Aufbau einer AAI im DFN

Ulrich Kähler, DFN-Verein
kaehler@dfn.de

Anwendungsbeispiele

DFN Deutsches Forschungsnetz

- **Bibliothekswesen und Verlage**

Elsevier, JSTOR, CSA, EBSCO, ThomsonGale, Proquest, GENIOS/GBI sind bereit,
bei OVID, ISI/Thomson, Springer, FIZ Technik, IZ-Sozialwissenschaften und DIPF in Arbeit,
ReDI, vascoda, DFG-Nationallizenzen

- **Software-Verteilung**

Erweiterung von MSDNAA (Microsoft Developer Network Academic Alliance) auf alle Hochschulen über DFN-AAI
AUTOCAD für Studierende

- **E-Learning**

SaxIS: alle Hochschulen in Sachsen verfügen über IdM

- **D-GRID**

C3-Community, Text-Grid, (INGRID),
Server für kurzlebige Grid-Zertifikate (SLCS)

Wie funktioniert AAI ?

Nutzerin

Nutzung

Ressource
des Anbieters

Authentifizierung

Nutzerdaten

Autorisierung

Lizenzvereinbarung

Hochschule
Anwender

Wie funktioniert AAI ?

Nutzerin

Heimateinrichtung
Anwender

(1)

(2)

(3)

(4)

(5)

(6)

(7)

(8)

(9)

Nutzerin bekannt?

nein

ja

Lokalisierungsdienst

Nutzerin berechtigt?

ja

gestattet

Zugriff

nein

verweigert

Anbieter

Shibboleth-System

Was ist Shibboleth ?

Shibboleth ist eine Entwicklung aus INTERNET2 und baut auf folgende Standards auf:

HTTP
XML
XML Schema (XSD)
XML Signatur (XMLDisg)
SOAP
SAML 1.1 (später 2.0)

Was ist DFN-AAI ?

- **DFN-AAI** ist ein Dienst des DFN-Vereins für Wissenschaftseinrichtungen und (auch kommerziellen) Anbietern zur Nutzung einer AAI.

- **DFN-AAI** schafft das für notwendige **Vertrauensverhältnis** zwischen vielen Anwendern und vielen Anbietern und einen **organisatorischen Rahmen** für den Austausch von Nutzerinformationen.

Wo ist das Problem ?

DFN Deutsches Forschungsnetz

- Anbieter muss dem Anwender **vertrauen**.

  - Es geht um **Geld.**

- **„Vertrauen“** heißt im Geschäftsleben: **„Vertrag“.**

- Es müssen **belastbare vertragliche Regelungen** getroffen werden.

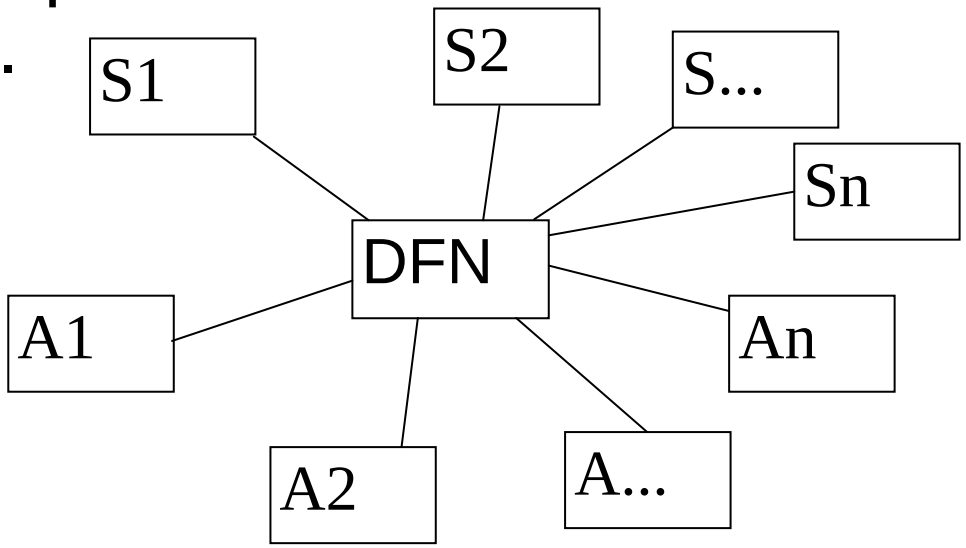
Aufgaben des DFN-Vereins

- Vorgabe von Richtlinien (Policy)
- Vertragsgestaltung und -abschluss
- zentrale betriebliche Aufgaben
- Public Relations
- internationale Vertretung

