Identity-Management in den Hamburger Hochschulen ... ... und ihren Bibliotheken!

Dr. Stefan Gradmann
Universität Hamburg / Regionales Rechenzentrum
stefan.gradmann@rrz.uni-hamburg.de
www.rrz.uni-hamburg.de/RRZ/S.Gradmann

Übersicht

- Das Projekt eCampus I und die AG Basisdienste
- Konzeption für ein gemeinsames Identity-Management der Hamburger Hochschulen
- Einbindung der Bibliotheken?!
- Umsetzung: eCampus II

eCampus I

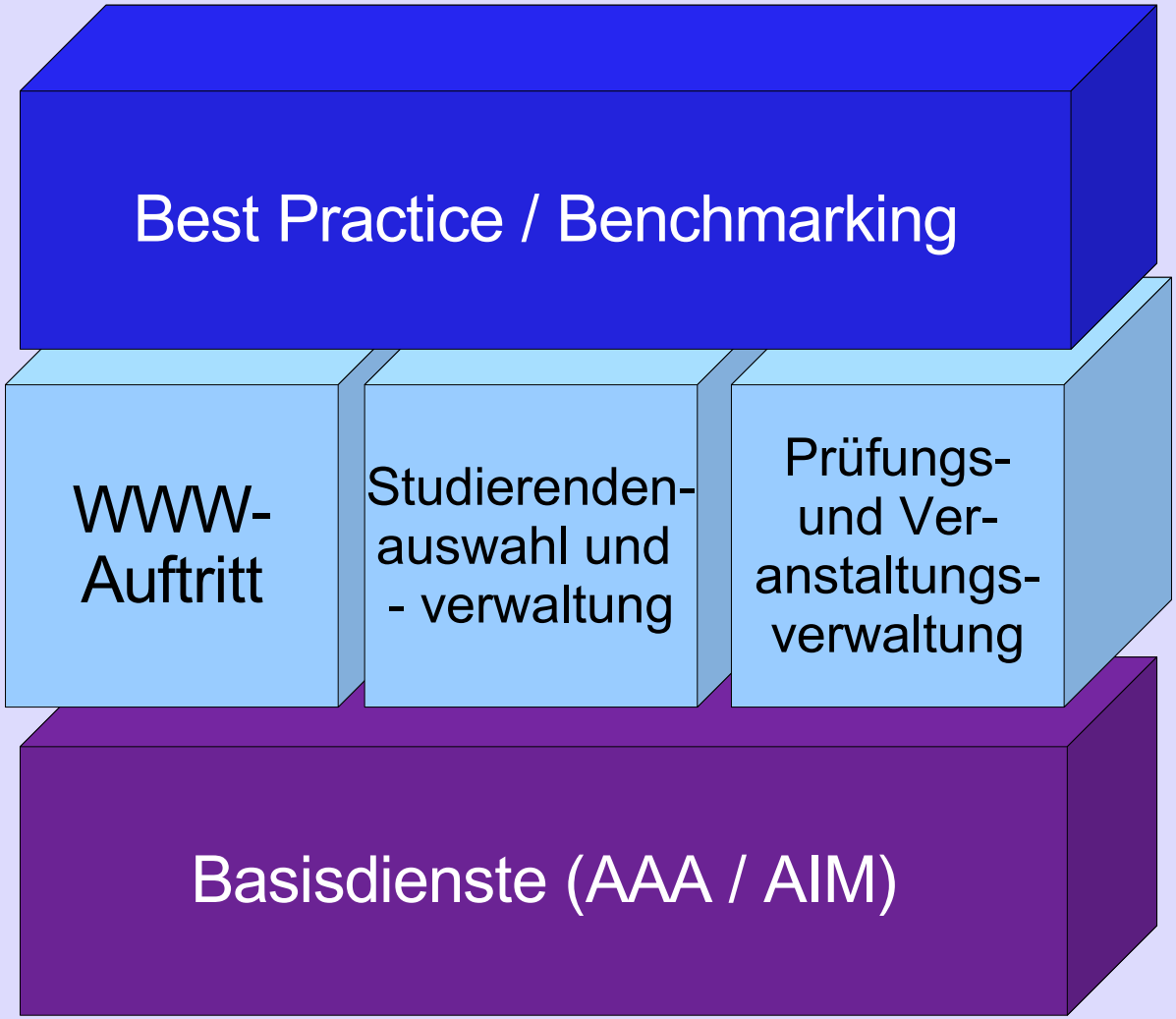
- Projekt der öffentlichen Hamburger Hochschulen und der Behörde für Wissenschaft und Forschung (BWF)
- Oktober 2004 – Dezember 2005
- Kooperations- und Synergiepotentiale ausloten durch:
  - Erfahrungsaustausch zu IT-Infrastrukturen und Services
  - Strategieentwicklung zu Verfahren, Systemen und Organisationsprozessen
- => Unterstützung von Modernisierungsvorhaben und
- => Interoperabilität und Ressourcensharing

