FernUniversität in Hagen

Diplomarbeit

Architektur eines Identitätsmanagementsystems an einer Hochschule

Steffen Hofmann
steffen.hofmann@fu-berlin.de

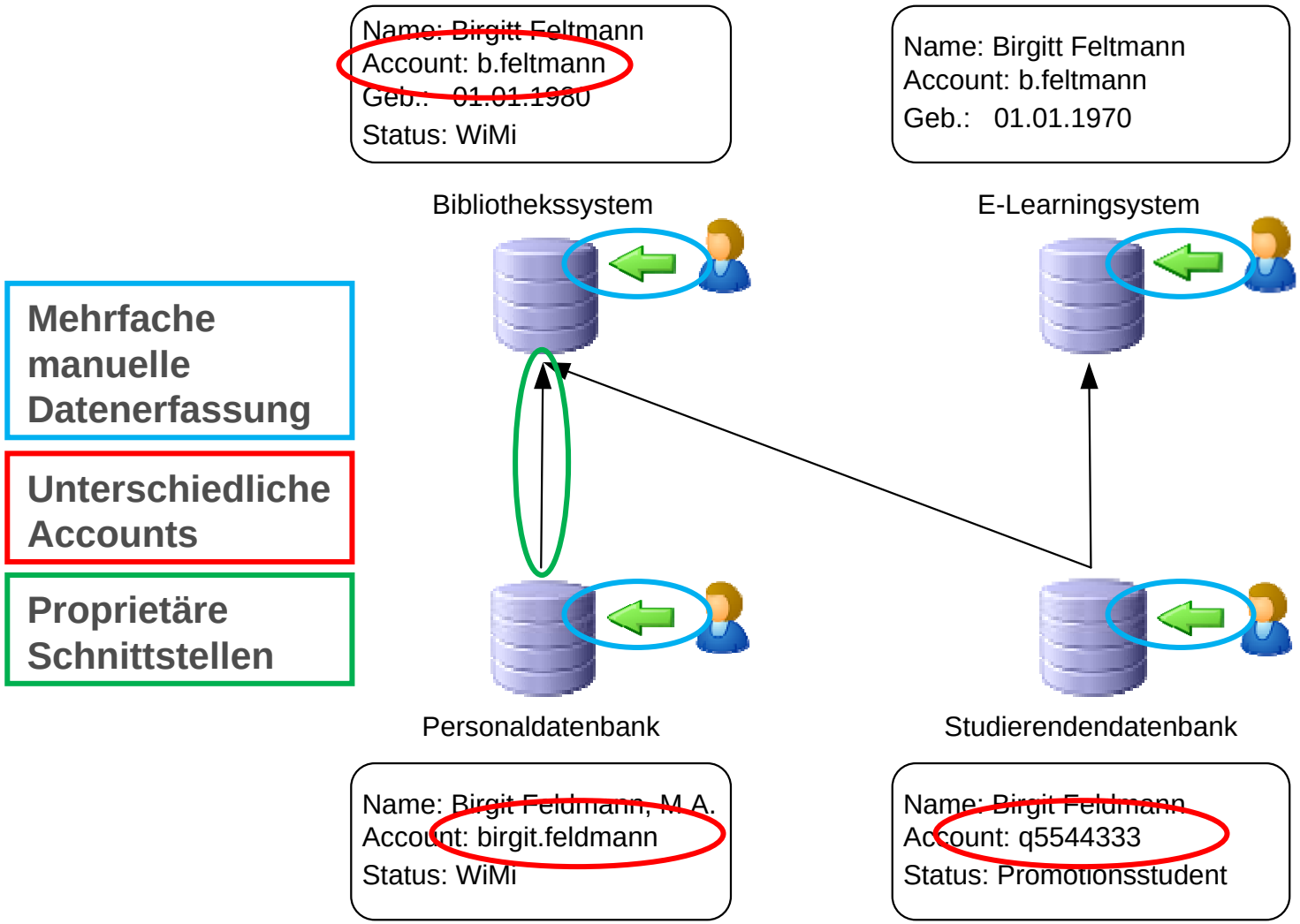
betreut von Birgit Feldmann
an der Fakultät für Mathematik und Informatik,
Lehrgebiet Informationssysteme und Datenbanken,
Prof. Dr. Gunter Schlageter,
der FernUniversität in Hagen

eingereicht im Juni 2007

Gliederung des Vortrags

- Ziele der Diplomarbeit
- Grundlagen und Stand der Forschung (ausgewählte Themen)
- Rahmenbedingungen (kurze Übersicht)
- Architektur (Ausschnitte)
- Fazit
- Ausblick

Motivation


Name: Birgitt Feltmann
Account: b.feltmann
Geb.: 01.01.1980
Status: WiMi
Name: Birgitt Feltmann
Account: b.feltmann
Geb.: 01.01.1970
Bibliothekssystem
E-Learningsystem
Mehrfache manuelle Datenerfassung
Unterschiedliche Accounts
Proprietäre Schnittstellen
Personaldatenbank
Studierendendatenbank
Name: Birgit Feldmann, M.A.
Account: birgit.feldmann
Status: WiMi
Name: Birgit Feldmann
Account: q5544333
Status: Promotionsstudent

Ziele

- Skizzierung einer Architektur für ein Identitätsmanagementsystem
- Berücksichtigung der historisch gewachsenen, heterogenen IT-Infrastruktur einer Hochschule

Themen in „Grundlagen und Stand der Forschung“

- Definition Architektur
- **Identitätsmanagementsysteme**
- Datenmodelle für Datenbanken
- Verzeichnisdienste und LDAP
- **Grundlagen zur Datenintegration**
- Sicherheit von IT-Systemen
- Authentifizierungsverfahren
- **Autorisierungsmodelle**
- Architekturansätze für Identitätsmanagementsysteme
- Serviceorientierte Architekturen
- Standards für föderierte Identitätsmanagementsysteme
- Initiativen für föderierte Identitätsmanagementsysteme
- Workflowmanagement

