R|R|Z|N
Regionales Rechenzentrum für Niedersachsen

Leibniz Universität Hannover

Shibboleth® – föderiertes Identitätsmanagement

M. Sc. Ralf Gröper & M. Sc. Benjamin Henne, RRZN Sicherheitstage, 18.11.2009

Ein Schibboleth

„Schornsteinfeger Stefan fischt im Nest nach Wurst."

- Je nach Herkunft wird 1x, 2x, 3x oder 4x „st" als „scht" ausgesprochen

Agenda

- Was ist Shibboleth?
- Komponenten von Shibboleth
- Ablauf bei Shibboleth-Login
- Shibboleth und Attribute
- SAML
- Shibbolisierung von Anwendungen

Bedeutung des Wortes Schibboleth

- Eigentlich: hebräisch „Getreideähre“
- Altes Testament, Buch Richter Kapitel 12 Vers 5ff

> „Wenn ephraimitische Flüchtlinge (kamen und) sagten: *Ich möchte hinüber!* fragten ihn die Männer aus Gilead: *Bist du ein Ephraimiter?* Wenn er *Nein* sagte, forderten sie ihn auf: *Sag doch einmal ‚Schibboleth‘*. Sagte er dann *Sibboleth*, weil er es nicht richtig aussprechen konnte, ergriffen sie ihn und machten ihn dort an den Fluten des Jordan nieder. So fielen damals zweiundvierzigtausend Mann aus Ephraim.“

- Schibboleth ist somit wohl das erste biometrische Authentifizierungsverfahren gewesen
- Daher Bedeutung heute: „Kennwort“ oder „Codewort“

Was ist die Software Shibboleth?

- Shibboleth ist eine von Internet2 entwickelte Architektur und Implementierung einer föderierten identitätsbasierten AAI für Webanwendungen basierend auf SAML
- AAI: Authentifizierungs- und Autorisierungsinfrastruktur
- Föderiert: Über Organisationsgrenzen hinweg
- SAML: Security Assertion Markup Language

Was ist Shibboleth *nicht*?

- Shibboleth ist kein Identity Management System
  - Shibboleth hat keine Schnittstellen für Nutzerverwaltung
  - Shibboleth hat keine eigene Datenbank

- Shibboleth ist nicht (sinnvoll) einsetzbar für organisationsinterne Lösungen
  - Zu viel Overhead, da Vertrauen hier explizit gegeben ist

R|R|Z|N

Leibniz Universität Hannover

Stakeholder

Heimateinrichtungen

Nutzer

TIB | Technische Informationsbibliothek
UB | Universitätsbibliothek Hannover

Dienstanbieter

Anforderungen aus Nutzersicht

- Ortsunabhängiger Zugriff auf die Dienste
- Single Sign-On
  - Zugriff auf alle verfügbaren Webressourcen nach einmaliger Authentifizierung
- Nur ein Account (z.B. Benutzername/Passwort) für möglichst viele Webanwendungen
- Datenschutz bzw. Datensparsamkeit

Anforderungen aus Sicht der Heimateinrichtungen

- Die Heimatorganisation des Nutzers verwaltet seine Identität
  - Authentifizierungsinformationen und Attribute
- Bestehendes Identitätsmanagement (IdM) nutzen
  - z. B. basierend auf LDAP-Verzeichnis
- Möglichst wenig Änderungen am bestehenden IdM

Anforderungen aus Diensteanbietersicht

- Schutz von Webressourcen
- Eigene Benutzerverwaltung vereinfacht
  - Authentifizierung wird an Heimatorganisation übertragen
- Autorisierung von Zugriffen
  - Wer darf was auf Grund welcher Eigenschaft?

