User Provisioning, Federation and Federated Identity

Kevin Dockx
Architect

@KevinDockx https://www.kevindockx.com

Coming Up

Integrating local users with external users

Federated authentication and federated identity

Provisioning users

Linking third-party providers to a user

Integrating Local Users with External Users

Linking users across IDPs should happen at level of the IDP, not at level of the client

- Puts less responsibility on the client
- IDP has the (necessary) context and information the client doesn't have
- Avoids having to implement this in all clients

Integrating Local Users with External Users

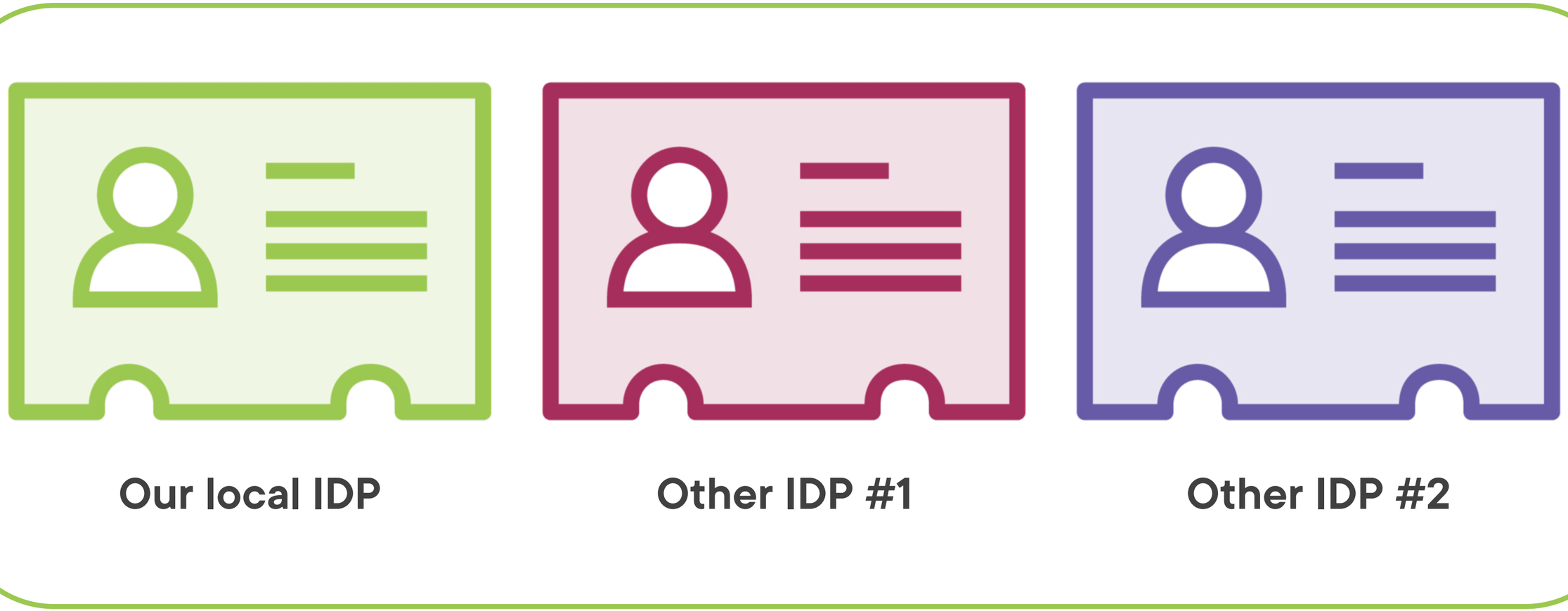
The local user's sub value is returned, regardless of how/at what level the user authenticated

