Mathias Roland

mathias.roland@cms.hu-berlin.de

Humboldt-Universität zu Berlin
Computer- und Medienservice

2008-02-26

Inhalt

- Bibelstunde
- Wer und Was?
- Komponenten
- Nutzerdaten
- Ablauf (schematisch und technisch)
- Links und Fragen

Bibelstunde

- AT Buch Richter Kapitel 12 Vers 5 und 6:
  - (5) und die Gileaditer besetzten die Furten des Jordans vor Ephraim. Wenn nun einer von den Flüchtlingen Ephraims sprach: Lass mich hinübergehen!, so sprachen die Männer von Gilead zu ihm: Bist du ein Ephraimiter? Wenn er dann antwortete: Nein!,
  - (6) ließen sie ihn sprechen: Schibboleth. Sprach er aber: Sibbolet, weil er's nicht richtig aussprechen konnte, dann ergriffen sie ihn und erschlugen ihn an den Furten des Jordans, sodass zu der Zeit von Ephraim fielen zweiundvierzigtausend.

Wer und Was?

- Middleware Architecture Committee for Education (MACE) des Internet2-Konsortiums
- Authentifzierung, Authorisierung und Datenaustausch (im WWW)
- Single-Sign-On/Logout (organisationsintern und/oder organisationsübergreifend)
- HTTP / HTML / XML / SAML (=Security Assertion Markup Language)
  - Shibboleth hat eigene Profile (eduPerson)
- aktuell: Version 1.3 unter Apache-2.0-Lizenz

Komponenten (1)

- IdP (Identity Provider)
  - verwaltet Nutzerdaten
- SP (Service Provider)
  - geschützte Ressource
- WAYF-Service („Where Are You From?“)
  - optionale Komponente
  - Bestimmung des Identity Providers

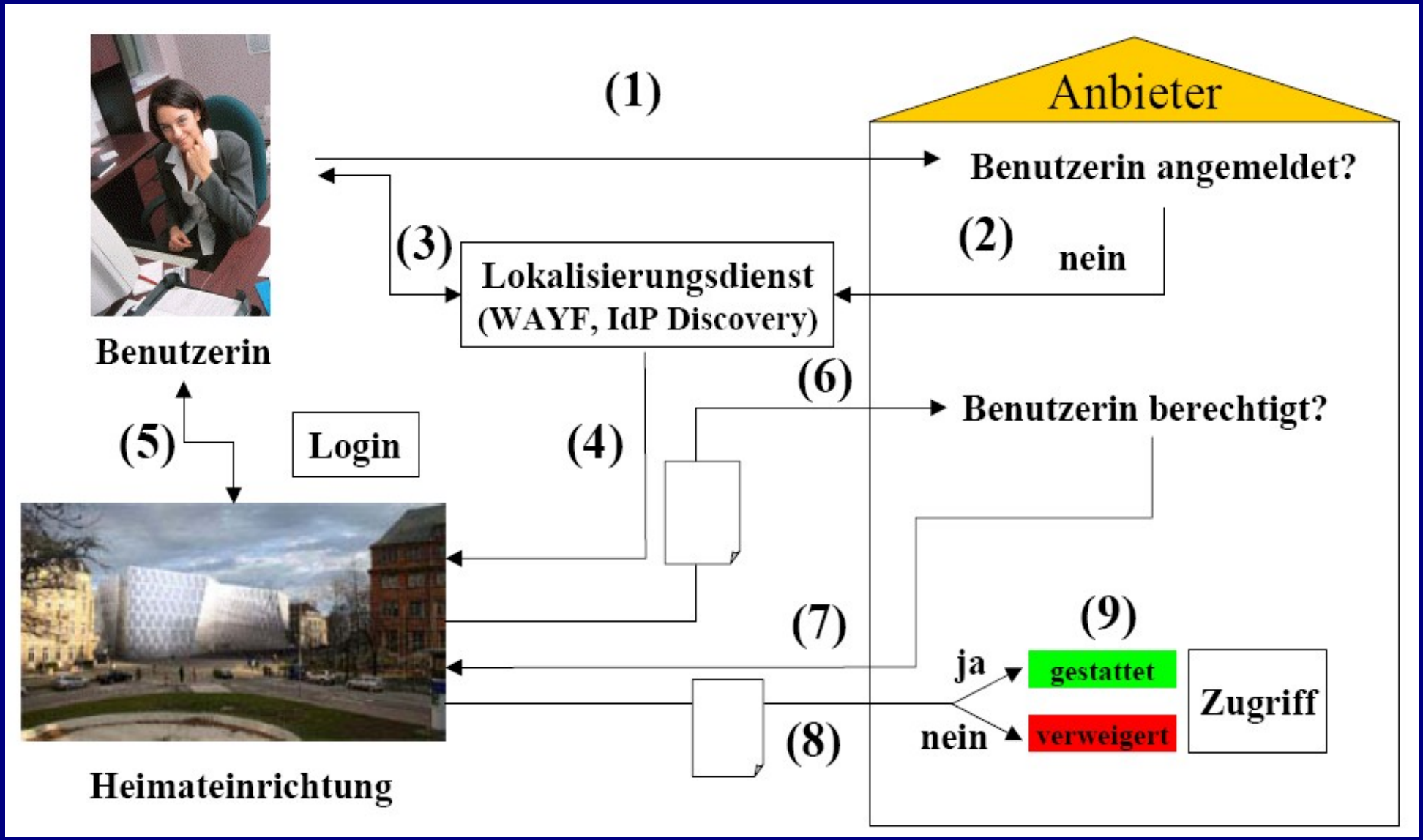
Komponenten (2)

