

# Aufbau einer AAI im DFN

Ulrich Kähler, DFN-Verein  
kaehler@dfn.de

- Physiker aus unterschiedlichen Hochschulen sollen auf einen gemeinsamen Datenbestand zugreifen.
- Mitarbeiter und Studierende einer Hochschule sollen im Rahmen einer speziellen Lizenzvereinbarung auf Fachinformationen zugreifen.  
(z.B. DFG-Nationallizenz)
- Ein von SAP bereitgestelltes eLearning-System soll von BWL-Studenten ausgewählter Hochschulen genutzt werden können.

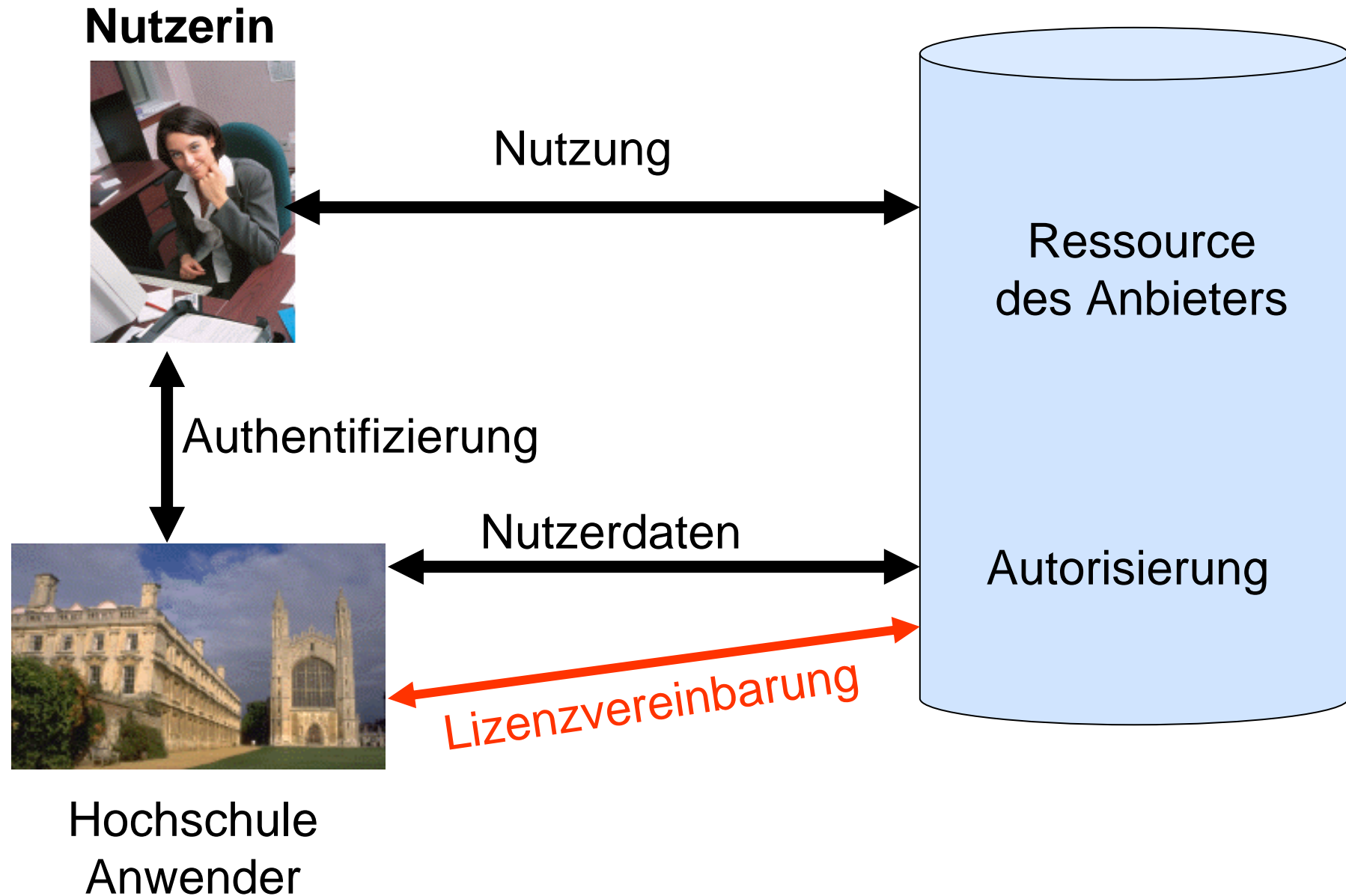
## Verbesserung und Vereinfachung des Zugriffs auf geschützte Ressourcen von Anbietern

