Patterns for Web Applications

Dominick Baier
http://leastprivilege.com
@leastprivilege

Brock Allen
http://brockallen.com
@brocklallen

identity SERVER

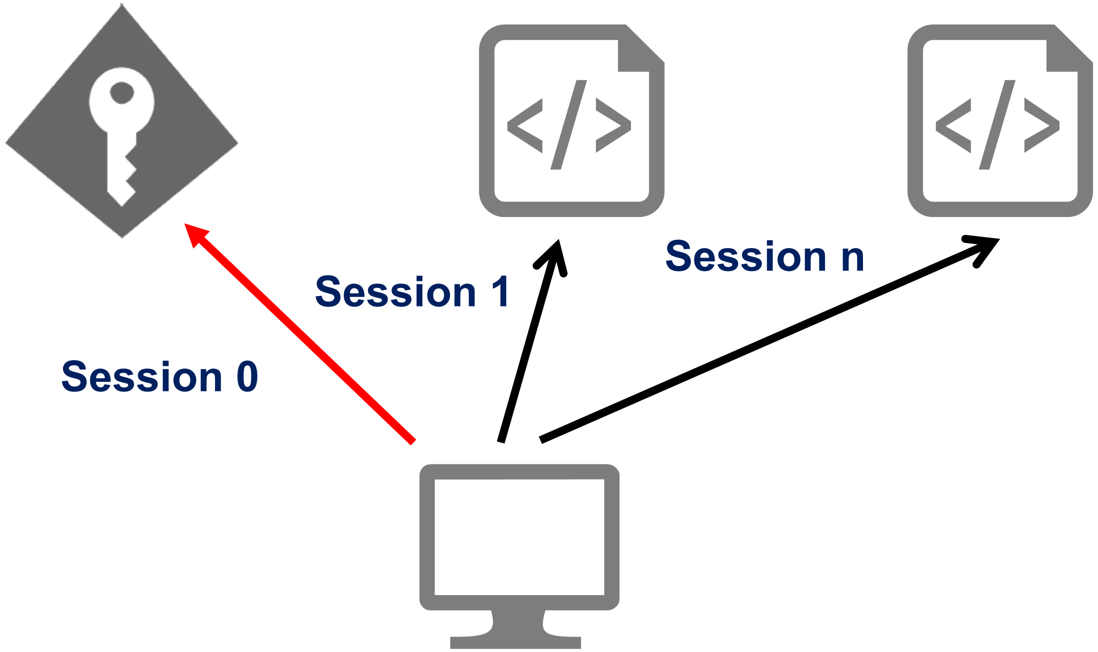
identity MODEL

Objectives

- **Single Sign On**
- **Single Sign Off**
- **Federation**
- **Home Realm Discovery**

Single Sign-On

- **OpenID Connect provider establishes a logon session with browser**
  - multiple clients in same browser use provided
  - for the duration of session, clients can request authentication user interaction
  - after successful authentication request, each client establishes its own session

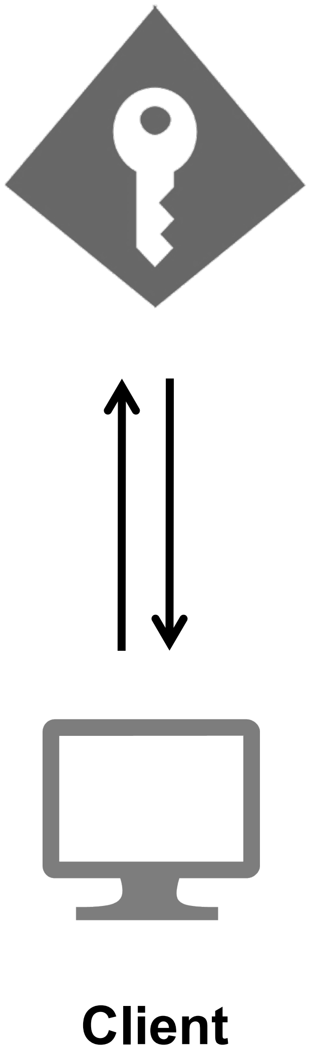


Single Sign-Out

- **Complete sign-out process consists of**
  1. clean up session at local RP
  2. clean up session at the STS
  3. clean up resources at all other RPs in the same session
  4. (clean up session at potential upstream STS)

