



Einführung in Shibboleth

*5. Shibboleth-Workshop der
AAR in Kooperation mit der DFN-
AAI*

17.10.2007, Berlin

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 durch Internet2 entwickelt
→ <http://shibboleth.internet2.edu>
- Basiert auf SAML:
Security Assertion Markup Language
- 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)
 - bestehendes Identity-Management nutzen
 - Einfache Anbindung an das bestehende Identity-Management
- **Anbieter**
 - Schützen der lizenzpflichtigen Inhalte
 - Keine eigene Benutzerverwaltung
 - Kontrolle über die Nutzung (wer darf was?)
 - Statistische Auswertung (auch für Abrechnungen wichtig!)



Woher kommt "Shibboleth"?

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

Woher kommt "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 **Ephraimite**? Wenn er dann antwortete: Nein...

Woher kommt "Shibboleth"?



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

Woher kommt "Shibboleth"?



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

Woher kommt "Shibboleth"?



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

Woher kommt "Shibboleth"?



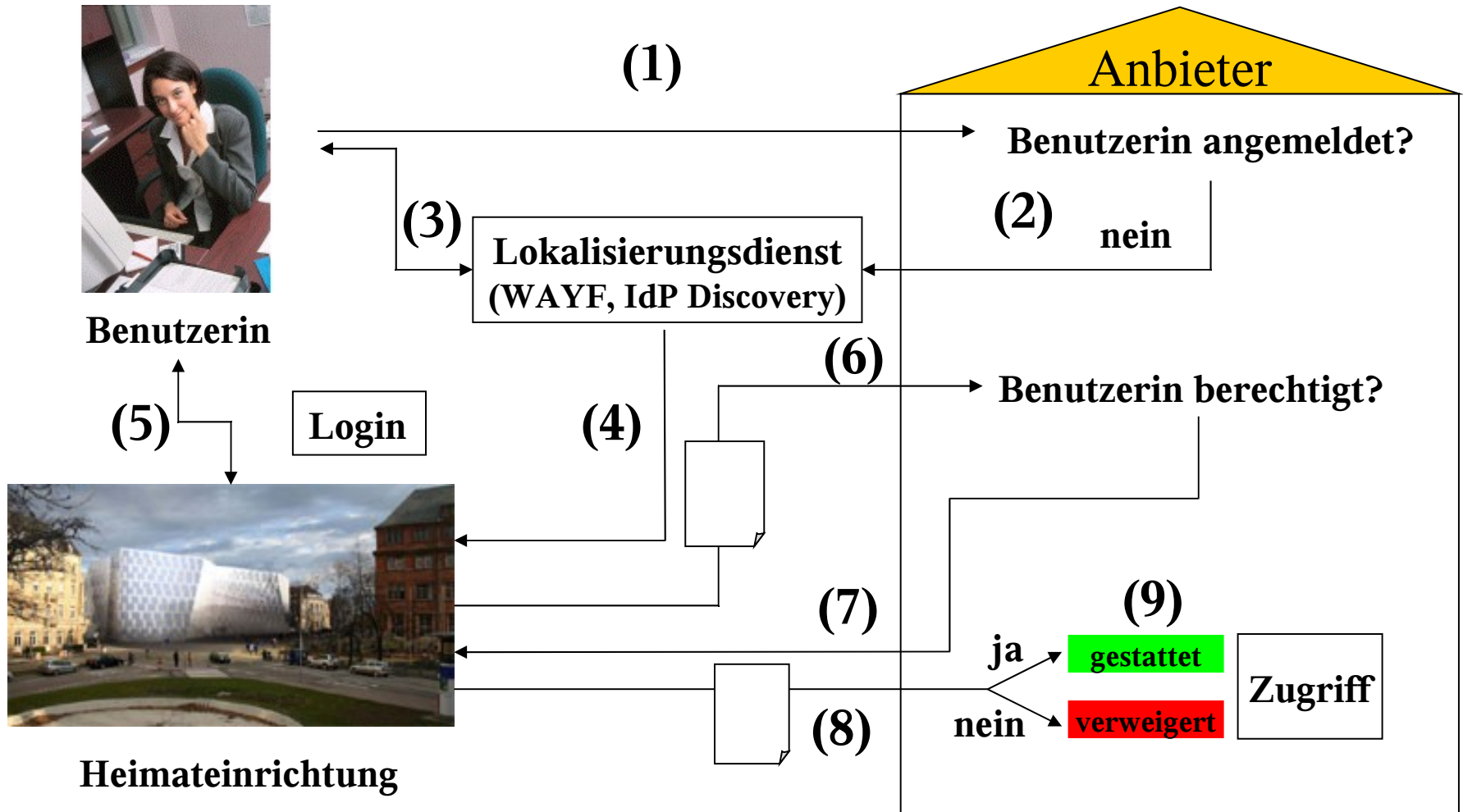
der Zeit von Ephraim fielen zweiundvierzigtausend.



