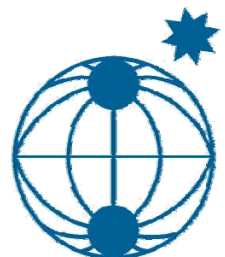


*Ein Plädoyer, eine der Schlüsselfragen von  
eScience wahrzunehmen:*

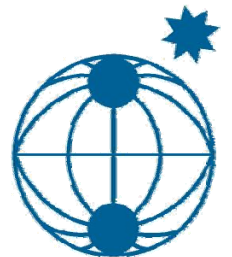
*Authentisierung und rollenbasierte  
Autorisierung*

*H. Pfeiffenberger  
Alfred Wegener Institut, Bremerhaven*



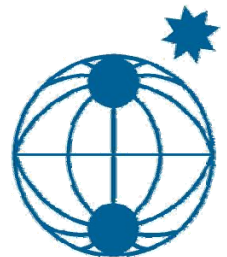
# Agenda

- *„Historische“ Motivation und Blickwinkel*
- *Kontext Science (wie ich ihn verstehe)*
- *(Anwendungs-) Beispiele*
- *Was bedeuten also Identität,..., Rollen in diesem Umfeld*
- *Lösungen, über die gesprochen wird*
- *Was ist also das Problem?*
- *Zusammenfassung*



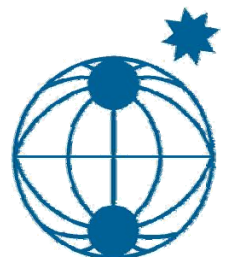
# *„Historische“ Motivation und Blickwinkel*

- *Das Internet seit dem Web – ein Massenmedium*
- *Das (Un-)Sicherheits „Vorbild“ SMTP*
  - **werden wir den selben Fehler noch einmal bei eScience machen ?**
  
- *Meine persönlichen Blickwinkel*
  - **Anwender (aus dem Bereich Earth Sciences)**
  - **Betreiber von Informations- und Kollaborationsdiensten**
  - **Entwickler einschlägiger Anwendungen und Dienste**
  - **NICHT: Entwickler von Sicherheitslösungen**
- *Diese werde ich nach Gusto mischen*



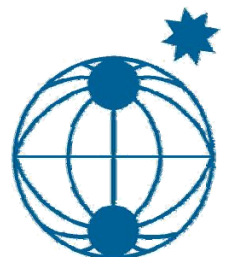
# *Kontext eScience (wie ich ihn verstehe)*

- *High Performance Computing – Accounting! ☑*
- *Open Access - Veröffentlichungswesen*
  - **Budapest – „Instituts-Server“ für Publikationen**
  - **Berliner Erklärung - auch Daten, Software!**
- *DFG „Empfehlungen zur Sicherung guter wissenschaftlicher Praxis“ (1998) – Wissenschaft als Prozess*
- *(Zwei verschiedene Phasen des wissenschaftlichen Prozesses!!)*
- *Cyberinfrastruktur – Blue Ribbon „1/3 .. to support data repositories and digital libraries“*
- *Kollaborations-Systeme (als Provisioning-Problem)*
  - **E-Mail-Listen, Content-Management, ... , Workspaces**



# Beispiel 1 : Innerorganisatorisch

- *Redundante Daten in Forschung, Lehre und Administration*
  - Facility Management (wer darf – warum - Räume reservieren?)
  - Learning Management Systeme (wer ist Lehrender, Lernender ?) vs. Vorlesungsverzeichnis
  - Häufung von Workshops (auch hier: NRW, ZKI, DFN-AT)
    - *Warum trage ich hier Eulen nach Athen ??*
- *Personenbezogene Daten !!*
  - Hohe Ansprüche an Systeme und Organisation
  - => Glaubwürdige Quelle für (globale) eScience-AA-Systeme!
  - so z.B. Authz für DFN-Roaming



# *Beispiel 2 : Vertrauende Domänen*

## ■ *Helmholtz-Gemeinschaft*

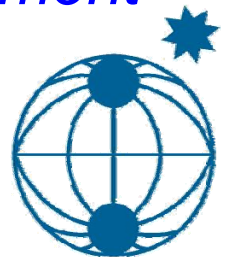
- 15 rechtlich, organisatorisch und technisch unabhängige Institutionen
- Sehr verschiedene Sicherheitsansprüche
- (nur!) 6 Fachbereiche (Überlappen mehrere Institutionen)
- Programmorientierte Förderung –  
Leitmotiv „Kooperation über Grenzen von Institutionen und Disziplinen hinweg“

## ■ *Einfaches Beispiel Küstenforschung*

- Beteiligte : AWI und GKSS
- Jeder arbeitet aber auch noch mit anderen zusammen

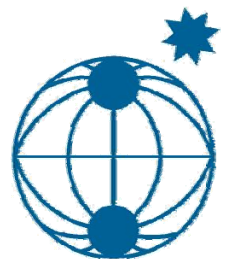
## ■ *Gemeinsames Reporting - gleiche Semantiken von Verzeichnissen, Organisationsbezeichnungen, etc.*