- **Nutzer:** Zugriff unabhängig vom Ort und dem Zugriffsweg, Zugriff auf mehrere Anbieter nach nur einmaliger Authentifizierung (Single Sign-on)
- **Anbieter:** Schutz vor unberechtigtem Zugriff, möglichst geringer Aufwand
- **Anwender:** Gewährung berechtigten Zugriffs, möglichst geringer Aufwand

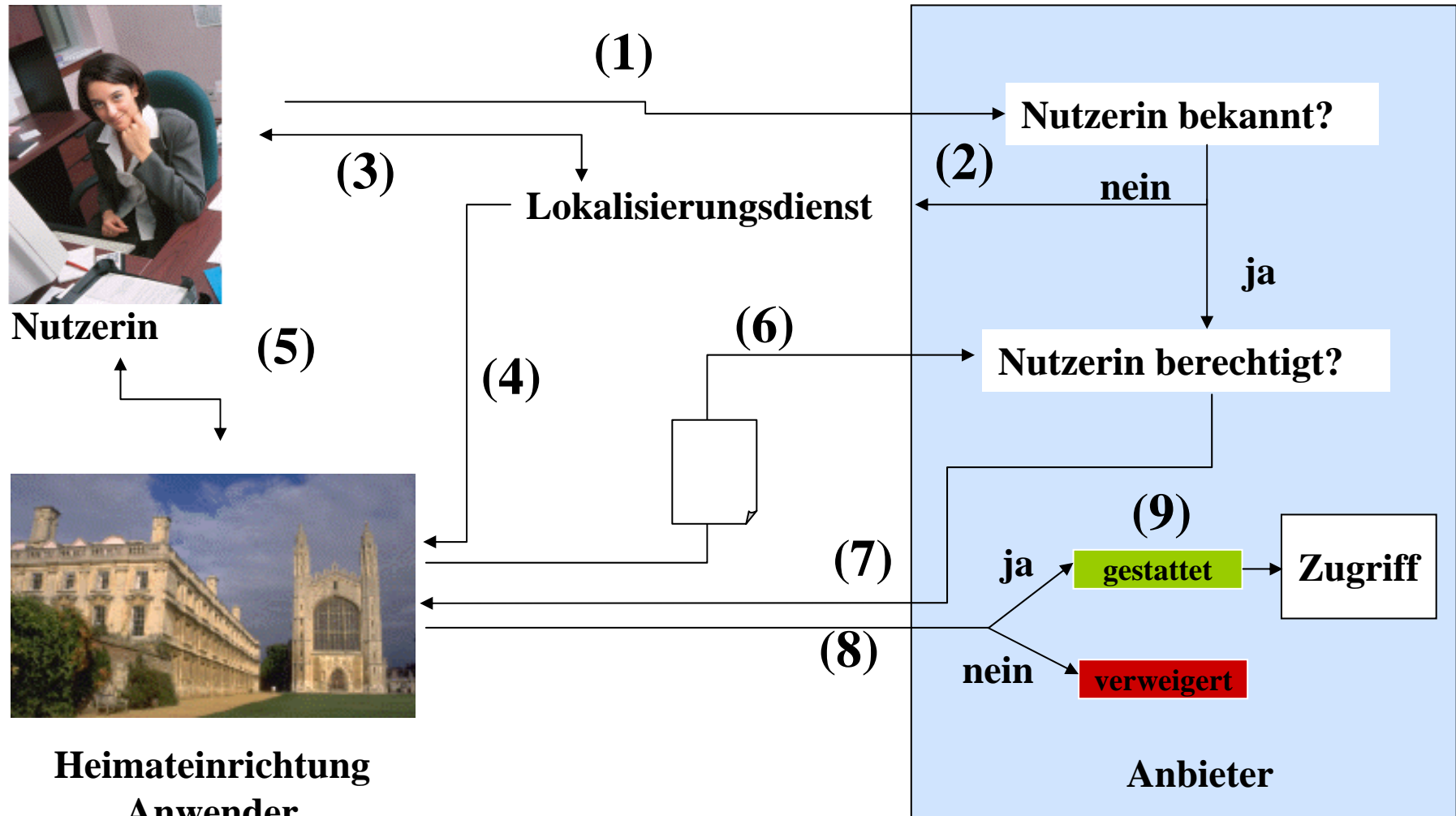
# AAI

Authentifizierung  
Autorisierung  
Infrastruktur

# Wie funktioniert AAI ?



# Wie funktioniert AAI ?



## Shibboleth-System

# Was ist Shibboleth ?

**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)

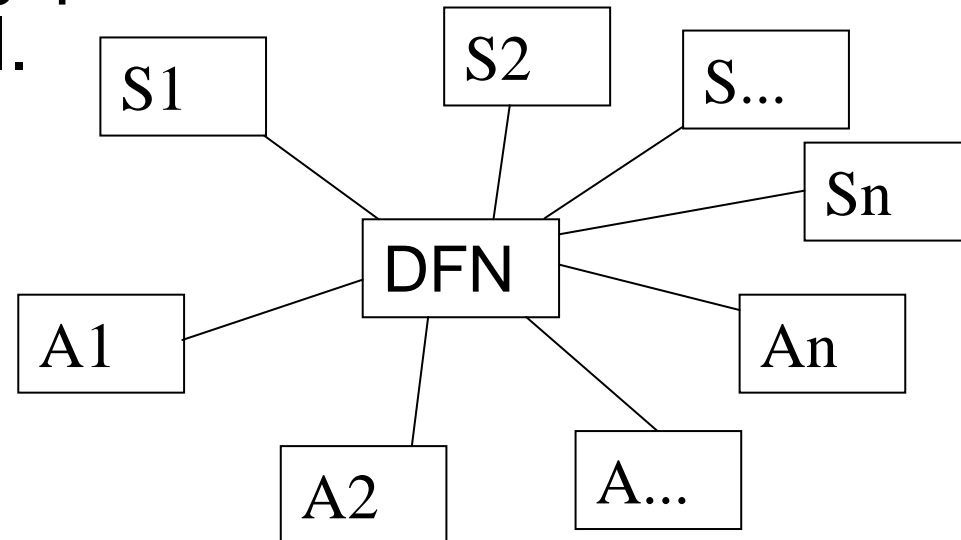
- Anbieter muss dem Anwender **vertrauen**.
- Es geht um **Geld**.
- „**Vertrauen**“ heißt im Geschäftsleben: „**Vertrag**“.
- Es müssen **belastbare vertragliche Regelungen** getroffen werden.

- **DFN-AAI** ist ein Dienst des DFN-Vereins für Wissenschaftseinrichtungen und (auch kommerziellen) Anbietern zur Nutzung einer AAI.
- **DFN-AAI** schafft das für notwendige **Vertrauensverhältnis** zwischen vielen Anwendern und vielen Anbietern und einen **organisatorischen Rahmen** für den Austausch von Nutzerinformationen.

- **Vorgabe von Richtlinien (Policy)**
- **Vertragsgestaltung und -abschluss**
- **zentrale betriebliche Aufgaben**
- **Public Relations**
- **internationale Vertretung**

