RWTH AACHEN UNIVERSITY

Identity Management – Grundlagen und Erfahrungsbericht

Thomas Eifert
Guido Bunsen
Denise Dittrich
Rechen- und Kommunikationszentrum der RWTH Aachen

Einführung

- **Einführung von Identity Management (IdM) an der RWTH 2003 Auslöser: Bedarf für automatisiertes Bereitstellen und Entziehen von Accounts**
- **Start mit Massendiensten (Netz-Einwahl, VPN, Email, ..)**
- **Anbindung von „hochwertigen“ Diensten (Hochleistungsrechner, Datenarchiv)**
  - → Seither keine User-/Passwortpflege durch Admins dieser Dienste
  - → Wesentliche Aufwertung in der Wahrnehmung von IdM
- **Inzwischen: Aufnahme aller handelnder Personen in IdM**
- **Viele Erkenntnisse**

Standardprozesse im IdM

IdM: Integrale Plattform für Identitäten, deren Lifecycles über unterschiedliche Prozesse gepflegt werden

Prozesse, um Personen

- **zu registrieren,**
  - → einen oder mehrere weitere Kommunikationswege zu etablieren,
  - → sie mit Anmelde-/Authentifizierungsinformationen (sog. „Credentials“) zu versorgen und
- **Rechte zu deaktivieren, wenn keiner der jew. führenden Pflegeprozess diese Rechte mehr vorsieht.**

- **Pflege und Aktualisierung der personenbezogenen Informationen,.**
- **Unterstützung für den Fall verlorener Credentials („Passwort vergessen“).**

Aufnahme von Personen in das IdM

- **Anlass für die Aufnahme einer Person in das IdM ist immer die gewünschte Teilnahme an einem der zahlreichen IT-basierten Prozesse**

- **Etablierte Massen-Prozesse der Aufnahme**
  - → Immatrikulation
  - → Einstellung

Prozessoptimierung durch IdM

- **Betreiber angeschlossener Dienste können Lifecycle-Management und Authentifizierung als Infrastruktur-Dienste von IdM nutzen**

- **Effizient nur, wenn alle Nutzer von IdM bereitgestellt werden, da ansonsten unterschiedliche Abläufe für den selben Zweck gelten müssen**

Alle Nutzer ?!

Unterschiedliche Personengruppen

- **Weitere Personengruppen an einer Hochschule**
  - → Lehrbeauftragte
  - → Bewerber
  - → Stipendiaten
  - → Gastwissenschaftler
  - → Projekt-/Kooperationspartner
  - → Mitarbeiter von An-Instituten
  - → …

- **Beliebig viele unterschiedliche Pflegeprozesse mit unterschiedlicher Intention, Datenqualität, Berechtigungen, ...**
  Wie kann IdM hier unterstützen?

Standardprozesse in IdM (2)

- **Erfassen personenbezogener Information**
  - → Nutzung zur Identifikation („Passwort vergessen“, Datenabgleich, ..)
  - → Nutzung durch Dienste (Anschreiben, ..)
  - → Unterschiedlicher Bedarf der Dienste beim Informationsumfang
  - → Unterschiedliche Anforderungen an die Qualität der benötigten Daten (News ⇔ Bibliothek)
  - → Unterschiedlicher Aufwand bei Datenerfassung [Selbstregistrierung .. Persönliches Erscheinen mit Identifikation]

Unbeherrschbare Vielfalt ?

Unterschiedliche Quellen

Identitäten kommen aus unterschiedlichen Quellen

- **Studierendensekretariat und Personalverwaltung der Hochschule**
- **Kooperierende Einrichtungen**
- **Einzelne Gastgeber**
- **An-Institute**

Einfacher „Daten-Import“ nicht möglich, da

- **Quellen nichts voneinander wissen (sollen / dürfen),**
- **Quellen nicht-disjunkte Personenmengen liefern,**
- **zentraler Abgleich Zugriff auf viele personenbezogene Daten bedürfte**
- **aber wesentliche Vorteile von IdM voraussetzen, dass jede Person nur einmal (als Identität) erfasst ist**

Übersicht über die Quellen

- **Die Beziehung einer Person zu unterschiedlichen Organisationen ist nur an einer Stelle bekannt**

