Die Dienste der DFN-AAI

Ulrich Kähler, DFN-Verein
kaehler@dfn.de

Was ist DFN-AAI?

DFN Deutsches Forschungsnetz

AAI

Authentifizierung
Autorisierung
Infrastruktur

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**-Verfahren verwendet.

Wie funktioniert Shibboleth?

Benutzerin

Erster Zugriff

(1)

Anbieter

Shibboleth-Sitzung vorhanden?

(2) nein

(3)

Discovery-Service

(4)

Authentifizierungsanfrage

(5)

(6)

Login

Heimateinrichtung

AuthN & Attribute

(7)

(8)

Ja

Nein

Zugriff

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

Leistung des DFN-Vereins

- **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**

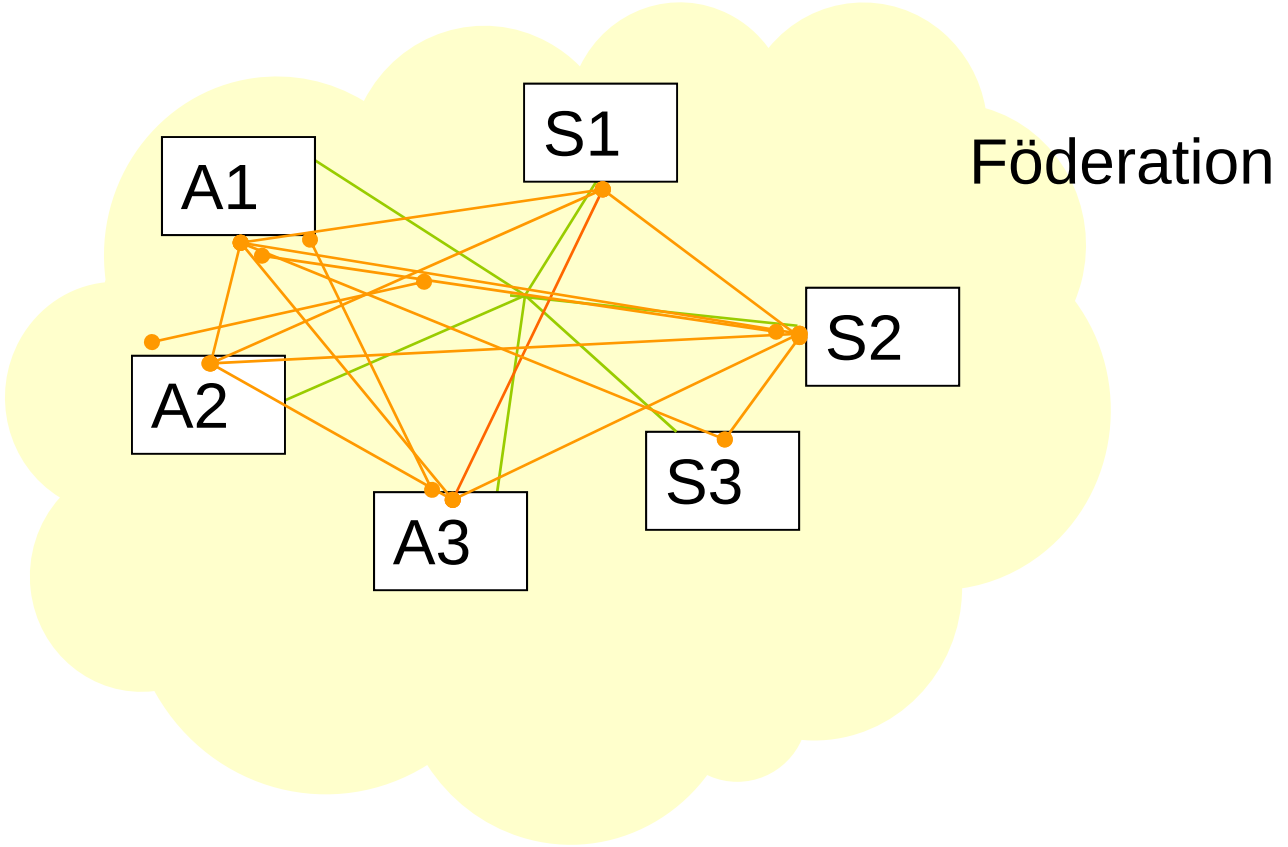
- **Aber: DFN übernimmt NICHT den Abschluss von Lizenzverträgen (z.B. mit Verlagen)**

