Wie funktioniert Shibboleth? Ein technischer Überblick

3. AAR-Workshop

Freiburg, 10. Oktober 2006

Franck Borel, UB Freiburg
E-Mail: borel@ub.uni-freiburg.de

Übersicht

- Was ist Shibboleth?
- Warum Shibboleth?
- Wie funktioniert Shibboleth?
- Identity-Management und Shibboleth
- Autorisierung und Zugriffskontrolle
- Föderation
- Ausblick: Shibboleth 2.0

Was ist Shibboleth?

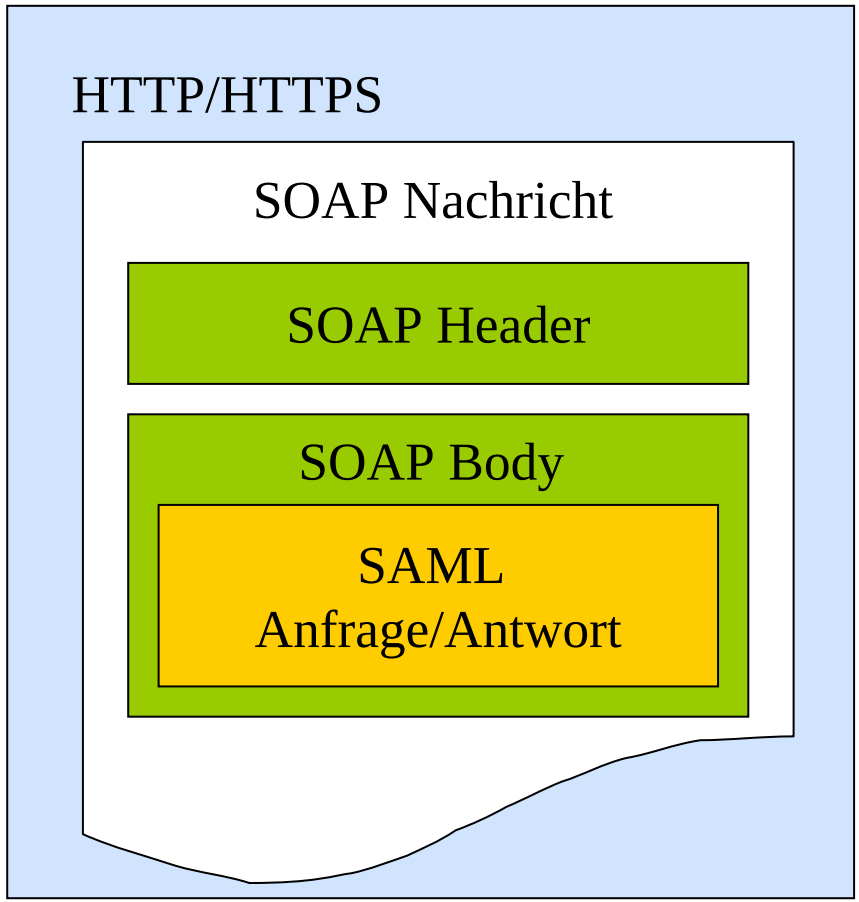
- **Shibboleth** ist ein **Internet2/MACE-**Projekt
  (MACE = Middleware Architecture Committee for Education)
- **Shibboleth** ist ein einrichtungsübergreifender **SSO-Dienst** für den Zugriff auf geschützte **Web-Ressourcen**

Warum Shibboleth?

- Autorisierung und Zugriffskontrolle erfolgt über **Attribute** mit der Möglichkeit zur **anonymen/pseudonymen Nutzung** von Angeboten
- **Aufwand für Integration** mit vorhandenem Identity-Management und webbasierten Anwendungen ist **vergleichsweise gering**
- **weltweit hohe Akzeptanz**, auch bei kommerziellen Anbietern (Elsevier, JSTOR, EBSCO, CSA, Ovid, GENIOS...)
- **Open-Source**
- basiert auf **bewährter Software** (Apache, Tomcat, OpenSSL) **und Standards...**

Wie funktioniert Shibboleth?

- Shibboleth baut auf folgende Standards auf:
  - SSL/TSL
  - HTTP/HTTPS
  - XML
  - XML Schema (XSD)
  - XML Signatur (XMLDisg)
  - SOAP
  - SAML (**S**ecurity **A**ssertion **M**arkup **L**anguage)



Wie funktioniert Shibboleth?

