



Shibboleth

- Infrastruktur für das Grid -

Siegfried Makedanz, Hans Pfeiffenberger

Rechenzentrum

Alfred-Wegener-Institut



■ Helmholtz-Zentrum für Polar- und Meeresforschung



- ... to be able to **integrate, federate, and analyze** information from many **disparate and distributed** data sources

(including data **archives** as well as networks of **sensors** ...)

and to **access and control computing resources** and **experimental equipment** at remote sites

- Cyberinfrastructure for e-Science
Tony Hey and Anne E. Trefethen
Science, Vol 308, Issue 5723, 817-821 ,
6 May 2005

- ~1995 DFN-RPC – blieb im Laborstadium
- **Collaborative Climate Community Data and Processing Grid**
 - Erdsystem-Modelle, Modell-Vergleiche, Szenarien-Rechnungen, Daten-Assimilation
- **Teil der Earth Science Community**
 - **global, multidisziplinär**
- **IPY: International Polar Year 2007/8**
 - Schnappschuss des Planeten Erde
 - ~ 10.000 Wissenschaftler, ~ **250 Institute**, ~ 100 Schiffe, Flugzeuge, Satelliten, Stationen
 - Datenbereitstellung nahe Real-Time

- Internet2/MACE (Middleware Architecture Committee for Education) Projekt (seit ~2000)
- Primäres Ziel: „to support **inter-institutional sharing of web resources subject to access controls**“
- Schutz der Privatsphäre
 - anonymer (Elsevier), pseudonymer Zugriff
- Nutzt SAML
 - Aktuell Version 1.1
 - Ab Q3 2006: SAML Version 2.0
- Standard-Schema: eduPerson

- Shibboleth-Nutzer organisieren sich in Föderationen, meist auf nationaler Ebene
 - USA: InCommon, Schweiz: SWITCHaai, etc.
 - Kick-Off German Federation, Berlin 14. März 06
- Policy ist die Vertrauensbasis der
 - Dienstnutzer und -anbieter
 - Mitglieder und Partner
- Föderation
 - Betreibt WAYF (Where Are You From)
 - Ist der Vertragspartner der Mitglieder u. Partner

- Internet2/MACE Spezifikation
- LDAP Objektklasse mit Standard-Attributen
 - Uid, cn, displayName, location, mail, etc.
- Und spezifischen Erweiterungen, Beispiel:

eduPersonPrincipalName: hans.pfeiffenberger@awi.de

eduPersonAffiliation: member

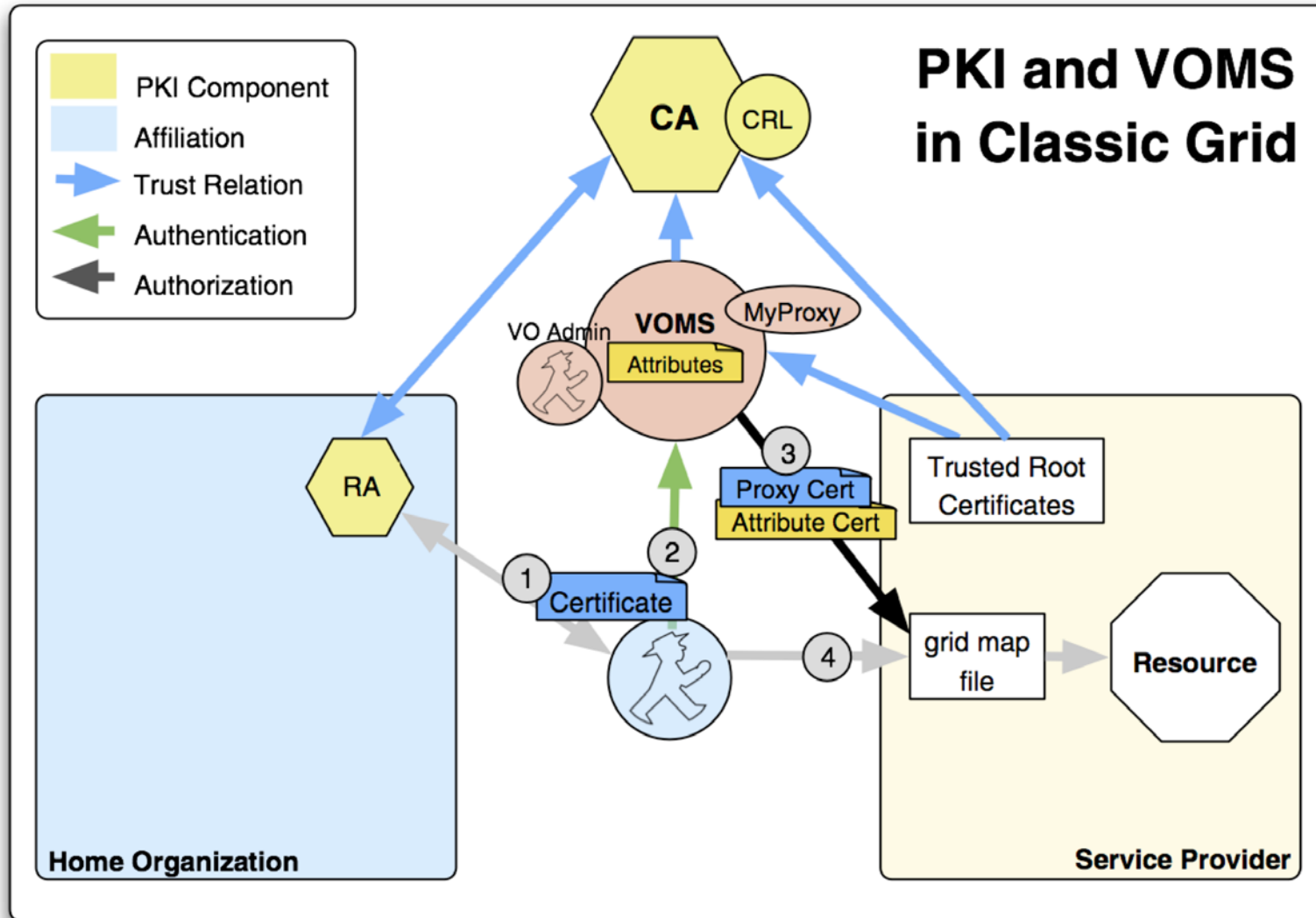
eduPersonScopedAffiliation: member@awi.de

eduPersonScopedAffiliation: member@c3-grid.de

eduPersonTargetedId: x128@awi.de (Pseudonym für Tracking)

eduPersonEntitlement: urn:mace:awi.de:Archive:Curator

- Basiert auf PKI
- Authentisierung
 - X.509 Zertifikate
- Autorisierung
 - VOMS mit Attribut-Zertifikaten
- Problem: Skalierbarkeit
 - Grid mit Zehntausenden Nutzern!