Themen in „Grundlagen und Stand der Forschung“

- Definition Architektur
- **Identitätsmanagementsysteme**
- Datenmodelle für Datenbanken
- Verzeichnisdienste und LDAP
- **Grundlagen zur Datenintegration**
- Sicherheit von IT-Systemen
- Authentifizierungsverfahren
- **Autorisierungsmodelle**
- Architekturansätze für Identitätsmanagementsysteme
- Serviceorientierte Architekturen
- Standards für föderierte Identitätsmanagementsysteme
- Initiativen für föderierte Identitätsmanagementsysteme
- Workflowmanagement

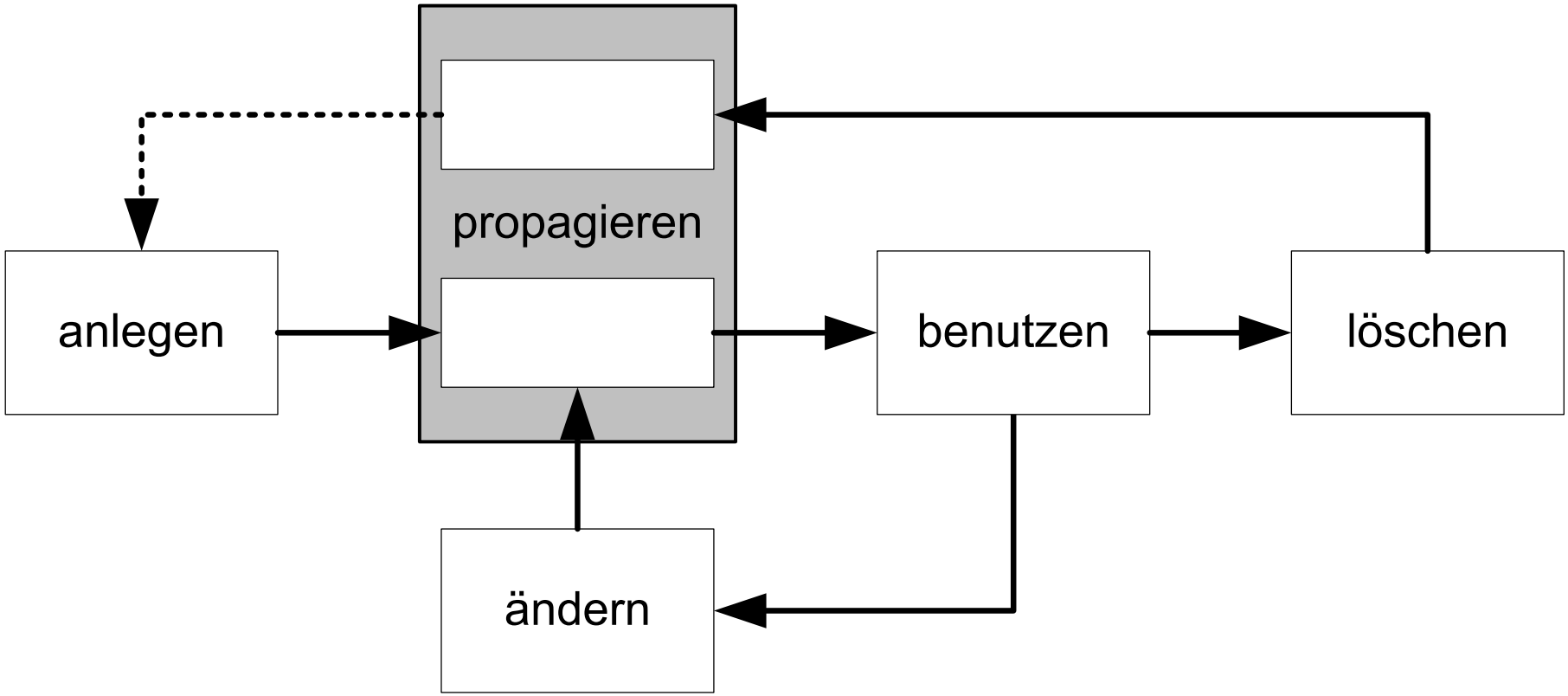
Definition: Identität

- ***Identität:***

  „A digital identity contains data that uniquely describes a person or thing […] but also contains information about the subject's relationships to other entities." *

* Windley, Phillip J. (2005): *Digital Identity (Seite 8).* Beijing u. a.: O'Reilly Media.