- Sicherheitsmechanismen
  - SSL/TSL: *Man-in-the-Middle*, *Manipulieren von Nachrichten*, *Lauschangriff*
  - XMLsig: *Manipulieren von Nachrichten*
  - Eingeschränkte Gültigkeitsdauer von Sitzungen, Bestätigungen, Attributen (engl. *Lifetime*, *TTL)*: *Wiederverwendung von Sitzungsdaten*, *DoS*
  - Metadaten: *DoS*, *Manipulieren von Nachrichten*
  - Es werden keine personenbezogenen Daten übermittelt, sondern Stellvertreter (engl. *Handler)*: *Lauschangriff*

Wie funktioniert Shibboleth?

Benutzerin

Erstkontakt

(1)

Anbieter

Benutzerin angemeldet?

(2) nein

(3)

Lokalisierungsdienst
(WAYF, IdP Discovery)

(4)

(5)

Login

(6)

Benutzerin berechtigt?

Heimateinrichtung

(7)

(8)

(9)

ja

gestattet

nein

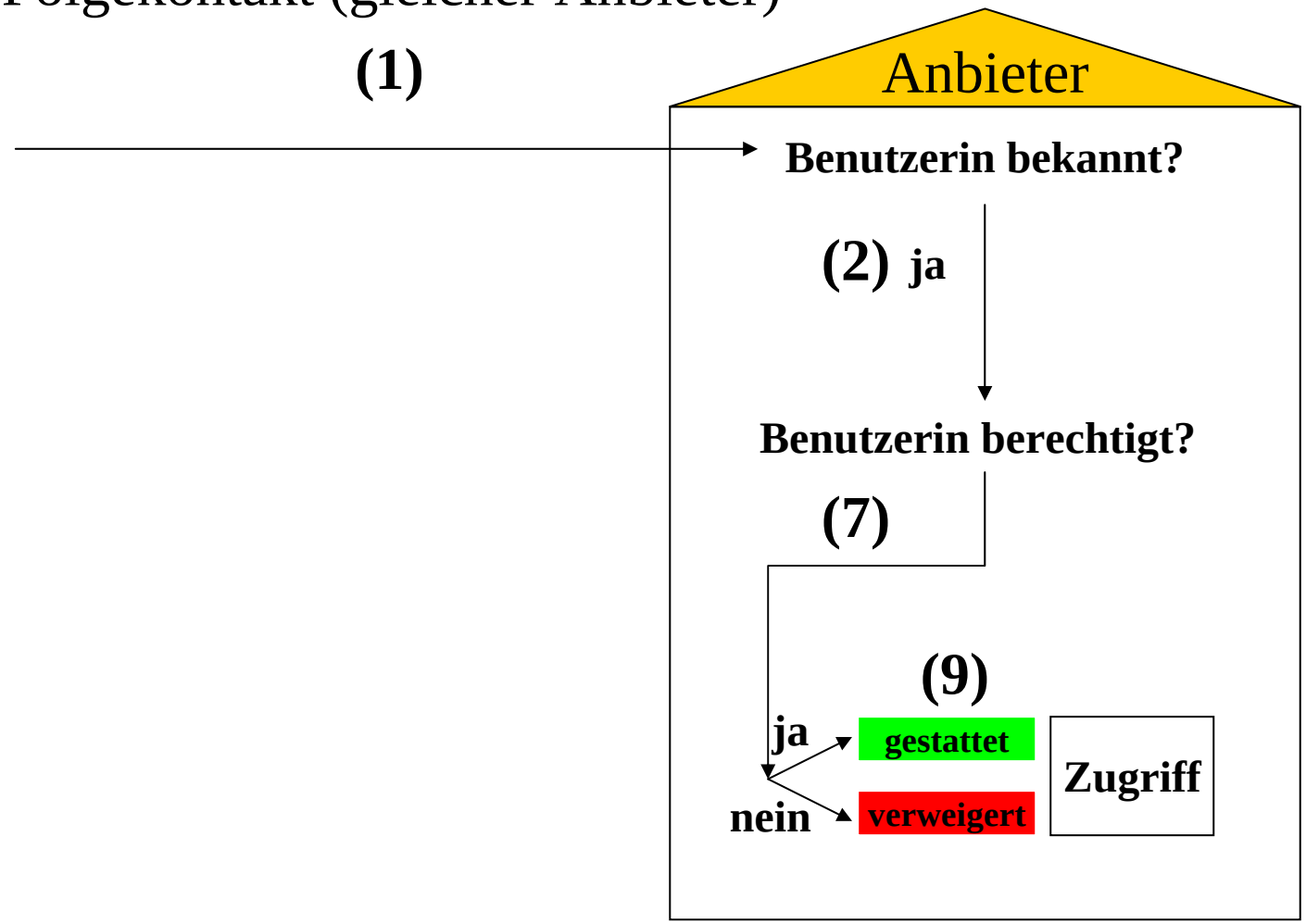
verweigert

Zugriff

Wie funktioniert Shibboleth?

Folgekontakt (gleicher Anbieter)