eCampus I: Teilnehmer

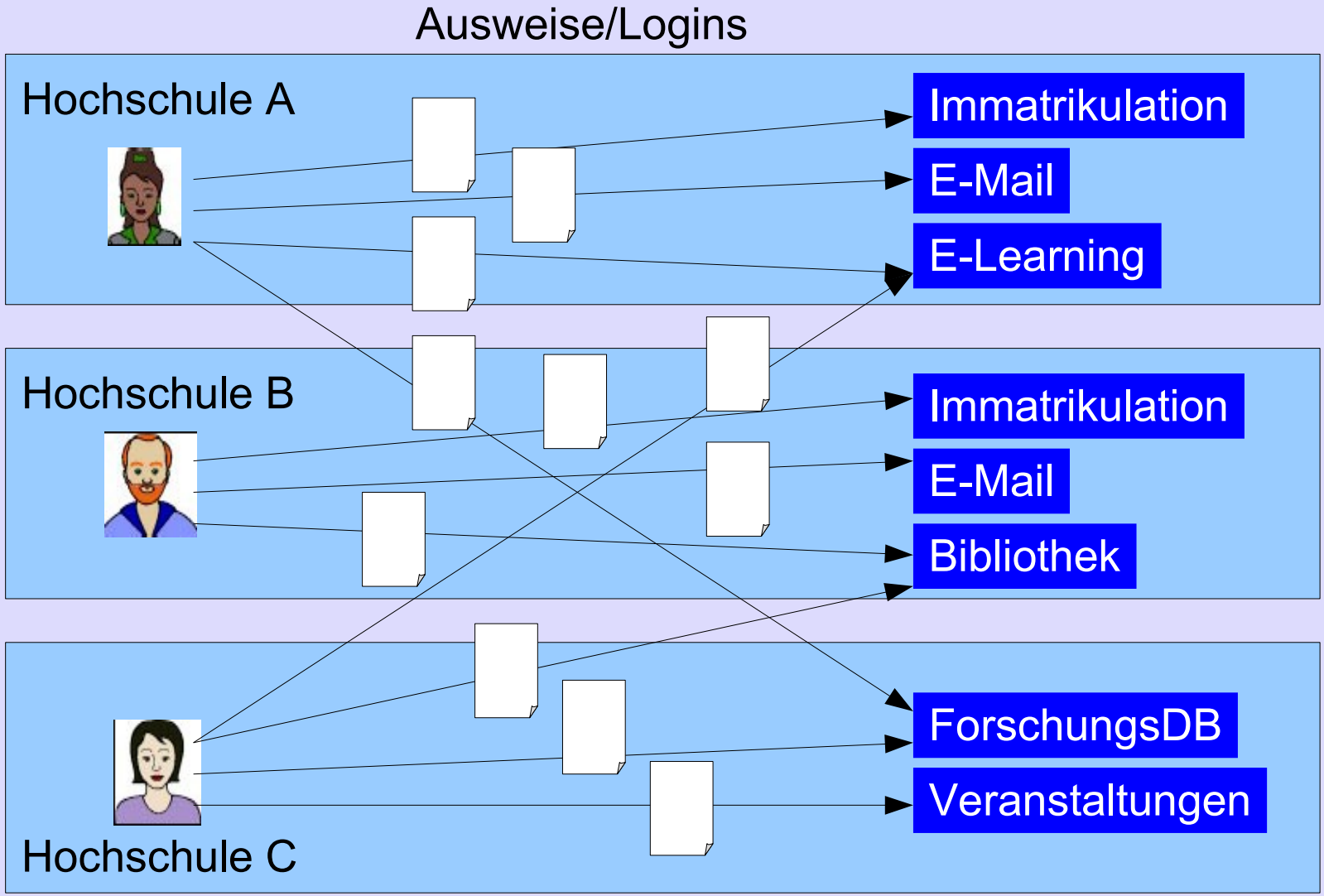
Teilnehmer

- Die Hamburger Hochschulen
  - Hochschule für Angewandte Wissenschaft Hamburg (HAW)
  - Hochschule für Bildende Künste Hamburg (HfbK)
  - Hochschule für Musik und Theater Hamburg (HfMT)
  - Technische Universität Hamburg-Harburg (TUHH)
  - Universität Hamburg (UHH)
  - Hamburger Universität für Wirtschaft und Politik (HWP)
  - Hafen City Universität (HCU)
- BWG/BWF
- MMKH als Geschäftsstelle