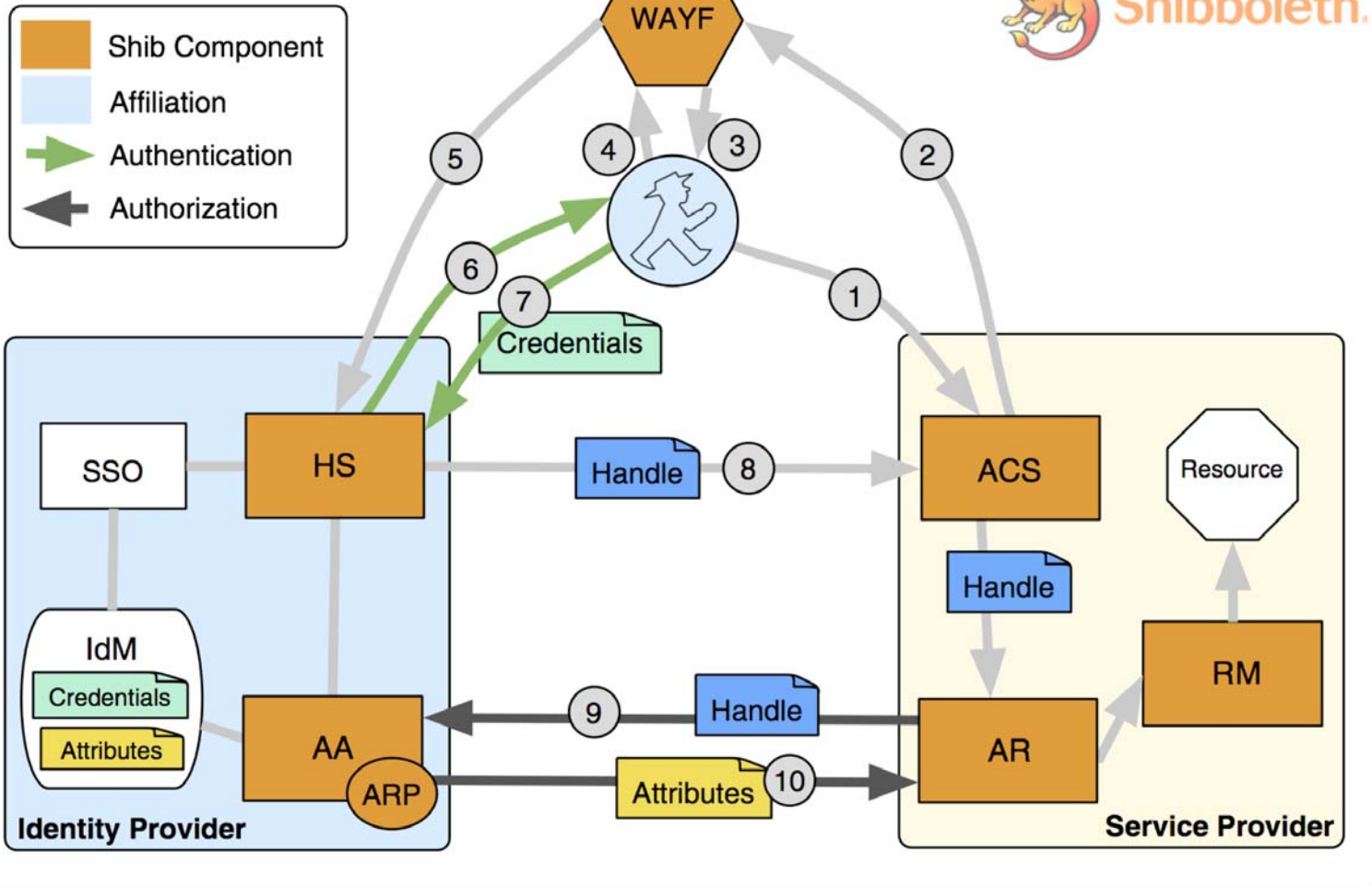


© AWI 2006

- Identity Provider (IdP)
 - Basiert auf Identity Management (IdM) der Heimateinrichtung (home organization)
 - IdM: LDAP oder SQL oder flat files
 - gleiche organisat. Plattform wie RA ?
- IdP Komponenten
 - Handle Service (HS)
 - Attribute Authority (AA)
 - Attribute Release Policy (ARP)