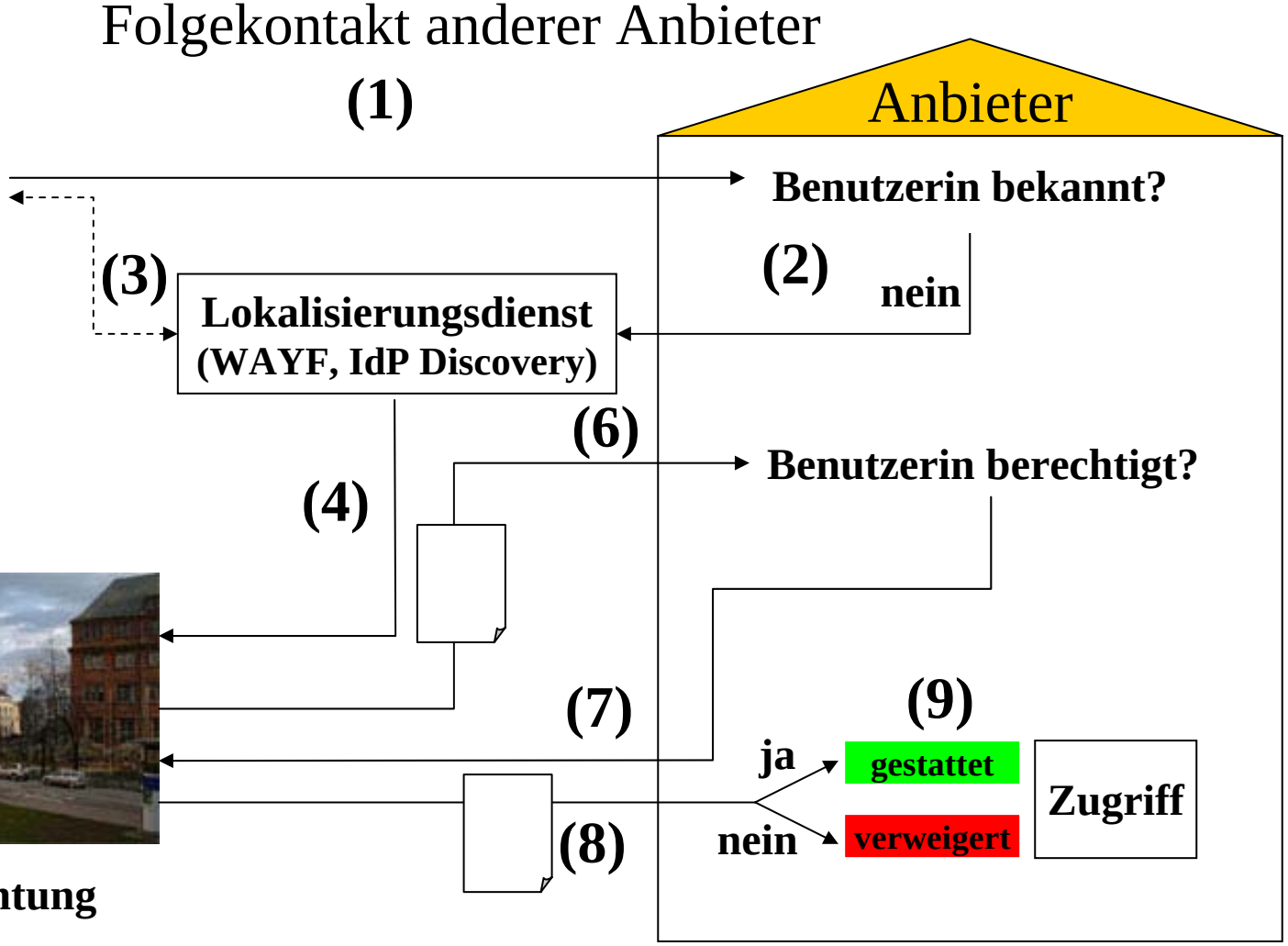
Benutzerin



