Autorisierungsattribute in einer Shibboleth-Föderation

Peter Gietz, DAASI International GmbH

peter.gietz@daasi.de

DFN-Shibboleth-Workshop,

Berlin, 28. Februar 2007

DAASI International

Directory Applications for Advanced Security and Information Management

Agenda

- Einführung in (Federated) Identity Management
- Attribute: Standardisiertes LDAP-Schema
- Datenschutz
- DFN-AAI

DAASI International
Directory Applications for Advanced Security and Information Management

Einführung in Federated Identity Management

DAASI International

Directory Applications
for Advanced Security
and Information Management

Ausgangsposition vor Identity Management

- Historisch gewachsene Infrastrukturen und Prozesse
- Isolierte, voneinander unabhängige Verzeichnisse und Datenbanken mit den gleichen Identitätsdaten
  - keine Interaktion
  - kein Vertrauen bezüglich der Richtigkeit der Daten
- Jede dieser Datensammlungen hat
  - eigene Administratoren
  - Benutzerverwaltungen
  - Zugriffskontrollmechanismen
- Redundanz der Daten und der Datenpflege
  - => Mehrfacharbeit

DAASI International
Directory Applications for Advanced Security and Information Management

Probleme

- Identitätsinformationen sind in verschiedenen Datensammlungen unterschiedlich
  - unterschiedliche Daten: Meyer vs. Meier
  - unterschiedliche Datenschemata: Nachn vs. Nachname
- Jede neue Anwendung vergrößert den Leidensdruck (= neue Redundanz durch neue Benutzerverwaltung)
- Wo liegen die aktuellen Infos über eine Person?
  - Ist Musterfrau noch Studentin?
  - Ist sie berechtigt auf bestimmte Ressourcen zuzugreifen?
- Woher kommen autoritative Antworten?

DAASI International
Directory Applications for Advanced Security and Information Management

Noch mehr Probleme

- Prozesse sind langsam
- Benutzer bekommen zu spät Zugriff auf Ressourcen
- Helpdesk wird überlastet durch das „Passwort-Vergessen-Syndrom“
- Nach Weggang des Mitarbeiters werden nicht alle Accounts und Berechtigungen gelöscht
- Sicherheit ist oft nicht gegeben
- DFN-AAI-”Readiness” ist nicht gegeben

DAASI International
Directory Applications for Advanced Security and Information Management

IdM ist die Lösung

- Definition von Spencer C. Lee:
  - *Identity Management bezieht sich auf den Prozess der Implementierung neuer Technologien zum Verwalten von Informationen über die Identität von Nutzern und zur Kontrolle des Zugriffs auf Firmenressourcen.*
  - *Das Ziel von Identity Management ist es Produktivität und Sicherheit zu erhöhen und gleichzeitig Kosten der Verwaltung von Benutzern, ihrer Identitäten, Attribute und Berechtigungsnachweise zu senken*

DAASI International
Directory Applications for Advanced Security and Information Management

Was ist neu an IdM?

- Benutzerverwaltungen gibt es seit den Anfängen der EDV
  - etc/passwd in Unix ist auch Benutzerverwaltung!
- Identity Management Systeme sorgen dafür dass
  - man ein Gesamtkonzept der IT-Landschaft entwickelt
  - Daten aus autoritativen Datenquellen kommen und nicht überall neu eingetippt werden müssen
  - Die Benutzerverwaltung automatisiert wird
- Automatisierte Prozesse bewirken, dass
  - Berechtigungen gleich nach der Einstellung zur Verfügung stehen
  - aber auch gleich nach dem Austritt aus der Organisation entzogen werden

DAASI International
Directory Applications for Advanced Security and Information Management

Was gehört zu IdM?

