DFN
Deutsches Forschungsnetz

DFN-AAI in der Praxis

Ulrich Kähler, DFN-Verein
kaehler@dfn.de

Was ist DFN-AAI?

- DFN-AAI ist ein **regulärer Dienst** des DFN-Vereins. (keine Extrakosten, enthalten in Internet-Dienstentgelten)

- DFN-AAI schafft
  - den **organisatorisch / technischen Rahmen** für den Austausch von Nutzerinformationen,
  - das notwendige **Vertrauensverhältnis** zwischen den Anwendern und den Anbietern

- Der DFN-Verein ist der **zentrale Vertragspartner** für alle Teilnehmer der AAI.

- Der DFN-Verein übernimmt **zentrale betriebliche Aufgaben.**
  - In der DFN-AAI wird das **Shibboleth**-System verwendet.

Anwendungen

DFN Deutsches Forschungsnetz

- **Bibliotheken und Verlage**
- **Verteilung lizenzierter Software**
- **GRIDs**
- **E-Learning**
- **Interne Dienste innerhalb von Hochschulen**
  - Schreibrechte für TYPO3
  - personalisiertes Web-Portal für Studenten

Anwendung Bibliotheken

Bibliotheken und Verlage waren die treibende Kraft für den Aufbau der deutschen Föderation!

- **Status:**
  z.Zt. ca. 30 Verträge unterschrieben:
  Fachportal Bildung/FIS Bildung (DIPF), EBSCO, CSA Illumina (ProQuest), OvidSP, ERL/WebSIRS (Ovid), Munzinger, JSTOR, ScienceDirect (Elsevier), Gale/Cengage Learning, Metapress mit 174 Verlagen, Web of Science (Thomson), Uni Freiburg (REDI), HBZ (Vascoda), Uni Göttingen (Nationallizenzen), ...

- **Wünsche:**
  Beibehaltung des Sicherheitsniveaus wie im IdP-Vertrag und IdM-Empfehlung vereinbart

Anwendung Software-Verteilung

DFN Deutsches Forschungsnetz

Verteilung lizenzierter Software im Wissenschafts-bereich an z.B. Studenten

- **Status:**
  Microsoft (Dreamspark): Autorisierung ohne Attributprüfung, sehr geringes Sicherheitsniveau

  Anfrage der Fa. SUN, etc.

  im Aufbau:
  JOBZIPPERS Ltd.: Studentenportal (Stellenvermittlung) aus der Schweiz

- **Wünsche:**
  - niedrigeres Sicherheitsniveaus wäre ausreichend
  - Ausdehnung auf möglichst viele Teilnehmer

Wünsche GRIDs

DFN-AAI ist Bestandteil der DGRID-Infrastruktur.

- **Status:**
  DFN-AAI wird genutzt von:
  C3-Community, Text-Grid, INGRID, Medi-Grid

  DFN-Verein betreibt einen Server für kurzlebige Zertifikate (SLCS).

- **Wünsche:**
  E-Mail-basierende Identifikation

Anwendung E-Learning

DFN Deutsches Forschungsnetz

E-Learning ist im Kommen!

- **Status:**
  Aktivitäten in mehreren Bundesländern:
  Bayern, Sachsen (BPS), Niedersachsen,
  Thüringen, Baden-Württemberg, (ZKI)

  Definition von E-Learning-Attributen abgeschlossen

Anwendung E-Learning

- **Bildung einer Arbeitsgruppe mit Mitarbeitern aus verschiedenen E-Learning-Umgebungen:**
  - Jörg Deutschmann, TU Ilmenau
  - Peter Gietz, DAASI International GmbH
  - Wolfgang Hommel, Leibniz-Rechenzentrum
  - Renate Schroeder, DFN-Verein
  - Jens Schwendel, BPS Bildungsportal Sachsen
  - Tobias Thelen, Universität Osnabrück

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

Attributauswahl für E-Learning

- **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 Commitee (SCHAC)**
  - Geburtsdatum (schacDateOfBirth)
  - Geschlecht (schacGender)
  - Matrikelnummer (schacPersonalUniqueCode)

Attribute zum Studiengang

- **DFN-Attribute für**
  - Fächergruppe (z.B. Ingenieurwissenschaften)
  - Studienbereich
  - Studienfach
  - Studienfachbezeichnung laut Hochschule
  - Studienabschluss (z.B. Bachelor)
  - Studienart (z.B. Zweitstudium)
  - Fachsemester (z.B. 5)
  - Kombinierte Studieninformatonen
    - Fach und Abschluss
    - Fach und Fachart (für Fachart z.B. “HF” für Hauptfach)
    - Kombination aller Attribute außer Fachsemester

Wünsche E-Learning

DFN Deutsches Forschungsnetz

E-Learning ist im Kommen!