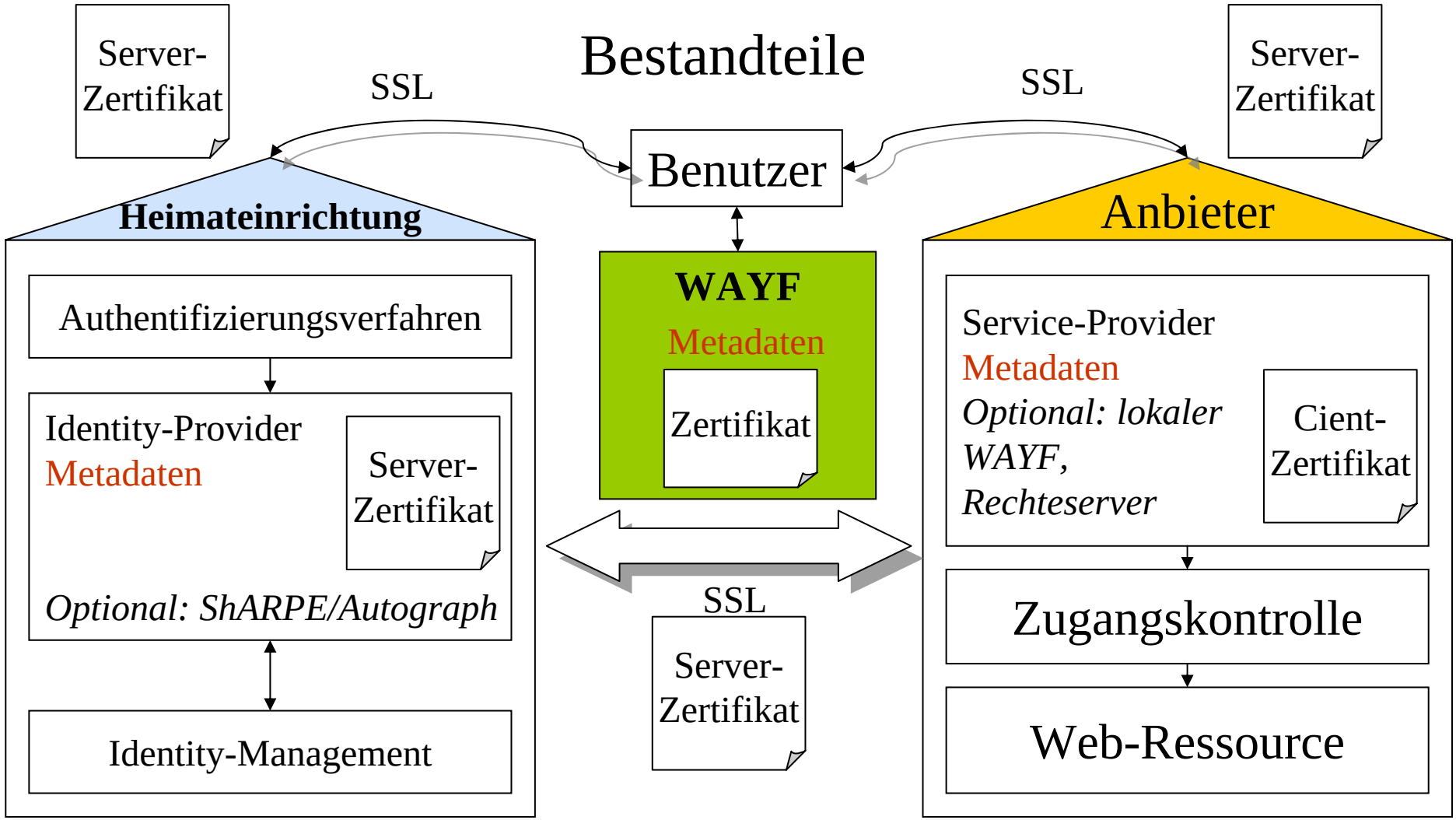
Wie funktioniert Shibboleth?