Lebenszyklus einer Identität



Themen in „Grundlagen und Stand der Forschung“

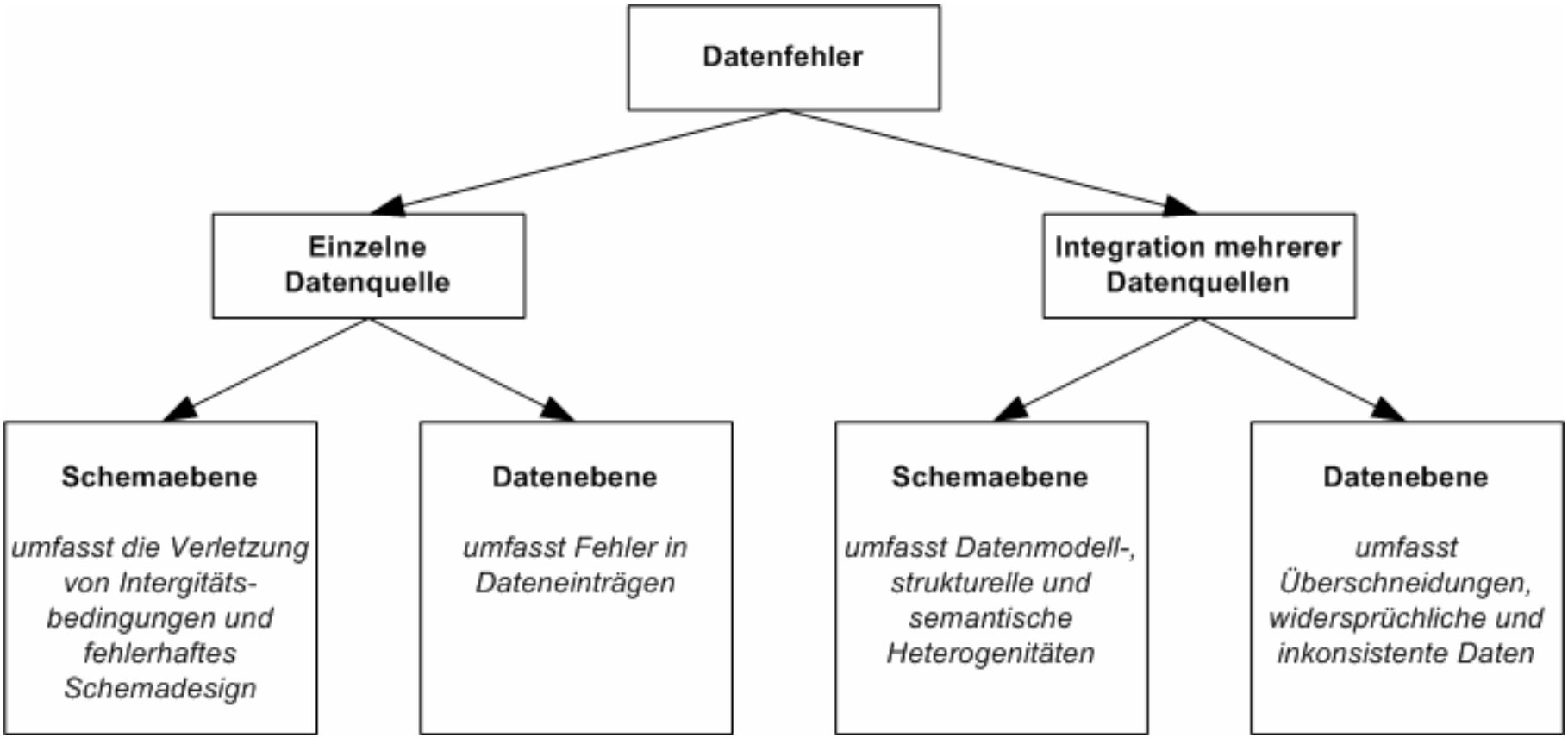
- Definition Architektur
- **Identitätsmanagementsysteme**
- Datenmodelle für Datenbanken
- Verzeichnisdienste und LDAP
- **Grundlagen zur Datenintegration**
- Sicherheit von IT-Systemen
- Authentifizierungsverfahren
- **Autorisierungsmodelle**
- Architekturansätze für Identitätsmanagementsysteme
- Serviceorientierte Architekturen
- Standards für föderierte Identitätsmanagementsysteme
- Initiativen für föderierte Identitätsmanagementsysteme
- Workflowmanagement

Problemfelder der Datenintegration

- Verteilung
- Autonomie
- Heterogenität

→ Transparenz

Datenfehler



Duplikatenerkennung

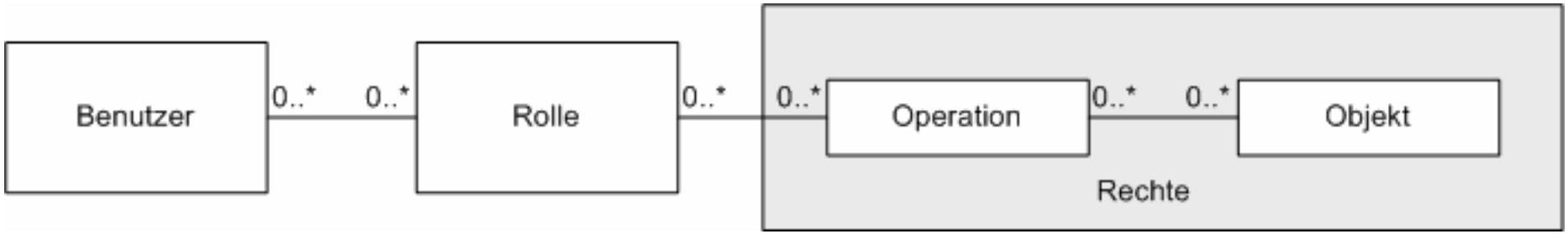
Ähnlichkeitsmaße

- Editierabstände
  - Hamming-Distanz (Strings gleicher Länge)
  - Levenshtein-Distanz (Problem Abkürzungen)
- Tokenbasierte Ähnlichkeitsmaße
  - Jaccard Ähnlichkeit
  - Term-Frequency/Inverse-Document-Frequency (TFIDF)
- Phonetische Ähnlichkeitsmaße

Themen in „Grundlagen und Stand der Forschung“

- Definition Architektur
- **Identitätsmanagementsysteme**
- Datenmodelle für Datenbanken
- Verzeichnisdienste und LDAP
- **Grundlagen zur Datenintegration**
- Sicherheit von IT-Systemen
- Authentifizierungsverfahren
- **Autorisierungsmodelle**
- Architekturansätze für Identitätsmanagementsysteme
- Serviceorientierte Architekturen
- Standards für föderierte Identitätsmanagementsysteme
- Initiativen für föderierte Identitätsmanagementsysteme
- Workflowmanagement

Role-Based Access Control (RBAC) - Basiselemente



Role-Based Access Control (RBAC) - Erweiterungen

- RBAC0 → Basismodell
- RBAC1 → Erweiterung um Hierarchien (generelle und limitierte)
- RBAC2 → Dynamische und statische „Separation Of Duty“ (SoD)
- RBAC3 → RBAC1 + RBAC2

