

idm@eCampus.hh

Kooperatives Identity Management in den Hamburger Hochschulen

Prof. Dr. Martin Gennis (HAW),



Dr. Stefan Gradmann (UHH-RRZ),



Stefanie Winklmeier (MMKH)



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: Architekturoptionen
- Umsetzungsprojekt eCampus II
- Nutzen und Synergien
- Warum der hochschulübergreifende Ansatz?

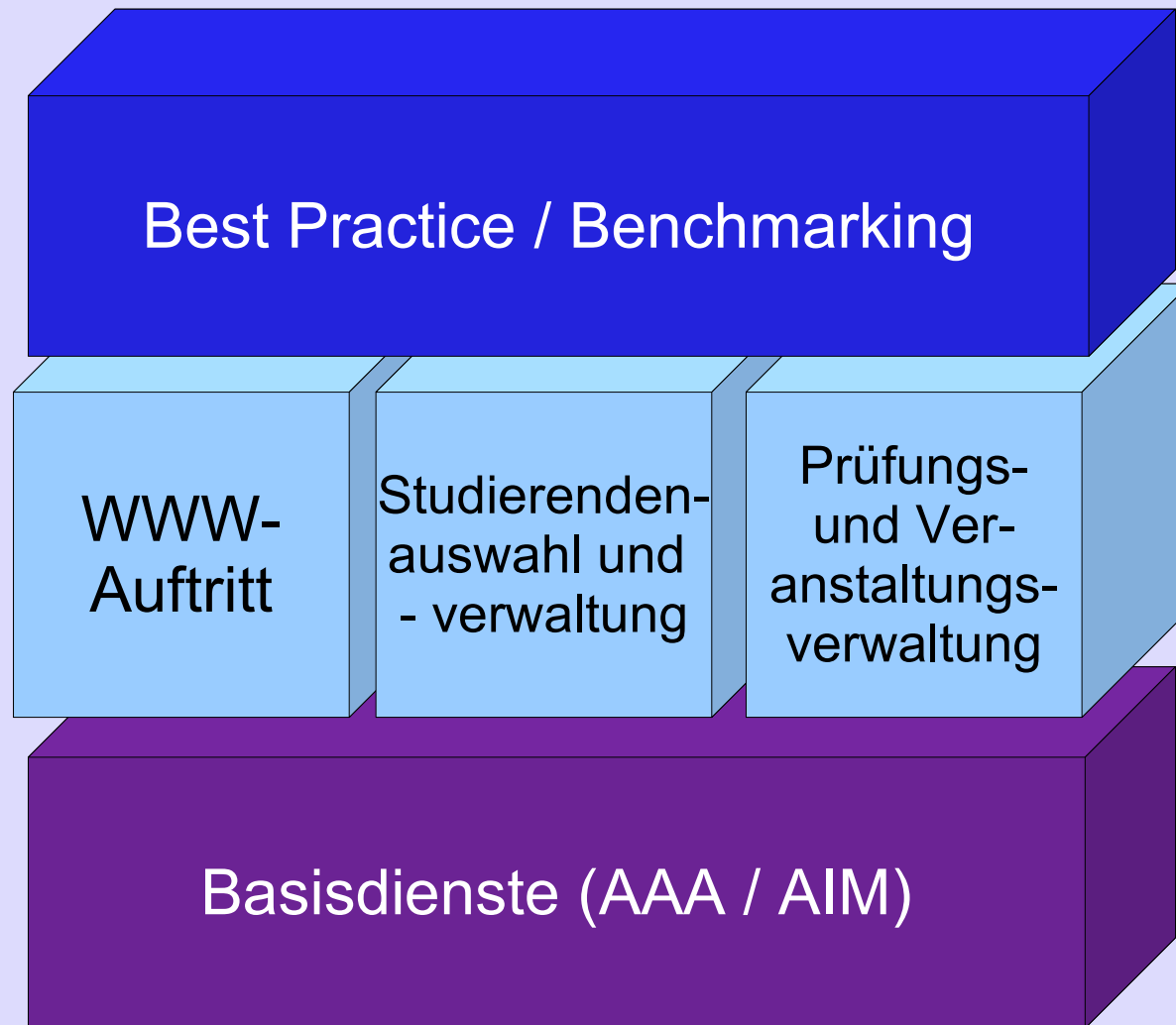


- Projekt der öffentlichen Hamburger Hochschulen und der Behörde für Wissenschaft und Forschung (BWF)
- Oktober 2004 – Dezember 2005
- Kooperations- und Synergiepotentiale ausloten durch:
 - Erfahrungsaustausch zu IT-Infrastrukturen und Services
 - Strategieentwicklung zu Verfahren, Systemen und Organisationsprozessen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