Benutzerin

Heimateinrichtung

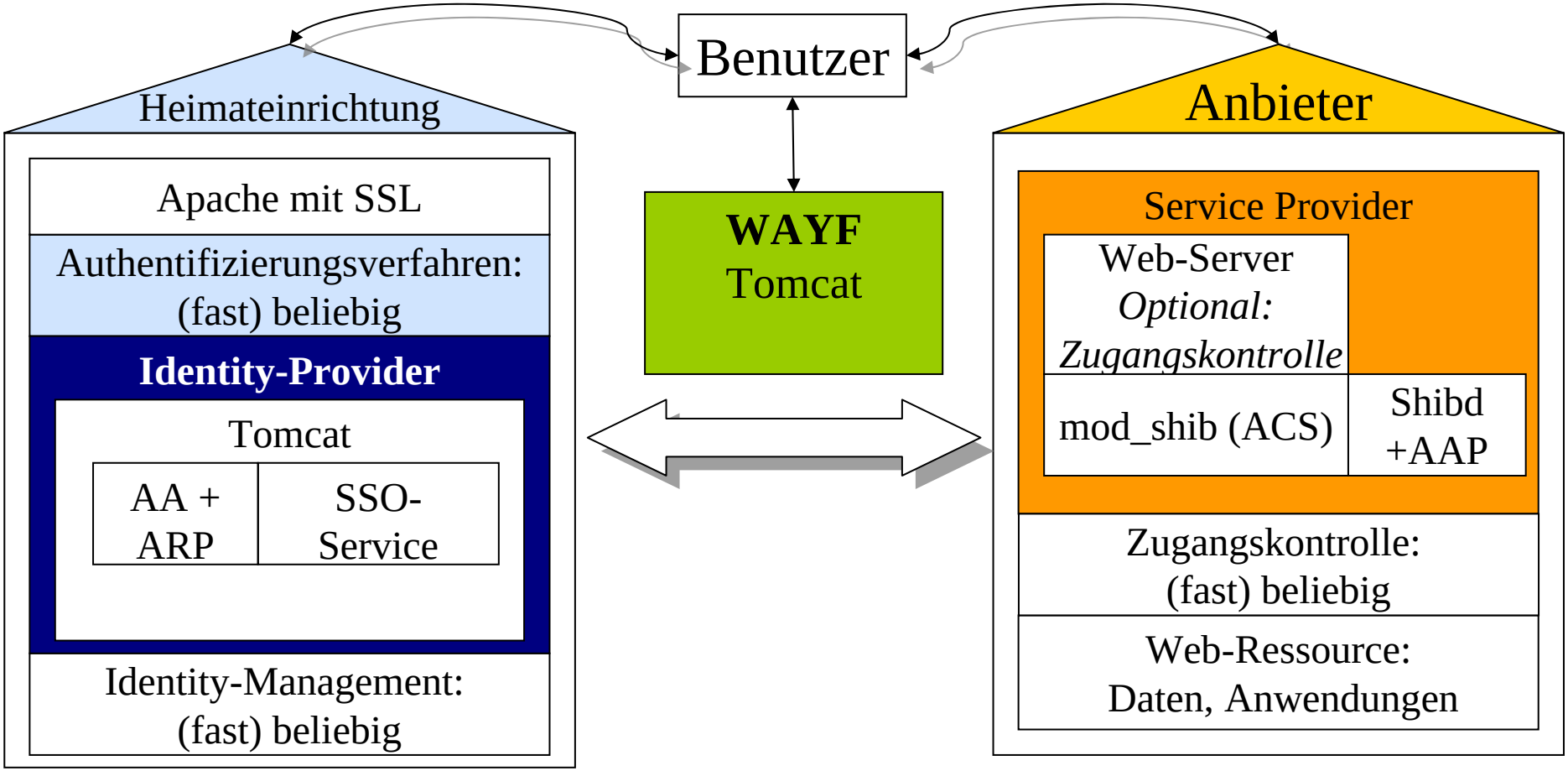


Wie funktioniert Shibboleth?



Wie funktioniert Shibboleth?