- **Status:**
  Aktivitäten in mehreren Bundesländern:
  Bayern, Sachsen (BPS), Niedersachsen,
  Thüringen, Baden-Württemberg, (ZKI)

  Definition von E-Learning-Attributen abgeschlossen

- **Wünsche:**
  Erhöhung des Sicherheitsniveaus bei Authentifizierung von Professoren

Mitwirkung Hochschulen (IdM)

- **Geregelt im Teilnehmervertrag**
  - **Der Teilnehmer betreibt ein System zur Nutzerverwaltung und stellt sicher, dass seinen Nutzern Attribute zugeordnet werden und Änderungen zeitnah (innerhalb von zwei Wochen) in der Nutzerverwaltung gepflegt werden.**
- **Betrieb eines eigenen IdM (mind. LDAP)**
- **Teilnahme am Dienst DFN-PKI**

IdM Wünsche

Bei den IdMs ist noch viel Spielraum nach oben!

- **Status:**
  Sehr unterschiedliche Qualität des Identity Managements an den einzelnen Hochschulen!
  Mängel:
  langsame Änderungsprozeduren, „falsche“ Einträge, fehlende Prozesse/Konzepte, mangelnde Unterstützung durch Hochschulleitung, etc. .....
- **Wünsche:**
  Teilnahme an DFN-AAI auch von weniger verlässlichen IdPs

Status Betrieb

DFN Deutsches Forschungsnetz

	Produktion	Test
SPs	31	69
IdPs	36	97
Summe	67	166

Wünsche Übersicht

DFN Deutsches Forschungsnetz

Anwendung	Wünsche
Bibliotheken	Sicherheitsniveau beibehalten
Software-Verteilung	Niedrigeres Sicherheitsniveau
GRIDs	Niedrigeres Sicherheitsniveau
E-Learning	Höheres Sicherheitsniveau
IdMs	Niedrigeres Sicherheitsniveau

Klassen der Verlässlichkeit

DFN Deutsches Forschungsnetz

Die Verlässlichkeit bei der Authentifizierung wird durch die folgenden drei Kriterien bestimmt:

- **I: das Verfahren, mit dem die nutzende Einrichtung die Identität ihrer Angehörigen feststellt,**
- **A: das Verfahren, mit dem sich eine Identität gegenüber einem Anbieter ausweist und**
- **D: die Datenhaltung und die Prozesse, mit denen die nutzende Einrichtung die Identität ihrer Angehörigen pflegt.**

Identifizierung

Verfahren zur Identifizierung durch die nutzende Einrichtung (I)
Die nutzende Einrichtung muss natürlichen Personen elektronische Identitäten zuordnen. Hierzu sind im Rahmen der DFN-AAI mehrere Verfahren möglich.

Klasse	Mindestanforderung	Bemerkung
Test	Verfahren freigestellt	In dieser Klasse ist es der nutzenden Einrichtung freigestellt, wie sie die Identität ihrer Angehörigen feststellt. Diese Klasse ist typischerweise für Testzwecke geeignet.
Basic	Identifizierung anhand der Rückantwort von einer eindeutigen Adresse (z.B. eMail-Adresse, Telefonanschluss, Postanschrift)	Dieses Verfahren erlaubt eine einfache und schnelle Identifizierung, die ggf. für einige Ressourcen ausreichend ist. Bei dieser Identifizierung bleibt lediglich ungeprüft, ob sich hinter einer eindeutigen Adresse tatsächlich die vermutete Identität verbirgt. (Oder ob sich z.B. jemand anders eines Briefes an eine Postadresse bemächtigt hat.)
Advanced	Identifizierung durch das persönliche Vorsprechen gegenüber einer Vertrauensinstanz mit einem amtlichen Dokument zur Identitätsfeststellung.	Mit diesem Verfahren kann eine Identität zweifelsfrei sichergestellt werden. (Beispiel: Persönliches Vorsprechen mit Personalausweis bei einer RA der DFN-PKI oder Verfahren "Post-Ident".)

Authentifizierung

DFN Deutsches Forschungsnetz

Verfahren zum Ausweis einer Identität (A)

Die elektronischen Identitäten müssen sich vor der Nutzung einer Ressource mit einem vorgegebenen Verfahren identifizieren. Hierbei sind im Rahmen der DFN-AAI mehrere Verfahren möglich.

Klasse	Mindestanforderung	Bemerkung
Test	Verfahren freigestellt	In dieser Klasse ist es der nutzenden Einrichtung freigestellt, welche Verfahren sie zum Ausweis der Identität ihrer Angehörigen bereitstellt. Diese Klasse ist typischerweise für Testzwecke geeignet.
Basic	Ausweisen anhand einer eindeutig zuzuordnenden digitalen Adresse.	Dieses Verfahren erlaubt eine einfache Prüfung, die voraussichtlich für eine Menge von Ressourcen ausreichend ist. Bei dieser Prüfung bleibt lediglich offen, ob sich hinter einer ausgewiesenen Adresse tatsächlich die vermutete Identität verbirgt. Anbieter von Ressourcen können sich so z.B. darauf beschränken zu prüfen, ob eine IP-Adresse in einem bestimmten Adressbereich liegt (wie z.B. bei einem Terminal in einer Bibliothek).
Advanced	Ausweis anhand eines personalisierten Accounts mit einer Nutzerkennung und einem Passwort oder digitalem Zertifikat, die im Rahmen einer ausreichend sicheren Vergaberichtlinie ausgestellt wurden.	Mit diesem Verfahren kann eine Identität sich zweifelsfrei ausweisen, sofern bei der Ausstellung der personalisierten Accounts ausreichend sichere Vergaberichtlinien eingehalten werden. Dies ist z.B. für digitale Zertifikate der DFN-PKI "Global" gegeben.