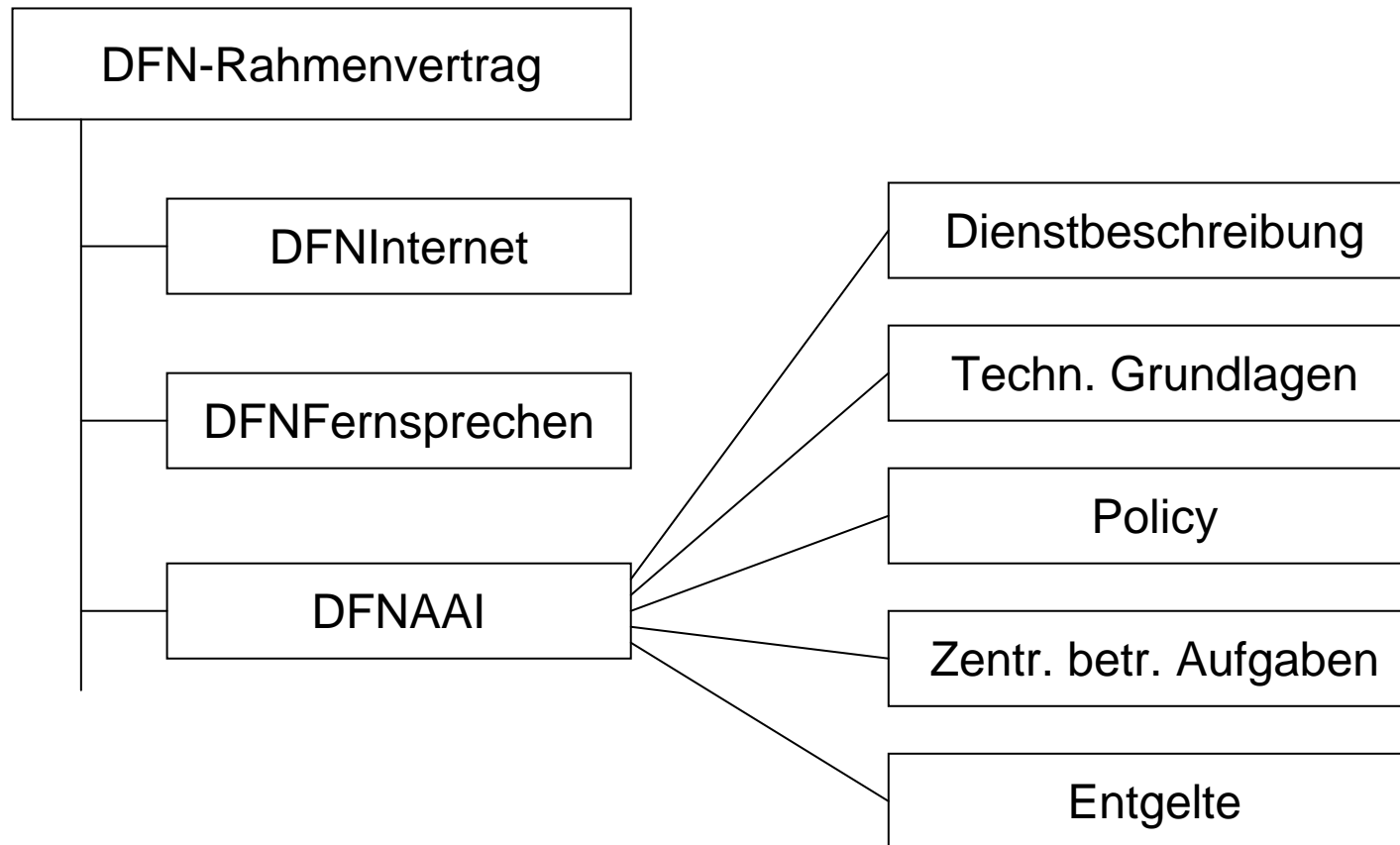
## Der DFN-Verein

- ist zentraler Vertragspartner für alle Teilnehmer der AAI.



- übernimmt **nicht** die Lizenzverträge.

# Vertragsgestaltung / -abschluss



- Metadatenverwaltung
- Testsystem
- WAYF-Server
- Zertifizierungsstelle (DFN-PKI)
- Beratung, Schulung
- internationale Vertretung