Bestandteile: Technik



Wie funktioniert Shibboleth?

- Wann erfolgt eine neue Anmeldung?
  - Die Sitzung (Session) des SSO ist abgelaufen (Timeout)
  - Der Browser wurde geschlossen
  - Benutzer hat mehrere Identitäten und für jede Identität andere Attribute und damit andere Rechte (technische Umsetzung?)
  - Single Log-Out (Shibboleth 2.0)
- Keine neue Anmeldung
  - Sitzung des Service-Provider wurde beendet (Anwendung oder SSO-Dienst)
  - Wechsel des Service-Provider

Identity-Management und Shibboleth

- Identity-Management wird benötigt für:
  - Authentifizierung (identifiziert den Benutzer)
  - Autorisierung (stellt die Attribute zur Verfügung)
- **Shibboleth** stellt keine besonderen **Anforderungen** an das Identity-Management
  - Fertige Schnittstellen zu LDAP, SQL-Datenbanken etc.
  - Nichtvorhandene Schnittstellen können programmiert werden
- Die **Föderation** stellt qualitative und rechtliche **Anforderungen** an das Identity-Management:
  - Verlässlichkeit
  - Aktualität
  - Nachvollziehbarkeit
  - Ausfallsicherheit
  - Datenschutz

Attribute und Zugriffskontrolle

- **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 ein funktionierendes **Identity-Management**

Attribute und Zugriffskontrolle

- **InCommon** hat mit eduPerson den Standard für den **Austausch von Attributen** vorgegeben.
- **Andere Föderationen** und **internationale Anbieter** orientieren sich an diesem Standard.
- Die **Anbieter** kommen mit **wenigen Attributen** aus:
  - eduPersonAffiliation: member, faculty, staff, student, ...
  - **eduPersonEntitlement:** beliebige Rechteinformationen, z.B. **urn:mace:dir:entitlement:common-lib-terms**
  - eduPersonPrincipalName: „Net-ID“ des Benutzers
  - eduPersonTargetedID: eindeutiges Pseudonym des Benutzers für einen Anbieter, z.B. für Personalisierung

Attribute und Zugriffskontrolle

- Attribute können **personenbezogene Daten** sein (Beispiele: Benutzerkennung, E-Mailadresse).
- Personenbezogene Daten dürfen nach den (EU-) **Datenschutzbestimmungen** nur weitergegeben werden, wenn dies für die Erbringung des Dienstes **notwendig** ist und der **Benutzer** der Weitergabe **ausdrücklich zustimmt**.
- Die Weitergabe der Attribute erfolgt in Shibboleth über **Attribute-Richtlinien** (Attribute Release Policies) auf Einrichtungs- und Benutzerebene.
- **MAMS** erweitert mit ShARPE/Autograph die Attribute-Richtlinien um die **Gruppenebene**.

