DFN-AAI

Ulrich Kähler, DFN-Verein
kaehler@dfn.de

Anwendungsbeispiele

DFN Deutsches Forschungsnetz

•**Bibliothekswesen und Verlage**
Verlage, ReDI, vascoda, DFG-Nationallizenzen

Die treibend Kraft für DFN-AAI!

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

•**D-GRID**
C3-Community, Text-Grid, (INGRID),
Server für kurzlebige Grid-Zertifikate (SLCS)

•**E-Learning**
Bildungsportal Sachsen, etc.

Was ist DFN-AAI?

- DFN-AAI ist ein **Dienst** des DFN-Vereins.

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

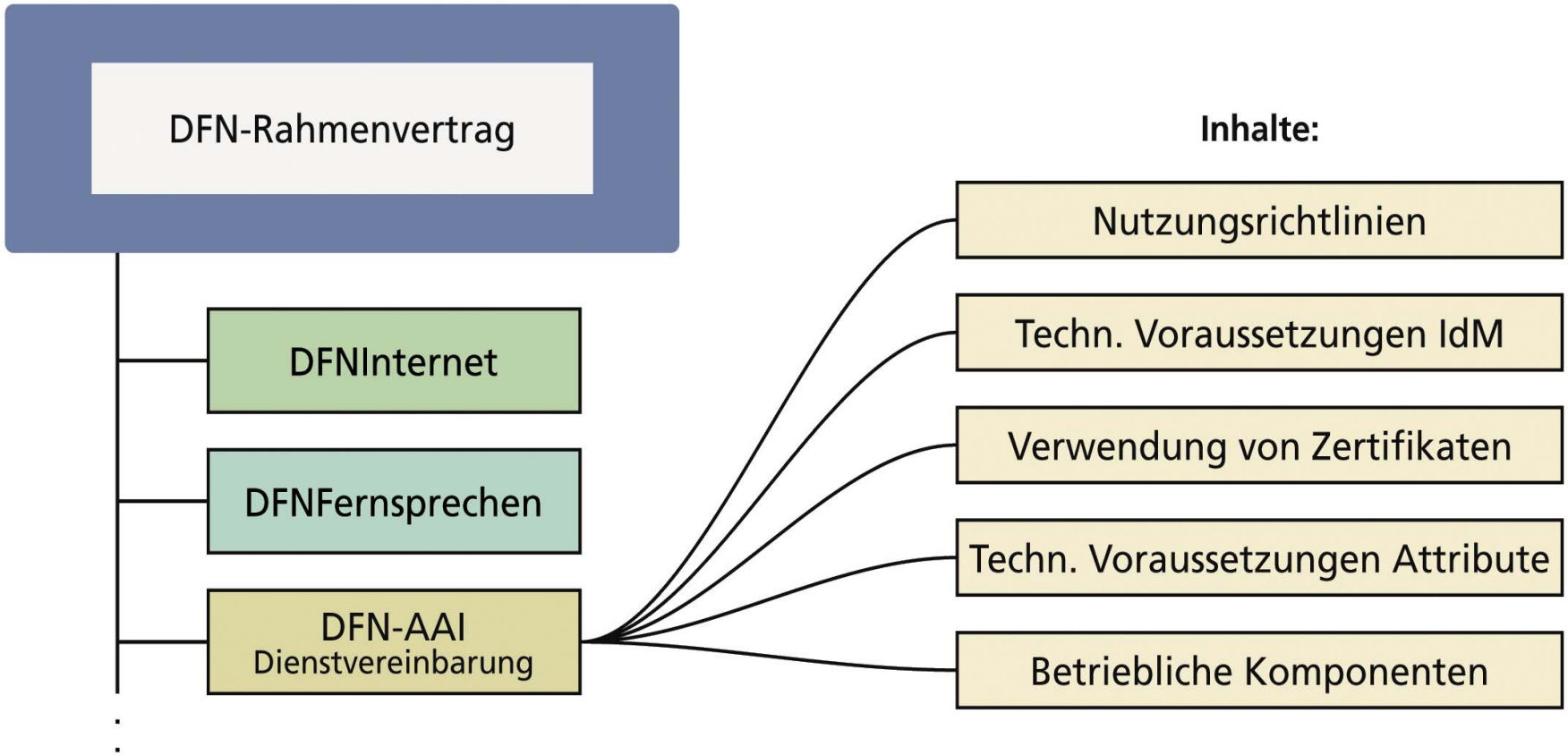
- Der DFN-Verein ist der **zentrale Vertragspartner** für alle Teilnehmer der AAI.

