

Identity Management und domainübergreifende Infrastrukturen

Treffen des ZKI-AK Verzeichnisdienste,
Frankfurt 4.-5.10.2005

Peter Gietz, CEO, DAASI International GmbH
Peter.gietz@daasi.de



Directory Applications
for Advanced Security
and Information Management

- Motivationen für Identity Management in domainübergreifenden Infrastrukturen
- Kontakt- und Identity-Informationen
 - Schemaharmonisierung (hisPerson, SCHAC, HEPerson)
 - eva|wiss ein Verzeichnisdienst für die Forschung in Deutschland
 - nationales LDAP-Index-System
- Authentifizierung und Autorisierung
 - LDAP, DSML, SAML, SPML, XACML
 - Architekturen
 - Shibboleth

- Directory Applications for Advanced Security and Information Management International
- Nachfolgeinstitution von BMBF-DFN-Projekten zum Thema Verzeichnisdienste
- Offizielles Spin-Off der Universität Tübingen
- Vorlieben: Offene Standards, Open Source, Datenschutz, Forschung
- Kunden: Forschungseinrichtungen, Bibliotheken, Behörden, KMUs
- Expertise: Verzeichnisdienste, Authentifizierung, PKI, Identity Management, Informationsmanagement, Digital Libraries, XML, Semantic Web, Grid Computing
- Aktiv in: IETF, Internet2, GGF, TERENA, ZKI-AK Verzeichnisdienste, Teletrust AG7 „PKI“, bwconn:boss

Was soll Identity Management?

- Personen wollen:
 - Informationen über sich veröffentlichen, um z.B. kontaktiert werden zu können
 - Informationen über andere Personen erhalten
 - Sich authentifizieren, also ihre Identität beweisen, um Ressourcen und Dienste in Anspruch nehmen zu können
 - Im Netz bezahlen
- Organisationen wollen
 - Identitätsinformationen über Mitarbeiter oder Mitglieder verwalten
 - Benutzer ihrer Ressourcen verwalten
 - Konsistenz der Identitäten in verschiedenen Informationsspeicher erreichen
 - Vortäuschung falscher Identitäten verhindern
- Mobilität erhöht die Anforderungen an Identity Management

Was gehört zu Identity Management?

- Passwort-Verwaltung und –Synchronisierung
- Identitätszertifizierung mit Public Key Infrastructure
- Externe Identitätsdienste (MS Passport, Liberty Alliance)
- Single Sign On Mechanismen
- Rollenkonzepte und Berechtigungen
- Verwaltung des Zugriffs auf Ressourcen
- Authentifizierung und Autorisierung
- Verzeichnisdienste können genutzt werden zur Speicherung von Identitätsinformation, Passwörtern, Zertifikaten, Rollen und Berechtigungen, Policy
- Metadirectories dienen zur Synchronisierung verschiedener Datenspeicher und Vermeidung von Inkonsistenzen
- Provisioning Systeme verwalten Berechtigungen und versorgen Anwendungen mit Identitätsinformation
- Auditing- und Reportkomponenten sind notwendig, um Compliance zu rechtsverbindlichen Vorschriften zu erreichen (auch an Hochschulen?)

Von Identität zu Authorisierung

Datensätze

bilden Identitäten ab von

Personen

welche

Organisationsbeziehungen
und Eigenschaften

haben, die auf

Berechtigungen

gemappt werden, die den Zugriff auf

Dienste

Regeln, welche von

Service Providern

angeboten werden

Nach: Keith Hazelton, Univ. of Wisconsin-Madison:

Directory based Middleware Services, Internet2 Advanced CAMP, Boulder Colorado, 31-Jul-02

DAASI
International

Directory Applications
for Advanced Security
and Information Management

Motivationen für domainübergreifende Infrastrukturen

- Studenten werden immer mobiler, wechseln die Hochschule öfters
- Studiengänge der verschiedenen Hochschulen müssen kompatibel sein
- Forschung funktioniert immer vernetzter
 - eScience und Grid-Computing
 - Forscher aus verschiedenen Hochschulen benötigen Zugriff auf im Netz verteilte Ressourcen
- Verlagslizenzen für Datenbanken, die von Hochschulbibliotheken online gestellt werden, verlangen Autorisierungsattribute
 - Solche Lizenzen können auch an Hochschulverbünde erteilt werden

Bologna-Prozess

- Auch Europaweit wird hochschulübergreifendes Identity Management notwendig:
 - 1999 haben 29 europäische Minister für Bildung und Forschung die Bologna-Deklaration unterzeichnet, in der bis 2010 ein einheitlicher europäischer Hochschulraum angestrebt wird
 - Zur Erhöhung der Mobilität von Studierenden und Hochschulabgänger
 - Ein europaweit gültiger Hochschulabschluss soll über ein Credit-System erreicht werden
 - Das Credit-System soll im Rahmen von lebenslangen Lernen weiter ausgebaut werden

Metadirectory und Personenschema

- Konzept Metadirectory verwendet einen Verzeichnisdienst zur Synchronisierung von Datenbeständen aus verschiedenen Datenbankquellen
- Voraussetzung ist, dass alle zu synchronisierenden Daten im Verzeichnisdienst abbildbar sind
- Das entsprechende Schema muss standardisiert sein, damit verschiedene Anwendungen darauf zugreifen können
- Dies gilt umso mehr für hochschulübergreifende Systeme
- Internationale Standards sollten deshalb mindestens den Ausgangspunkt bilden:
 - Person, organizationalPerson, inetOrgPerson