Woher kommt "Shibboleth"?

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

Wie funktioniert Shibboleth?

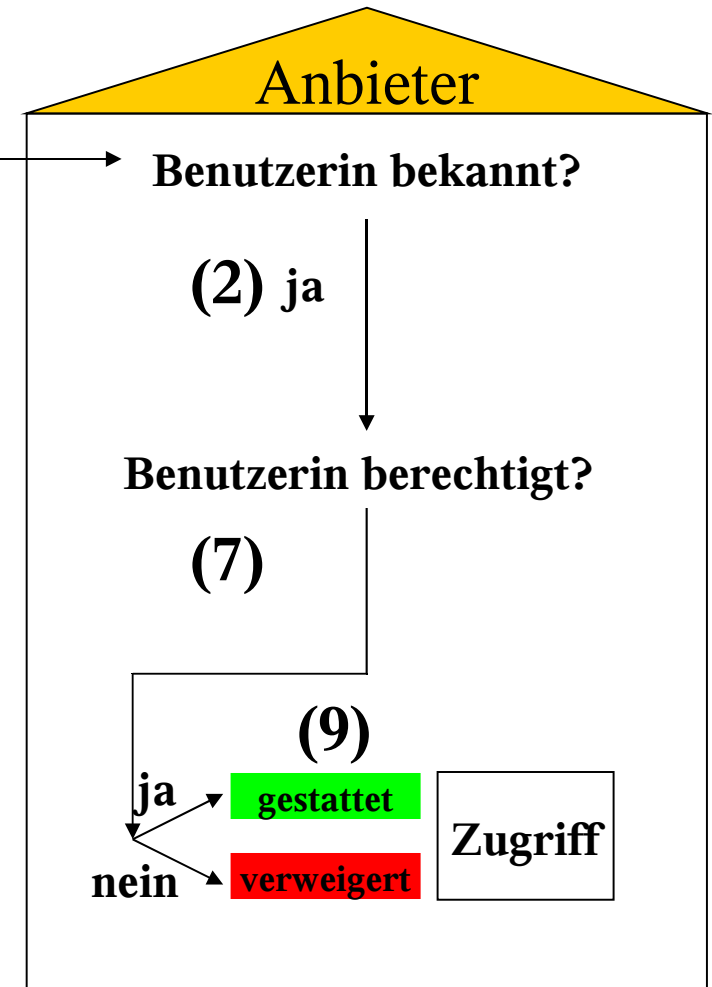


Wie funktioniert Shibboleth?



Benutzerin

(1)



