DFN-AAI

LoA und ausgelagerter IdP

Ulrich Kähler

DFN
Deutsches Forschungsnetz

Klassen der Verlässlichkeit in der DFN-AAI

Gegenwärtige Lage 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?

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

Realisierung

- **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.

DFN-AAI-Dienstvereinbarung

1 Leistungen des DFN-Vereins

...

Der DFN-Verein koordiniert in Rücksprache mit den Teilnehmern und Anbietern die Modalitäten und Richtlinien für die Kommunikation innerhalb der DFN-AAI und passt sie dem technischen Fortschritt an, insbesondere durch:

- Empfehlungen zur Verwendung von Attributen zur Autorisierung von Nutzern,
- Veröffentlichung der Empfehlungen von Attributen, z.B. auf seinen WWW-Seiten,
- Festlegung von Mindestanforderungen an die zu verwendenden Software-Versionen und Veröffentlichung der Mindestanforderungen, z.B. auf seinen WWW-Seiten,
- **Festlegung von Klassen der Verlässlichkeit bei der Authentifizierung in der DFN-AAI,**
- Festlegung von Kriterien zur Verwendung von Zertifikaten,
- Festlegung der betrieblichen Abläufe.

DFN-AAI-Dienstvereinbarung

2 Mitwirkung des Teilnehmers

ALT:
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.

NEU:
Der Teilnehmer betreibt ein System zur Nutzerverwaltung und stellt sicher, dass seinen Nutzern Attribute zugeordnet werden.
Der Teilnehmer legt fest, welcher Klasse der DFN-AAI (vgl. Festlegung von Klassen der Verlässlichkeit bei der Authentifizierung in der DFN-AAI) er zugeordnet werden soll und stellt die damit verbundenen Mindestanforderungen sicher.

Teilnehmer

- **Unterschriebene Verträge: 113**
  davon Service Provider: 60
  und Identity Provider: 53

- **Im Test:**
  ca. 200 Einrichtungen

- **Verdoppelung gegenüber Vorjahr**

- **Baden-Württemberg (Uni Freiburg) hat fast komplett auf DFN-AAI umgestellt.**

  Fast!

  Was fehlt?

DFN Deutsches Forschungsnetz

Auslagerung des Shibboleth-IdPs in der DFN-AAI

Wie funktioniert DFN-AAI?

Benutzerin

Anbieter

(1)

Shibboleth-Sitzung vorhanden?

(3)

(2) nein

Discovery-Service

(4)

Authentifizierungsanfrage

(6)

Login

(5)

Heimateinrichtung

(8)