Skalierbarkeit

- Diese Anforderungen sind nur durch ein Vertrauensverhältnis zwischen allen Beteiligten zu erfüllen
- Vertrauensverhältnis skaliert nicht wenn jeder Diensteanbieter mit jeder Heimateinrichtung in Verbindung treten muss
  - Dies bedeutet u. a. Austausch von X.509 Zertifikaten
- Zentrale Verwaltung ist also notwendig: Die Föderation

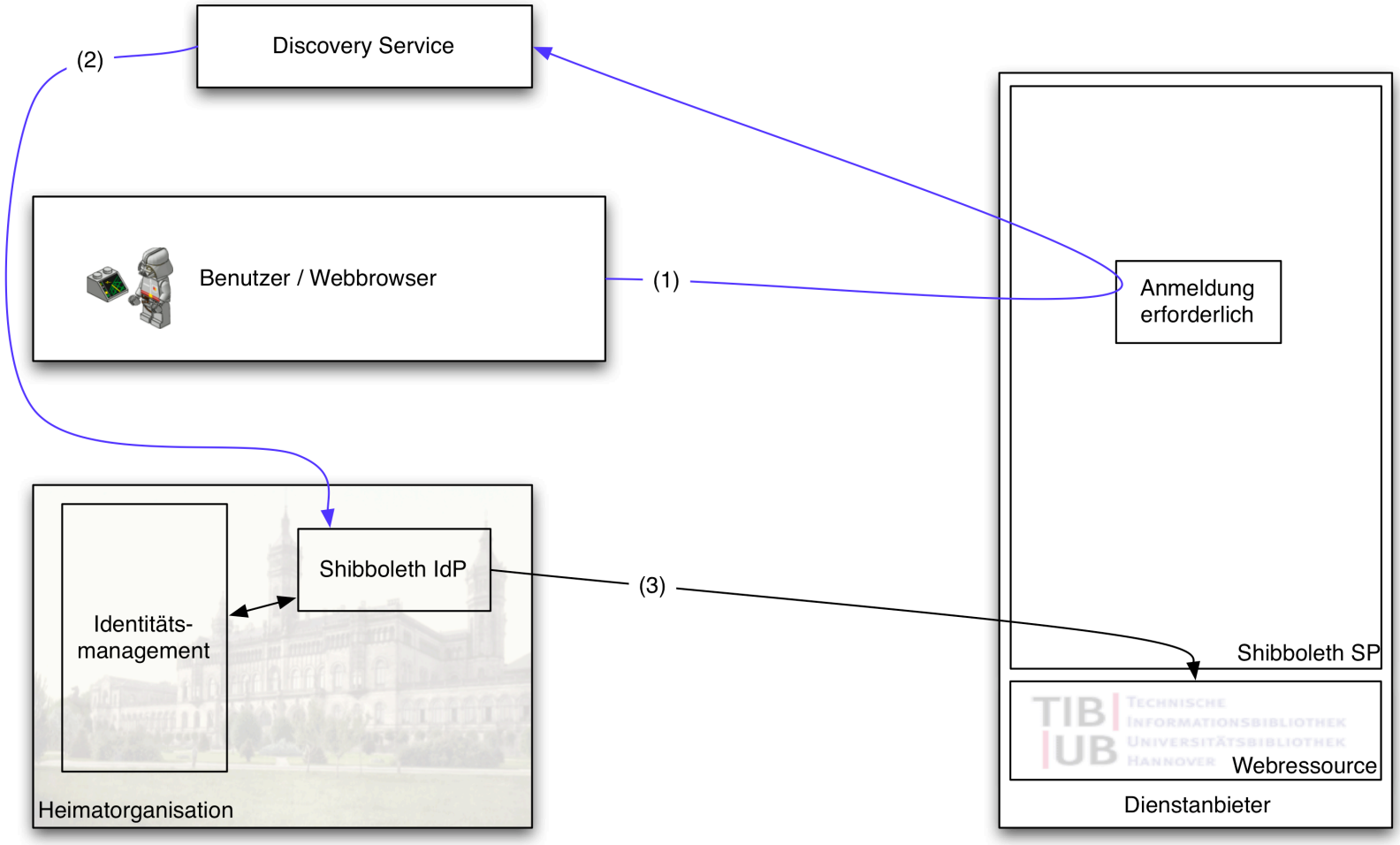
Die Föderation

- Die Föderation organisiert das Vertrauen zwischen allen Beteiligten
- Organisatorisches Vertrauensverhältnis
  - Verträge
- Technisches Vertrauensverhältnis
  - Sichere, eindeutige, nicht-fälschbare Übertragung der Informationen innerhalb der Föderation
  - Transport Level Security: SSL/TLS
  - Public Key Infrastruktur: PKI
- Dies regelt alles die Shibboleth Föderation
  - „Metadaten" der Föderation werden bereitgestellt

