Attribute in der DFN-AAI

ZKI Arbeitskreis Verzeichnisdienste
3.11.2008

Renate Schroeder, DFN-Verein

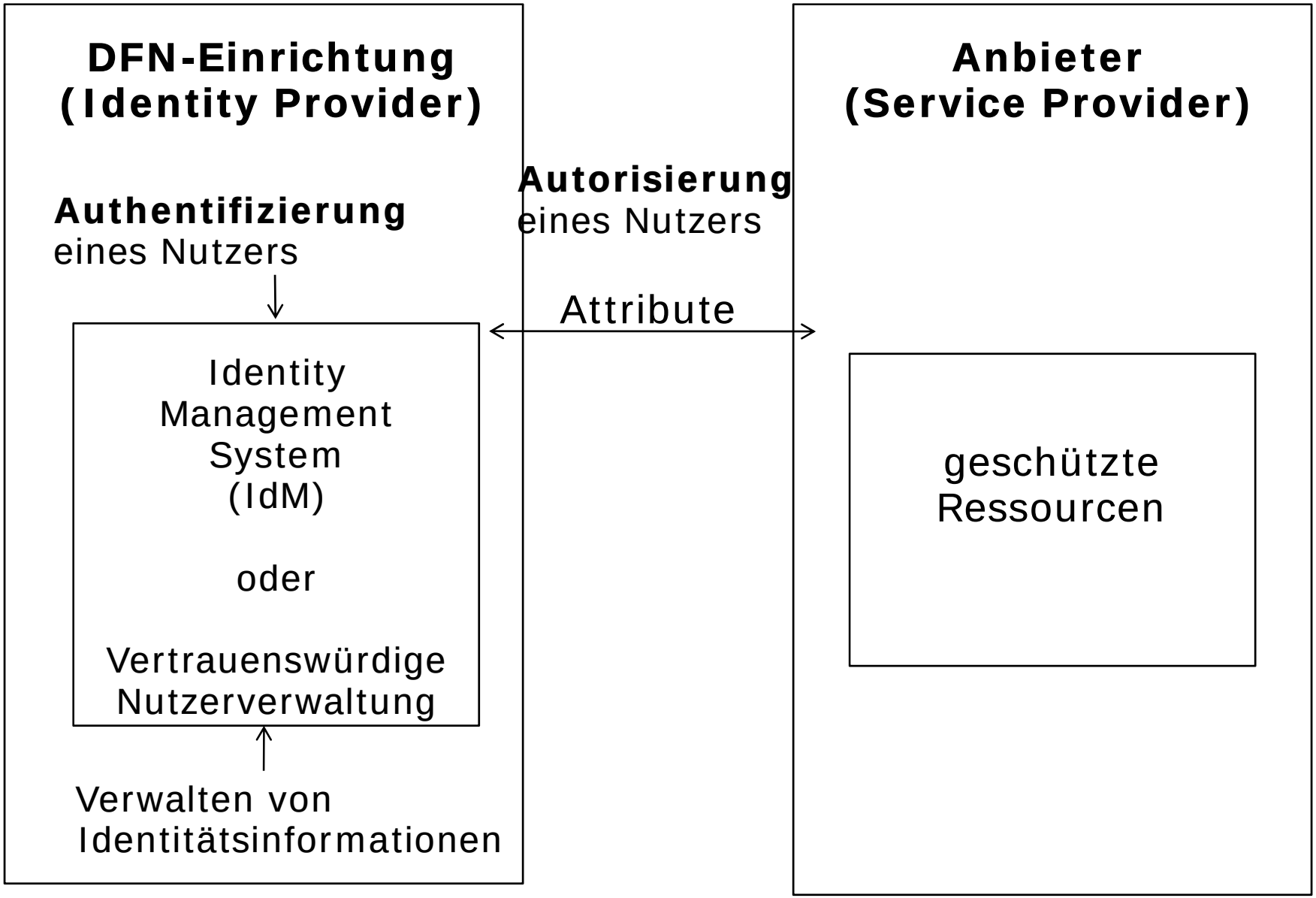
Inhalt

- Allgemeines zur DFN-AAI und zu Attributen
- Attribute für alle Anwendungen (Basis-Attributset)
- Attribute für d. Bereich E-Learning (E-Learning-Profil)
- Verlässlichkeitsstufen: können dabei Attribute eine Rolle spielen?