Ja

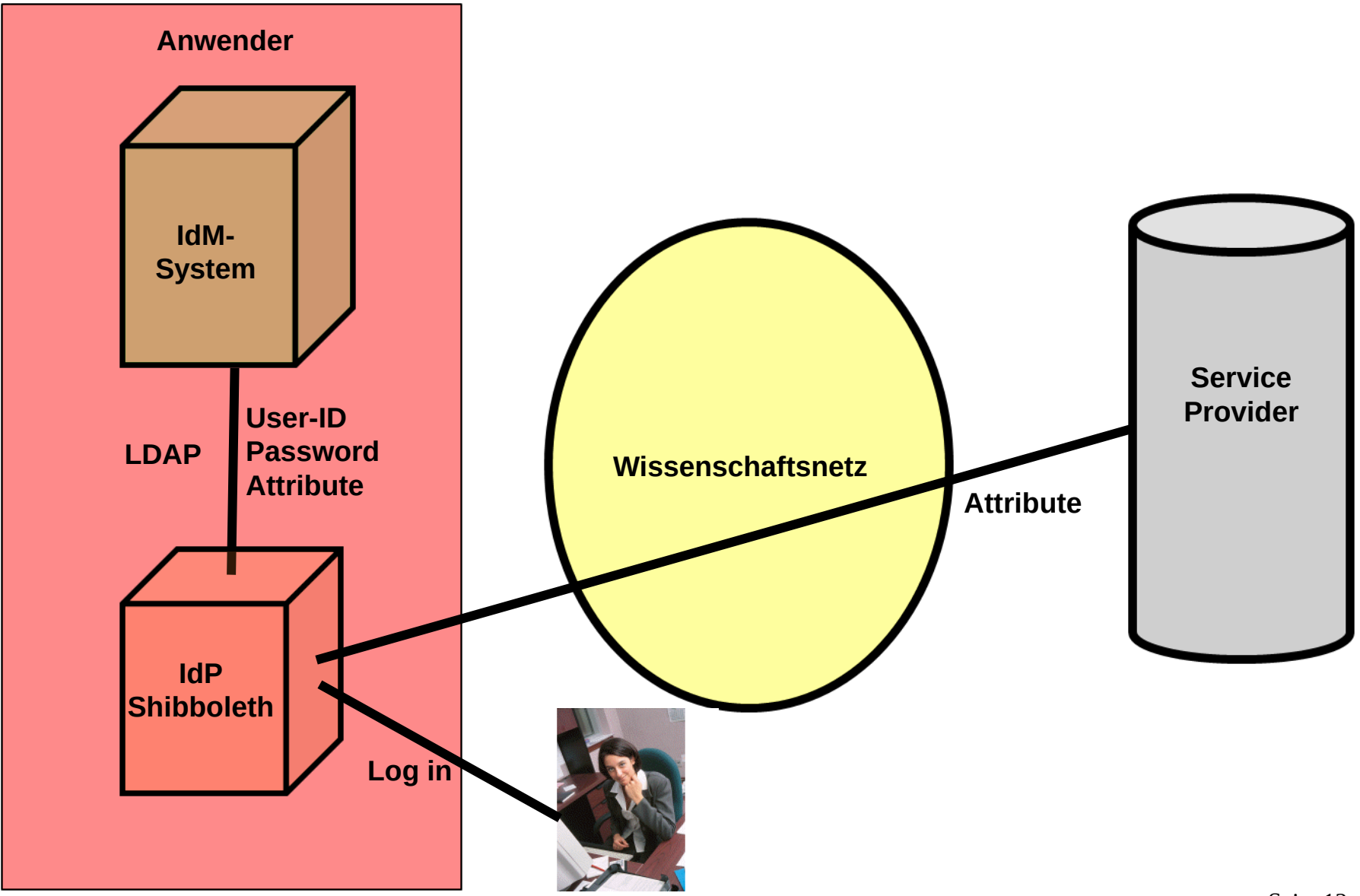
Zugriff

Nein

