UB Universitätsbibliothek Freiburg

Fallstudie Universität Freiburg: IdM, Personalrat, Datenschutz

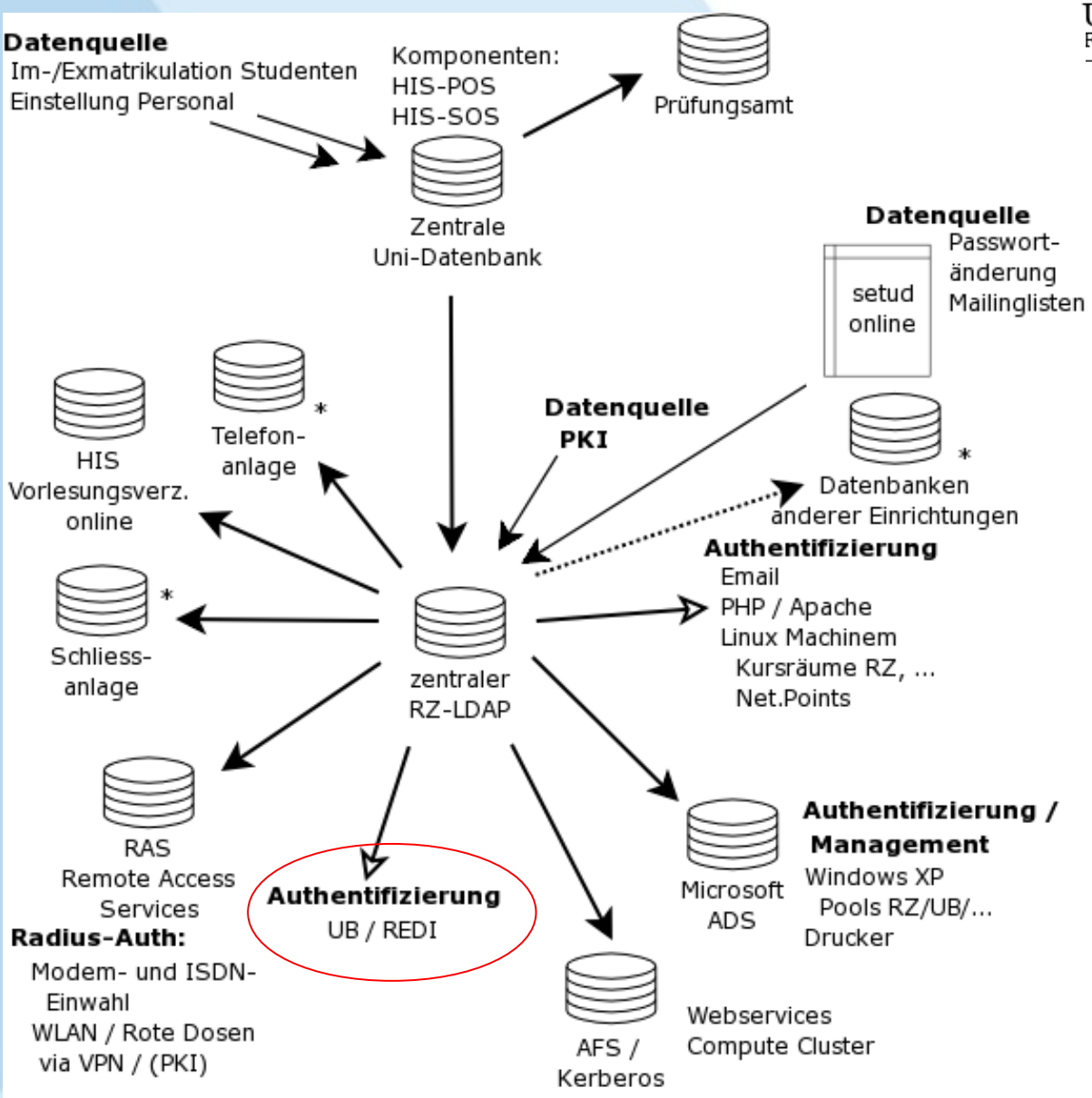
Ato Ruppert
UB Freiburg
Shibbolethworkshop, Stuttgart, WLB
23. Juni 2009

Identitätsmanagement (IdM)

UB Universitätsbibliothek Freiburg

- Zentrales System, in dem eine einheitliche Authentifizierung und Autorisierung durch die Einrichtung erfolgen kann.
- Dazu:
  - „Sammlung“ der Daten aus unterschiedlichen Quellen (Studierende, MitarbeiterInnen, etc)
  - Zusammenführen in einem einheitlichen Schema
  - Technische Schnittstelle für die unterschiedlichen Anwendungen (LDAP)