- One user, different sets of credentials

Federated authentication

Federating out authentication to a third party

Federated Authentication and Federated Identity



All part of the same federation

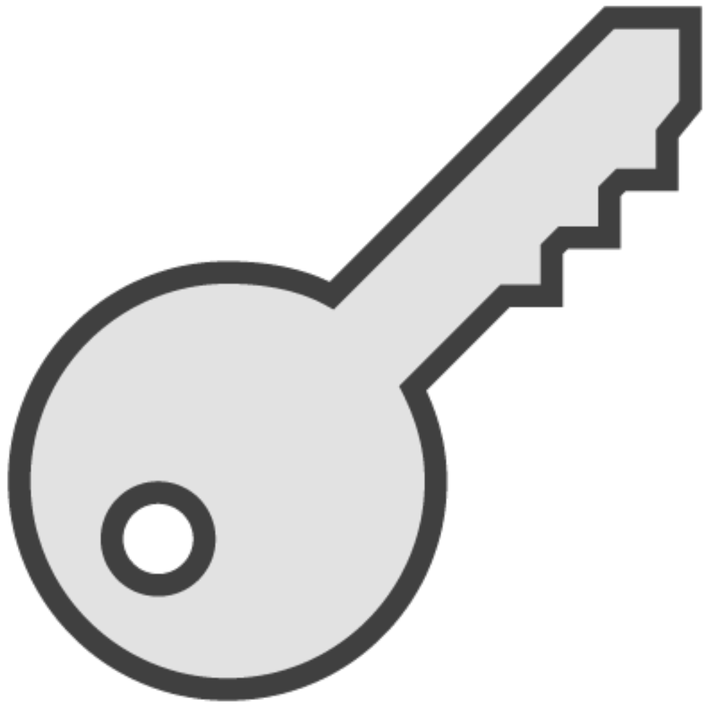
Federated identity

The means of linking a person's electronic identity and attributes, stored across multiple distinct identity providers

Federated Authentication and Federated Identity

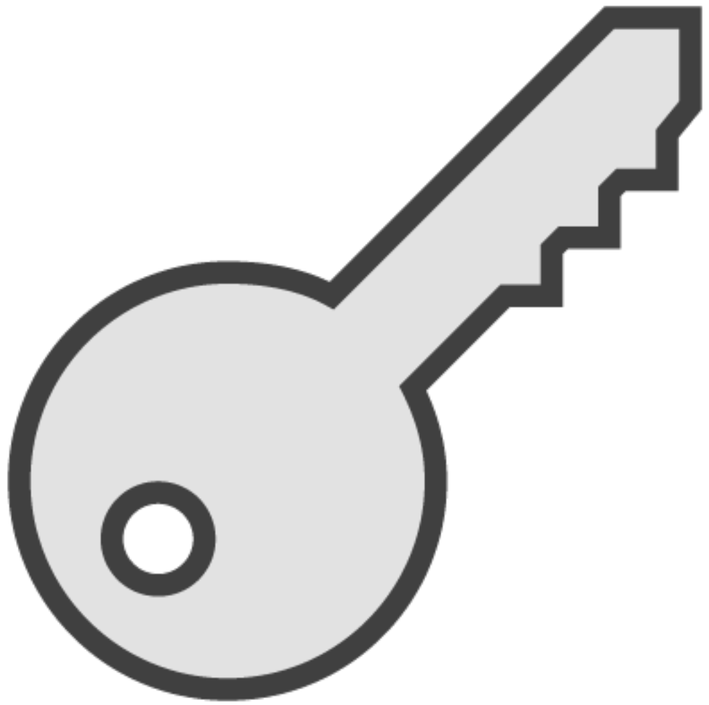
Federated identity

- Claims can live at level of various IDPs
- Together they make up the user's identity
- It's common to store external claims locally and update them regularly (but the external provider = master)



To link identities we need a key that exists in both systems and that can be trusted

- A good example is a verified e-mail address
- On the quality of the key rests the reliability of the federated identity