Komponenten

- Bei der Heimateinrichtung
  - Identity Provider (IdP)
  - Attribute
- Beim Dienstanbieter
  - Service Provider (SP)
- Bei der Föderation
  - Where Are You From? / Discovery Service (WAYF/DS)
  - Metadaten

Web-Browser Single Sign-On (vereinfacht)



Web-Browser Single Sign-On (vereinfacht)

1. Nutzer möchte auf Webressource zugreifen und wird an, Discovery Service weitergeleitet
2. Nutzer authentifiziert sich bei seiner Heimateinrichtung
3. Wenn der Nutzer berechtigt ist bekommt er Zugriff auf die Webressource

Identity Provider (IdP)

- Komponente bei der Heimateinrichtung
  - „Asserting Party“
- 1. Authentifizierung der Nutzer (SSO-Komponente)
  - Frei wählbare Authentifizierungsmethode
    - Entsprechende Apachemodule können eingesetzt werden
    - Username/Password, Zertifikatsbasiert,...
  - Authentifizierungsinformationen aus Identity Management
- 2. Ausgabe von Attributen (Attribute Authority)
  - Ebenfalls aus Identity Management

Service Provider (SP)

- Komponente beim Diensteanbieter
  - „Relying Party“
- Realisiert die Zugriffskontrolle auf Webressourcen
- Erwartet vom IdP erfolgreiche Authentifizierung
  - Information: „Nutzer ist erfolgreich Authentifiziert“
- Kann Attribute vom IdP für Autorisierung benutzen
  - Information: „Nutzer ist Student an der Uni Hannover“

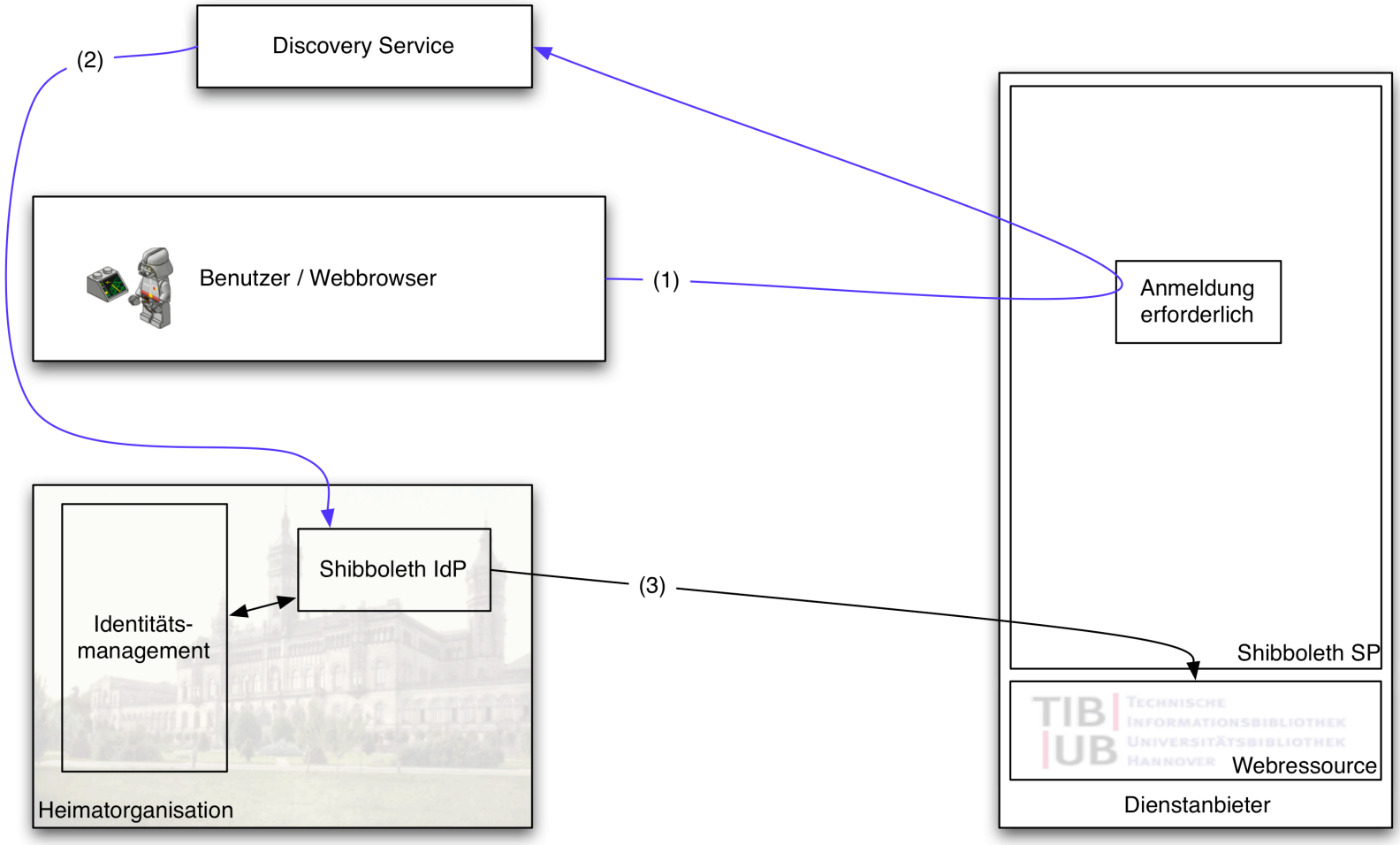
Where Are You From (WAYF) / Discovery Service (DS)