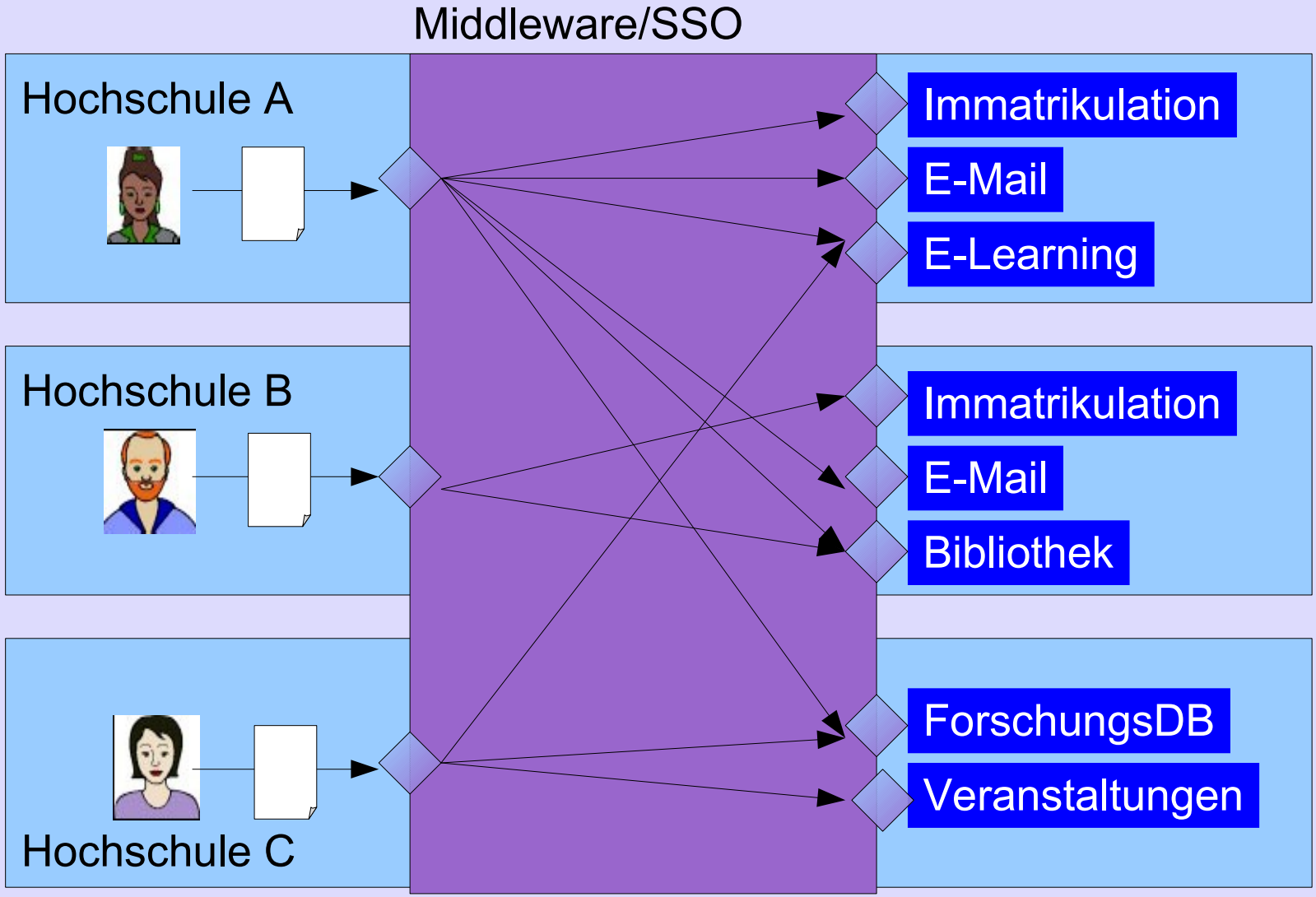
eCampus: Teilprojekte



eCampus: IST-Situation



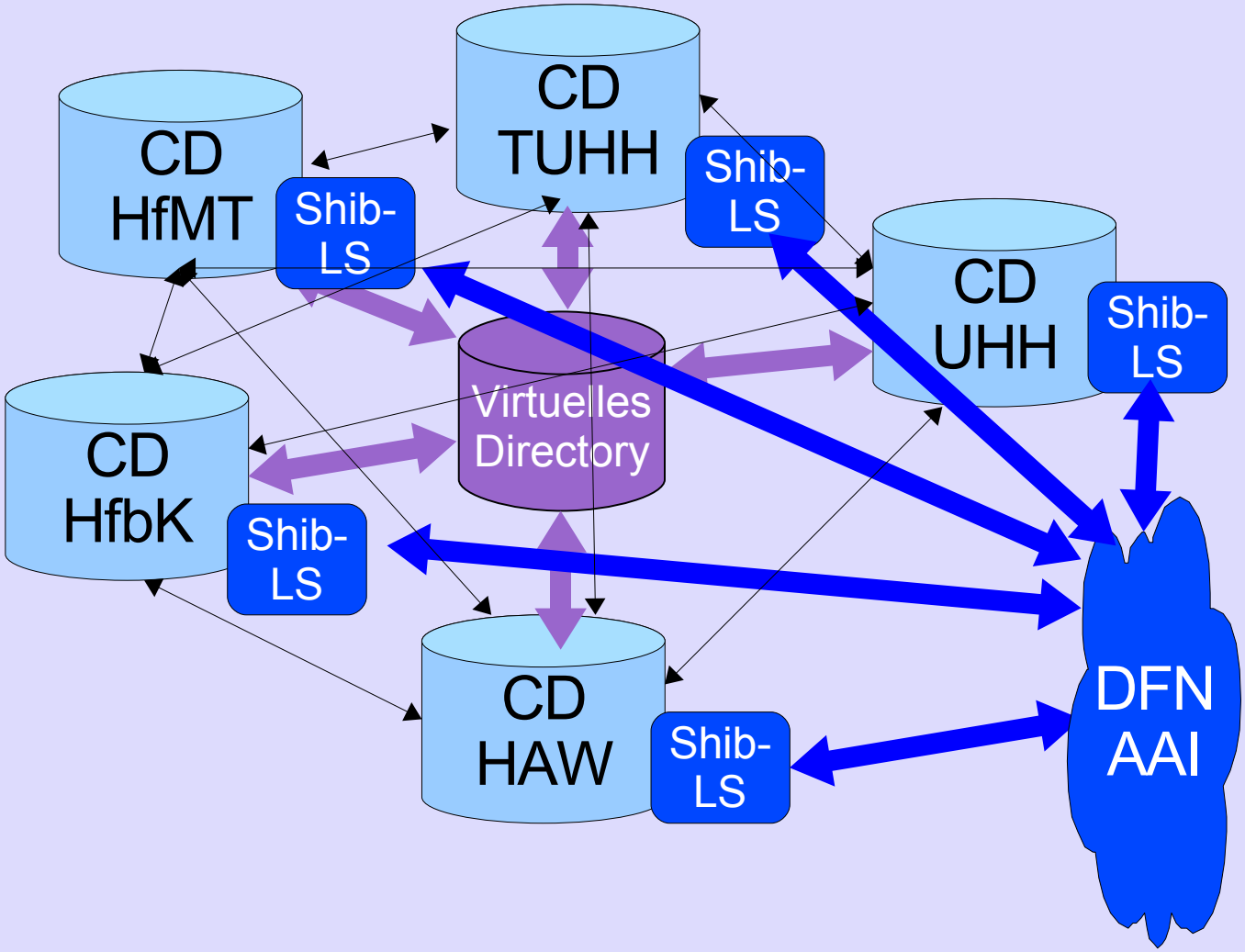
eCampus: SOLL-Situation



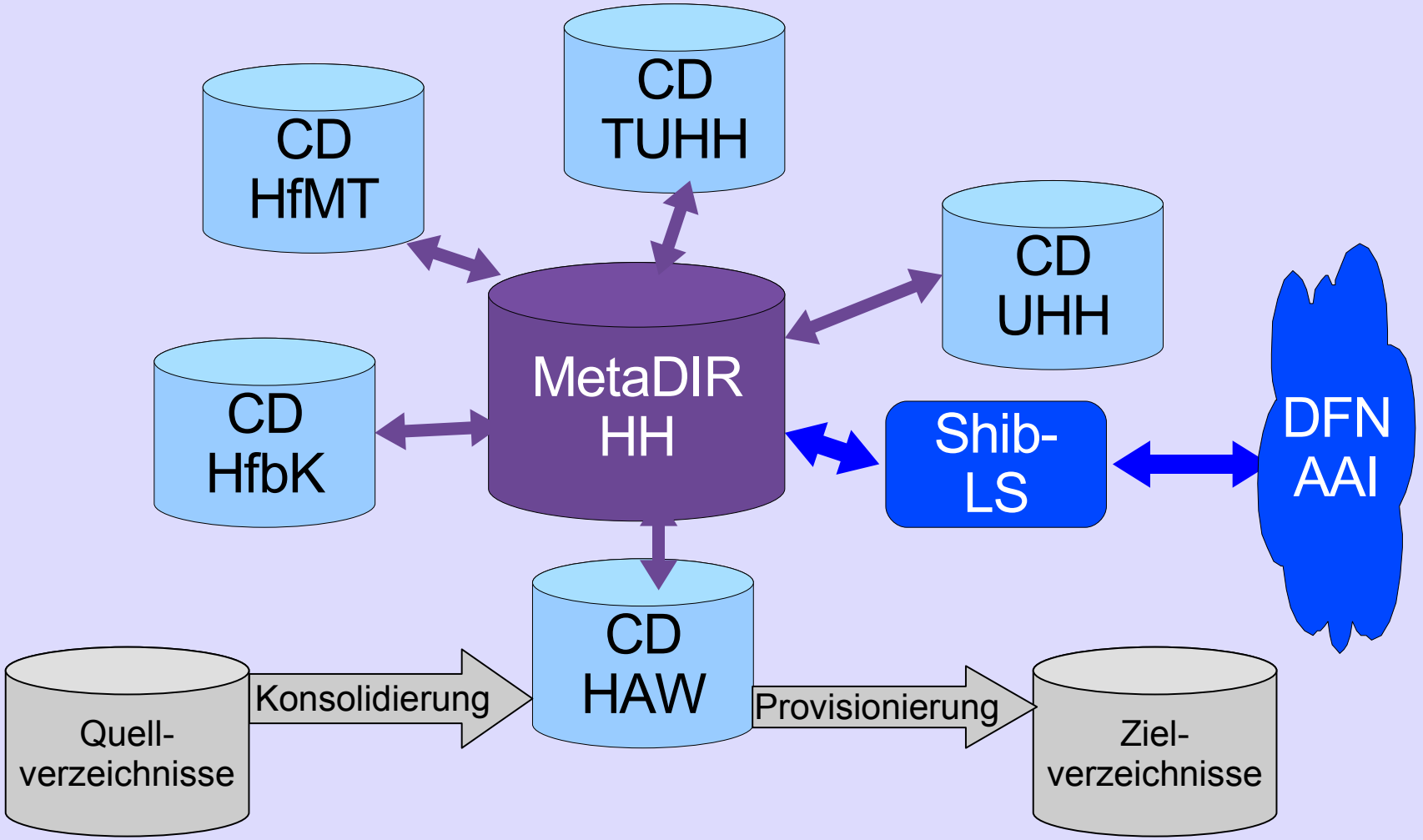
AG Basisdienste: Arbeitsschritte

- Marktsichtung Hersteller: Sun (ID-Manager), Novell (E-Directory), Microsoft (AD/MIIS), Siemens (Dir-X), IBM (Tivoli)
- Kontaktaufnahme zu Authentifizierungsprojekten und verwandten Initiativen im Hochschulumfeld: SWITCH-AAI, UB Freiburg (BMBF/AAR), Universität Oldenburg (Siemens), Niedersachsen (SOI), NRW (IBM), Géant2/Terena, CI-NSF (Atkins), JISC, EGG …
- Lösungsanbieter: Dataport, DFN-Verein
- Standards: LDAP/LDIF, SAML (Liberty/Shibboleth), SOAP …
- Stand an den Hochschulen
- Festlegungen und Spezifikationen: hhEduPerson, Identifier, Architekturmodell IDMS, Definition Umsetzungsprojekt