DFN-AAI

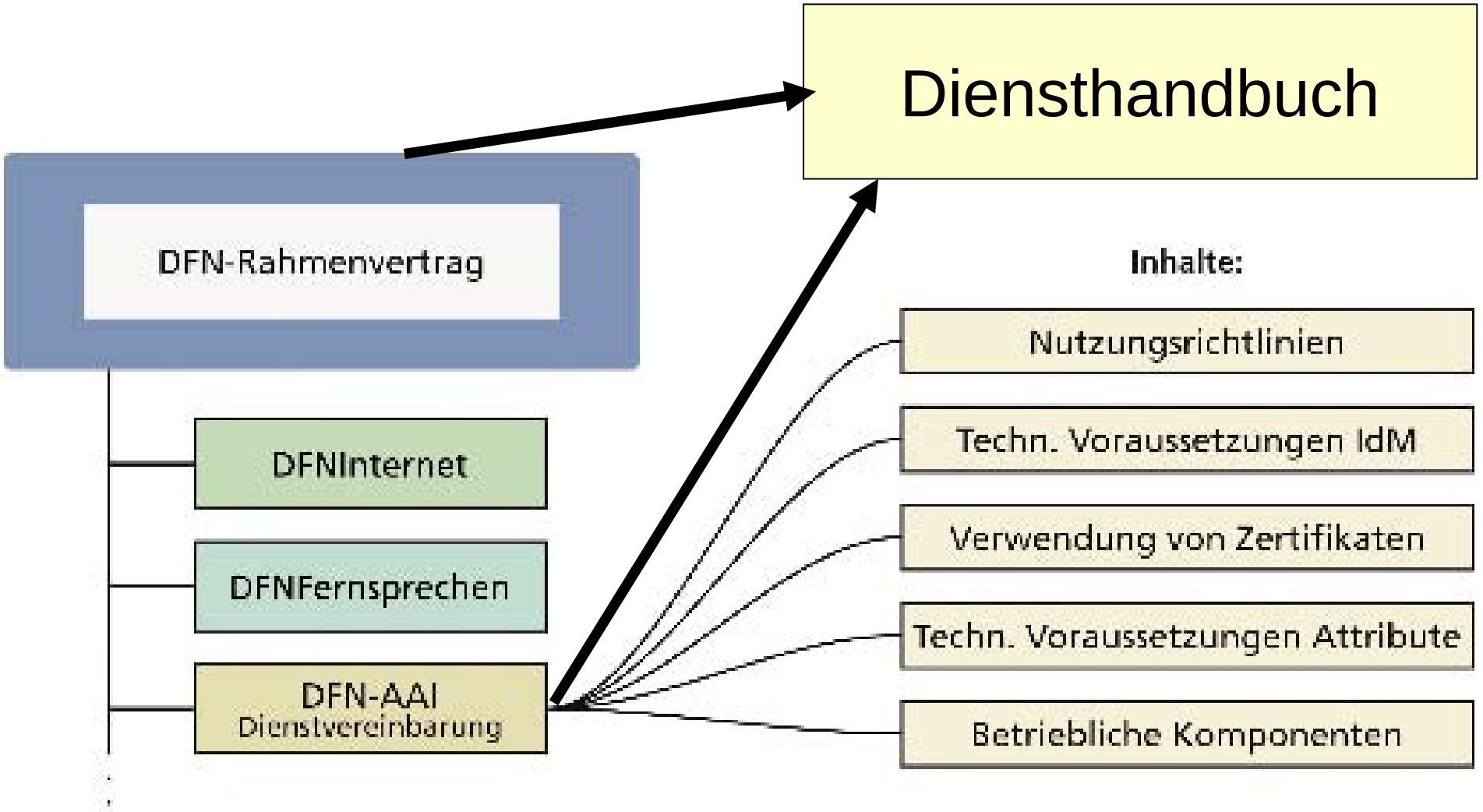
Der DFN-Verein

- ist zentraler Vertragspartner für alle Teilnehmer der AAI.