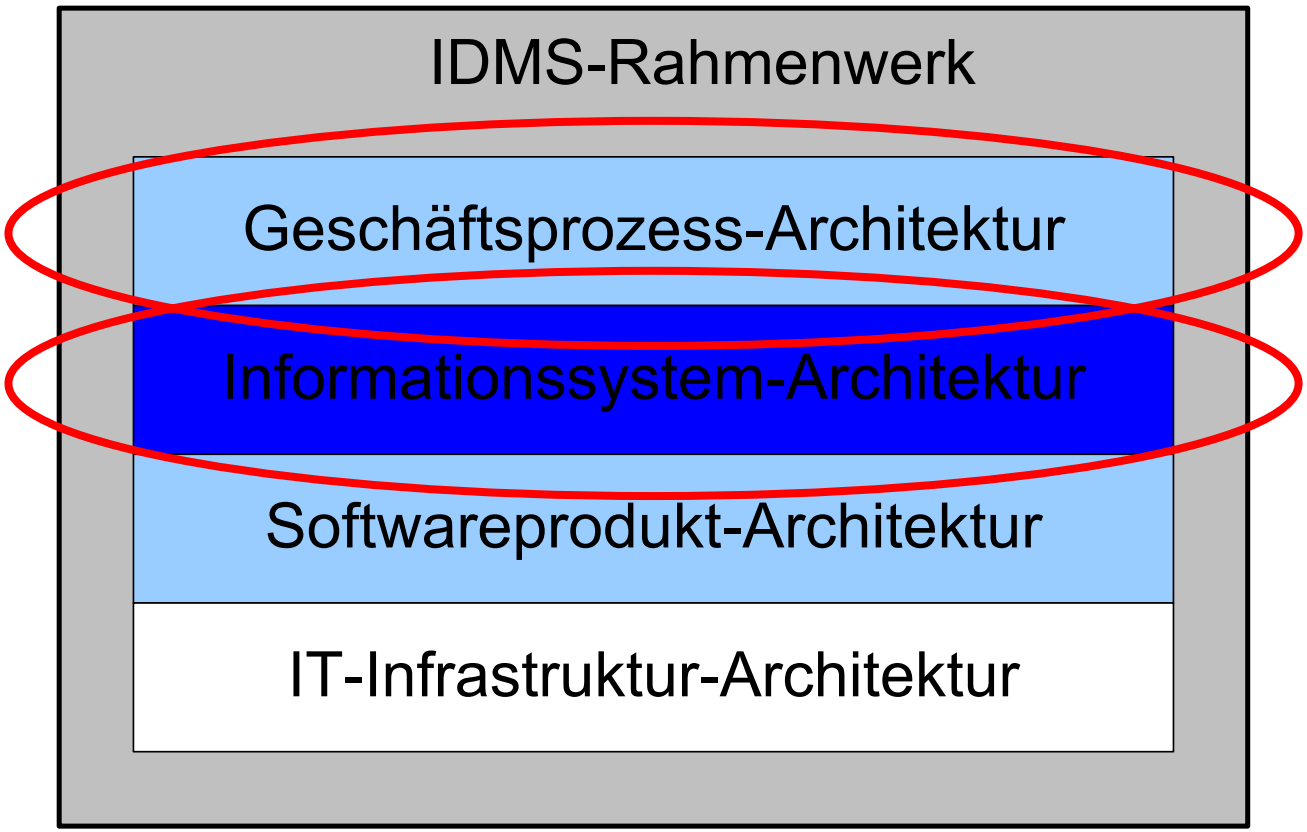
Role-Based Access Control (RBAC) – Gruppen vs. Rollen

- ***Rolle:***
  - Zusammenfassung von Rechte
  - Name/Beschreibung geben die Funktion innerhalb des Anwendungskontextes wieder
- ***Gruppe:***
  - Ausschließlich Strukturierungshilfe
  - dient der Gruppierung von Benutzern, Rollen oder Rechten und stellt keine Beziehung zwischen diesen drei Elementen her.

Themen in „Rahmenbedingungen“

- Organisatorische Strukturen
- Technische Strukturen
- Rechtliche Anforderungen
- Hochschulpolitische Vorgaben und Rahmenbedingungen

