12. Shibboleth-Workshop

23. Mai 2012
Universität Kaiserslautern

Raoul Borenius, DFN-Verein
Wolfgang Pempe,DFN-Verein
Bernd Oberknapp, Universität Freiburg
Ulrich Kähler, DFN-Verein

Tagesordnung

DFN Deutsches Forschungsnetz

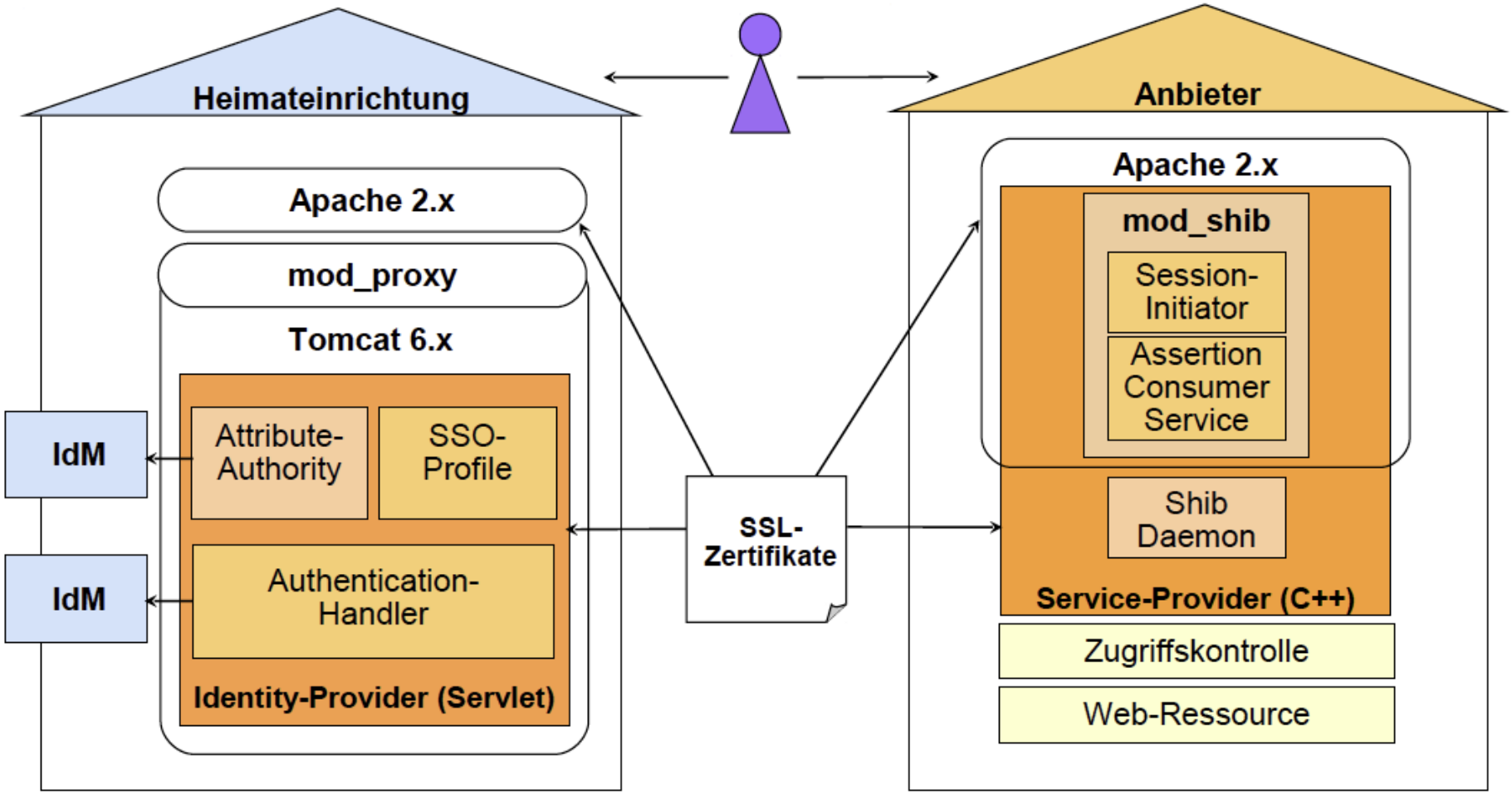
12. Shibboleth-Workshop

23. Mai 2012, Universität Kaiserslautern

11:00 Uhr	Begrüßung, Übersicht, Aktuelles, Verlässlichkeitsklassen	Ulrich Kähler, DFN-Verein
11:30 Uhr	Pflege und Aktualisierung eines Shibboleth-Identity Providers	Wolfgang Pempe, DFN-Verein
13:00 Uhr	Mittagspause	
14:00 Uhr	Anwendungen schützen mit dem Shibboleth Service Provider	Bernd Oberknapp, Universität Freiburg
15:30 Uhr	Shibboleth-Attribut-Management	Raoul Borenius, DFN-Verein
16:30 Uhr	Abschlussdiskussion	alle
17:00 Uhr	Ende	

Shibboleth-Architektur

DFN Deutsches Forschungsnetz



Was ist DFN-AAI?

