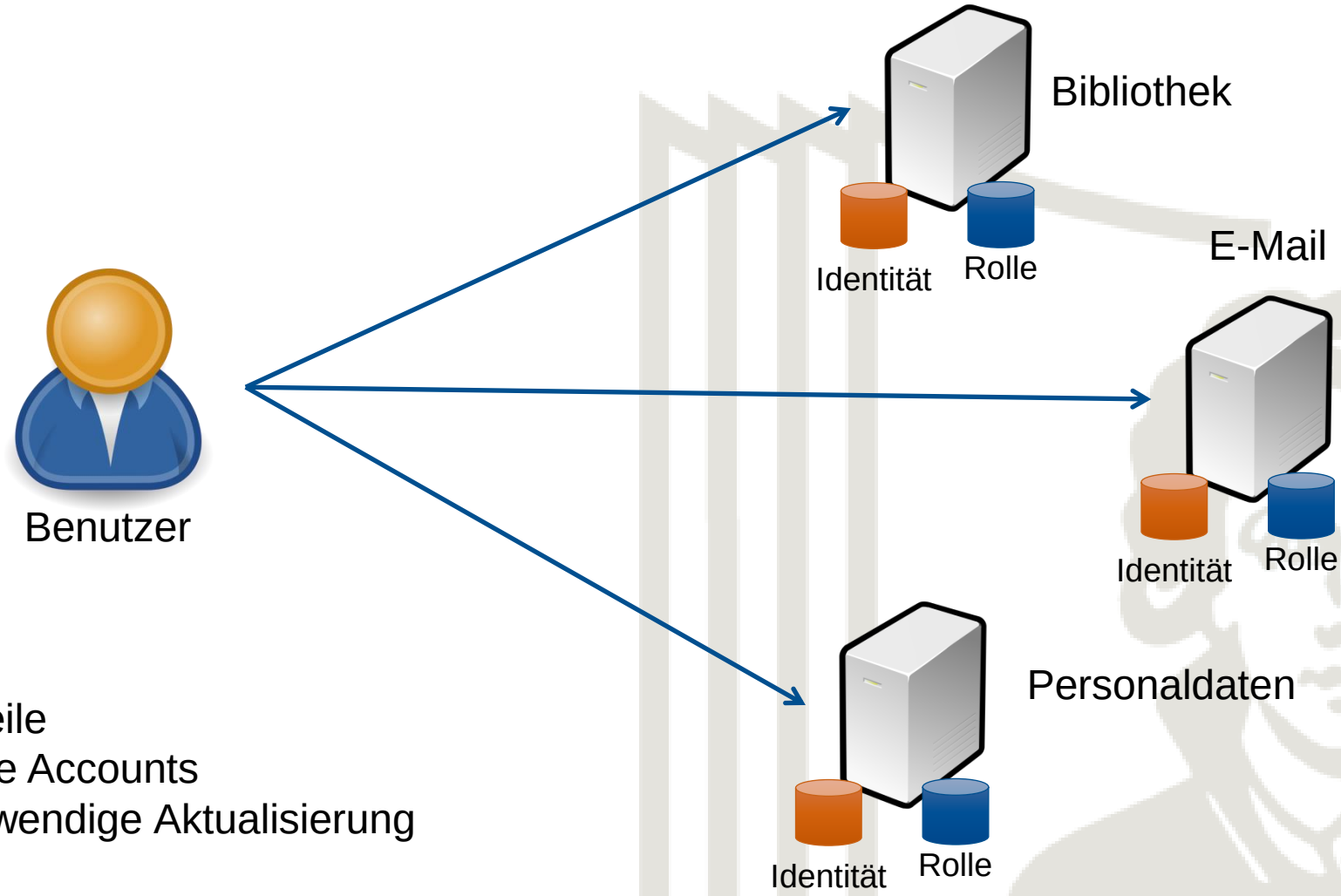
UNIVERSITÄTS BIBLIOTHEK FRANKFURT AM MAIN