- Quelldatenbanken und Zielsysteme
  - authoritative Datenquellen und Anwendungen
- Verzeichnisdienste sind zentrale Bestandteile
  - speichern Identitätsinformation, Passwörtern, Zertifikate, Rollen und Berechtigungen, Policy
  - Standards: X.500, LDAP
  - Implementierungen: OpenLDAP, Novell eDirectory, MS Active Directory
- Metadirectories dienen zur
  - Synchronisierung verschiedener Datenspeicher
  - Vermeidung von Inkonsistenzen
  - Passwort-Verwaltung und –Synchronisierung
- Konnektoren verbinden
  - Datenquellen mit Metadirectory
  - Metadirectory mit Zielsystemen (Provisioning)

DAASI International
Directory Applications for Advanced Security and Information Management

Was wird durch IdM ermöglicht?

- Eindeutige Identifizierung eines Benutzers
  - Die Studentin, die gleichzeitig eine Anstellung hat, wird als eine Person geführt
  - Dies ermöglcht auch Personalisierung
- Unified Login / Single Log On
  - Integrative zentrale Benutzerverwaltung die Anwednungen direkt bedient (LDAP)
  - Nicht integrierte Anwednungen können mit Accountdaten provisioniert werden
  - Benutzer müssen sich nur noch ein Passwort merken
- Single Sign On
  - BenutzerInnen müssen sich nur einmal (am Tag) authentifizieren und haben danach Zugang zu allen Anwendungen
  - Wichtig ist auch Single Log Off

DAASI International
Directory Applications for Advanced Security and Information Management

Was ist Federated Identity Management?

- FIdM ist Identity Management, welches über die Grenzen einer Organisation hinweg Identitätsinformationen zur Verfügung stellt und im Rahmen von Föderationen zum Zwecke der Authentifizierung und Autorisierung nutzt.
- Hierbei werden die lokalen IdM-Systeme bzw. Authentifizierungsdienste genutzt, sodass nicht jeder Benutzer in jeder Organisation einen Account benötigt
- Voraussetzung ist ein Vertrauensbund zwischen den Organisationen, der über Verträge hergestellt wird
- Es kommen hierbei moderne Standards zum Einsatz, insbesondere SAML (Security Assertion Markup Language)
- Technologien sind z.B.: Liberty Alliance, Shibboleth, WS-Security

DAASI International
Directory Applications for Advanced Security and Information Management

Motivation für Federated Identity Management

- Studenten werden immer mobiler, wechseln die Hochschule öfters
- Studiengänge der verschiedenen Hochschulen müssen kompatibel sein (s.a. e-Learning)
- 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

DAASI International
Directory Applications for Advanced Security and Information Management

Föderativer Ansatz

- Lokale Organisationen verwalten und authentifizieren ihre Benutzer
- Ressourcenanbieter kontrollieren den Zugang zu den Ressourcen
- Autorisierung und Zugriffskontrolle wird über Attribute geregelt, die in den lokalen Organisationen gepflegt werden
- Ressourcenanbieter erfragt (bzw. bekommt automatisch geliefert) die Attribute eines Benutzers, der eine Ressource in Anspruch nehmen möchte
- Hierbei können personenbezogene Attribute zum Zwecke des Datenschutzes unterdrückt werden
- Aufgrund der Attribute entscheidet der Ressourcenanbieter über Zugriff

DAASI International
Directory Applications for Advanced Security and Information Management

Standards für FIdM 1

- LDAP (Lightweight Directory Access Protocol)
  - IETF-Standard zum Speichern und Übertragen von Benutzerdaten, sowie für Authentifizierungsprozesse
- SAML (Security Assertion Markup Language) (OASIS)
  - XML-Dokumente enthalten Zusicherungen (Assertions) die ein IdP über Benutzer macht:
    - Authentication Statements, Zusicherung, dass sich ein Benutzer Authentifiziert hat
    - Authorization Statement, Zusicherung über bestimmte Zugriffsrechte
    - Attribute Statement, Zusicherung über bestimmte Eigenschaften eines Benutzers, die in Form von Attributen weitergegeben werden und dem SP bei der Entscheidung über Zugriff unterstützen
  - Profile spezifizieren welche Assertions wie zwischen IdP und SP ausgetauscht werden

DAASI International
Directory Applications for Advanced Security and Information Management