DFN-AAI

- AAI im DFN
  - Infrastruktur zur Authentifizierung und Autorisierung
  - Vertrauensbeziehung zwischen Anbietern und DFN-Einrichtungen, die die Ressourcen der Anbieter nutzen wollen
- Einsatz von Shibboleth
  - bietet Single Sign On
  - hohe Akzeptanz bei Anbietern von Ressourcen
- Föderativer Ansatz:
  - DFN-Einrichtungen authentifizieren ihre Nutzer
  - Anbieter kontrollieren Zugang zu ihren Ressourcen
  - Autorisierung der Nutzer über Attribute

DFN-AAI


DFN-Einrichtung
(Identity Provider)
Authentifizierung
eines Nutzers
Identity
Management
System
(IdM)
oder
Vertrauenswürdige
Nutzerverwaltung
Verwalten von
Identitätsinformationen
Autorisierung
eines Nutzers
Attribute
Anbieter
(Service Provider)
geschützte
Ressourcen

Papiere für die DFN-AAI

- Mai 2006:

  Empfehlungen zum **Identity Management**
- November 2006:

  Attribut-Empfehlungen für alle Anwendungen (Basis-Attributset)
- Juni 2008:

  Überarbeitung des Basis-Attributsets
- November 2008:

  Attribut-Empfehlungen für den Bereich E-Learning (E-Learning-Profil)

Warum Attribut-Empfehlungen? (I)

- Empfehlung für Attribute gibt den Beteiligten Sicherheit
  - DFN-Einrichtungen können die Attribute rechtzeitig in ihre IdMs (Identity Management Systems) einpflegen
  - Anbieter können Attribute aus den Attribut-Empfehlungen auswählen

- => notwendig für ein gemeinsames Verständnis der Attribute in der DFN-AAI

Warum Attribut-Spezifikation? (II)

- auch Aushandlung der Attribute zwischen einer DFN-Einrichtung und einem Anbieter möglich
- Nutzung dieser bilateral ausgehandelten Attribute in der DFN-AAI möglich
- DFN-Einrichtungen und Anbietern steht es frei
  - Attribute bilateral auszuhandeln oder
  - Attribut-Empfehlungen der DFN-AAI verwenden

Attribute für alle Anwendungen

- Erstes Attribut-Papier für die DFN-AAI
  - Spezifikation von anwendungsübergreifenden Attributen (Basis-Attributset)

Spezifikation eines Basis-Attributsets

- Entwickelt von einer Autorengruppe, vorläufige Fertigstellung November 2006, Überarbeitung Juni 2008
- Beteiligte aus den Einrichtungen AWI Bremenhaven, Universität Freiburg, DAASI International und DFN
- Ziel: Beschreibung von allgemeinen Attributen, die im Rahmen der DFN-AAI verwendet werden
- beschrieben wurden
  - Attribute für Autorisierungszwecke
  - Attribute, die Kontaktdaten enthalten

Attributauswahl

- Attribut-Spezifikation enthält einen Satz von 18 Attributen, die von verschiedenen Anwendungen genutzt werden können (anwendungsübergreifend)

- für die Auswahl der Attribute wurden **Standardobjektklassen** herangezogen **und** die für Autorisierungsattribute wichtige **Objektklasse *eduPerson***
  - fast alle Attribute der Objektklasse *eduPerson*
  - ausgewählte Attribute aus den Standardobjektklassen *inetOrgPerson* (zusammen mit den Unterklassen *organizationalPerson* und *person*)

Einteilung der Attribute

- Einteilung der Attribute in
  - “grundlegend“ (wichtige Attribute, ohne die viele Anwendungen nicht genutzt werden können)
  - “ergänzend” (weitere Attribute, die für einzelne Anwendungen oder bestimmte Funktionalitäten in Anwendungen benötigt werden)

Ausgewählte Attribute (I)

Nr	Attribut	LDAP-Name des Attributs	aus Objektkl.				Klasse	
			1	2	3	4	G	E
1	Name	cn (commonName)	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	Telefonnr. (Dienst)	telephoneNumber	x					x
9	E-Mailadresse (Dienst)	Mail			x		x	
10	Organisationsname	organisationName		x				x
11	Organisationseinheitsname (OU)	organisationalUnitName		x				x

Ausgewählte Attribute (II)

Nr	Attribut	LDAP-Name des Attributs	aus Objektkl.				Klasse	
			1	2	3	4	G	E
12	DN der Organisation	eduPersonOrgDN	x					x
13	DN der Organisationseinheit	eduPersonOrgUnitDN	x					x
14	Name in Form von Netz-ID	eduPersonPrincipleName			x		x	
15	Art der Zugehörigkeit zur eigenen Organis.	eduPersonAffiliation			x			x
16	Art der Zugehörigkeit + Domain Namen	eduPersonScopedAffiliation			x		x	
17	Berechtigung	eduPersonEntitlement			x		x	
18	Eindeutiges Pseudonym	eduPersonTargetedID		x			x	

