Single Sign-On an der Universität Freiburg

Das Projekt **myLogin**

07.02.08

Dr. Jochen Lienhard - UB Freiburg

Übersicht

- Was ist myLogin?
- Warum myLogin?
- Wer nutzt myLogin?
- von der Idee bis zur Umsetzung
- Wie funktioniert myLogin?
- Anwendungen, die myLogin verwenden
- Ausblick

Was ist myLogin?

- **Definition**: *myLogin ist der zentrale Single Sign-On Dienst der Universität Freiburg*
- Basiert auf **Shibboleth**
- ist **hochverfügbar**
- eine **gemeinsame Entwicklung** der UB, des Rechenzentrums, des Klinikrechenzentrums und des Rektorats

Warum myLogin?

- viele unterschiedliche Dienste (Bibliothek, RZ, Studierendenverwaltung) mit einem einzigen Account nutzen zu können.
- Zugriff auf Dienste von überall her, unabhängig von Zeit und Ort.
- Anbindung von Anwendungen, die gemeinsam genutzt werden
- eliminieren von IP-Listen (durch gewachsene Strukturen oft chaotisch) und lokalen Authentifizierungsdiensten (entsprechen oft nicht Sicherheits- und Datenschutzanforderungen)
- Bisherige Authentifizierungs- und Autorisierungsverfahren durch **eine** einheitliche Schnittstelle ersetzen, welche auch interne und externe Anbieter unterstützen
- Anstoß von Erweiterungen im IdM-System

Wer nutzt myLogin?

- **Mitglieder und Angehörige** der Universität (Studierende und Mitarbeiter)
- **Mitarbeiter** des Universitätsklinikums
- **Externe** Nutzer (Inhaber eines Bibliotheksausweises)
- ***Walk-In Patrons*** (Benutzer, die Recherche-Rechner innerhalb der UB verwenden)

von der Idee bis zur Umsetzung (1)

1. **lokale Anwendungen** der UB auf Shibboleth umgestellt (z.B. Nagios, Stokat)
2. Umstellung von **ReDI** auf Shibboleth mit einer Anbindung zum bisherigen Authentifizierungs- und Autorisierungsverfahren
3. Ablösung der Anbindung über **ReDI** (proprietäres Protokoll) durch eine **Anbindung an den LDAP** des Rechenzentrums
4. Anbindung des **LDAP**s des **Klinikrechenzentrums** und der öffentlichen **Recherche-Rechner** an Shibboleth
5. Aufbau eine Hochverfügbarkeitsclusters zur Sicherung des laufenden Betriebs

von der Idee bis zur Umsetzung (2)

- Zwei **wichtige Schritte**, die für die Entwicklung von myLogin notwendig waren, sollen hier näher dargestellt werden:
  - Organisation des IdMs
  - Entwicklung eines neuen Zugangs zu den Authentifizierungssystemen der Universität und eines Verfahrens, um die LDAP-Attribute auf Standardattribute der DFN-AAI abzubilden