Attribute und Zugriffskontrolle

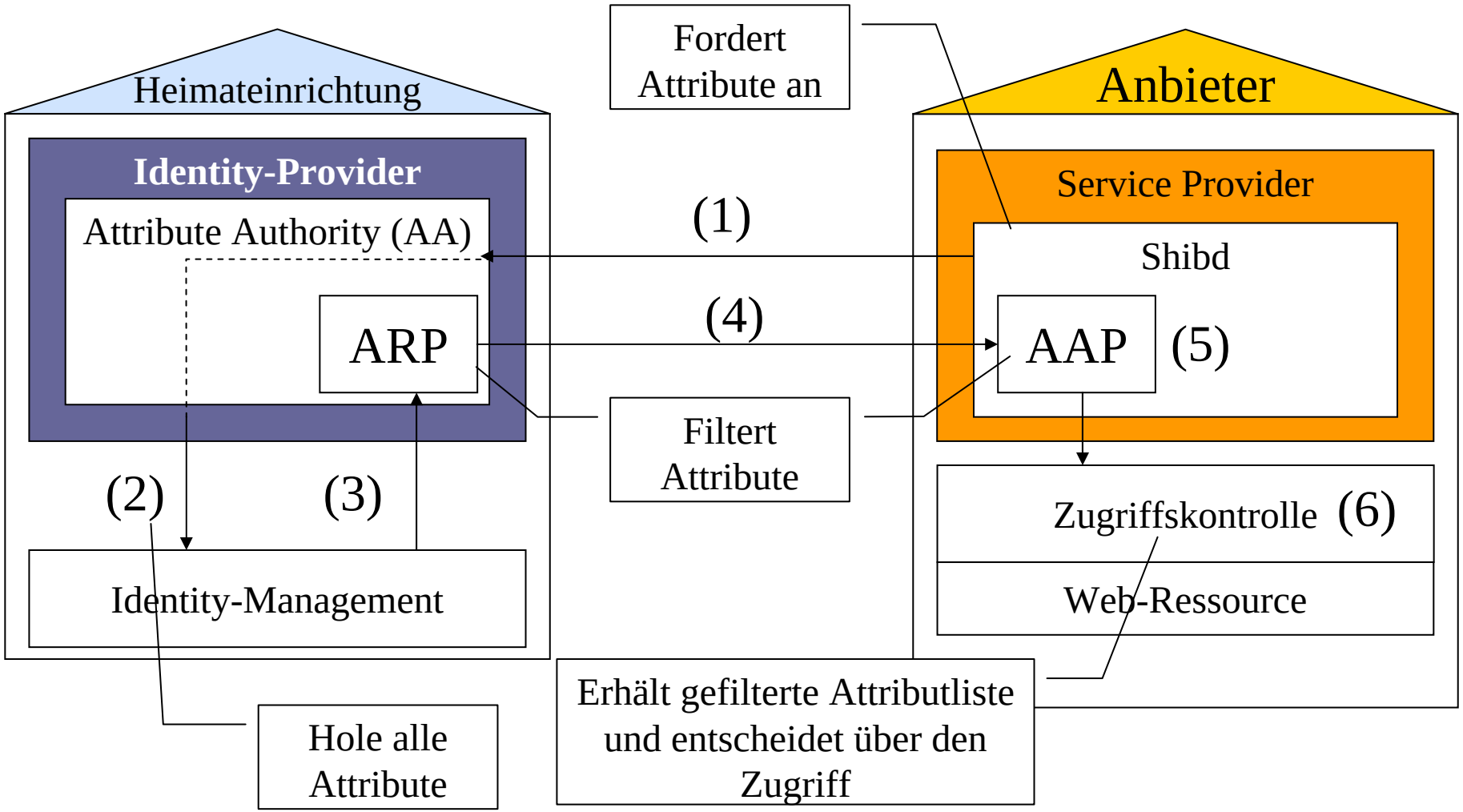
- MAMS (Meta-Access Management System, Australien) hat Werkzeuge für die **Verwaltung der ARPs** entwickelt (siehe http://tinyurl.com/dzhfk):
  - **ShARPE** (Shibboleth Attribute Release Policy Editor, Administrationsschnittstelle) und
  - **Autograph** (Benutzerschnittstelle)
- Die Attribute, die an einen Service-Provider weitergegeben werden, werden den Benutzern in Form von **Visitenkarten** präsentiert.
- Die Benutzer können für jeden Service-Provider **sehr intuitiv** individuelle Visitenkarten erstellen.