  Diese Person selbst

Fragestellung

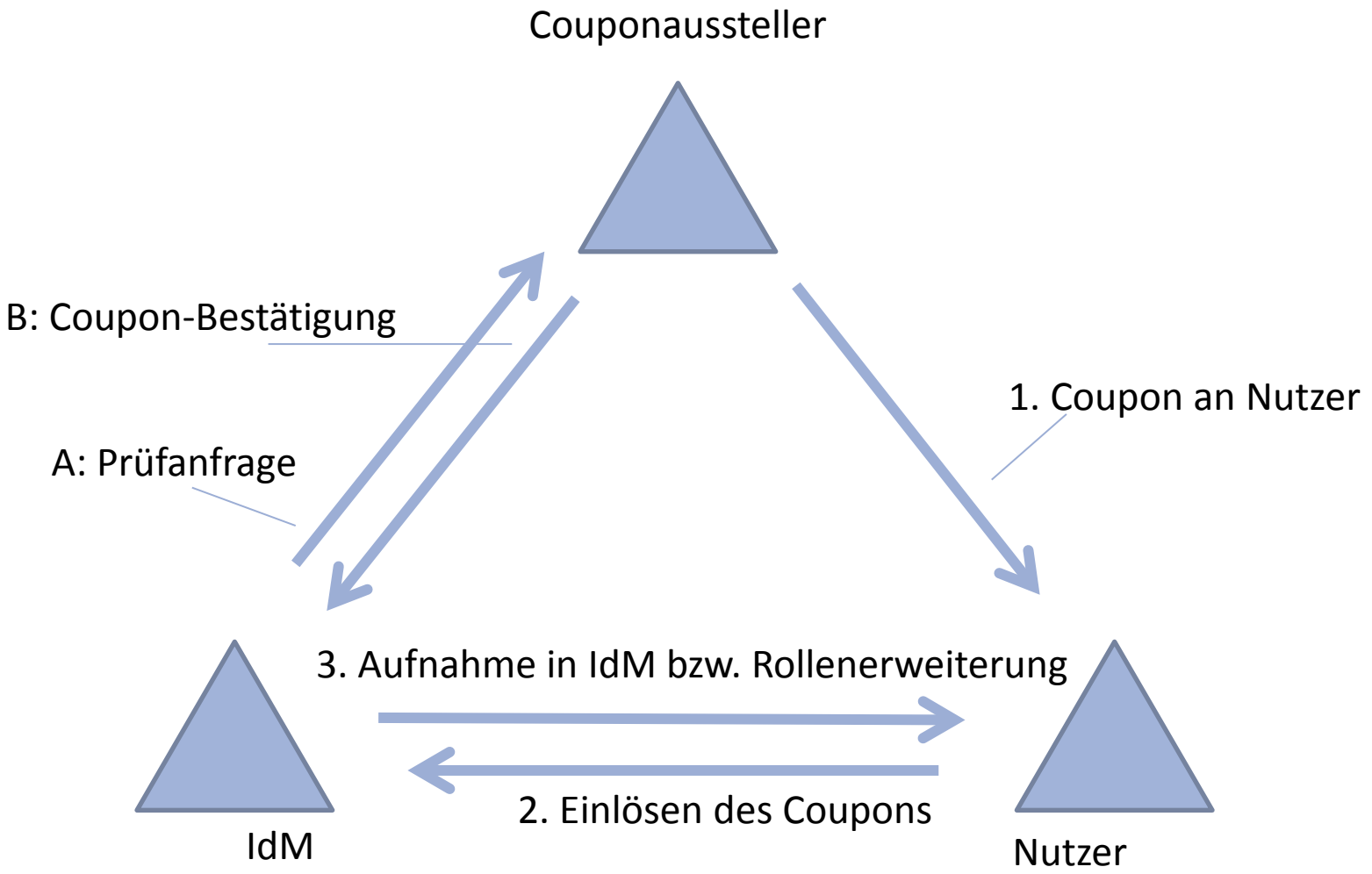
- **Die Information aus einer Quelle von Personendaten müssen mit einer Identität verknüpft werden oder**
- **Es muss eine neue Identität angelegt werden**
- **Die Person („Nutzer“) muss Quelle und IdM verbinden**
- **Identität und Quell-Objekt müssen verbunden werden**

