

Nico Urbanczyk  
Plattformen & Serverdienste

# Authentifizierung Shibboleth Identity Provider

[Kolloquium-Wi] 15.1.

IdP, SP, Shibboleth, SAML, ...

und wie hängt das alles zusammen?

# Agenda

- Begrifflichkeiten
- Authentifizierung (Ablauf)
  - Logisch
  - Technisch
- Strategische Ausrichtung
- Beispiel

# Begrifflichkeiten

Begrifflichkeiten | Authentifizierung | Strategie | Beispiel

1. Provisionierung
- 2. Authentifizierung**
  - IdP / SP / P / DS
  - Shibboleth
  - SAML
  - SSO
3. Autorisierung

# Provisionierung

Begrifflichkeiten | Authentifizierung | Strategie | Beispiel

- „Versorgungsprozess“
- Personendaten
- Add / Mod / Del / Suspend
- Accounts

# Autorisierung

Begrifflichkeiten | Authentifizierung | Strategie | Beispiel

„Was darf ich?“

- Rechte
- Rollen



# Authentifizierung

Begrifflichkeiten | Authentifizierung | Strategie | Beispiel

## „Wer bin ich?“

- Identity Provider (IdP) **!=** IdM
- Service Provider (SP)
- Principal (P)
- *Discovery Service (DS)*

# Discorvery Service

Begrifflichkeiten | Authentifizierung | Strategie | Beispiel



The screenshot shows a web browser window with the URL <https://shibboleth.net/shibboleth>. The page features the Shibboleth logo, which is a stylized orange and red phoenix-like creature. Below the logo, the text reads "Choose an Identity Provider". A paragraph explains that users should select their home organization, or "ProtectNetwork" if not supported. A dropdown menu is open, showing a list of institutions with "Universität Münster" selected. An "OK" button is visible next to the dropdown.

Choose an Identity Provider

In order to log in to this service, please select the home organization with which you're affiliated. If your organization is not supported, you may select **ProtectNetwork** and create a free account there for our services.

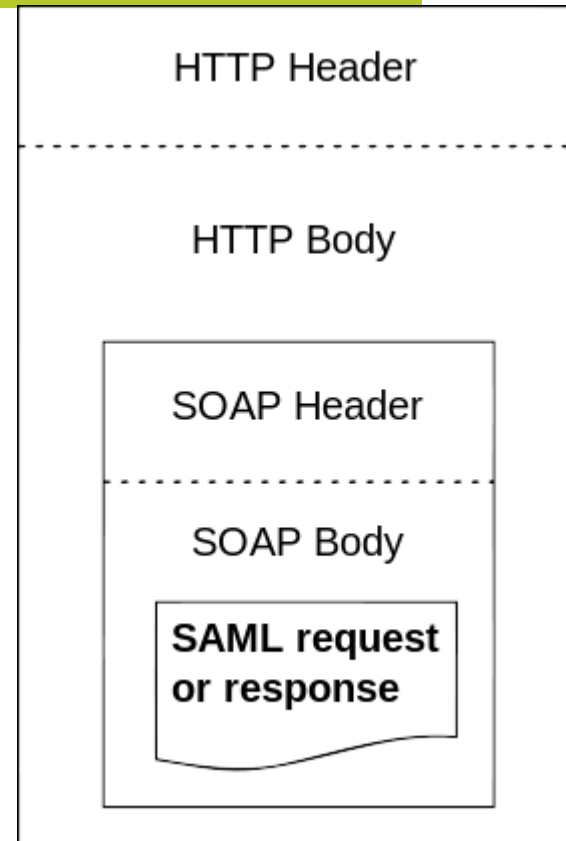
Institution aus folgender Liste wählen:

- University Campus Suffolk
- Universität Frankfurt
- Universität Jaume I
- Universität Mainz
- Universität Münster
- Universität Oberta de Catalunya
- Universität of Munich (LMU)
- Universität Politècnica de Catalunya
- Universität Politècnica de València
- Universität Pompeu Fabra