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

Leistung des DFN-Vereins

- **Fortgeschrittene Zertifikate über Dienst DFN-PKI**
- **Betrieb der technischen Infrastruktur DFN-AAI**
- **Vertragspartner für Teilnehmer (insbesondere Hochschulen) und externe Anbieter (z.B. Verlage)**
- **Anpassung an neue Anwendungsfälle**
  - **Verlage, Bibliotheken, eLearning, Grid uvm.**
- **Organisation der internationalen Einbettung**
- **Beratung und Schulung**
- **Nicht Leistung von DFN: Lizenzverträge (z.B. mit Verlagen)**

Vertragsgestaltung / -abschluss



Vertragsgestaltung und Abschluss

DFN Deutsches Forschungsnetz

1. **Teilnehmervertrag liegt vor**
   Ca. 20 Einrichtungen haben unterschrieben ohne Änderungswünsche.

2. **Anbietervertrag liegt vor (Vorlage: Schweiz)**
   - **unterschrieben von:**
     OVID, Thomson, EBSCO, Uni Freiburg (REDI), HBZ (Vascoda), Uni Heidelberg, Uni Göttingen (Nationallizenzen), Microsoft

   - **in Vorbereitung:**
     Metapress (Springer), Elsevier, JSTOR

Zentrale betriebliche Aufgaben

DFN Deutsches Forschungsnetz

1. **Metadatenverwaltung: Betrieb ab Oktober 07**

2. **WAYF-Server: Betrieb ab Oktober 07**

3. **Testsystem: Betrieb ab Oktober 07**

4. **Web-Portal: vorhanden, wird ausgebaut**

5. **Schulung, Beratung:**
   5 Shibboleth-Workshops bisher

Testsystem

DFN Deutsches Forschungsnetz

Sinn der Testumgebung ist

- das Vertrautwerden mit den Shibboleth-Komponenten und deren Konfiguration

- die Überprüfung, ob die eigenen technischen und organisatorischen Voraussetzungen für den Einsatz in der DFN-Föderation erfüllt sind

- neue Software-Versionen und -Varianten ausprobieren zu können ohne die Produktions Systeme benutzen zu müssen.