IDM: Architekturoptionen 1

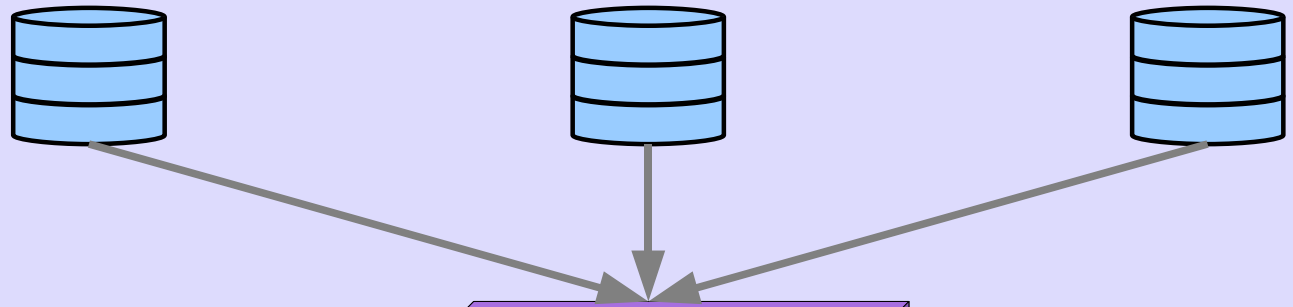


Architekturoptionen 2



IDMS: Funktionsprinzipien 1

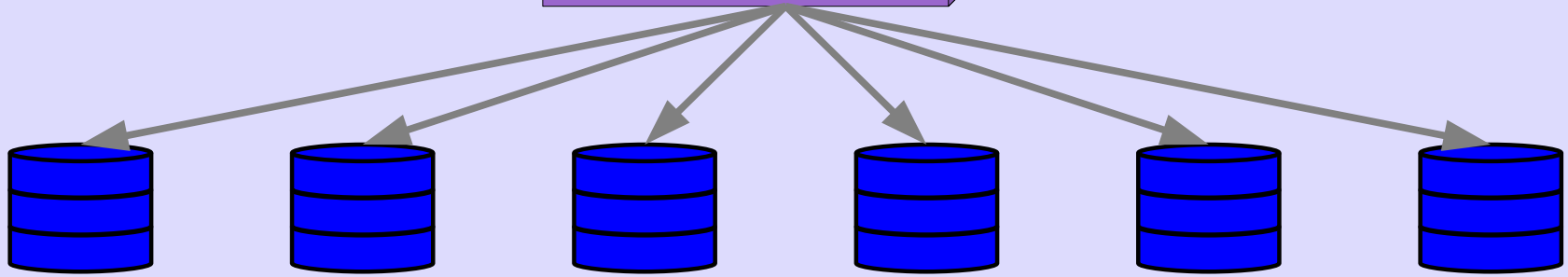
Quellsysteme: Personaldatenverwaltung, Studierendendatenverwaltung, LBS etc.



Identity Management System verhält sich nach außen wie eine Black Box. Zutritt nur für besonders Autorisierte.

IDMS (Konsolidierung Provionierung)

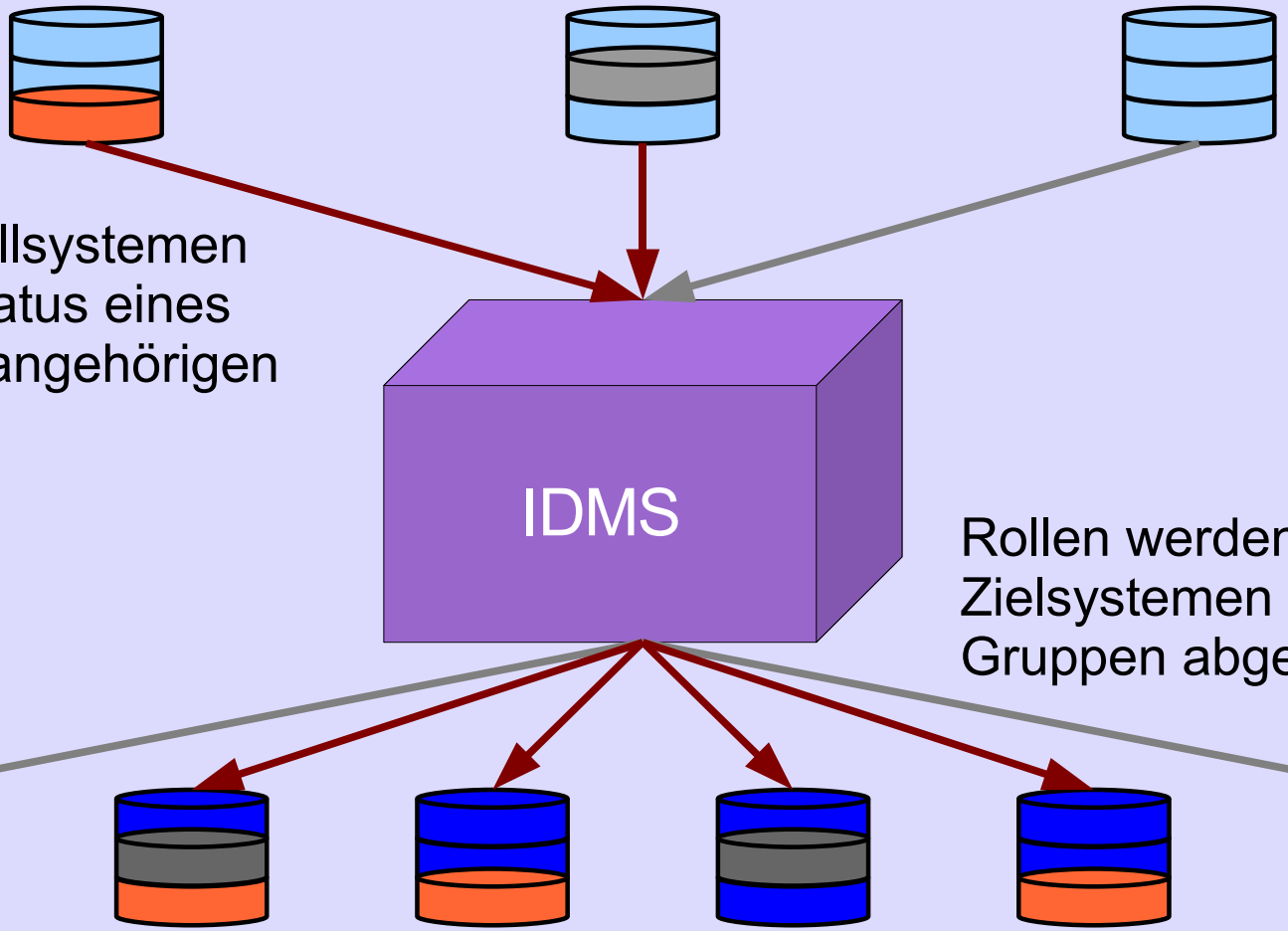
Rollen müssen korrekt abgebildet und in Zugriffsrechte umgesetzt werden.



Zielsysteme: LDAP-CD, Dateisystem, Datenbanken, Bibliothekssystem etc.

IDMS: Funktionsprinzipien 2

Quellsysteme: Personaldatenverwaltung, Studierendendatenverwaltung, LBS etc.



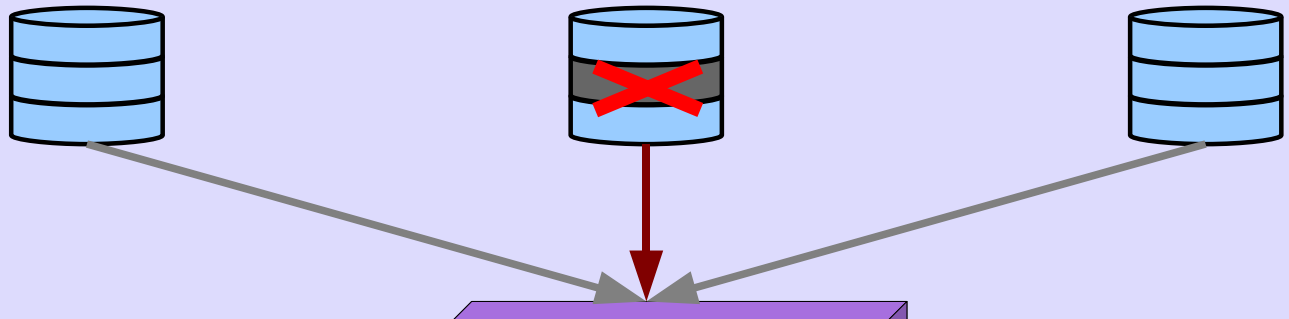
In den Quellsystemen wird der Status eines Hochschulangehörigen verwaltet.

Rollen werden in den Zielsystemen auf Gruppen abgebildet.