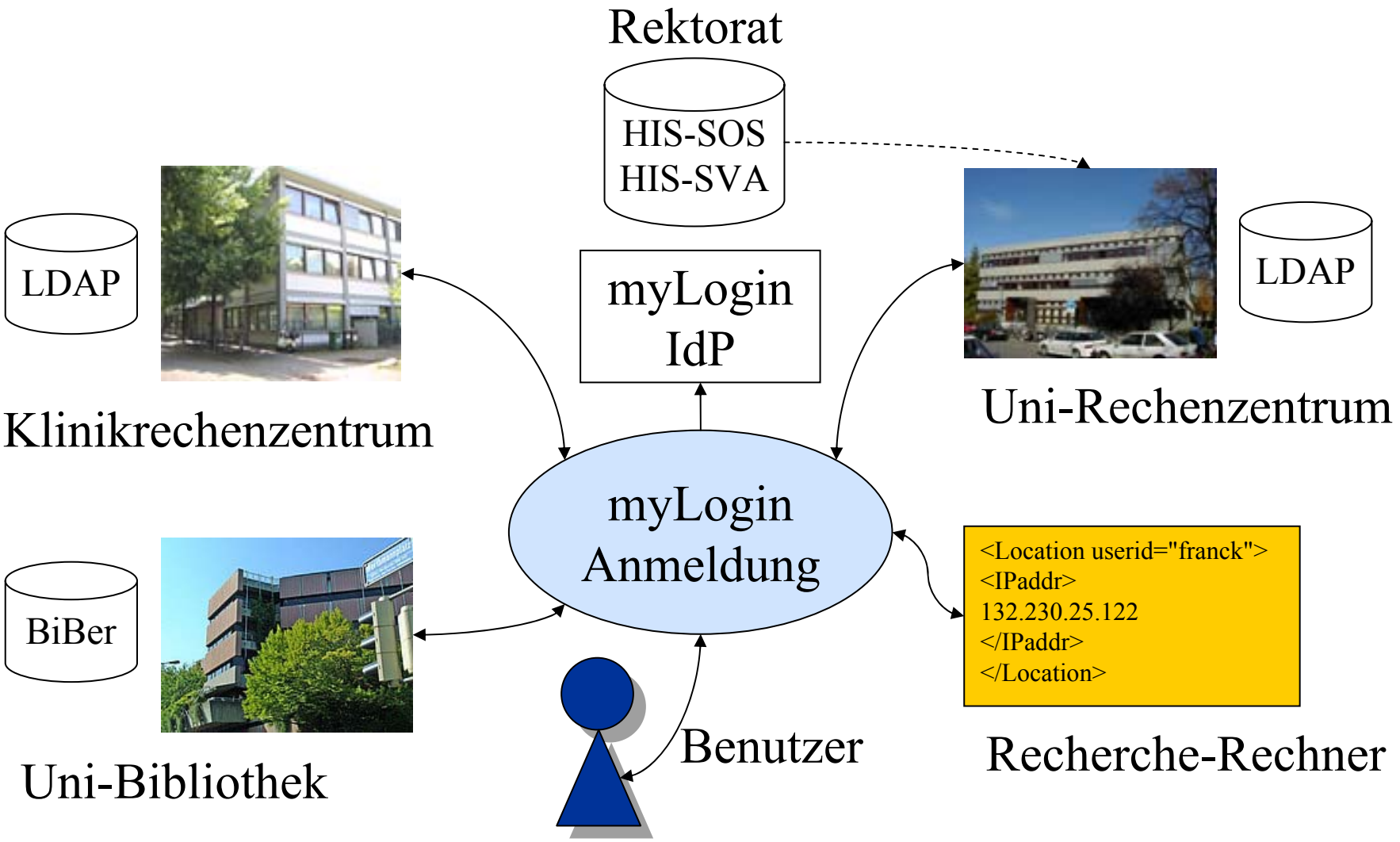
Organisation des IdMs

- Organisation der IdMs:
  - **Abläufe** mussten geändert oder erweitert werden
    - Gültigkeitsdauer eines Accounts
  - Behandlung von **Sonderfällen**
    - Z.B. Ein Mitarbeiter arbeitet für die UB, ist aber an der PH angestellt und daher nicht im LDAP-Verzeichnis des Rechenzentrums verzeichnet. Wie kann er trotzdem über myLogin authentifiziert/autorisiert werden?
  - **Datenbestand**
    - Welche Attribute müssen im LDAP stehen?
    - Abgleich der Datenbestände zwischen Rektorat und Rechenzentrum (Konsistenz, Aktualität, UB Kontonummer)
  - **Semantik**
    - Wer ist ein Angehöriger, ein Mitglied einer Hochschule? (§9 LHG)
    - Welche Rechte hat ein Angehöriger, ein Mitglied an der Hochschule?