- Wird weltweit zu einem defacto-Standard für Hochschulen, der durch nationale Schemata ergänzt wird
- Attributtypen z.T. USA-lastig spezifiziert
 - Kontrolliertes Vokabular für eduPerson(Primary)Affiliation:
 - faculty, student, staff, alum, member, affiliate, employee
 - Vorschlag Uni-Potsdam: guest
- eduPersonPrincipalName ist als Identitäts-Token gedacht:
 - „The "NetID" of the person for the purposes of inter-institutional authentication“
- eduPersonEntitlement zur Abbildung von Rechten:
 - „URI (either URN or URL) that indicates a set of rights to specific resources“
- eduPerson(Primary)OrgUnitDN zur Abbildung der Organisationszugehörigkeit bei einem flachen Personenbaum
- eduPersonOrgDN für organisationsübergreifende Verzeichnisse

Diskussion über eduPerson

- Drei der hier definierten Attribute (*eduPersonOrgDN*, *eduPersonOrgUnitDN* und *eduPersonPrimaryOrgUnitDN*) sind nur relevant, wenn die Personeneinträge nicht unter den dazugehörigen Organisationseinträgen eingetragen werden, sondern in einer flachen Hierarchie unter einem Eintrag wie z.B. "ou=Mitarbeiter".
- Ein solches Vorgehen hat aus zwei Gründen Vorteile:
 - Bei dem an Hochschulen häufiger vorkommenden Wechsel der Organisationseinheit muss nur das entsprechende Attribut geändert werden und nicht der ganze Personeneintrag von einer Stelle der Baumhierarchie zu einer anderen verschoben werden
 - Die Zugehörigkeit zu mehreren Organisationseinheiten lässt sich sehr einfach abbilden
- Der Vorteil, Personeneinträge in der Organisationshierarchie unterzubringen, soll hier aber nicht verschwiegen werden:
 - Zugriffskontrollregeln lassen sich wesentlich einfacher definieren, z.B. die Sekretärin der Organisationseinheit darf alle Einträge unterhalb der Organisationseinheit modifizieren.



Weitere Schemastandardisierung in Europa

- TERENA Projekt DEEP hat eine Umfrage zu Erweiterungen von eduPerson durchgeführt
 - www.daasi.de/projects/DEEP
- TERENA Task Force EMC2 (European Middleware Coordination and Cooperation)
 - SCHAC (Schema Harmonization Coordination) spezifiziert eine Liste von Attributen,
 - die nicht von eduPerson abgedeckt werden
 - Die insbesondere im Rahmen von Identity Management relevant sind (z.B. Geburtstag)
 - Eine Hauptmotivation ist der Bologna Prozess
 - Wird mit den Arbeiten an HisPerson koordiniert

Internet2

- Im Augenblick entsteht eine Internet2-Studie über nationale Erweiterungen von eduPerson:
 - Brendan Belinda, Peter Gietz: Higher Education Person
 - Arbeiten in SCHAC und zu hisPerson wurden berücksichtigt



Harmonisierungsentwicklung in Deutschland

- Durch die Spezifizierung eines HIS-Personenschema wird eine Schema-Vereinheitlichung in Deutschland erreicht, welcher hochschulübergreifenden Datenaustausch erleichtern wird
- Diskussionsprozess in der Community hat weitere Attributvorschläge hervorgebracht, z.B. hisProgressOfStudy
 - Weitere Änderungsvorschläge in Bezug auf namensgebende Attribute (uid statt cn, Einsatz von multivalues RDNs)
 - Eine Version 1.0 der Schemaspezifikation wird diese Vorschläge berücksichtigen
- Erste Implementierungsansätze in der neuen HIS-Software (SVA, KOP, FSV, BAU)
 - Für HIS-interne Systemverwaltung können Rollendaten aus LDAP gelesen werden und für Zugriffsrechte und Views, etc. ausgewertet werden

Hochschulübergreifendes Verzeichnis

- **Eva|wiss (Elektronisches Verzeichnis für Anwender in der Wissenschaft)**
 - Nachfolgedienst von AMBIX
 - Erweiterte Such- und Datenänderungs-Möglichkeiten
 - Erweiterter Satz von Attributen, z.B. Photo, Arbeitsgebiete, Link auf CV, Link auf Weblog, Instant Messaging Ids, etc.
 - Neues Businessmodell:
 - Grundeintrag kostenlos, erweiterter Eintrag 7 Euro pro Jahr pro Person
 - Gesamtpakete und erweiterte Dienste für Hochschulbeteiligung

Ein deutschlandweiter LDAP-Index

- Wurde im Rahmen der DFN-Projekte betrieben
 - Jetzt nur noch best effort
- Ein Relaunch wie bei AMBIX -> eva|wiss ist geplant
 - Allerdings kann der nicht auch von DAASI vorfinanziert werden
 - Es fehlt nach wie vor ein tragfähiges Finanzierungsmodell für solche hochschulübergreifenden Infrastrukturdienste



AA(A)

- Authentifizierung und Autorisierung (und Accounting)
- Im Folgenden ein kleiner Technologieüberblick in Bezug auf hochschulübergreifende Strukturen
- Hier spielt XML eine wesentliche Rolle
- Allerdings sind alle hierbei relevanten XML-Standards kompatibel zu LDAP

LDAP und XML

- DSML: Directory Service Markup Language
 - Bildet das komplette Informationsmodell ab
 - Kann also beliebige LDAP-Daten in einem XML-Format darstellen
 - In Version 2.0. Können auch alle LDAP-Operationen abgebildet werden
- XED: XML enhanced Directory
 - Neue Arbeitsgruppe in der IETF
 - XML Daten können vollständig in LDAP Server abgebildet werden
- Grundsätzlich sind die Datenmodelle von LDAP und XML kompatibel