Standards für FidM 2

- XACML (eXtensible Access Control Markup Language) (OASIS)
  - XML-Dokumente enthalten Botschaften über Autorisierungsentscheidungen und Zugriffskontrollregeln (policy)
- SPML (Service Provisioning Markup Language(OASIS)
  - XML-Dokumente enthalten Benutzerinformationen, die an Anwendungen (auch über Organisationsgrenzen hinweg) provisioiert werden.
- SOAP (Simple Object Access Protocol)
  - XML-Protokoll zum Verschicken von Botschaften (meist XML-Dokumente) zwischen Prozessen auf verschiedenen Rechnern (wie RPC)

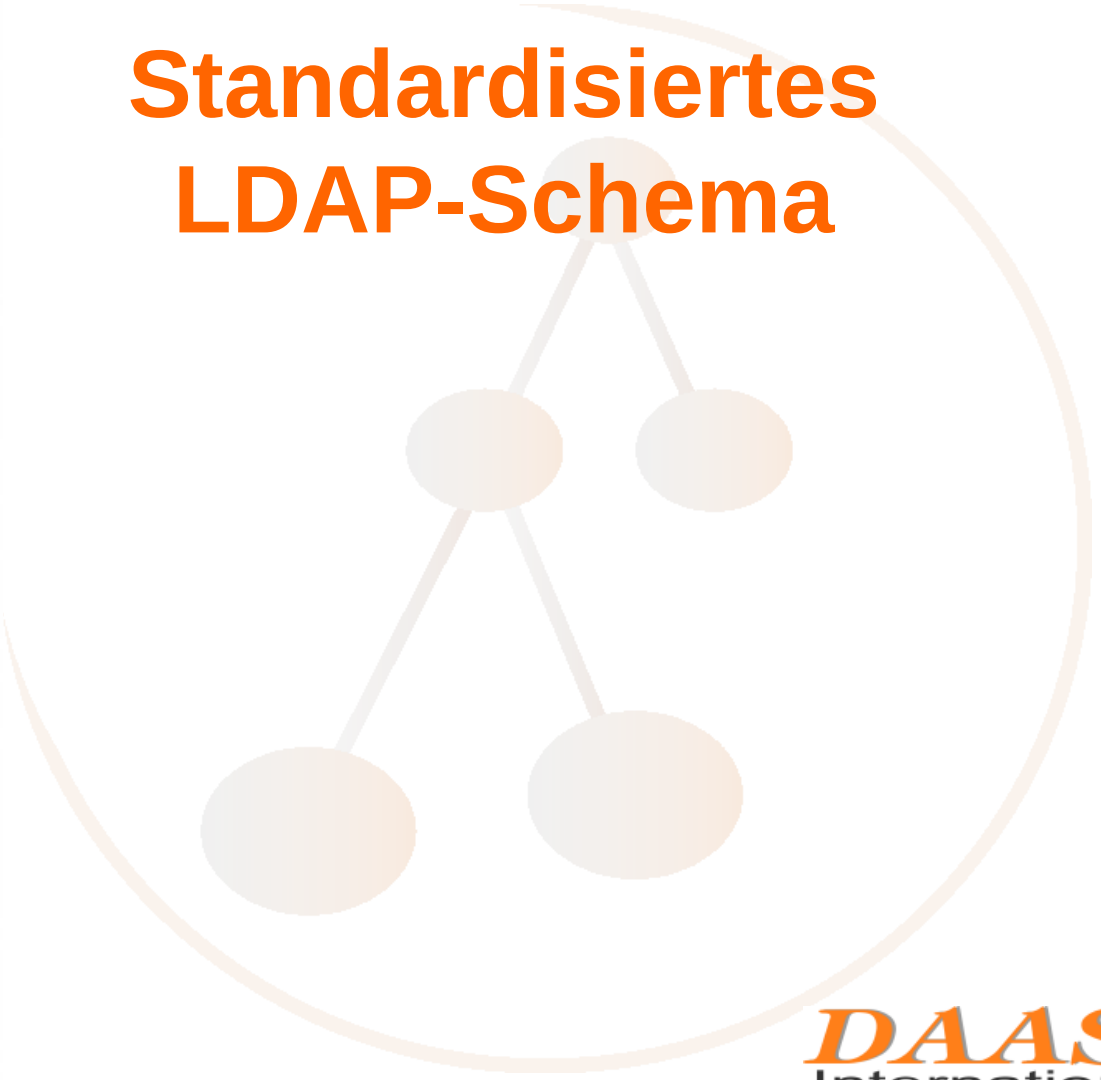
DAASI International
Directory Applications for Advanced Security and Information Management

