Fachhochschule Köln
University of Applied Sciences Cologne
Institut für Informatik

Identity Management für personalisierte Web-Dienste

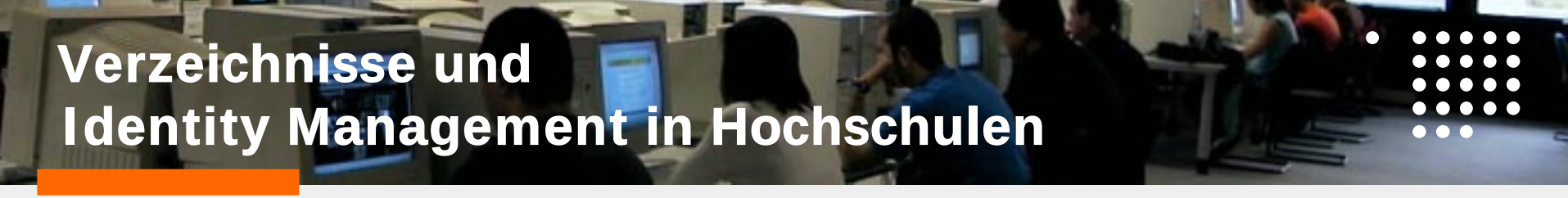
DINI-Workshop „Personalisierte Webportale“
Adlershof, 11.9.2006

H. Stenzel, FH Köln

Worum geht's?

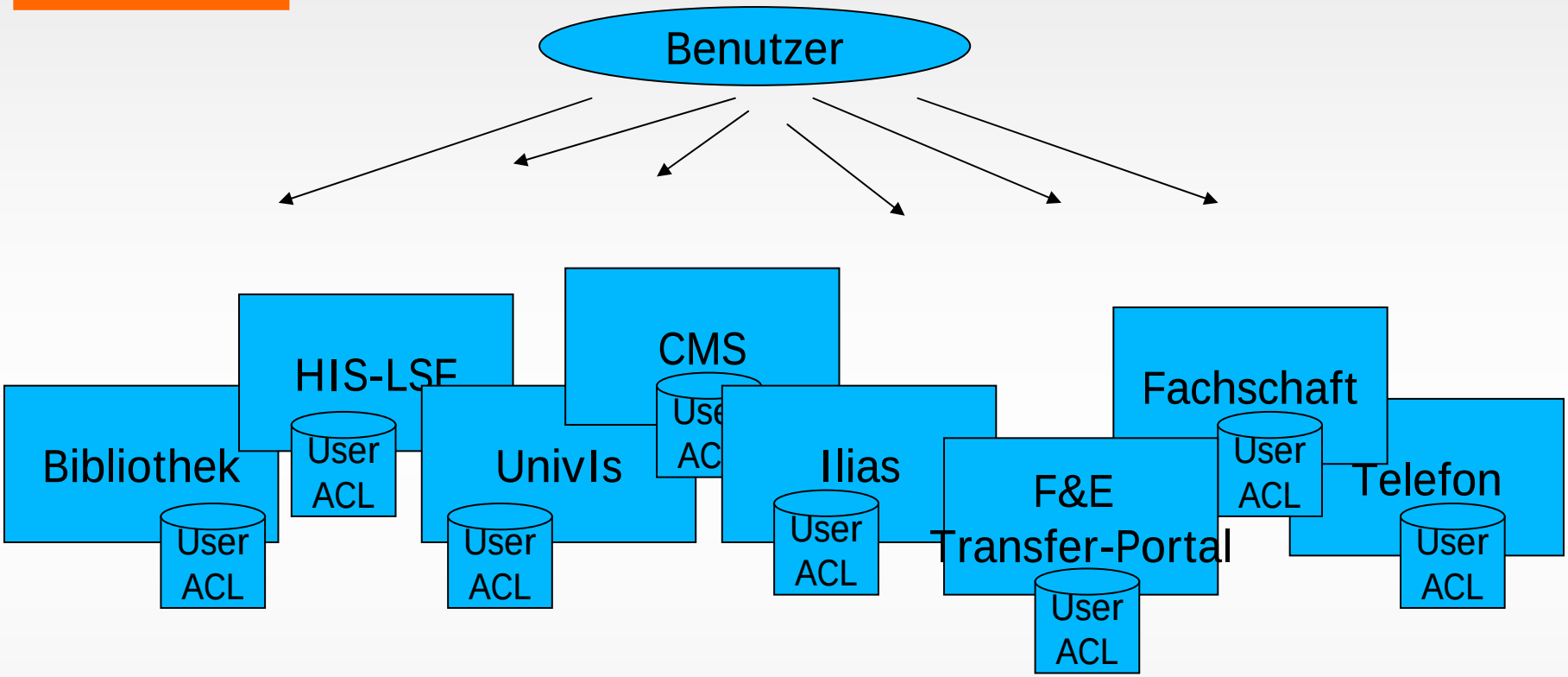
Hochschulsicht auf:

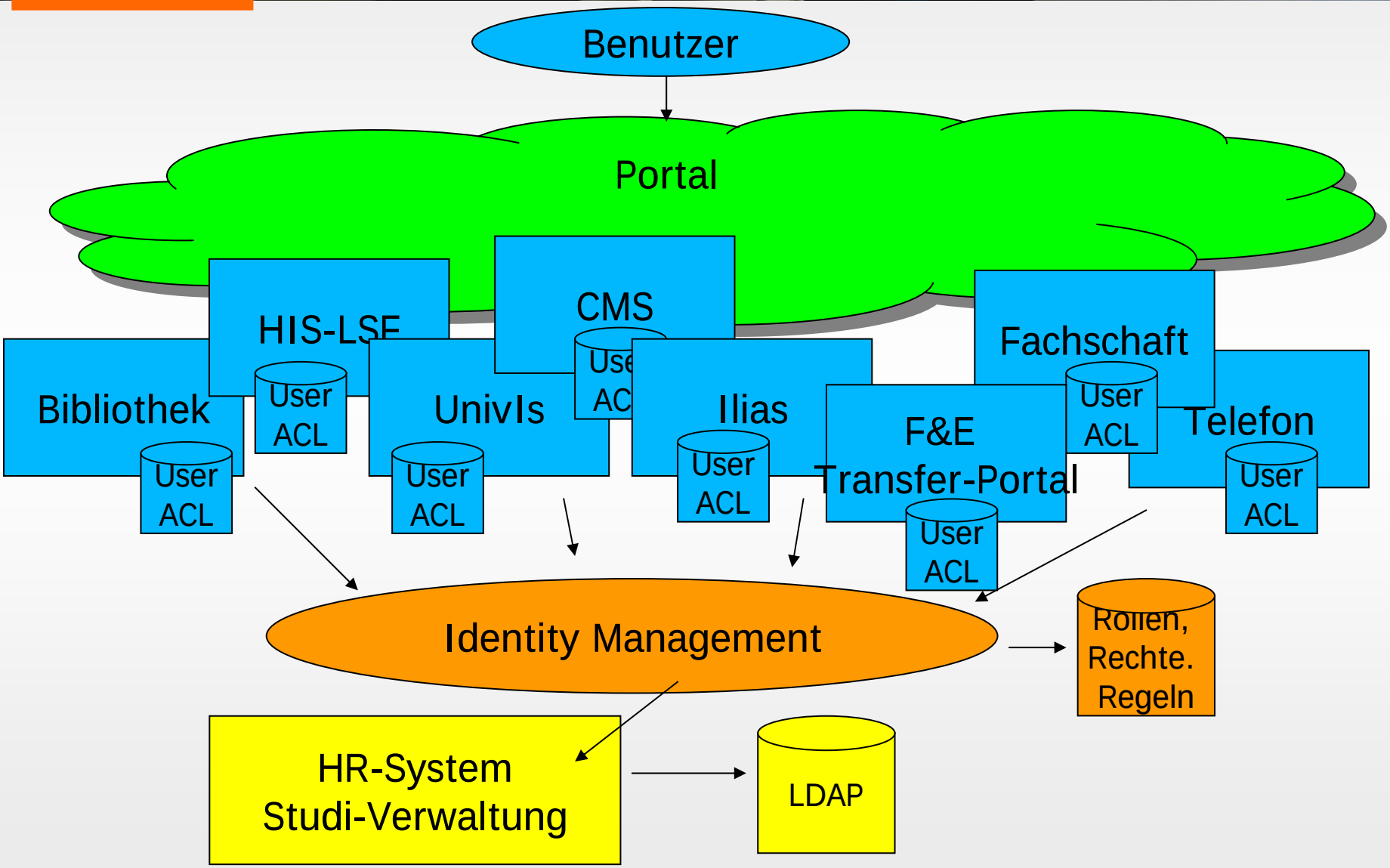
- Geschäftsprozesse und Portale
- zentral verwaltete Identitäten
- rechtliche Implikationen



Verzeichnisse und Identity Management in Hochschulen

- IT-Landschaft der Hochschulen:
  vielfältige, nicht kompatible Benutzerschnittstellen
  Angebote für zunehmend nicht-professionelle Nutzer
- „Portale“ lösen alle Probleme
  - „Kundenbindung“
  - Single point of contact, personalisiert
  - Sicherheit
  - Selbstbedienungsfunktionen
- Web-Services
- Identity Management


Benutzer
Bibliothek
User
ACL
HIS-LSF
User
ACL
UnivIs
User
ACL
CMS
Use
AC
Ilias
User
ACL
F&E
Transfer-Portal
User
ACL
Fachschaft
User
ACL
Telefon
User
ACL


Benutzer
Portal
HIS-LSF
CMS
Fachschaft
Bibliothek
UnivIs
Ilias
F&E
Transfer-Portal
Telefon
User
ACL
Identity Management
Rollen,
Rechte.
Regeln
HR-System
Studi-Verwaltung
LDAP

KFR-Empfehlungen 2006-2010

Empfehlung der Kommission für Rechenanlagen der DFG 2006-2010, „Informationsverarbeitung an Hochschulen –Organisation, Dienste und Systeme“,

