H. Schier IVS-CPT

M. Palzenberger MPDL

Shibboleth שבולת

- hebräisch, wörtlich “Getreideähre”
- wird synonym zu Passwort gebraucht

  Richter 12, Vers 5:

  “Gilead besetzte die nach Efraim führenden Übergänge über den Jordan. Und wenn efraimitische Flüchtlinge (kamen und) sagten: Ich möchte hinüber!, fragten ihn die Männer aus Gilead: Bist du ein Efraimiter? Wenn er Nein sagte, forderten sie ihn auf: Sag doch einmal «Schibbolet». Sagte er dann «Sibbolet», weil er es nicht richtig aussprechen konnte, ergriffen sie ihn und machten ihn dort an den Furten des Jordan nieder. So fielen damals zweiundvierzigtausend Mann aus Efraim.“

- Aussprache des Schin: שִׁבֹּולֶת (Schibboleth) שִׂבֹּולֶת (Sibboleth)
- deutsches Shibboleth: “Eichkatzenschwanz”

  Oachkatzlschwoaf gegen Eekkattensteert

  „Schornsteinfeger Stefan fischt im Nest nach Wurst.“

Shibboleth Internet2

- **Internet2**
  Weiterentwicklung der nicht-kommerziellen Internet-Technologie, vor allem im Bereich der verteilten Höchstleistungsrechenzentren.
  University Corporation for Advanced Internet Development (UCAID)
  - 100 Gigabit/s Verbindung zwischen Ost- und Westküste der USA, 10 Gigabit-Anschluss der Teilnehmer
  - Deutschland: X-Win vom DFN
    bis jetzt 10G, diese Jahr 20 Gigabit/s Anschlüsse
- **MACE** Middleware Architecture Committee for Education
  - MACE-DIR, directory schema
  - MACE-PKI, public key infrastructure
  - MACE-Shibboleth,
    web-based inter-institutional resource sharing mechanism
  - MACE-WebISO, web initial sign-on

Nutzung von geschützten Ressourcen I

- Wer Bist Du?
  - Authentifizierung
  - Benutzerkennung / Passwort
  - Hardwaretoken (Smartcard) / Passwort
  - Softwaretoken (öffentlicher Schlüssel) / (Passwort)
  - ...
- Was darfst Du?
  - Nichts
  - Alles
  - nur lesen
  - lesen und schreiben

Nutzung von geschützten Ressourcen II

- Woher kommst Du?
  - schwacher Ersatz für
    „Wer bist Du / Was darfst Du“
  - „einfach“ zu verwalten
    sehr viel weniger Herkunftsnetze als Benutzer
  - keine differenzierte Rechte möglich
- Verlagerung des Problems auf Netzzugang
  - Netz-Identität gegen persönliche Identität
  - verschiedene Netze mit verschiedenen Rechten
    „Gästenetze“
  - Netzstruktur wird aufgebläht
    mehrstufige interne Firewalls

Netzzugang

- grundlegende Anforderung in der Wissenschaft
- zur Zeit noch über Ortsgebundenheit (IP-Adresse)
- historisch
  - Rechner waren Riesenkisten, nicht beweglich
- im Institut alle Rechte
  - Annahme: IP-Adresse gehört zu Lokalität
- außerhalb des Institutes keine Rechte
  - Rechner sind mobil
  - Institute werden verteilt (virtuell)
- nicht mehr akzeptabel

Idee: „Netzwerke erweitern“

- Verschleierung der Herkunft
  - viele Verträge basieren auf der Lokalität des Benutzers, IP-Adressen
  - Aussagekraft einer IP-Adresse wird heruntergesetzt
- Vertrauensbruch gegenüber dem Vertragspartners
  - IP-Adresse wird beliebig umgeschrieben

- Problem des ungeschützten Datenverkehrs
  - „jeder“ kann mitlesen
- Schutz auf Transportebene,
  - Verschlüsselung
- Tunnellösungen
  Virtual Privat Networks (VPN)
- Stellvertreterlösungen (Proxies)
  siehe Vortrag Biliothekstagung 2003
- technisch komplexe Lösungen
- **Lösung des falschen Problems**