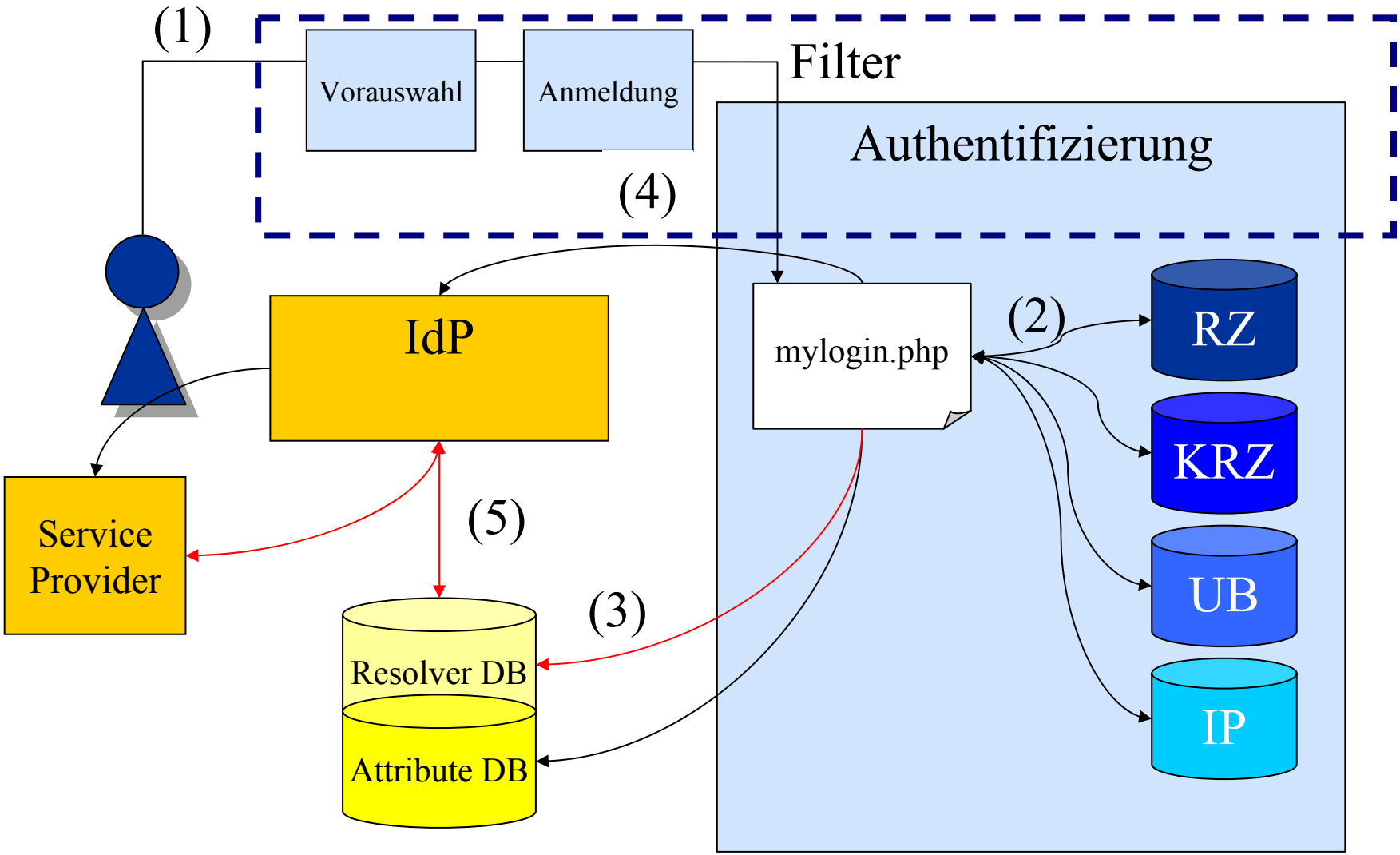
neue AA-Zugangsverfahren

- Entwicklung eines neuen Zugangs- und Abbildungsverfahren von Attributen
  - Gestaltung der Anmeldung (Design, Texte zur Erläuterung)
  - Vorauswahl (RZ, Klinikum, UB, IP)
  - Weitergabe von zusätzlichen Parametern (IP-Adresse und Einrichtungsauswahl) - Standardschnittstelle unterstützt nur die Verarbeitung von Benutzername/Kennwort
  - Schnittstelle, welche anhand der Parameter das richtige IdM abfragt
  - Erweiterung um eine IP-Kontrolle
  - Abbildung der LDAP-Attribute auf Standardattribute