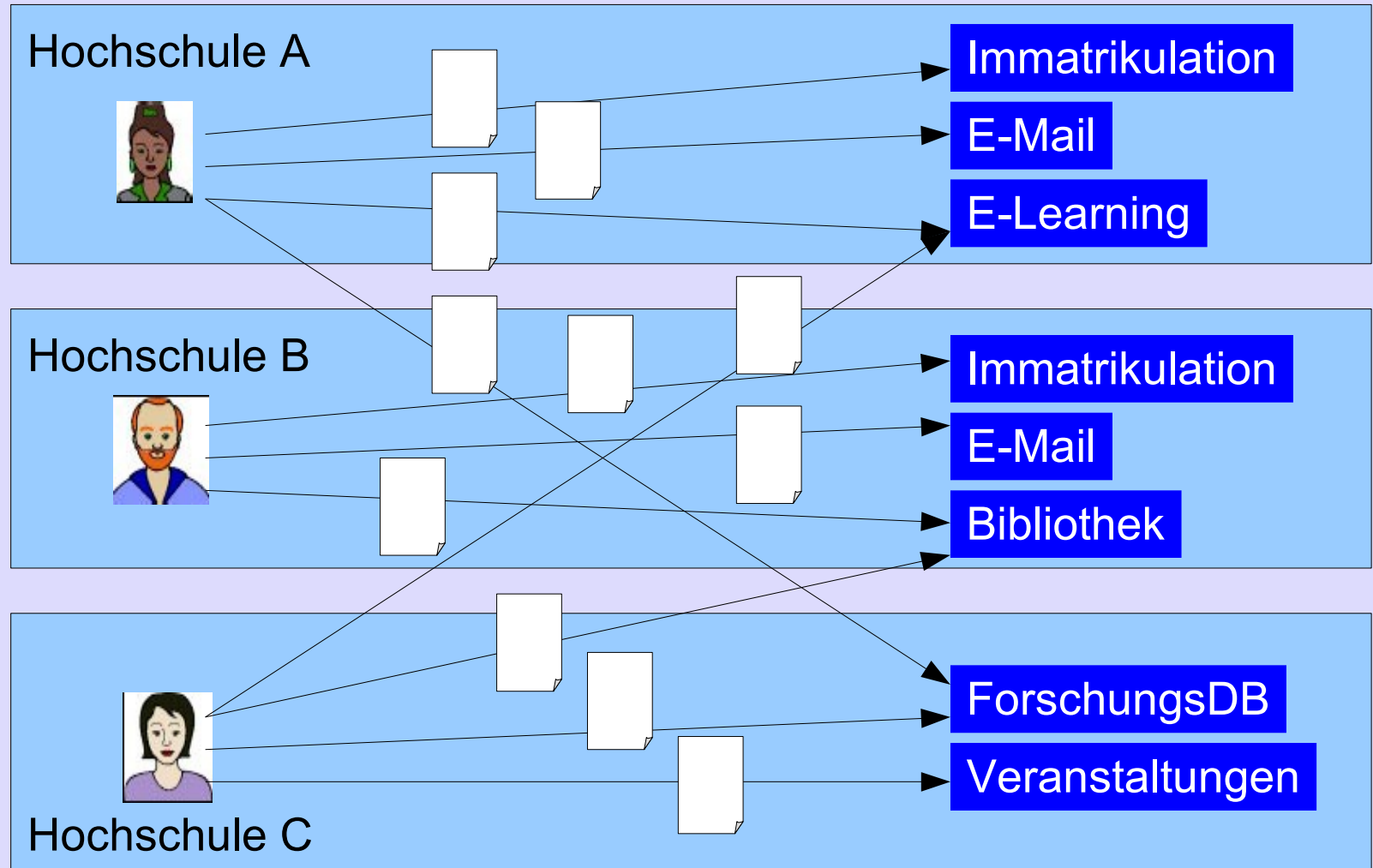


Teilnehmer

- 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)]*
- Ministerium (BWG/BWF)
- MMKH als Geschäftsstelle