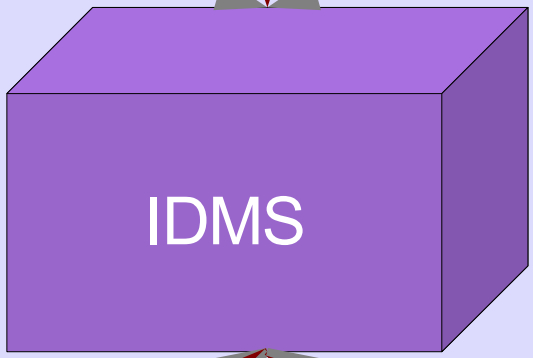
Zielsysteme: LDAP, Dateisystem, Datenbanken, Bibliothekssystem etc.

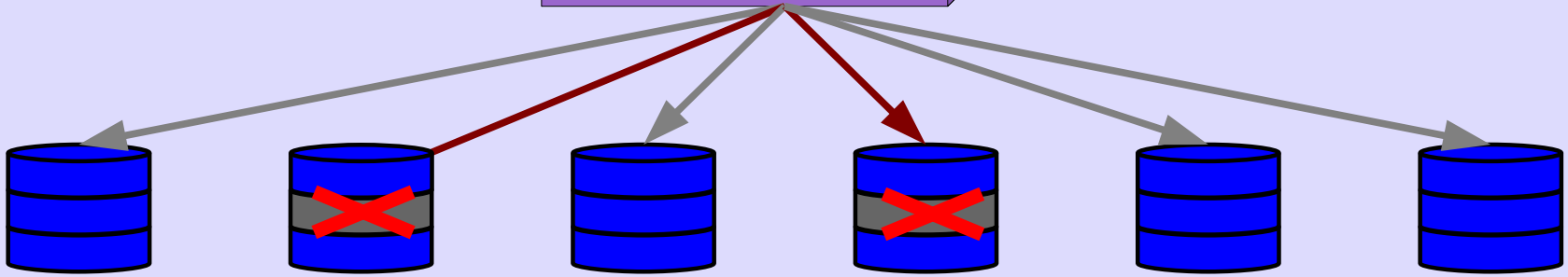
IDMS: Funktionsprinzipien 3

Quellsysteme: Personaldatenverwaltung, Studierendendatenverwaltung, LBS etc.



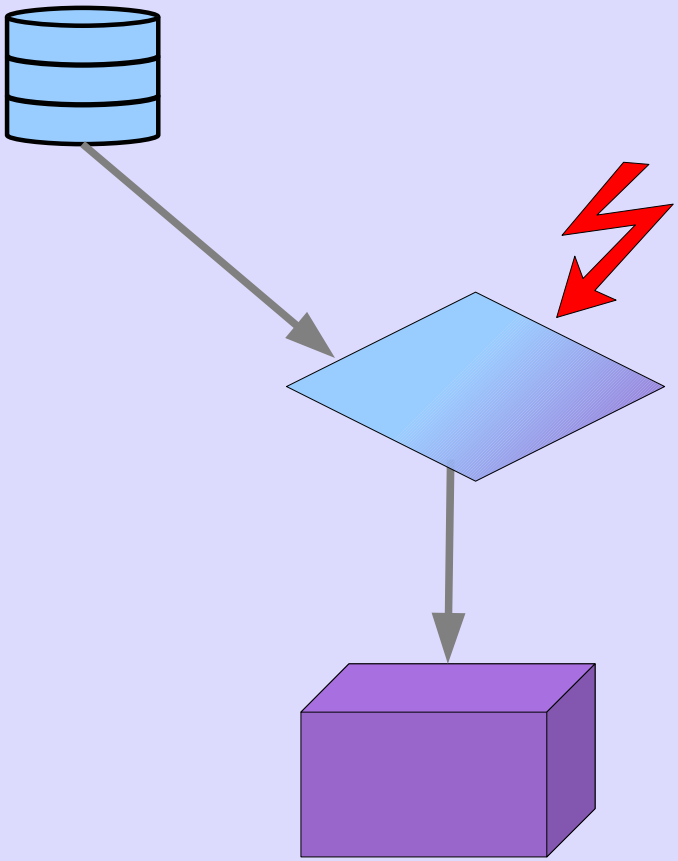
In allen angeschlossenen Systemen können Sperrungen zuverlässig umgesetzt werden.





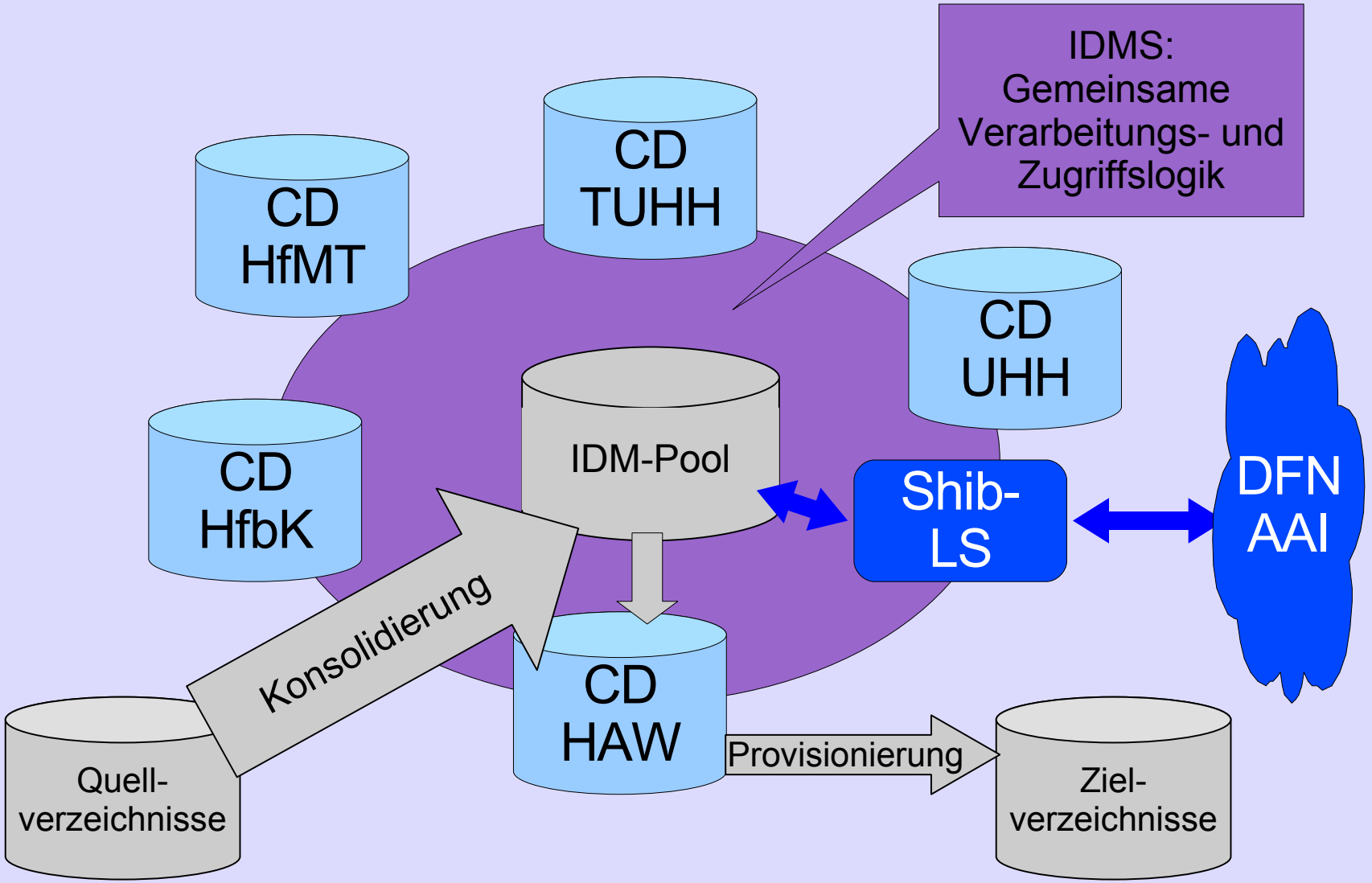
Zielsysteme: LDAP, Dateisystem, Datenbanken, Bibliothekssystem etc.