- Zentrale Komponente der Föderation
- Problem: SP weiß nicht, an welchen IdP der Nutzer verwiesen werden soll
- Lösung: Zentraler WAYF
  - Nutzer wählt aus Pull-Down Menü seine Heimateinrichtung aus
- Information wird in Cookie gespeichert
  - Nutzer muss also nicht bei jedem Zugriff seine Heimatorganisation erneut auswählen

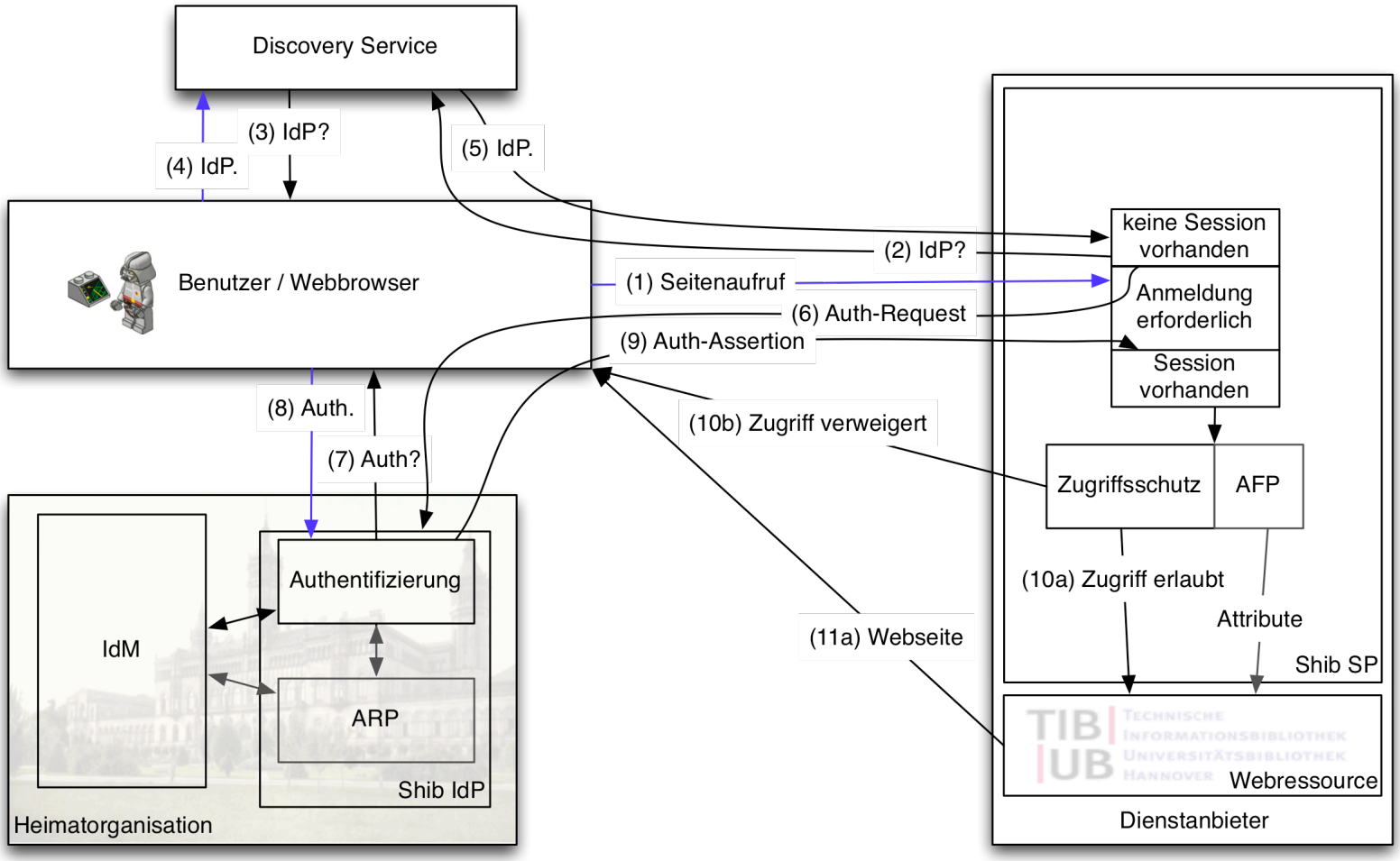
Metadaten

- Werden von der Föderation bereitgestellt
- Enthalten alle notwendigen Informationen für vertrauensvolle Kommunikation in der Föderation
- Inhalt
  - URLs bzw. Endpunkte aller Dienste
  - X.509 Zertifikate aller IdPs und SPs
  - Informationen über Scopes
    - Nur IdP der Uni Hannover darf Attribute ...@uni-hannover.de ausstellen
  - Weitere Metainformationen
    - Admins, Kontaktdaten,...

Web-Browser Single Sign-On (vereinfacht)



Web-Browser Single Sign-On



Web-Browser Single Sign-On

1. Nutzer möchte auf Webdienst zugreifen und ist nicht angemeldet
2. SP leitet Nutzer an Discovery Service weiter
3. DS bietet Nutzer Liste verfügbarer Heimatorganisationen an
