DFN
Deutsches Forschungsnetz

DFN-AAI

DEUTSCHE WISSENSCHAFTSFÖDERATION

Ulrich Kähler, DFN-Verein
kaehler@dfn.de

Was ist DFN-AAI?

DFN
Deutsches Forschungsnetz

AAI

Authentifizierung
Autorisierung
Infrastruktur

Was ist DFN-AAI?

DFN
Deutsches Forschungsnetz

- 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, internationale Projekte (CLARIN, etc.)**
- **E-Learning**
- **Interne Dienste innerhalb von Hochschulen**
  - Schreibrechte für TYPO3
  - personalisiertes Web-Portal für Studenten

Anwendung Bibliotheken

DFN Deutsches Forschungsnetz

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), ...

Leistung des DFN-Vereins

DFN
Deutsches Forschungsnetz

- Betrieb der technischen Infrastruktur DFN-AAI
- Vertragspartner für Teilnehmer (insbesondere Hochschulen) und externe Anbieter (z.B. Verlage)
- Anpassung an neue Anwendungen
  - Verlage, Bibliotheken, e-Learning, Grids uvm.
- Organisieren der internationalen Einbettung
- Beratung und Schulung
- Fortgeschrittene Zertifikate über Dienst DFN-PKI

- Aber: DFN übernimmt NICHT den Abschluss von Lizenzverträgen (z.B. mit Verlagen)

Zentrale betriebliche Aufgaben

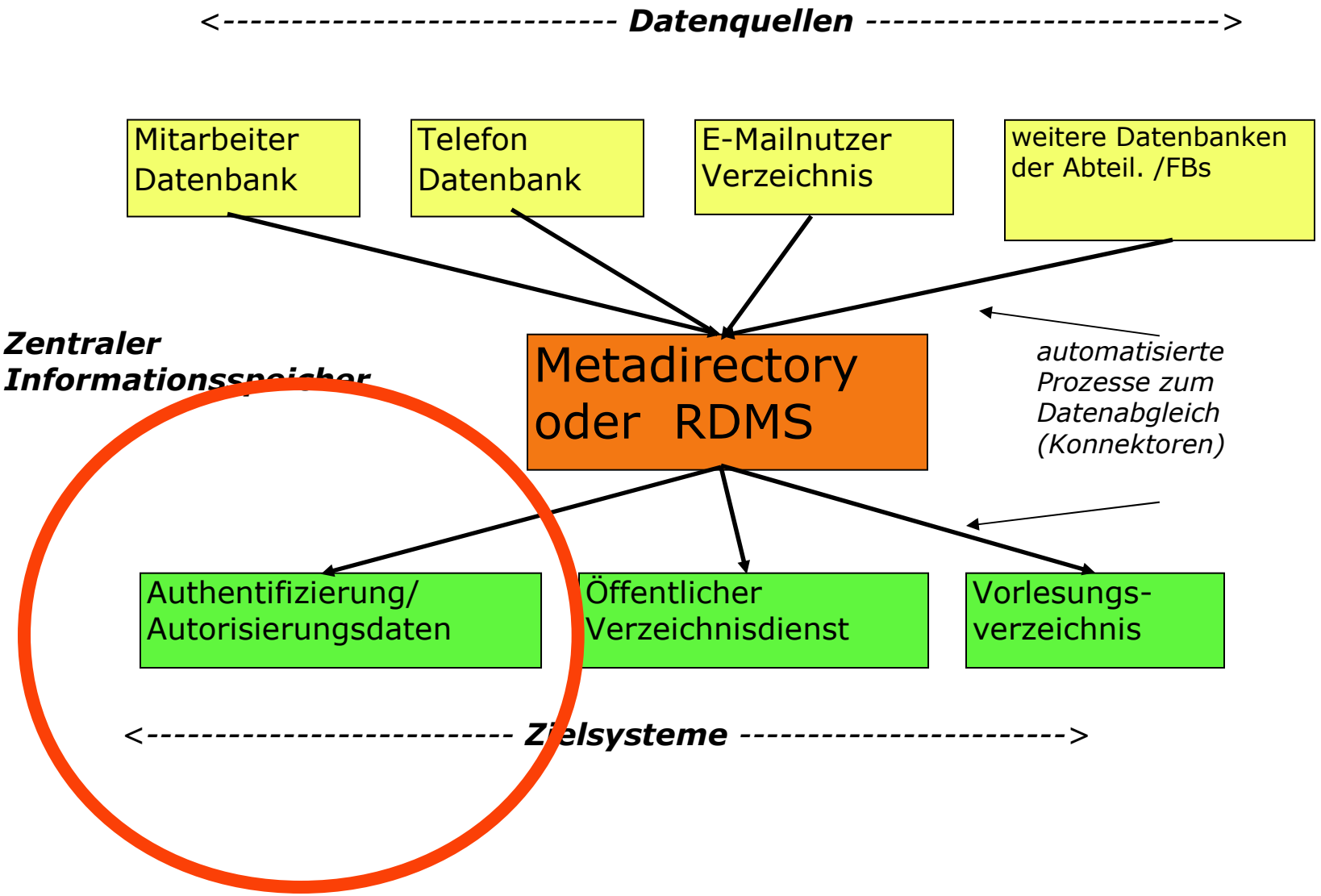
DFN Deutsches Forschungsnetz

- **Administration von Metadaten**
- **Betrieb des WAYF-Servers/Discovery-Service**
- **Betrieb des Test-Systems**
- **Betrieb des Web-Portals**
- **Beratung, Weiterbildung:**
  - **Nutzer-Hotline**
  - **Shibboleth-Workshops**
  - **etc.**

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 in der Nutzerverwaltung gepflegt werden.**
- **Betrieb eines eigenen IdM (mind. LDAP)**
- **Teilnahme am Dienst DFN-PKI**

Identity Management



IdM Wünsche

DFN Deutsches Forschungsnetz

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. .....