Zugangskontrolle auf Dienstebene

- ermöglicht abgestufte Berechtigungen für Benutzer (Rollen)
- keine (falsche) Annahme über Lokalität
- Problem: unzählige Benutzer
  - Applikation muss die Benutzer verwalten
- **jede** Applikation muss die Benutzer verwalten
  - ein Benutzer ist in vielen verschiedenen Systemen
- Wiedererfindung des Rades
- Multiplikation des Problems
  - Vermehrung der Angriffspunkte

zentrale Benutzerverwaltung

- Historisch
  - klassisches Rechenzentrum
  - ein Rechner, ein Verzeichnis
- „zentral“ auf Arbeitsgruppenebene
  - früher ein Rechner, ein Verzeichnis
  - heute viele Rechner, (möglichst) ein Verzeichnis
    z.B MS Active Directory
- „zentral“ auf Campusebene
- „zentral“ auf Organisationsebene
- „zentral“ auf Nationaler Ebene

  Athens (in England, wird gerade abgeschafft)

Probleme zentraler Benutzerverzeichnisse

- Datenschutz
  - schlechte Beispiele, MS-Passport, Kreditdaten, Steuerdaten ...
- Aktualität
  - wie schnell wird ein ein Benutzer eingetragen
  - wie schnell wird ein Benutzer ausgetragen
- Flexibilität
  - wie können verschieden lokale Strukturen abgebildet werden
- Validität
  - gibt es den Benutzer noch
  - wer darf an- und abmelden
  - werden Benutzer überhaupt entfernt

Kopplung von Benutzerverwaltungen

- „Zentral“ ist eine Frage der beschränkten Sichtweise
- Austausch von Daten zwischen „zentralen“ Verzeichnissen
  - historisch durch Kopplung von Großrechnern
- Kopieren von Benutzerdaten
  - erlaubt Filtern, Konvertieren
  - funktioniert nur im „selben“ Netz
- Hierarchische Verzeichnisdienste
  - „wenn ich Dich nicht kenne, dann frage ich den nächsten“
  - verteilte Verzeichnisse

Directory Services

- proprietäre Verzeichnissdienste
  - MS Active Directory
  - Novell
  - Sun
- Offen Verzeichnisdienste
  - Radius
  - LDAP
- Schutz der Daten immer auf Transportebene
  - verschlüsselter Kanal
  - SSL
  - TLS

Kopplung auf Applikationsebene

- Idee:

  einmal registrieren und Ticket (temporärer Ausweis) beim Heimatinstitut abholen
- dann zu allen anderen Diensten das Ticket verschicken
- Ersatz von User-ID/Passwort durch Server-Zertifikat mit Beschreibung

- Anorderungen
  - Nachricht muss abgesichert sein (verschlüsselt)
  - Austausch der Nachrichten muss geregelt sein
  - trotzdem lesbar von berechtigten Empfängern
  - Inhalt muss abgesprochen sein

Shibboleth

- verteilter Single-Sign-On Service (SSO) für geschützte Web-Anwendungen

  mittlerweile auch für Grid-Computing (nicht Web-Anwendung)
- Offener Standard
  - Internet 2, MACE
  - Platformunabhängig (MS-Windows, Linux, Solaris, Mac)
- basiert auf **SAML**
  Securtity **A**ssertion **M**arkup **L**anguage (xml Sprache)
- wird weltweit eingesetzt
  - Nationale Zusammenschlüsse (Federations)
  - lokale Zusammenschlüsse
    DAML (MPI-NL + 2 Partner)

Shibboleth Föderationen

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

Security Assertion Markup Language (SAML)

- **SAML** besteht aus:
  - **SAML-Assertions**
    hier werden Informationen zu Authentifizierung, Autorisierung sowie weiter Session-Attribute hinterlegt
  - **SAML-Protokoll**
    definiert die Interaktion zwischen einem SAML-Requester und einem SAML-Responder
  - **SAML-Bindings**
    legen fest, wie SAML-Request-Response-Nachrichten über Standard-Übertragungsprotokolle abgebildet werden
  - **Profile**
    spezifizieren, wie SAML Assertions in ein Message Framework oder ein Protokoll eingebunden und wieder extrahiert werden
- Einzelheiten siehe Poster