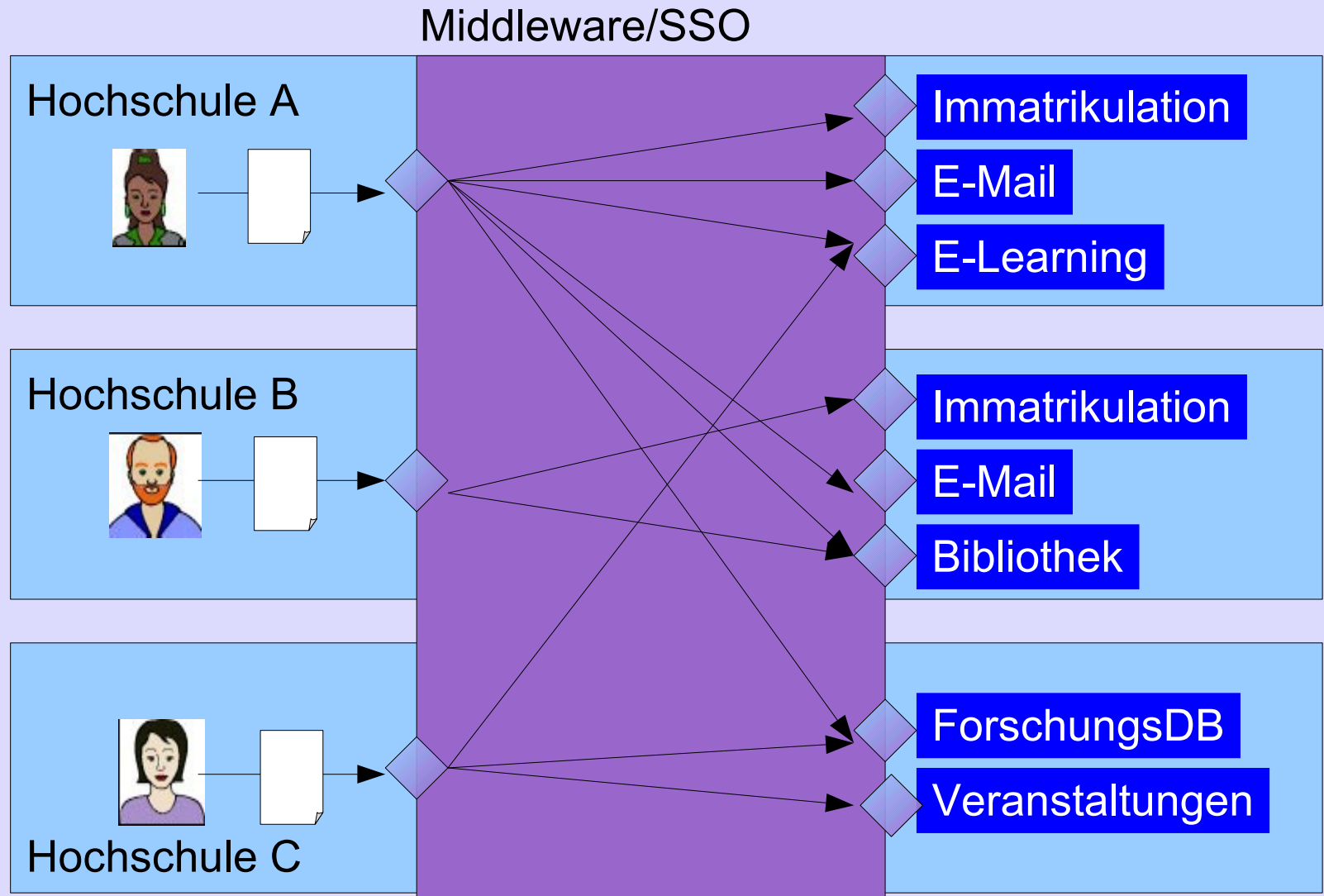


Ausweise/Logins





eCampus: SOLL-Situation

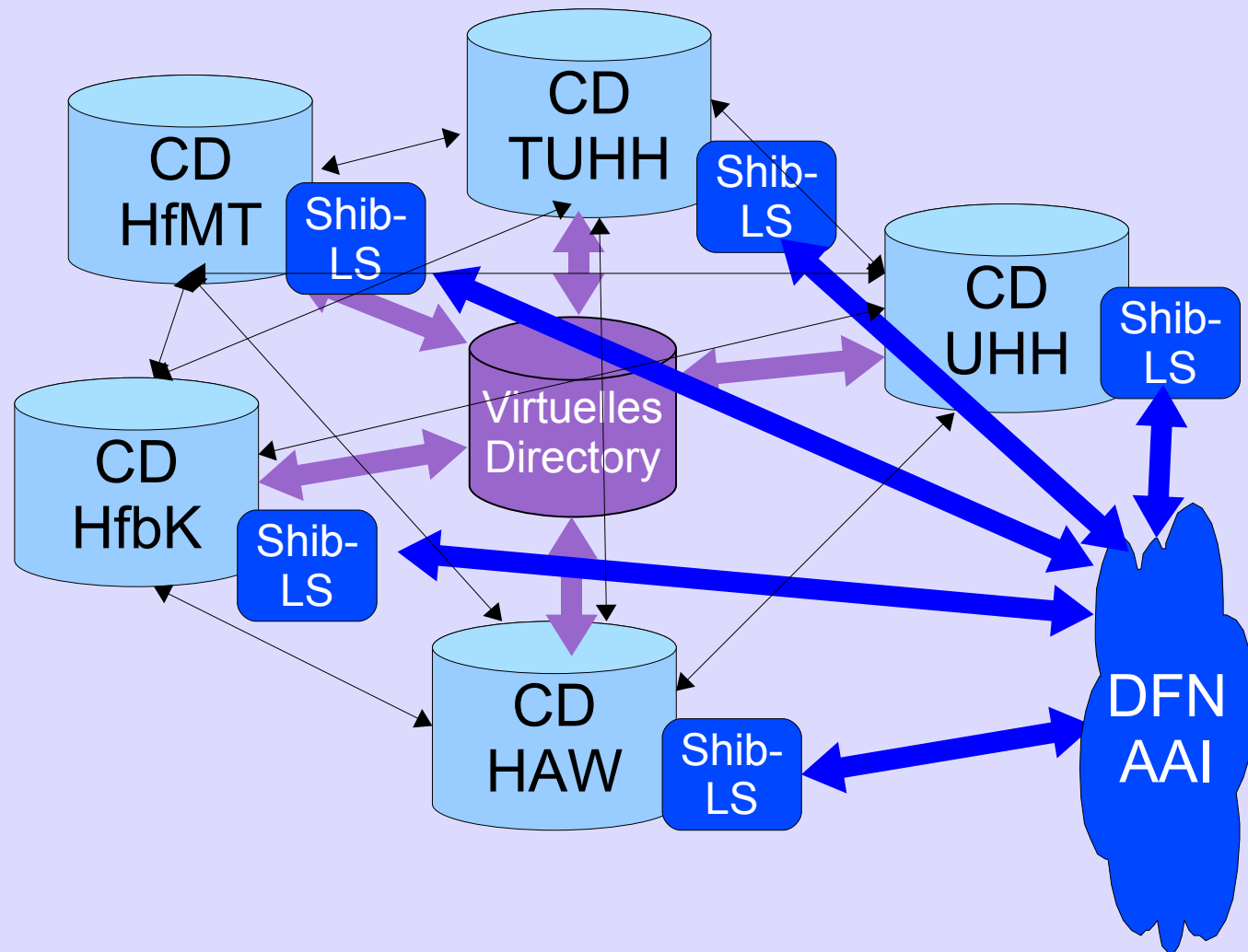


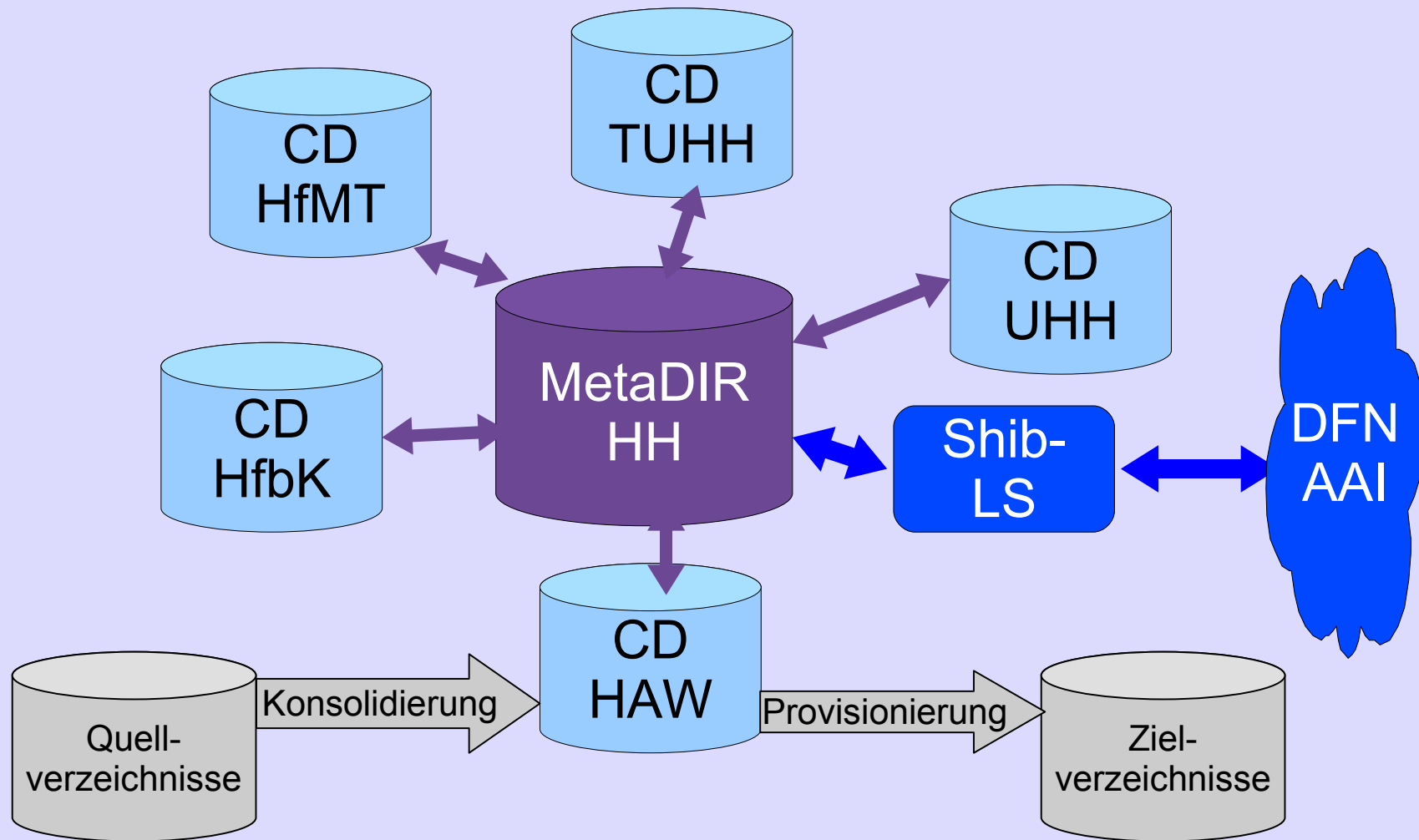


AG Basisdienste: Arbeitsschritte und Ergebnisse

- 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
- Ergebnisse, Festlegungen und Spezifikationen: [hhEduPerson](#), [Identifier/Accountsyntax](#), [Architekturmodell IDMS](#), [Definition und Grobplanung Umsetzungsprojekt \(02/2006!\)](#)