4. Nutzer wählt Heimatorganisation aus
5. DS teils SP die Heimatorganisation für Session-Aufbau mit
6. SP initiiert Session-Aufbau durch Kontakt zum IdP
7. IdP fragt Nutzer nach Identität und Nachweis
8. Nutzer authentifiziert sich (z. B. durch Nutzername/Passwort)
9. IdP sendet Authentifizierungsinformation an SP. Attribute werden nach Filterung durch Attribute Release Policy (ARP) hinzugefügt.
10. SP entscheidet anhand von Nutzerinformatioen, ob Zugriff erlaubt ist. Ist Nutzer autorisiert, so wird Zugriff auf Webdienst gewährt. Webdienst erhält Zugriff auf Nutzerattribute nach Filterung durch Attribute Filtering Policy (AFP)

Attribute

- Attribute bilden die Grundlage für die Autorisierung und Zugriffskontrolle mit Shibboleth
  - IdP stellt sie bereit, SP wertet sie aus

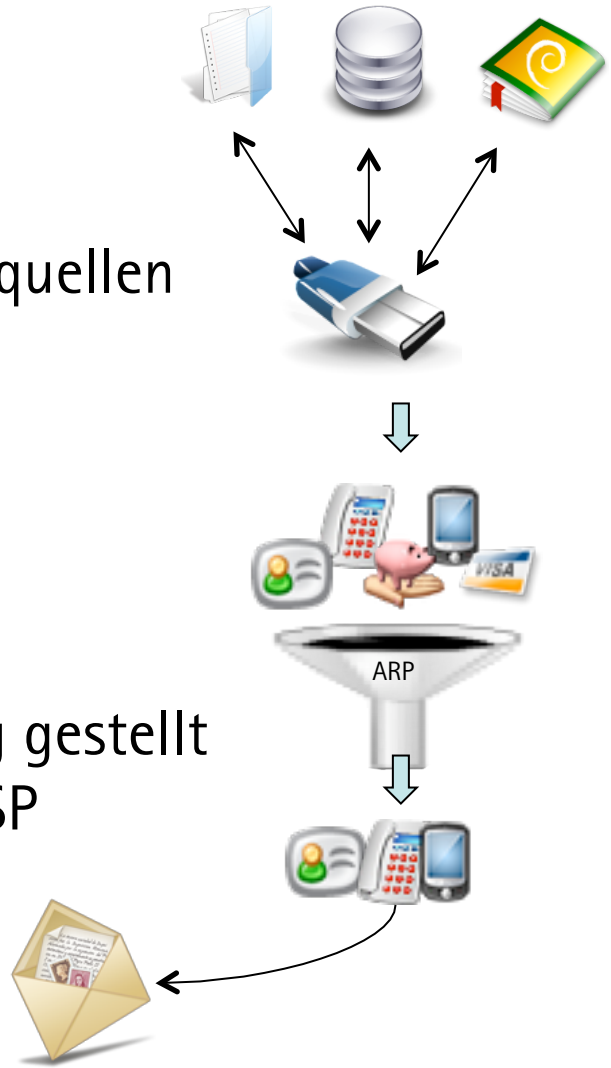
➢ Absprachen zwischen IdP und SP nötig
  - Festlegung gemeinsamer Attribute, Namensräume/Schemata, Darstellungen und zulässiger Werte
    - verbreitete Grundlage: eduPerson LDAP-Schema

