



Identity Management Einführung in die Diskussion

*Hans Pfeiffenberger
Alfred Wegener Institut, Bremerhaven*



1
*Hans Pfeiffenberger, Alfred Wegener Institut
Identity Management Workshop Universität Bremen 2005-06-13*



Agenda

- *Begriffe (Damit wir alle über dasselbe sprechen)*
- *Motivation, strategische Ziele*
 - **Integrierte Informationssysteme (Effizienz des Betriebs)**
 - **eScience / Grids: Zukünftige Forschungs-Infrastruktur**
– (für eLearning haben Sie hier andere Experten)
 - **(Security nur am Rande => besonderes Thema)**
- *(Institutions-interne) “Geschäftsprozesse”*
 - **Wie wirken sich “Policies” / Regeln aus?**
- *Vorgehensweise(n)*
 - **Best Practise**
 - **F&E-Felder**
- *Zusammenfassung & Ratschlag*



2
*Hans Pfeiffenberger, Alfred Wegener Institut
Identity Management Workshop Universität Bremen 2005-06-13*



Begriffe

Wer darf was (wann und warum)?

Wer hat was wann getan ?

- **AAA (IAAA, Identifikation+AAA)**
 - **Authentisierung, Autorisierung, Accounting / Auditing**
 - **≈ technischer Teil von Identity + Access Management**
- **Verzeichnisdienste und mehr**
 - **LDAP, ADS (Identifier, IT-orientierte Inhalte und Struktur)**
 - **+ Attribute aus vielfältigen Quellen (HIS, SAP)**
- **(De-) Provisioning (Bereitstellung): Dienste, pro Person**
- **(„Geschäfts-“) Prozesse und Regeln,**
 - **BPR : Business Process Reengineering**



3

Hans Pfeiffenberger, Alfred Wegener Institut
Identity Management Workshop Universität Bremen 2005-06-13



Caveat !

- **Bei Identity Management geht es auch um Technik**
 - **LDAP, ADS, Systemintegration,.....**
 - **... in leicht zu unterschätzendem Umfang**
- **Aber weit mehr geht es um Organisation !**
 - **Alle-Mann-Manöver (bei internen Systemen, s. folgende Folie)**
 - **Internationale Gremien, Vertrauensverhältnisse (bei externen Systemen)**
- **Sie werden um Änderung von Regeln und Verfahren nicht herum kommen !!!!**
 - **Weil Sie Ihre Regeln de facto (in aller Konsequenz) gar nicht kennen (oder zumindest nicht aufgeschrieben haben)**
 - **Weil de facto stets Ausnahmen „ad personam“ gemacht werden**
 - **Siehe McRae, gegen Ende!!**
 - **aber IT-Systeme stets alles „wörtlich nehmen“ (Prozesse ≈ Workflows)**