Zentrale betriebliche Aufgaben

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

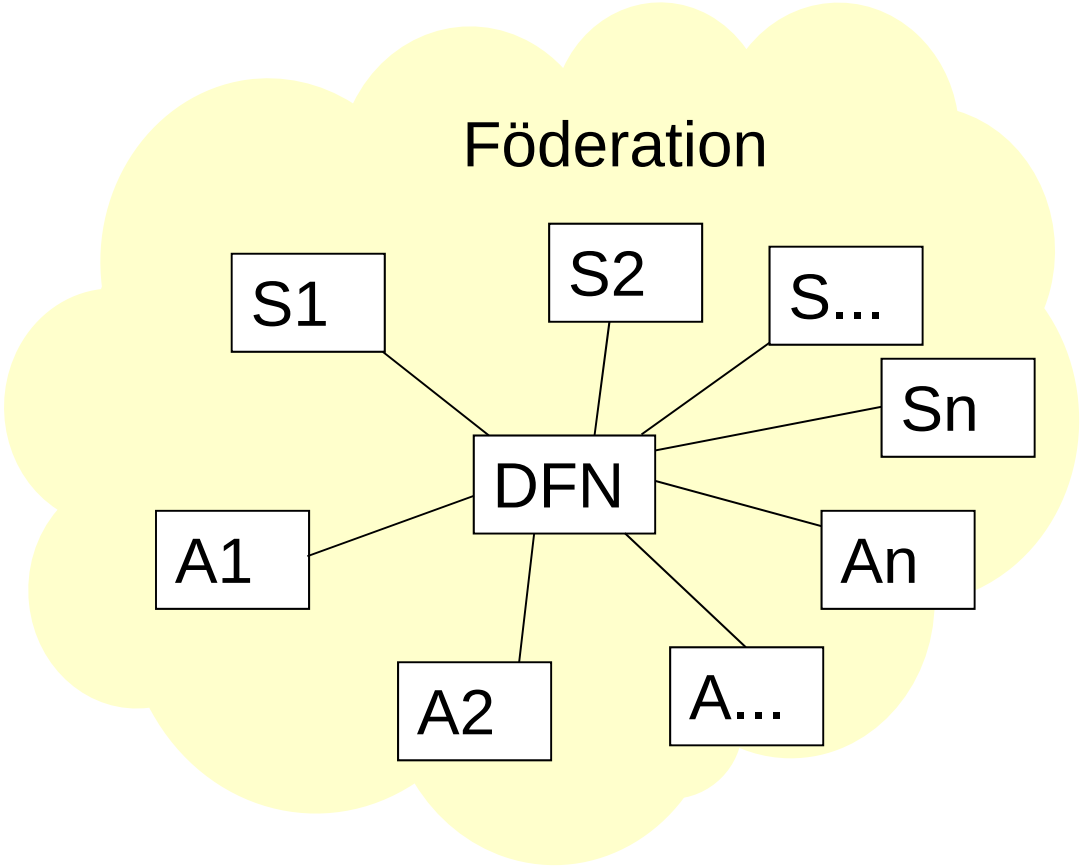
Dezentraler Vertragsabschluss

Jeder Anbieter schließt mit jedem Anwender einen Vertrag ab.