DSMLv1 Struktur

```
<dsml:dsml xmlns:dsml="http://www.dsml.org/DSML">
    <!-- a document with both -->
    <dsml:directory-schema>
        <dsml:class id="..." ...>...</dsml:class>
        <dsml:attribute-type id="..." ...>...</dsml:attribute-type>
    </dsml:directory-schema>
    <dsml:directory-entries>
        <dsml:entry dn="...">...</dsml:entry>
        <dsml:entry dn="...">...</dsml:entry>
        <dsml:entry dn="...">...</dsml:entry>
        ...
    </dsml:directory-entries>
<dsml:dsml>
```



DSMLv1 Eintrag

```
<dsml:entry dn="uid=prabbit,ou=development,o=bowstreet,c=us">
  <dsml:objectclass>
    <dsml:oc-value>top</dsml:oc-value>
    <dsml:oc-value>person</dsml:oc-value>
    <dsml:oc-value>organizationalPerson</dsml:oc-value>
    <dsml:oc-value>inetOrgPerson</dsml:oc-value>
  </dsml:objectclass>
  <dsml:attr name="cn"><dsml:value>Peter Rabbit</dsml:value>
  <dsml:attr name="sn"><dsml:value>Rabbit</dsml:value></dsml:attr>
  <dsml:attr name="uid"><dsml:value>prabbit</dsml:value></dsml:attr>
  ....
</dsml:entry>
```



DSMLv2 Struktur

➤ Anfrage:

```
<batchRequest xmlns="urn:oasis:names:tc:DSML:2:0:core">
  <modifyRequest>...</modifyRequest>
  <addRequest>...</addRequest>
  <delRequest>...</delRequest>
  <addRequest>...</addRequest>
</batchRequest>
```

➤ Antwort:

```
<batchResponse xmlns="urn:oasis:names:tc:DSML:2:0:core">
  <modifyResponse>...</modifyResponse>
  <addResponse>...</addResponse>
  <delResponse>...</delResponse>
  <addResponse>...</addResponse>
</batchResponse>
```

DSMLv2 Modify-Beispiel

➤ Anfrage:

```
<modifyRequest dn="CN=Bob Rush,OU=Dev,DC=Example,DC=COM">
  <modification name="telephoneNumber" operation="replace">
    <value>536 354 2343</value>
    <value>234 212 4534</value>
  </modification>
  <modification name="sn" operation="replace">
    <value>Rush</value>
  </modification>
</modifyRequest>
```

➤ Antwort:

```
<modifyResponse>
  <resultCode code="53" descr="unwillingToPerform"/>
  <errorMessage>System Attribute may not be modified</errorMessage>
</modifyResponse>
```

SAML

- Die Security Assertion Markup Language (SAML) definiert einen Standard, sicherheitskritische Informationen in XML zu beschreiben und auszutauschen.
- Insbesondere zum Austausch von Authentifizierungs- und Autorisierungsinformation
- SAML v.1.1. Herausgegeben von OASIS (www.oasis.org)
- Unterstützt Passwörter, Kerberos, Zertifikate (X.509, SPKI, XKMS, SSL/TLS) und XML digitale Signaturen
- Wird z.B. verwendet in Liberty Alliance, Shibboleth, PAPI
- Aber auch in Provisioning-Produkten von:
 - IBM Tivoli, Netegrity, Novell, Oblix, RSA Security, Sun
 - Geplant in Novell nSure und CA eTrust, .Net
 - Achtung: SAML-Kommunikation ist eher Komplex (mind. 6 Kommunikationsschritte)
- Opensource Implementierung einer SAML-Library:
 - <http://www.opensaml.org/>

SAML

- SAML definiert Protokolle, durch welche Clients sog. Assertions von SAML-Autoritäten anfordern und deren Antworten empfangen können.
- Die SAML-Autoritäten können diverse Informationsquellen, beispielsweise externe Policy-Repositories oder in der Anfrage bereits enthaltene Assertions, benutzen, um ihre Antworten zu generieren.
- Assertions werden dann zu einem SAML-Ausweis gebündelt, der zusammen mit der Anforderung an den PEP der angeforderten Ressource geschickt wird.
- Dieser entscheidet dann über den Zugriff
- Der SAML-Ausweis wird digital unterschrieben, um Modifikationen zu verhindern.
- Deswegen können SAML-Ausweise wiederverwendet werden, ohne eine erneute Authentifizierung erforderlich zu machen.
- SAML ermöglicht damit single sign-on (SSO)