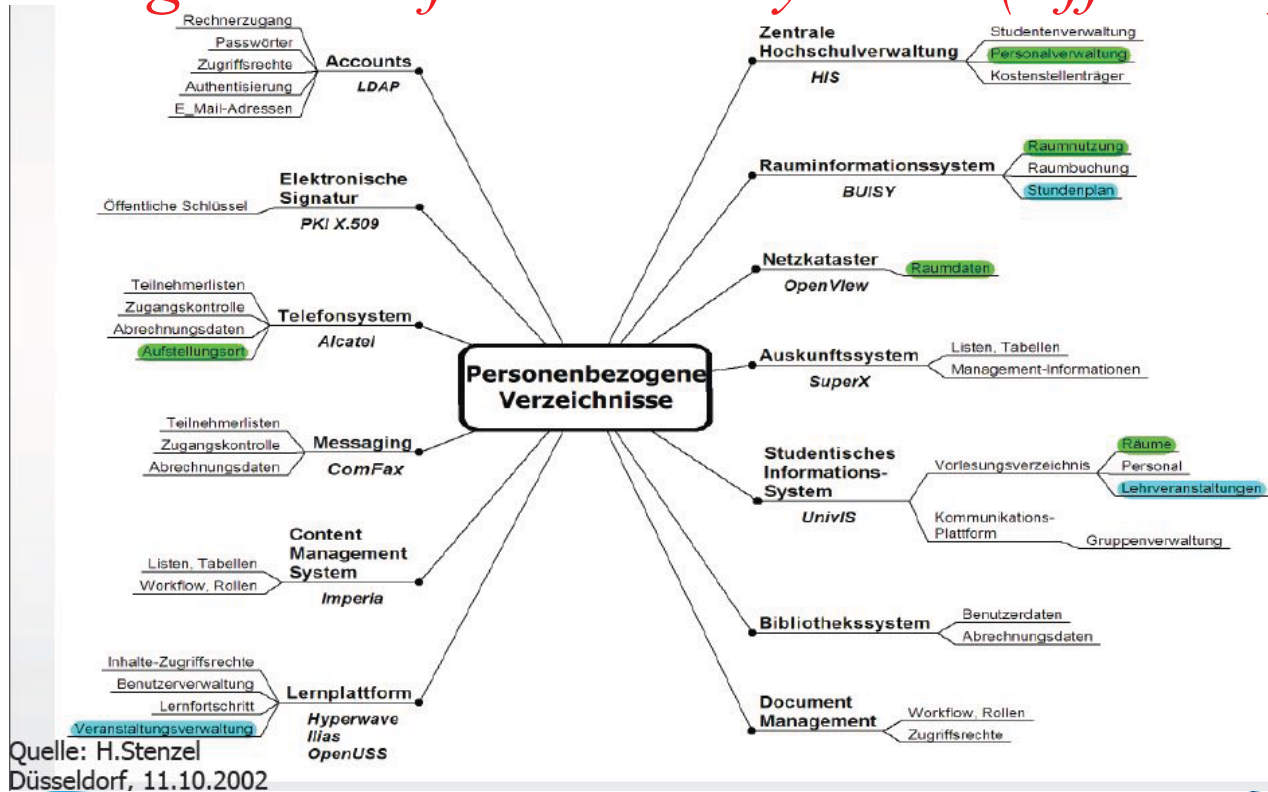


4

Hans Pfeiffenberger, Alfred Wegener Institut
Identity Management Workshop Universität Bremen 2005-06-13



Integrierte Informationssysteme (Effizienz)



5

Hans Pfeiffenberger, Alfred Wegener Institut
Identity Management Workshop Universität Bremen 2005-06-13



Geschäftsprozesse und Regeln (triviales Bsp.)

- Ein Mitglied der Universität darf (muss) einen E-Mail Zugang der Universität nutzen (ZfN-Server, ...???)
 - .u.U. notwendiger Teil von Workflows (Prozessablauf) !!
- Mitgliedschaft wird entweder von Personalstelle oder Immatrikulationsamt bestätigt
- => ab wann kann die Person mit E-Mail arbeiten?
- Soll ein(e) frisch berufener Wissenschaftler(in) den Mail-Account schon vor Arbeitsaufnahme nutzen ??
- Ausnahmen: Kooperationspartner ??

6

Hans Pfeiffenberger, Alfred Wegener Institut
Identity Management Workshop Universität Bremen 2005-06-13



Deutsche Beispiele (ZKI AK Verzeichnis)

Hochschule	Projektstatus	Eigenentwicklung/Produkt
RWTH Aachen	Fertig gestellt, Ergänzungen geplant	IBM TIM, mit eigenen Java-Webanbindungen
Uni Bielefeld	Entwurf, Feinkonzept in Arbeit	vermutlich TIM
Ruhr-Uni Bochum	Fertig gestellt	Eigenentwicklung, Oracle
FH Braunschweig-Wolfenbüttel	Fertig gestellt	Eigenentwicklung mit SunOne Directory
Uni Braunschweig, RRZN Hannover, TU Clausthal, Uni Oldenburg	Feinkonzept erstellt, Pilotierungsphase	SUN
TU Chemnitz	Fertig gestellt	Eigenentwicklung
Uni Duisburg/Essen	Feinkonzept vorhanden, Umsetzung in Arbeit	TIM
FAU Erlangen-Nürnberg	Fertig gestellt, Erweiterungen geplant	GDS Server 2001 von BT Syntegra
Fern Uni Hagen	Fertig gestellt	Enterprise security station 3.2 (ESS), BMC Software GmbH, Control-SA
TU Ilmenau, Uni Jena, Uni Weimar	Erste Teile in Betrieb	Nsure Identity Manager (Novell)
Fachhochschule Köln	Entwurf, Feinkonzept geplant	openLDAP, ITIM geplant
Uni Mainz	Testphase	Microsoft Identity Integration Server
LRZ München	Testphase	Novel eDirectory + NIM2 + Eigenentwicklung
TU München	Entwurf	Voraussichtlich Novell-basiert
Uni Paderborn	Fertig gestellt	openLDAP, Umstellung auf ITIM geplant
Uni Rostock	teilweise fertig gestellt	Siemens „DirX“