- **Cleanup is complicated - thus three specs**
  - front-channel notification
  - back-channel notifications
  - JS-based notifications

Example: Front-Channel Cleanup

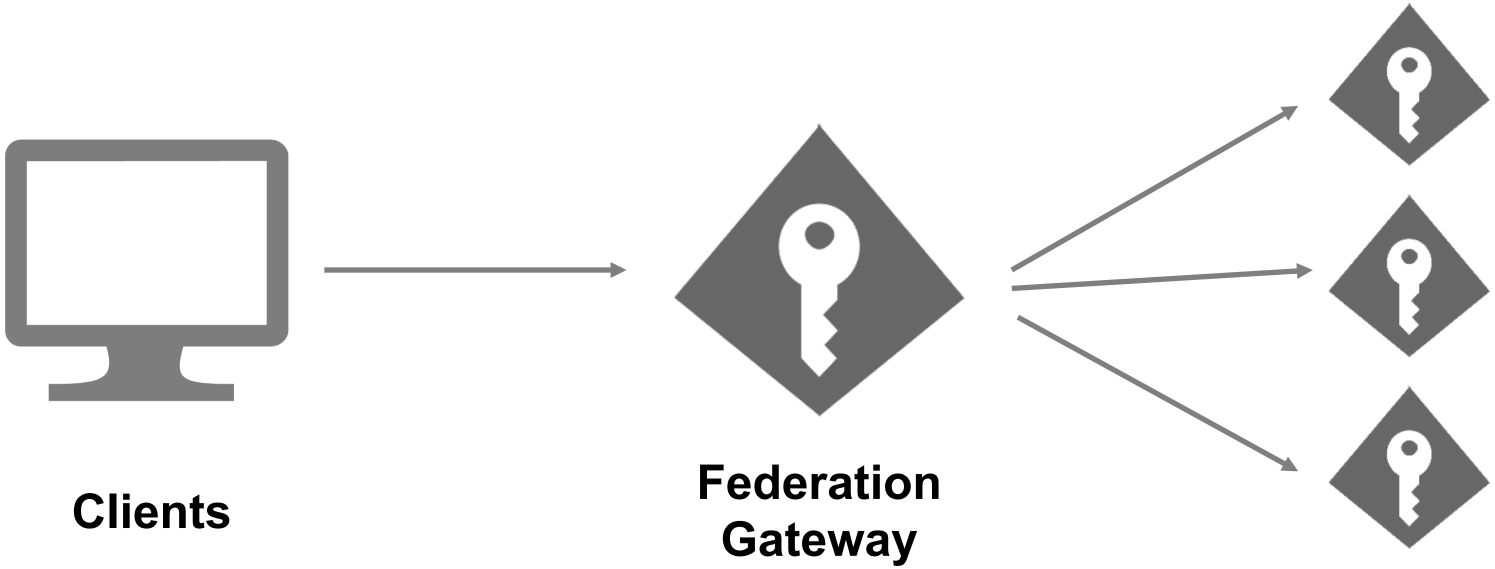


GET /end_session

```
<iframe style="visibility:hidden"
     src="https://client1/signout?sid=123">
</iframe>
<iframe class="visibility:hidden"
     src="https://client2/signout?sid=123">
</iframe>
<iframe class="visibility:hidden"
     src="https://client3/signout?sid=123">
</iframe>

<a href="https://client1">return</a>
```

Federation Gateway Pattern



Clients

Federation Gateway

- Active Directory
- Azure AD/B2C
- Business Partner
- Social Identities..