- übernimmt **nicht** die Lizenzverträge.

Vertragsgestaltung / -abschluss



Vertragsgestaltung und Abschluss

DFN Deutsches Forschungsnetz

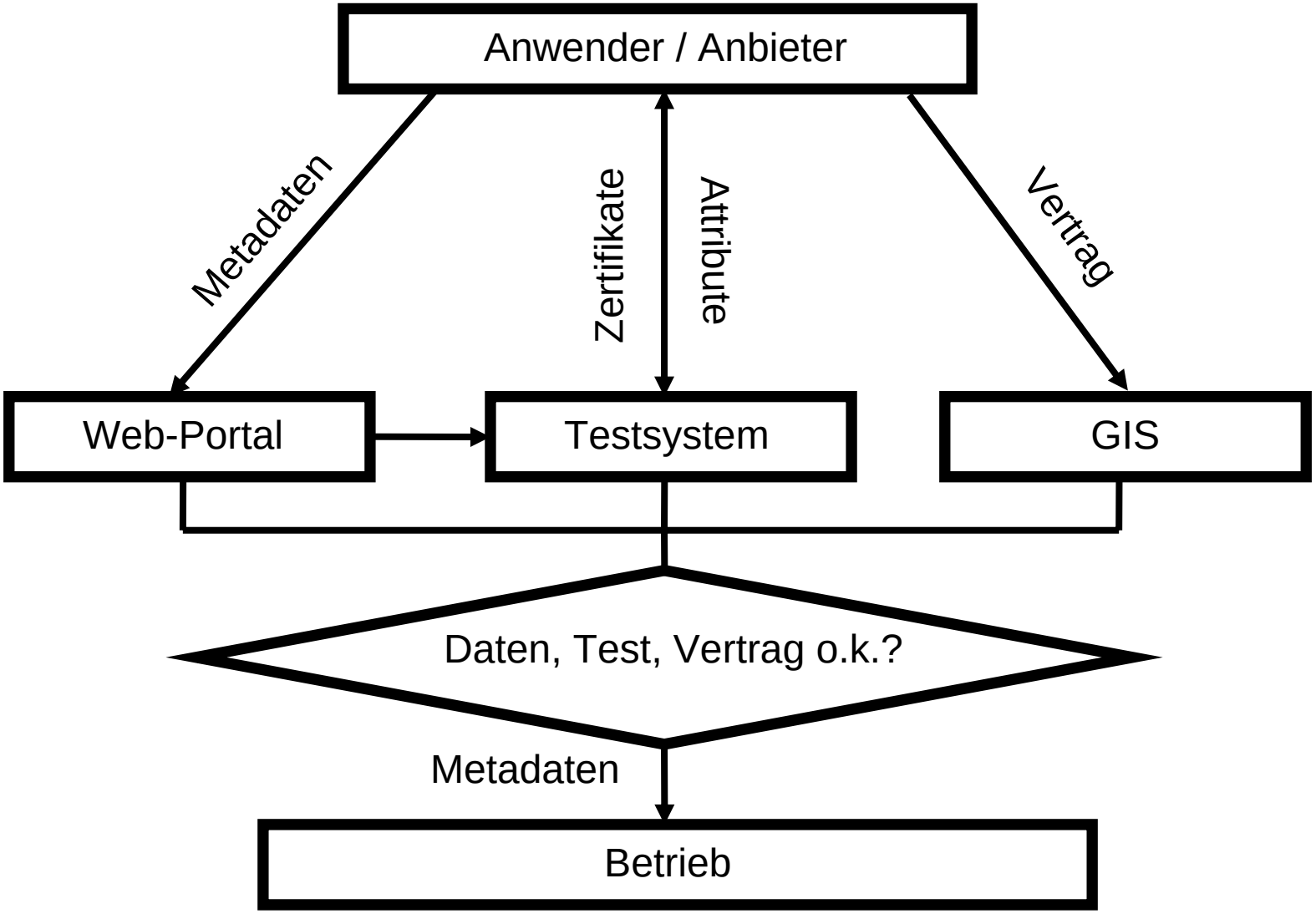
1.Teilnehmervertrag liegt vor

2. Anbietervertrag in Arbeit
- **DFN-Teilnehmer**
- **Verlage: gem. Abstimmung auf europ. Ebene**

Zentrale betriebliche Aufgaben

1. **Metadatenverwaltung: Testbetrieb**
2. **WAYF-Server: Testbetrieb**
3. **Testsystem: Testbetrieb**
4. **Web-Portal: vorhanden, wird ausgebaut**
5. **Schulung, Beratung: WS4 im Februar,**
   WS5 für Oktober geplant

Anschaltprozedur



Wie funktioniert AAI ?

Nutzerin

(1)

(3)

Lokalisierungsdienst

(2)

Nutzerin bekannt?

nein

ja

(6)

Nutzerin berechtigt?

(5)

(4)

(9)

(7)

ja

gestattet

Zugriff

(8)

