Einführung in Shibboleth

07.02.2008, Stuttgart

Franck Borel - UB Freiburg

Übersicht

- Was ist Shibboleth?
- Warum Shibboleth?
- Wie funktioniert Shibboleth?
- Attribute
- Metadaten
- Föderation

Was ist Shibboleth?

- **Shibboleth** ist ein einrichtungsübergreifender **SSO-Dienst** für den Zugriff auf geschützte **Web-Ressourcen**
- Wird von Internet2 entwickelt
  → http://shibboleth.internet2.edu
- Basiert auf SAML:
  Security **A**ssertion **M**arkup **L**anguage
- Open-Source Lizenz

Warum Shibboleth?

- **Nutzer**
  - Zugriff auf Dienste von überall her
  - Alle Dienste sollen nach einmaliger Authentifizierung und Autorisierung zur Verfügung stehen (**Single Sign-On**).
- **Einrichtungen** (etwa Hochschulen)
  - bestehende Benutzerverwaltung nutzen
  - Einfache Anbindung an die bestehende Benutzerverwaltung
- **Anbieter**
  - Schützen der lizenzpflichtigen Inhalte
  - Keine eigene Benutzerverwaltung
  - Kontrolle über die Nutzung (wer darf was?)

Ursprung des Wortes "Shibboleth"

Hintergrund ist eine Stelle aus dem **Alten Testament**, Buch Richter Kapitel 12 Vers 5ff

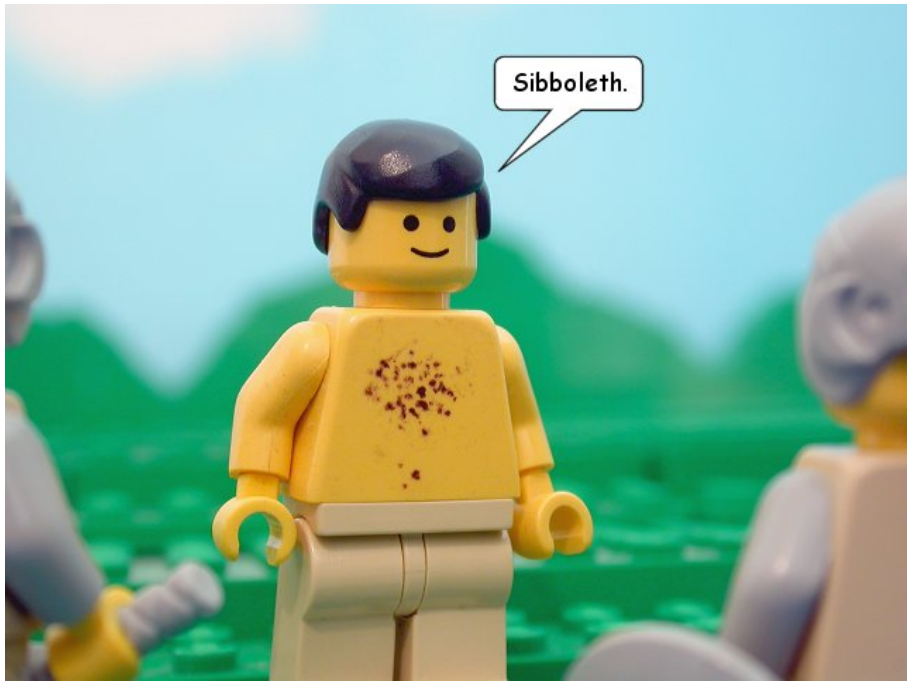
Ursprung des Wortes "Shibboleth"

Und die ***Gileaditer*** nahmen ein die Furt des Jordans vor Ephraim. Wenn nun sprachen die Flüchtigen Ephraims: Laß mich hinübergehen, so sprachen die Männer von Gilead zu ihm: Bist du ein ***Ephraiter***? Wenn er dann antwortete: Nein...