Bestandteile von SAML 1/2

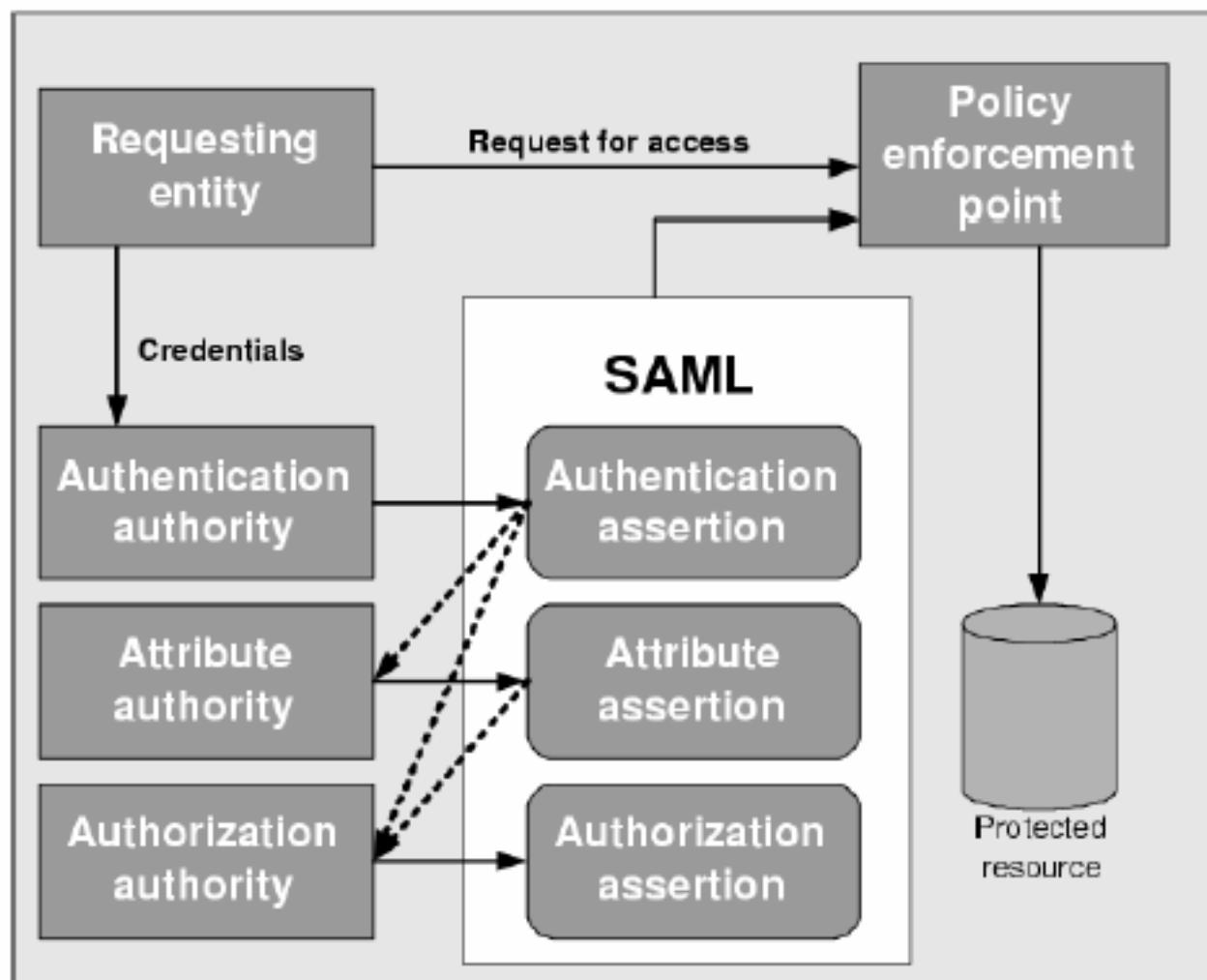
► 1.) Assertion:

- Aussagen einer Identitäts-Authorität (IA) über einen Benutzer oder einer sonstigen Identität
- IA ist eine vertrauenswürdige Quelle für Authentifizierung und Autorisierung
- Es gibt drei Arten der Assertion:
 - Authentifizierung
 - Autorisierung
 - Attributierung

Bestandteile von SAML 2/2

- 2.) Protokolle
 - Jeder Assertion-Typ hat ein eigenes Protokoll (Request/Response)
 - Zusätzlich: Artefacts: Zeiger auf Assertions
- 3.) Bindings
 - Transportmechanismus für die SAML-Protokolle
 - SOAP über HTTP
 - Direktes HTTP in Planung
- 4.) Profiles
 - Beschreibt wo im Transportmechanismus die SAML-Statements zu finden sind. Bisher definiert für
 - SOAP
 - Web Browser (HTML-Formulare, Web-SSO)

SAML Architektur



Nach: RUBENKING, NEIL J.: Securing web services.
PC Magazine, 2002.

DAASI
International

Directory Applications
for Advanced Security
and Information Management

Wo wird SAML eingesetzt?

- Shibboleth (s.u.) SSO mit SAML
- WS-Security verwendet SAML um SOAP-Messages zu sichern
- Liberty Alliance verwendet SAML für SSO und um Identity-Information an Web Services zu vermitteln



XACML

- Extended Access Control Markup Language
- OASIS-Standard
- Es gibt XACML-Profile für SAML und LDAP/DSML, sowie für RBAC
- Generisch: Zugriffsregeln (Policy) können Anwendungsunabhängig spezifiziert werden
- Verteilt: Eine Policy kann sich auf eine andere an einem anderen Ort gespeicherte Policy beziehen
- Komplex: Im Prinzip eine eigene Programmiersprache
- Da Access Controll oft sehr produktspezifisch angesehen wird, ist die Implementierung von XACML im Gegensatz zu den verwandten Standards nicht sehr häufig anzutreffen

XACML-Elemente

- PolicySet: Container für Policies bzw. weitere PolicySets
- Policies und policySets können mit Algorithmen kombiniert werden
- Bedingungen setzen sich zusammen aus Subjekt, Ressource und Aktion
- Environment
- Policy Decision Point (PDP)
- Policy Enforcement Point (PEP)
- Target: Sammlung vereinfachter Bedingungen
- Rule: Access Control Regeln
- Attribute