Shibboleth und Grid Computing

- Shibboleth ist auch im Bereich Grid Computing ins Zentrum des Interesses gerückt
  - GridShib ist eine Implementierung von Shibboleth für die Web Services basierte Open Source Grid-Infrastruktur Globus Toolkit
- Virtuelle Organisationen, wie z.B. internationale Forschungsprojekte, die sich Grid-Ressourcen (CPUs, Storage, Services) teilen, benötigen ein föderiertes Identity Management
- In BMBF-geförderten Grid-Forschungsprojekten wird u.a. an Shibboleth-Integration
  - TextGrid (Community Grid für Textwissenschaftler)
  - IVOM (VO-Management, XACML mit Permis)

DAASI International
Directory Applications for Advanced Security and Information Management

Standardisiertes LDAP-Schema



DAASI International

Directory Applications
for Advanced Security
and Information Management

Personenschema im X.500 Standard

- X.500 wurde in der Version 1 1988 als weltweiter Verzeichnisdienst spezifiziert
- Erste Anwendung war internationales Telefonbuch (White Pages und Yellow Pages)
- Deshalb wurde im Standard selbst bereits Schema u.a. zur Abbildung von Personen spezifiziert
- Diese Standard-Schemaspezifikationen wurden in LDAP übernommen (RFC 4519, ehem. 2256)

DAASI International
Directory Applications for Advanced Security and Information Management

Die Objektklasse person

- Die Objektklasse *person* wurde bereits im X.500(88) Standard spezifiziert.
- Für den LDAP-Standard wird sie in [RFC 4519, ehem. 2256] spezifiziert.
- Sie beschreibt eine beliebige Person.
  - Surname, commonName sind MUST-Attribute
- Weitere personenbezogene Objektklassen werden von *person* abgeleitet (s.u.).

DAASI International
Directory Applications for Advanced Security and Information Management

Die Objektklasse organizationalPerson

- Die Objektklasse *organizationalPerson* wird ebenfalls in X.500(88) und in [RFC 4519, ehem. 2256] spezifiziert.
- Sie beschreibt eine in einer Organisation arbeitende Person und wird von *person* abgeleitet.
- Sie enthält nur MAY-Attribute.

DAASI International
Directory Applications for Advanced Security and Information Management

Probleme mit organizationalPerson

- Attributtyp title ist nur für Firmenfunktion gedacht
  - „title, such as "Vice President", of a person in their organizational context“
- personalTitle ist zwar in RFC 1274 spezifiziert aber nicht ins LDAP-Schema übernommen
- Zur vollständigen Abbildung der postalischen Adresse in Einzelattributen fehlt Attributtyp countryName / c
- Internettypische Attribute fehlen ganz

DAASI International
Directory Applications for Advanced Security and Information Management

Objektklasse inetOrgPerson

- Die Objektklasse *inetOrgPerson* wird in [RFC 2798] spezifiziert.
- Sie beschreibt weitere MAY-Attribute, die v.a. für im Internet aktive in Organisationen arbeitende Personen relevant sind.
- Mittlerweile hat sich *inetOrgPerson* als Standard etabliert, der in den allermeisten Anwendungen implementiert wurde.
- *inetOrgPerson* wird von *organizationalPerson* abgeleitet.