Ursprung des Wortes "Shibboleth"

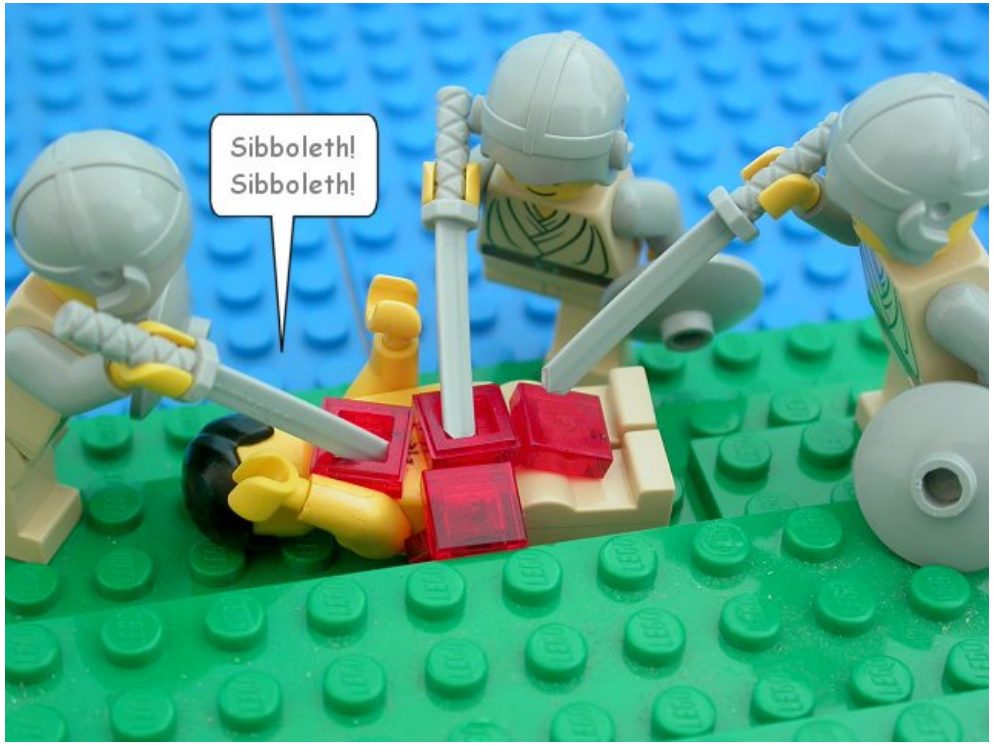
...so hießen sie ihn sprechen: *Schiboleth*

Ursprung des Wortes "Shibboleth"



...so sprach er: *Siboleth*, und konnte es nicht recht reden.

Ursprung des Wortes "Shibboleth"



So griffen sie ihn und schlugen ihn an der Furt des Jordans...

Ursprung des Wortes "Shibboleth"

der Zeit von Ephraim fielen zweiundvierzigtausend.

Ursprung des Wortes "Shibboleth"

- „Shibboleth“ ist somit wohl das erste biometrische Autorisierungsverfahren gewesen.

Wie funktioniert Shibboleth?

Benutzerin

(1)

(3)

Anbieter

Benutzerin angemeldet?

(2) nein

Lokalisierungsdienst
(Discovery-Service)

(6)

Benutzerin berechtigt?

(5)

Login

(4)

Heimateinrichtung

(7)

(9)