Identity Management an den hessischen Hochschulen

HeBIS Verbundkonferenz
26.9.2017, Frankfurt

Dr. Thomas Risse

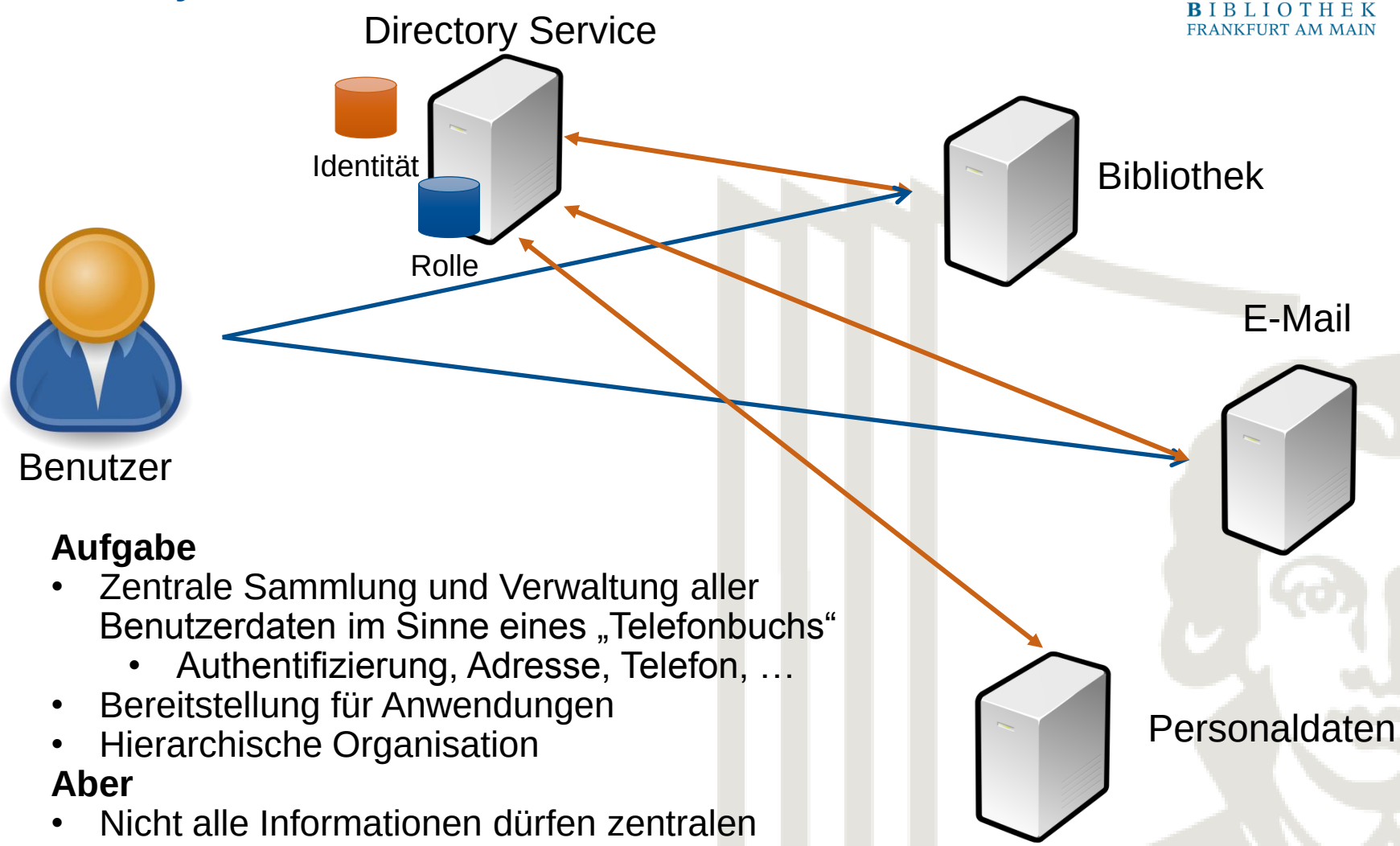
Wie alles begann



Nachteile

- Viele Accounts
- Aufwendige Aktualisierung

Directory Services



Aufgabe

- Zentrale Sammlung und Verwaltung aller Benutzerdaten im Sinne eines „Telefonbuchs“
  - Authentifizierung, Adresse, Telefon, …
- Bereitstellung für Anwendungen
- Hierarchische Organisation

Aber

- Nicht alle Informationen dürfen zentralen Directory administriert werden z.B. Personaldaten

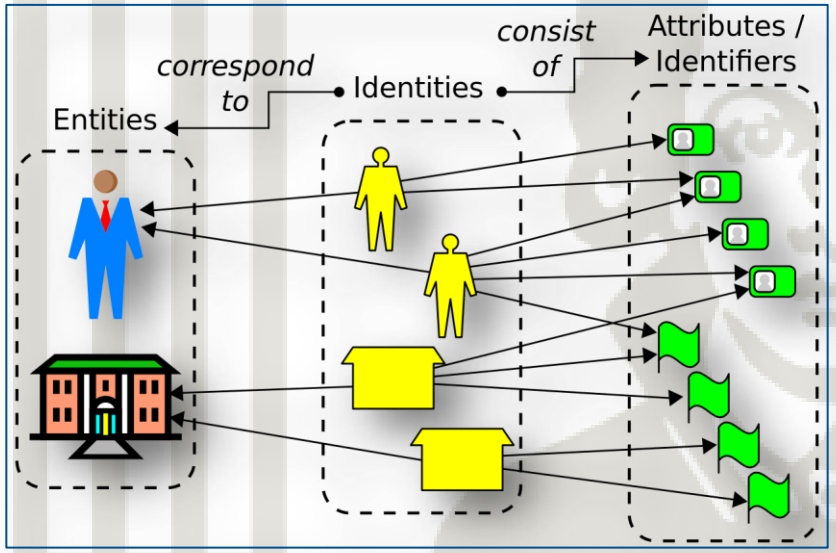
Identitätsmanagement

Ziel

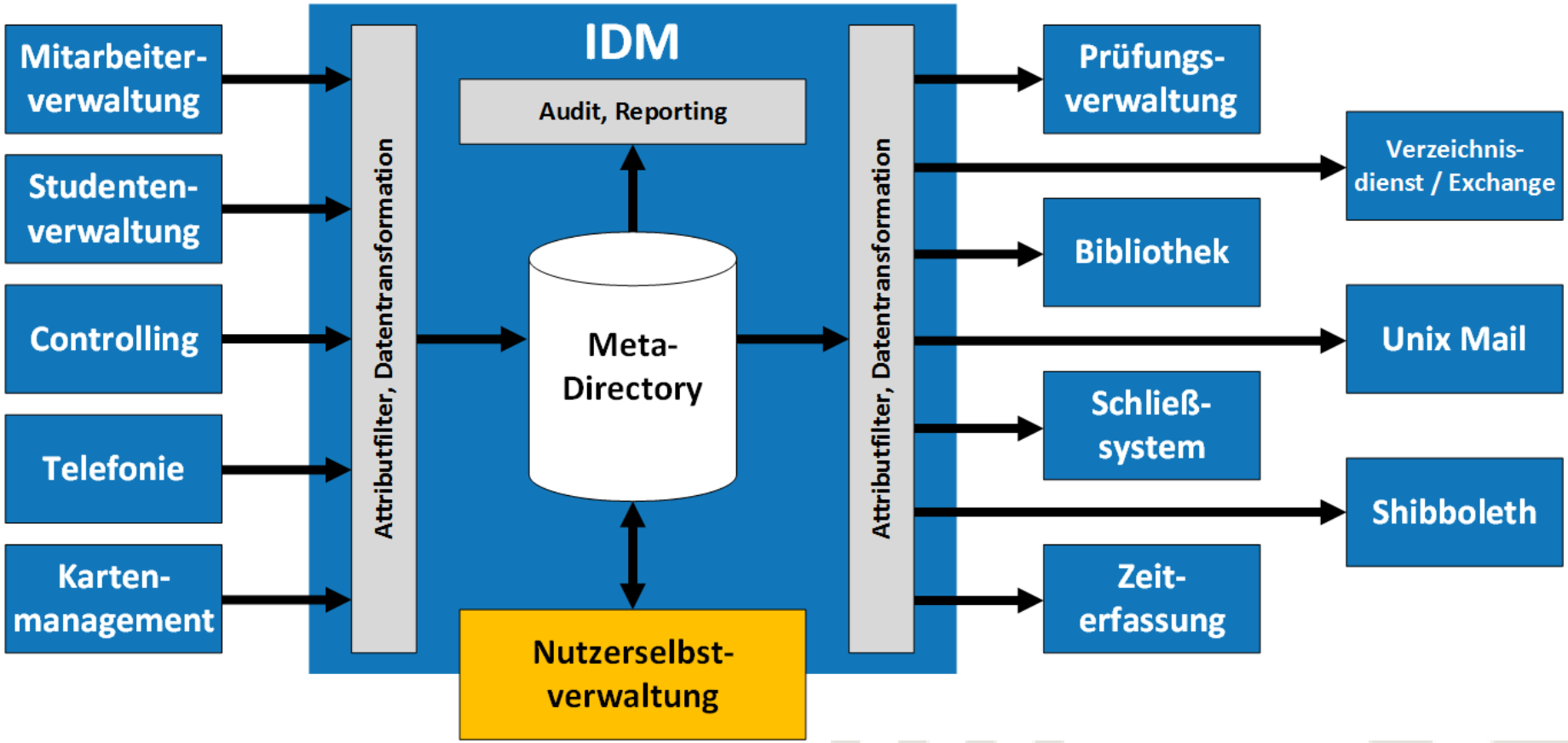
- Zielgerichtete und bewusste Umgang mit Identität, Anonymität und Pseudoanonymität
  Beispiel: Personalausweis ist eine staatlich vorgegebene Form der Identifizierung
- Klarheit schaffen, was mit den Daten passiert