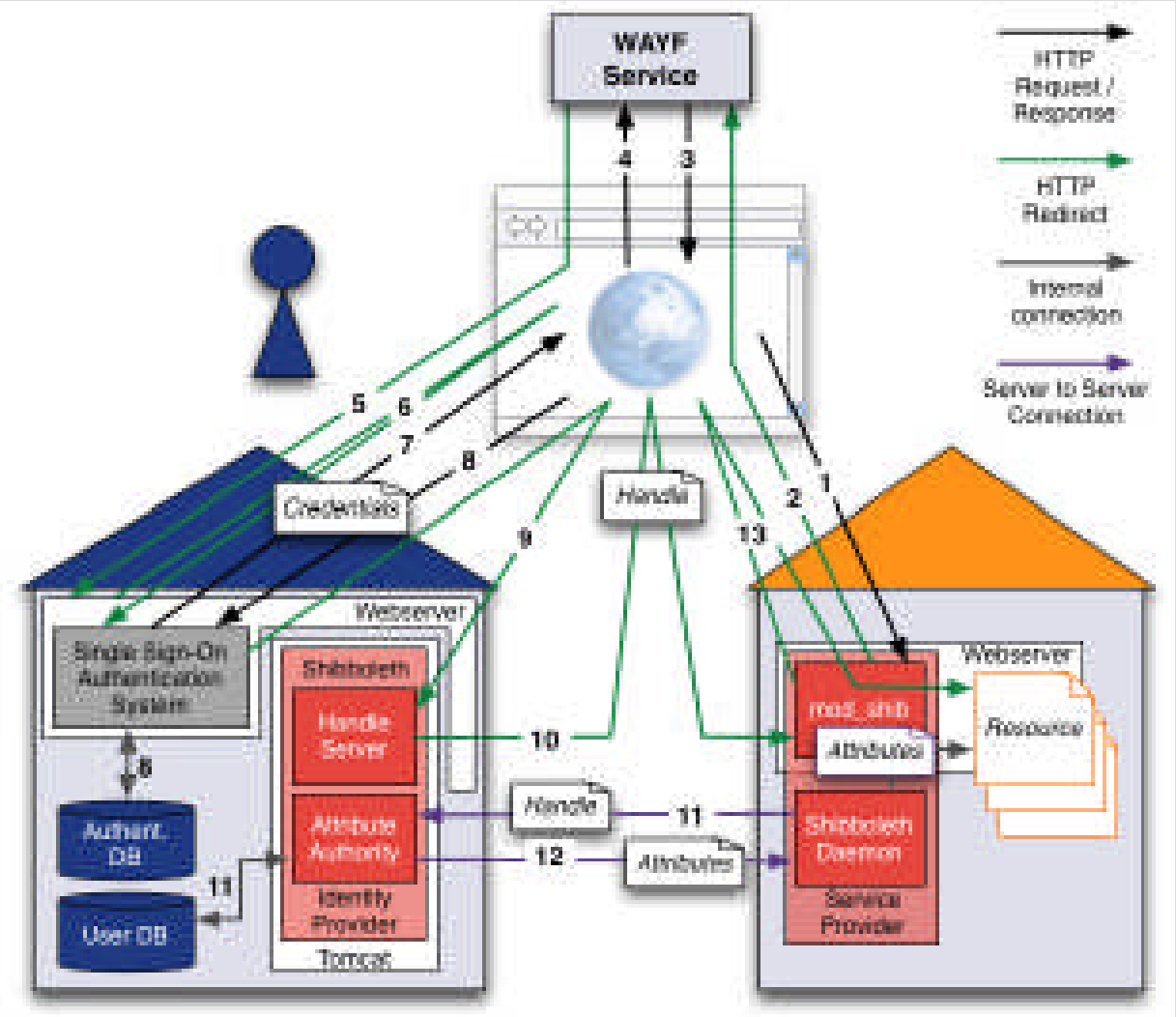
Bestandteile von Shib

- **Service Provider (SP)** bietet einen geschützten Dienst an (Zugriffskontrolle)

  erwartet

  1. erfolgreiche Authentifizierung
  2. Attribute
- **Identity Provider** (Heimat-Institut)
  - Authentifizierung (frei wählbar)
    - Benutzerverwaltung (frei wählbar)
  - Autorisierung (Bestandteil von Shibboleth)
    - Benutzerverwaltung (frei wählbar)
- **Discovery-Service** „**W**here **A**re **Y**ou **F**rom?“ (WAYF)
  - Liste der Teilnehmer (IdPs)
  - optional