ja

gestattet

Zugriff

nein

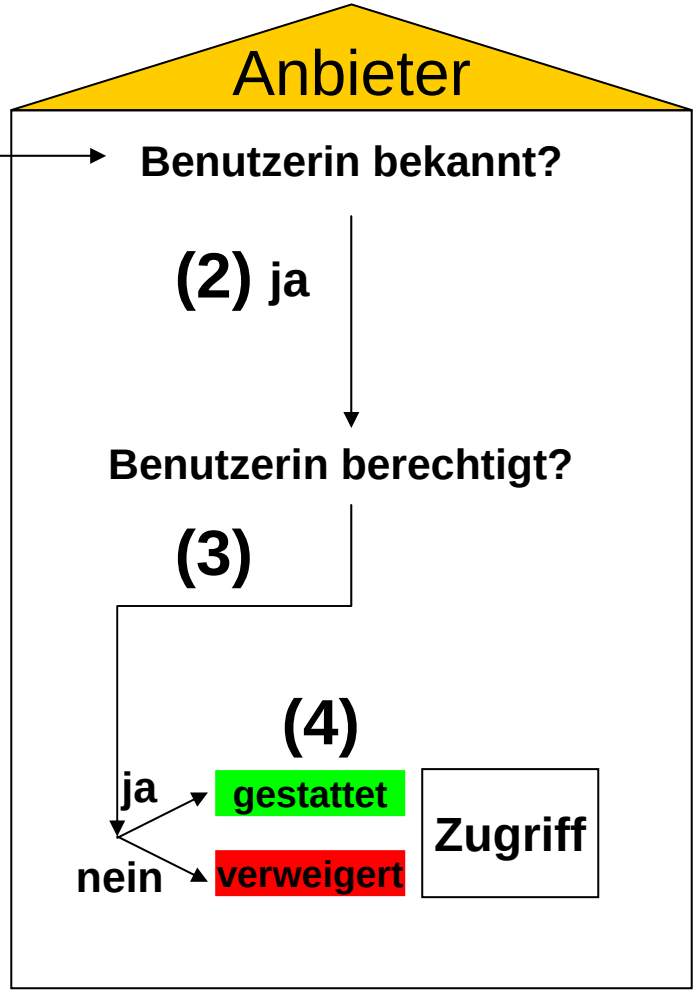
verweigert

(8)

Wie funktioniert Shibboleth?

Benutzerin

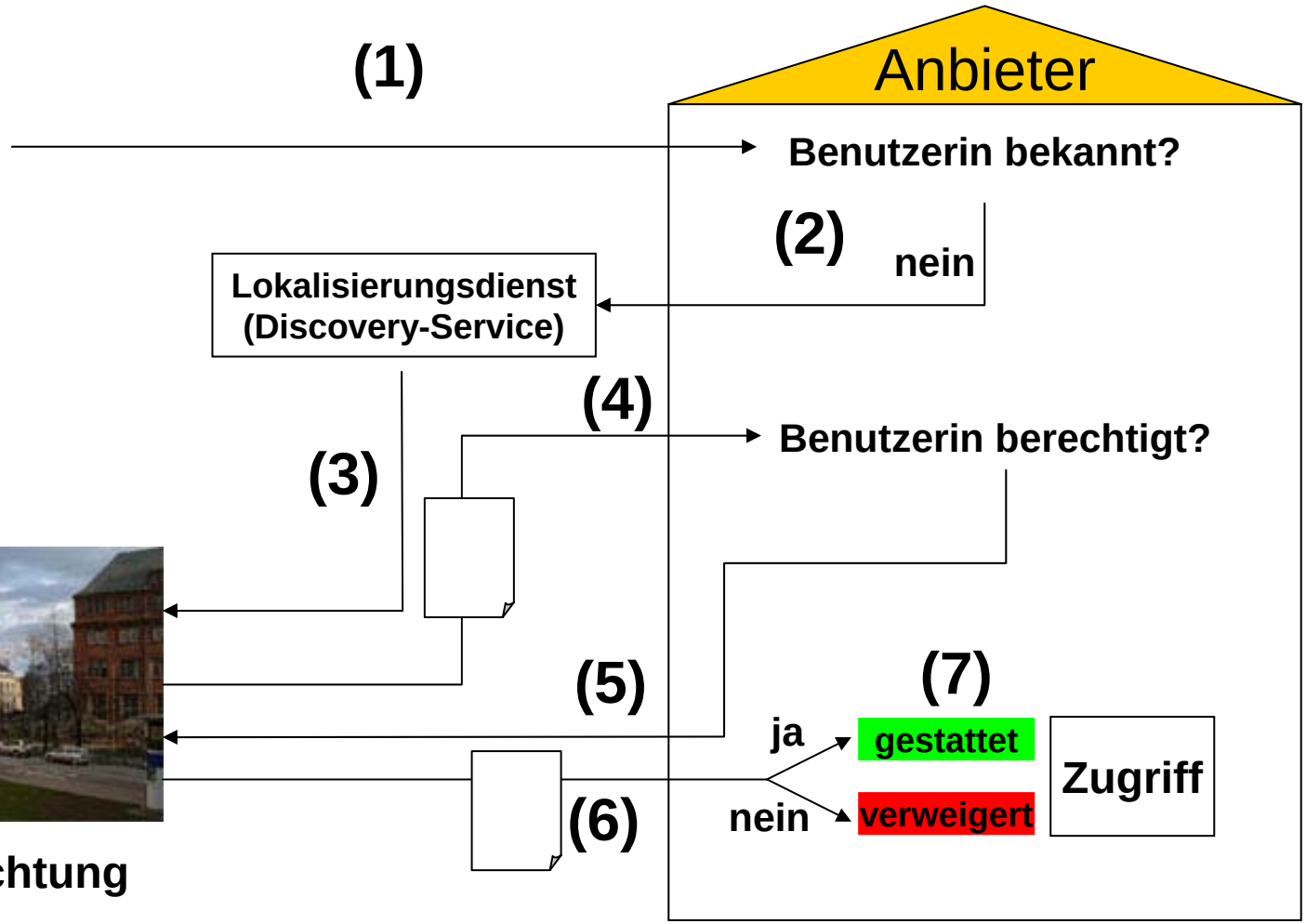
(1)