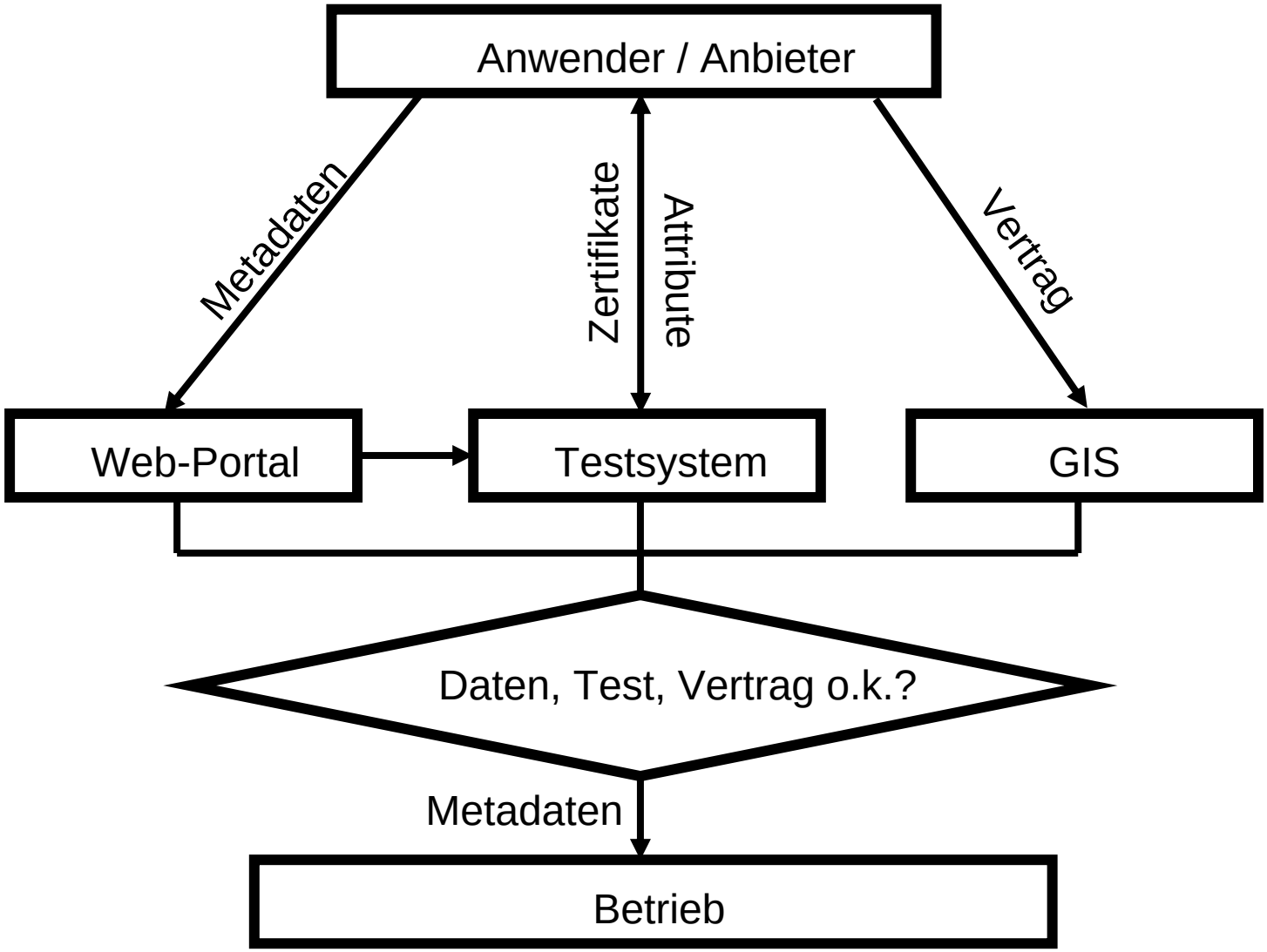
Testsystem

Voraussetzung für die Teilnahme am DFN-AAI-Regelbetrieb ist das vorausgegangene erfolgreiche Durchlaufen des Testsystems!

Einzelne Schritte:

- **Registrierung des SPs bzw. IdPs**
- **Download der aktualisierten Metadaten**
- **Konfiguration des SPs bzw. IdPs für das Testsystem**
- **Funktionstest mit Hilfe des DFN-IdPs und SPs.**

Anschaltprozedur



Wie funktioniert AAI ?

Nutzerin

(1)

(2)

(3)

(4)

(5)

(6)

(7)

(8)

(9)

Nutzerin bekannt?

nein

ja

Lokalisierungsdienst

Nutzerin berechtigt?