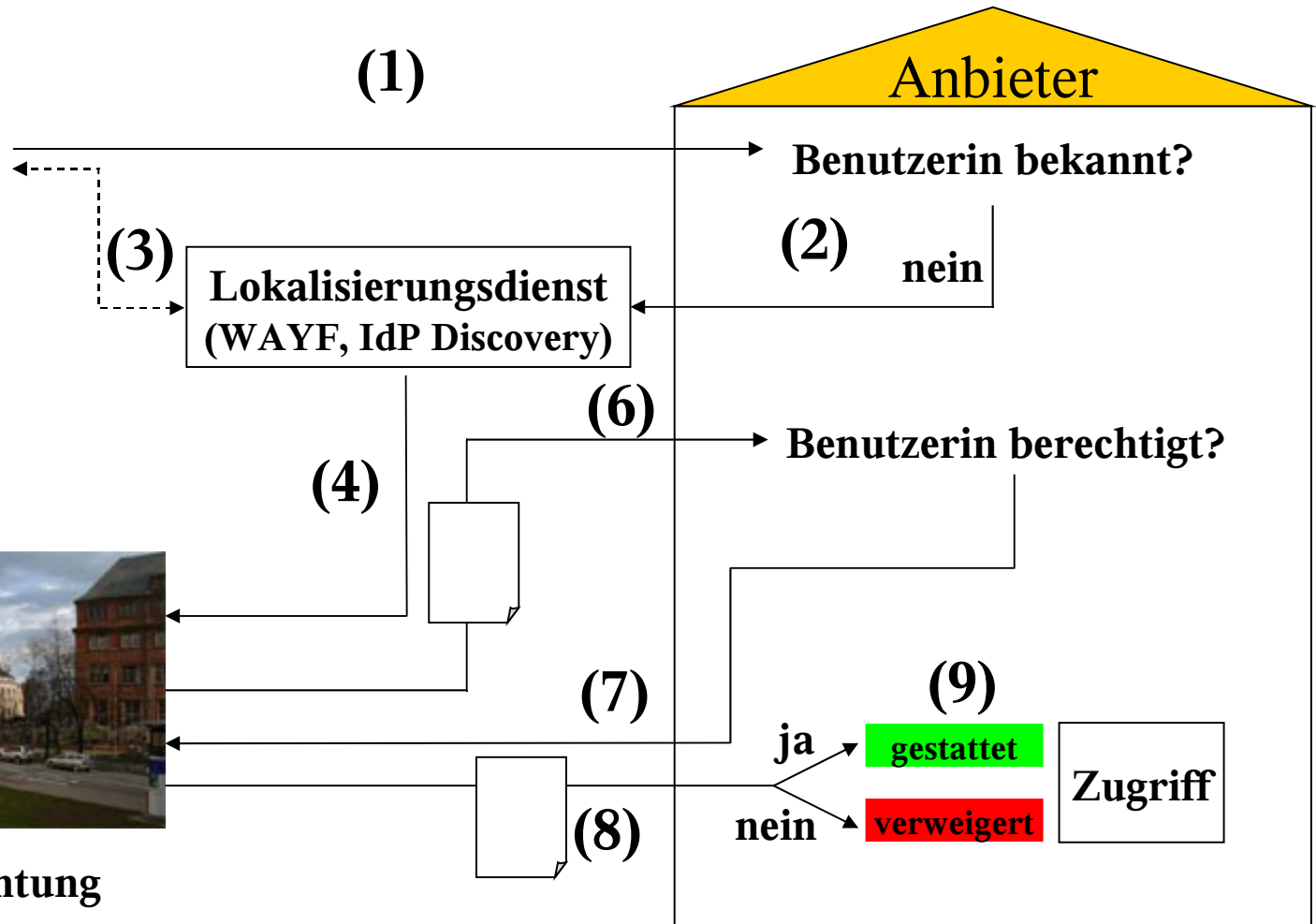
Wie funktioniert Shibboleth?