eduPerson-Schema

- Typische Attribute aus dem eduPerson-Schema und Beispiele
  - Name (cn): `Benjamin Henne`
  - Nachname (sn): `Henne`
  - Email-Adresse (mail): `henne@rrzn.uni-hannover.de`
  - eduPersonPrincipalName: `bhenne@rvs.uni-hannover.de`
  - eduPersonPrimaryAffiliation: `employee`
  - eduPersonScopedAffiliation: `staff@rvs.uni-hannover.de`
  - eduPersonEntitlement: `luh:rrzn:cluh`
    - Berechtigungen (für Ressourcen)
  - eduPersonTargetedID: `ae38m811lve0bzk`
    - Eindeutige identitäts-unabhängige ID

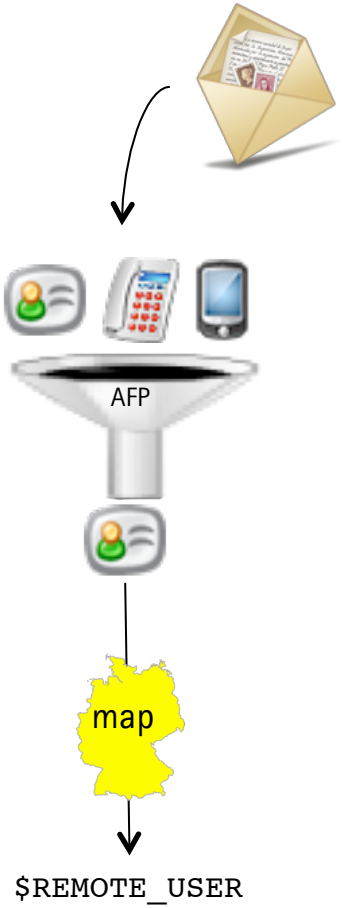
Attribute am Identity Provider

- IdP ist Attribute Provider/Authority
- **Attribute Resolver** konnektiert IdM-Datenquellen
  - LDAP, RDBMS, statisch (Datei), ...
- **Attribute Release Policies** (ARP)
  - Attribut-Filter des IdP
  - welche Attribute werden zur Verfügung gestellt und zurückgehalten gegenüber einem SP



Attribute am Service Provider

- SP ist Attribute Consumer
- **Attribute Filtering Policies** (AFP)[1]
  - Attribut-Filter des SP
  - welche Attribute (Name/Inhalt) werden von welchem IdP angenommen
- **Attribute Map** legt Weitergabe der Attribute an Ressource-Manager/Applikation fest
  - z. B. Abbildung auf HTTP-Umgebungsvariablen



[1] auch bekannt als Attribute Acceptance Policies (AAP)

Security Assertion Markup Language (SAML)

- Shibboleth baut auf SAML-Implementierung OpenSAML auf
  - Shibboleth 1.3: SAML 1.x
  - Shibboleth 2.x: SAML 2 (aktuell: Shibboleth 2.1)
- SAML
  - XML-basierter offener Standard der OASIS
  - Framework für Kommunikation von Benutzerattributen und Authentifizierungsinformationen

