myLogin:
Single Sign-On an der Universität Freiburg

5. Shibboleth-Workshop der
AAR in Kooperation mit der DFN-AAI
17.10.2007, Berlin

Franck Borel - UB Freiburg

Übersicht

- Was ist myLogin?
- Warum myLogin?
- Wer nutzt myLogin?
- Genese
- Wie funktioniert myLogin?
- Ausblick

Was ist myLogin?

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

Warum myLogin?

- Zunächst sind dies die Gründe, die **allgemein** für Shibboleth angeführt werden:
  - Z.B. Zugriff auf Dienste von überall her, SSO, bestehendes Identity-Management nutzen
- Aber auch **spezielle** Gründe:
  - Anbindung von Anwendungen die gemeinsam genutzt werden
  - Sauberere Lösung im Vergleich zu den bisher genutzten Verfahren, wie IP-Kontrolle und lokale Accounts
  - Bisherige Authentifizierungs- und Autorisierungsverfahren durch **eine** einheitliche Schnittstelle ersetzen, welche auch Anbieter unterstützen

Wer nutzt myLogin?

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

Genese

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
   - Zentrale Schnittstelle ist eine Datenbank
3. Ablösung der Anbindung über **ReDI** durch eine **Anbindung an den LDAP** des Rechenzentrums
4. Anbindung des **LDAP**s des **Klinikrechenzentrums** und der öffentlichen **Recherche-Rechner** an Shibboleth

Genese

- Zwei **wichtige Schritte**, die für die Genese von myLogin notwendig waren, sollen hier näher dargestellt werden:
  - Organisation des IdMs
  - Entwicklung eines neues Authentifizierungsverfahren und eines Verfahrens, um die LDAP-Attribute auf Standardattribute abzubilden

