

Die Dienste der Föderation DFN-AAI

Ulrich Kähler, DFN-Verein
kaehler@dfn.de

- 1. Was ist die DFN-AAI ?**
- 2. Leistungen des DFN-Vereins**
- 3. Mitwirkung der Teilnehmer**
- 4. Klassen der Verlässlichkeit in der DFN-AAI**
- 5. Auslagerung des Shibboleth-IdPs in der DFN-AAI**
- 6. Attribute in der DFN-AAI**
- 7. Sicherheit in der DFN-AAI**
- 8. Rechtliche Aspekte der DFN-AAI**

1. Was ist die DFN-AAI ?

AAI

Authentifizierung
Autorisierung
Infrastruktur

- 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.

- **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

Bibliotheken und Verlage waren die treibende Kraft für den Aufbau der deutschen Föderation!

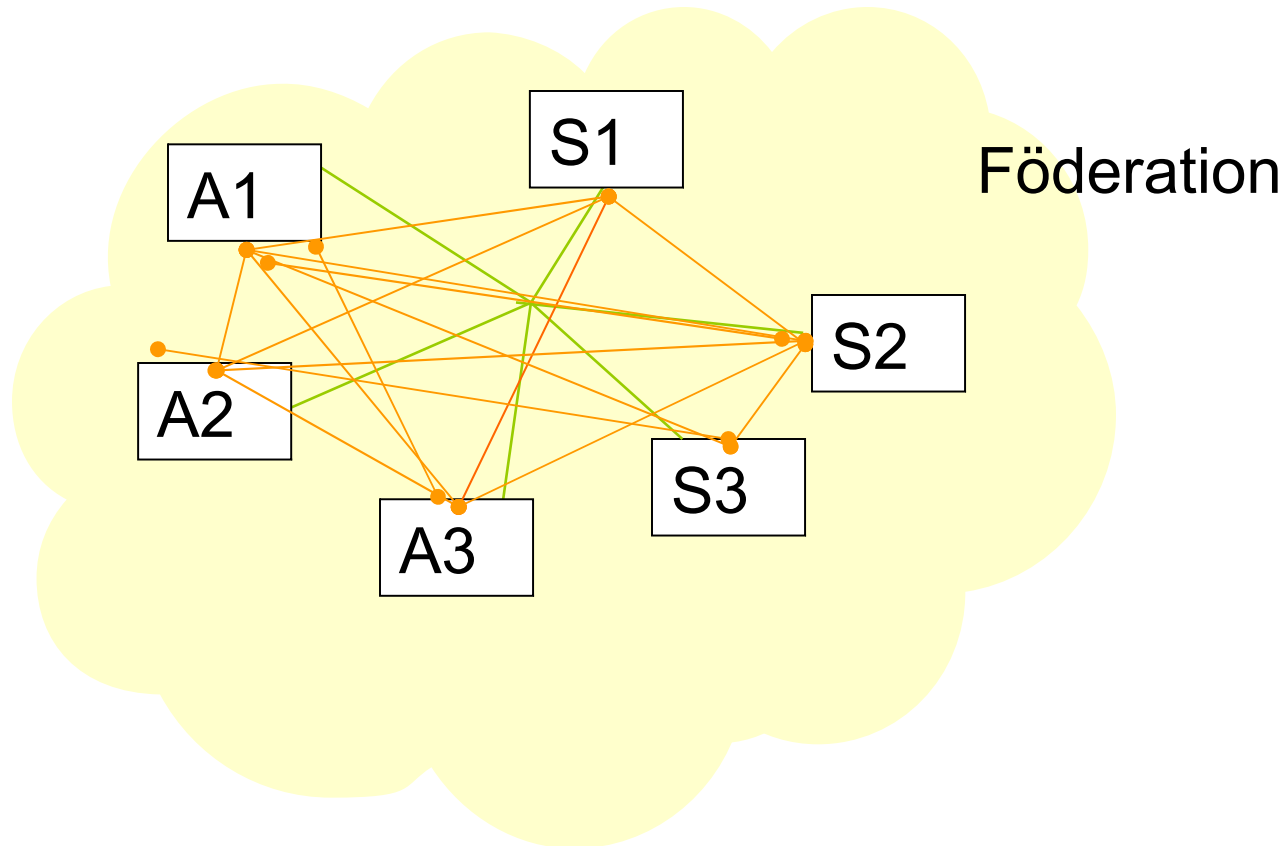
- **Status:**
z.Zt. ca. 60 Verträge unterschrieben:
Fachportal Bildung/FIS Bildung (DIPF), EBSCO, CSA
Illumina (ProQuest), OvidSP, ERL/WebSIRS (Ovid),
Munzinger, JSTOR, ScienceDirect (Elsevier),
Gale/Cengage Learning, Metapress mit 174 Verlagen,
Web of Science (Thomson), Uni Freiburg (REDI), HBZ
(Vascoda), Uni Göttingen (Nationallizenzen), ...