Authentifizierung - LDAP



Fallstudie Freiburg: Verwendete Daten des LDAP

Universitätsbibliothek Freiburg

- uid
- owner (Test auf Gruppen- und Kursaccount)
- rufAnmeldeDatum (eindeutiges Merkmal)
- rufStatus (Status des Accounts)
- rufAccountType (Status des Nutzers)
- rufMatNr (Test auf EUCOR-Studierende)
- rufDienst (Test auf Dienst redi in Sonderfällen)
- rufUniExpiry (Ablaufdatum der Universitäts-Mitgliedschaft/Angehörigkeit)
- rufKostenstelle

Fallstudie Freiburg: Verwendete Attribute der DFN-AAI

UB Universitätsbibliothek Freiburg

(Realbetrieb)

- eduPerson**ScopedAffiliation**:**member@uni-freiburg.de**
  - Ermöglicht grundlegende Rollen: member, faculty, staff, employee, student, alum, affiliate und library-walk-in
- eduPerson**TargetedID**:
  - Eindeutiges, persistentes Pseudonym z.B. zur Personalisierung
  - „Ruppert,EBSCO“ wird durch MD5 zu: „be83f47a1e56731eceddde08e8a76fa3“
- eduPerson**Entitlement**:**common-lib-terms**
  - Frei definierbar, URN/URI-Syntax (Absprachen zwischen IdP und SP erforderlich)
- eduPerson**PrincipalName**: **ruppert@uni-freiburg.de**
  - Eindeutiger, persistenter Identifier (Datenschutz beachten!)

Fallstudie Freiburg: Generierte Attribute

Universitätsbibliothek Freiburg

- uid (aus uid)
- **eduPersonPrincipalName** (aus: uid)
- **eduPersonAffiliation** (aus: rufAccountType, rufMatNr, rufDienst und rufUniExpiry)
- **eduPersonEntitlement** (aus: eduPersonAffiliation und für UB-Anwendungen zusätzlich aus Rechtedatenbank)
- **eduPersonTargetedID** (aus: uid, owner und rufAnmeldeDatum)
- departmentNumber (aus: rufKostenstelle)

- Herausgegeben werden jeweils nur die Attribute, die für die Anwendungen notwendig sind!

Der Dienst myLogin

UB Universitätsbibliothek Freiburg

- myLogin ist der zentrale Authentifizierungs- und Autorisierungsdienst der Universität Freiburg
- Idee hat sich im Laufe der Umstellung von Anwendungen auf Shibboleth herauskristallisiert
- Gemeinsame Entwicklung von UB, Rechenzentrum (RZ), Klinikrechenzentrum (KRZ) und Rektorat
- Absprachen und Planung ab Anfang 2006
- Implementierung ab Anfang 2007 (basierend auf ReDI)
- Inbetriebnahme am 1. Oktober 2007
- Beitritt der Universität Freiburg zur DFN-AAI mit myLogin als Identity-Provider im November 2007
- Seit März 2008 hochverfügbar (Linux-HA Cluster)