IDM: Architekturoptionen 1

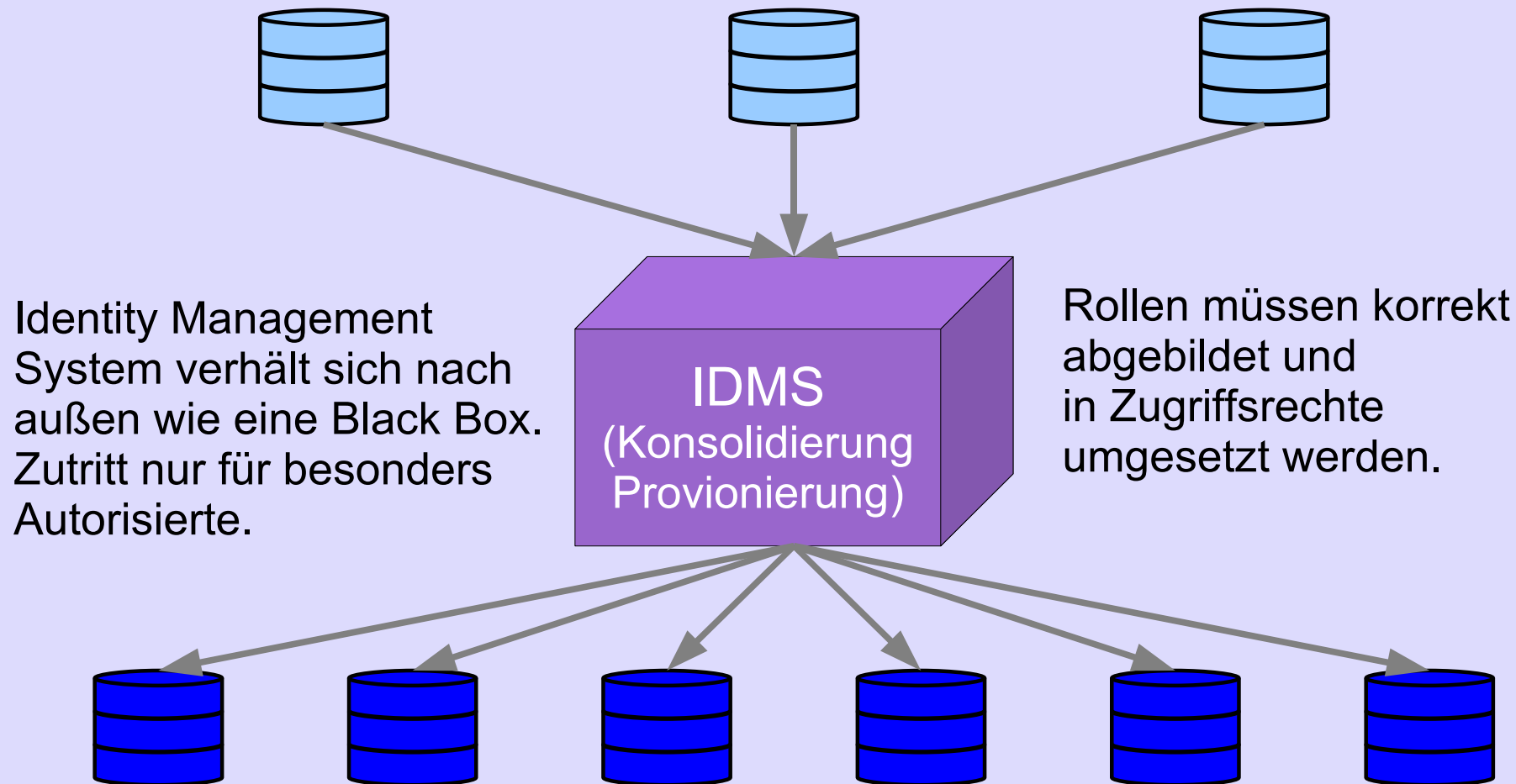






IDMS: Funktionsprinzipien 1

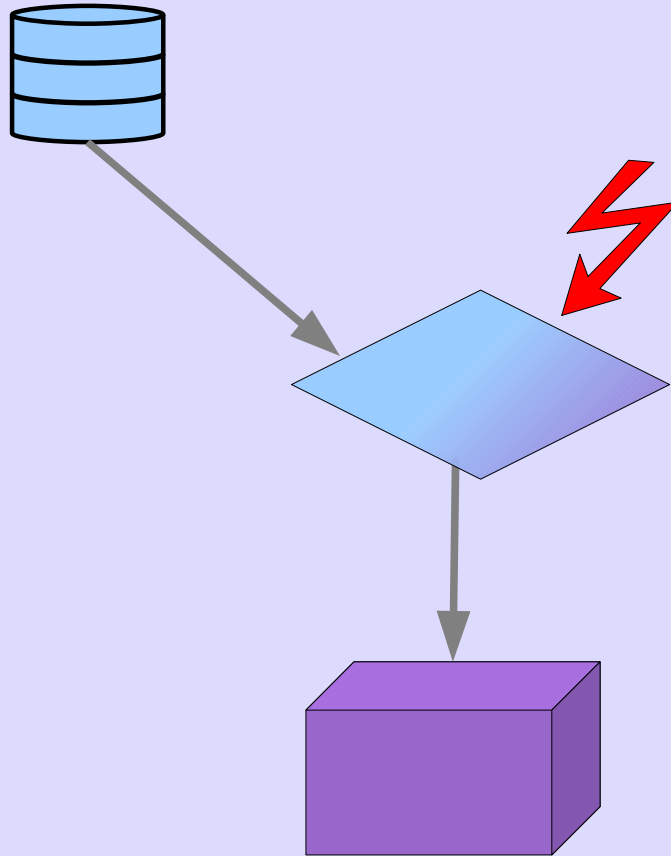
Quellsysteme: Personaldatenverwaltung, Studierendendatenverwaltung, STiNE, LBS etc.



¹¹
Zielsysteme: LDAP-CD, Dateisystem, Datenbanken, Bibliothekssystem etc.