Identitätsmanagement umfasst

- Den Identifikationsprozess einer Entität
- Informationen, die mit einer Entität innerhalb eines Kontextes verbunden sind
- Sichere Verwaltung der Informationen der Entität

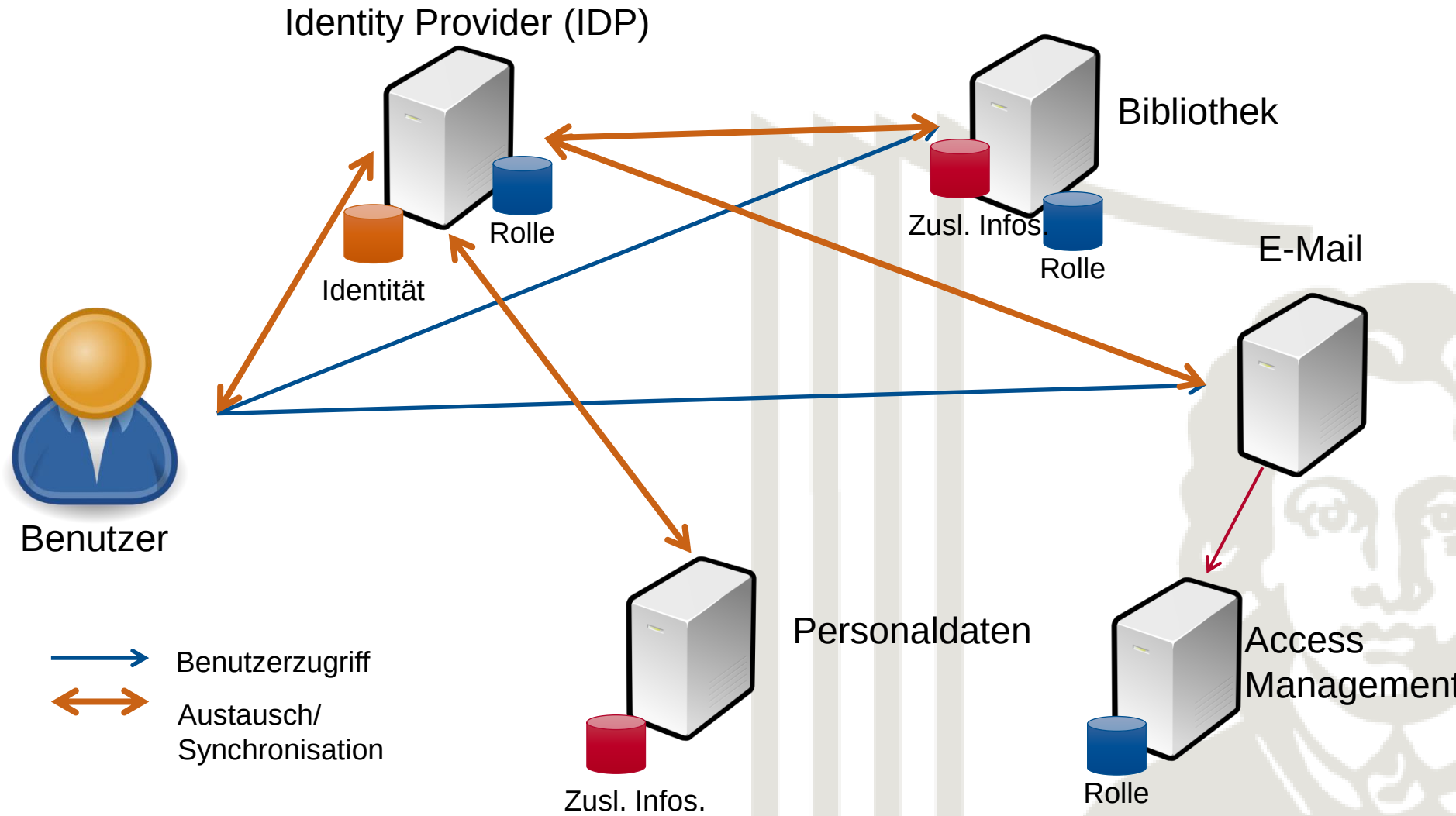


Integrationspotentiale

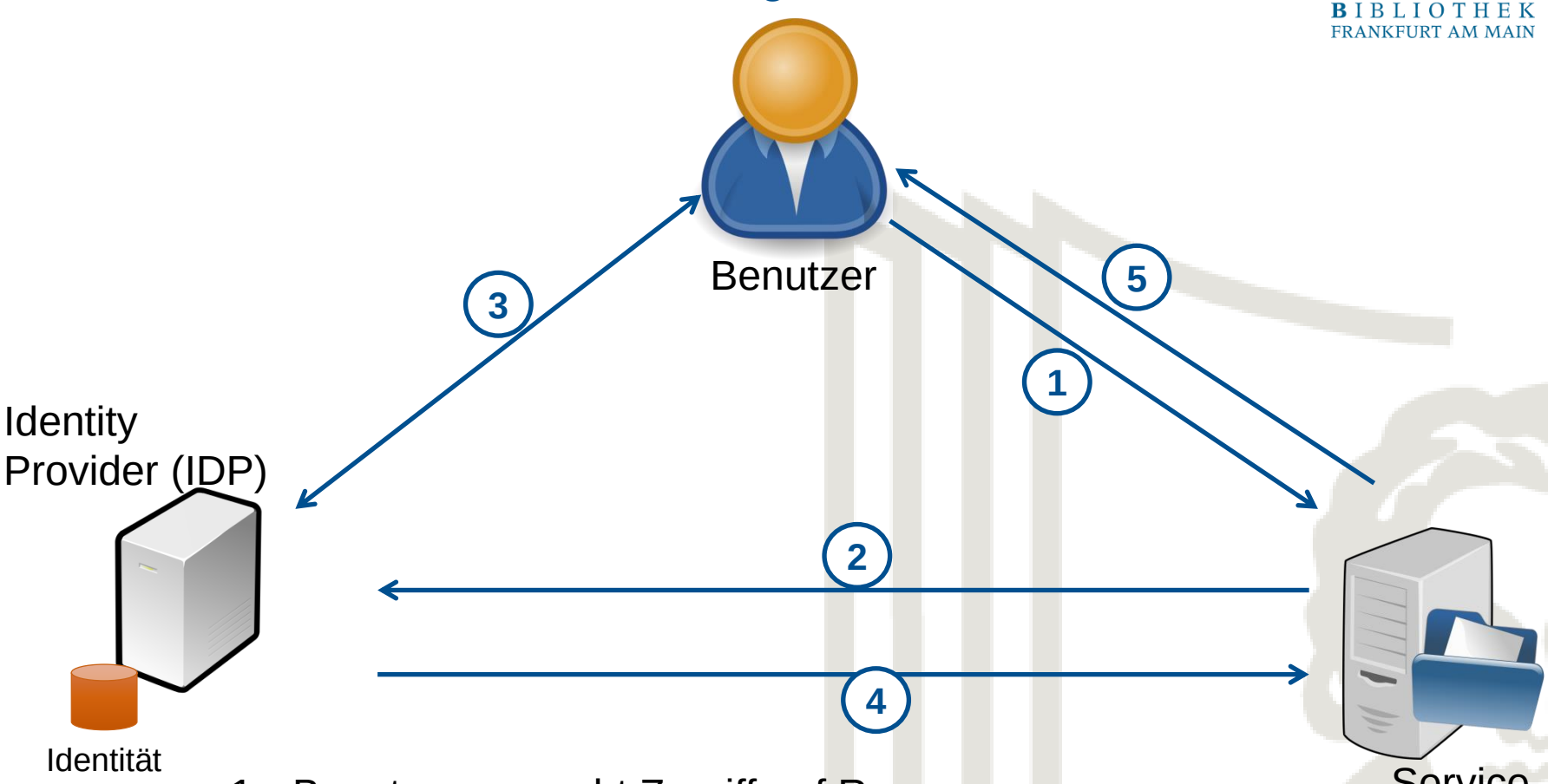