IDMS-Rahmenwerk



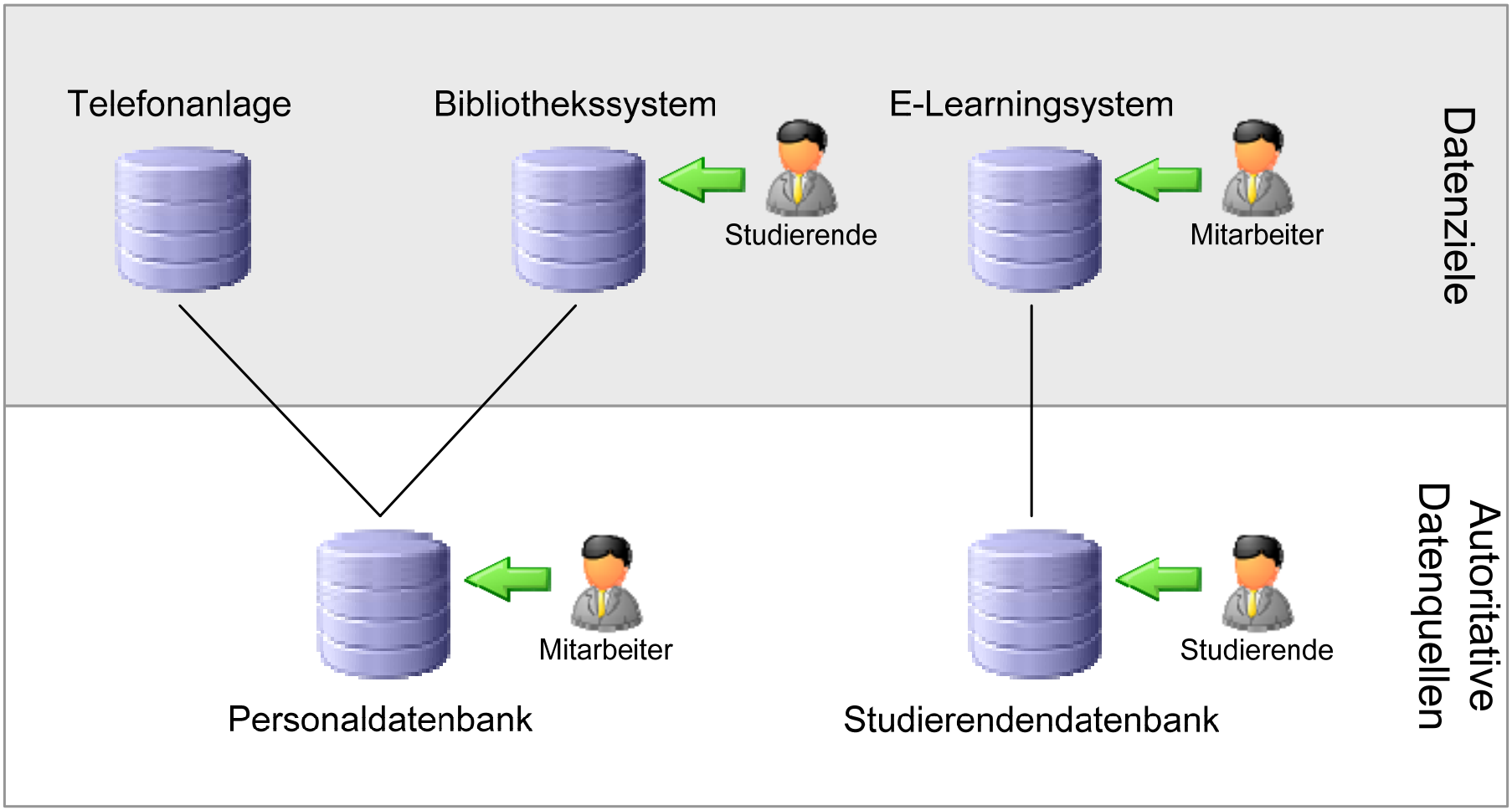
Ziele der Geschäftsprozess-Architektur

- Verfahren zur Erfassung
- Verfahren zur Bewertung

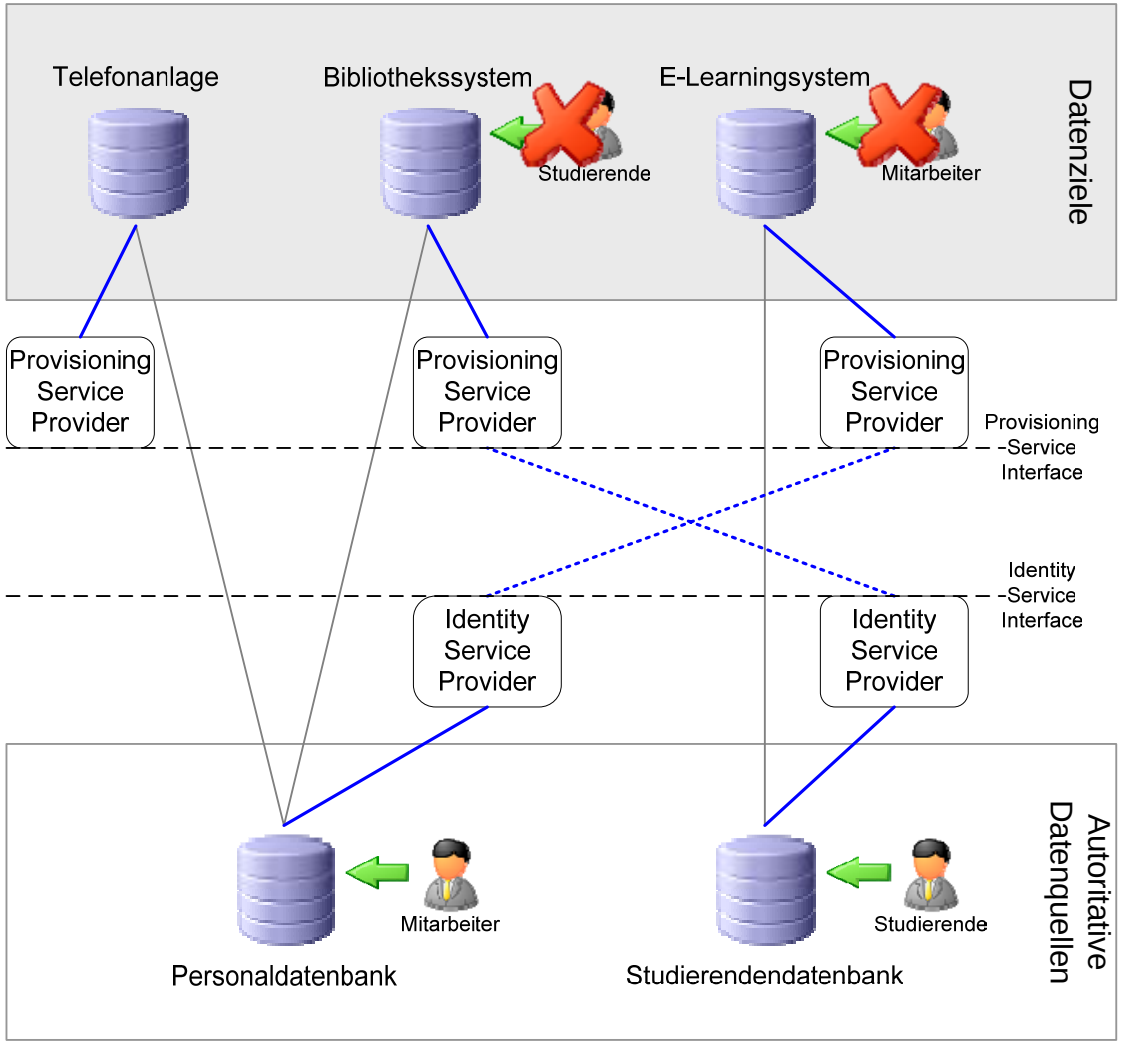
Nutzung der Ergebnisse der Geschäftsprozess-Architektur

- Neugestaltung von Prozessen
- Trennung in obligatorische und optionale Systeme
- Festlegung der Sicherheitsanforderungen für IT-Systeme
- Festlegung der involvierten Personen für ein Identitätsmanagementsystem
- Festlegung von Anforderungen an die Informationssystem-Architektur