1 Objektklasse person
2 Objektklasse organisationalPerson
3 Objektklasse inetOrgPerson
4 Objektklasse eduPerson

G = gundlegend
E = ergänzend

Ergänzungen des Basis-Attributsets

- für Bibliotheken ist Basis-Attributset ausreichend, da nur ein Attribut benötigt wird (eduPersonEntitlement)
- für weitere Anwendungen (E-Learning, D-Grid) sind Ergänzungen notwendig

Ergänzung für E-Learning

- Zweites Attribut-Papier für die DFN-AAI
  - Spezifikation von Attributen für den Bereich E-Learning (E-Learning-Profil)

Treffen mit Learning-Experten

- DFN-AAI-Treffen mit E-Learning-Experten der Landesinitiativen
  - Virtuelle Hochschule Bayern (vhb)
  - Bildungsportal Sachsen (BPS)
  - Nds-AAI (Niedersachsen)
- und aus den Bundesländern
  - Thüringen
  - Baden-Württemberg
  - Nordrhein-Westfalen
  - Hessen
  - Berlin

Gründe für E-Learning-Profil

- kompatible Studiengänge an verschiedenen Hochschulen
- hochschulübergreifende Studiengänge
- Landesiniativen wie Bildungsportale oder virtuelle Hochschulen
- Learning Management Systeme werden hochschulübergreifend eingesetzt
- es werden Attribute benötigt, die über den Basis-Attributset hinausgehen
- Vorschläge dazu von E-Learning-Experten

E-Learning-Profil (I)

- Bildung einer Arbeitsgruppe mit Mitarbeitern aus verschiedenen E-Learning-Umgebungen:
  - Jörg Deutschmann, TU Ilmenau
  - Wolfgang Hommel, Leibniz-Rechenzentrum
  - Jens Schwendel, Bildungsportal Sachsen
  - Tobias Thelen, Universität Osnabrück

  - Peter Gietz, DAASI International GmbH
  - Renate Schroeder, DFN-Verein

- Ziel: Spezifikation eines gemeinsamen Satzes von Attributen für verschiedene Learning Management Systeme

E-Learning-Profil (II)

- Spezifikation von insgesamt 16 Attributen
  - vorwiegend Attribute für Autorisierungszwecke
  - einige Attribute zur Unterstützung der Anwendung
- alle Attribute sind optional
- benötigte Attribute nicht in Standardobjektklassen enthalten
  - Ausnahme: Bevorzugte Sprache(preferred Language)
- Verwendung von Attributen definiert vom europäischen Harmonization Committee (SCHAC)
  - Geburtsdatum (schacDateOfBirth)
  - Geschlecht (schacGender)
  - Matrikelnummer (schacPersonalUniqueCode)

E-Learning-Profil (III)

- Für weitere Informationen mussten DFN-Attribute definiert werden
  - Kostenstelle (dfnEduPersonCostCenter)
  - Titel (personalTitle)
  - alle Attribute zum Studiengang

Abbildung von Studiengangsinformationen

- Wie kann eine Abbildung von Studiengangsinformationen aussehen?
- Wahl fiel auf dreistufige numerische Klassifikation des Statistischen Bundesamtes:
  - “Klassifikation von Studienfächern des Statistischen Bundesamtes der Form: Fächergruppen, Studienbereiche und Studienfächer”
- Verwendung von numerischen Schlüsseln
  - z.B. Studienfach=26 (Biologie)

Attribute zum Studiengang

- Fächergruppe (z.B. Mathematik u. Naturwissensch.)
- Studienbereich (z.B. Informatik)
- Studienfach (z.B. Wirtschaftsinformatik)
  - Studienfachbezeichnung laut Hochschule
- Studienabschluss (z.B. Bachelor)
- Studienart (z.B. Zweitstudium)
- Kombinierte Studieninformatonen
  - Fachsemester
  - Fach und Abschluss
  - Fach und Fachart (für Fachart z.B. “HF” für Hauptfach)
  - Kombination aller Attribute zu einem Attribut (außer “Studienfachbezeichnung laut Hochschule”)

Datenschutz (I)