Security Assertion Markup Language (SAML) (2)

- Komponenten unabhängig definiert
  - Assertions
    - Authentifizierung, Attribute, Autorisierung
    - direkt oder als Artefakte
  - Protocols
    - Request-Response-Protokolle für verschiedene Zwecke
      - z. B. Authn-Request, Attribute-Request, Artifact-Resolution, SLO

Security Assertion Markup Language (SAML) (3)

- Komponenten unabhängig definiert
  - Bindings
    - Festlegung des Transports von SAML-Nachrichten über existierenden Standardprotokolle
      - z. B. SAML Redirect, SAML POST, SAML SOAP
  - Profiles
    - Profile legen Kombination verschiedener Assertions, Protokolle und Bindings für einen bestimmten Zweck fest
      - z. B. Web-Browser Single Sign-On
    - Attribut-Profile legen Interpretationen von Attributen in Assertions fest, z. B. X500/LDAP

Shibbolisierung von Applikationen

- Shibbolisierungsaufwand abhängig von Applikation

> *„Viele Applikationen gehen davon aus, Kontrolle über die Benutzerauthentifizierung zu haben. SSO ist die Kunst der Applikation diese Kontrolle zu nehmen und sie zu lehren sich auf die Authentifizierung ihrer Laufumgebung zu verlassen.“*

Shibbolisierung von Applikationen

- Shibbolisierung
  - Shibboleth-Session initiieren
    - Session-Handling durch SP (required Session)
    - Session-Handling durch Applikation (lazy Session)
  - Authn-Information und Attribute an Applikation zustellen
    - Auslesen von Umgebungs-/Header-Variablen
      - z. B. `$REMOTE_USER`
    - Auslesen ganzer SAML-Assertions über SP-lokale URL
  - ! Aufnahme als SP in die Föderation

Shibbolisierung (einfacher Zugriffsschutz)

- Apache-basierter Zugriffsschutz

```
# .htaccess-Schutz
<Location /secure>
 AuthType Basic
 AuthUserFile /usr/admin/web/.htusers
 Require user groeper henne
</Location>
```

```
# Shibboleth-Schutz
<Location /secure>
 AuthType shibboleth
 ShibRequireSession On
 Require affiliation staff@rvs.uni-hannover.de
</Location>
```

- XML-basiert in SP-Konfiguration

```
<Host name="shibca1.gridlab.uni-hannover.de">
 <Path name="secure" authType="shibboleth" requireSession="true">
  <AccessControl>
   <AND>
    <OR>
     <Rule require="affiliation">staff@rvs.uni-hannover.de</Rule>
     <Rule require="affiliation">staff@nm.ifi.lmu.de</Rule>
    </OR>
    <Rule require="entitlement">dfn:pki:slcs</Rule>
   </AND>
  </AccessControl
 </Path>
</Host>
```

Shibboleth und LUH-IdM

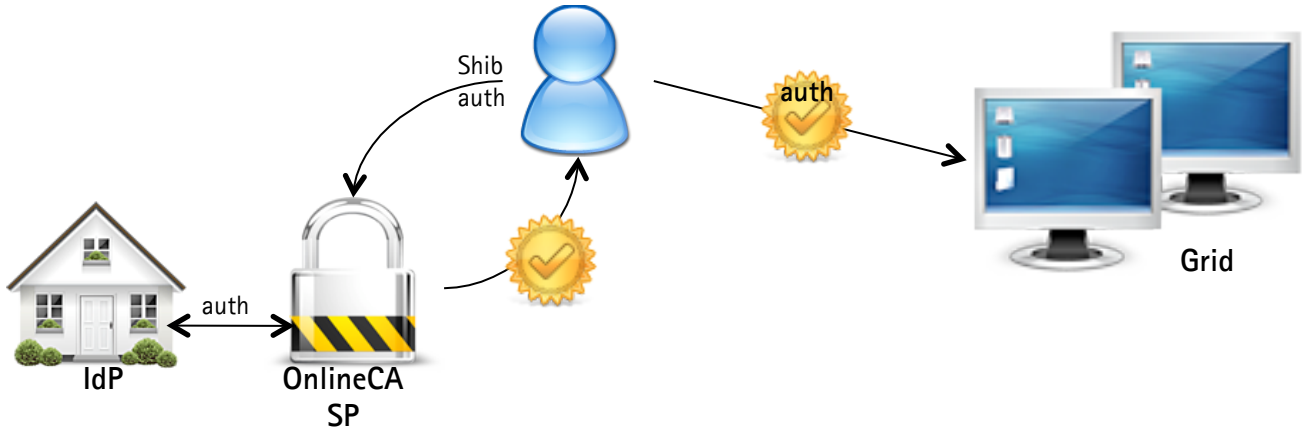
- Identitätsmanagement an der LUH seit WS 08/09
  - Studenten etabliert, Mitarbeiter folgen
- Shibbolisierung
  - Einsatz von Shibboleth geplant
  - LUH-IdM als Mitglied der DFN-AAI-Föderation
  - Nutzung fremder Dienste mit LUH-Accounts
    - z. B. Stud.IP anderer Universitäten oder Nutzung eines Bibliothekensystems aus Föderation