IDMS: Funktionsprinzipien 4

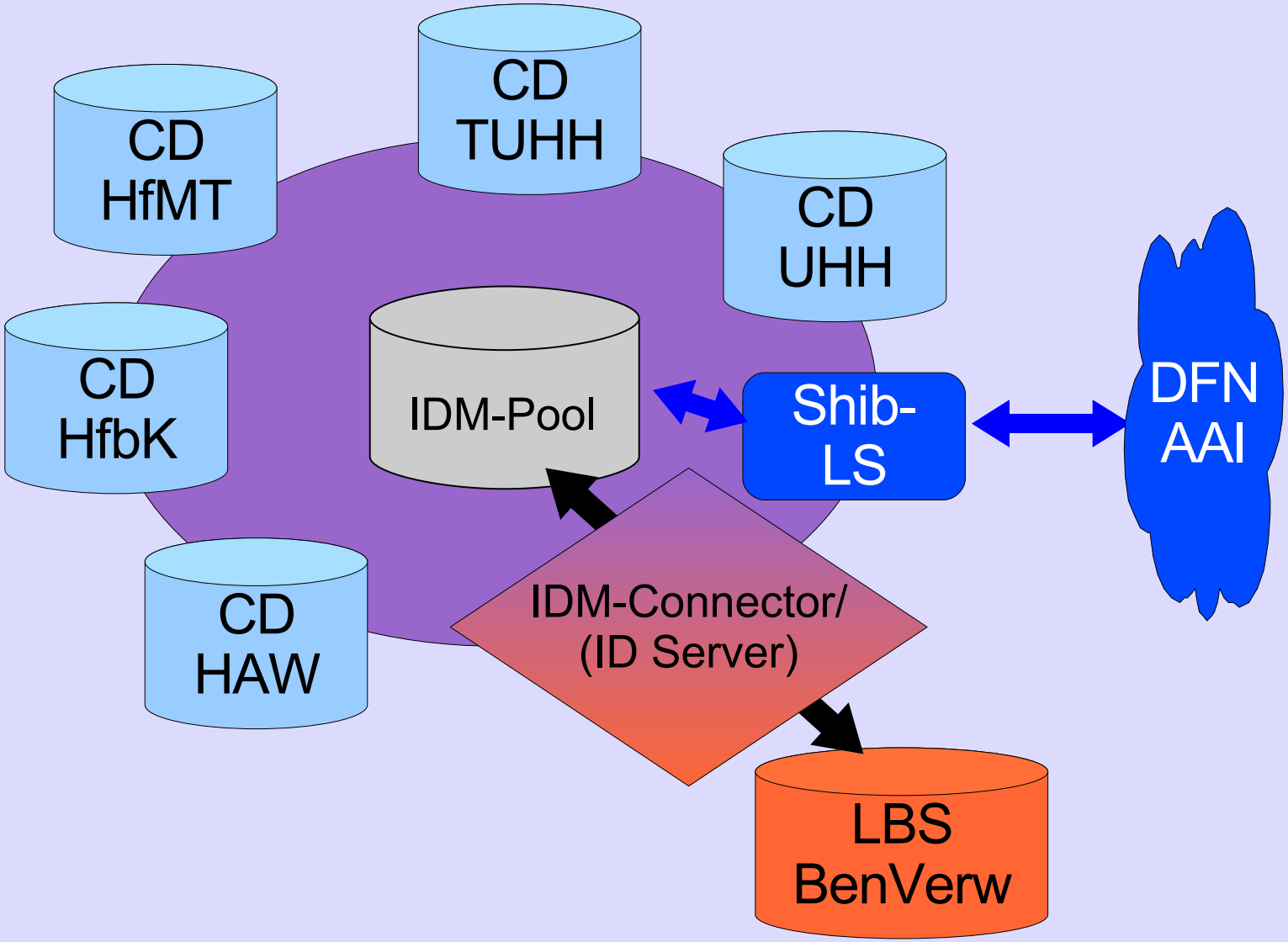


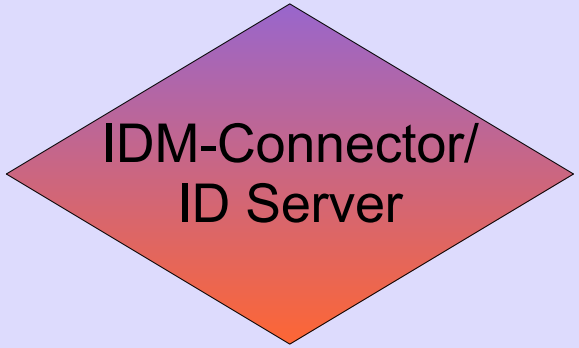
- Konnektoren stellen die Verbindungen von und zu Quell- und Zielsystemen her.
- Sie werden durch Ereignisse ausgelöst.
- Durch Konfigurationen wird bestimmt, welche Daten in welcher Form im- oder exportiert werden.

