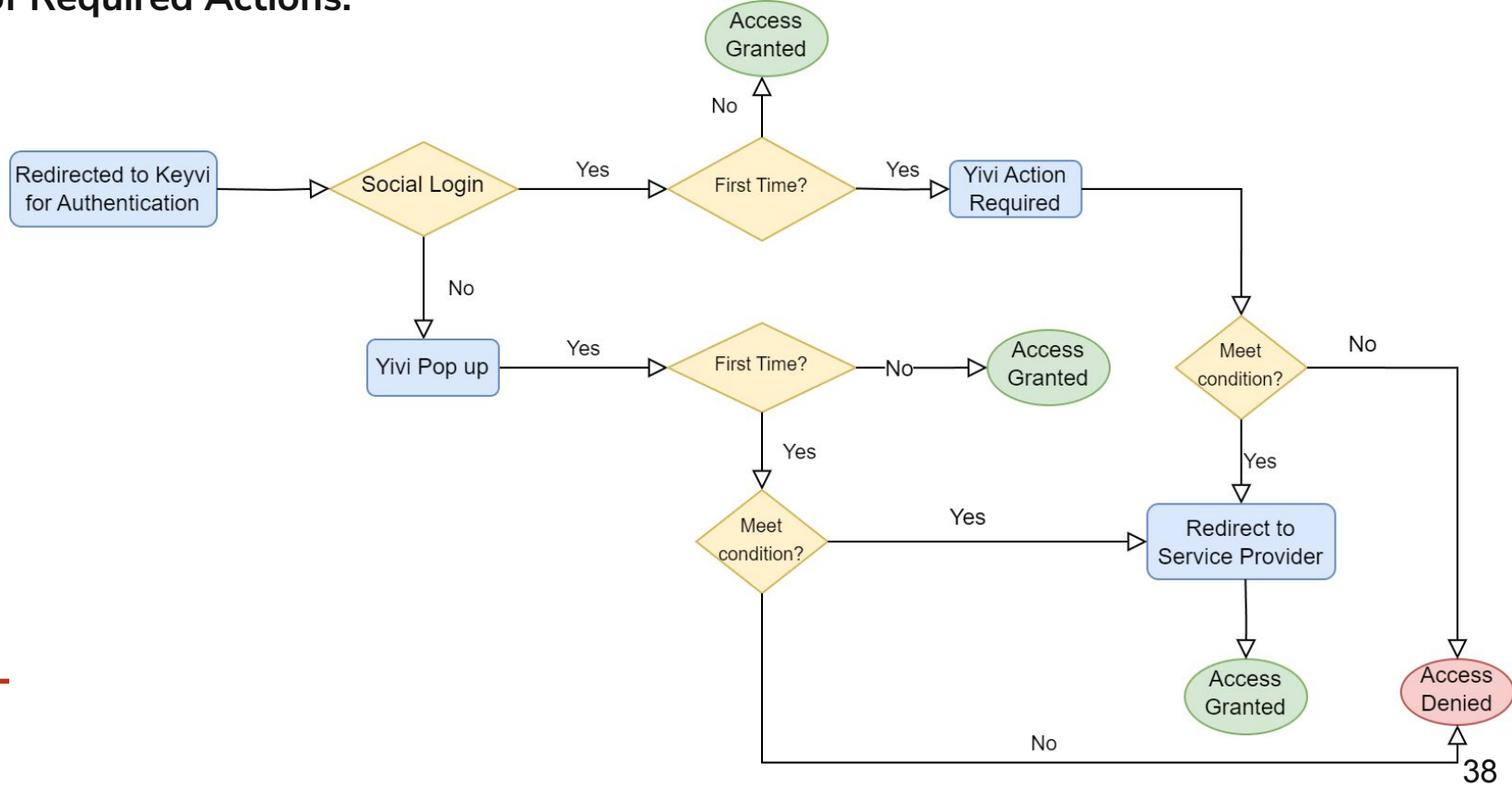
# Backup slides



# Backup slides



→ Point of Required Actions:



# Bibliography

**[1]** E. Birrell and F. B. Schneider, "Federated Identity Management Systems: A Privacy-Based Characterization," in *IEEE Security & Privacy*, vol. 11, no. 5, pp. 36-48, Sept.-Oct. 2013, doi: 10.1109/MSP.2013.114. keywords: {Identity management;Data storage systems;Authentication;Metasearch;authentication of humans;privacy;identity management systems}