2. Leistungen des DFN-Vereins

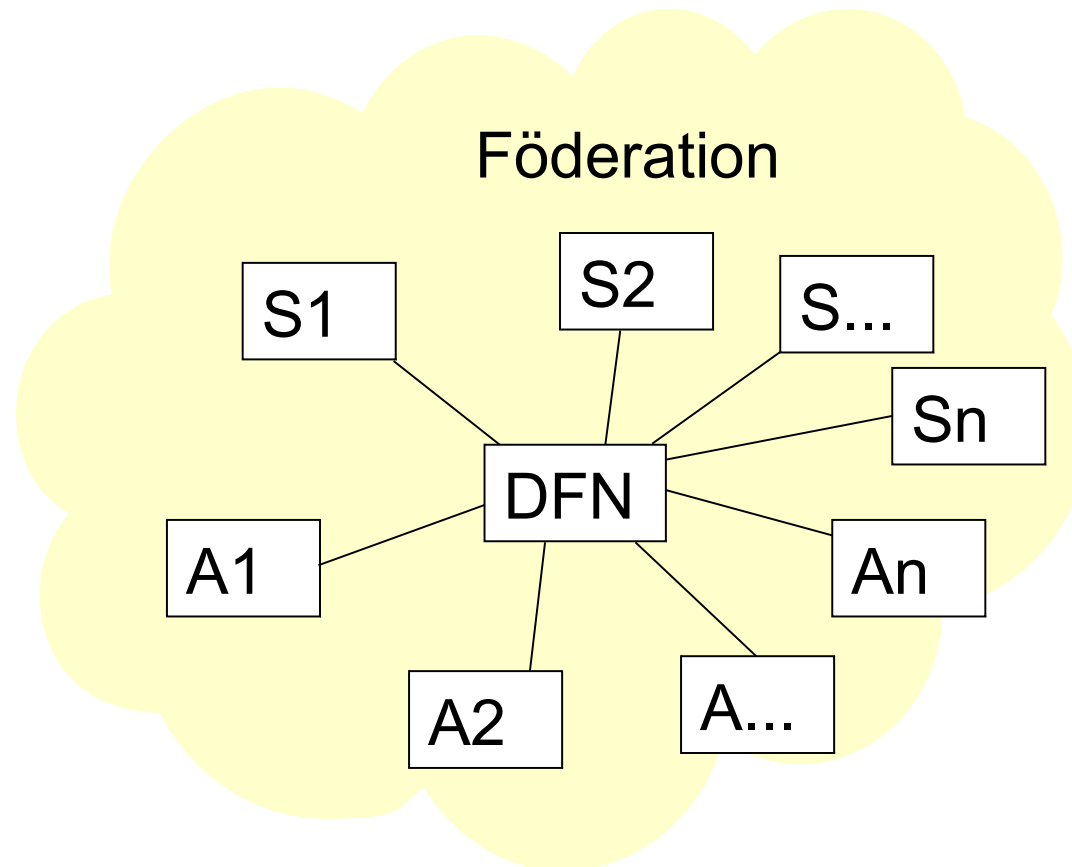
- **Betrieb der technischen Infrastruktur DFN-AAI**
- **Vertragspartner für Teilnehmer (insbesondere Hochschulen) und externe Anbieter (z.B. Verlage)**
- **Anpassung an neue Anwendungen**
 - **Verlage, Bibliotheken, e-Learning, Grids uvm.**
- **Organisieren der internationalen Einbettung**
- **Beratung und Schulung**
- **Fortgeschrittene Zertifikate über Dienst DFN-PKI**
- **Aber: DFN übernimmt NICHT den Abschluss von Lizenzverträgen (z.B. mit Verlagen)**