Quelle: TU Bergakademie Freiberg, Aufbau des Identitätsmanagementsystems, 2017

Identitätsmanagement

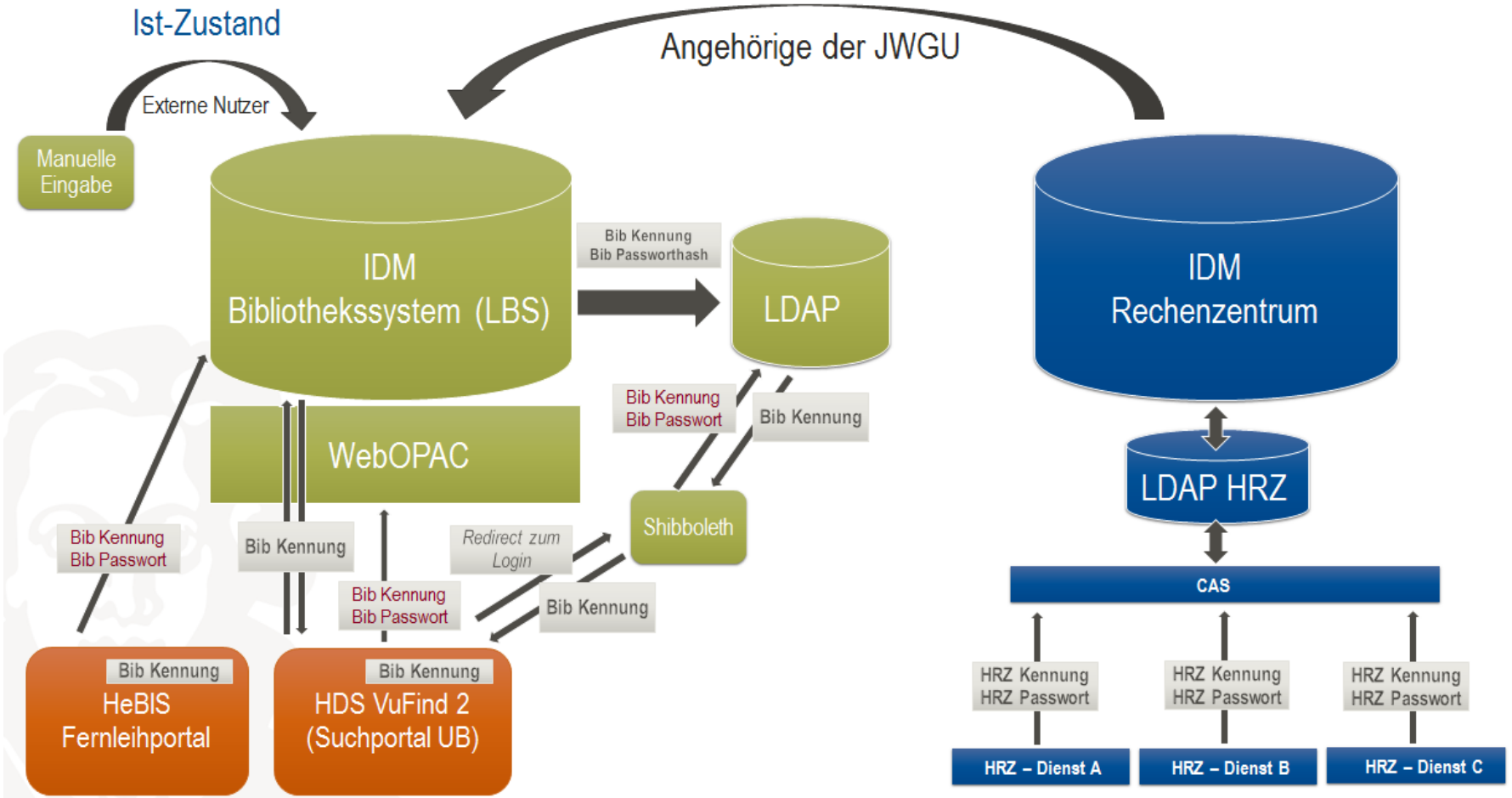


Vereinfachtes Shibboleth Flow Diagramm

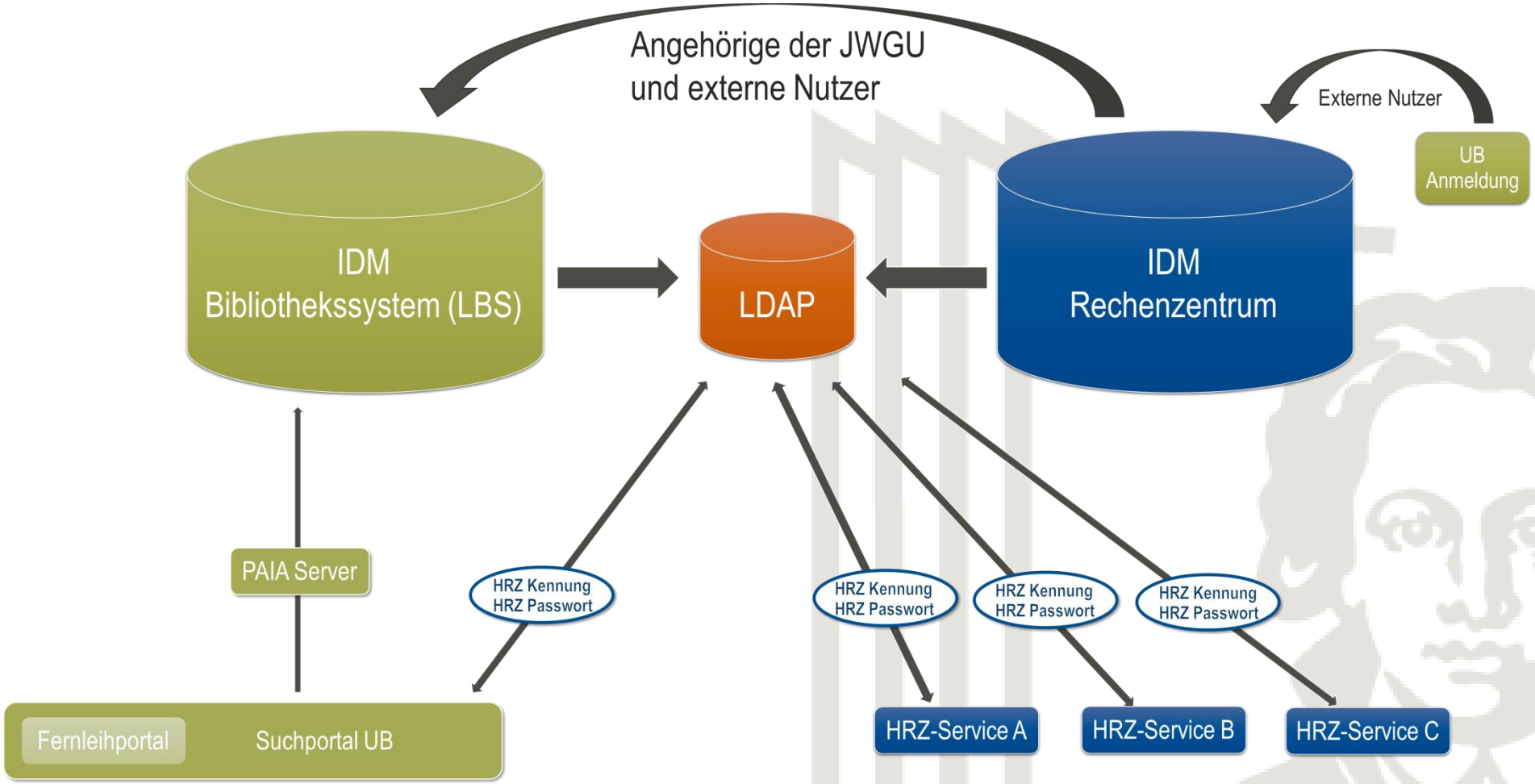


1. Benutzer versucht Zugriff auf Ressource
2. Benutzer wird zum Identity Provider umgeleitet
3. Benutzer muss sich gegenüber dem IDP authentifizieren
4. Austausch der Benutzerinformationen (sofern gestattet)
5. Service erlaubt oder verweigert den Zugriff

Beispiel: Johann Wolfgang Goethe-Universität (Ausgangslage)



Beispiel: Johann Wolfgang Goethe-Universität (Ziel)



Herausforderungen auf der Landesebene

UNIVERSITÄTS BIBLIOTHEK FRANKFURT AM MAIN

Warum ein Landesweites IDM?