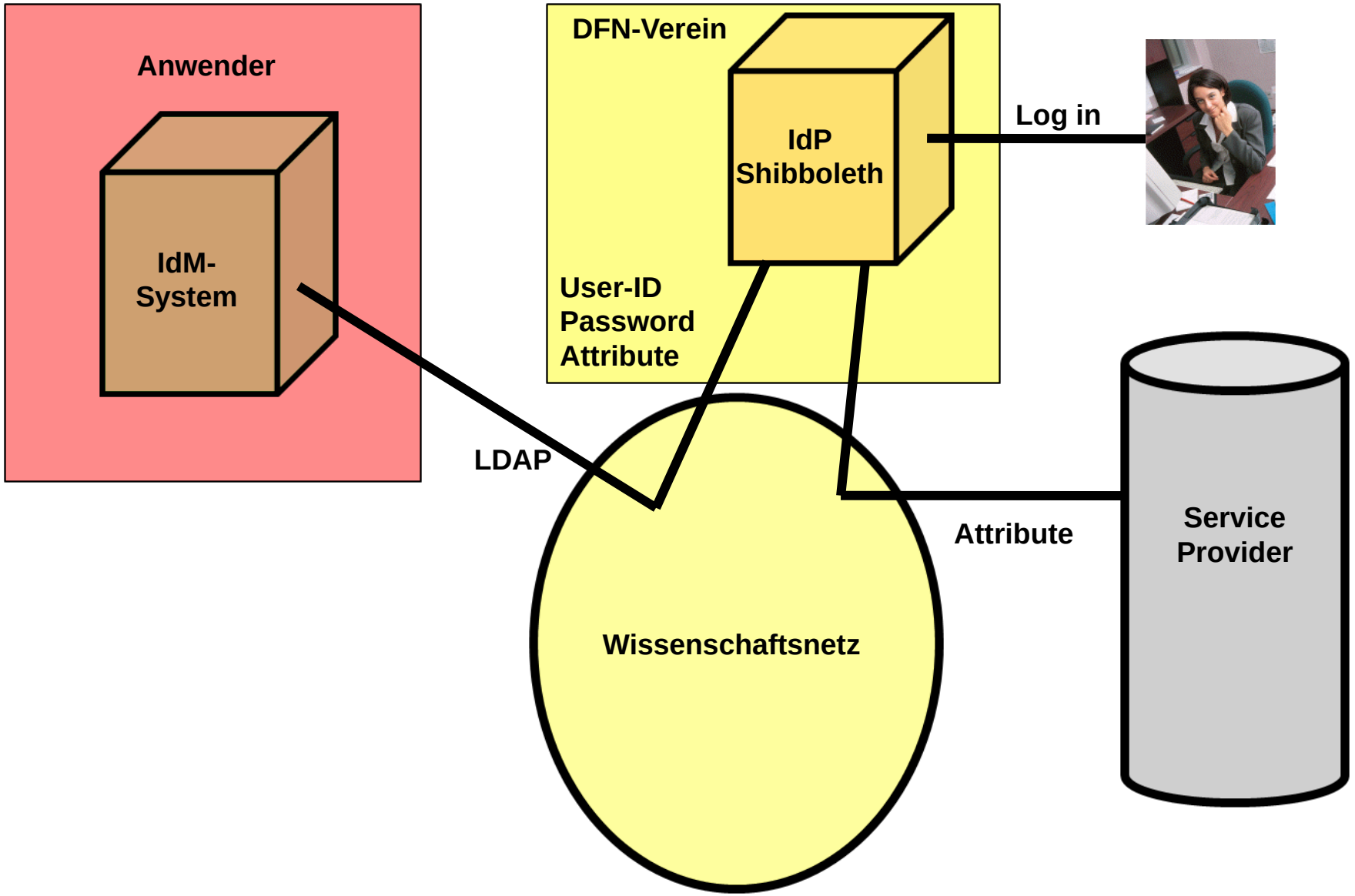
AuthN & Attribute

(7)