XACML-Beispiel

```
<Policy PolicyId="SamplePolicy",
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:
        rule-combining-algorithm:permit-overrides">
<Target>
    <Subjects> <AnySubject/> </Subjects>
    <Resources>
        <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
(DataType="http://www.w3.org/2001/XMLSchema#string">SampleServer
</AttributeValue>
            <ResourceAttributeDesignator
(DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-
id"/>
            </ResourceMatch>
        </Resources>
        <Actions>
            <AnyAction/>
        </Actions>
    </Target>
```

XACML-Beispiel

```
<Target>
    <Subjects>
        <AnySubject />
    </Subjects>
    <Resources>
        <AnyResource />
    </Resources>
    <Actions>
        <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">login</Attribute
                Value>
            <ActionAttributeDesignator
                DataType="http://www.w3.org/2001/XMLSchema#string"
                AttributeId="ServerAction" />
        </ActionMatch>
    </Actions>
</Target>
```

Das Interdomänen-Problem

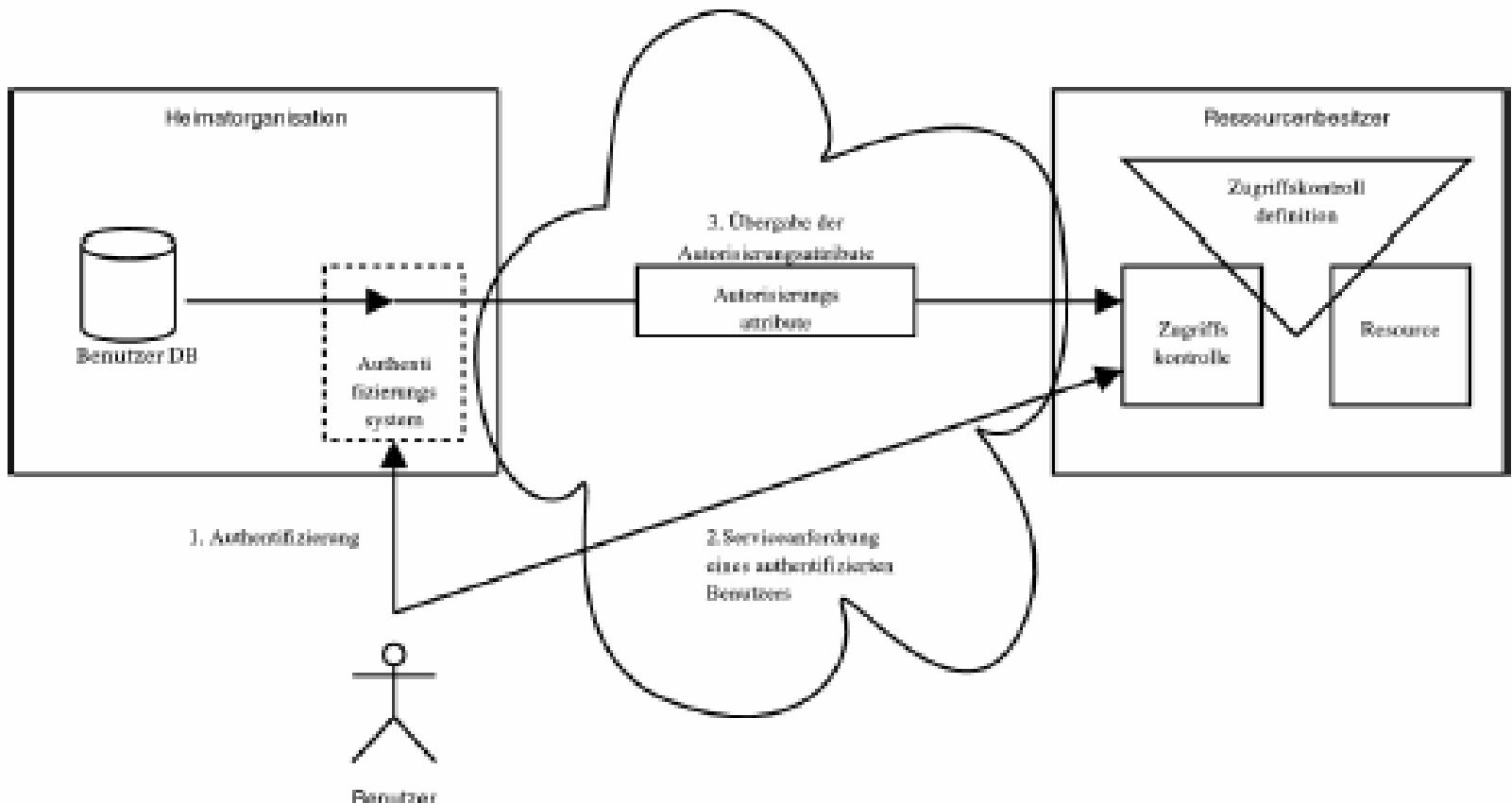


Abbildung 1: Modell eines Systems zur Authentifizierung und Autorisierung (nach [45])

Aus Strattmann: Authentifizierung und Autorisierung in verteilten Systemen, DA Tübingen 2004
nach TERENA TF-AACE: Deliverable B.1.