Wie funktioniert Shibboleth?

Benutzerin

Heimateinrichtung



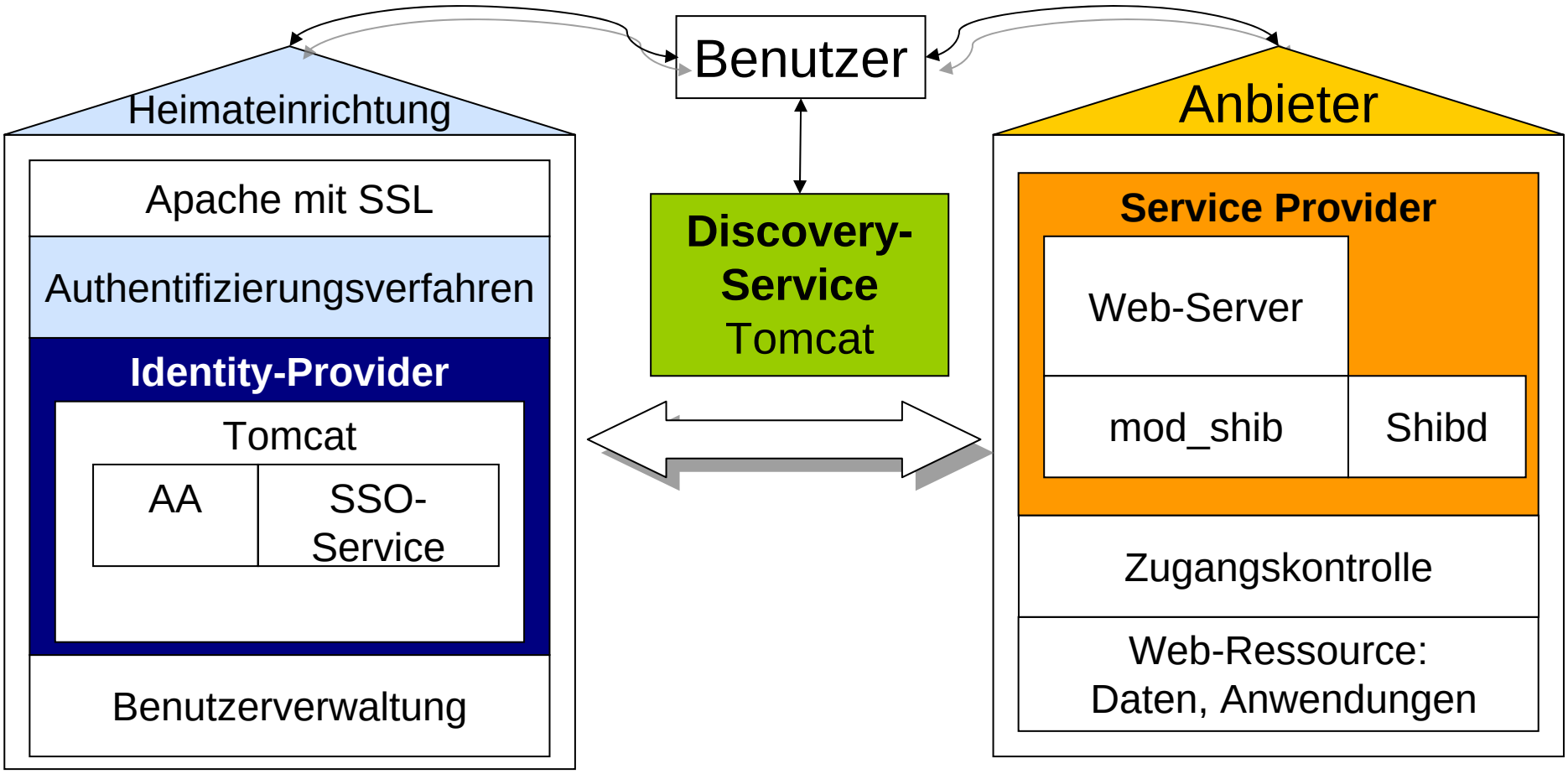
Wie funktioniert Shibboleth?