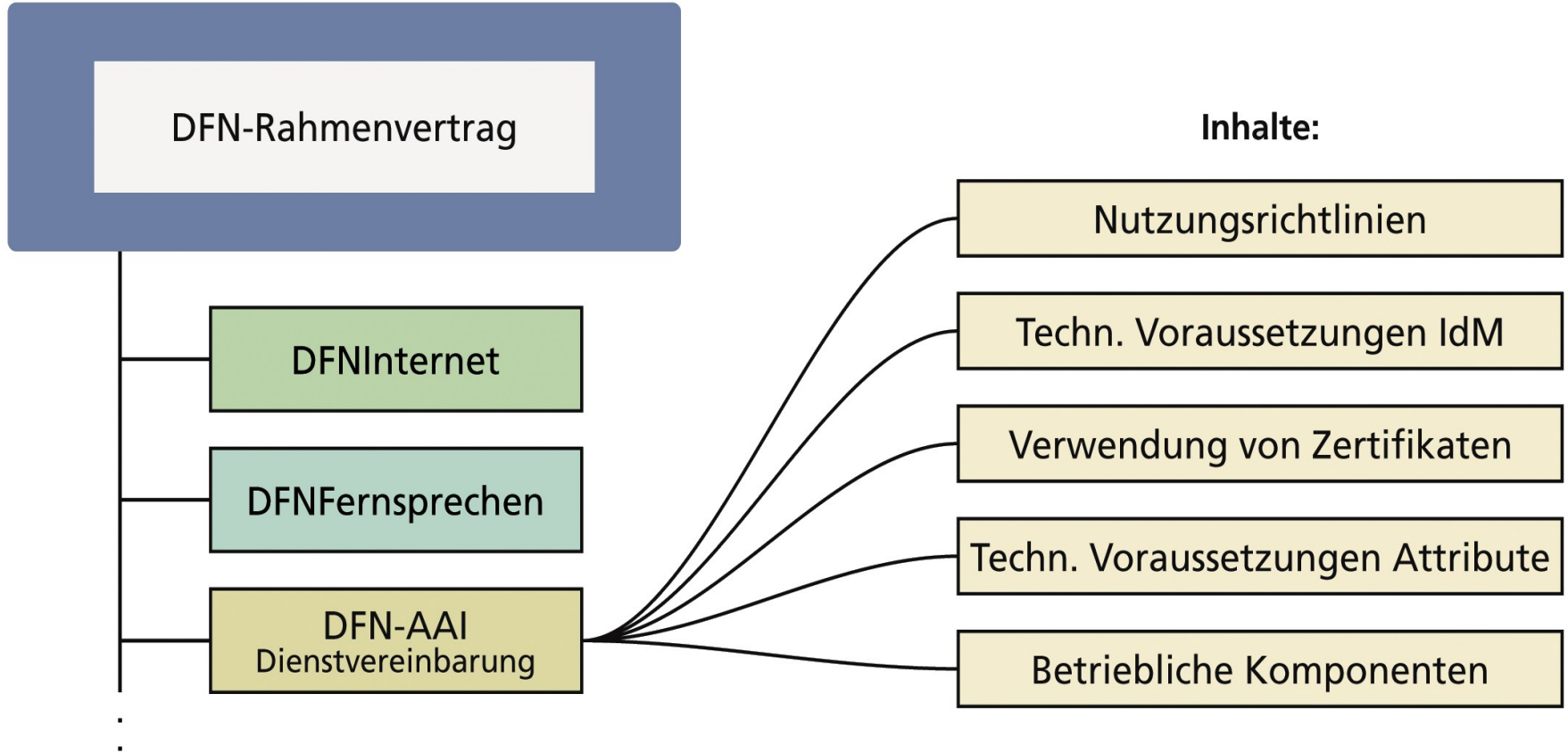
- **Administration von Metadaten**
- **Betrieb des WAYF-Servers/Discovery-Service**
- **Betrieb des Test-Systems**
- **Betrieb des Web-Portals**
- **Beratung, Weiterbildung:**
 - **Nutzer-Hotline**
 - **Shibboleth-Workshops**
 - **etc.**

Jeder Anbieter schließt mit jedem Anwender einen Vertrag ab.



