DFN
Deutsches Forschungsnetz

DFN-AAI

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

- **D-GRID**

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

- **E-Learning**

SaxIS: alle Hochschulen in Sachsen verfügen über IdM

Lösungen bisher

- Benutzerkennung und Passwort (beim Anbieter)
  Nachteile: hoher Aufwand, Aktualisierung problematisch, Nutzer hat viele Passwörter, ...
- IP-Adressenprüfung
  Nachteile: Zugriff von Zuhause, Reisende, nicht personenbezogen, ...
- Viele fantasievolle Einzellösungen

Wie funktioniert AAI ?

Benutzerin

(1)

(2)

(3)

(4)

(5)

(6)

(7)

(8)

(9)

Benutzerin bekannt?

nein

ja

Lokalisierungsdienst

Benutzerin berechtigt?

ja

gestattet

Zugriff

nein

verweigert

Anbieter

Heimateinrichtung

Was ist Shibboleth ?

DFN Deutsches Forschungsnetz

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)

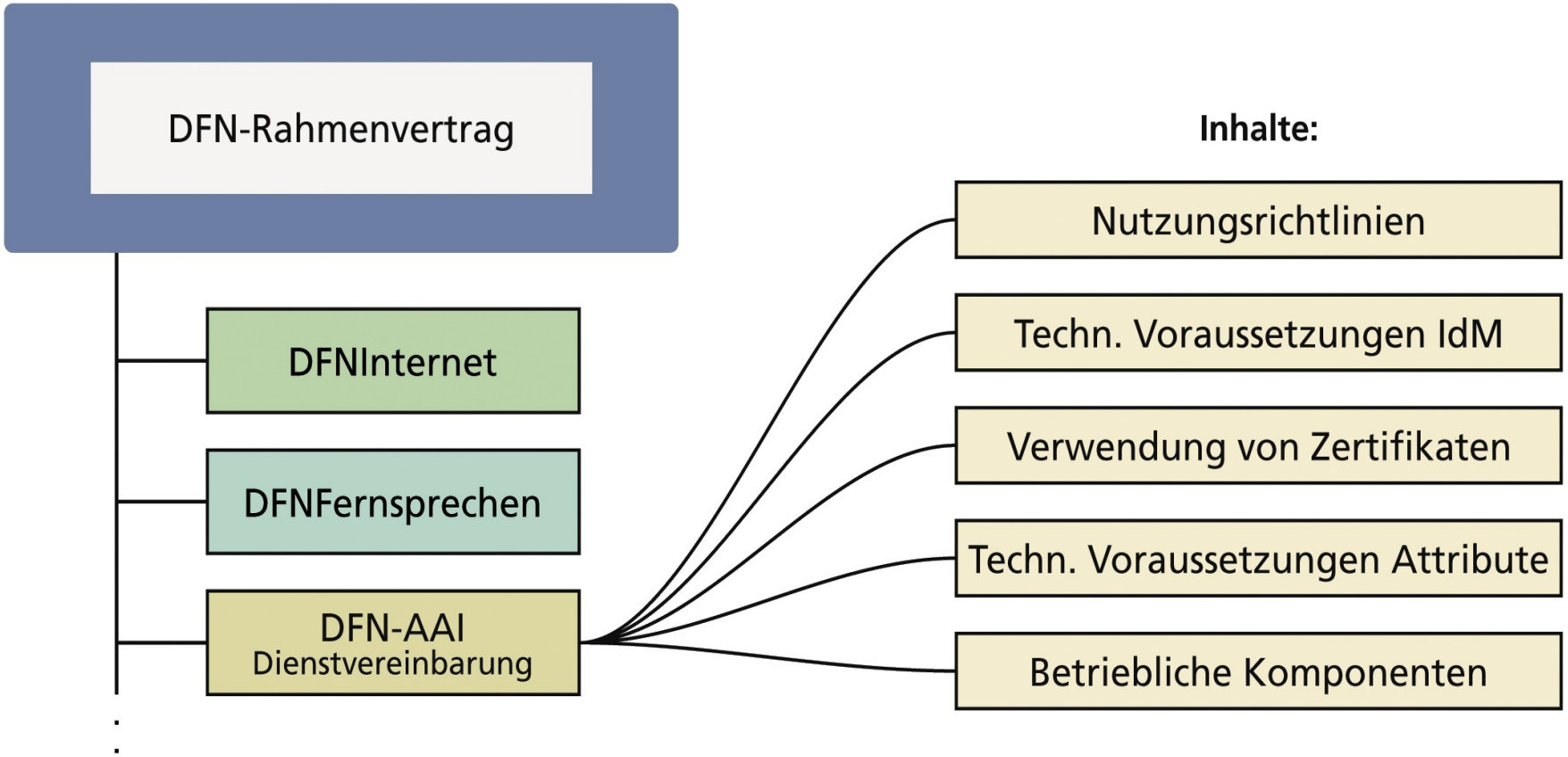
Was ist DFN-AAI?