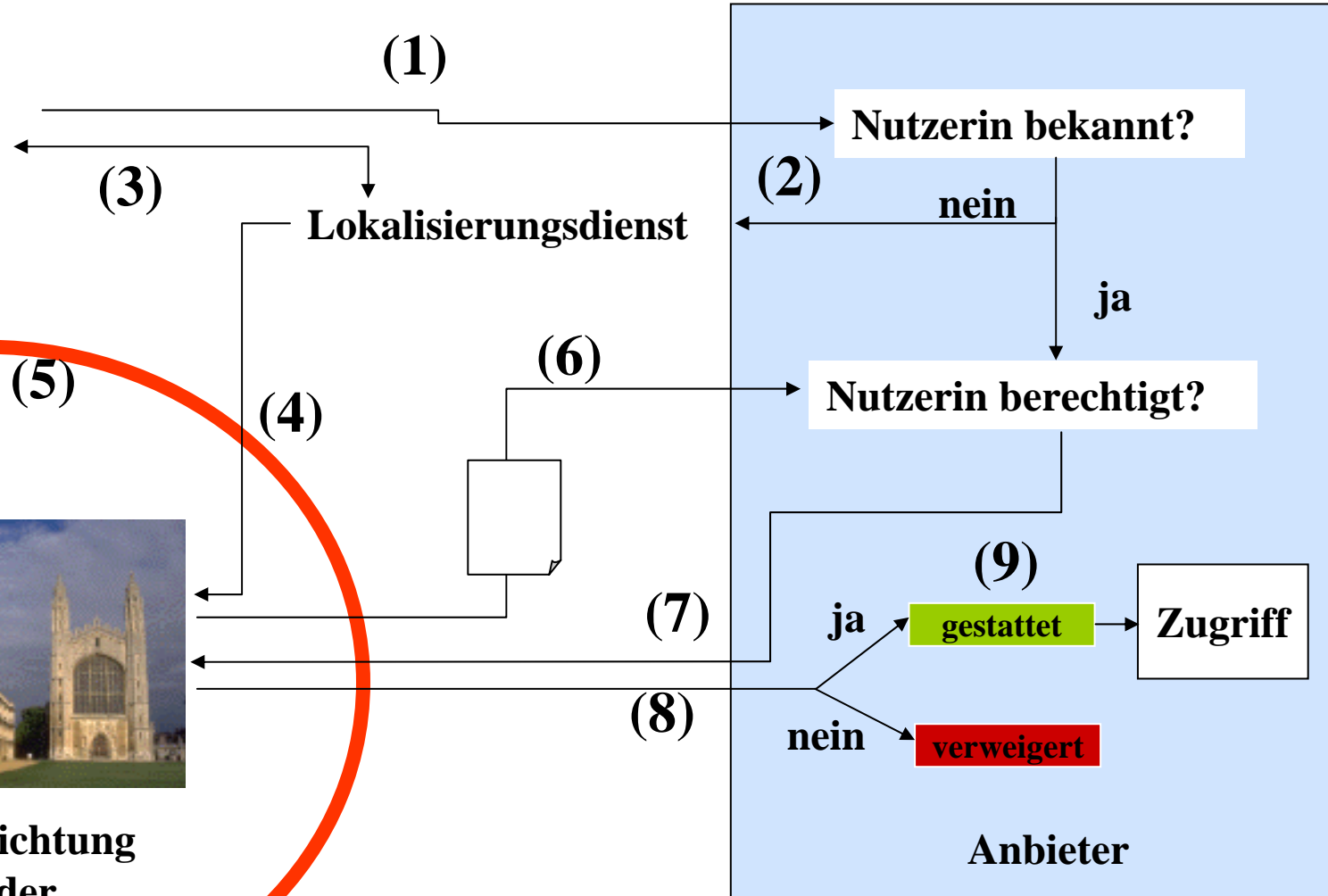
# Wie funktioniert AAI ?