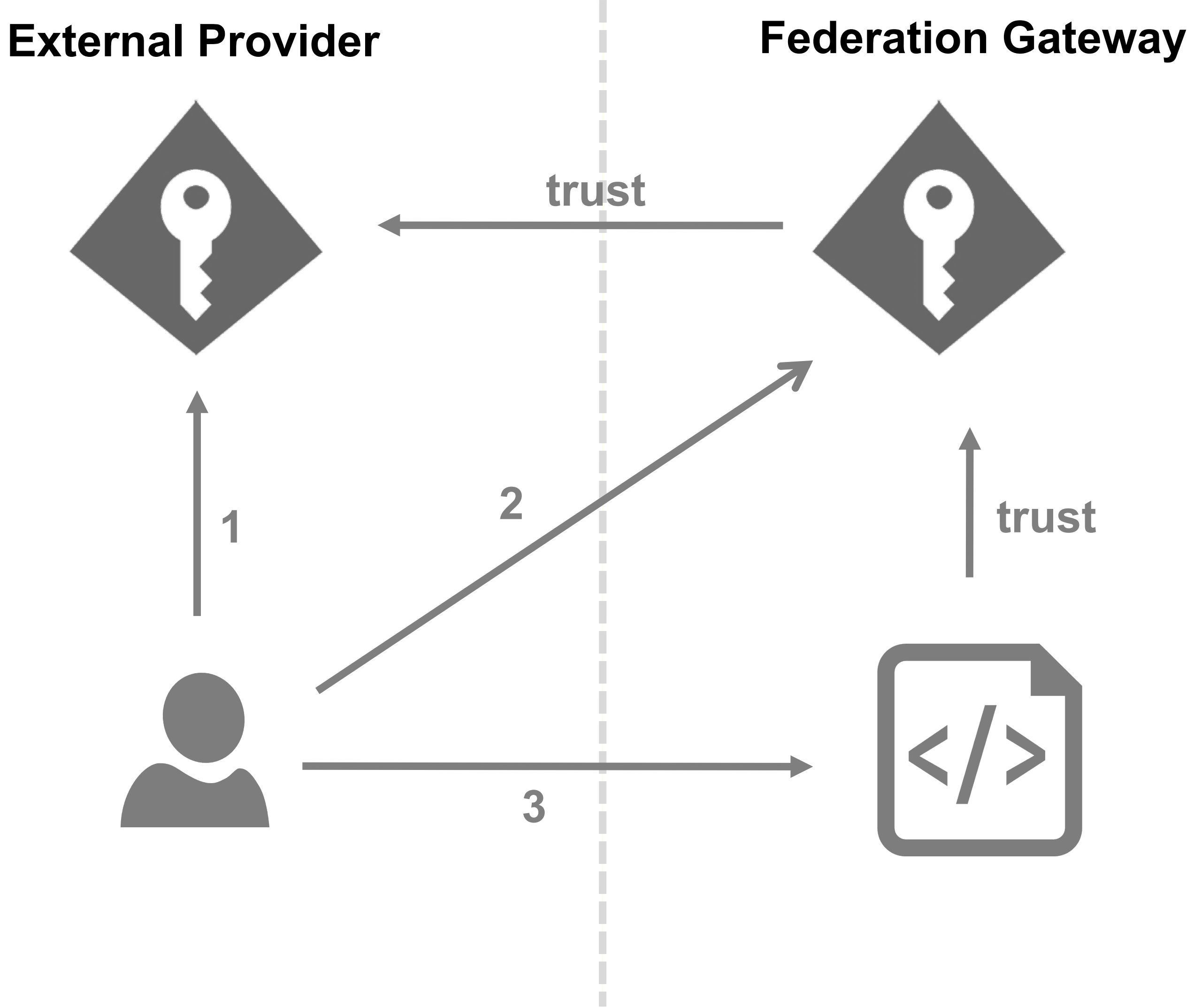
Benefits

- **Clients only "knows" about single provider (the gateway)**
- **Client shielded from all technical details (and changes over time)**