- Problem: Es fehlen Spezialattribute für Forschungs-Personen

DAASI International
Directory Applications for Advanced Security and Information Management

Objektklasse eduPerson

- Von Internet2 MACE Dir entwickelt
- Als Ergänzung zu inetOrgPerson gedacht
- Wird weltweit zu einem defacto-Standard für Hochschulen, der durch nationale Schemata ergänzt wird

```
( 1.3.6.1.4.1.5923.1.1.2 NAME 'eduPerson'
      AUXILIARY
      MAY ( eduPersonAffiliation $ eduPersonNickname $
            eduPersonOrgDN $ eduPersonOrgUnitDN $
            eduPersonPrimaryAffiliation $
            eduPersonPrincipalName $
            eduPersonEntitlement $
            eduPersonPrimaryOrgUnitDN $
            eduPersonScopedAffiliation $
            eduPersonTargetedID )
```

DAASI International
Directory Applications for Advanced Security and Information Management

eduPerson-Attribute 1

- eduPerson(Primary)Affiliation zur Abbildung Grundrollen innerhalb der Hochschule (faculty, student, staff, alumn, member, affiliate)
- eduPersonScopedAffiliation dito mit Zusatz der „security domain“, z.B. student@uni-tuebingen.de
- eduPersonEntitlement zur Abbildung von Rechten:
  - „URI (either URN or URL) that indicates a set of rights to specific resources“
  - z.B.: urn:mace:dir:entitlement:common-lib-terms
    - „standard higher-ed population consisting of regular full-time faculty, staff, and students (of a particular institution), also including anyone physically present in that institution's library regardless of affiliation“
  - Inhalt dieses Attributs muss innerhalb einer Föderation festgelegt werden. Hierzu ist eine URN-Registry hilfreich.

DAASI International
Directory Applications for Advanced Security and Information Management

eduPerson-Attribute 2

- eduPerson(Primary)OrgUnitDN zur Abbildung der Organisationszugehörigkeit bei einem flachen Personenbaum
- eduPersonOrgDN für organisationsübergreifende Verzeichnisse
- eduPersonNickname für einen Spitznamen
- eduPersonPrincipalName ist als Identitäts-Token gedacht:
  - „The "NetID" of the person for the purposes of inter-institutional authentication“
- eduPersonTargetedID eine eindeutige pseudonyme Kennung von der aus nicht auf die reale BenutzerIn geschlossen werden kann. Wird für Personalisierungs-dienste beim SP verwendet, wenn dieser nicht die identifizierbare Kennung eduPersonPrincipleName erhalten soll. Nur der IdP kann dieses Pseudonym auflösen.

DAASI International
Directory Applications for Advanced Security and Information Management

Weitere Schemastandardisierung in Europa

- 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
    - Wurde mit den Arbeiten an HisPerson koordiniert

DAASI International
Directory Applications for Advanced Security and Information Management

(Federated) Identity Management und Datenschutz

DAASI International
Directory Applications for Advanced Security and Information Management

IdM und Datenschutz

- IdM erzwingt oft die Übermittlung von personenbezogenen Daten innerhalb der Organisation
  - HIS => Metadirectory => Anwendung)
  - Dies muss vom Datenschutzbeauftragten und Personalrat genehmigt werden
  - Zu beachten: Datensparsamkeit und Zweckbindung
    - von den Anwendungen her argumentieren
  - => Zuerst ein Gesamtkonzept, um Genehmigungsprozess nur einmal durchzugehen