Qualität des IdMs

Datenhaltung und Prozesse zur Pflege der Identitäten (D):
Die nutzende Einrichtung muss ihre elektronische Identitäten pflegen und insbesondere bei Änderungen aktualisieren.

Klasse	Mindestanforderung	Bemerkung
Test	Verfahren freigestellt	In dieser Klasse ist es der nutzenden Einrichtung freigestellt, welche Datenhaltung und Prozesse sie zur Pflege der Identitäten verwendet. Diese Klasse ist typischerweise für Testzwecke geeignet. Es ist den Anbietern von Ressourcen jedoch durchaus freigestellt, wenn sie Ressourcen auch ohne besonderen Anspruch an die Qualität der Datenhaltung und Prozesse der Aktualisierung einer Identität zur Verfügung stellen.
Basic	Mit Verpflichtung bzgl. Korrektheit und Aktualisierung innerhalb von 3 Monaten	In dieser Klasse muss die nutzende Einrichtung sicherstellen, dass die Daten der Identitäten korrekt sind und bei Änderungen diese innerhalb von drei Monaten eingepflegt werden.
Advanced	Mit Verpflichtung bzgl. Korrektheit und Aktualisierung innerhalb von 2 Wochen	In dieser Klasse muss die nutzende Einrichtung sicherstellen, dass die Daten der Identitäten korrekt sind und bei Änderungen diese innerhalb von zwei Wochen eingepflegt werden.

Klassen der Verlässlichkeit

Aus der Erfüllung der Stufen der Einzelkriterien (I, A und D) lässt sich in jedem Einzelfall die Klassen der Verlässlichkeit bestimmen:
die niedrigste Stufe der Einzelkriterien ist der Wert für die Klasse der Verlässlichkeit.

„Verlässlichkeit“ kann die Klasse

- undefined
- basic
- advanced

annehmen.

Realisierung

Schritte:

- **DFN-Föderation mit der Verlässlichkeitsstufen**
  - **basic und**
  - **advanced**
  - (undefined entspricht der Testföderation)

- **Einführung eines Attributes „Verlässlichkeit“ ist im internationalen Kontext möglich, aber nicht kurzfristig (2-3 Jahre) möglich.**

DFN-AAI-Dienstvereinbarung

1 Leistungen des DFN-Vereins

...

Der DFN-Verein koordiniert in Rücksprache mit den Teilnehmern und Anbietern die Modalitäten und Richtlinien für die Kommunikation innerhalb der DFN-AAI und passt sie dem technischen Fortschritt an, insbesondere durch:

- Empfehlungen zur Verwendung von Attributen zur Autorisierung von Nutzern,
- Veröffentlichung der Empfehlungen von Attributen, z.B. auf seinen WWW-Seiten,
- Festlegung von Mindestanforderungen an die zu verwendenden Software-Versionen und Veröffentlichung der Mindestanforderungen, z.B. auf seinen WWW-Seiten,
- **Festlegung von Klassen der Verlässlichkeit bei der Authentifizierung in der DFN-AAI,**
- Festlegung von Kriterien zur Verwendung von Zertifikaten,
- Festlegung der betrieblichen Abläufe.

DFN-AAI-Dienstvereinbarung

2 Mitwirkung des Teilnehmers

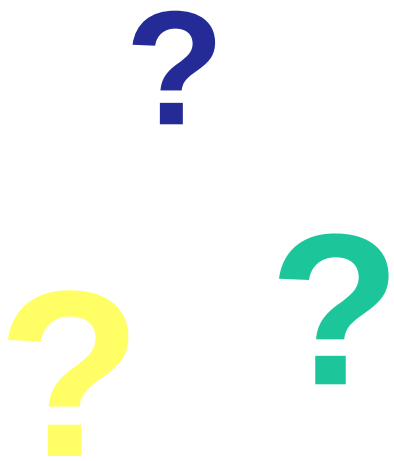
ALT:
Der Teilnehmer betreibt ein System zur Nutzerverwaltung und stellt sicher, dass seinen Nutzern Attribute zugeordnet werden und Änderungen zeitnah (innerhalb von zwei Wochen) in der Nutzerverwaltung gepflegt werden.

NEU:
Der Teilnehmer betreibt ein System zur Nutzerverwaltung und stellt sicher, dass seinen Nutzern Attribute zugeordnet werden.
Der Teilnehmer legt fest, welcher Klasse der DFN-AAI (vgl. Festlegung von Klassen der Verlässlichkeit bei der Authentifizierung in der DFN-AAI) er zugeordnet werden soll und stellt die damit verbundenen Mindestanforderungen sicher.

Fragen ...?

Deutsches Forschungsnetz

Vielen Dank!



aai@dfn.de