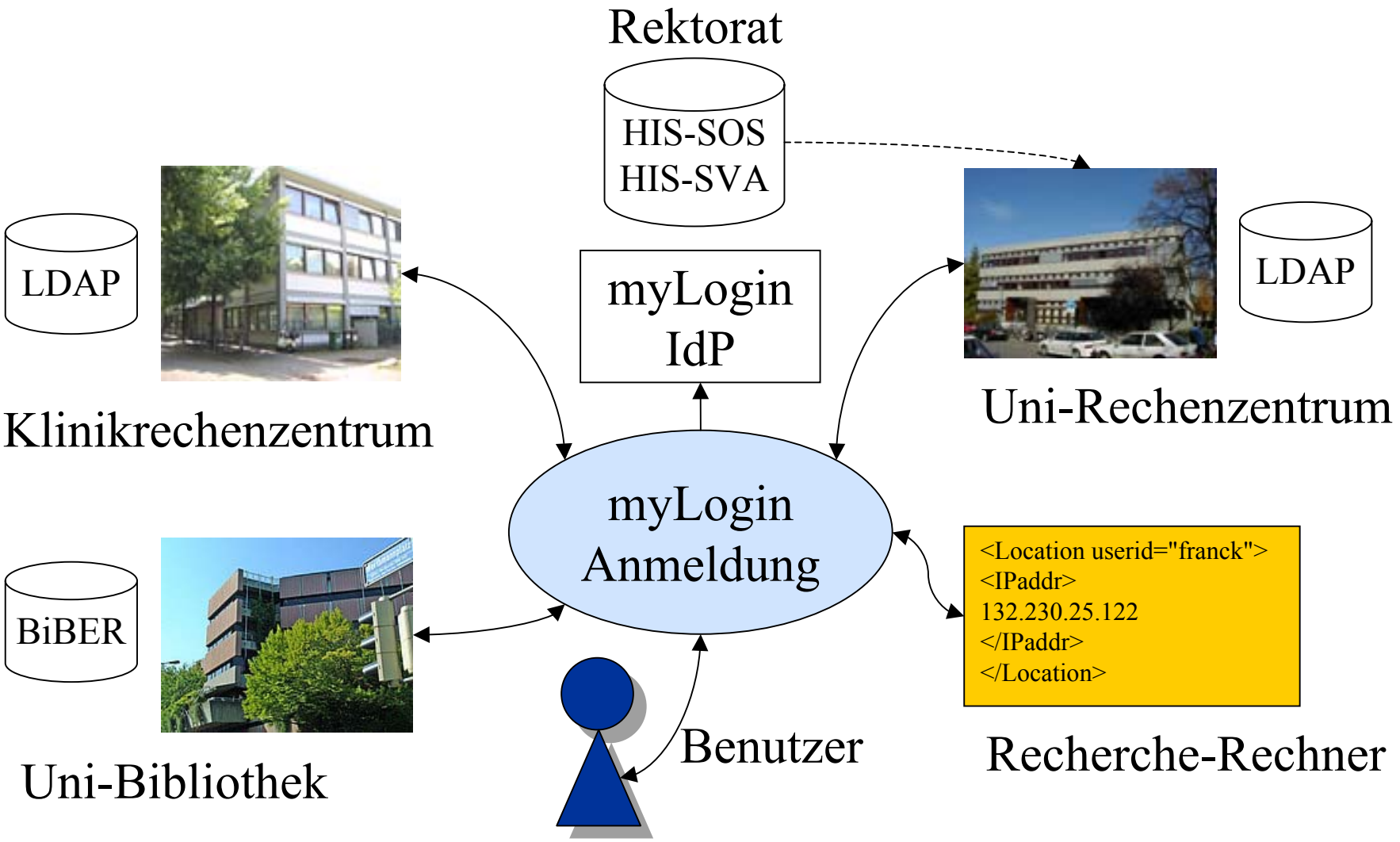
Genese

- Organisation der IdMs:
  - **Abläufe** mussten geändert oder erweitert werden
    - Gültigkeitsdauer eines Accounts, wenn ein Mitglied ausscheidet
  - 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)
  - **Semantik**
    - Wer ist ein Angehöriger, ein Mitglied einer Hochschule?
    - Welche Rechte hat ein Angehöriger, ein Mitglied oder ein Student an der Hochschule?