➔ **Wie kann das Wissen der Person genutzt werden?**

Unsere Lösung: Das Coupon-Verfahren

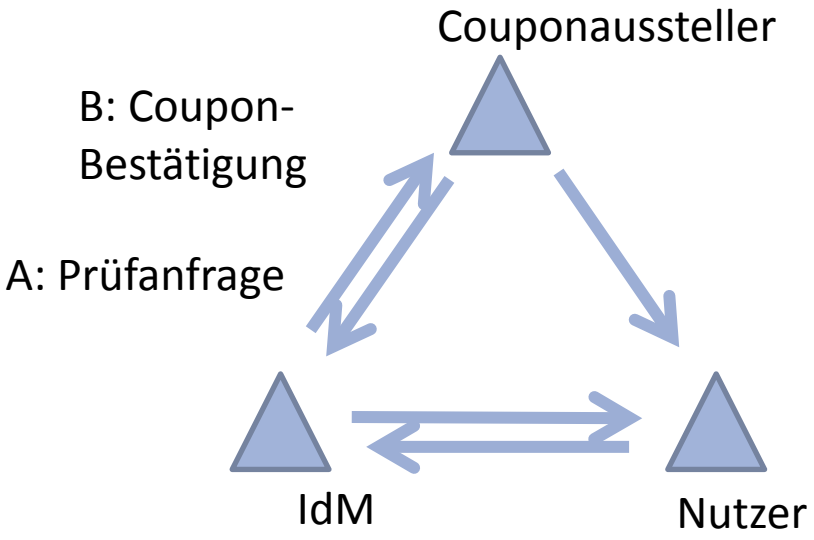
Coupon: Referenz-Information

Das Coupon-Verfahren

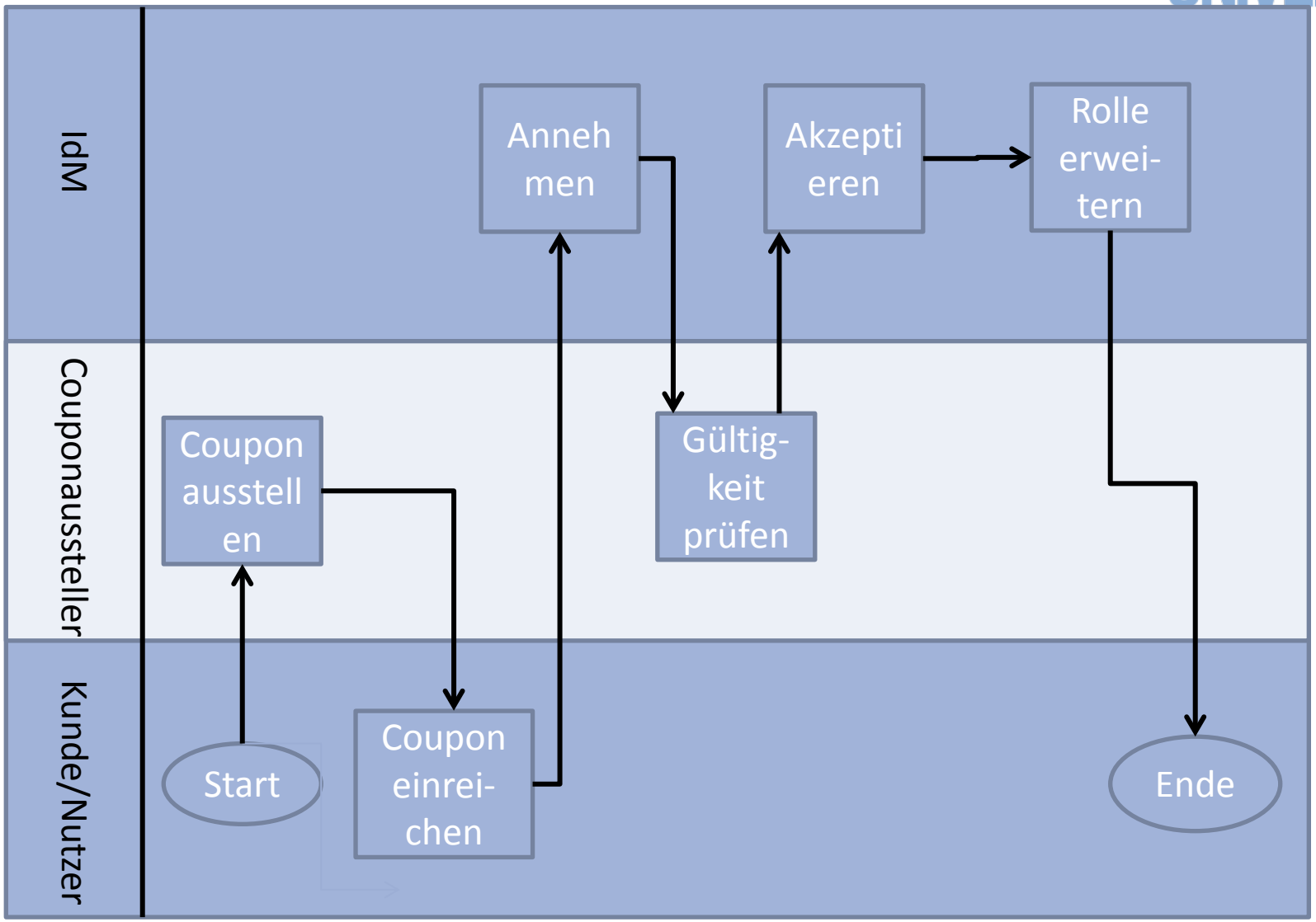


Einrichtungsübergreifende Lifecycle

- **Periodisches Wiederholen von Prüfanfrage und Coupon-Bestätigung ➔ Identity-Lifecycle**
- **Automatischer Entzug impliziter Berechtigungen**



Coupon-Verfahren in Prozessdarstellung



Einrichtungsübergreifende Prozesse

- **Einrichtungs- und organisationsübergreifend geltende Identitäten (ggf. über Referenz verknüpft)**

- **Dies erlaubt Bezug auf die selben Personen**
  - → Zentrale Authentifizierung als Infrastruktur-Service
  - → Einrichtungsübergreifende, IT-gestützte Prozesse
    - →Verwaltungsworkflows
    - →Forschungs-Workflows

Identitätsbasierte Rollen und Rechte

- **Prozesse bedingen Rollen und Berechtigungen**
  - → Lange gelöst innerhalb von Einrichtungen

- **Einrichtungsübergreifende Identitäten als Basis für einrichtungsübergreifende Rollen**
  - → Prozesse können medienbruchfrei mehrere Einrichtungen umfassen
  - → Rollenvergabe und Rollen-Nutzung können auf unterschiedliche Einrichtungen verteilt sein
    - →Delegation von Aufgaben im Kontext einer Einrichtung
    - →Nutzung in verteilten oder zentralen Prozessen

Implizite und individuelle Rollen

- **Implizite Rollen: abzuleiten aus Personendatenquelle bzw. Coupon-Aussteller**
  - → Studierendensekretariat ➔ Studierender
  - → Personalabteilung ➔ Mitarbeiter der Hochschule
  - → Kooperierende Einrichtung ➔ Partner; Rechte gem. Kooperationsvertrag
  - → Individueller Gastgeber ➔ individueller Gast
  - …
- **Individuelle Rollen: explizit an Person vergeben**
- **Vielzahl von Rollen pro Person möglich**
- **Rollen-Modell macht Unterscheidung Rolle / Status überflüssig**