- Bestandteile:
  - Identity-Provider (bei der Heimateinrichtung)
    - Authentifizierung (frei wählbar)
      - Benutzerverwaltung (frei wählbar)
    - Autorisierung (Bestandteil von Shibboleth)
      - Benutzerverwaltung (frei wählbar)
  - Service-Provider (beim Anbieter)
    - Zugriffskontrolle
      - Erwartet:
        - » Erfolgreiche Authentifizierung
        - » Attribute
  - Discovery-Service (Lokalisierungsdienst)
    - optional
    - Liste mit Einrichtungen
    - Als selbständiger Dienst oder beim Anbieter

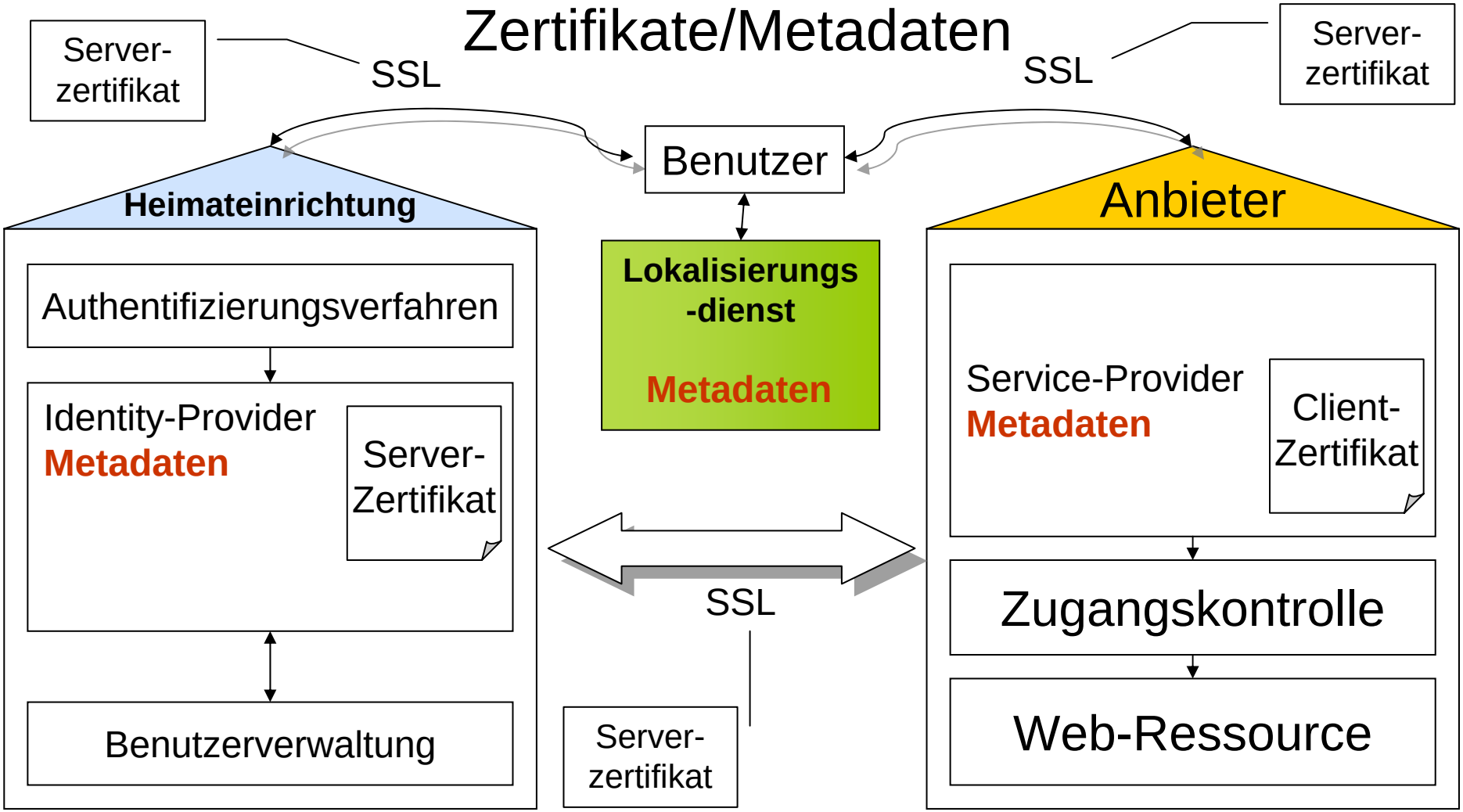
Bestandteile/Software

- Unterstützte Betriebssysteme:
  - Linux
  - Solaris
  - Windows
  - Mac OS-X
- Typische Software unter Linux:
  - Identity Provider:
    - Tomcat 5.5
    - Apache 2.2 mit mod_ssl und mod_jk (Verbindung zum Tomcat)
    - JDK 1.5
  - Service Provider:
    - Apache + mod_ssl (für HTTPS)

Bestandteile



Wie funktioniert Shibboleth?



Attribute

- **Attribute** bilden die Grundlage für die **Autorisierung und Zugriffskontrolle** in Shibboleth:
  - Identity-Provider stellen mit Attributen die notwendigen Informationen über ihre Benutzer zur Verfügung.
  - Service-Provider werten die Attribute anhand ihrer Regeln aus und gestatten oder verweigern je nach Ergebnis den Zugriff.
- Hierfür sind **Absprachen zwischen Identity- und Service-Providern** notwendig, die durch Verwendung eines einheitlichen Schemas vereinfacht werden!
- Voraussetzung sind verlässliche Benutzerdaten, also eine funktionierende **Benutzerverwaltung**

eduPerson-Schema

- Schemata legen eine Menge von Attributen, die zulässigen Werte und deren Bedeutung fest.
- **InCommon** empfiehlt das auf eduPerson basierende Schema für den Austausch von Attributen: http://www.incommonfederation.org/docs/policies/federatedattributes.pdf