Benutzerin



Heimateinrichtung



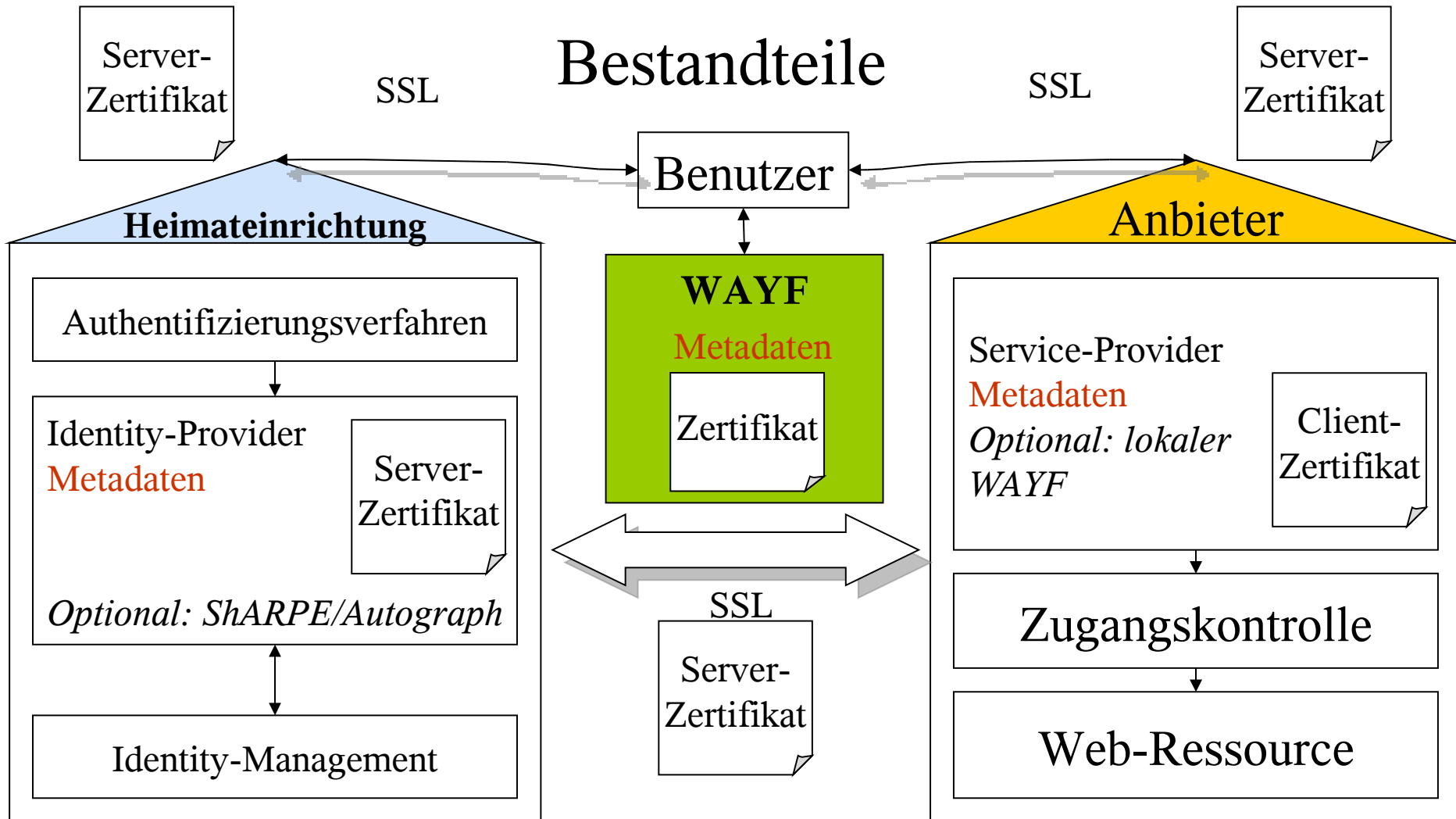


Wie funktioniert Shibboleth?

- Bestandteile:
 - IdP (bei der Heimateinrichtung)
 - Authentifizierung (frei wählbar)
 - Identity Management (frei wählbar)
 - Autorisierung (Bestandteil von Shibboleth)
 - Identity Management (frei wählbar)
 - SP (beim Anbieter)
 - Zugriffskontrolle
 - Erwartet:
 - Erfolgreiche Authentifizierung
 - Attribute
 - WAYF (Lokalisierungsdienst)
 - optional
 - Liste mit Einrichtungen und Anbietern
 - Als selbständiger Dienst oder beim Anbieter



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 ein funktionierendes **Identity-Management**



Attribute

- **InCommon** hat mit **eduPerson** den **Standard** für den **Austausch von Attributen** vorgegeben.
- **Andere Föderationen** und **internationale Anbieter** orientieren sich üblicherweise an diesem Standard.
- Die **meisten Service-Provider** kommen dabei mit **wenigen Attributen** aus, häufig verwendet werden:
 - 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

- **Regeln**, welche Informationen die Attribute enthalten dürfen, wird von Shibboleth **nicht vorgeschrieben!**
- 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.