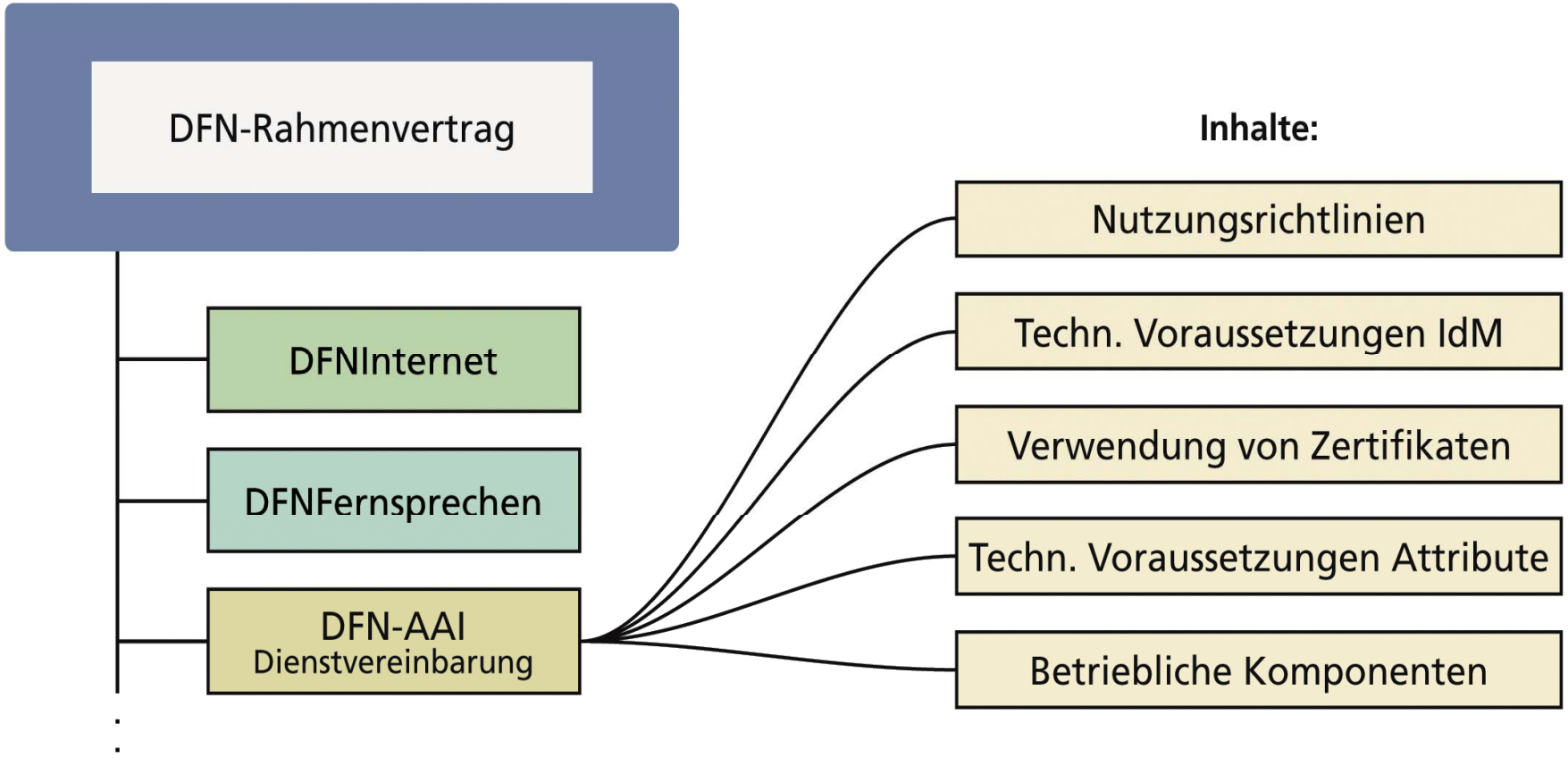


Zentraler Vertragsabschluss

Der DFN-Verein als zentraler Vertragspartner für alle Teilnehmer der AAI.