AAAARCH

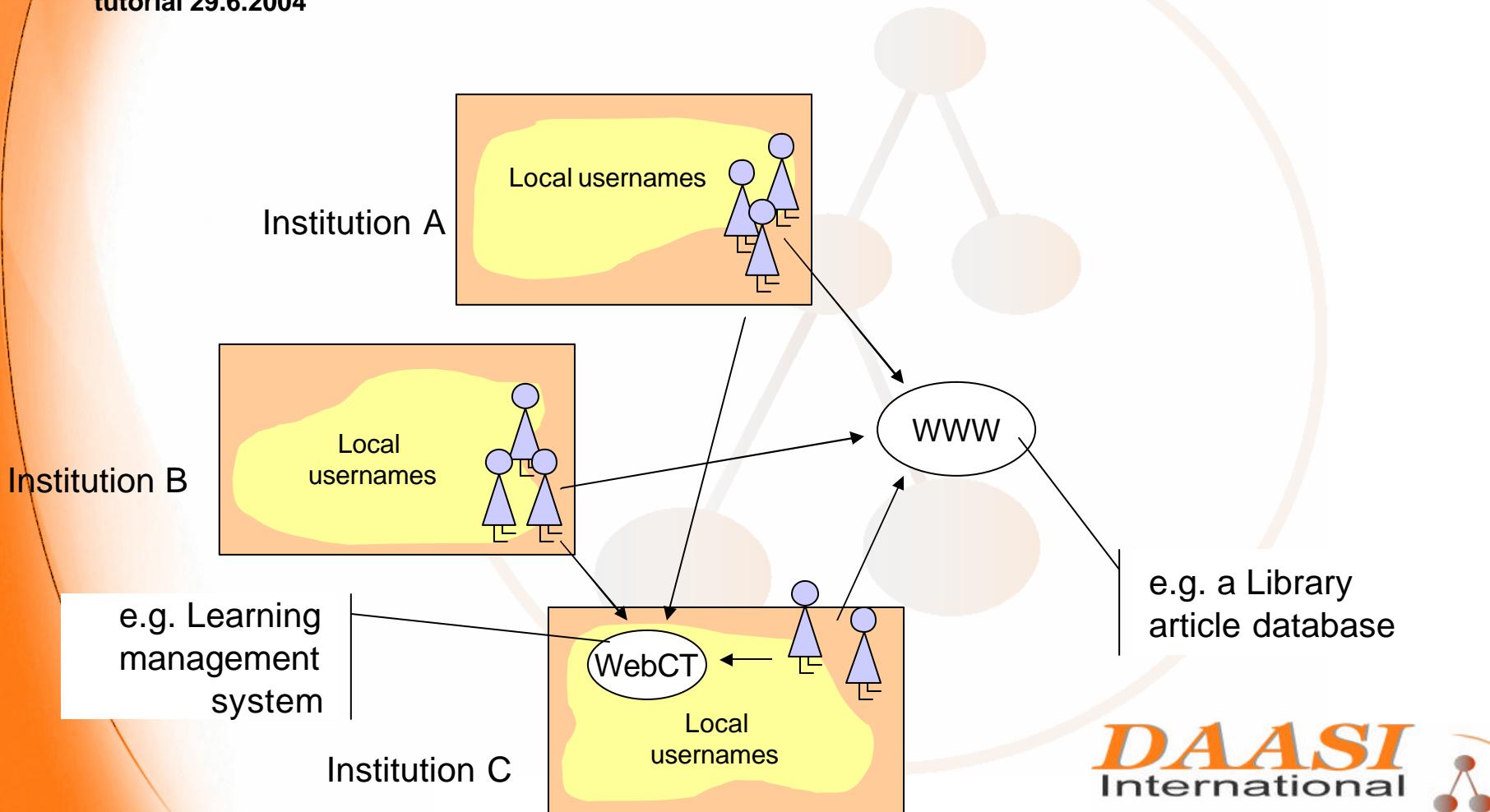
- Authorization, Authentication and Accounting
ARCHitecture research group (AAAARCH)
- Forschungsgruppe der IRTF
- Ziel:
 - Kapselung der AAA-Prozesse
 - ein generisches Modell für eine Gruppe von untereinander verbundenen AAA-Servern zu definieren
 - und eine Schnittstelle, die es Anwendungen erlaubt, AAA-Funktionen abzurufen.
 - Verschiedene Architekturmodelle mit folgenden Entitäten:
Benutzer, Heimorganisation, Service-Provider

Policy in AAAArch

- PRP
 - Eine Policy wird an einem Policy Retrieval Point (PRP) abgefragt
- PDP
 - an einem Policy Decision Point (PDP) ausgewertet
- PEP
 - an einem Policy Enforcement Point (PEP) durchgesetzt.
- AAA-Server
 - kann eine Policy abfragen und auswerten
- Servicegerät
 - kann eine Policy durchsetzen
- Policy-Repositories
 - können bei AAA-Servern angelegt werden oder sich anderswo im Netzwerk befinden.
- PIP
 - Informationen darüber, welche Policybedingungen ausgewertet werden, sind an sogenannten Policy Information Points (PIP) erhältlich.

Was ist föderierte Identität ?