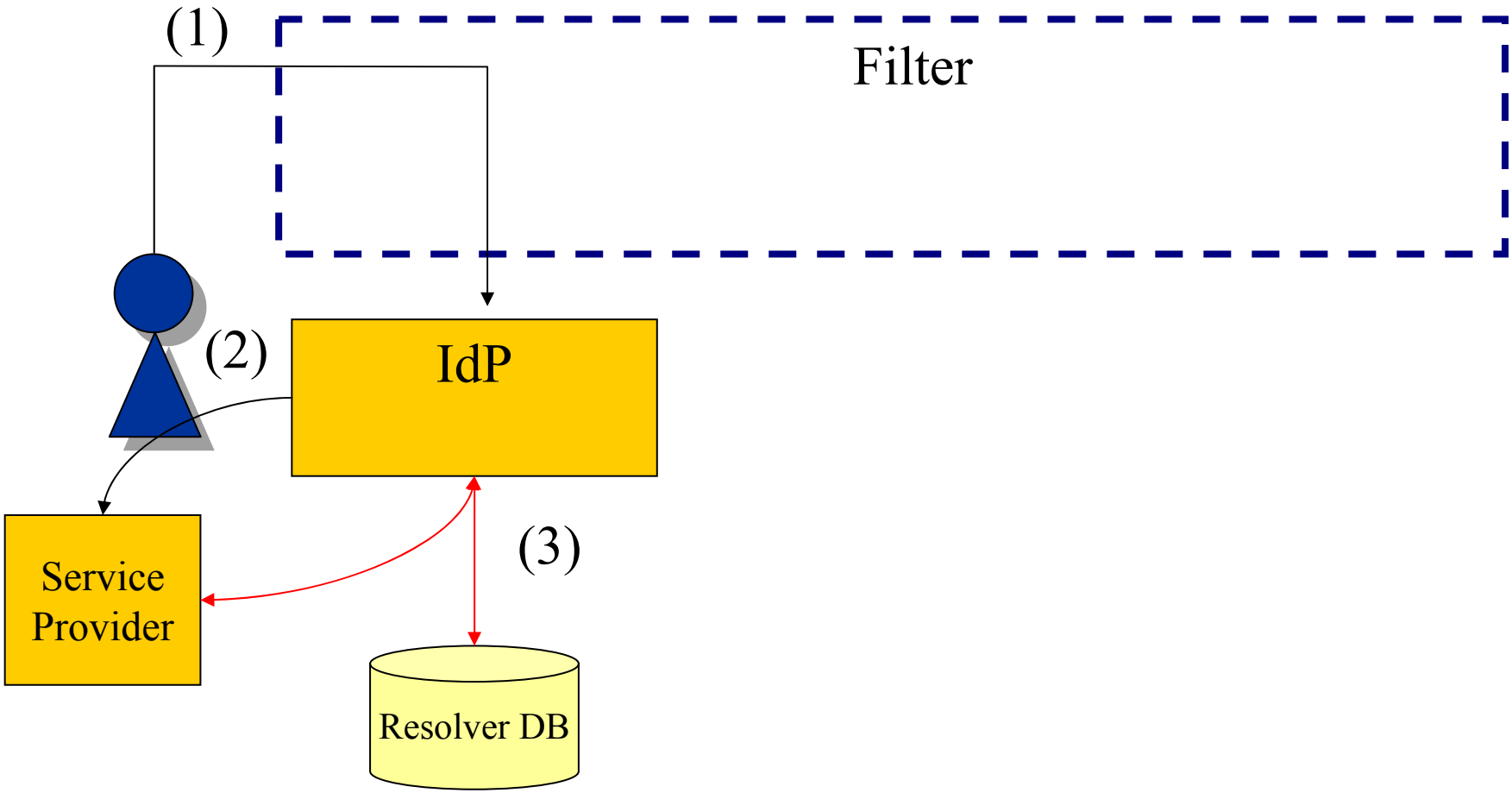
Wie funktioniert myLogin?



Wie funktioniert myLogin?



Wie funktioniert myLogin?



Wie funktioniert myLogin?

- Demo
  - Suchportal: http://www.ub.uni-freiburg.de
  - Wiso: http://www.wiso-net.de/wissen.ein
  - Nagios: https://nagios.ub.uni-freiburg.de/nagios
  - EZproxy: http://www.redi-bw.de/db/start.php?database=GLC-online

Wie funktioniert myLogin?

- Welche Attribute verwenden wir?
  - eduPersonEntitlement (common-lib-terms)
  - eduPersonTargetedID (abhängig vom Nutzer und Provider z.B. d303043714fca7420e24c872a70e303d@uni-freiburg.de)
  - uid (z.B. ruppert)
  - eduPersonPrincipalName: ruppert@uni-freiburg.de
  - eduPersonAffiliation: member, employee, affiliate
  - departmentNumber (Kostenstelle → Zugehörigkeit zum Institut)

Hochverfügbarkeit von myLogin

- Voraussetzungen:
  - LDAPs und Bibliothekssystem sind hochverfügbar
- 2-Knoten-Cluster mit Failover für folgende Ressourcen
  - IP-Adresse / Hostname
  - Webserver (Apache)
  - IdP Container (Tomcat)
  - DRDB (Distributed Replicated Block Device) (Filesystem für gemeinsame Daten)
  - Datenbank (PostgreSQL)

Anwendungen die myLogin unterstützen

- ReDI (625 Datenbanken)
- EZproxy (Rewriting Proxy, Service Provider, der für Anbieter, die kein Shibboleth verwenden, die Authentifizierungs- und Autorisierungsanfrage übernimmt)
- Suchportal der Universitätsbibliothek (IPS)
- Online-Standortkatalog
- Verwaltungssysteme der UB (Systematiken, DTV, u.a.)
- Administrative Anwendungen (BackupPC, Nagios, u.a.)
- Anwendungen im Rahmen der DFN-AAI (OVID, EBSCO, vascoda…)

Ausblick

- UB-Ausleihsystem auf myLogin umstellen
- Shibboleth 2.0
- Forschungsdatenbank, Stellenbörsen, Veranstaltungskalender, SuperX (Kassenberichte) an myLogin anschließen
- myAccount (RZ) umstellen

Danke für Ihre Aufmerksamkeit!

AAR ist ein Projekt der

UB Freiburg

Gefördert vom BMBF (PT-NMB+F)

AAR kooperiert mit dem DFN

info@aar.vascoda.de

lienhard@ub.uni-freiburg.de