Architekturoptionen 3



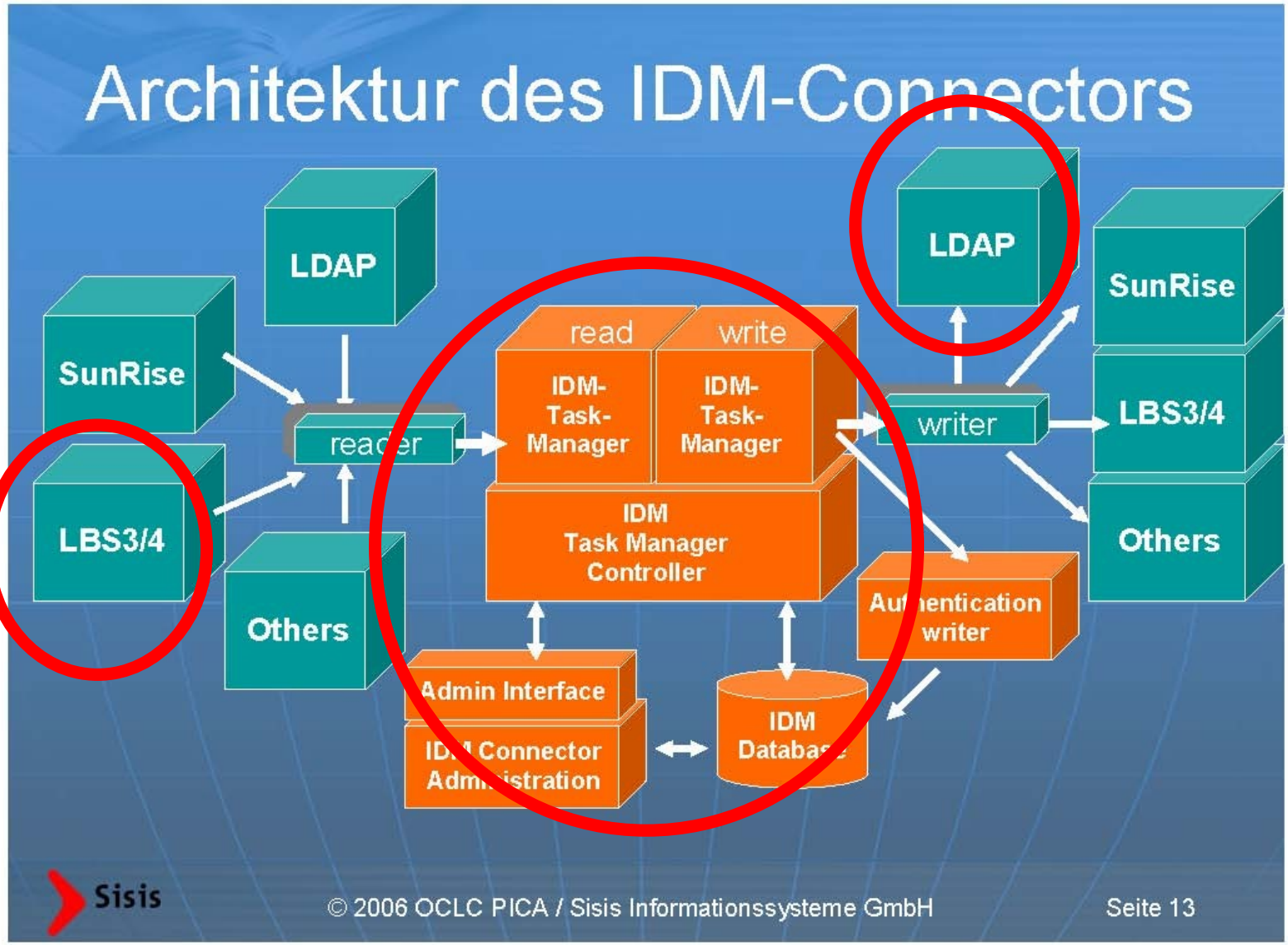
Architekturoptionen 4



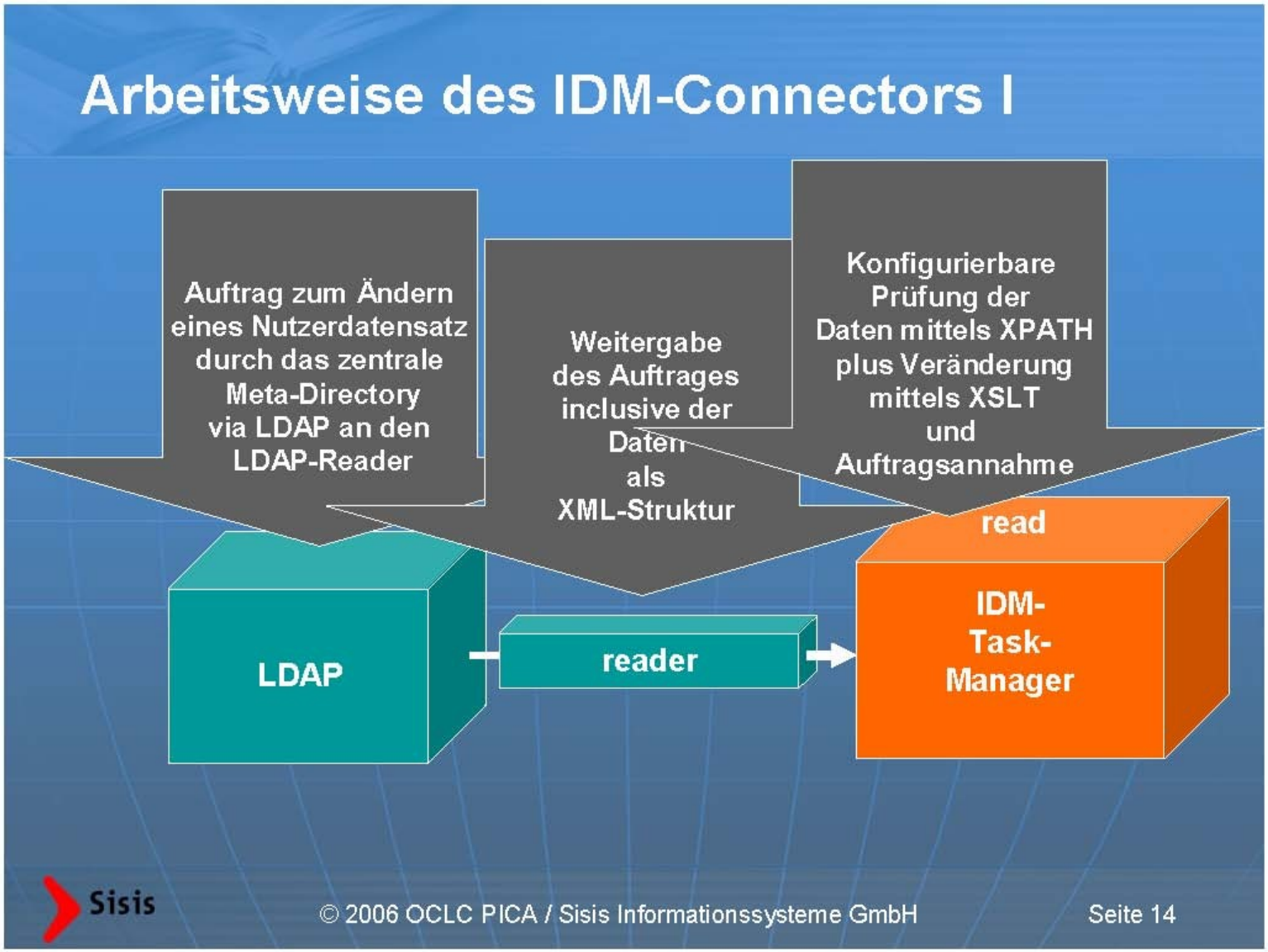


- IDM-Connector
  - Online Synchronisation von Nutzerdaten in LBS/SunRise mit beliebigen Anwendungen
  - Festlegung von Regeln für den Austausch und das Mapping der Daten pro Anwendung
- Identity Server
  - Unterstützung von LDAP für die Authentifizierung im WebOPAC/InfoGuide sowie für SB-Anwendungen
  - Erlaubt den Komponenten des Bibliothekssystems die Authentifizierung eines Nutzers mit seiner globalen oder lokalen ID
  - Dazu verwendet er parametrisierbar seine eigene IDM Datenbank oder den LDAP Dienst des zentralen Meta-Directories
  - Die Kommunikation mit den lokalen Komponenten erfolgt über SLNP und wird mittels Zertifikaten verschlüsselt