- DFN-AAI ist ein **regulärer Dienst** des DFN-Vereins.
  (keine Extrakosten, enthalten in Internet-Dienstentgelten)

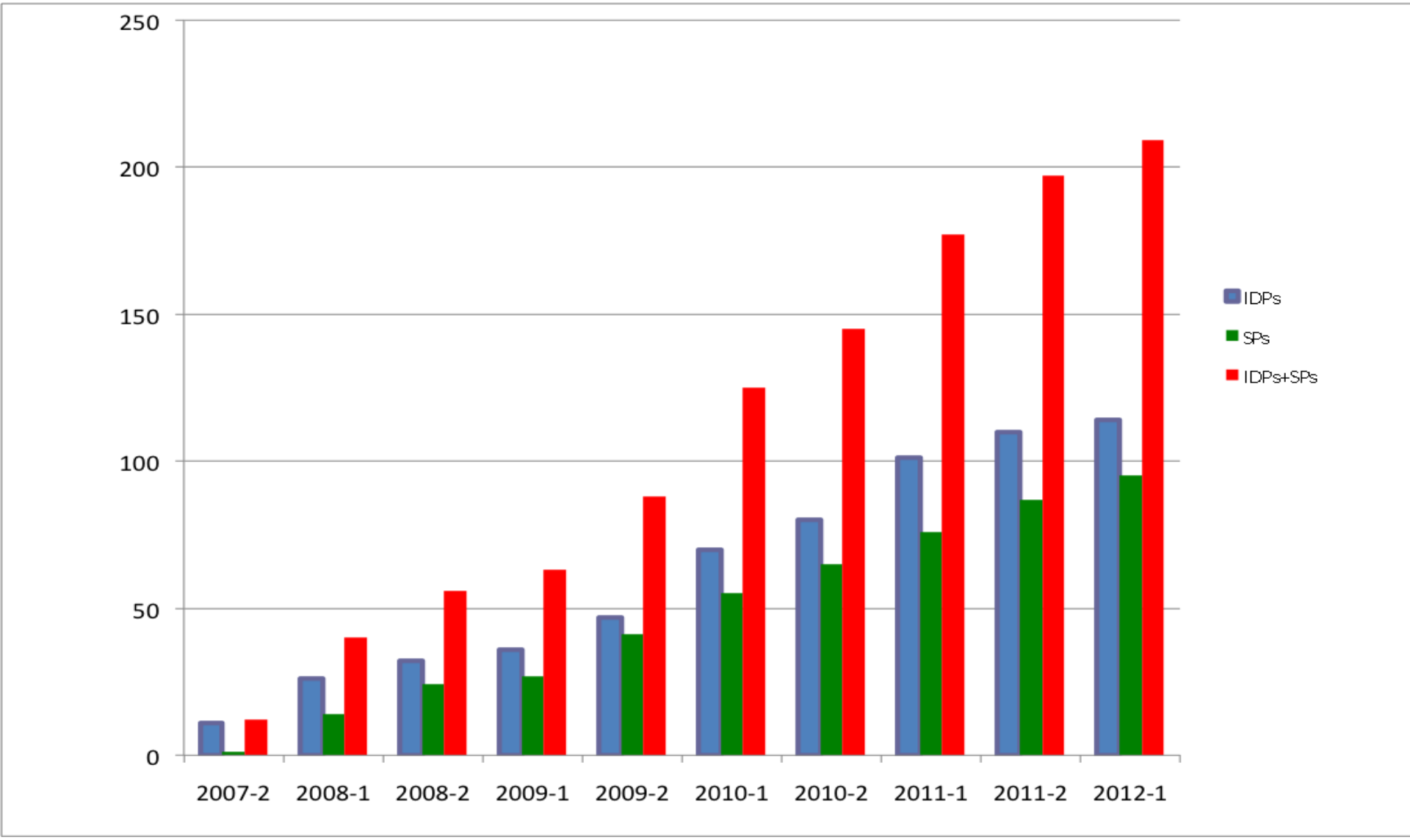
- DFN-AAI schafft
  - den **organisatorisch / technischen Rahmen** für den Austausch von Nutzerinformationen,
  - das notwendige **Vertrauensverhältnis** zwischen den Anwendern und den Anbietern

- 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.