Attribute und Zugriffskontrolle

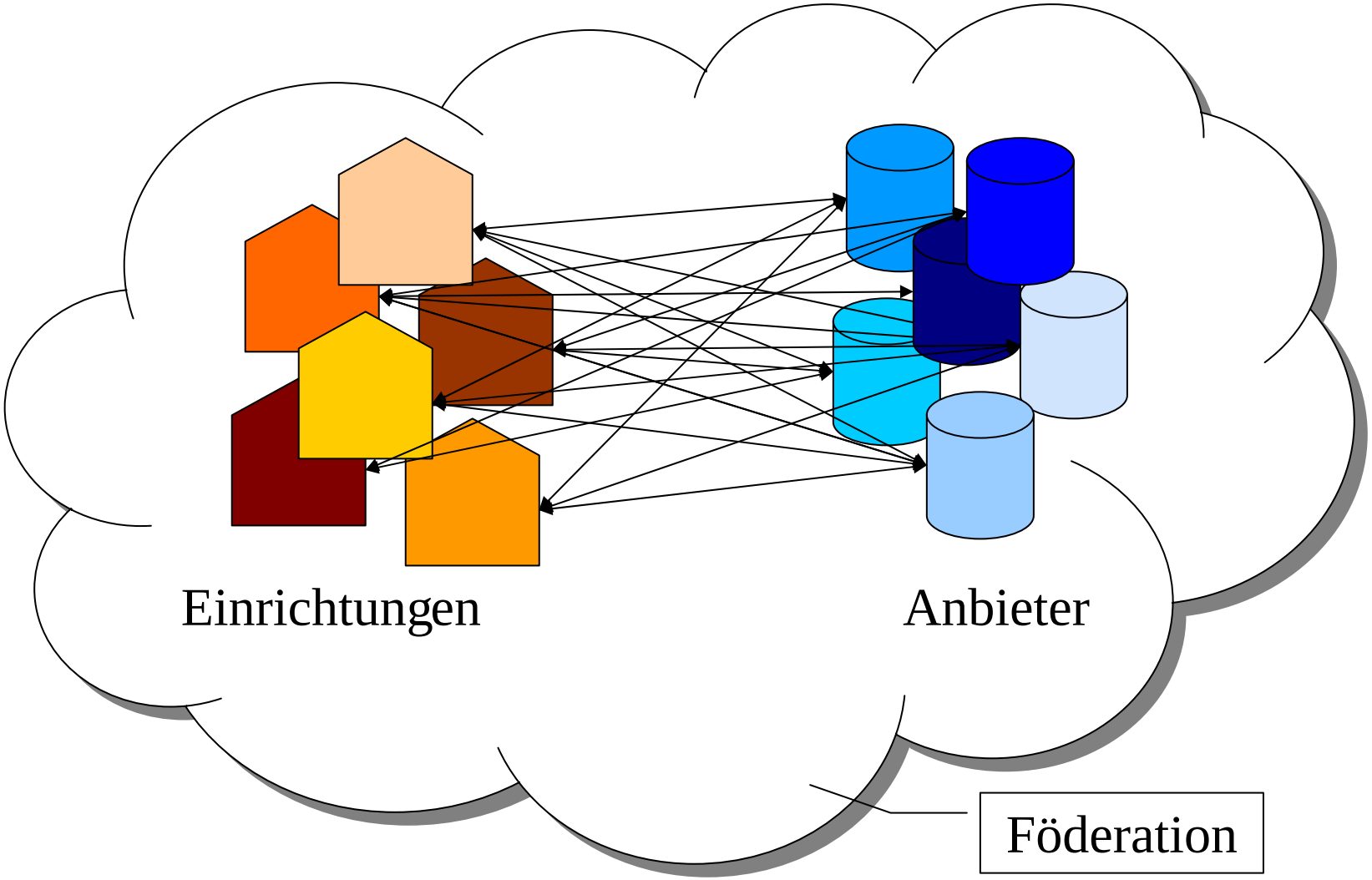
MAMS Visitenkartenmodell
Sie geben folgende Daten an den Dienstanbieter weiter. Wenn Sie einzelne Daten nicht weitergeben wollen, löschen Sie bitte die Markierung:

Auswirkung:
Ohne EMail-Adresse ist die Nutzung des Alert-Dienstes nicht möglich.

Attribute und Zugriffskontrolle



Föderation



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.
- Unter Koordination des DFN ensteht eine **deutschlandweite Föderation** (**DFN-AAI**)

Ausblick: Shibboleth 2.0

- Zeitrahmen für Shibboleth 2.0: Anfang 2007?
- Kompatibel mit Shibboleth 1.3
- erweiterte **Authentifizierungsfunktionalität**
- **Single Logout** (technisch schwer umzusetzen!)
- **Service-Provider** als 2.3 Java-Servlet
- Attribut-Verwaltung (IdP) wird erweitert:
  - Filterfunktion auf Gruppenebene (bisher nur Filterfunktionen auf Einrichtungs- und Benutzerebene)
  - Dynamisches Laden der Filtereinstellungen
  - Unterstützt **ShARPE/Autograph**
- statt WAYF: **Discovery-Service** mit Rückleitung zum Service-Provider

Shibboleth in Aktion

- DEMO

Vielen Dank für Ihre Aufmerksamkeit!

AAR ist ein Projekt der
UB Freiburg und UB Regensburg.
Gefördert vom BMBF (PT-NMB+F)

aar.vascoda.de
info@aar.vascoda.de
borel@ub.uni-freiburg.de