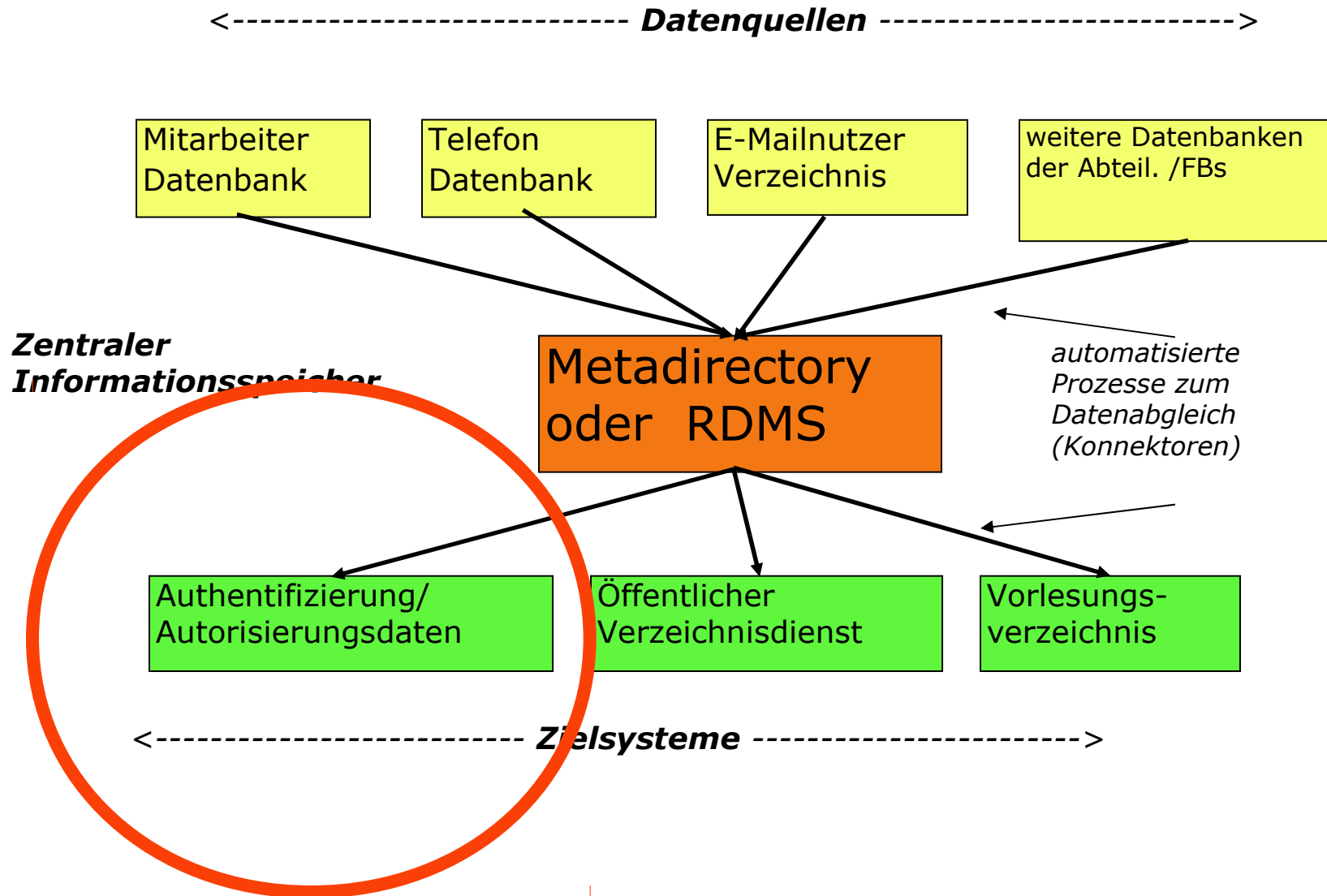
Der DFN-Verein als zentraler Vertragspartner für alle Teilnehmer der AAI.





3. Mitwirkung der Teilnehmer

- **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**



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.

4. Klassen der Verlässlichkeit in der DFN-AAI

- Hohe Ansprüche an IDM
 - Einige Anbieter von Ressourcen haben hohe Ansprüche an die Verlässlichkeit der Identifizierung (Verlage, e-Learning)
 - Darum müssen alle Teilnehmer an DFN-AAI anspruchsvolle Anforderungen an das Identity-Management (IDM) erfüllen
 - **Effekt:** Roll-out des Dienstes wird gebremst durch teilweise komplexe Aufgabe für die Teilnehmer, ihre Prozesse an ein hochwertig gepflegtes IdM anzupassen
- Erkenntnis aus dem jetzt ca. 2-jährigen Betrieb
 - Es gibt inzwischen auch Anbieter, die mit schwächeren Ansprüchen an die IdMs zufrieden wären
 - Die gegenwärtigen Regeln der DFN-AAI verwehrt aber Teilnehmern mit schwächer gepflegten IdMs die Teilnahme
- Wie lässt sich diese Situation ändern?