Entwicklung AAI-Verträge

DFN
Deutsches Forschungsnetz



Anwendungen

- **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
  - Gigamove
  - DFN-VC, DFN-MailSupport

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**

Erfahrungen

- 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 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?

Antwort

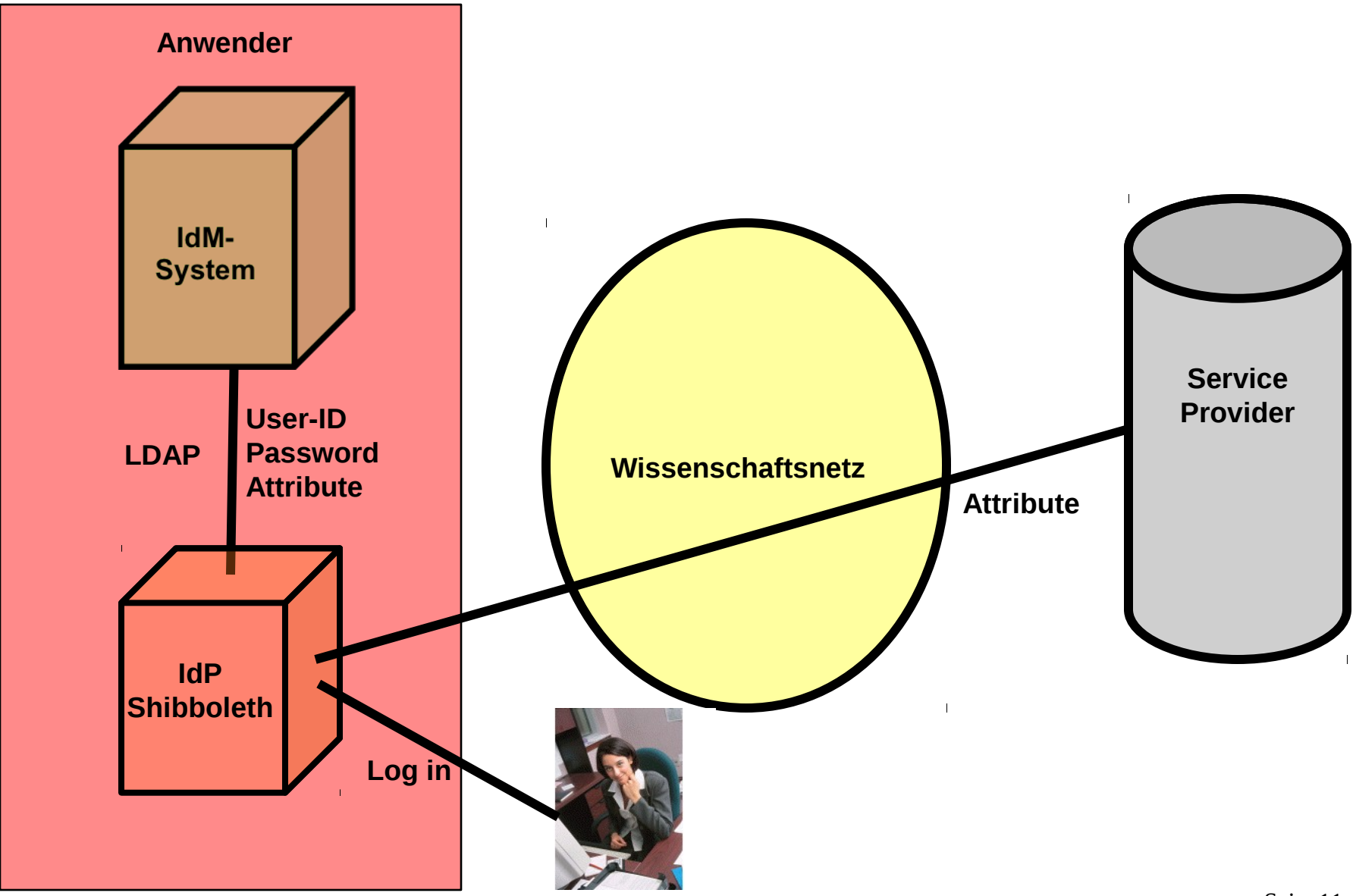
- Einführung von **drei Klassen der Verlässlichkeit** mit verschiedenen Anforderungen an die IdM der Teilnehmer
  - **Test**: Keine Anforderungen an die IdMs
  - **Basic**: Schwächere Anforderungen an die IdMs
  - **Advanced**: Heutige Anforderungen an die IdMs
- Anbieter und Teilnehmer stufen sich im 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