Stenzel
Mai 05



7

Hans Pfeiffenberger, Alfred Wegener Institut
Identity Management Workshop Universität Bremen 2005-06-13



eScience / Grid

- *Grosse globale Kollaborationen – an denen auch Mitglieder der Universität Bremen mitwirken (könnten)*
 - CERN (10.000 Personen global),
 - ITER (verschränkt mit bestehenden, EFDA)
 - IPY 2007-08 (hunderte Institute, Dutzende Schiffe....)
- *Tausende von EU-Projekten*
 - Uni HB ist sicher an Hunderten beteiligt ;-))
- *Alle benötigen informationstechnisch realisierte, gemeinsame Ressourcen (LHC-Grid, C3-Grid, Wikis)*
- *Virtuelle Organisationen*
=> *föderiertes Identitätsmanagement*
 - eduRoam, Shibboleth (nicht oder kaum: PKI, Zertifikate)



8

Hans Pfeiffenberger, Alfred Wegener Institut
Identity Management Workshop Universität Bremen 2005-06-13



Forschungsgebiet IdM (Middleware)

■ Begriffsbildung

- Single Sign On (SSO) (≈ Ein Name, ein Passwort)
- Verzeichnisdienst, Meta-Directory => Identity Management
- Rollen und Rechte (RBAC) (Internet2 „Grouper“)
- Entitlements (Internet2 „Signet“)

■ Protokolle und Formate

- Kerberos => Shibboleth (Internet2, NMI)
- Radius: SSO simpel, eduRoam WLAN-Zugang (Terena)
- SAML Security Assertion Markup Language (Shib, Industrie)

■ Organisatorisches

- Föderationen
- Begrenzte Zusammenarbeit, Vertrauen, Verträge



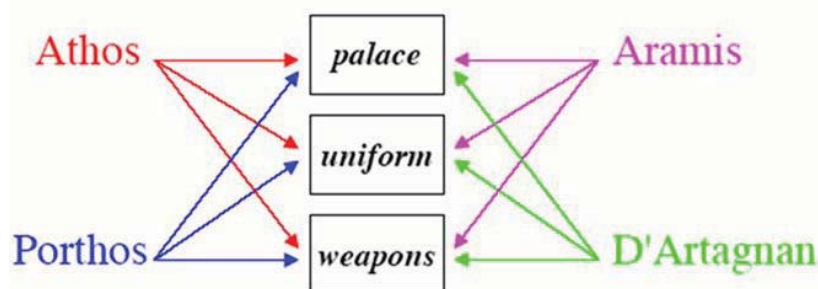
9

Hans Pfeiffenberger, Alfred Wegener Institut
Identity Management Workshop Universität Bremen 2005-06-13

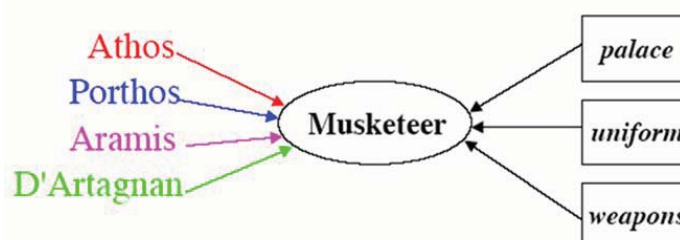


Wieso Forschung ? - RBAC: Musketeers

Example: The Three Musketeers (User/Permission Association)



Example: The Three Musketeers (RBAC)



Hans Pfeiffenberger, Alfred Wegener Institut
Identity Management Workshop Universität Bremen 2005-06-13



Signet, Entitlements, L. McRae, Stanford

Assignment example

By authority of <i>the Dean</i>	grantor
as soon as you are <i>principal investigator</i>	role (group) ←
and have completed <i>training</i>	prerequisite
you can <i>approve purchases</i>	function
in the <i>School of Medicine</i>	scope
for your <i>research project</i> up to \$100,000	limits
until <i>January 1, 2006</i>	condition