- Einführung von **drei Klassen der Verlässlichkeit** mit verschiedenen Anforderungen an die IdM der Teilnehmer
 - **Test**: Keine Anforderungen an die IdMs
 - **Basic**: Schwächere Anforderungen an die IdMs
 - **Advanced**: Heutige Anforderungen an die IdMs
- Anbieter und Teilnehmer stufen sich im Sinne einer Konformitätserklärung selbst diesen Klassen zu
 - Anbieter können in eigener Verantwortung ihre Ressourcen in einer oder mehreren Klassen zur Verfügung stellen
 - Teilnehmer stufen sich in einer Klasse ein und können auf alle Ressourcen zugreifen, die von den Anbietern zugeordnet werden
- Erwünschtes Ergebnis: Nutzbarkeit des Dienstes stärken und damit auch Roll-out des Dienstes befördern

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

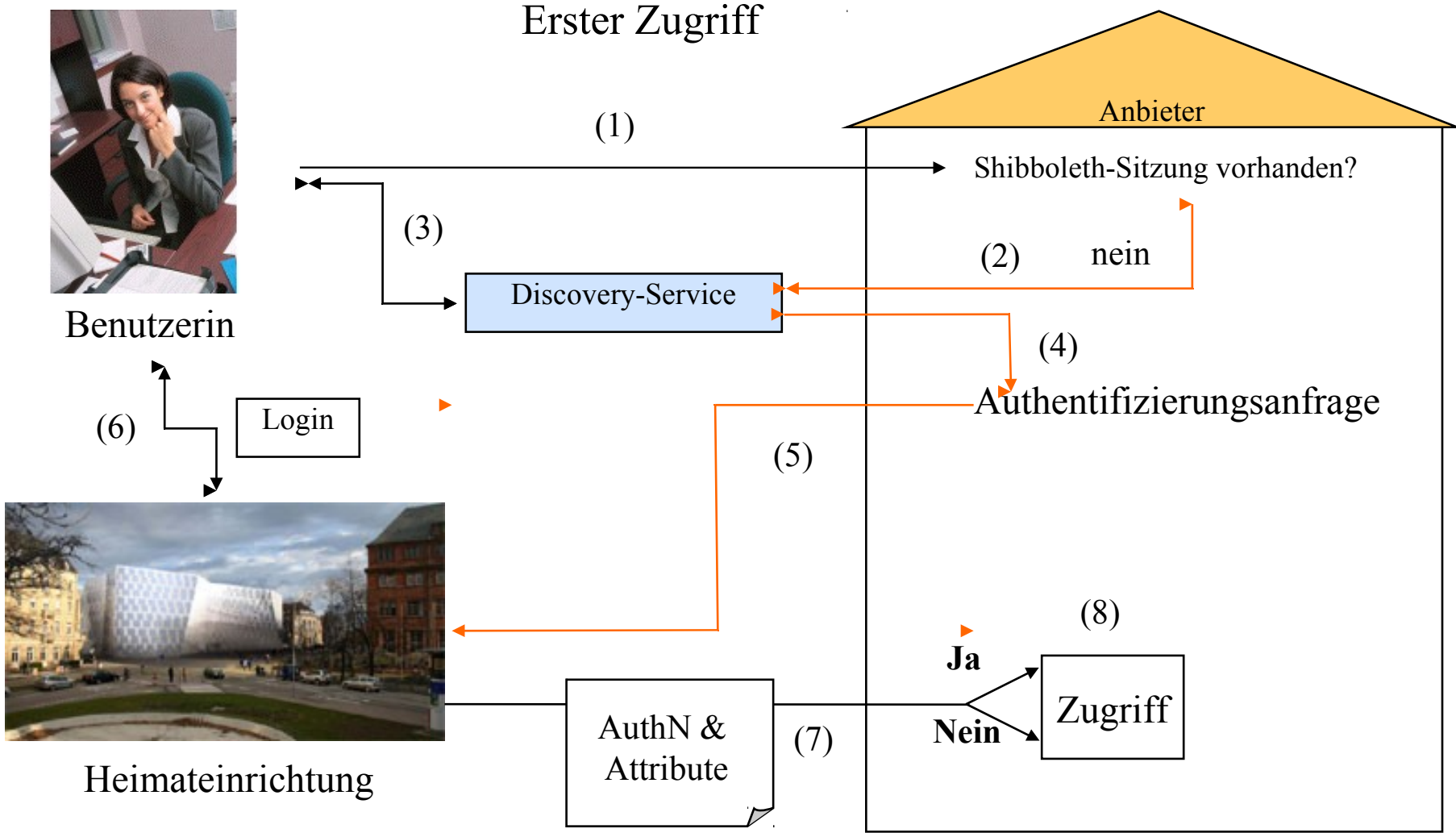
- **Wunschlösung:**
Einführung eines Attributes „Verlässlichkeit“
ist im internationalen Kontext möglich,
aber nicht kurzfristig (2-3 Jahre) möglich.
- **Plan B:**
DFN-Föderation mit der Verlässlichkeitsstufen
 - basic und
 - advanced
 - (undefined entspricht der Testföderation)