Attribute

- **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

MAMS Visitenkartenmodell

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

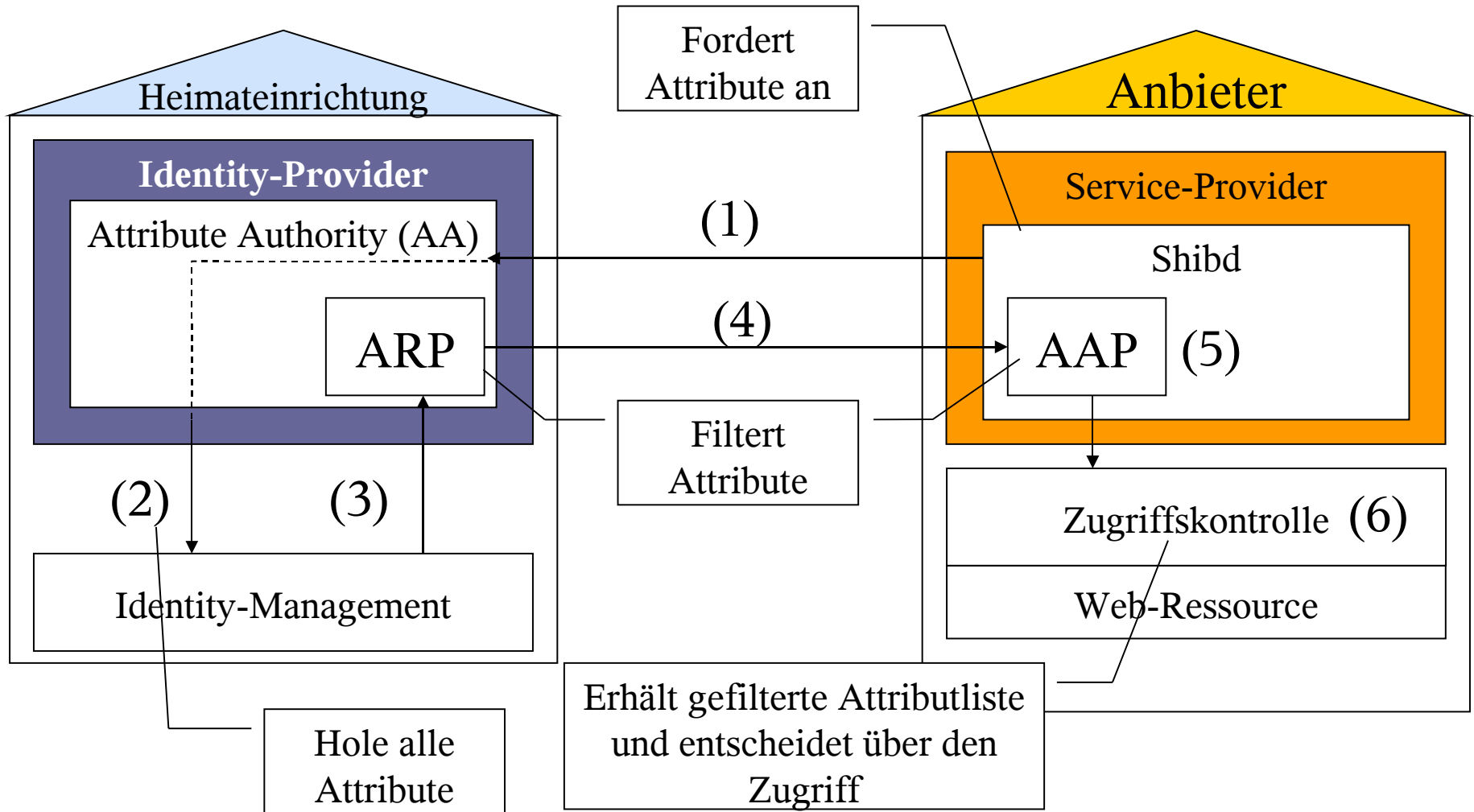
	ALBERT-LUDWIGS- UNIVERSITÄT FREIBURG
Namen: Franck Borel	
Mitgliedstyp: Staff	<input checked="" type="checkbox"/>
E-Mail: borel@uni-freiburg.de	<input checked="" type="checkbox"/>

Auswirkung:

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



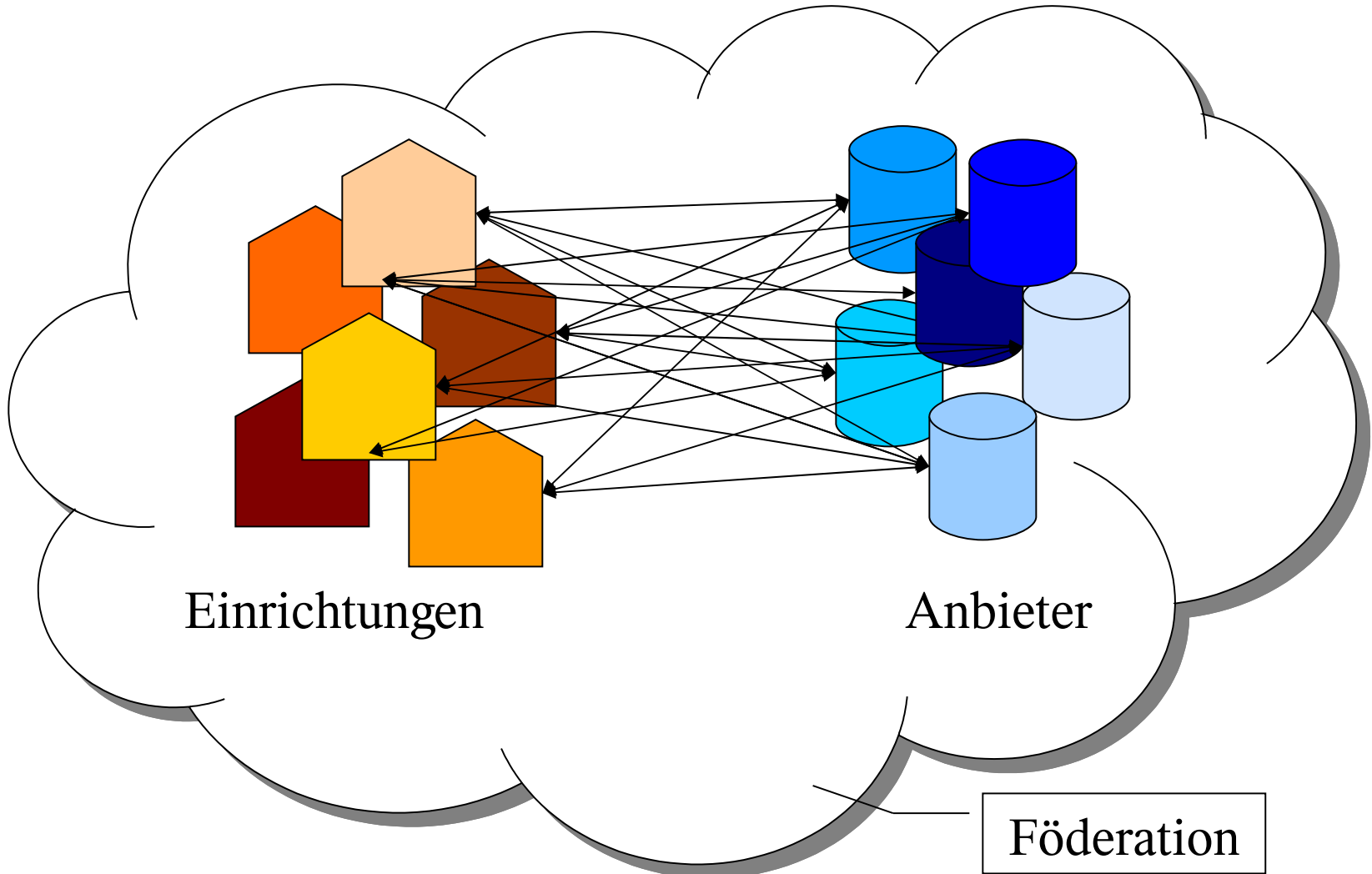
Attribute und Zugriffskontrolle





Metadaten

- **Vertrauen & Sicherheit:** Infos über Zertifikate und *providerID*, damit man weiss mit wem man Daten austauscht.
- Metadaten werden **signiert**, um ihre Authentizität und Integrität zu gewährleisten. Mit gefälschten Metadaten wäre es möglich, sämtliche Shibboleth-Sicherheitsmechanismen auszuhebeln!
- Metadaten sind fundamental für die Föderation!
- Metadaten müssen **aktuell** und **synchron** sein, sonst klappt die Interoperabilität nicht.
- Werkzeuge für die Verwaltung der Metadaten werden benötigt.





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 entsteht eine **deutschlandweite Föderation (DFN-AAI)**



Föderation

- Föderationen weltweit (Quelle: Internet2, DFN-AAI)
 - Australien (MAMS)
 - Dänemark (DK-AAI)
 - **Deutschland (DFN-AAI)**
 - Finnland (HAKA)
 - Frankreich (CRU)
 - Norwegen (FEIDE)
 - Schweden (SWAMID)
 - Schweiz (SWITCH)
 - UK (SDSS)
 - US (InCommon)



Unterstützung von Shibboleth bei Diensteanbietern

Index of Shibboleth-Enabled Applications and Services (Quelle: internet2)

- American Chemical Society
- ArtSTOR
- CSA
- Digitalbrain PLC
- EBSCO Publishing
- Elsevier ScienceDirect
- JSTOR
- The Literary Encyclopedia
- NSDL
- OCLC
- Ovid
- Projekt MUSE
- Proquest Information and Learning
- Serials Solutions
- SCRAN
- Thomson Gale
- Thomson ISI/Scientific (7/2008)
- EZProxy
- Metapress (7/2008)

▪ In Deutschland

- Infoconnex
- Vascoda (?)
- ReDI
- SaxIS
- FIZ-Technik (7/2008)
- GBI/Genios
- Springer (7/2008)
- DIPF
- GBV/NL



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