6/12/2005

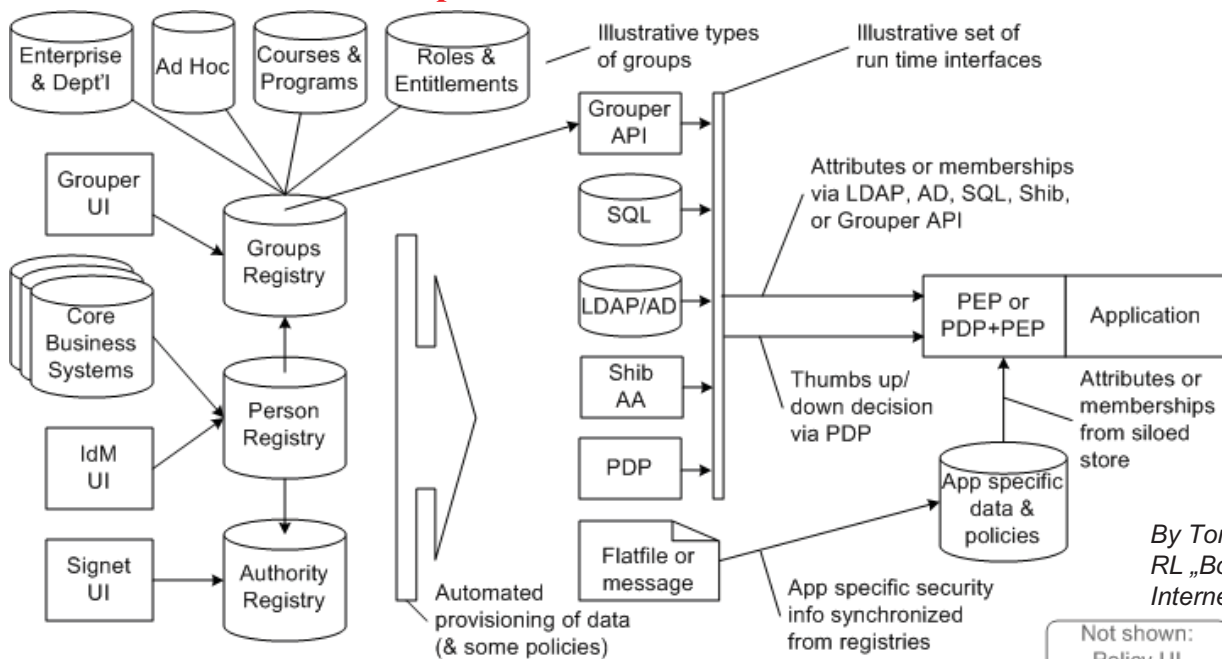
33

11

Hans Pfeiffenberger, Alfred Wegener Institut
Identity Management Workshop Universität Bremen 2005-06-13

Middleware Architecture Committee for Education

<http://middleware.internet2.edu/MACE/>



By Tom Barton,
RL „Bob“ Morgan,
Internet2 MACE

Options for provisioning run time authorization

12

Hans Pfeiffenberger, Alfred Wegener Institut
Identity Management Workshop Universität Bremen 2005-06-13

Zusammenfassung

- Identity Management ist technisch und vor allem organisatorisch **extrem aufwendig**
- Technisch gesehen ist IdM nur ein Mittel zum Zweck: **Integrierte Informationssysteme**
- Es gibt 2-3 mögliche Rechtfertigungen für den Aufwand
 - (Bessere "Accountability" i.S. von : Wer konnte / hat was getan. => Abschreckung / Verhinderung von Missbrauch)
 - Bessere Nutzung der Ressourcen der Universität
 - Globale Integration in die entstehenden eScience / Grid Netze
- Umsetzung (heute) ist nur sinnvoll, wenn man sich
 - intensiv mit Best Practises (global) auseinandersetzt und beraten lässt
 - zur Zukunftssicherheit auch auf IdM als F&E-Thema einlässt



Ratschlag

- Sie brauchen ein gemischtes Team
 - Rektor, Verwaltung, IT und F&L (als „Betroffene“ + Nutzniesser)
- Sie brauchen einen Masterplan
 - Was soll wann (zu welchem Zweck) erreicht werden
- Das Team studiert Best Practise
- Sie lernen nichts, ohne etwas zu tun
 - Wenn Sie ab sofort etwas „tun“ (implementieren):
Seien Sie bereit, es in einem / zwei Jahren komplett wegzuwerfen => Spielwiese
- Sie brauchen **RESSOURCEN** – und zwar Personal !!
- **IdM ist Chefsache, sonst ist sie nicht durchzusetzen !**