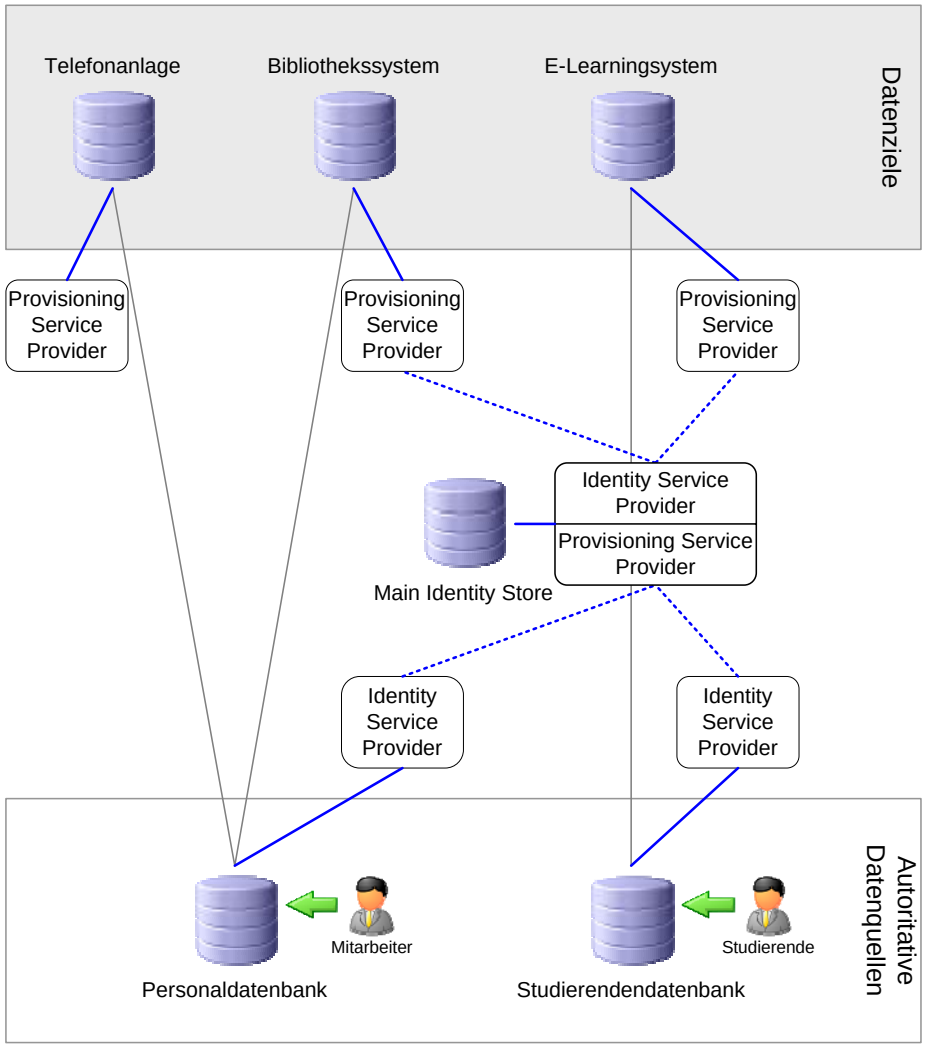
Architekturbeispiel - Ausgangssituation



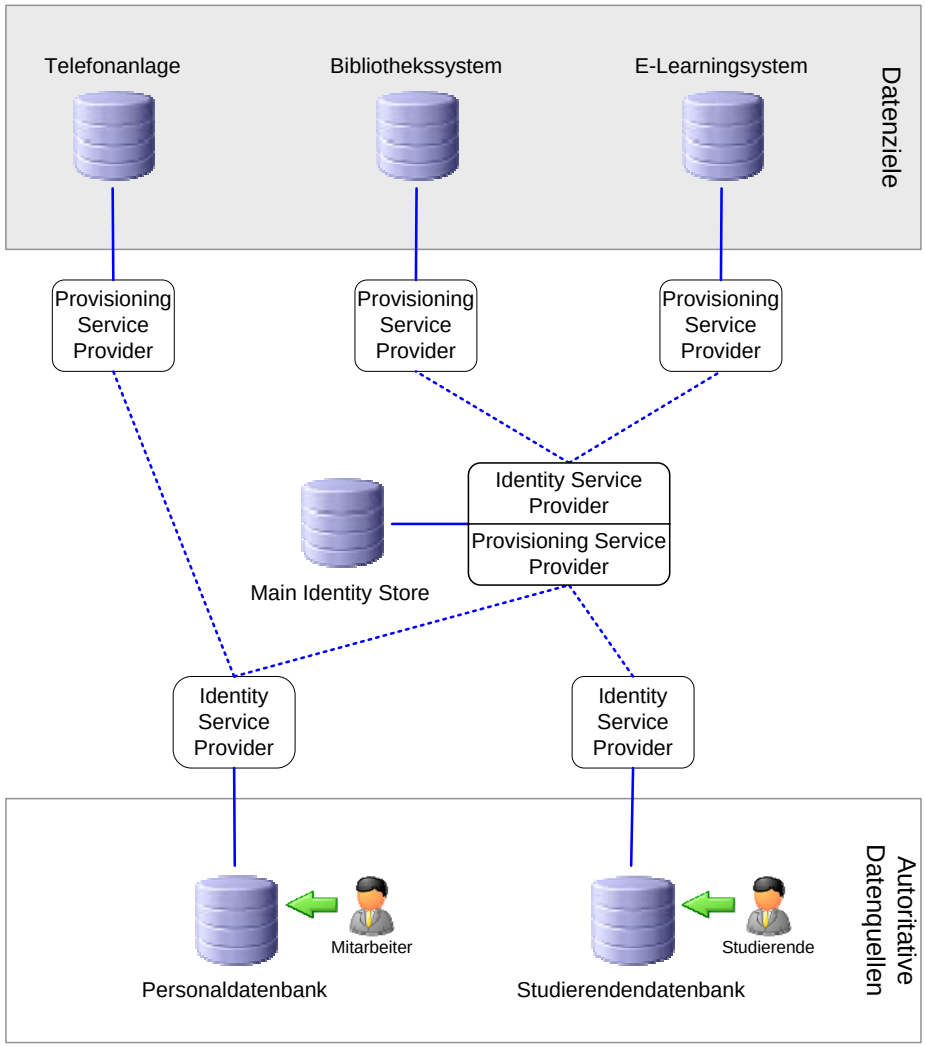
Architekturbeispiel - Erweiterung um Service Provider