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

- Fortgeschrittene Zertifikate über Dienst DFN-PKI
- Betrieb der technischen Infrastruktur DFN-AAI
- Vertragspartner für Teilnehmer (insbesondere Hochschulen) und externe Anbieter (z.B. Verlage)
- Laufende 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

- Teilnehmervertrag liegt vor (auch schon unterzeichnete Verträge)

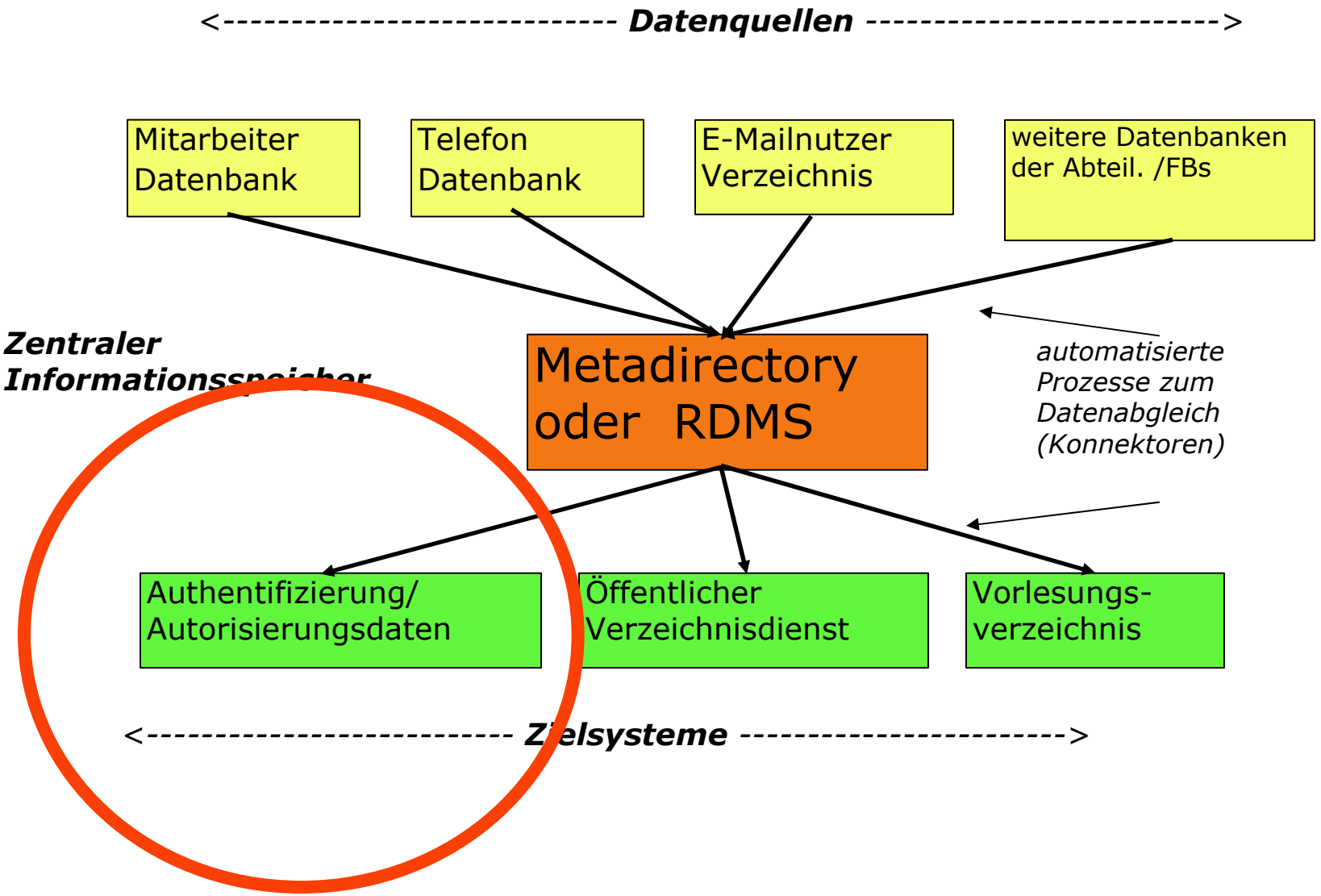
- Anbietervertrag in Arbeit
  - DFN-Teilnehmer o.k.
  - Verlage: gem. Abstimmung auf europ. Ebene

Mitwirkung

- 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
- Teilnahme am Dienst DFN-PKI

Identity Management



Attribute

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

- 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!

Datenschutz

DFN Deutsches Forschungsnetz

Der Datenschutzbeauftragte frohlockt!

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

Nutzung von Zertifikaten

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

- seit Januar 2006: Regelbetrieb DFN-PKI
- November 2006: Konzept DFN-AAI fertig
- seit März 2007: Pilotbetrieb
- seit April 2007: Teilnehmervertrag fertig
- seit Mai 2007: Akquisition weiterer Anbietern (z.Zt. aktuell: Verlage)
- Geplant ab Herbst 2007: Regelbetrieb
- Geplant ab 2008: Hochverfügbarkeit durch Redundanzkonzept