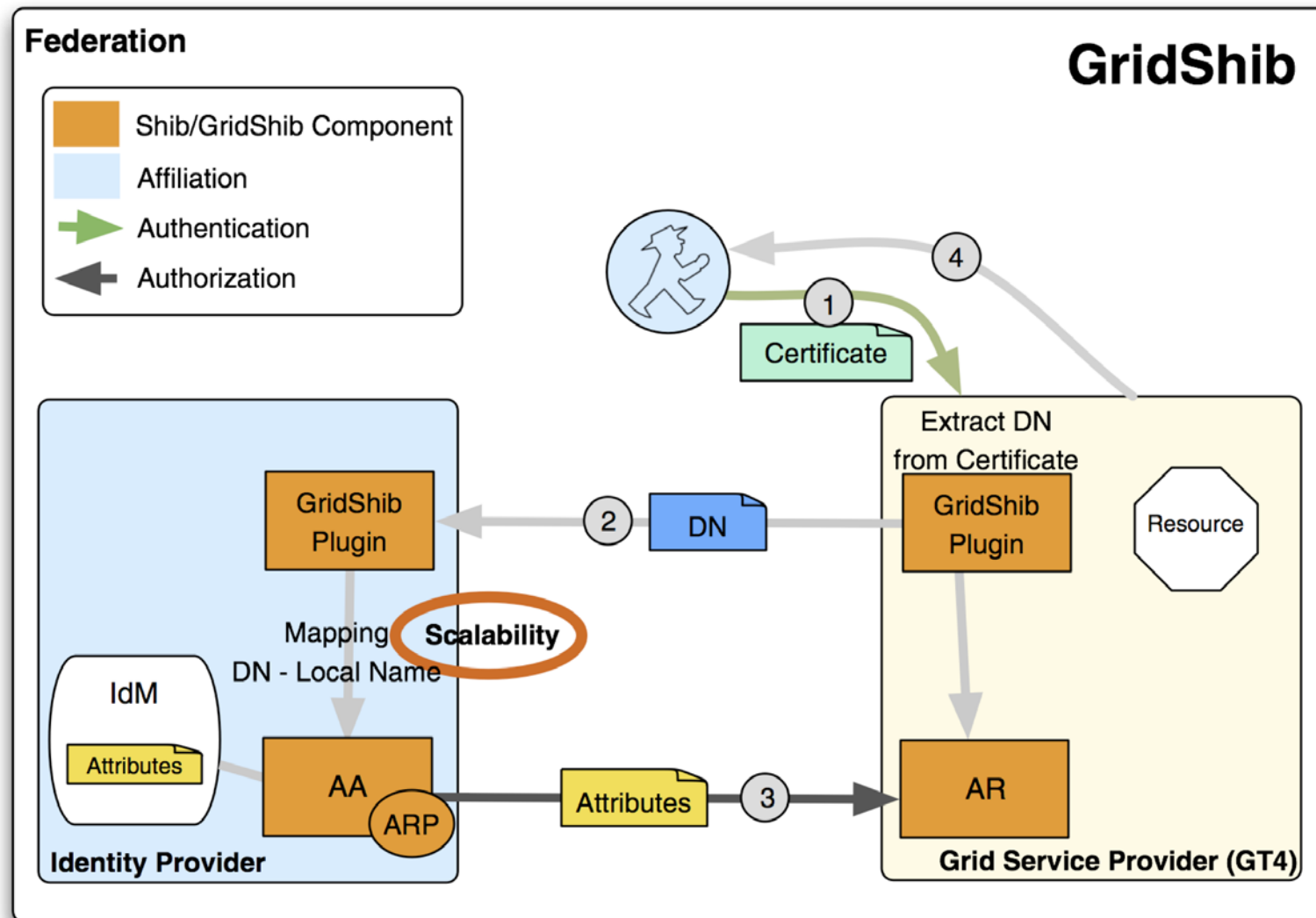
- Service Provider (SP)
 - Einem Dienst, einer Ressource vorgeschaltet
- SP Komponenten
 - Assertion Consumer Service (ACS)
 - Attribute Requestor (AR)
- SAML Assertions
 - Autorisierungszusicherung
 - Vom IdP an den SP

Federation



© AWI 2006

- Projekt des NCSA, U of Chicago, ANL
- 1. Projekt zur Integration von Shibboleth und Grid
- Ziel: Grid-**Autorisierung** durch Abbildung von VO in Shibboleth
- Erweiterung GT 4, Beta-Status
- **Authentisierung** „grid-klassisch“
 - X.509 Zertifikat



© AWI 2006

- Integration Grid und Shibboleth
 - Autorisierung **und** Autorisierung
- Shib-Enable Ansatz:
 - Grid-Zugang per Shibboleth
 - Beispiel: Portal mit Online CA erzeugt Proxy-Zertifikate für Grid-Job
- Projekte
 - GridShib 2, ShibGrid, MAMS, EGEE-2 ...
 - Siehe GGF16: Shib BoF

- Shibboleth: <http://shibboleth.internet2.edu/>
- eduPerson: <http://www.educause.edu/eduperson/>
- GridShib: <http://gridshib.globus.org/>
- GGF16 Shib BoF:
<http://grid.ncsa.uiuc.edu/papers/GGF16-Shib-BOF-Report.pdf>
- DGI FG3-4 Bericht: Analyse von AA-Infrastrukturen in Grid-Middleware

- Fragen?