# Authentifizierung

Begrifflichkeiten | Authentifizierung | Strategie | Beispiel

- Shibboleth
  - SP
  - IdP
- (Open)SAML
- **Single-Sign-On**



Quelle: <http://en.wikipedia.org/wiki/File:Sam1-over-soap-over-http.gif>



# Authentifizierung

Begrifflichkeiten | Authentifizierung | Strategie | Beispiel

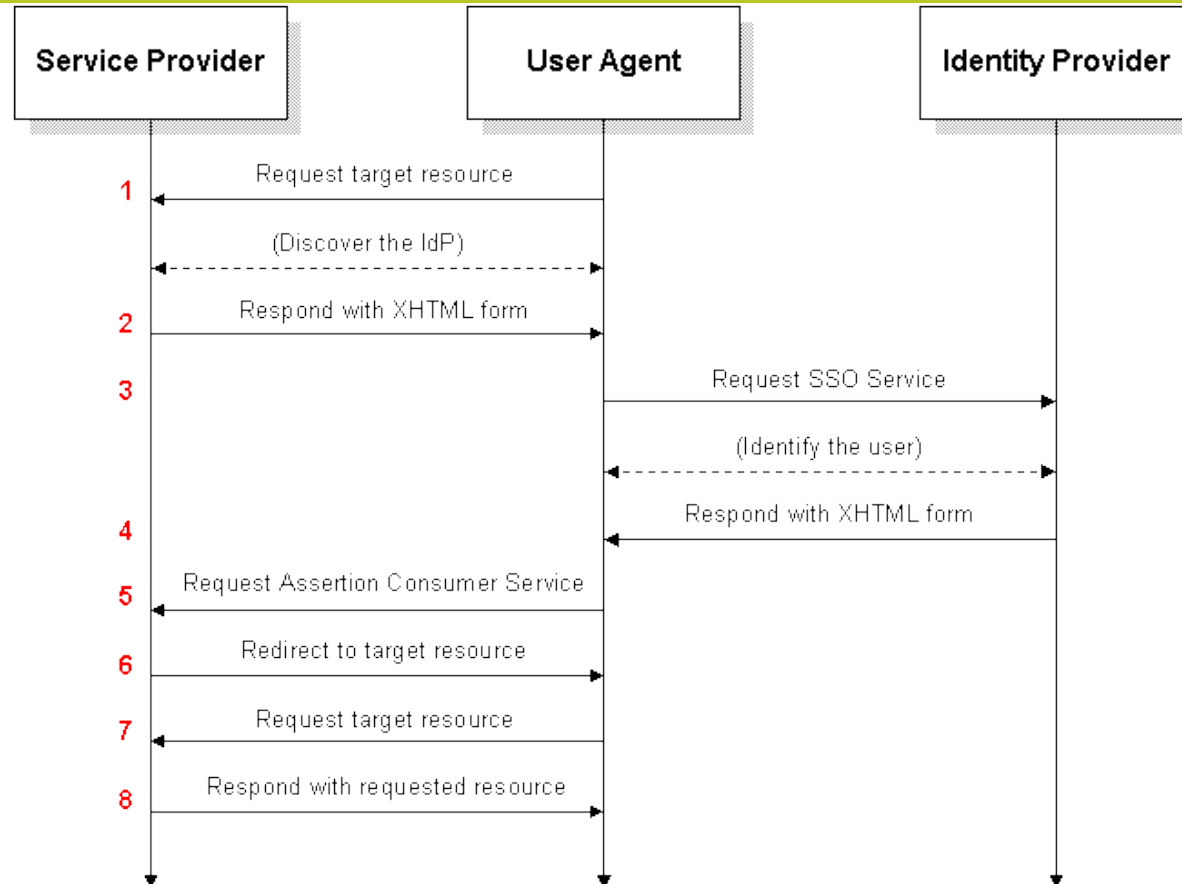
P

SP

IdP

# Authentifizierung

Begrifflichkeiten | Authentifizierung | Strategie | Beispiel

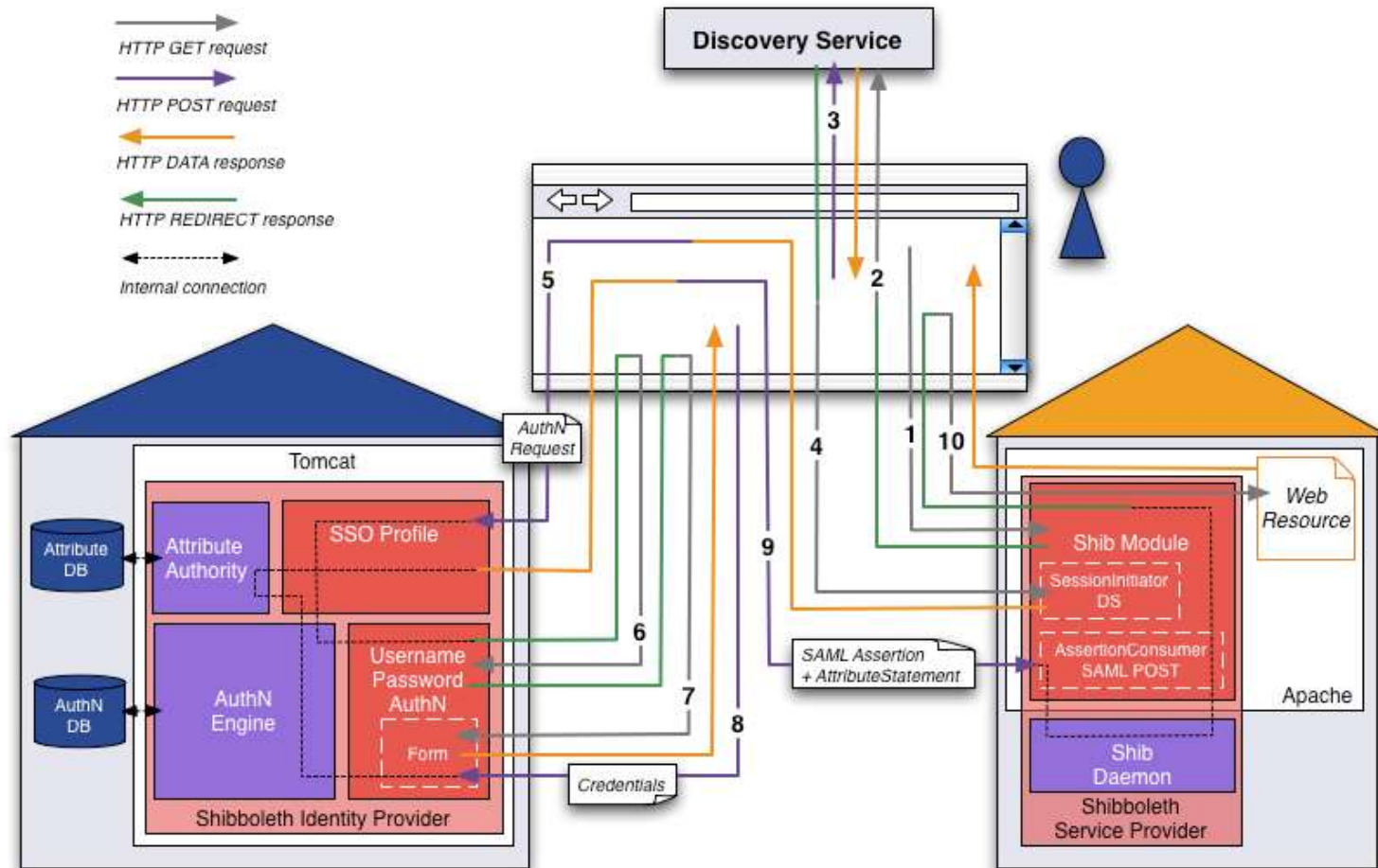


Quelle: <http://en.wikipedia.org/wiki/File:Saml2-browser-ss-post.gif>

# Ich will mehr!


Begrifflichkeiten | Authentifizierung | Strategie | Beispiel

<https://www.switch.ch/aai/demo/expert/>



# Strategische Ausrichtung

Begrifflichkeiten | Authentifizierung | Strategie | Beispiel

- Etablierung  IdP-Service
- Teil einer Gesamtlösung
- Zentral
  - Benutzerdaten
  - Authentifizierung
- Überführung vom BIS IdP
  - PVP
  - DFN-AAI

# Strategische Ausrichtung

Begrifflichkeiten | Authentifizierung | Strategie | Beispiel

- Für (alle) Webressourcen
- Keine lokalen Benutzer / Passwort DBs
- Föderiertes SSO
- DFN-AAI  
Authentifikations- und Autorisierungs-  
Infrastruktur



# Beispiel

Begrifflichkeiten | Authentifizierung | Strategie | Beispiel



Danke für ihre Aufmerksamkeit!