- **Andere Föderationen** und **internationale Anbieter** orientieren sich üblicherweise an dieses Schema:
  - eduPerson (InCommon)
  - swissEduPerson (SWITCH)
  - funetEduPerson (HAKA)

eduPerson-Schema

- **Service-Provider** kommen mit **wenigen Attributen** aus, häufig verwendet werden:
  - eduPersonAffiliation
  - **eduPersonEntitlement**
  - eduPersonPrincipalName
  - eduPersonTargetedID

eduPersonScopedAffiliation

- Ermöglicht die Zuordnung der Nutzer einer Einrichtung zu einigen grundlegenden Rollen.
- Zulässige Werte sind: **member**, **faculty**, **staff**, **employee**, **student**, **alum** und **affiliate**.
- Beispiel: **member@uni-freiburg.de**
- Probleme:
  - Die Bedeutung der Werte ist auf internationaler Ebene nicht wirklich einheitlich festgelegt (z.B.: Was ist ein *student*?).
  - Es fehlen wichtige Rollen wie Gastbenutzer.

eduPersonEntitlement

- Ermöglicht den Austausch beliebiger Benutzerinformationen.
- Zulässige Werte: URIs, d.h. URNs oder URLs, wobei meistens URNs verwendet werden.
- Die Bedeutung der Entitlement-Werte muss zwischen Identity- und Service-Providern abgesprochen werden
- Absprachen auf Föderationsebene oder sogar föderationsübergreifend sind wünschenswert!

eduPersonEntitlement

- Wichtigster Entitlementwert im Bibliotheksbereich: **urn:mace:dir:entitlement:common-lib-terms**
- Bedeutung: „Nutzer ist berechtigt, die von seiner Einrichtung im Rahmen einer Standardlizenz lizenzierten Inhalte zu nutzen“ (bei Hochschulen: Mitglied der Hochschule oder Walk-in Patron).
- Die meisten (kommerziellen) Anbieter unterstützen oder erwarten sogar, dass dieser Entitlementwert in Standardfällen verwendet wird.