- Zugriff auf Dienste an anderen Einrichtungen
- Professor/Mitarbeiter/Student wechseln zwischen Universitäten
  → Mehrere Accounts

Nebeneffekt

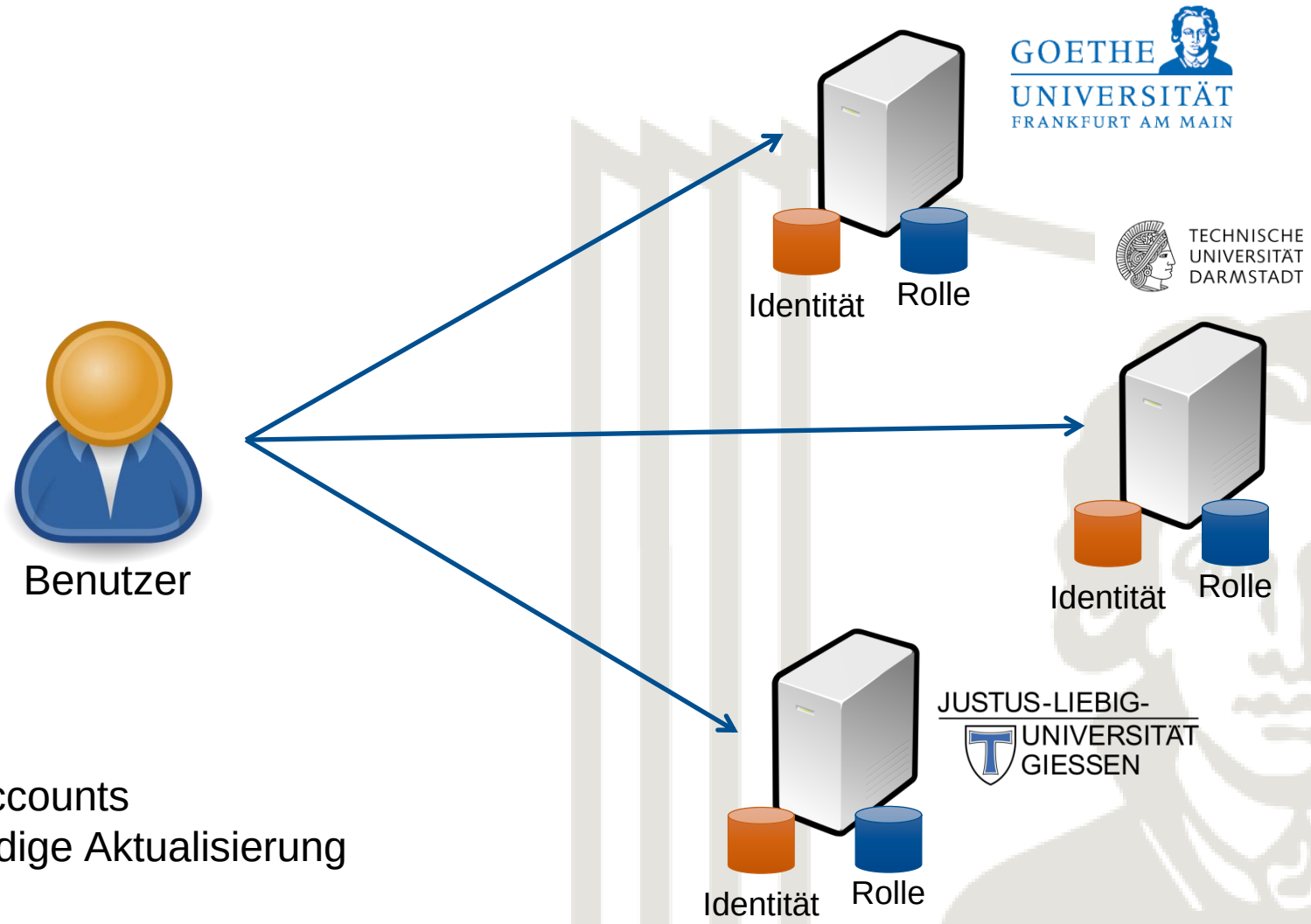
- Anpassung aller System auf ein einheitliches Niveau: DFN-AAI Mindeststandard
- Zusammenführen von UB und HRZ Accounts

Herausforderungen

- Viele Teilnehmer mit
  - unterschiedlichen Anforderungen
  - unterschiedlichen Implementierungen
- Datenschutzbestimmungen
- Architektur: Zentral vs. Dezentral vs. Hybrid