Ziele von myLogin

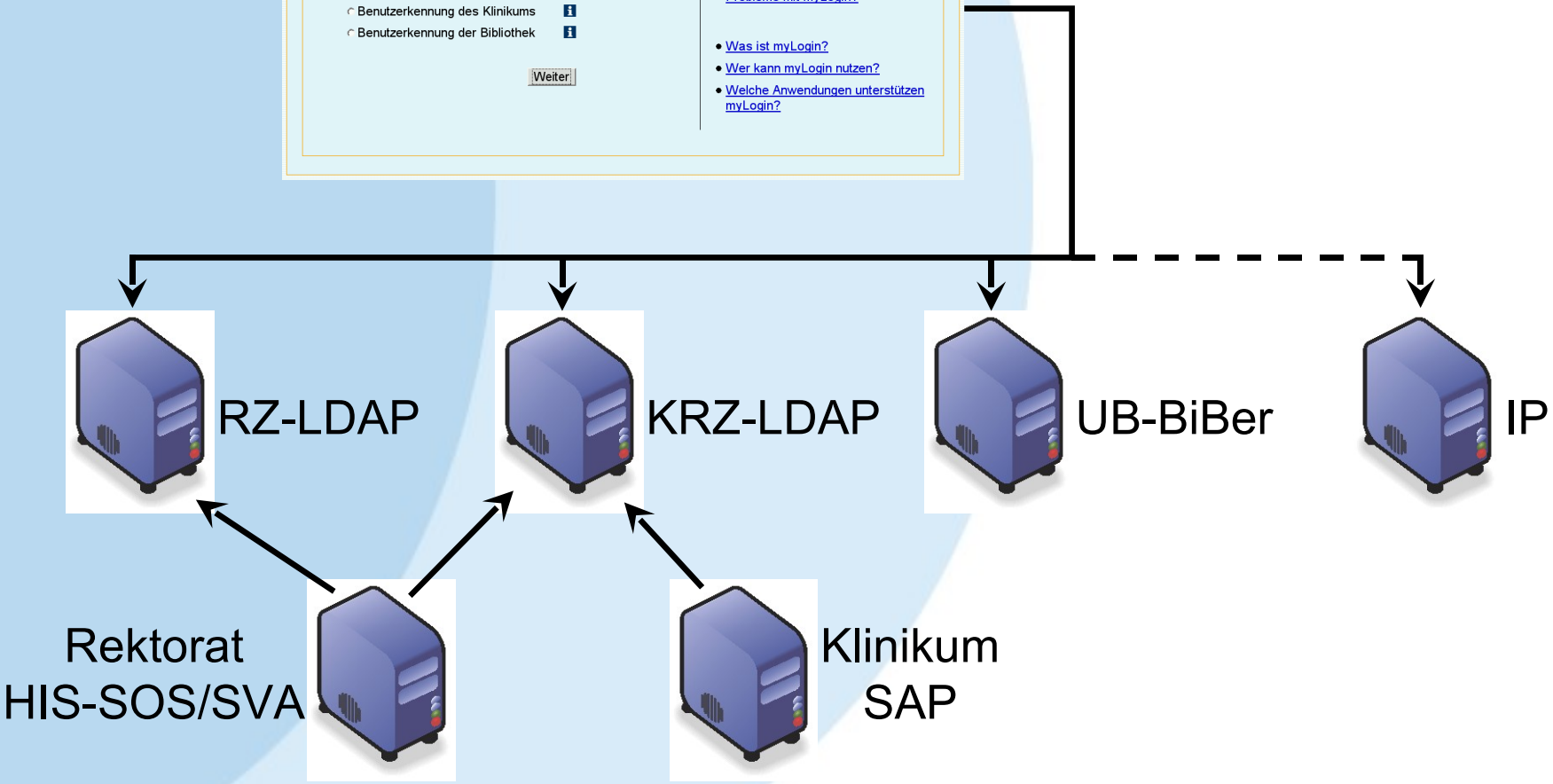
UB Universitätsbibliothek Freiburg

- Ein Login für alle Anwendungen, Single Sign-on
- Eine einheitliche Authentifizierungs- und Autorisierungsschnittstelle, sowohl für Universitäts-interne als auch für externe Anwendungen/Anbieter
- Ablösung von
  - lokalen Authentifizierungslösungen
  - direkten LDAP-Zugriffen (Datenschutz!)
  - IP-Kontrolle
- Abdeckung aller Nutzergruppen in der Universität:
  - Mitglieder und Angehörige der Universität (LDAP des RZ)
  - Mitarbeiter des Klinikums (LDAP des KRZ)
  - externe Nutzer der UB (BiBer-Ausleihsystem der UB)
  - Walk-In Patrons (IP-Kontrolle…)