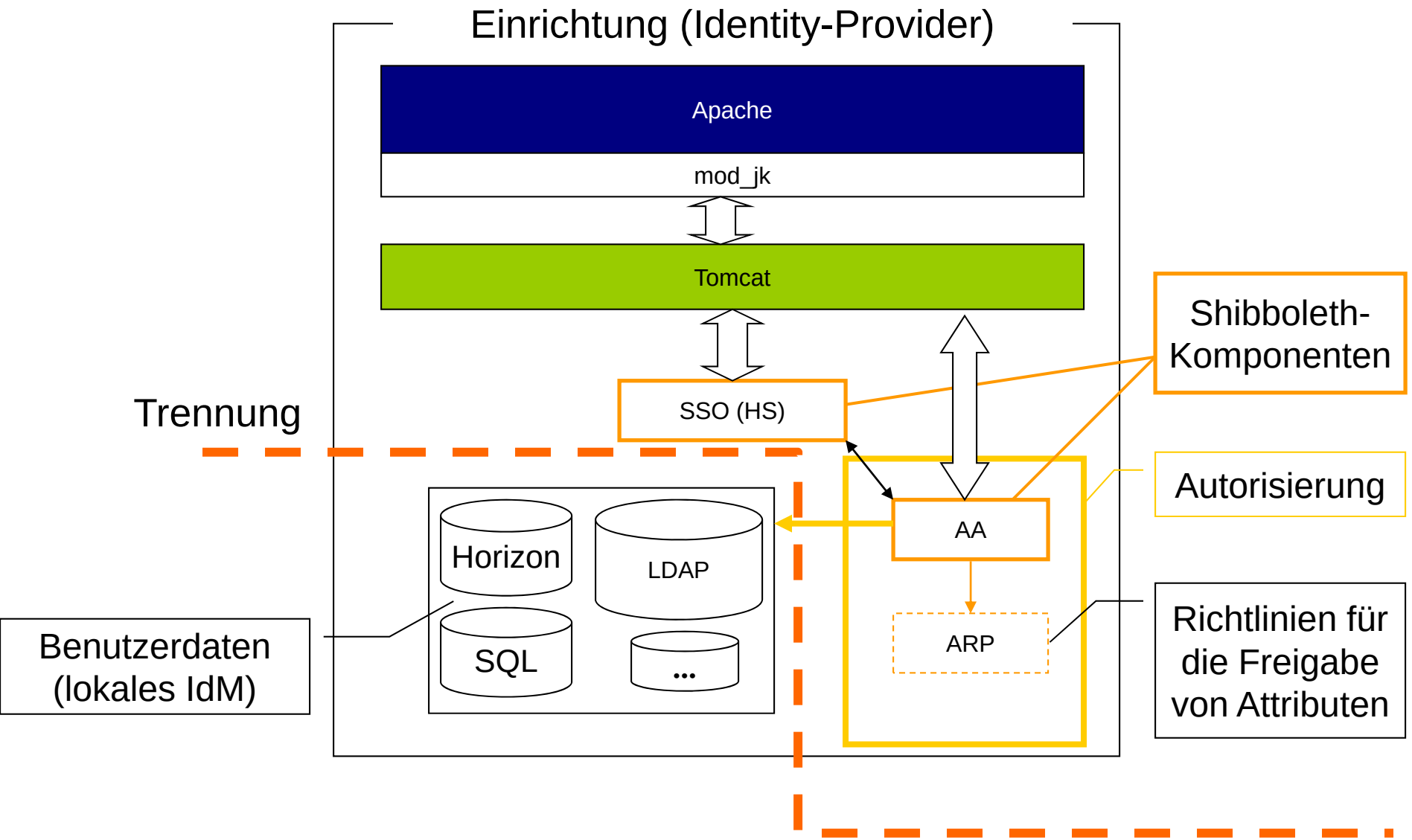
Interner IdP



Ausgelagerter IdP



Identity-Provider Architektur



Ausgelagerter IdP

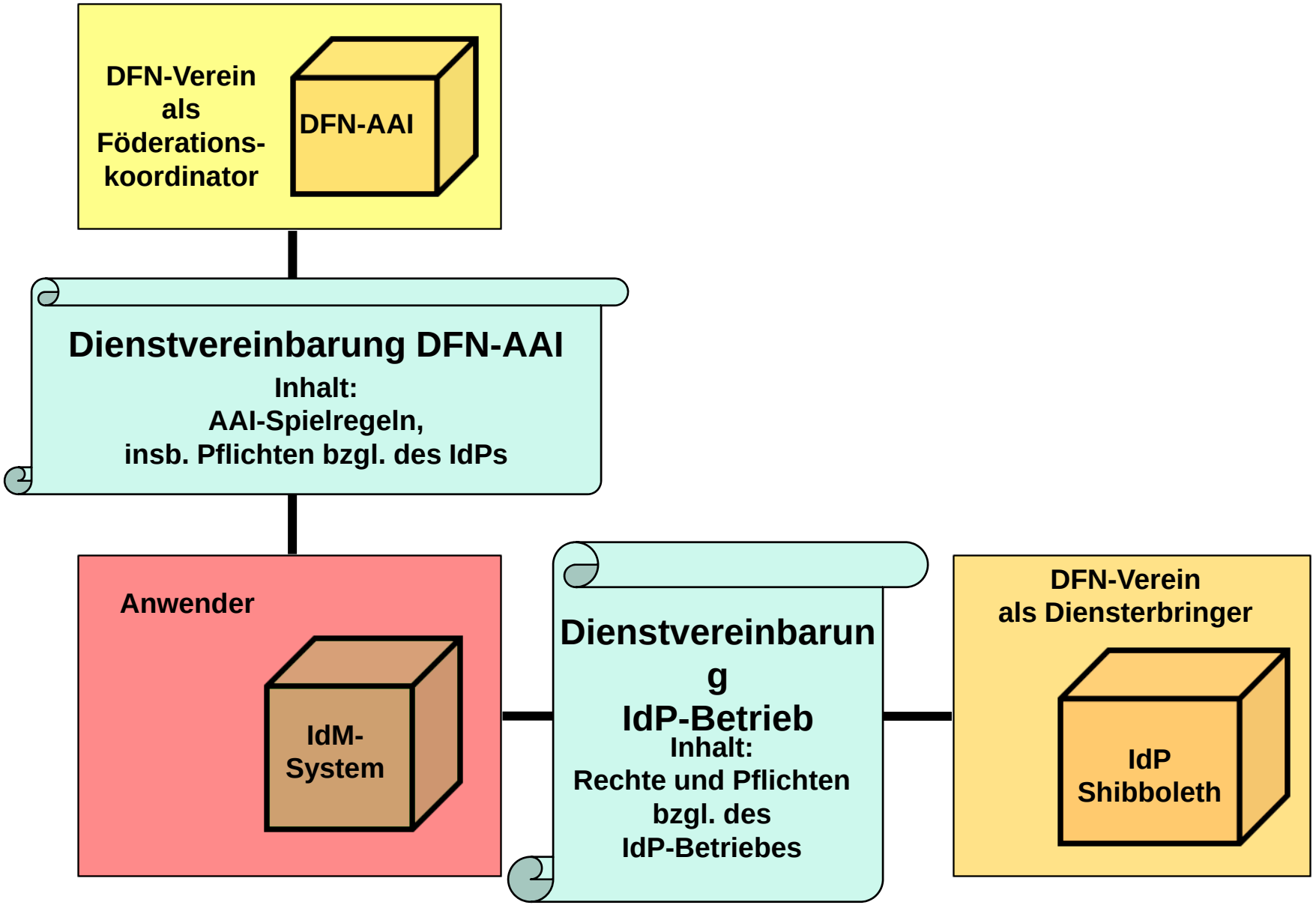
- **Dienst des DFN-Vereins ab Sommer 2010 geplant**

- **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.

Vertragsgestaltung



Vertragsgestaltung

DFN Deutsches Forschungsnetz

Vertragsgegenstände:

- Zusammenarbeit bei der Anbindung an das IdM des Anwenders
- Konfigurierung des Shibboleth-IdPs
- SLAs für IdP-Betrieb
- Datenschutzregelungen

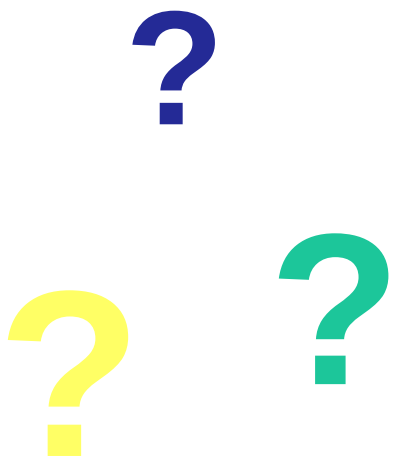
Offene Fragen:

- IdP-Vertrag nur als Ergänzung zur AAI-Dienstvereinbarung?
- Entgelt?
- Haftung, Gewährleistung wie im Rahmenvertrag?

Fragen ...?

Deutsches Forschungsnetz

Vielen Dank!



aai@dfn.de