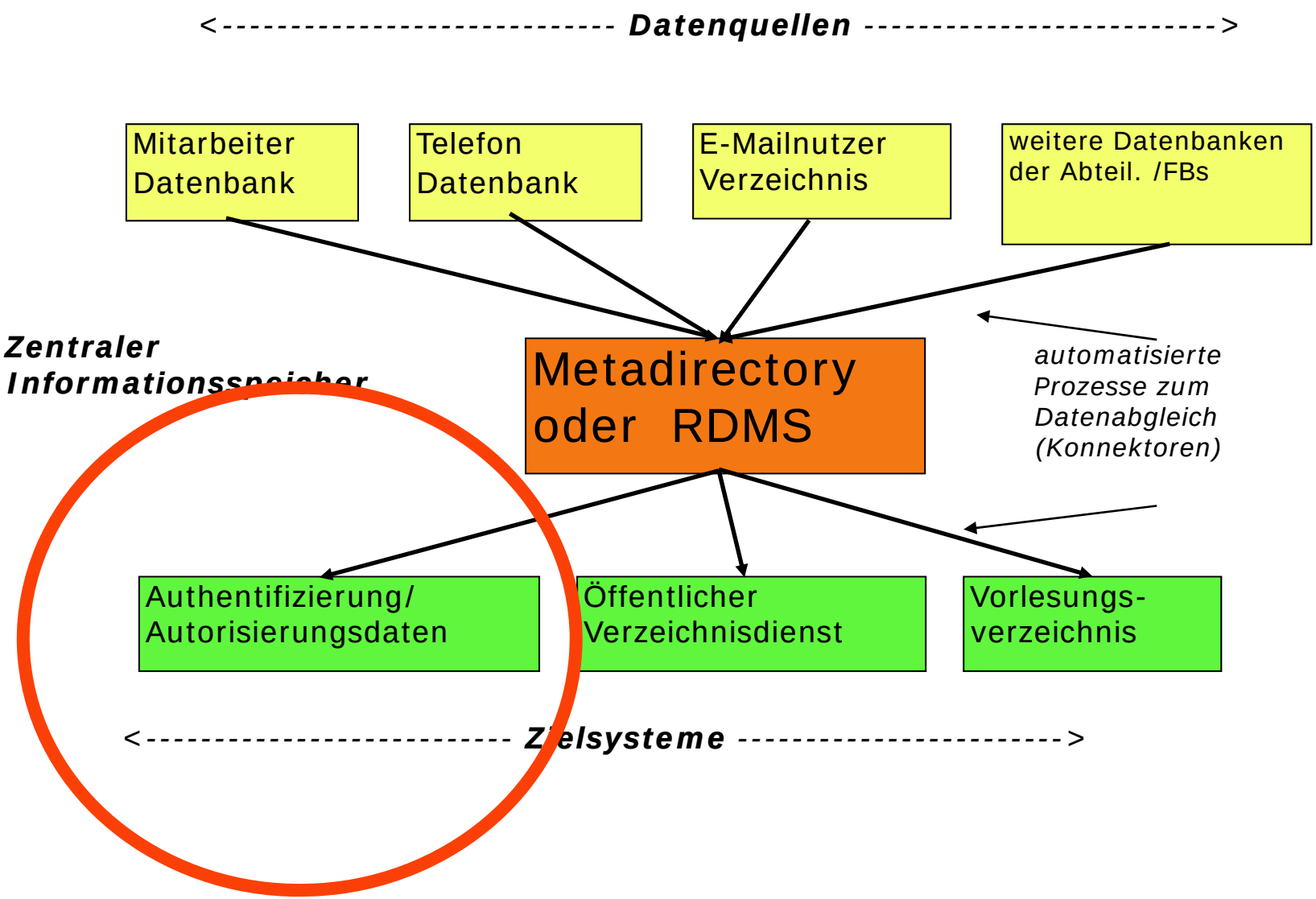
Vertragsgestaltung / -abschluss



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 Situation

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. .....

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

Wie funktioniert Shibboleth?

Benutzerin

Erster Zugriff

(1)

Anbieter

Shibboleth-Sitzung vorhanden?

(2) nein

(3)

Discovery-Service

(4)

Authentifizierungsanfrage

(5)

(6)

Login

Heimateinrichtung

AuthN & Attribute

(7)