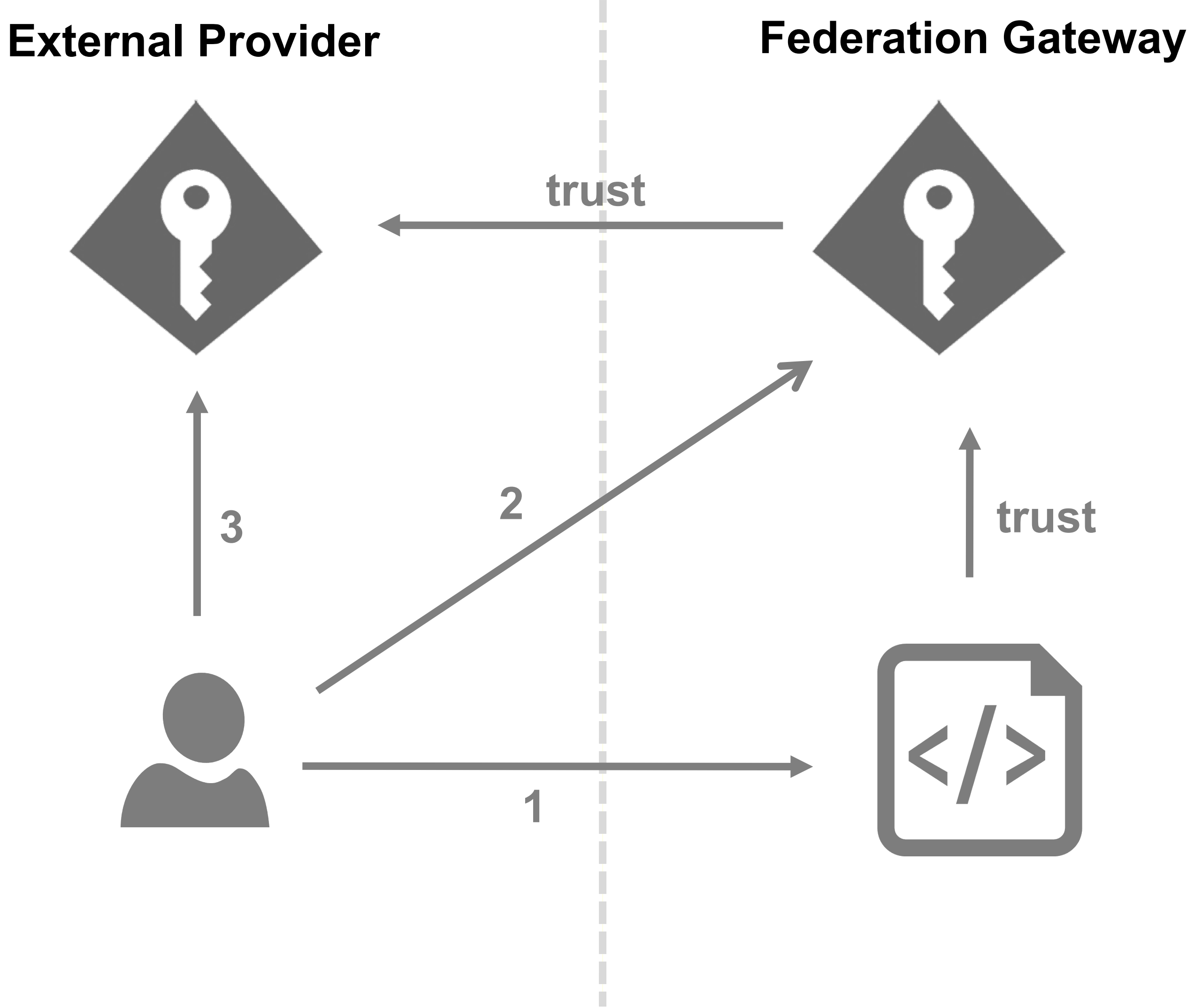
- **Gateway deals with all complexity**
  - protocols
  - token types
  - claim types and transformation
  - provisioning of external users

- **Gateway acts as single client to external provider**
  - can save money in IdaaS scenarios