Klassen der Verlässlichkeit

DFN Deutsches Forschungsnetz

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.

Verlässlichkeitsklassen

DFN Deutsches Forschungsnetz

Klasse	Identifi-zierung	Authentifi-zierung	Qualität des IdMs
Test	Verfahren freigestellt	Verfahren freigestellt	Verfahren freigestellt
basic	eindeutige Adresse (E-Mail, Telefonnummer, Postanschrift, etc.)	eindeutige digitale Adresse	Verpflichtung bzgl. Aktualität von 3 Monaten
advanced	pers. Vorsprechen gegenüber Vertrauensinstanz unter Vorlage amtlicher Dokumente	pers. Account bzw. digitales Zertifikat (sichere Vergaberichtlinie)	Verpflichtung bzgl. Aktualität von 2 Wochen

Attribute

DFN Deutsches Forschungsnetz

- Unterstützung der Objektklassen
  - **inetOrgPerson** (mit person und organizationalPerson)
  - **eduPerson**
- Beispiele:

– **surname**	Nachname
– **mail**	Mailadresse
– **eduPersonPrincipleName**	Name + Domain
– **eduPersonScopedAffiliation**	Rolle + Domain
– **eduPersonEntitlement**	Berechtigung
– **eduPersonTargetedID**	Pseudonym f. Anbieter

- **Attribute müssen applikationsbezogen festgelegt werden!**
- **Erweiterung der Attributliste kann notwendig werden durch neue Anwendungen oder neue Anforderungen der Anbieter!**
  z.B. E-Learning, GRIDs, Stärke der Authentifizierung, etc.

Attributauswahl für E-Learning (I)

- **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)

Attributauswahl für E-Learning (II)

- **Für alle folgenden Informationen mussten DFN-Attribute definiert werden**
- **Dies sind**
  - Kostenstelle (dfnEduPersonCostCenter)
  - Titel (personalTitle)
  - alle Attribute zum Studiengang

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

Sicherheit

- Die Sicherheit in der DFN-AAI ist eine entscheidende Voraussetzung für deren Nutzung
- Sicherheit umfasst mehrere Komponenten
  - Vertraulichkeit
  - Integrität
  - Authentizität
  - Verfügbarkeit
- DFN-PKI hat sich als wichtige Basis etabliert

utzung von Zertifikaten

DFN
Deutsches Forschungsnetz

In der DFN-AAI kommen Zertifikate in drei Bereichen zum Einsatz:

- **zur Signierung der Metadaten**
- **für die Kommunikation der beteiligten Server/Clients**
- **ggfs. zur Authentifizierung von Nutzern**

DFN-PKI ist vorhanden!

Recht: verschiedene Blickwinkel

- **Rechtliche Sicht aus verschiedenen Blickwinkeln**
  - **Datenschutz**
  - **Personalrat**
  - **Haftung**
  - **Telemediengesetz**
  - **Signaturgesetz**
  - **Datensicherheit**

Recht: Datenschutz

- **Authentifizierung durch die Hochschule**
  - **Vorteil: Anonymität gegenüber Anbieter**
  - **Voraussetzung: Vorhandenes IdM**
    - **Datenschutzrechtliche Fragen bei Errichtung**
    - **Landesrechtliche Besonderheiten**
  - **Problem: Grundsatz der Zweckbindung**
    - **Authentifizierung ist ggf. zweckändernde Nutzung**
      - **Erfordert gesetzliche Erlaubnis oder Einwilligung**

Recht: Einwilligung

- **Lösung: Elektronische Einwilligung auf der Startseite:**

  Beispiel:

  Mit der Verwendung der zu meiner elektronischen Hochschulidentität gespeicherten Daten zur Prüfung der Berechtigung zur Nutzung von mir ausgewählter Dienste bin ich einverstanden.

User ID …

Passwort …

Recht: Personalrat

- **Mitarbeiter als Nutzer**
  - **Authentifizierung in der Einrichtung ermöglicht festzustellen, welcher Nutzer auf welchen Anbieter zugegriffen hat (nicht Inhalte)**
- **Technische Leistungs- und Verhaltenskontrolle**
  - **z.B. § 72 Abs. 3 Nr. 2 LPersVG NRW**
  - **Objektive Eignung hierzu ausreichend**
- **Personalrat sollte beteiligt werden!**

Fragen ...?

DFN
Deutsches Forschungsnetz

Vielen Dank!

aai@dfn.de