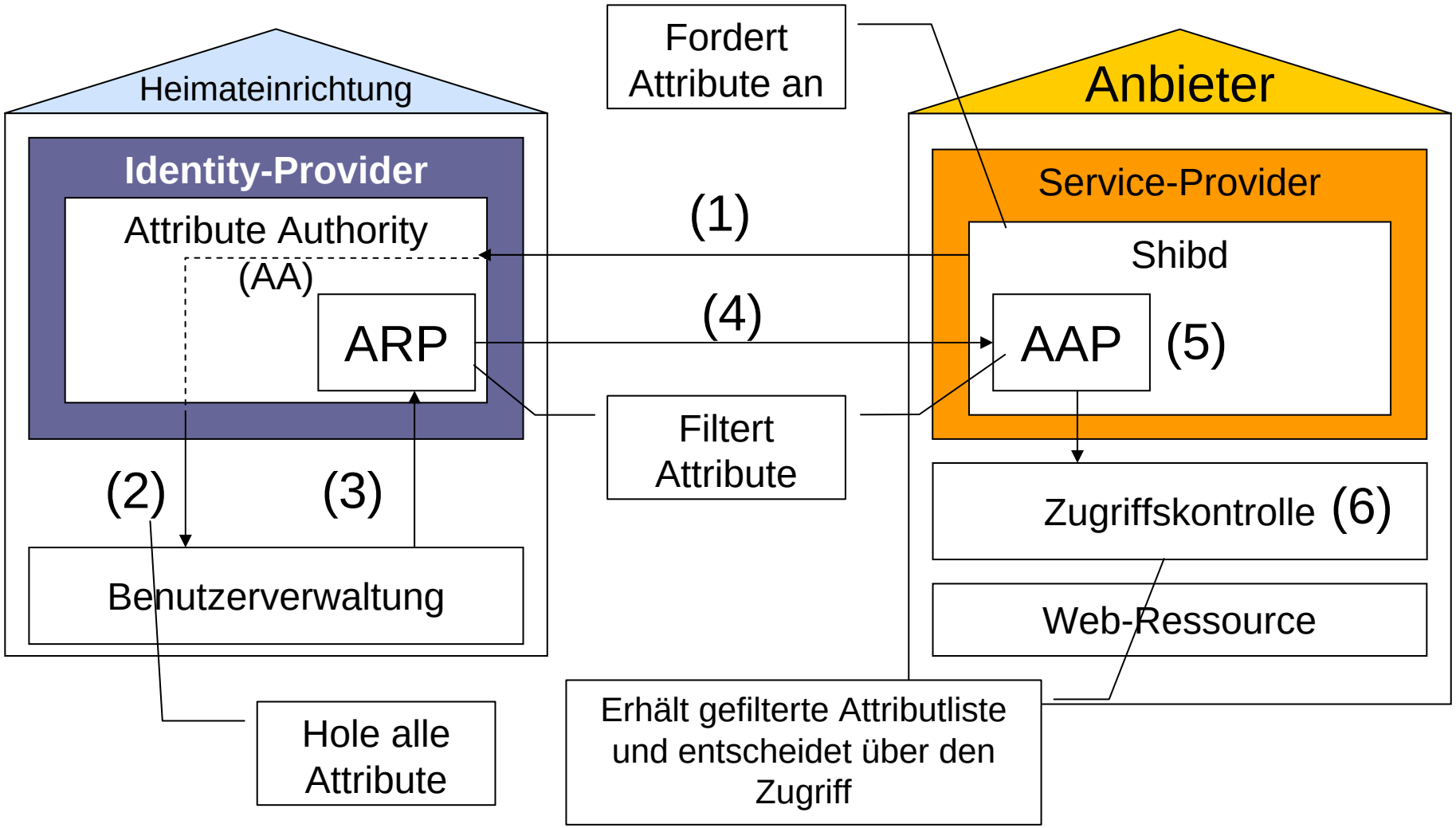
eduPersonPrincipalName

- Eindeutige, persistente Identität des Nutzers inklusive Domain („NetID“).
- Beispiel: borel@**uni-freiburg.de**
- Sollte aus Datenschutzgründen nur verwendet werden, wenn die Nutzung eines Dienstes nicht anonym oder pseudonym erfolgen kann!
- Beispiel: Schreibender Zugriff auf eine Anwendung, z.B. ein Wiki oder Forum, für den der Nutzer sich zu erkennen geben muss.

eduPersonTargetedID

- Eindeutiges, persistentes Pseudonym des Nutzers für einen Service-Provider.
- Ermöglicht die Wiedererkennung des Nutzers (z.B. für personalisierte Anwendungen), ohne seine Identität kennen zu müssen.