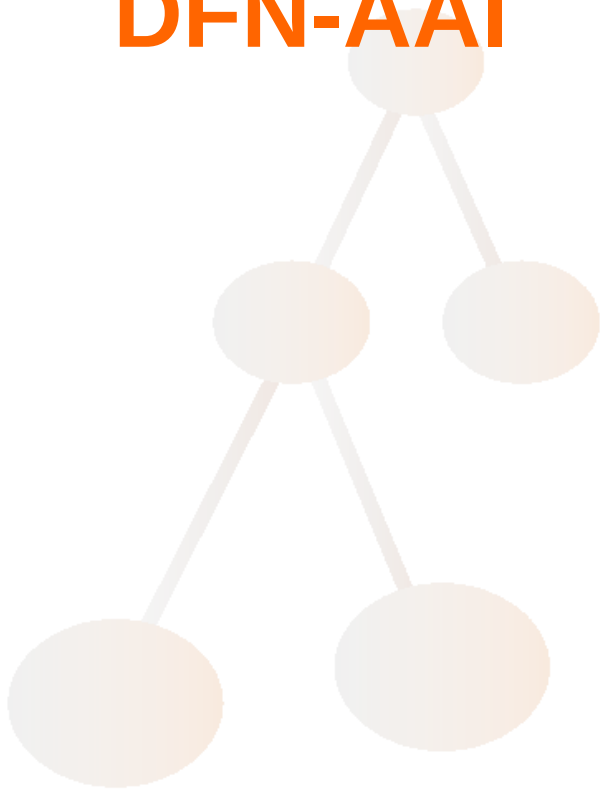
DAASI International
Directory Applications for Advanced Security and Information Management

FIdM und Datenschutz

- Bei FidM geschiet die Übermittlung über Organisationsgrenzen hinweg
- Shibboleth ermöglicht es, die Weitergabe von personenbezogenen Daten zu vermeiden und dennoch den SPs die Möglichkeit der Personalisierung zu bieten:
  - EduPersonTargetedId
- Der IdP bestimmt in seiner Attribute Release Policy (ARP), welche Attribute nach Außen gegeben werden
- Mit der Zusatzsoftware ShARPE (Shibboleth Attribute Request Policy Editor) kann dies komfortabel über einen Webbrowser spezifiziert werden (IdP-weit, benutzerspezifisch, aber auch gruppenspezifisch)
- Mit Autograph kann der Benutzer selbst spezifizieren, welche Attribute an welchen SP übertragen wird

DAASI International
Directory Applications for Advanced Security and Information Management

DFN-AAI



DAASI International

Directory Applications
for Advanced Security
and Information Management

Voraussetzungen IdM

1. Voraussetzung für Teilnahme der Anwender

- Betrieb eines Identity Management Systems
- mindestens Betrieb einer vertrauens-würdigen Nutzerverwaltung mit konsistentem und aktuellem Datenbestand

Die folgenden Folien sind einem Vortrag von Renate Schroeder, DFN-Verein entnommen

Voraussetzungen IdM

- Eine zeitnahe Verwaltung von digitalen Identitäten muss garantiert werden:
  - Person wird in Einrichtung aufgenommen
    - => digitale Identität wird zeitnah erzeugt
  - Person erhält Rolle und Berechtigungen
    - => zeitnahe Zuweisung entsprechender Attribute an digitale Identität
  - Person wechselt Rolle und Berechtigungen
    - => zeitnahe Aktualisierung der Attribute der digitalen Identität
  - Person verlässt die Einrichtung
    - Autorisierungsattribute werden zeitnah gelöscht

Voraussetzungen Attribute

DFN Deutsches Forschungsnetz

2. Voraussetzung für Teilnahme der Anwender:

- Unterstützung eines gemeinsamen Attributschemas
- Attribute sind Grundlage für Autorisierung und Zugriffskontrolle
  - Anwender stellen Attribute der Nutzer bereit
  - Anbieter überprüfen Wert und erlauben oder verweigern Zugriff

DAASI International
Directory Applications for Advanced Security and Information Management

Voraussetzungen Attribute

DFN Deutsches Forschungsnetz

Attributschema der DFN-AAI:

- Unterstützung der Objektklassen
  - *inetOrgPerson* (mit *person* und *organizationalPerson*)
  - *eduPerson*
- Liste von 21 obligatorischen und empfohlenen Attributen
- obligatorisch sind:
  - Surname (sn), aus person — Nachname
  - Mail, aus inetOrgPerson — Mailadresse
  - eduPersonPrincipleName — Name@Domain
  - eduPersonScopedAffiliation — Rolle@Domain
  - eduPersonEntitlement — Wert für Berechtigung
  - eduPersonTargetedID — Pseudonym