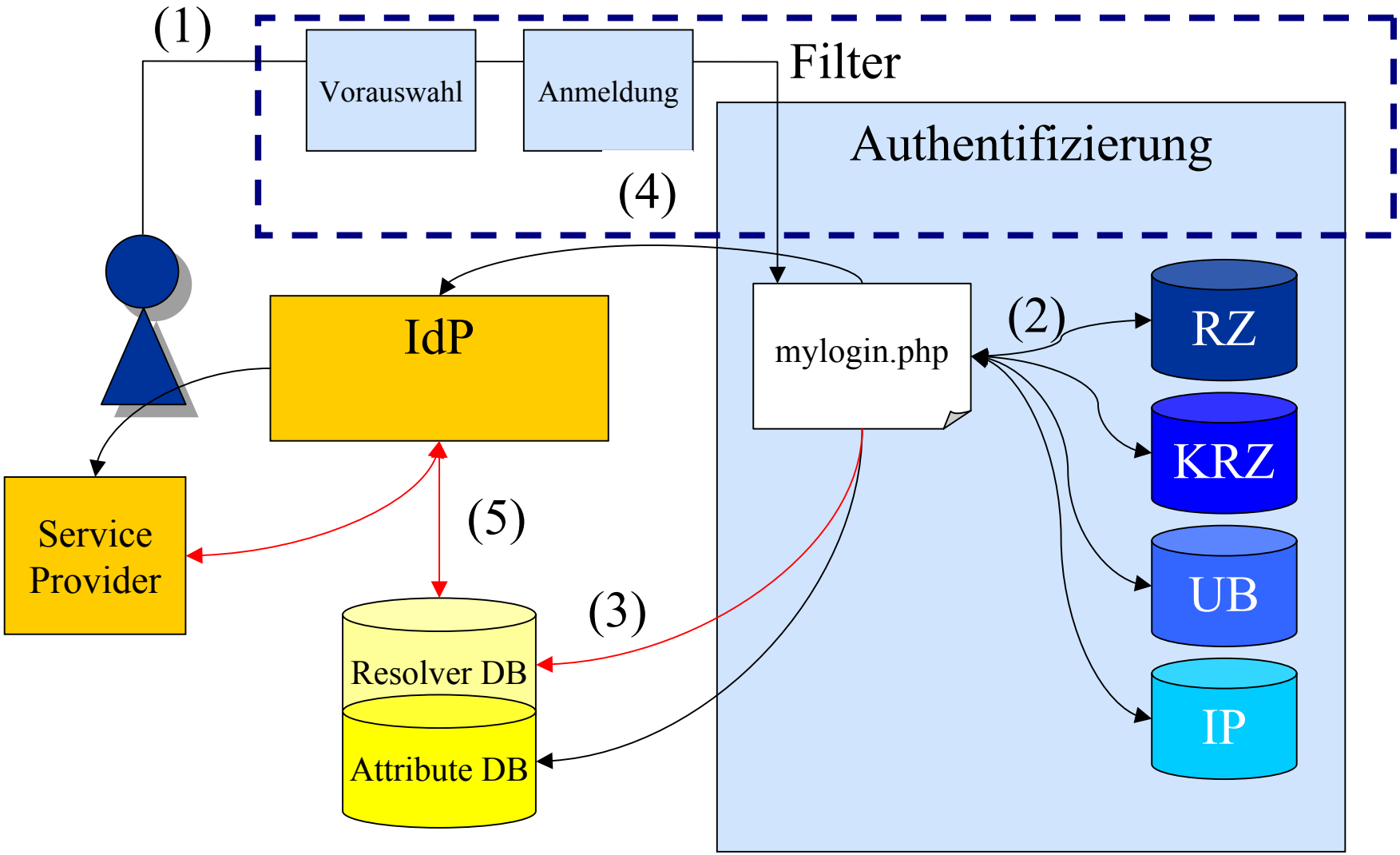
Genese

- Entwicklung eines neues Authentifizierungsverfahren- und Abbildungsverfahren von Attributen
  - Gestaltung der Anmeldung (Design, Texte zur Erläuterung)
  - Vorauswahl (UB, Universitätsklinikum, RZ, 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