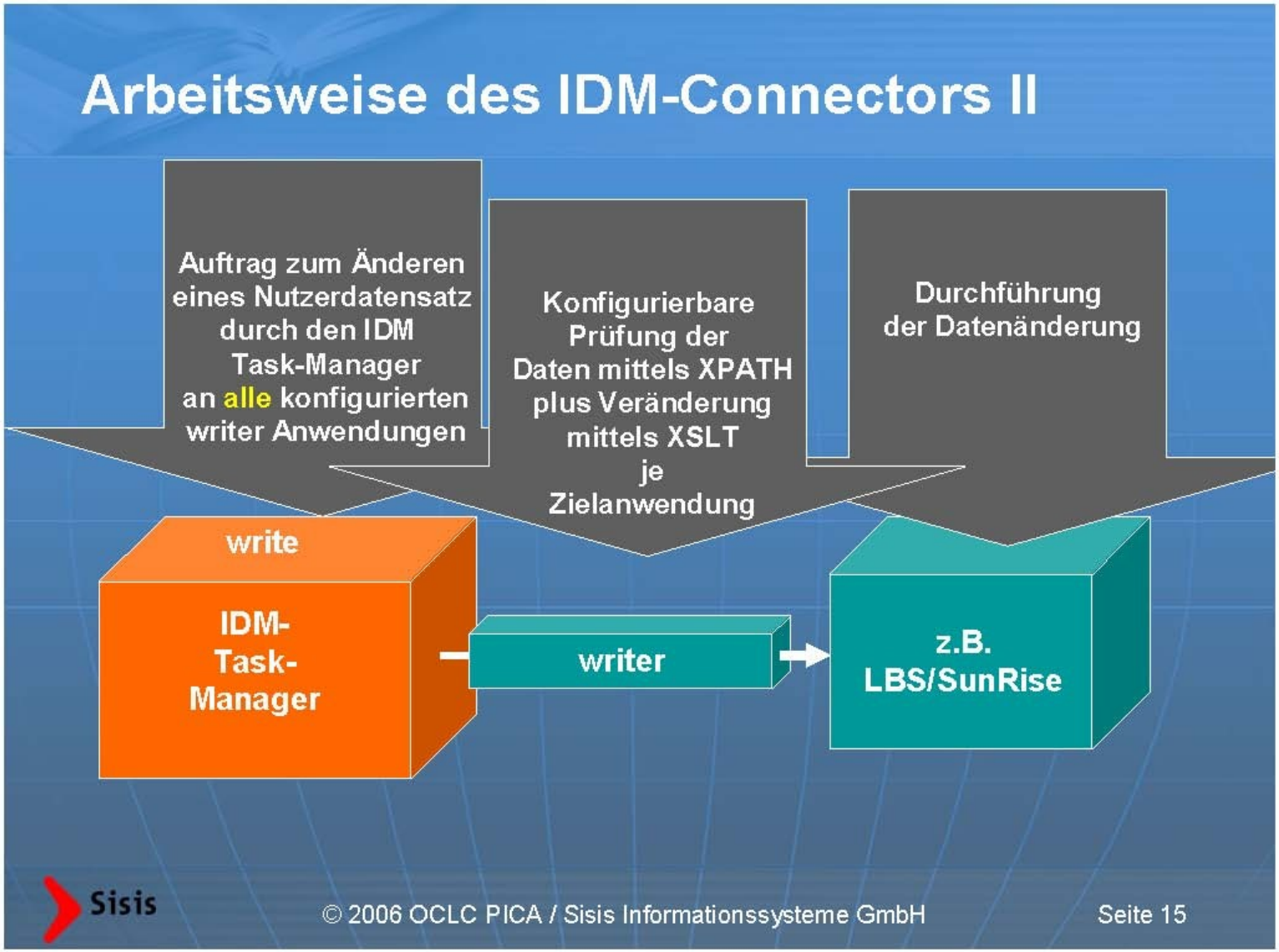
Architektur IDM-Connector



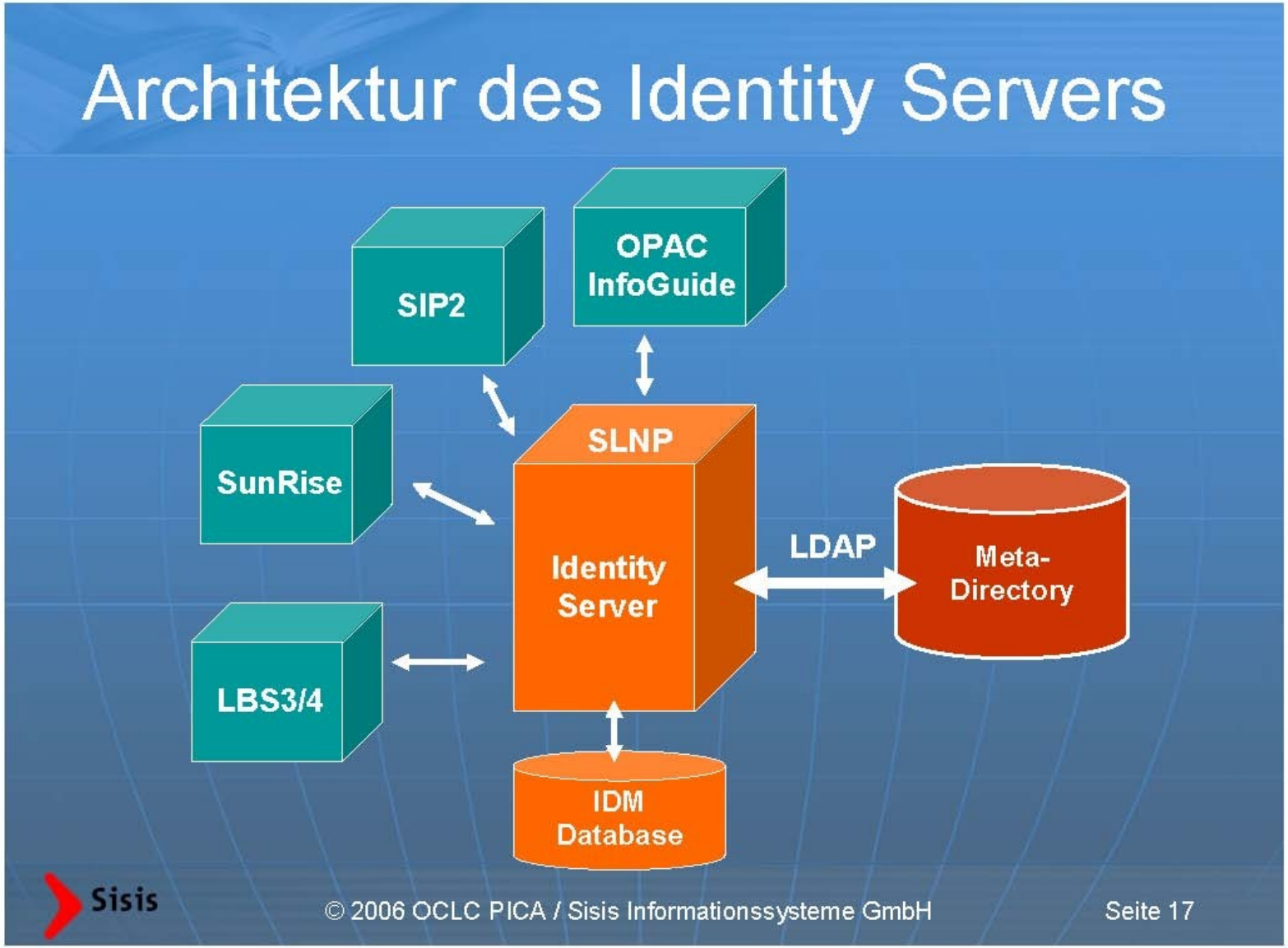
Arbeitsweise I



Arbeitsweise II



Architektur IDS



eCampus II und Schluß

- eCampus II setzt das Konzept für ein gemeinsames IDMS der Hamburger Hochschulen beginnend mit dem 01.11.2006 in einem Zweijahresprojekt um (Volumen: 550.000 €)
- Benefit der gemeinsamen zentralen Lösung soll in drei Bereichen demonstriert werden:
  - Corporate Directory der Hamburger Hochschulen
  - WLAN-Roaming an allen Hamburger Hochschulen
  - **Einbindung der Bibliotheken über eine Pilotimplementierung des IDM-Connectors/-servers**
- Dabei (hoffentlich) erworbenes Know-How geben wir gerne im Verbund weiter
- Charakteristikum unseres Konzeptes ist es, **nicht** die Benutzer-verwaltung des LBS zur führenden Authentifizierungsinstanz zu machen, sondern diese in einen größeren Ansatz für IDMS zu integrieren!