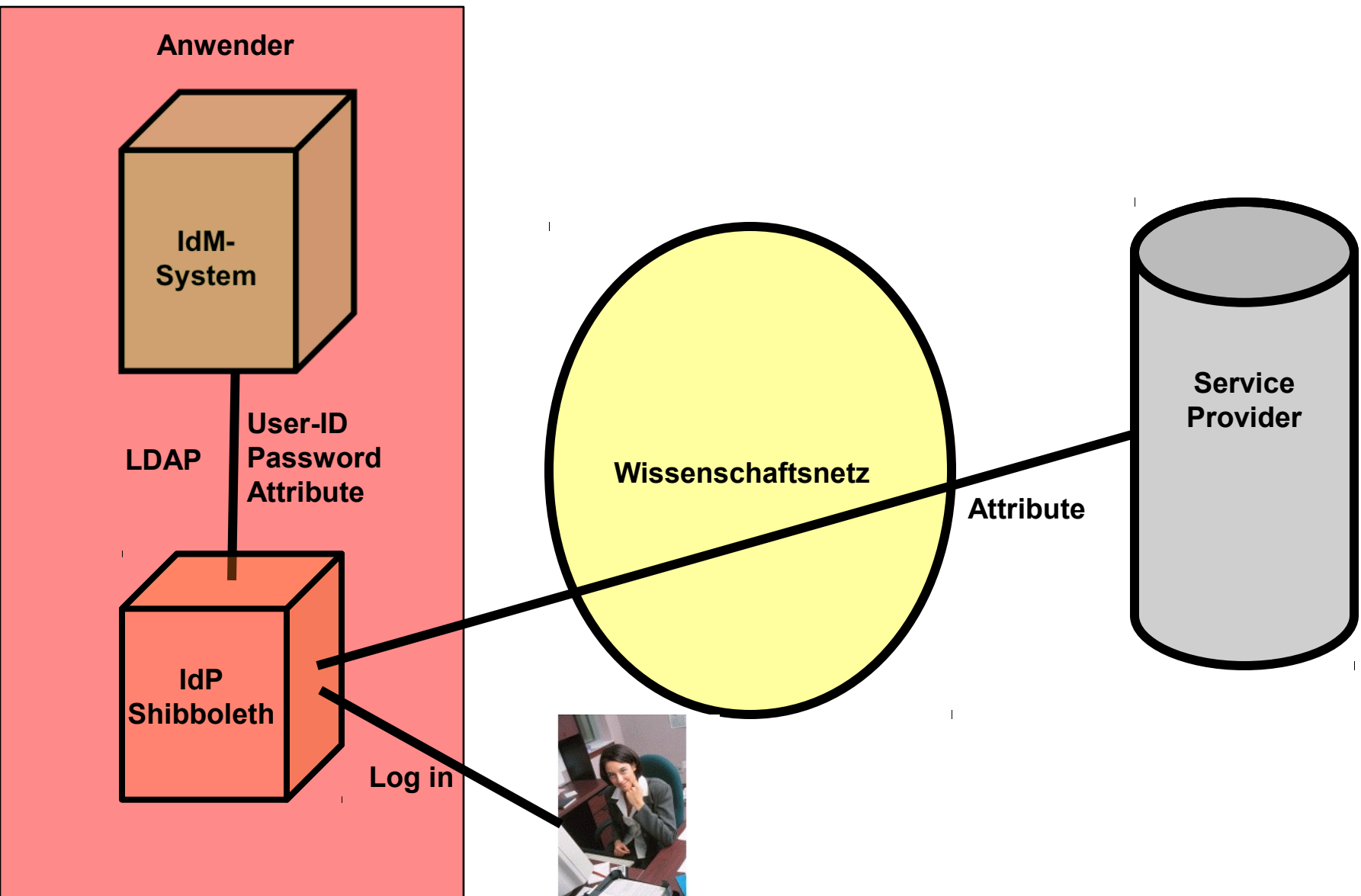
Ist umgesetzt in neuer Version der Metadatenverwaltung.