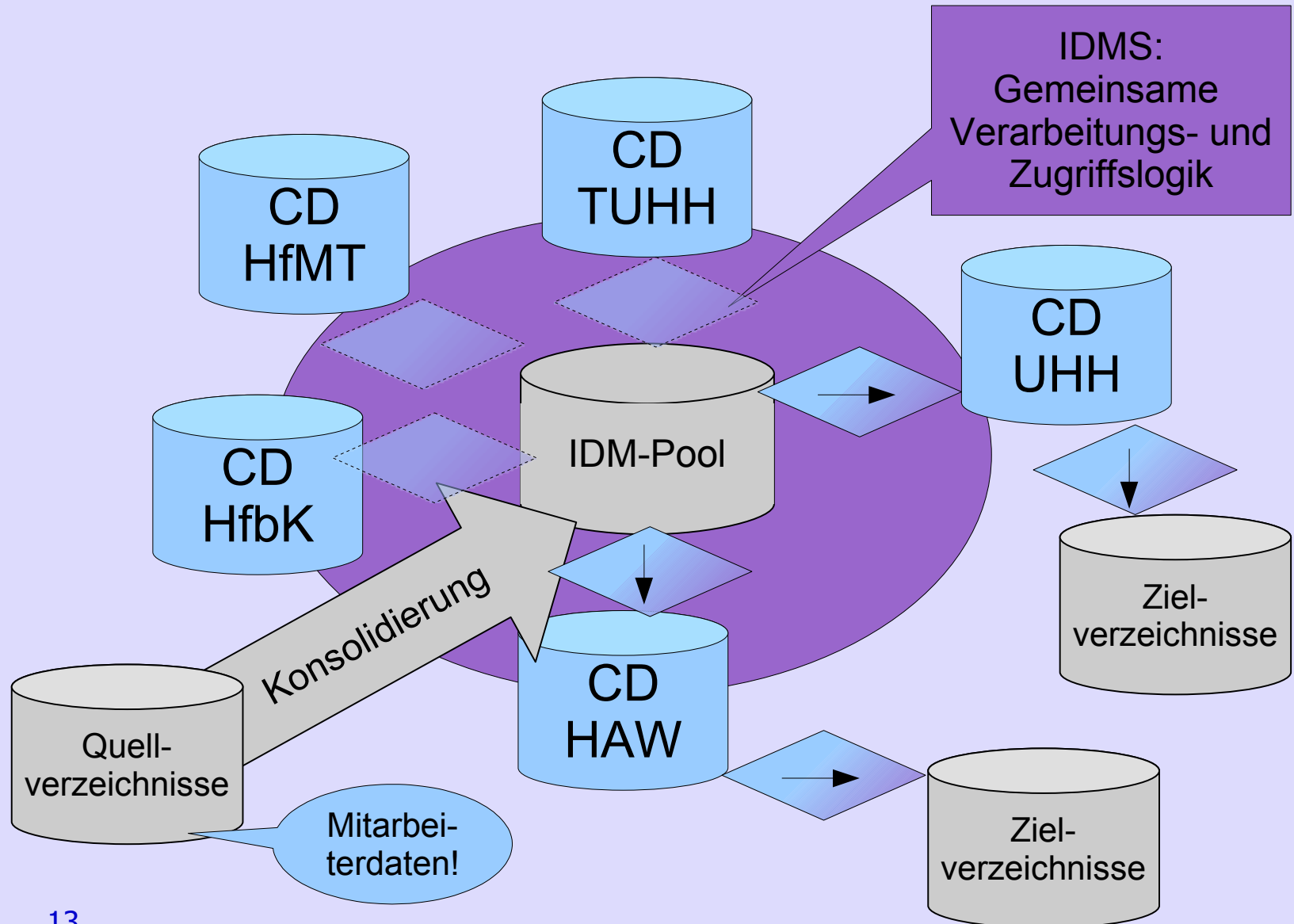


IDMS: Funktionsprinzipien 2



- 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





Vorteile & Synergien: für Studierende, Lehrende und Forschende

- Automatische Erstellung einer Zugangsberechtigung
- Automatische Verlängerung der Berechtigungen nach Rückmeldung bzw. automatische Löschung derselben
- Bereitstellung von Diensten unter Verwendung des Accounts:
 - Automatisch bereitgestellter E-Mail Zugang,
 - Zugriff auf zentralen Datenspeicher (*Homedirectory*),
 - Department- und Fakultäts-*Fileshare*
 - Funknetz-Zugang,
- Schnelle Passwortänderungen und ggf. Neuvergabe
- Entlastung von organisatorischen Aufgaben,
- Vereinfachte Kommunikationsmöglichkeiten mit den eigenen Studierenden
- Einfache und sichere Bereitstellung von Studienmaterialien
- Standardisierte und einfache, zeit- und ortsunabhängige Nutzung gemeinsamer Daten im Forschungsumfeld.



... für die Beschäftigten und IT-Administratoren der Hochschulen

- Reduzierung von Komplexitäten im Verwaltungsumfeld durch hochschulübergreifende Strukturen.
- Nutzung des Intranets mit der standardisierten Zugangsberechtigung zur Optimierung von Arbeitsprozessen in zentralen Bereichen – wie z.B. beim Personalservice.
- Automatische Erstellung einer Zugangsberechtigung, die die direkte Dienstaufnahme ermöglicht.
- Zeitnahe Änderungen an Personendaten mit unmittelbarer Provisionierung in die angeschlossenen Zielsysteme.
- Senkung des Administrationsaufwandes für die angeschlossenen Zielsysteme.
- Kostensenkung durch gemeinsame Ressourcennutzung, z.B. Abschluss gemeinsamer Software-Verträge für IDM-Komponenten.