ja

gestattet

Zugriff

nein

verweigert

Anbieter

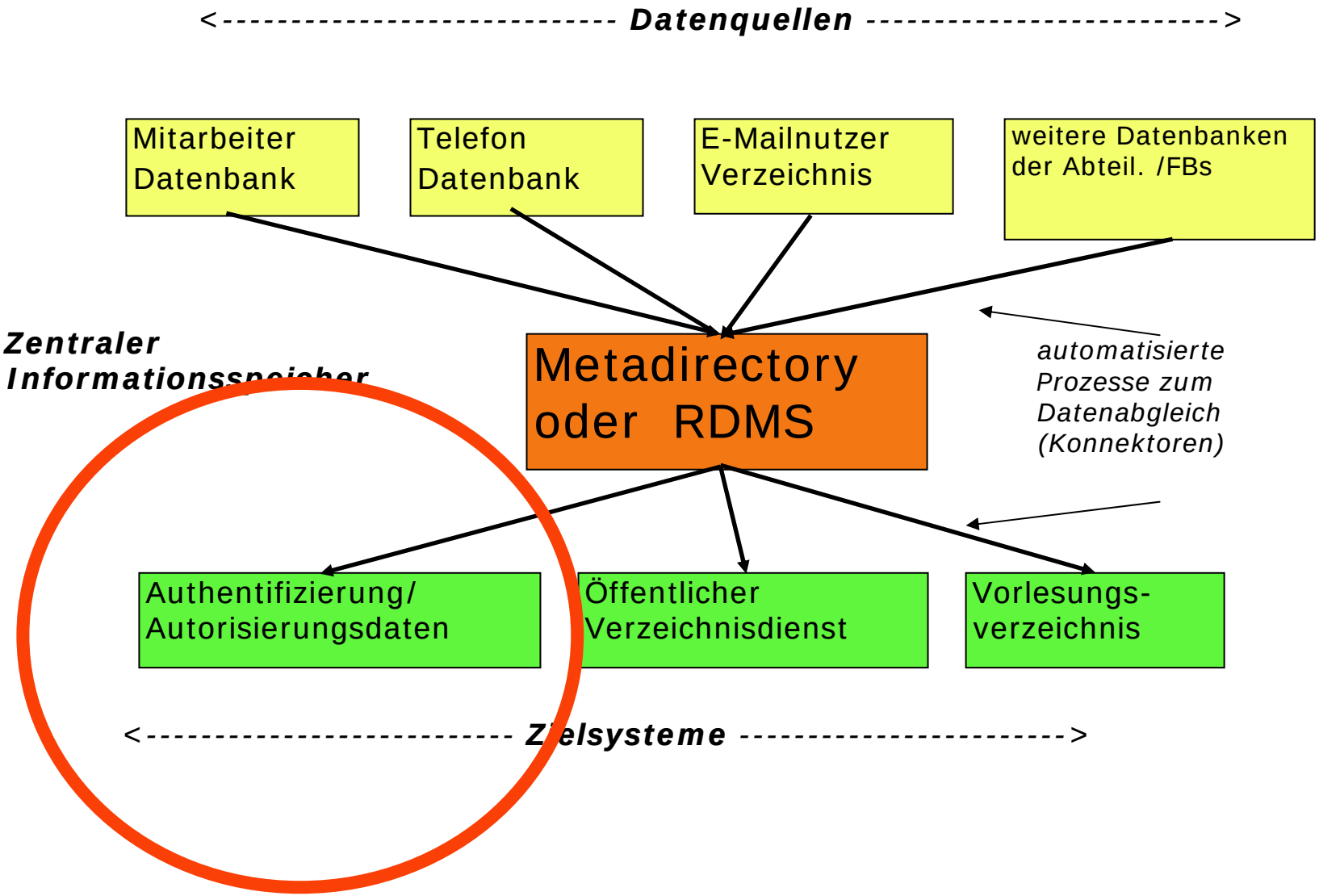
Heimateinrichtung
Anwender

Identity-Management-System

Mitwirkung: Hochschulen

- **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**

Identity Management



Forderungen aus AAI-Sicht

DFN Deutsches Forschungsnetz

- 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**
- 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.

Nutzung von Zertifikaten

DFN Deutsches Forschungsnetz

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

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

DFN-PKI ist vorhanden!

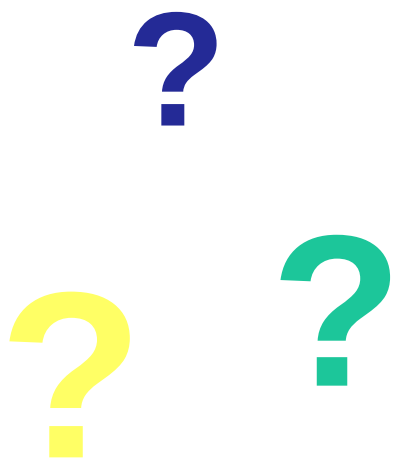
Zeitplan DFN-AAI

DFN
Deutsches Forschungsnetz

- seit Januar 2006: Regelbetrieb DFN-PKI
- November 2006: Konzept DFN-AAI fertig
- seit März 2007: Pilotbetrieb
- April 2007: Teilnehmervertrag fertig
- September 2007:Anbietervertrag fertig
- ständig: Akquisition weiterer Anbieter
- ab Oktober 2007: Regelbetrieb
- ab 2008: Hochverfügbarkeit durch Redundanzkonzept
- ab Januar 2008: Attribut-Definition für E-Learning
- 3. - 6. Juni 2008: Deutscher Bibliothekarstag
- In 2008: Umstieg auf Shibboleth 2.0

Fragen ...?

Vielen Dank!



aai@dfn.de