Shib Ablauf Diagramm



Quelle: http://www.switch.ch/aai/demo/expert.html

Schutz der Privatsphere

- Wer bekommt was zu sehen?
- SP
  - Forderung nach einer Liste von Attributen
- IdP
  - erzeugt Attribut-Liste pro User
  - attribute release policy
    filtert die Attribut-Liste für jeden SP
  - erzeugt die verschlüsselte Quittung, **assertion**,
    die nur der jeweilige SP lesen kann
    (verschlüsselt, unterschrieben)

Attribute

- Attribute bilden die Grundlage für dieAutorisierung und Zugriffskontrollein 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-Providernnotwendig, die durch Verwendung eines einheitlichen Schemas vereinfacht werden!
  - einheitliches Schema = Föderation, federation
- Voraussetzung sind **verlässliche Benutzerdaten**, also eine funktionierende **Benutzerverwaltung**, Identitty-Management

Attribute Schemata

- der Inhalt von Attributen werden in Schemata definiert
- eduPerson Schema
  - von InCommon (USA)
  - wurde von allen Anderen übernommen (und modifiziert)
- wichtige Attribute in eduPerson:
  - eduPersonScopedAffiliation
  - eduPersonEntitlement
    - urn:mace:dir:entitlement:common-lib-terms
  - eduPersonPrincipalName
  - eduPersonTargetedID

Attribute und Werte

- eduPersonScopedAffiliation **Attribut**
  - zulässige **Werte**
    member, faculty, staff, employee, student, alumni, affiliate
- Problem: an US-Unis ausgerichtetes Schema
- was ist ein „student“?
- keine Werte für
  - Gäste
  - Gastwissenschaftler
  - Kooperationen

Attribute für externe SPs

- Service-Providerkommen mit wenigen Attributen aus, häufig verwendet werden:
  - eduPersonAffiliation fkf.mpg.de
  - eduPersonEntitlement
  - eduPersonPrincipalName h.schier@fkf.mpg.de
  - eduPersonTargetedID opake Kennung, beliebiger Hash-Wert
- Web-Learning Anwendungen wollen (sehr) viele Attribute
- Interne Anwendungen müssen ihre Anforderungen definieren
  - MPG Intra-Net
  - MPG-Portal (Max-Net)

eduPersonEntitlement

- „freier Bereich“
  hier kann man im Prinzip beliebige Information hinterlegen,
- Namensraum mit Baumstruktur
  - urn:geant:dfn.de:mpg.de
  - urn:geant:dfn.de:mpg.de:aai
  - urn:geant:dfn.de:mpg.de:aai:test:
  - https://registry.dfn.de/delegationen.html
    wird vielleicht noch geändert ...
- Unterbäume für Test, GV, MaxNet ...
- muss natürlich mit allen Teilnehmer, SPs, abgesprochen sein

common-lib-terms

- gehört zu eduPersonEntitlement
  - wichtigstes Attribut für Grundversorgung
- „Nutzer ist berechtigt, die von seiner Einrichtung im Rahmen einer Standardlizenz lizenzierten Inhalte zu nutzen“(bei Hochschulen: Mitglied der Hochschule oder Walk-in Patron).
- Definition ist für uns sehr problematisch!
- verweist letztendlich auf die **zugrundeliegenden Verträge**
- **Shibboleth regelt nur die Zugriffstechnik, nicht die Vertragslage!!!**
  - wir dürfen die Attribute unseren Nutzern zuweisen
  - aber nur im Rahmen der bestehenden Verträge
  - jeder Vertrag sieht anders aus
  - siehe Poster Margit Palzenberger

Schema für MPG-AAI

- **eduPerson**
- ohne Erweiterungen
- alles Private kommt in den Entitlement Namensraum,
  zB: Direktor, Verwaltungsleiter ...

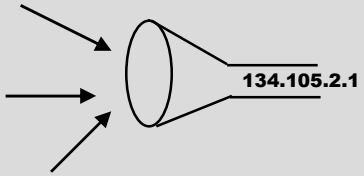
- Warum?
  - straight forward
  - einige Mitspieler neigen zu unproduktiver Kreativität
  - „Standard“ für alle externen SPs
  - kleinster gemeinsamer Nenner

Was bekommt man dafür?