Aus: Mikael Linden, Cross-organisational user administration aka Federated identity, EUNIS 2004 tutorial 29.6.2004



Shibboleth

- Internet2/MACE-Projekt
 - über Architekturen, Regelwerken, und praktischen Technologien zu AA
 - OpenSource Implementierung einer domainübergreifenden AA-Lösung
- Ziel: gemeinsame AA-Infrastruktur für Universitäten in USA



Shibboleth Architektur: Ursprungsdomäne

➤ Handle Server

- Triggert das lokale Campus-Authentifizierungssystem
- Authentifiziert den Benutzer mit Hilfe der lokalen Authentifizierungsmechanismen
- Erzeugt handles und merkt sich Mapping handle/User

➤ Attribute Authority

- Sammelt Attribute von Benutzern
- Übermittelt auf Verlangen die Informationen, die ein Benutzer freigegeben hat
- Gibt nur notwendige Attribute nach außen

➤ SHIRE

- Shibboleth Indexical Reference Establisher
- Umbenannt in Assertion Consumer Service
- Besorgt einen Handle zu dem Benutzer, ohne weitere Informationen über den Benutzer zu benötigen.
- Ohne diesen Handle wird der Benutzer zum WAYF-Server umgeleitet, um einen Handle zu besorgen

➤ WAYF

- Where are you from
- Leitet den Benutzer zurück zu seiner Heimorganisation

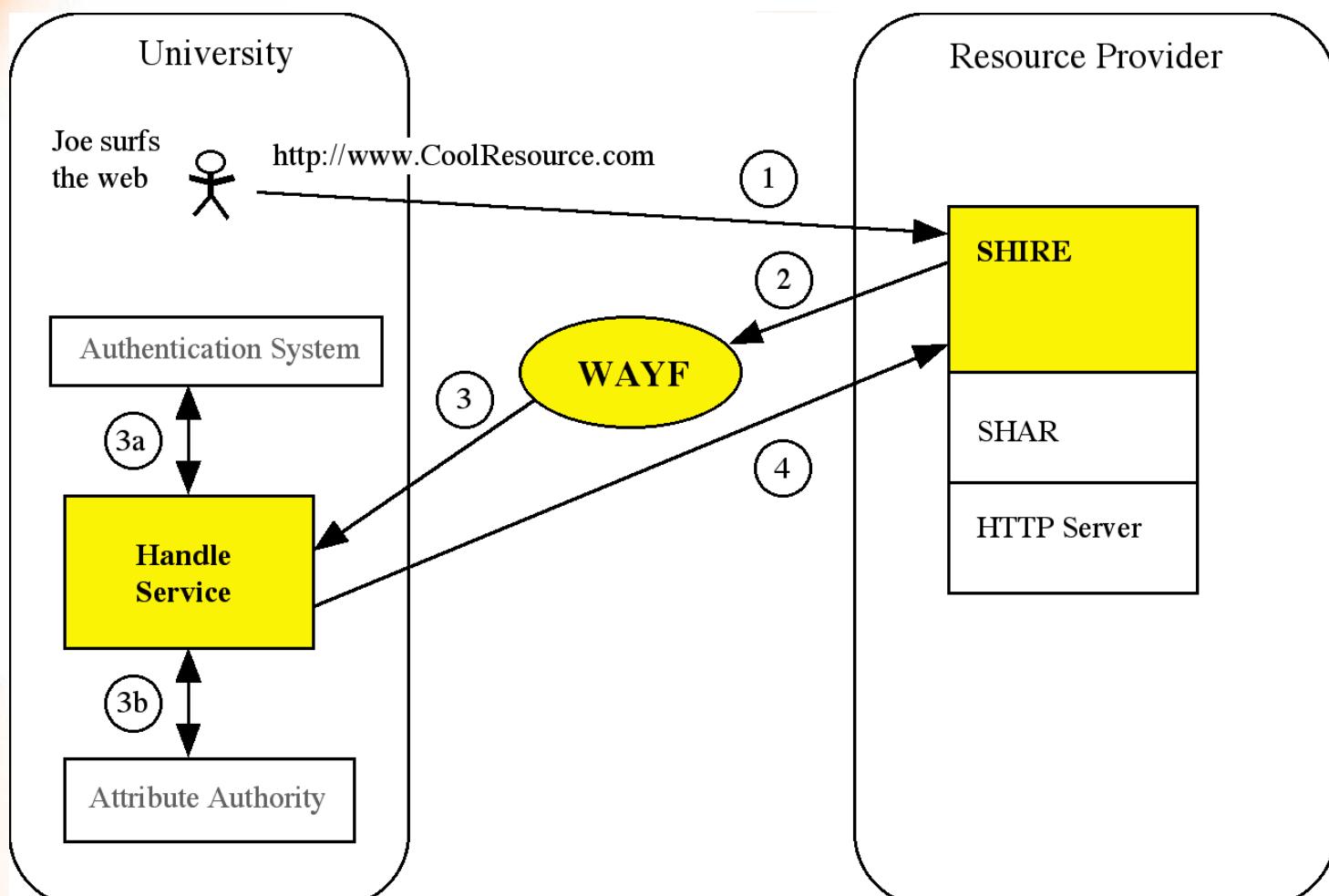
➤ SHAR

- Shibboleth Attribute Requestor
- Umbenannt in Attribute Requestor
- Besorgt mit Hilfe des Handles die vom Benutzer freigegebenen Informationen von der AA