Zentrale Verzeichnisse als Infrastruktur

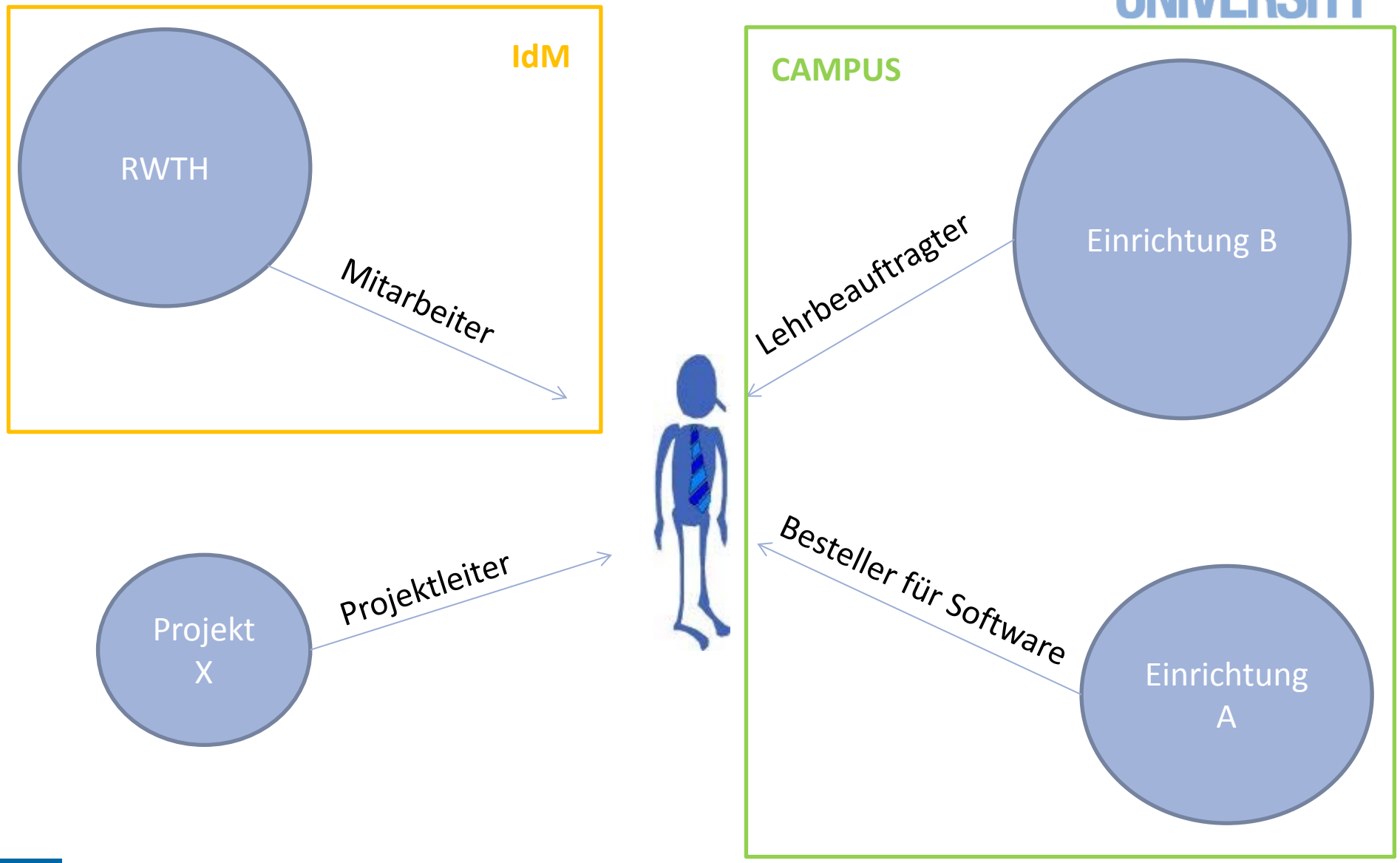
- **Einrichtungsübergreifend geltende Informationen über Identitäten und Rollen als zentrale Infrastruktur**
- **Personendatenquellen als Lieferant von Informationen**
  - → Erreichbare / verbindliche Datenqualität
  - → Annahmen / Begrifflichkeit von Informationen
- **IT-Service-Provider als Konsument der Informationen**
  - → Das Lesen ist der kritische Schritt
    - →Welches Verbindlichkeit wird benötigt?
    - →Verwendungszweck und Implikationen?
    - →Konsumieren muss mindestens so sauber definiert sein wie Einliefern!
- **Infrastrukur für einrichtungsübergreifende Prozesse**

Aktuelle Aktivitäten

- **Einführung eines zentralen Rechte und Rollenmanagements an der RWTH Aachen**
  - → Zentrale Infrastruktur für Rollen in RWTH-weiten Prozessen
  - → Bereitstellung von Rollen auf Basis von Identitäten

- **Ausgangssituation**
  - → Verwaltung von Identitäten im IdM
  - → Verwaltung von Rollen im Kontext von Einrichtungen im CAMPUS-Informationssystem (auf Basis der Mitarbeiterdaten einer Einrichtung)
  - → Vielzahl von Einzellösungen
  - → Wenig Verständnis für die Thematik

Rollen in verschiedenen Kontexten



Bisheriges Vorgehen

- **Zuerst: Erarbeitung eines Konzepts, gemeinsam mit der zentralen Hochschulverwaltung (= Prozess-Owner für viele Prozesse)**

- **Technisch:**
- **Brücke zwischen bisher getrennten Systemen (CAMPUS und IdM)**
  - → Auch hier: Verknüpfung wird durch Person selber erstellt!
  - → Verknüpfung zwischen Identitäten und schon vorhandenen Rollen
- **Aufbau einer gemeinsamen Infrastruktur**
- **Authentifizierung und Autorisierung aus einer Quelle**

Ausblick

- **Sichtbare Konsolidierung von Identitäten und Rollen**
- **Neue Oberfläche zur Verwaltung von Rollen**
  - → Vergabe von Rollen basiert auf Coupon Verfahren
  - → Wegfall von alten Einschränkungen (z.B. weitere Kontexte)
- **Entwicklung weiterer Rollen**
  - → Genehmigungsverfahren
- **Nutzung der Rollenverwaltung in weiteren zentralen Prozessen**
  - → Neues CampusManagementSystem

RWTH AACHEN UNIVERSITY

Vielen Dank für Ihre Aufmerksamkeit!