➢ Vortrag *Identitätsmanagement an der LUH* **morgen**

Forschung am RRZN: Shibboleth im Grid Computing

- Zugriff auf Authentifizierungsinformationen und Benutzerattribute der Heimatorganisation via Shibboleth möglich
- Authentifizierung im Grid-Computing typischerweise via X.509-Public-Key-Zertifikate

➢ Abbildung von Identitäten aus Heimatorganisationen auf kurzlebige Zertifikate via Online-Zertifizierungsstelle



Forschung am RRZN: Shibboleth im Grid Computing (2)

IdM der Heimatorganisation (LDAP-Eintrag)

```
# ldapsearch -b "ou=People,dc=rvs,dc=uni-hannover,dc=de" -x sn=henne
dn: uid=henne,ou=People,dc=rvs,dc=uni-hannover,dc=de
[...]
objectClass: eduPerson
uid: henne
cn: Benjamin Henne
sn: Henne
telephoneNumber: +49 511 762794366
mail: henne@rvs.uni-hannover.de
o: Leibniz Universitaet Hannover
ou: RRZN
eduPersonOrgDN: o=Leibniz Universitaet Hannover
eduPersonOrgUnitDN: ou=RRZN,o=Leibniz Universitaet Hannover
eduPersonPrincipalName: bhenne@rvs.uni-hannover.de
eduPersonAffiliation: staff
eduPersonPrimaryAffiliation: employee
eduPersonScopedAffiliation: staff@rvs.uni-hannover.de
eduPersonNickname: Benjamin
description: WiMi RVS RRZN Benjamin Henne
```

Kurzlebiges Zertifikat für Grid

```
#openssl x509 -in usercert.pem -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 5035 (0x13ab)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=de, DC=uni-hannover, DC=shibca, O=GridShibUsers
        Validity
            Not Before: Nov 18 09:29:43 2008 GMT
            Not After : Feb 12 21:29:43 2009 GMT
        Subject: DC=de, DC=uni-hannover, DC=shibca, O=GridShibUsers,
                 OU=UniHannover, CN=bhenne@rvs.uni-hannover.de
        [...]
```

Links

- Bibel: http://www.bibleserver.com/
- DFN-AAI: https://www.aai.dfn.de/
- eduPerson: http://middleware.internet2.edu/eduperson/
- OASIS: http://www.oasis-open.org/
- RRZN: http://www.rrzn.uni-hannover.de/
- Shibboleth: http://shibboleth.internet2.edu/

Abkürzungen

- AA Attribute Authority
- AAI Authentifizierungs- und Autorisierungs-infrastruktur
- AFP Attribute Filtering Policy
- AAP Attribute Acceptance Policy
- ARP Attribute Release Policy
- DFN Deutsches Forschungsnetz
- DS Discovery Service
- HTTP Hypertext Transport Protocol
- IdM Identity Management
- IdP Identity Provider
- LDAP Lightweight Directory Access Protocol
- OASIS Organization for the Advancement of Structured Information Standards
- PKI Public Key Infrastructure
- RDBMS Relationales Datenbank-Managementsystem
- SAML Security Assertion Markup Language
- SOAP Simple Object Access Protocol
- SP Service Provider
- SSO Single Sign-On
- SSL Secure Sockets Layer
- TLS Transport Layer Security
- URL Uniform Resource Locator
- WAYF Where Are You From
- XML eXtensible Markup Language