Auswahl und Login

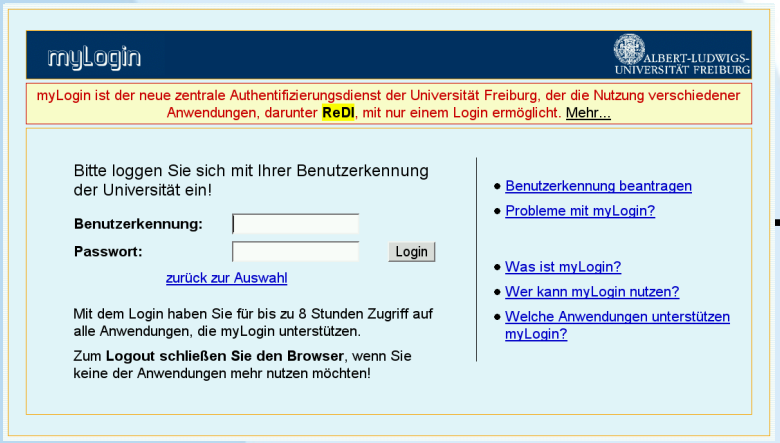
Universitätsbibliothek Freiburg

1. Auswahl des IdM-Systems

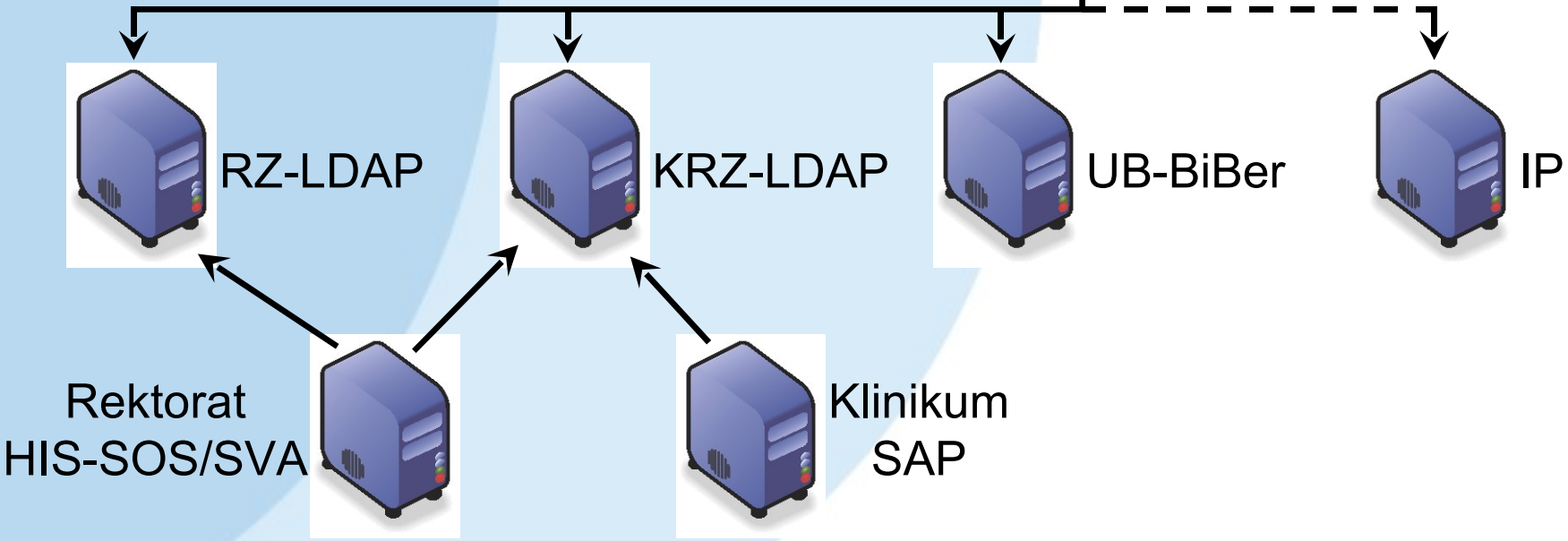


Auswahl und Login

Universitätsbibliothek Freiburg



2. Einmalige Authentifizierung gegen das gewählte IdM-System



Absprachen, Beteiligungen

UB Universitätsbibliothek Freiburg

- Lokaler Personalrat: Briefwechsel
- Rektorat (und Senat): Rollen und Rechte
- Datenschutz: Verfahrensanmeldung
- DFN-AAI: Föderationsverträge
- Und natürlich:
  - Lizenzverträge mit Anbietern
  - Absprachen mit Anbietern über Attribute

Fazit oder „wem nützt was“?

UB Universitätsbibliothek Freiburg

- Die Nutzer haben deutlich vereinfachte Verfahren beim Zugang zu lizenzierten Diensten
- Die Daten der Nutzer liegen nur noch an einer Stelle (bei der „Heimateinrichtung“)
- Sichere Übertragungswege mit einem weltweit einheitlichen Verfahren
- Die vertrauenswürdige Infrastruktur der Föderation unterstützt auch die Bedürfnisse der (externen) Anbieter
- Einheitliche Authentifizierung und Autorisierung innerhalb einer Einrichtung
- Kein direkter Zugang zum Authentifizierungssystem für Administratoren, daher besserer Schutz.

Universitätsbibliothek Freiburg

Ich danke für die Aufmerksamkeit!

ruppert@ub.uni-freiburg.de