2. Prozesse und Organisation,

2.1 Integriertes Informationsmanagement:

„… Technischer Kern einer Strategie für das Integrierte Informationsmanagement einer Hochschule ist insbesondere ***ein*** von allen Untereinheiten gemeinsam erarbeiteter ***zentraler Verzeichnisdienst***, der die Kooperation aller Einzelkomponenten ermöglicht. Auf dieser gemeinsamen Basis können dann durch die ***Schaffung gemeinsamer Schnittstellen*** zwischen den verschiedenen Anwendungen Dienste ausgetauscht und sachgerechte Entscheidungen über Zentralisierung oder Dezentralisierung der Dienste-Erbringung getroffen werden. … “

Verzeichnisdienste in Hochschulen: Erwartungen und Ziele

- Prozess-Orientierung (top down vs. bottom up)
  - Kontrollierte Erteilung und Entzug von Rechten
  - Durchsetzung von Policies (compliance)
  - Nachvollziehbare Aktionen (auditing)
- Innovationsmöglichkeit, Kostensenkung
  - Selbstbedienungsfunktionen
  - Vermeidung von Mehrfacharbeit
  - Zentralisiertes Helpdesk
  - Dienstebetreiber nicht gleichzeitig Benutzerverwalter
- Überörtlicher Kollaborationsbedarf
  - Schnittstellen für externen Datentransfer, e-Bologna
  - Schnittstellen zu HR-Systemen

ZKI Arbeitskreis Verzeichnisdienste
Zielsetzung

- Verzeichnisdienste: „Wesentliches technisches Mittel zur Ermöglichung effizienter Prozesse und Abläufe in der Hochschule”
- Themen des AK:
  - Erfahrungsaustausch über die Einführung von Verzeichnisdiensten, Identity Management, Single Sign On, User Provisioning und verwandten Aufgaben
  - Förderung der Kooperation zwischen Bereitstellern und Nutzern von Personen-Informationen
  - Integration von PKI, sowie
  - Domain-übergreifende Authentifizierung

ZKI Arbeitskreis Verzeichnisdienste: Aktivitäten

- 1/2-jährliche Treffen, Informationsaustausch und Diskussion:
  - Techniken
  - Projekte, Lösungen
  - Produkte
  - 50 – 60 Teilnehmer pro Sitzung
- Nächste Sitzung: November in Halle
- {www.zi.fh-koeln.de/zki-ak → www.zki.de}

Überörtliche Aktivitäten

- Thüringen: Codex
- Baden-Württemberg: PKI/LDAP
- Nordrhein-Westfalen: RV-NRW, 10er-Gruppe
- Niedersachsen: Service-orientierte Infrastruktur

HR-Systeme und Identity Management

- Verantwortung für HR-Systeme
  = Personalverwaltung
  → Betrieb der HR-Systeme
- Wechselbeziehung
  Web-basierte Dienste ↔ HR-Daten
- HIS kündigt Schnittstellen an
  - Früher: Do It Yourself
  - 2005: Staging-Tabellen
  - 2006: PSV, HIS-LADAP (≠ Identity Management)
  - 2008: Web-Services

HR-Systeme und Identity Management

- Forderungen

  (u.a. Übel, NRW, Deutschmann, Ilmenau, Hommel, TUM, Maurer, Karlsruhe)

  – Eineindeutige globale Kennung jeder Person
  – Beim Anlegen einer Person in einem System wird geprüft, ob diese Person schon existiert
  – Einfaches Zurückschreiben von Self-Service-Werten
  – Stabile Schnittstellen
  – WSDL-Wrapper für semantische Sicherung
  – Federated Identities

DFN-AAI

- Projekt AAR, Ruppert, Freiburg: Federation für Bibliotheksnutzer und Verlags-Server
- DFN:
  - Vertrags-Vermittler
  - Verwaltung der Metadaten
  - Betrieb eines zentralen WAYF-Servers
  - Betrieb eines Testsystems
  - dauerhafte Nutzerberatung und Support für Shibboleth
  - Support beim Aufbau von IdMs, Schulungen
- Anforderungen an Identity-Server

Projekt CoFIM

Personen-Infosystem als lokaler Prototyp für Federated Identity Management

- CRM in Hochschulen: Betreuung von Kontaktsuchenden für Studium, Weiterbildung und F&E-Transfer
- Zentraler Verzeichnisdienst, Identity Management
  = monolithischer Identity-Server?
- Provisionierung
  = zentrale Befehlsgewalt (Regeln durchsetzen)
- Verteilte Kompetenzen und dezentrale Systeme
  → dezentrale, unkoordinierte Account-Verwaltung und Rechtevergabe
- „beyond federations“, Vision: Persönliche Information liegt beim Individuum und nur dort

Rechtliches

- Datenschutz-Freigabe
  - Minimalitätsprinzip
- Informationale Selbstbestimmung
- Informationsfreiheit
- Mitbestimmung
  - Eingriff in Arbeitsabläufe ?
  - Rahmendienstvereinbarung (Thüringen)