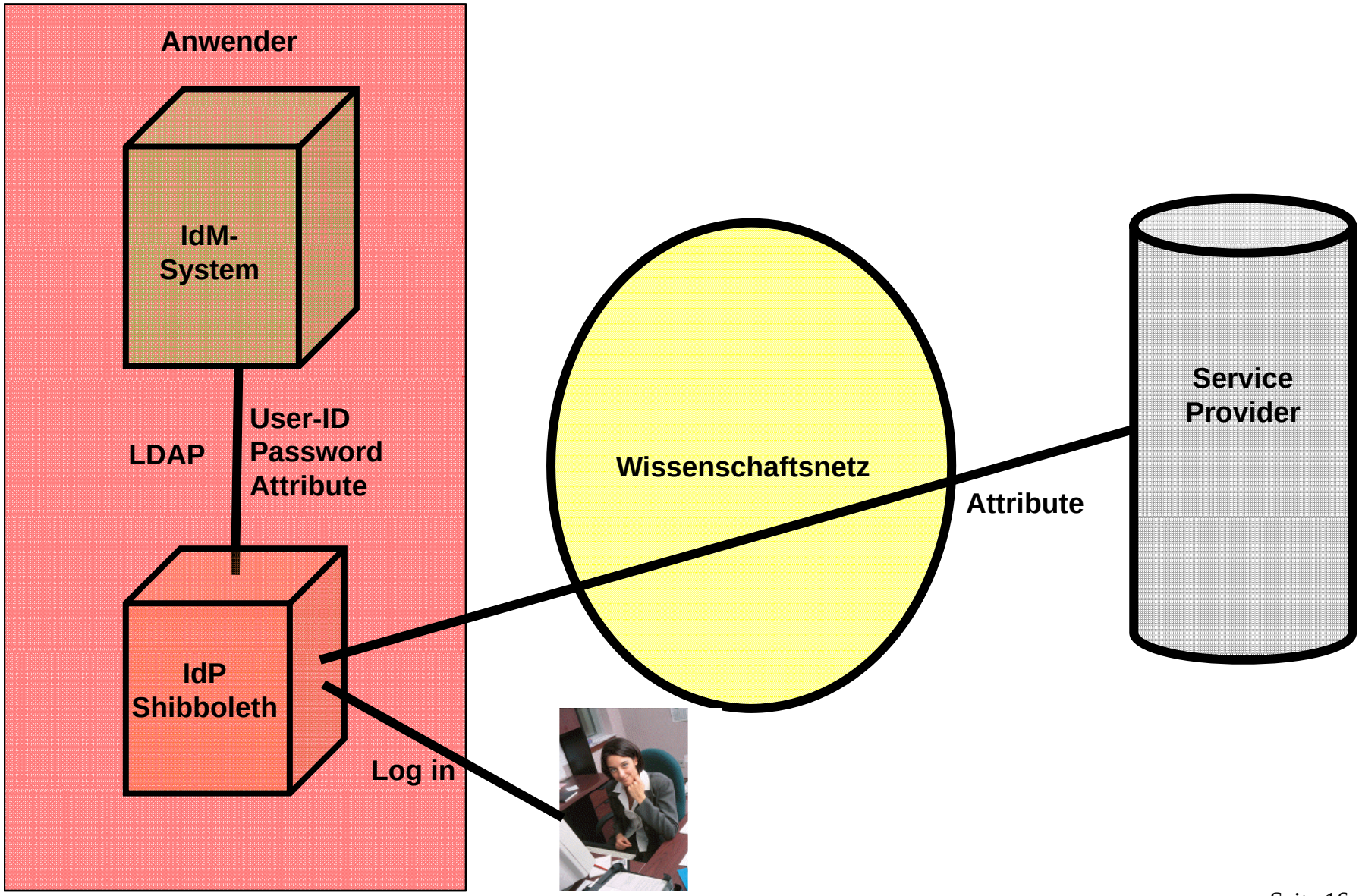
(8)