Quelle: das Marburger Online Magazin

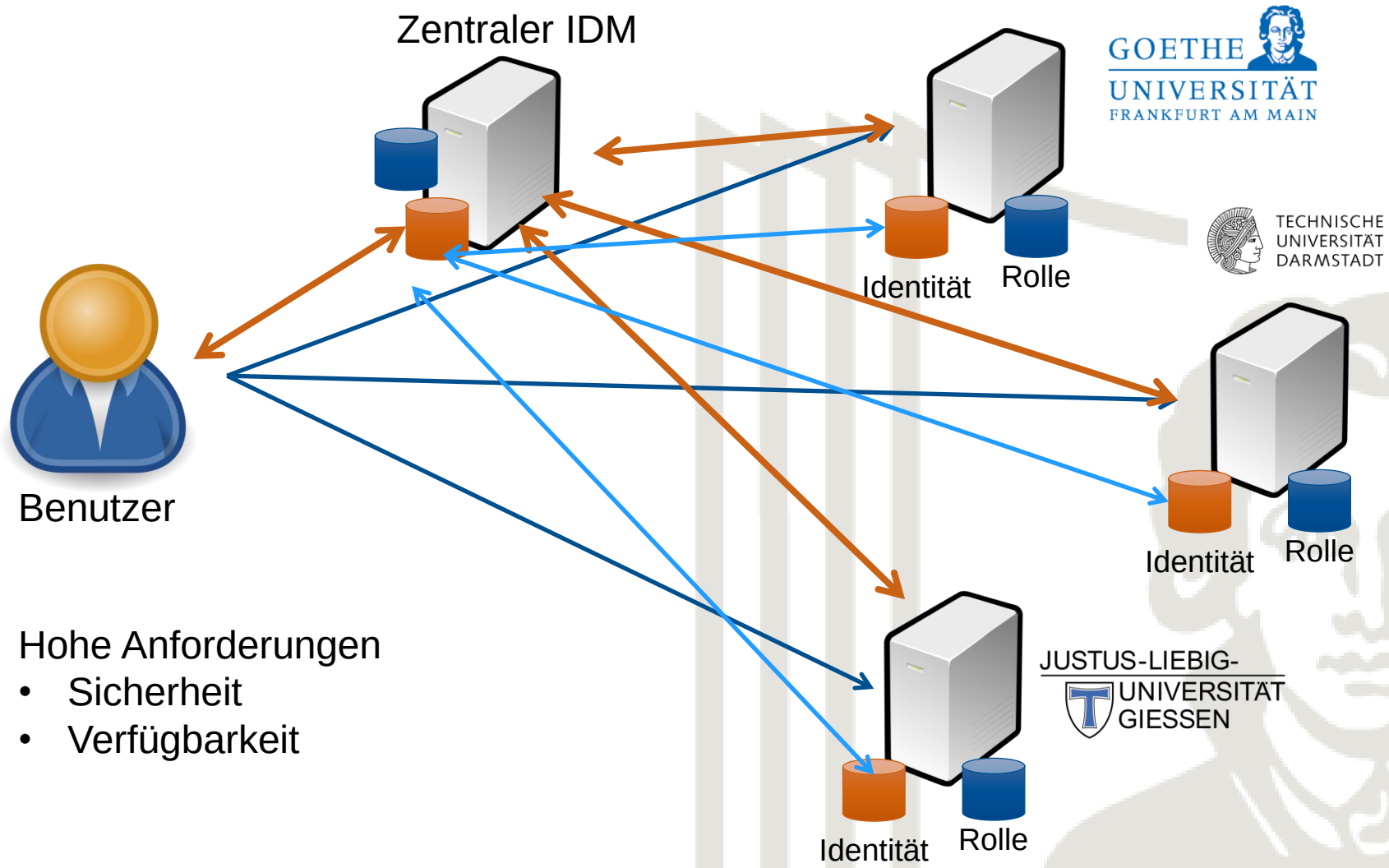
Umsetzung mit lokalem Identitätsmanagement