nein

verweigert

Heimateinrichtung
Anwender

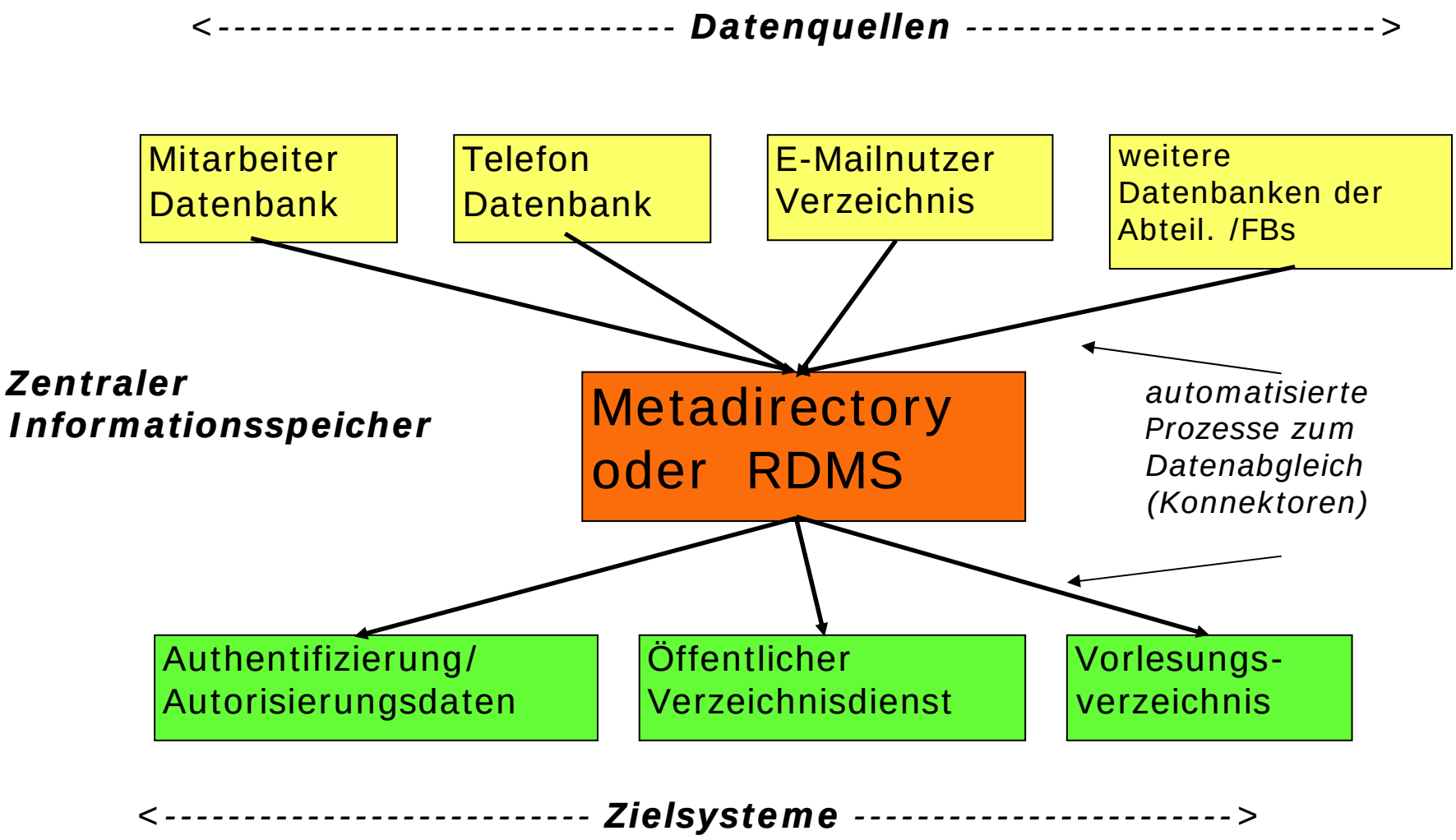
Anbieter

Identity-Management-System

Identity Management

- Jeder Person wird eine digitale Identität zugewiesen.
  - eindeutiger Name oder eine Nummer oder ein Login-String
- Jede Person kann über diese digitale Identität von verschiedenen Systemen identifiziert werden.
- Eine digitale Identität besitzt verschiedene Merkmale (Attribute)
  - Vor- und Nachname
  - E-Mail-Adresse
  - Telefonnummer
  - Zugehörigkeit zu Gruppen
  - Rollen
  - etc.

Identity Management



Forderungen aus AAI-Sicht

- **Personen erhalten elektronische Identität**
  - Attribute beschreiben die Rolle der Person

- **Qualitätsanforderungen**
  - Verlässlichkeit
    Sicherheitsstufen, Missbrauchverhinderung
  - Aktualität
    zeitnahe Änderung
  - Nachvollziehbarkeit
    Dokumentation, Logging
  - Ausfallsicherheit
    Back-up-Systeme

- **Einklang mit rechtlichen Vorgaben**
  - Datenschutzgesetz

Attribute

- Unterstützung der Objektklassen
  - **inetOrgPerson** (mit person und organizationalPerson)
  - **eduPerson**
- Obligatorische und empfohlene Attribute
- obligatorisch sind:
  - **surname** Nachname
  - **mail** Mailadresse
  - **eduPersonPrincipleName** Name + Domain
  - **eduPersonScopedAffiliation** Rolle + Domain