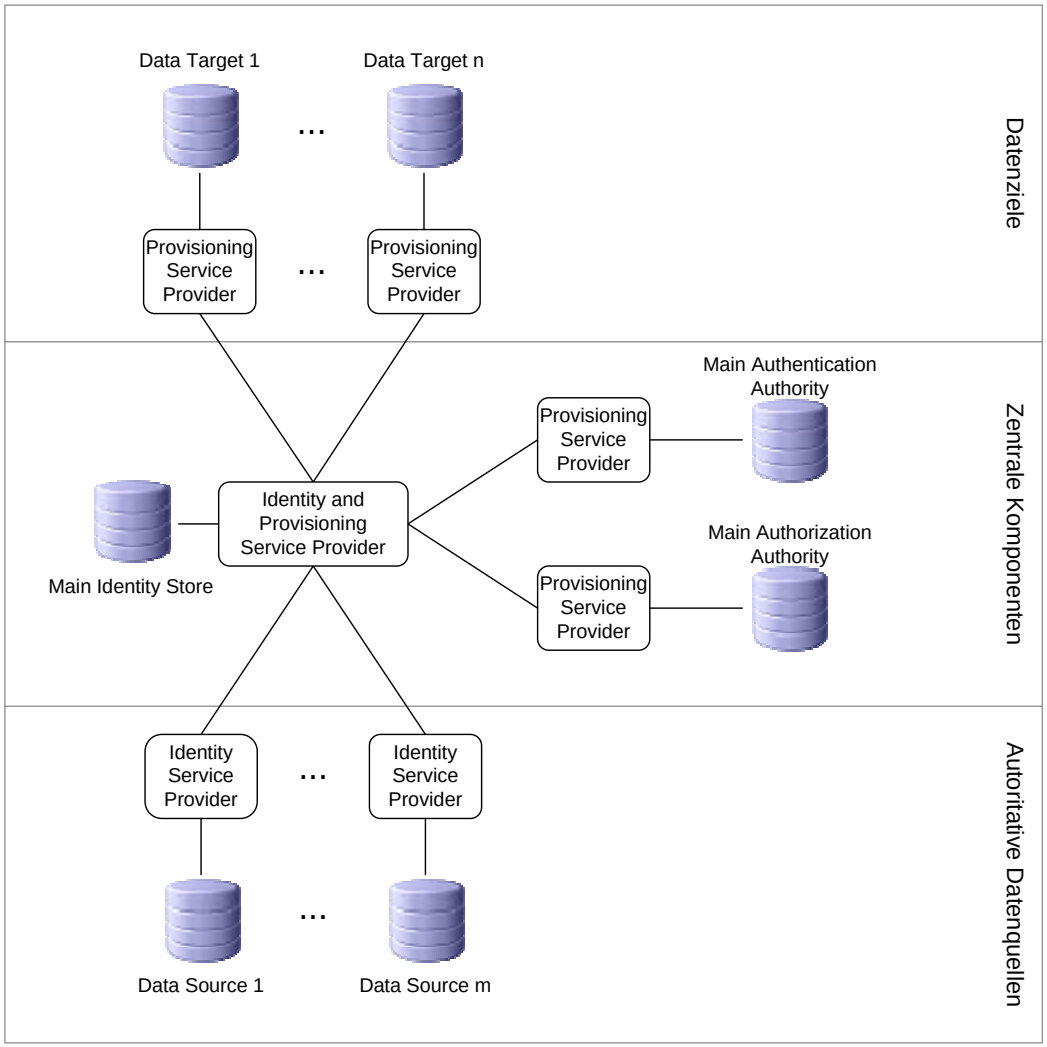
Architekturbeispiel – Main Identity Store



Architekturbeispiel - Vollständig serviceorientierte Architektur



Komponenten der Informationssystem-Architektur



Fazit

- Informationssystem-Architektur schrittweise umsetzbar in bestehende Architektur an einer Hochschule
- Neue Systeme einfach integrierbar
- Verschiedenste Realisierungsformen der Komponenten
- Austausch bestehender Systeme einfach
- Nicht nur für Hochschulen geeignet

Ausblick

- Umsetzung der Informationssystem-Architektur an der Freien Universität Berlin
  → Projekt „FUDIS“ (FU Directory- and Identity Service)
- Teilweise eigene Implementierung der Komponenten

Ende

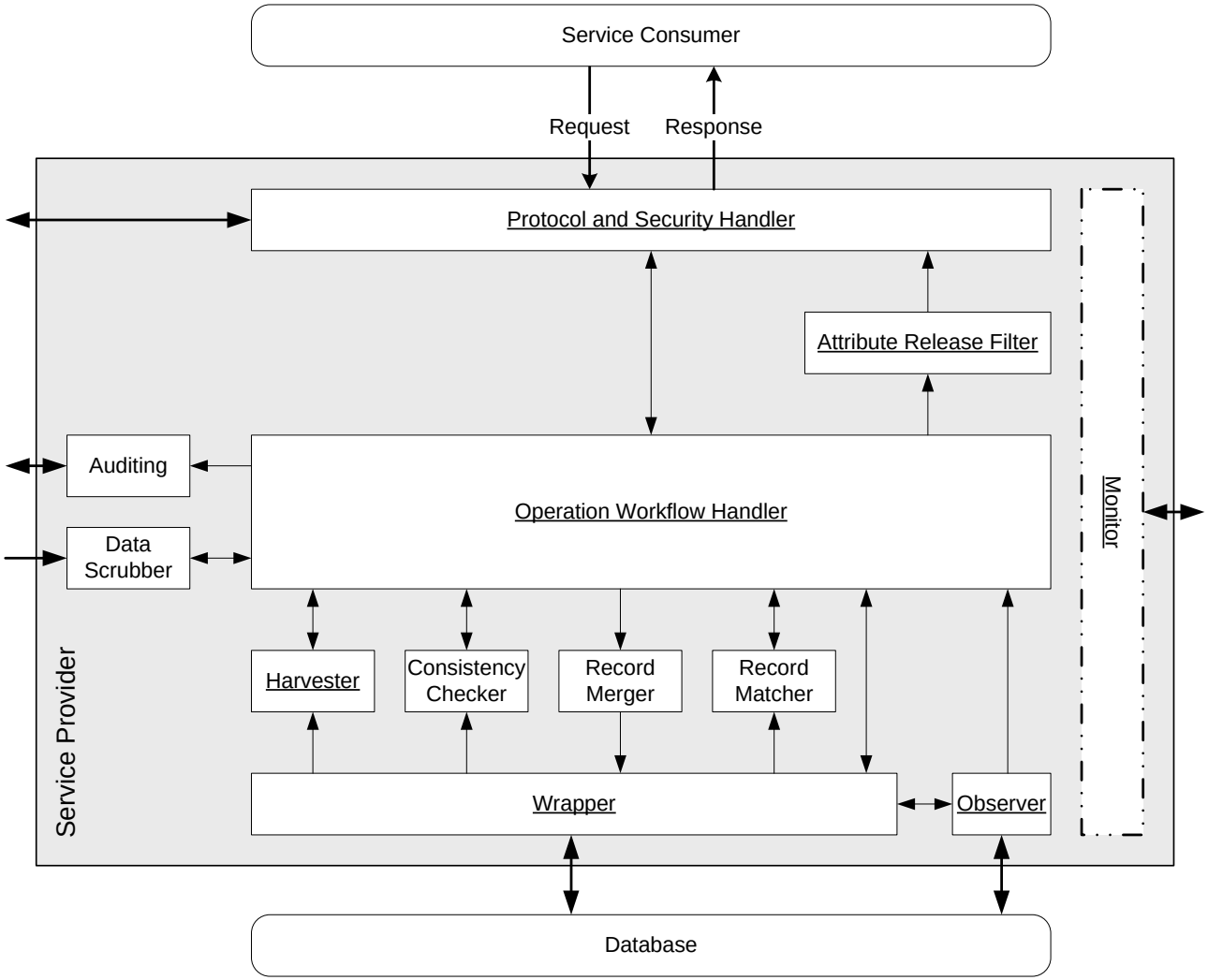
Vielen Dank für Ihre Aufmerksamkeit!