Attribute und Zugriffskontrolle



Attribute generieren: Resolver

Der **Resolver** des Identity-Providers **erzeugt die Attributliste** für den gegebenen Benutzer.

- Shibboleth bietet hierfür einige Standard-**Konnektoren**: echo, static, JDBC, LDAP
- Bei Bedarf können eigene Konnektoren implementiert werden.
- Beispiele:
  - eduPersonPrincipalName: echo
  - eduPersonEntitlement: JDBC

Attribute filtern im IdP: ARPs

- Die vom Resolver erzeugte **Attributliste** wird über die **Attribute Release Policy** (ARP) für den anfragenden Service-Provider **gefiltert**.
- Die Filterung erfolgt dreistufig:
  - Site-ARP: einrichtungsweit
  - (Group-ARP: auf Gruppenebene)
  - User-ARP: benutzerspezifisch
- Das Ergebnis erhält der Service-Provider in Form einer Quittung (*attribute **assertion***).

Attribute filtern im SP: AAP

Die **Attribute Acceptance Policy** (AAP) des Service-Providers legt fest:

- welche **Attribute und Attributwerte** von welchen Identity-Providern **akzeptiert** werden
- wie diese für die **Zugriffskontrolle** an den Ressource-Manager bzw. die Anwendung **weitergegeben** werden

Zugriffskontrolle

- Die vom IdP gelieferten und über die AAP **aufbereiteten Attribute** bilden die **Basis für die Zugriffskontrolle**
- **Shibboleth** bietet **Ressource-Manager** für Apache (Apache Access Control über mod_shib)
- Alternative ist ein **eigener Ressource-Manager** in der Anwendung: Attribute werden über HTTP-Header an die Anwendung übergeben.
- Beispiel ReDI: eduPersonEntitlements werden auf ReDI eigene Benutzergruppen abgebildet.

Metadaten

- Die Metadaten bilden die Föderation auf technischer Ebene ab
- Sie beinhalten eine vollständige Liste aller teilnehmenden Provider (IdP, SP)
- Zertifikate und providerID garantieren, dass die Provider immer wissen, wer gerade mit Ihm spricht
- Metadaten werden signiert, um Ihre Authentizität und Integrität zu gewährleisten
- Metadaten müssen aktuell sein, sonst klappt die Interoperabilität nicht
- Beispiel: http://aar.vascoda.de/test/DEMO2-metadata.xml

Föderation

- Eine **Föderation** ist ein Zusammenschluss von Einrichtungen und Anbietern auf Basis **gemeinsamer Richtlinien**.
- Eine Föderation schafft das notwendige **Vertrauen** zwischen Einrichtungen und Anbietern und den **organisatorischen Rahmen** für den Austausch von Benutzerinformationen.
- die **deutschlandweite Föderation** (**DFN-AAI**) läuft unter der Koordination des DFNs

Föderationen weltweit

- Australien (MAMS)
- Dänemark (DK-AAI)
- **Deutschland (DFN-AAI)**
- Finnland (HAKA)
- Frankreich (CRU)
- Norwegen (FEIDE)
- Schweden (SWAMID)
- Schweiz (SWITCH)
- UK (SDSS)
- US (InCommon)

Einsatzmöglichkeiten von Shibboleth

- Zugang zu geschützten (auch und gerade kommerziellen) elektronischen Informationsangeboten:
  - E-Zeitschriften, Datenbanken, E-Bücher, ...
  - Portale (z.B. vascoda, **ReDI**)
  - DFG-Nationallizenzen
  - Repositories (z.B. EPrint, DSpace)
  - **Informationsdienste**
- e-Learning
- e-Science
- **Verwaltungssysteme**
- Grid-Computing

Danke für Ihre Aufmerksamkeit!

AAR ist ein Projekt der

UB Freiburg

Gefördert vom BMBF (PT-NMB+F)

aar.vascoda.de

info@aar.vascoda.de

borel@ub.uni-freiburg.de