DAASI International
Directory Applications for Advanced Security and Information Management

Gesamtliste der in DFN-AAI empfohlenen Attribute 1/2

Nr	Attribut	LDAP-Name des Attributs	aus Objektklasse				Klassifizierung	
			person	org-Person	inetOrgPerson	eduPers	*obligatorisch*	*empfohlen*
1	Name	cn (common name)	x					x
2	Nachname	sn (surname)	x				x	
3	Vorname	GivenName			x			x
4	Angezeigter Name	DisplayName			x			x
5	User ID	Uid			x			x
6	Zertifikat	userCertificate			x			x
7	Postadresse (Dienst)	postalAddress		x				x
8	Telefonnummer (Dienst)	telephoneNumber	x					x
9	E-Mailadresse (Dienst)	Mail			x		x	
10	Organisationsname	organisationName (o)		x				x
11	Organisationseinheit (OU) z.B. Abteilung	organisationalUnitName (ou)		x				x

DAASI International
Directory Applications for Advanced Security and Information Management

Gesamtliste der in DFN-AAI empfohlenen Attribute 2/2

Nr	Attribut	LDAP-Name des Attributs	aus Objektklasse				Klassifizierung	
			person	org-Person	inetOrgPerson	eduPers	*obligatorisch*	*empfohlen*
12	DN der Organisation	eduPersonOrgDN				x		x
13	DN der Organisationseinheit	eduPersonOrgUnitDN				x		x
14	DN der wichtigsten OU	eduPersonPrimaryOrgUnitDN				x		x
15	Name in Form von Netz-ID	eduPersonPrincipalName				x	x	
16	Art d. Zugehörigrigkeit zur eigenen Organisation	eduPersonAffiliation				x		x
17	Hauptsächliche Art der Zugehörigkeit	eduPersonPrimary Affiliation				x		x
18	Art d. Zugehörigkeit plus Domain Namen	eduPersonScopedAffiliation				x	x	
19	Berechtigung	eduPersonEntitlement				x	x	
20	Eindeutiges Pseudonym f. Anbieter	eduPersonTargetedID				x	x	
21	Spitzname	eduPersonNickname						x

DAASI International
Directory Applications for Advanced Security and Information Management

DFN-AAI Zusammenfassung

- Anbieter vertraut darauf, dass nur berechtigte Nutzer Ressourcen nutzen
- Anwender muss das sicherstellen!
- Nur durch Betrieb eines Identity Management Systems (oder einer vertrauenswürdigen Nutzerverwaltung mit aktuellem und konsistentem Datenbestand) und

  Unterstützung eines gemeinsamen Attributschemas möglich

Referenzen

- Peter Valkenburg, Bert Sals, Thomas van Vooren, Federated Identity Management in Higher Education – Scenarios, services and solutions, Version 1.0, 02-10-2006
- P. Gietz, C. Grimm, H. Pfeiffenberger, J. Rauschenbach, R. Schroeder, Auf dem Weg zur DFN-AAI: Identity Management, In DFN Mitteilungen 71, Dezember 2006, www.dfn.de/content/fileadmin/5Presse/DFNMitteilungen/DFN_71.pdf
- P. Gietz, J. Lienhard, S. Makedanz, B. Oberknapp, H. Pfeiffenberger, J. Rauschenbach, A. Ruppert, R. Schroeder: DFN-AAI - Technische und organisatorische Voraussetzungen – Attribute, https://wiki.aai.dfn.de/wiki/images/9/98/DFN-AAI-Attribute-V08.doc

DAASI International
Directory Applications for Advanced Security and Information Management

Vielen Dank für Ihre Aufmerksamkeit

- Für Rückfragen und Anmerkungen:
  - Peter.gietz@daasi.de

- DAASI International GmbH
  - http://www.daasi.de
  - Info@daasi.de

DAASI International
Directory Applications for Advanced Security and Information Management