It’s not unusual NOT to find a trustworthy key

- Linking identities can become a manual process

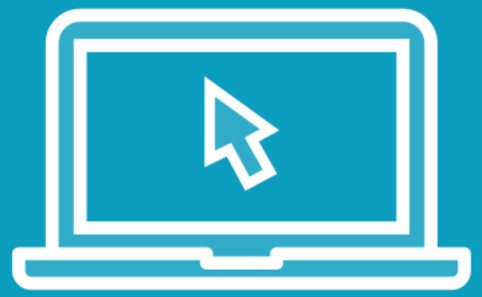
User provisioning

The process that ensures users are created, changed, disabled, deleted and/or given the permissions and/or claims they need

User provisioning

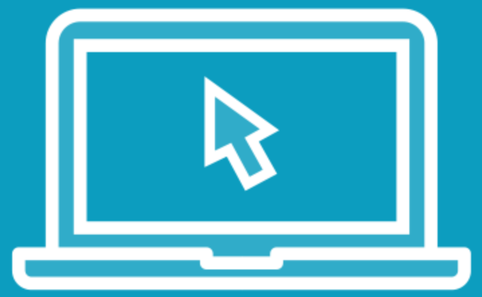
- Users can provision themselves (e.g.: by registering)
- Users can automatically be provisioned by our IAM system
- Provisioning can be a combination of both techniques

Demo



Enhancing the database schema for federated identity

Demo



Provisioning a new user with a federated identity (part one)

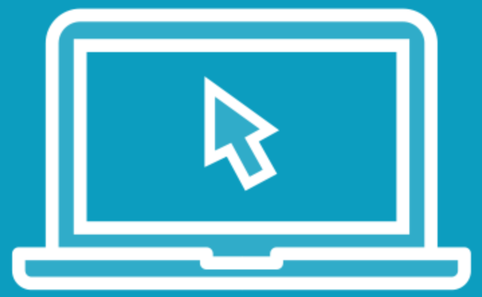
```
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
```

Transforming Claims

Claim types from an external provider often don’t match the types an IDP works with

- Transform them to claim types the IDP can work with
- Add, remove or change if required – you are in control

Demo



Provisioning a new user with a federated identity (part two)

Provisioning a New User with a Federated Identity – Flow Variations

Asking for additional claims to be inputted manually (e.g.: address, country, phone number, …)

- Custom work: create a new view, remember to pass through the `returnUrl` value

Provisioning a New User with a Federated Identity – Flow Variations

Requiring a user to choose a local password / local means of authentication

- Third-party integration is used for auto-filling of common claims (firstname, lastname, email, ...)
- Third-party authentication can be kept together with a local password or not

Provisioning a New User with a Federated Identity – Flow Variations

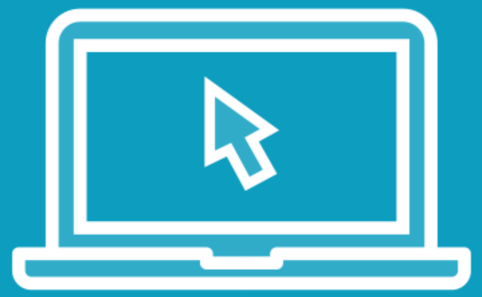
Requiring a user to activate an account via an activation link

- Requires less reliance on / trust in the process at level of the third party provider

Flow customization

Allows you to put more or less trust in the third party as you see fit

Demo



Linking a provider to an existing user

Additional Federated Identity Use Cases

Linking a third-party provider to an existing local account

- Manually via a user profile page instead of automatically
- Ask whether they want to link when you detect a potential match

Variation: linking multiple third-party providers

Additional Federated Identity Use Cases

Unlinking

- Typically via a user profile page

Deprovisioning a user

- Manually (by the user)
- Automatically (e.g.: when the user leaves the company)

Summary

Federated authentication

- Federating out authentication to a third party

Federated identity

- The means of linking a person's electronic identity and attributes, stored across multiple distinct IDP

Summary

IdentityServer is very customizable

- The UI is an ASP.NET Core web application

Finding a good key to link identities across IDPs is essential

- This cannot always be automated

Up Next:
Supporting Multi-factor Authentication