Ja

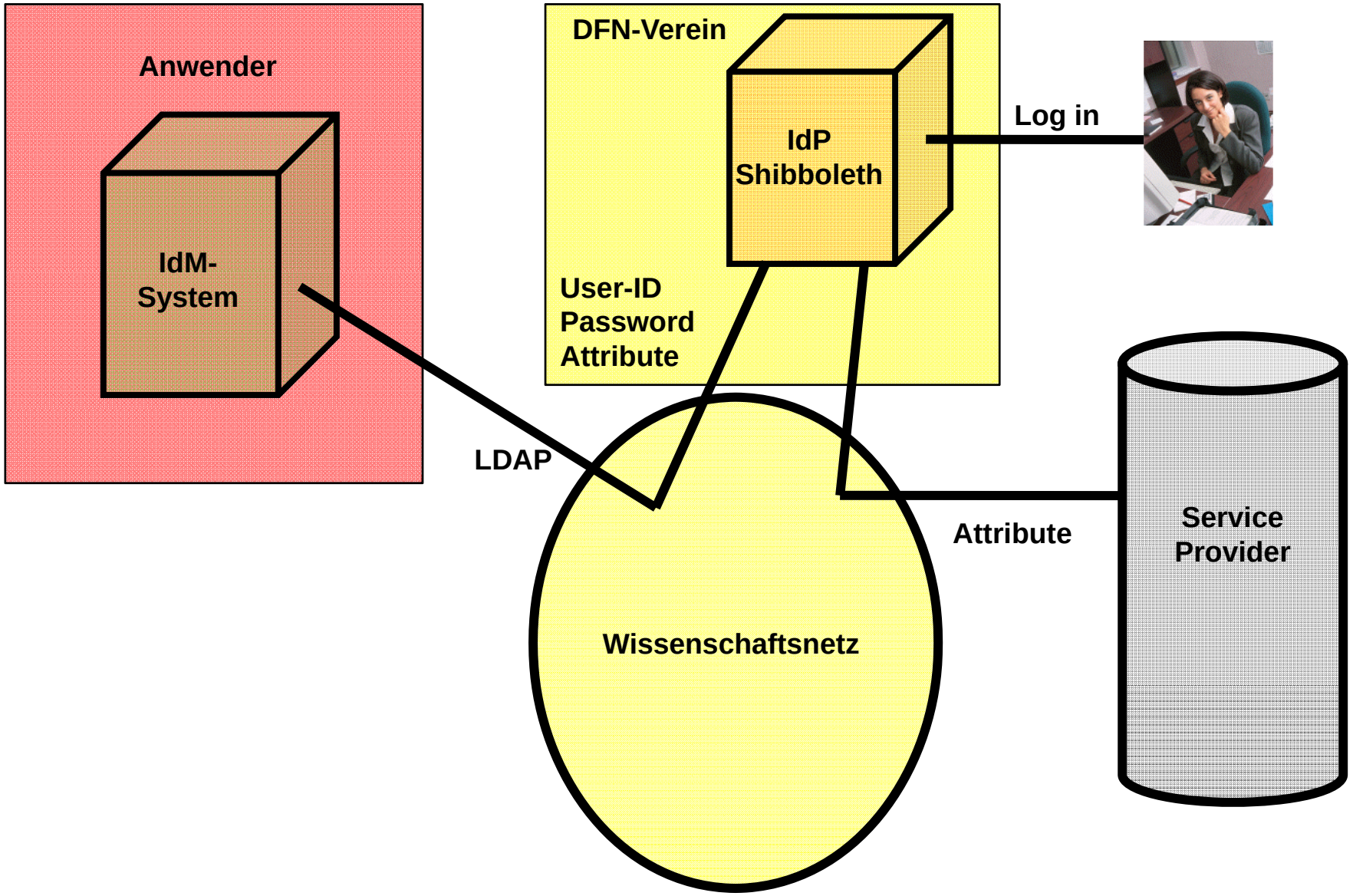
Nein

Zugriff

Interner IdP



Ausgelagerter IdP



Ausgelagerter IdP

- **Als Dienst des DFN-Vereins ab Herbst 2010 geplant**
- **Jedem Anwender wird ein eigener IdP zugeordnet.**
- **DFN-Verein konfiguriert mit Anwender den IdP.**
- **DFN-Verein stellt mit Anwender die Anbindung an das IdM des Anwenders her.**
- **DFN-Verein stellt Hochverfügbarkeit her.**
- **DFN-Verein verwendet immer aktuelle SW-Versionen.**
- **Vertragliche Regelung bzgl. Verarbeitung personenbezogener Daten muss getroffen werden.**

Vorteil für Anwender, insb. kleinere Einrichtungen:

Sie brauchen kein Shibboleth-Know-How.

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**

Nutzung von Zertifikaten

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!**

Aufwand für AAI-Teilnahme

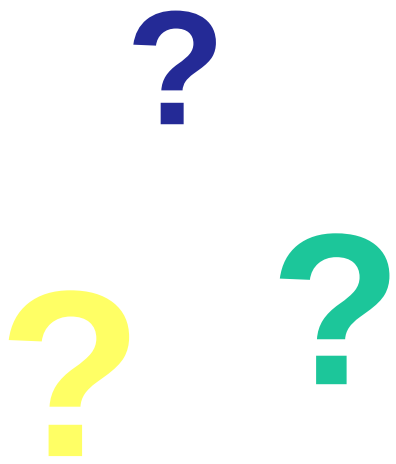
- **Voraussetzung:**
  verlässliches IdM-System
  „saubere“ Verwaltungsprozesse

- **kein zusätzliches Personal bei Auslagerung des IdPs notwendig**

- **keine zusätzliche Rechnertechnik bei Auslagerung des IdPs notwendig**

Fragen ...?

Vielen Dank!



aai@dfn.de