Nachteile

- Viele Accounts
- Aufwendige Aktualisierung

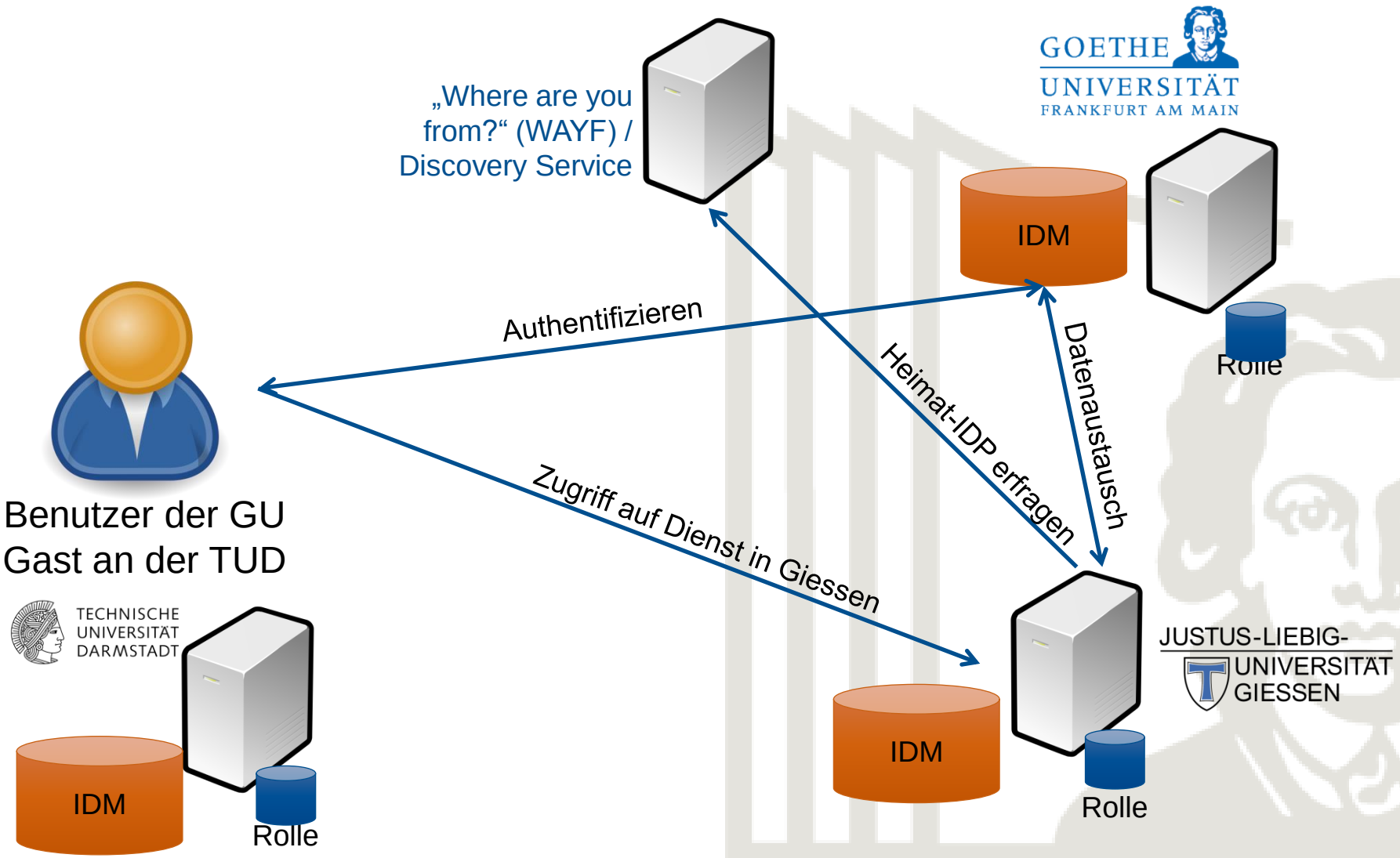
Zentralisierte Lösung



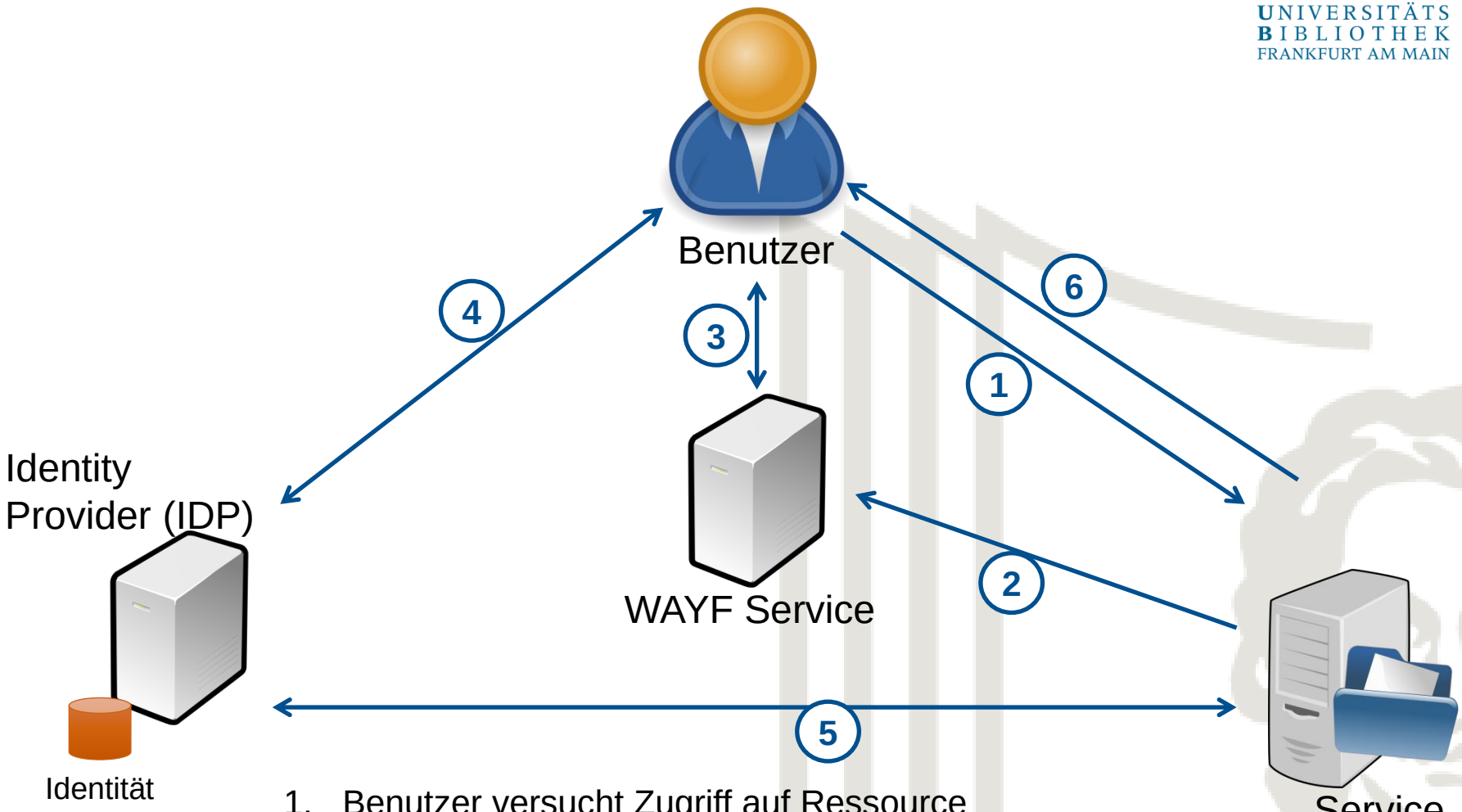
Hohe Anforderungen

- Sicherheit
- Verfügbarkeit

Hybride Lösung mit Discovery Service



Vereinfachtes Flow Diagramm für verteilte IDP



1. Benutzer versucht Zugriff auf Ressource
2. Benutzer wird zum Discovery Service umgeleitet
3. Benutzer wählt seine Heimatorganisation
4. Benutzer muß sich gegenüber dem IDP authentifizieren
5. Austausch der Benutzerinformationen (sofern gestattet)
6. Service erlaubt oder verweigert den Zugriff

Antragstellung HEIDI

HEIDI - HEssische IDentitätsmanagement Infrastruktur

- LHEP Antrag zum Aufbau einer hessischen IDM Lösung
- Federführend: Goethe Universität & Hochschule RheinMain
- Laufzeit: 3 Jahre
- Aktuell: Bestandsaufnahme
- Antrag zur Vorlage bei Hochschulen und Ministerium: bis Ende des Jahres

UB
UNIVERSITÄTS
BIBLIOTHEK
FRANKFURT AM MAIN

Dr. Thomas Risse
Leiter Elektronische Dienste
Tel. +49 69 798 39 905
Email: t.risse@ub.uni-frankfurt.de

Universitätsbibliothek J. C. Senckenberg
Bockenheimer Landstraße 134 - 138
60325 Frankfurt am Main
http://www.ub.uni-frankfurt.de