- Metadaten
  - XML-Liste
  - eindeutige Name der SPs und IdPs
  - öffentliche Schlüssel/Zertifikate von SPs und IdPs
  - Aktualisierung auf allen System
- AAI (=Authentication and Authorization Infrastructure)
  - Metadatenverwaltung
  - Regeln für Profile, Attribute und Werte
- Förderation

Nutzerdaten

- nach Authentifikation beim IdP
- Übertragung vom IdP zum SP mit Hilfe des Browser des Nutzers
- verschlüsselte und signierte XML-Daten (Zertifikate aus Metadaten)
- Filter auf IdP-Seite und SP-Seite
  - Profil / Attribute / Werte
  - Datenschutz!

Ablauf (schematisch)



Ablauf (2)

- Schritt 1: Aufruf einer Ressource: https://sp.example.org/ressource
- Schritt 2: Umleitung auf Identitätsprovider: https://idp.example.org/shibboleth/SSO?target=https://sp.example.org/myresource&shire=https://sp.example.org/shibboleth/SSO/POST&providerId=https://sp.example.org/shibboleth
  - target = angefragte Ressource
  - shire = shibboleth-Komponente auf SP-Seite
  - providerId = eindeutiger Name für Zertifikat

Ablauf (3)

- Schritt 3: Authentifiziertung beim IdP
- Schritt 4: Antwort vom IdP:

```
<form method="post"
action="https://sp.example.org/shibboleth/SSO/POST"
...>
    <input name="TARGET" type="hidden"
        value="https://sp.example.org/myresource/">
    <input name="SAMLResponse" value="XXX"
        type="hidden"/> ...
    <input type="submit" value="Submit"/>
</form>
```

  - XXX = verschlüsselte XML-Daten
  - Javascript zum automatischen Abschicken

Ablauf (4)

- Schritt 5: Überprüfung der Daten durch Shibboleth-Komponente des SP und Erzeugung von Sitzungsinformationen für Ressource
- Schritt 6: Weiterleitung an Ressource
- Schritt 7: Zugang zur Ressource durch Nutzer

Ende

- Shibboleth
  http://shibboleth.internet2.edu
- DFN-AAI
  http://www.aai.dfn.de

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?