Nutzerin

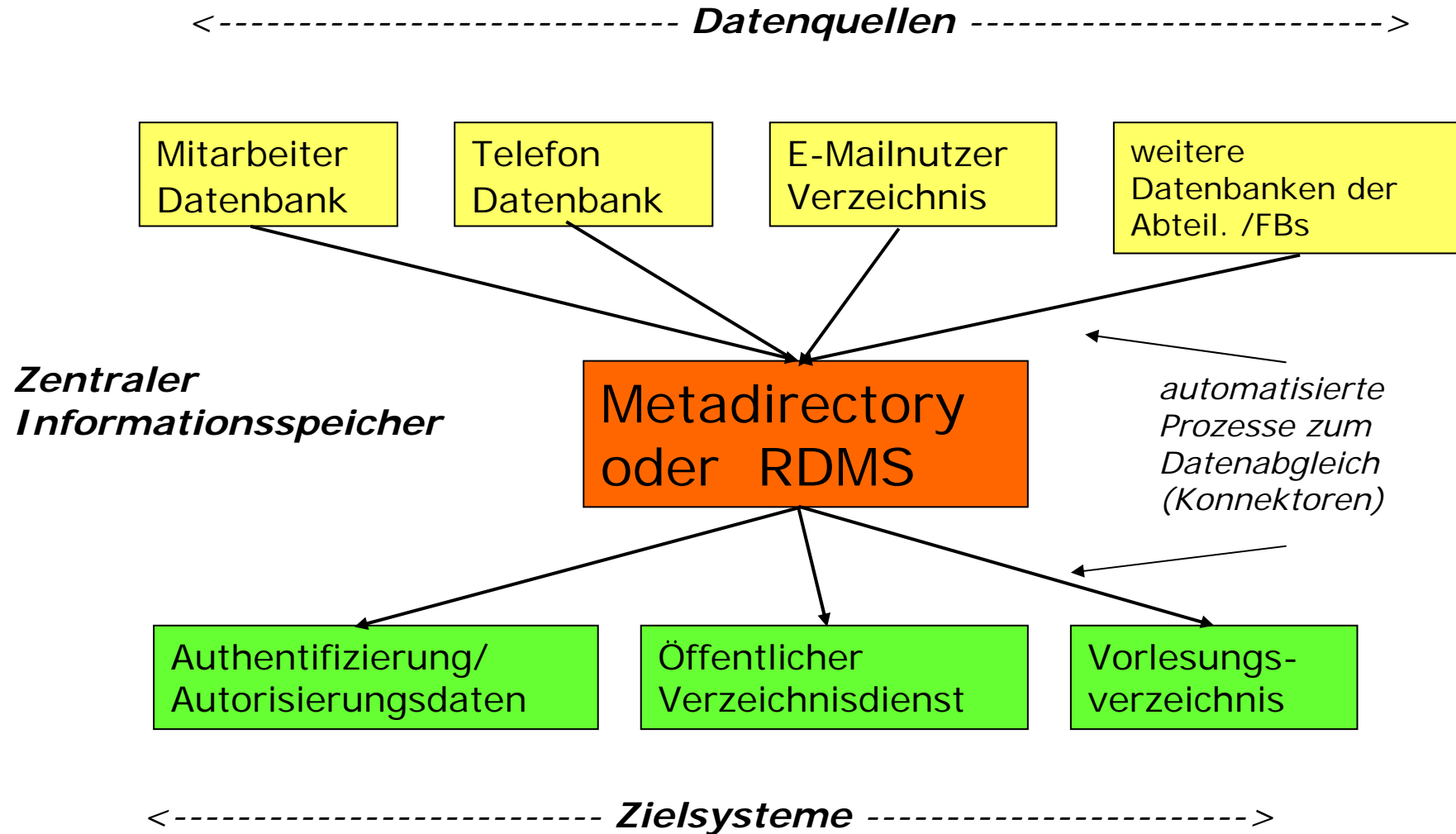


Heimateinrichtung  
Anwender



## Identity-Management-System

- Jeder Person wird eine digitale Identität zugewiesen.
  - eindeutiger Name oder eine Nummer oder ein Login-String
- Jede Person kann über diese digitale Identität von verschiedenen Systemen identifiziert werden.
- Eine digitale Identität besitzt verschiedene Merkmale (Attribute)
  - Vor- und Nachname
  - E-Mail-Adresse
  - Telefonnummer
  - Zugehörigkeit zu Gruppen
  - Rollen
  - etc.



- **Personen erhalten elektronische Identität**
  - Attribute beschreiben die Rolle der Person
  
- **Qualitätsanforderungen**
  - **Verlässlichkeit**
    - Sicherheitsstufen, Missbrauchverhinderung
  - **Aktualität**
    - zeitnahe Änderung
  - **Nachvollziehbarkeit**
    - Dokumentation, Logging
  - **Ausfallsicherheit**
    - Back-up-Systeme
  
- **Einklang mit rechtlichen Vorgaben**
  - Datenschutzgesetz

- **März 2006:**
  1. Treffen interessierter Teilnehmer  
Bibliotheken, GRIDs, eLearning, Anbieter
- **November 2006:**

Fertigstellung grundlegender Dokumente  
(Policy, Verträge, Dienstbeschreibung, etc.)
- **Frühjahr 2007:**

Beginn Vertragsabschlüsse und Betrieb

**Für alle Fragen rund um die DFN-AAI:**

E-Mail: [aai@dfn.de](mailto:aai@dfn.de)