- E-Learning Attribute sind sensible personenbezogene Daten
- DFN-Einrichtung muss Datenschutzbestimmungen einhalten
- DFN-Einrichtung sollte sich mit Datenschutzbeauftragten absprechen
- Einsatz eines Attribut-Freigabeverfahren (z.B. ArpViewer) wird empfohlen
- Haltung und Übertragung der Daten liegt außerhalb des Verantwortungsbereichs des DFN-Vereins

Datenschutz (II)

- In der Attributspezifikation für E-Learning sollen nur technische Aspekte beschrieben werden
- Ausführungen im Kapitel “Datenschutz” werden auf DFN-Webseiten veröffentlicht
- Behandlung des Themas Datenschutz, speziell bezogen auf E-Learning-Attribute, auf Datenschutz-Workshop im Frühjahr

Verlässlichkeit

- Attribute für Verlässlichkeitsstufen?
  - noch in Planung

Attribute für Verlässlichkeitsstufen?

- Bisher
  - Attribute werden nutzerspezifisch verwendet
    - für die Autorisierung von Nutzern
    - zur Übertragung von Nutzerinformationen
- Idee
  - möglichweise Abbildung von Sachverhalten auf Attribute (Verlässlichkeiten)
    - Wie wird Identifizierung der Nutzer vorgenommen?
    - Wie werden Nutzer authentifiziert?
    - Wie ist die Qualität der Datenbasis (IdM oder vertrauenswürdige Nutzerverwaltung oder noch geringer)

Hintergrund

- Forderungen an DFN-Einrichtungen in Dienstvereinbarung für die DFN-AAI
  - Datenbasis mit zeitnaher Aktualisierung (14 Tage)
  - geordnete Prozesse
- Sehr unterschiedliche Qualität der Datenhaltung bei einzelnen DFN-Einrichtungen
  - kein IdM, keine vertrauenswürdige Nutzerverwaltung
  - zum Teil Einträge nicht aktuell
  - zum Teil keine definierten Prozesse
- Aber: es gibt Anbieter, deren Anforderungen gering sind

Definition von Verlässlichkeitsstufen

- Wie kann ereicht werden, dass auch Einrichtungen mit geringeren Voraussetzungen
  - an der DFN-AAI teilnehmen und
  - auf Resourcen bestimmter Anbieters zugreifen können?
- Definition von Verlässlichkeitsstufen für
  - Identifizierung
  - Authentifizierung
  - Qualität des IdM

Stufen Identifizierung

DFN Deutsches Forschungsnetz

Stufe	Art der Identifizierung	Ggf. geeignet für	Bemerkung
undefined	unbekannt	Testaccounts	
basic	Rückantwort auf E-Mail	GRIDs SP, denen die Kenntnis eine E-Mailadresse reicht	Jeder, der über eine E-Mailadresse verfügt, erhält digitale Identität
advanced	Persönliche Identifizierung d. Vertrauens-instanz	Lizenzpflichtige Inhalte	Übliches Verfahren bei DFN-Einrichtungen
high level	Biometrische Verfahren	Sehr hoher Sicherheitsbedarf	ImWissenschafts umfeld noch keine Anwendung absehbar

Stufen Authentifizierung

DFN Deutsches Forschungsnetz

Stufe	Qualität	Bemerkung
undefined	Unbekannt	
basic	User-Id/Passwort Ungeprüft	keine Qualitätskontrolle bei Passwörtern
advanced	User-Id/Passwort Geprüft	mit Qualitätskontrolle bei Passwörtern
high level	Zertifikate? Smart Card?	aus DFN-PKI oder vergleichbar

Stufen Qualität IdM

Stufe	Qualität	Bemerkung
undefined	unbekannt	
basic	Aktualität? Korrektheit? Sicherheit?	noch zu definieren
advanced	Aktualität und Korrektheit des IdM entsprechend AAI-Vertrag	zeitnahe Aktualisierung, definierte Prozesse
high level	mit Audit	geprüft durch unabhängige Instanz

Stufen der Verlässlichkeit

- Aus Stufen der Einzelkriterien (Identifizierung, Authentifizierung, IdM) wird Stufe der Verlässlichkeit bestimmt
- niedrigste Stufe der Einzelkriterien ergibt Stufe der Verlässlichkeit
  - undefined
  - basic
  - advanced
  - high level

Realisierung

- Möglichkeiten
  - Einführung eines Attributs “Verlässlichkeit”
    - nur im internationalen Kontext, daher nicht kurzfristig möglich
  - DFN-Föderation mit mehreren Verlässlichkeitsstufen
    - Technisch leicht umsetzbar (mehrere Metadatensätze)
    - Anpassung der Verträge/Policy

Fragen ...?