Federation – logical model

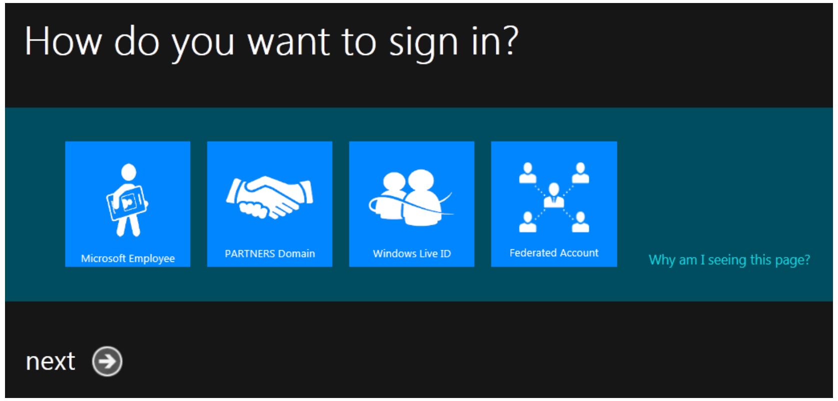


Federation – physical model



Home Realm Discovery (HRD)

- **How can we know which external provider to use when user is anonymous?**
  - some sort of hint required



How do you want to sign in?

Microsoft Employee

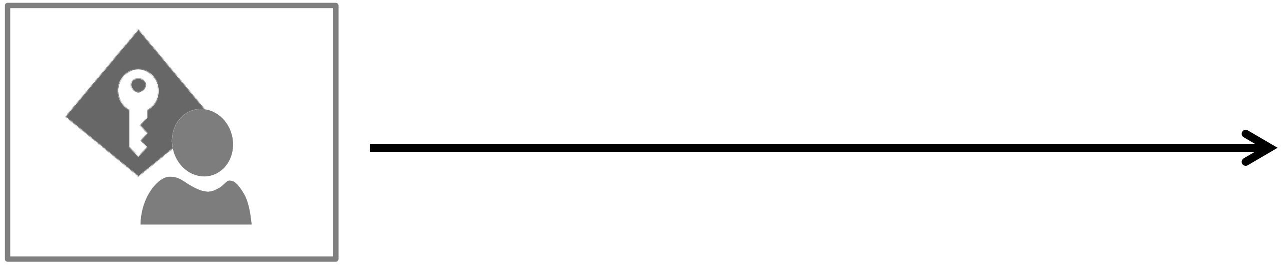
PARTNERS Domain

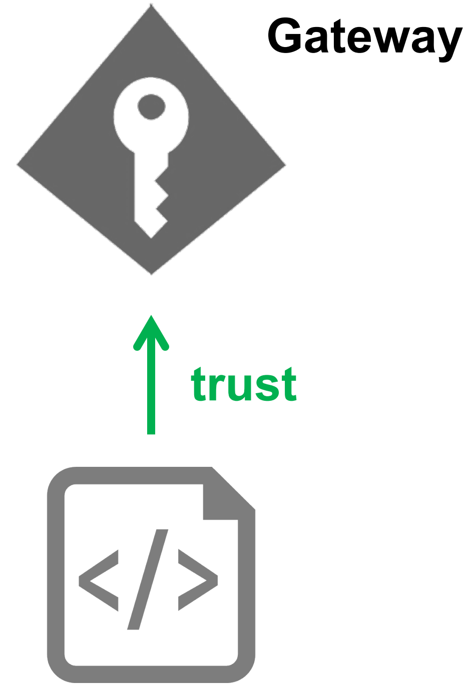
Windows Live ID

Federated Account

Why am I seeing this page?

next





Sending a home realm hint from client to provider

- **Unfortunately, no dedicated parameter in OpenID Connect**
  - Azure AD uses *domain_hint*
  - IdentityServer uses *acr_values*

Example: IdentityServer

```
https://idsrv/connect/authorize/?
  client_id=myapp&
  redirect_uri=https://www.myapp.com
  &acr_values=idp:ext_idp
```

Summary

- **In practice, external authentication is combined with some simple patterns**
  - single sign-on / off
  - federation
  - home realm discovery
- **Clients shouldn't trust more than one provider**
  - use the federation gateway pattern
- **Choose a strategy for HRD**
  - hint from user
  - hint from environment
  - hint from client