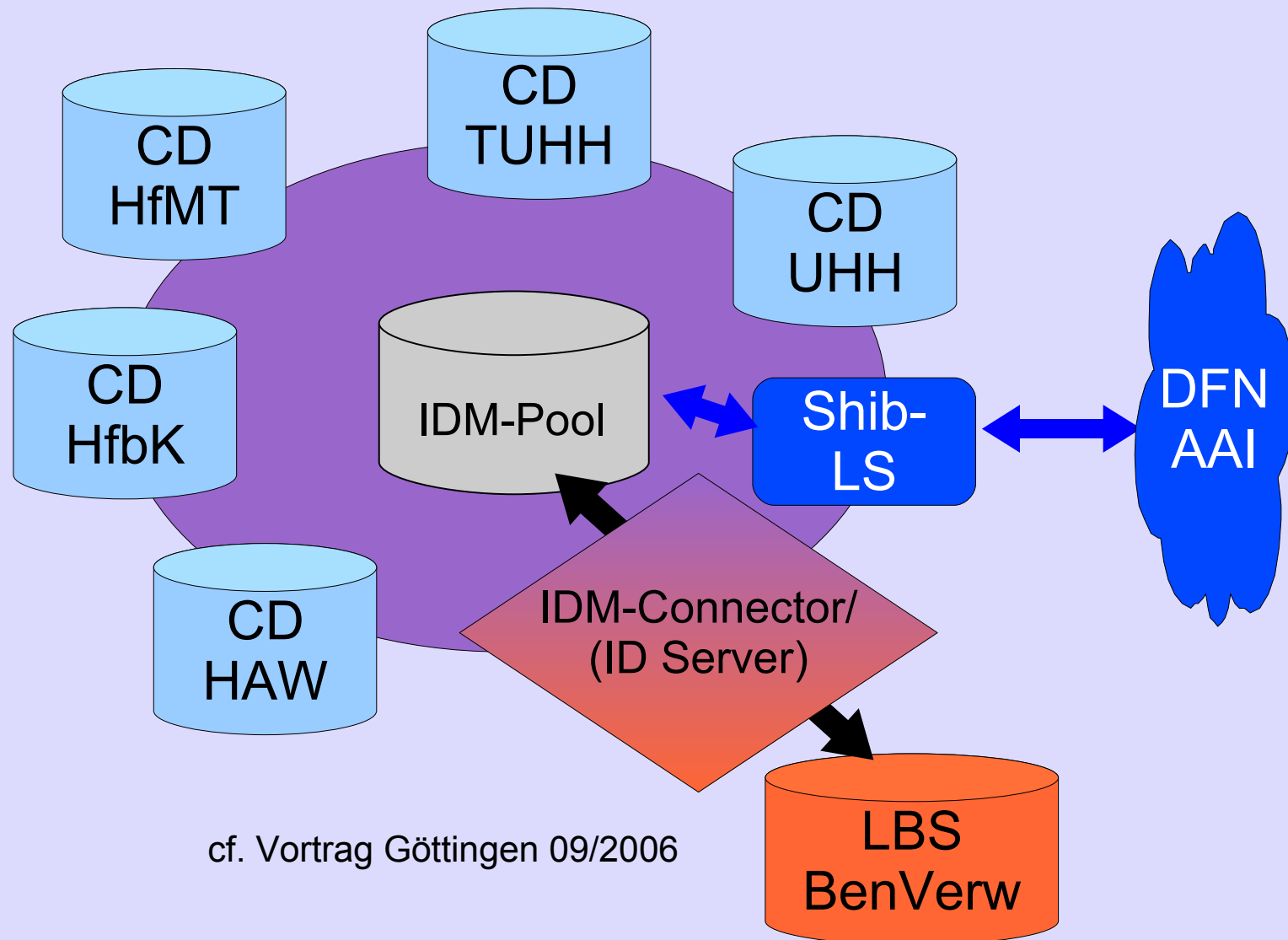


... und generell für die Hochschulen

- Erhöhte Sicherheit: Eine gemeinsame IDM-Lösung ermöglicht an zentraler Stelle eine Übersicht über Personen mit ihren Zugangs- und sonstigen Berechtigungen. Die IDM-Lösung schließt auch ein mögliches Sicherheitsrisiko durch nicht deaktivierte Accounts ausgeschiedener Personen aus.
- Verbesserte Integrierbarkeit weiterer Dienste wie z. B. Chipkarten- oder Gebäudezugangssysteme.
- Erhöhte Flexibilität bei der Umsetzung neuer Strukturen, z. B. bei der Anbindung neuer Einzelverzeichnisse oder neu zu schaffender Fakultätsinfrastrukturen



Architekturperspektiven im kooperativen Ansatz



Kooperation als Herausforderung

- Zentrale / gemeinsame vs. dezentrale / verteilte Strukturen, Komponenten und Verarbeitungslogik (technisch, funktional, organisatorisch)
 - Kooperation vs. Konkurrenz
 - Verschiedene Fächer und Wissenschaftskulturen, deren unterschiedliche technische Anforderungen und Befindlichkeiten
 - Einbeziehung der Bibliotheken über die SUB Hamburg ist ebenso vital wie ... herausfordernd!
- ⇒ Isoliertes Vorgehen einzelner Hochschulen wäre mindestens sehr schwierig!
- ⇒ Überzeugendes, übertragbares und skalierbares Architekturmodell ist kritisch
- ⇒ Phase zwischen ECI und ECII wurde für einen produktiven 'sportlichen' Wettlauf von HAW und UHH genutzt => Prototypen existieren schon!