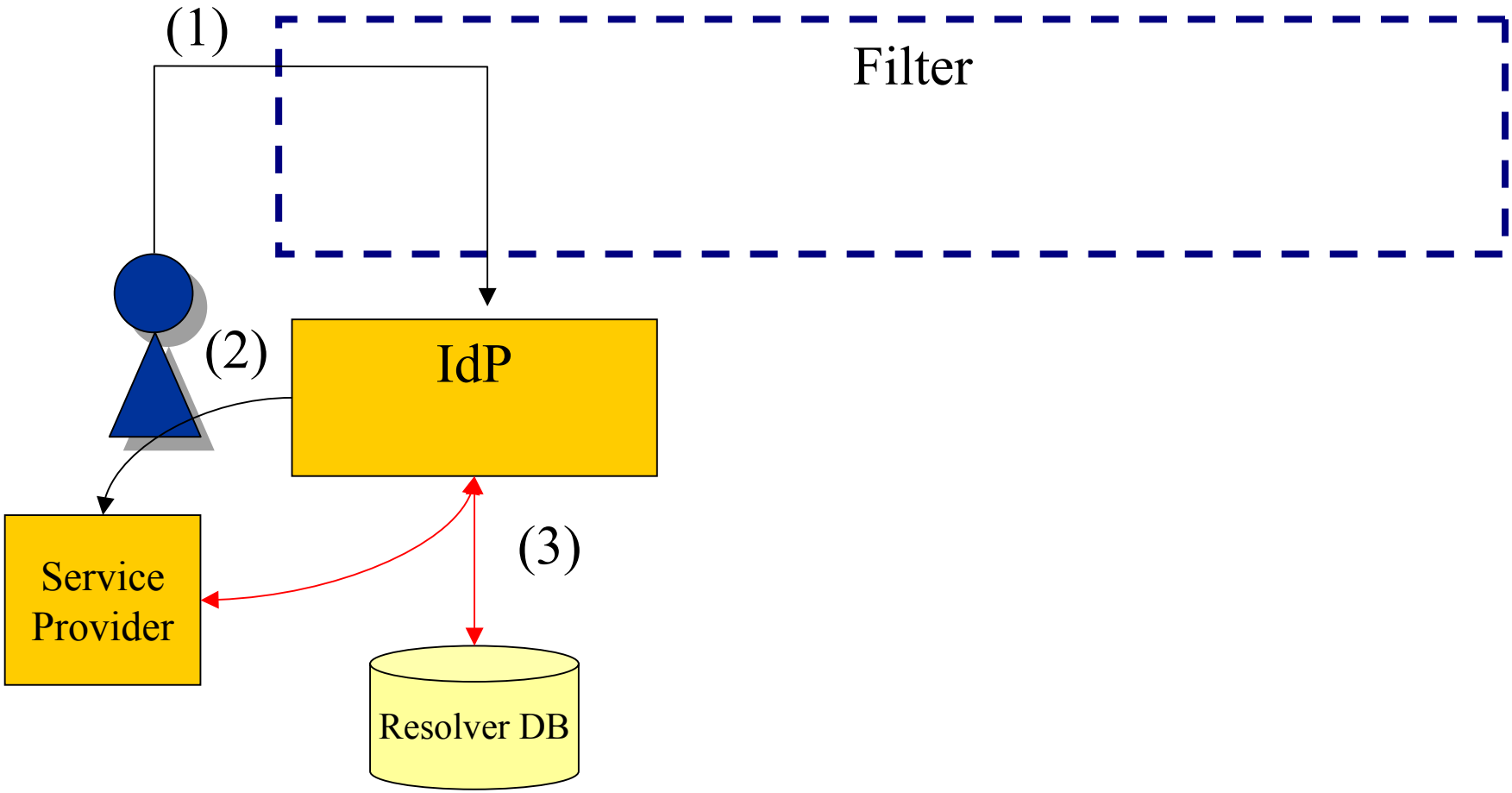
Wie funktioniert myLogin?



Wie funktioniert myLogin?



Wie funktioniert myLogin?



Wie funktioniert myLogin?

- Demo
  - Suchportal: http://www.ub.uni-freiburg.de
  - Wiso: http://shibboleth.gbi.de/cgi-bin/auswahl1
  - Nagios: https://nagios.ub.uni-freiburg.de/nagios

Wie funktioniert myLogin?

- Welche Attribute verwenden wir?
  - eduPersonEntitlement (common-lib-terms)
  - uid (z.B. fb91)
  - eduPersonPrincipalName: fb91@uni-freiburg.de
  - eduPersonAffiliation: member, employee, affiliate
  - departmentNumber (Kostenstelle → Zugehörigkeit zum Institut)

Anwendungen die myLogin unterstützen

- ReDI (625 Datenbanken)
- Suchportal der Universitätsbibliothek (IPS)
- Online-Standardkatalog
- WISO = Wirtschafts- und Sozialwissenschaften (GENIOS)
- Interne Anwendungen (Stokat, Nagios, Systematik, DTV)
- BackupPC

Ausblick

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

Danke für Ihre Aufmerksamkeit!

AAR ist ein Projekt der

UB Freiburg

Gefördert vom BMBF (PT-NMB+F)

info@aar.vascoda.de

borel@ub.uni-freiburg.de