Verlässlichkeitsklassen

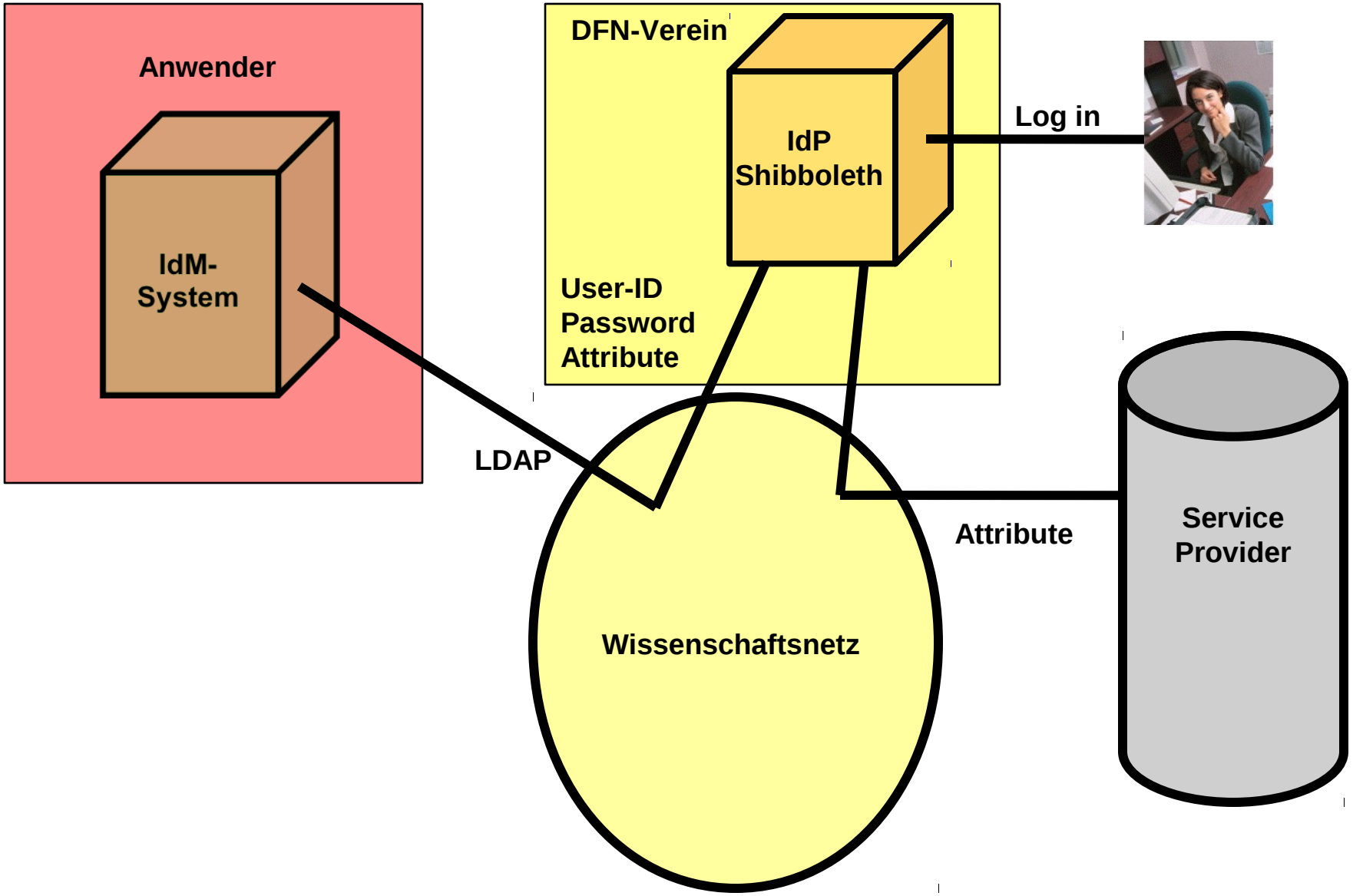
DFN Deutsches Forschungsnetz

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

Interner IdP



Ausgelagerter IdP



Ausgelagerter IdP

- **Dienst des DFN-Vereins**

- **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.

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.

Attributauswahl für E-Learning

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

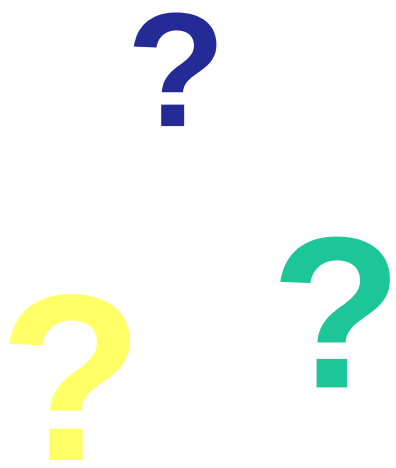
Attribute zum Studiengang

- **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

Fragen ...?

DFN
Deutsches Forschungsnetz

Vielen Dank!



aai@dfn.de