## ■ *E-Mail-Verteiler, Speicherbereiche, ... Web-Content-Management*



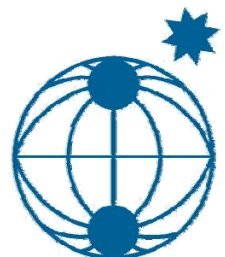
# *Beispiel 3 : Globale Kooperation I*

- *Internationale und interdisziplinäre Kooperation*
  - Solitäre Instrumente (CERN, DESY)
  - International vergleichende Studien (Soziologie)
  - Erde als Objekt („Geobiochemie“)
- *DataGrids für die Erdsystemforschung*
  - Historische Datensätze (Zeitreihen, Ozonsonden)
  - Teure Datensätze (Seeseismik, Southern Ocean Atlas)
  - Modellvergleiche
- *Authentisierung, Autorisierung und Rollen für*
  - Qualitätskontrolle (Reviewprozess, -workflow)
  - Zugriffsbeschränkung (zeitlich und für Gruppen)



# Beispiel 3 : Globale Kooperation II

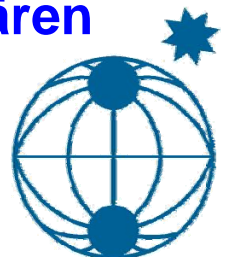
- „Historisches“ Beispiel NDSC Data Protocol –
  - gestaffelte Veröffentlichungspflicht nach ein bis 3 Jahren !
- Warum nicht ein ganz offener Zugang?
  - Skript-Kiddies können Infrastruktur blockieren
  - „offener“ Zugang erst nach Validierung
  - „offener“ Zugang erst nach eigener Nutzung
- (Inter-)nationale Projekte
  - DOE Earth System Grid
  - NERC Data Grid
  - C3-Grid (D, Proposal)
- Befragung Community C4: Klima- und Erdsystemforschung
  - Kein verteiltes Rechnen – aber transparenter, performanter,... Zugang zu Daten
  - Organisation in Virtual Organisations – hier verstanden als Organisationsmittel von Projekten !!





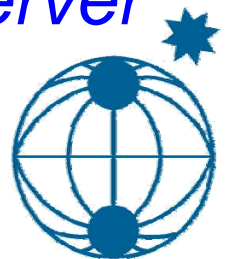
# Was bedeuten also Identität,..., Rollen

- *Der Kontext der Publikation bewirkt die Notwendigkeit einer PERMANENTEN elektronischen Identität*
  - **eduPerson EPPN ? Verbunden mit Zertifikat ?**
  - **pfeiff@awi... , Hans.Pfeiffenberger@dfn.de ??**
- *Rechte werden aus Zugehörigkeiten zu Gruppen abgeleitet*
  - **Mitglied des AWI-Rechenzentrums**
  - **Mitglied des AK2 der D-Grid Initiative**
- *und aus Rollen (innerhalb von Gruppen)*
  - **Stellv. Leiter AWI-RZ**
- *Rollen berechtigen dazu, Funktionen innerhalb des Kontextes auszuüben*
  - **Mitgliedschaft berechtigt zur Nutzung des Gruppen-E-Mail-Verteilers**
  - **Bsp.: Leitungsfunktion berechtigt, andere zu Mitgliedern zu erklären**



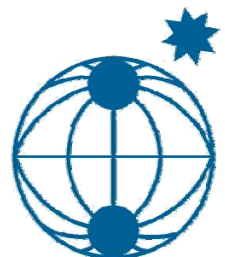
# *Lösungen, über die gesprochen wird*

- *Zertifikate für Globus (Grid)*
  - Proxy-Zertifikate? Unicore: nein! => Jobketten?
  - Usermapping ( Unix-Account ↔ Zertifikat ) nötig
- *Virtuelle Organisationen*
  - LDAP-Server mit Liste der Mitglieder-Zertifikate
  - Wie werden die Vertrauensstellungen der Verzeichnisse gemanaged?
- *Shibboleth, A-Select, ...*
  - Lösungen für Web-basierte Dienste
  - Shib übergibt nach Auth ggf. nur Attribut, nicht Identität
  - Club Shib
- *DFN-Roaming: RADIUS, Verzeichnis der Radius-Server*



# Was ist also das Problem?

- Technische Lösungen (Protokolle, Formate) sind da oder werden es bald sein (X.509, SAML,...)
- Semantiken – schon weniger;
  - eduPerson, eduOrg ?
  - US-zentrisch? („staff“, „faculty“)
- Organisation von Vertrauensstellungen
  - Installation von Authorities in Browsern / E-Mail-Clients
  - Chains, Circles of Trust – begrenzte Reichweite
    - Club Shib,
    - DFN-Roaming
    - Bridge CAs
  - Policies – wer sichert was vertrauenswürdig zu ?
    - Ist ein Student der Uni X tatsächlich noch ein solcher oder eine Karteileiche ?
    - Ist ein Accountinhaber am AWI auch ein Mitglied ? ( A: nein, es kann auch ein Dienstleister sein)
- => Standardisierung von Begrifflichkeiten und darauf aufbauenden Policies; Root-Autoritäten, also eher **Organisationsfragen !!**



# Zusammenfassung

- *D-Grid / e-Science Initiative* , „Start“ Juni 2004
  - **„neue Formen der Wissenschaftskollaboration etablieren“**
  - **Erfordert schnellstes Angehen der Probleme**
- AA ist vornehmlich ein organisatorisches Problem !
  - **Herangehen orientieren an erfolgreichen Analoga (DARE)**
- Selbst eine einfache, erste Lösung bedarf einiger Zeit
  - **Konzentration auf wenige Minimallösungen (Bsp.: eduPerson)**
  - **Diese müssen lokal um Spezifisches ergänzt werden**
- Von Anfang an internationale Ausrichtung !!
  - **„Politik“ hat deutsche Be- und Empfindlichkeiten sowie Kirchturmperspektiven zu beseitigen !!**