??? Fragen ???

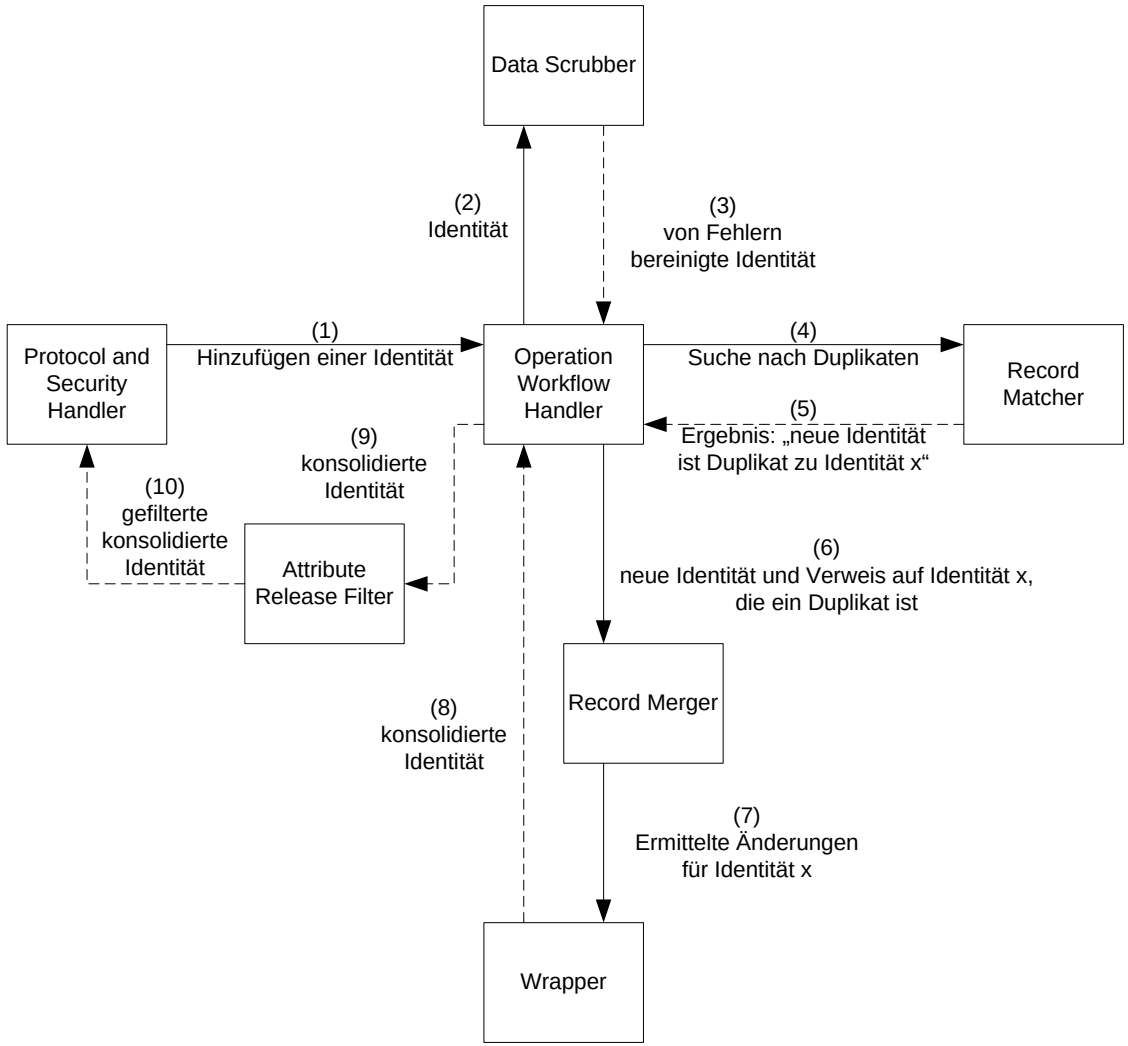
E-Mail: steffen.hofmann@fu-berlin.de
Telefon: 030 / 838-56031

Download der Diplomarbeit unter
http://www.zedat.fu-berlin.de/FUDIS/

Identity and Provisioning Service Provider (IPSP)



Vorgänge im IPSP beim Hinzufügen einer Identität mit Duplikat



Auszüge des ERD vom Main Identity Store