5. Auslagerung des Shibboleth-IdPs in der DFN-AAI

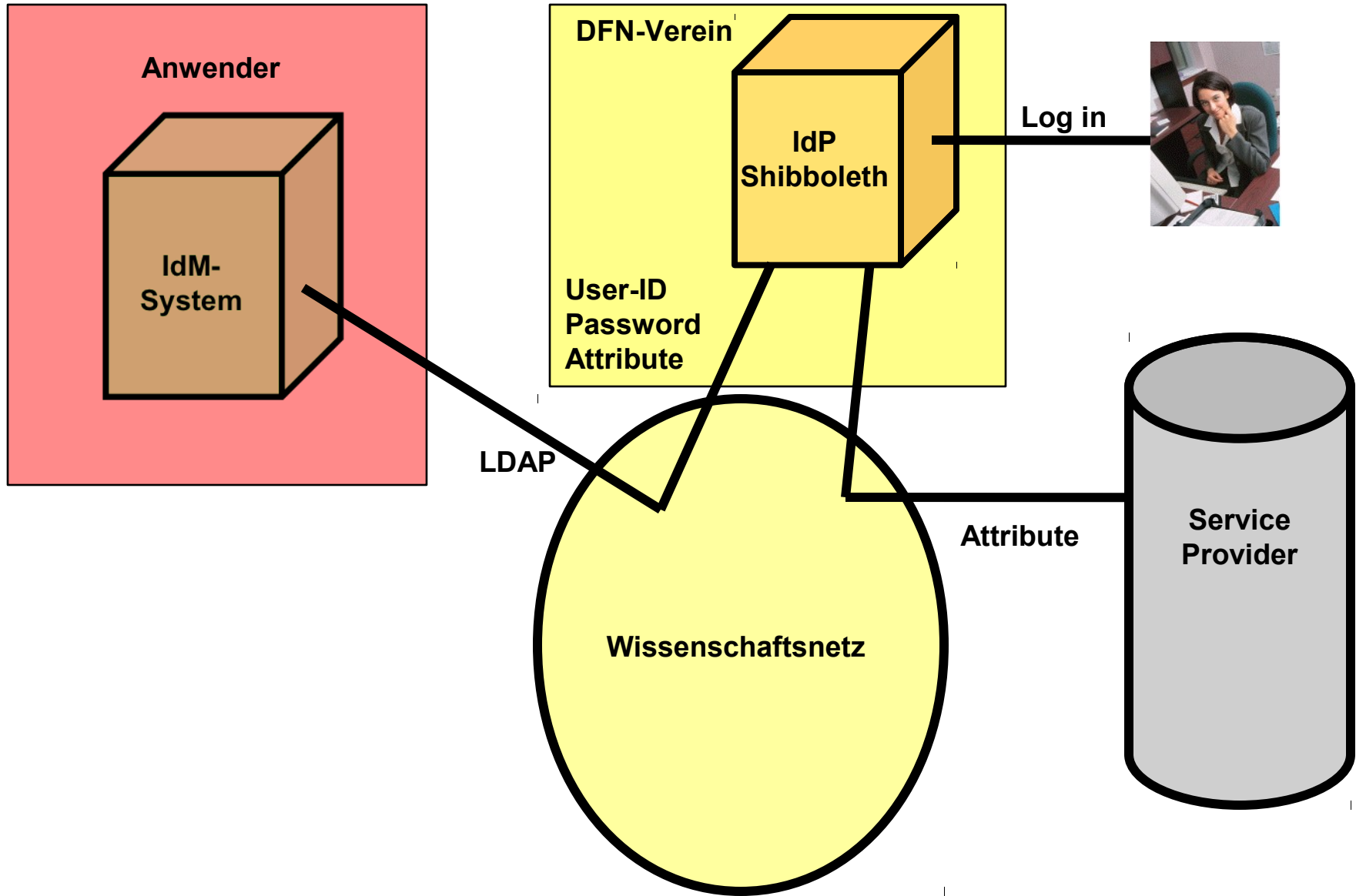
- **Unterschriebene Verträge: ca. 120
davon Service Provider: ca. 60
und Identity Provider: ca. 60**
- **Im Test:
ca. 200 Einrichtungen**
- **Verdoppelung gegenüber Vorjahr**
- **Baden-Württemberg (Uni Freiburg) hat fast
komplett auf DFN-AAI umgestellt.
Fast!
Was fehlt?**

Wie funktioniert Shibboleth?