  - **eduPersonEntitlement** Berechtigung
  - **eduPersonTargetedID** Pseudonym f. Anbieter
- Erweiterung der Attributliste kann notwendig werden durch neue Anwendungen oder Anforderungen der Anbieter!

Nutzung von Zertifikaten

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

- beim Betrieb von Shibboleth
- zur Authentifizierung der Web-Server, die die Dienste anbieten
- zur Authentifizierung von Nutzern

Zertifikate: Nutzer

- derzeit verwenden Nutzer zur Authentifizierung meistens Username/Password

- alternativ kann die Authentifizierung auch per Nutzerzertifikat erfolgen

- zukünftig kann auf Basis der Stärke der Authentifizierung die Nutzung von Diensten geregelt werden

Der Datenschutzbeauftragte frohlockt!

Personenbezogene Daten bleiben dort, wo sie hingehören.
Durch Flexibilität und Feingranulität brauchen personenbezogene Daten nicht übertragen zu werden.

Zeitplan

- **März 2006:**
  1. Treffen interessierter Teilnehmer

- **November 2006:**
  Fertigstellung grundlegender Dokumente
  (Vorauss. an IdM, Attribute-Schema, Zertifikate)

- **seit März 2007:**
  Pilotbetrieb

- **ab April 2007:**
  Vertragsabschlüsse mit Teilnehmern

- **ab Mai 2007:**
  Akquisition von Anbietern

Kontakt

Für alle Fragen rund um die DFN-AAI:

E-Mail: aai@dfn.de