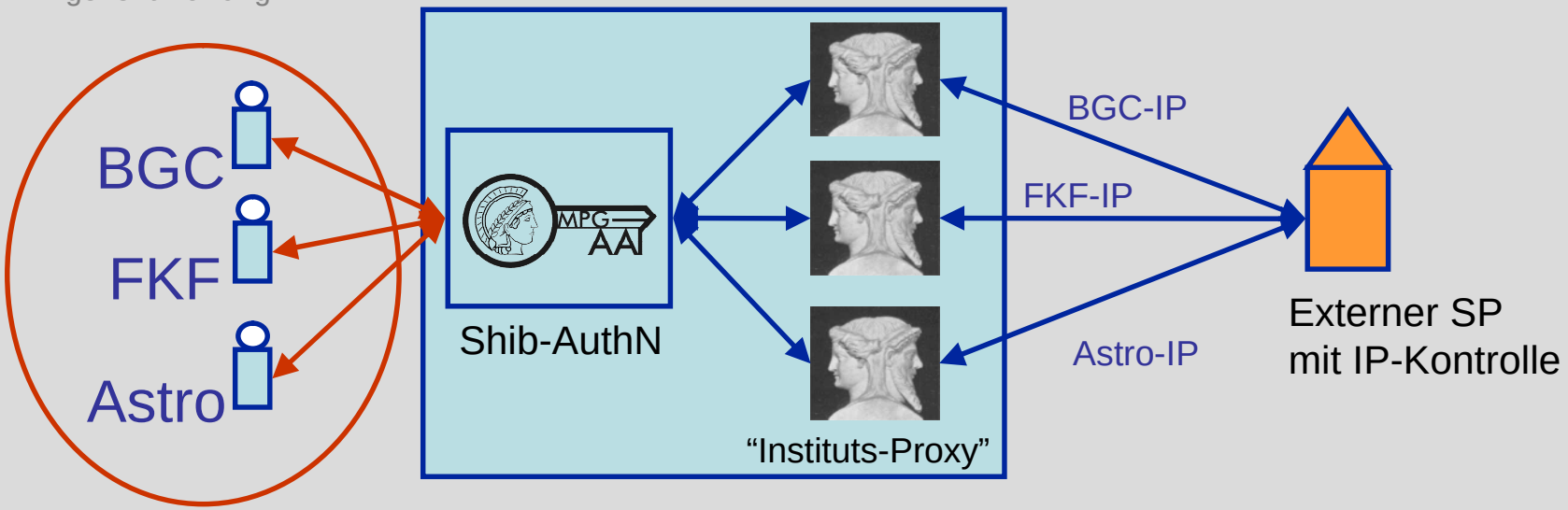
- neue Anwendungen
  - Edu-Roaming / MPG-Roaming
    Login in jedes WLAN-Netz in Deutschland, EU
  - GridShib
    Zugang zu Grid-Computing Resourcen,
    erstes MPG-Projekt: Klima-Modelle
  - Bio-Informatik Portal, Midenas
- MPG-Web-Proxy (travelling scientist problem)
  - legacy problem
  - IP-Authorisierung wird es weiter geben
  - Übergang Shib-IP-Autorisierung

MPG-Web-Proxy

- Web-Proxy ist Stellvertreter
  - setzt alles auf einen Ausgang (IP-Adresse) um
- Standardlösung zerstört das Accounting auf Institutsebene!
  - nicht akzeptabel für uns
  - nicht akzeptabel für viele SPs



- Eigenentwicklung



Non MPG-IP

Prototyp: T. Soddemann, RZG

Was muß man dafür bezahlen?

- Benutzerverwaltung (Identity-Management)
  - bis jetzt oft historisch gewachsen, ohne klare Struktur
  - Gemenge aus verschiedensten Personenkreisen
- Institute müssen **klare Regeln** einführen
  - **wie** das ist und beleibt Institutssache
  - abstrakte Vorgaben aus der Föderation
    „wann muss ein Account nach Ausscheiden deaktiviert werden?“
- Trennung in
  - Benutzer mit offiziellen Status, nach aussen durch den IdP vertreten
  - Interne Benutzer, nicht in der Föderation

Zusammenfassung

- Übergang von „Netzwerk-ID“ auf „Personen-ID“
  - geht nicht von MPG aus
- Shibboleth hilft hier bei der technischen Umsetzung
- neue Dienste sind einfacher zu realisieren
- Legacy-Dienste werden mit eingebunden (Web-Proxy)
- Problem ist **nicht** die Technik
- Problem liegt auf der **sozialen** Ebene
  - die Institute müssen aufräumen
  - die Anbieter müssen dem neuen System **vertrauen**