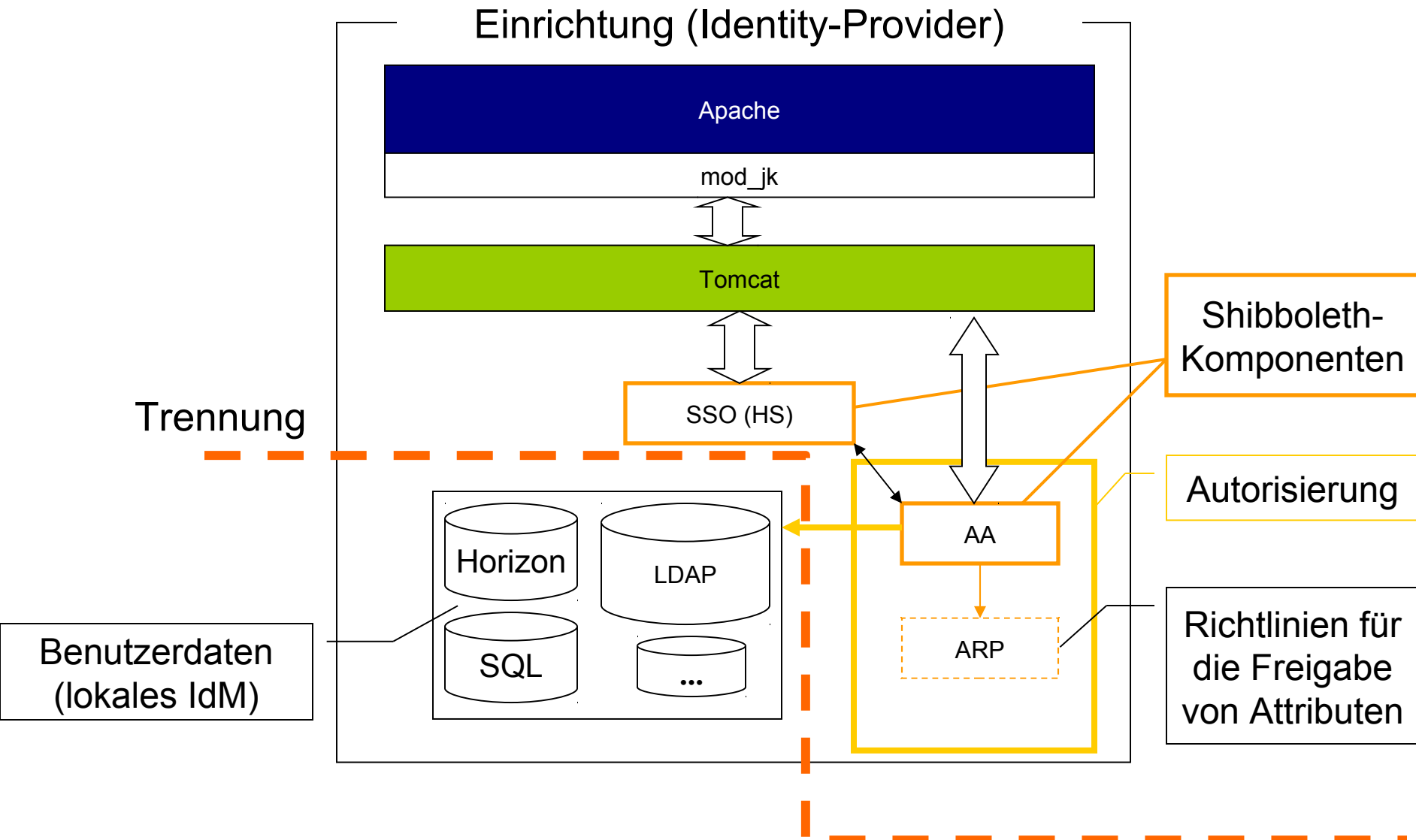




Ausgelagerter IdP



Identity-Provider Architektur



- **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:
Er braucht kein Shibboleth-Know-How.**

6. Attribute in der DFN-AAI

- 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.

- **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 Committee (SCHAC)**
 - Geburtsdatum (schacDateOfBirth)
 - Geschlecht (schacGender)
 - Matrikelnummer (schacPersonalUniqueCode)

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

7. Sicherheit in der DFN-AAI

- **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

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!

8. Rechtliche Aspekte der DFN-AAI

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

- **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**

- 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 ...

Password ...

- **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!**

Vielen Dank!



aai@dfn.de