➤ RM Resource Manager

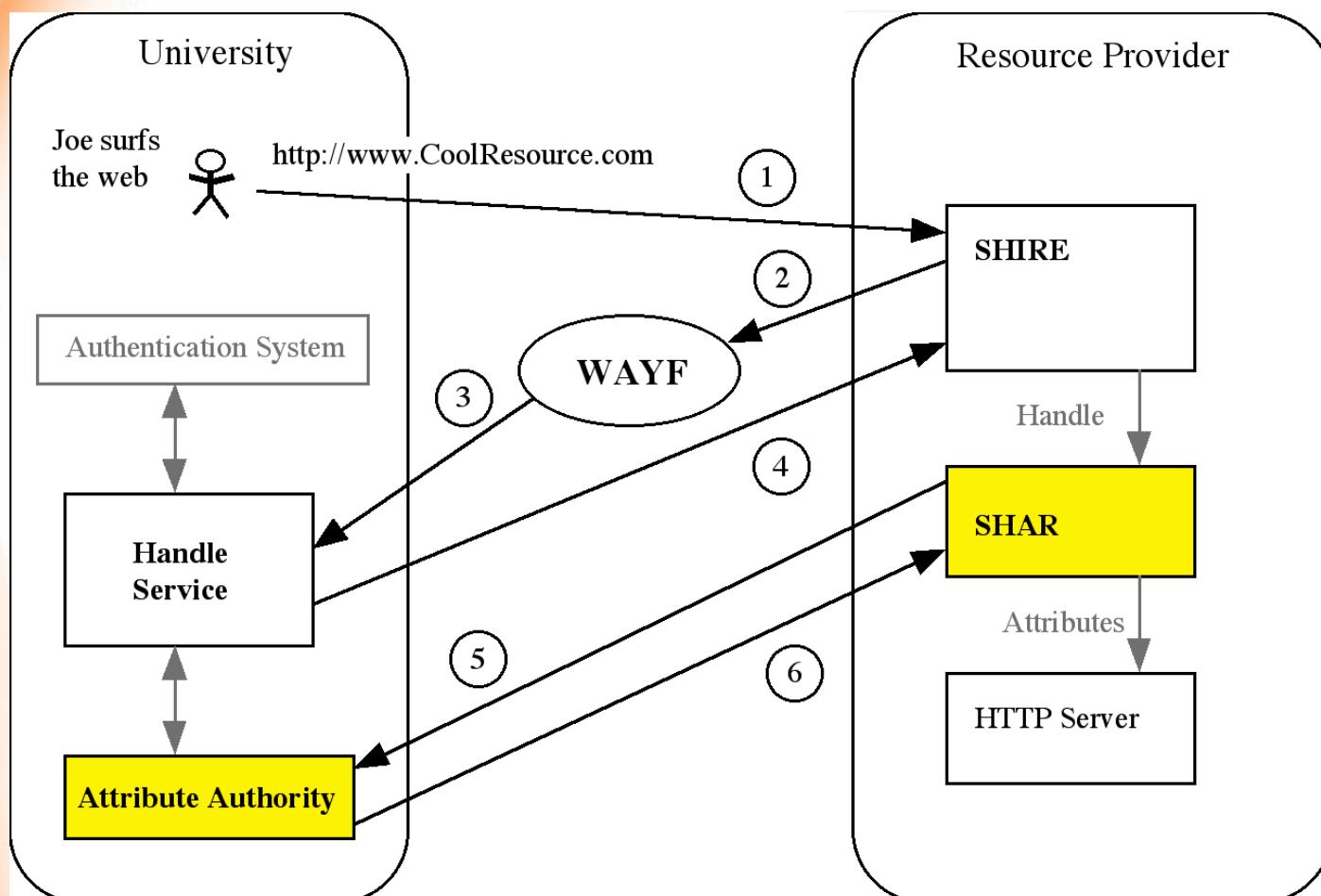
- Entscheidet über den Zugriff
- basierend auf den erhaltenen Informationen.

Shibboleth Authentifizierung



Aus: Ken Klingensteins: Shibboleth Update, ALA May 1, 2002,
<http://shibboleth.internet2.edu/shib-presentations.html>

Shibboleth Autorisierung



Aus: Ken Klingenstein: Shibboleth Update, ALA May 1, 2002,
<http://shibboleth.internet2.edu/shib-presentations.html>

Neue Spezifikationen

- **Alle Shib-Dokumente unter**
<http://shibboleth.internet2.edu/shibboleth-documents.html>
- **Shibboleth Architecture Protocols and Profiles**
 - **10 September 2005**
 - internet2-mace-shibboleth-arch-protocols-200509
- **Shibboleth Architecture Technical Overview**
 - Working Draft 02, 8 June 2005
 - draft-mace-shibboleth-tech-overview-02

Implementierungen von Shibboleth

- Mehrere Federations of Trust in Amerika, z.B.:
 - inCommon:
 - Internet2-Community
 - Zentralisierter WAYF-Dienst
 - Authentifizierung basiert auf einer PKI
 - Gemeinsamer Satz von Attributen
- Aber auch in Europa, z.B. UK, Finnland und Schweiz
 - SWITCH AAI-Projekt könnte Vorbild für Deutschland sein, siehe www.switch.ch/aai
- Im Bibliotheksreich scheint man die Nützlichkeit von Shib entdeckt zu haben:
 - Universitätsbibliothek Freiburg
- Aber auch im Grid-Computing



GridShib

- Integration von Shibboleth im Globus Toolkit (die Opensource Referenz für Grid computing)
 - <http://grid.ncsa.uiuc.edu/GridShib/>
- Zweijahresprojekt, Dezember 2004 gestartet
- NSF Middleware Initiative (NMI) Grant:
Policy Controlled Attribute Framework
- Ermöglicht Autorisierung im Grid
- Verwendung eines Identifiers in einem X.509-Zertifikat als Subject-Handle
- Virtuelle Organisationen einigen sich auf den Satz von Attributen
- Gridshib wird im Rahmen des D-Grid-Projekts evaluiert
 - DGI IP Fachbereich Security, AP AAI

Vielen Dank für Ihre Aufmerksamkeit!

- Noch Fragen?
- DAASI International GmbH
 - www.daasi.de
 - Info@daasi.de



DAASI
International

Directory Applications
for Advanced Security
and Information Management

