# Einbindung von Lokalen Bibliothekssystemen in das Identity Management einer Hochschule

## (und weiteres zum Identity Management von der VZG)

Till Kinstler

Verbundzentrale des GBV, Göttingen

# Agenda

- Identity Management / Identitätsmanagement
- Beispiel innerhalb einer Hochschule: FH Braunschweig/Wolfenbüttel
- Beispiel organisationsübergreifend: “Virtual Home Organization” für die Einzelnutzer der Nationallizenzen

# Identity Management / Identitätsmanagement (IdM)

- Verwaltung von Personendaten
- oft gebraucht als Begriff für die zentrale Zusammenfassung und Verwaltung von Personendaten in einer Organisation
- Ziel: Person hat eine eindeutig zugeordnete digitale Identität zur Nutzung aller Dienste einer Organisation
- oft: zentrale Authentifzierung und Autorisierung

➔ Trennung von Personendaten und Anwendungen / Diensten bzw. mindestens Import- / Exportmöglichkeit von Personendaten

➔ Zusammenfassung aller zur Nutzung von Diensten notwendigen Eigenschaften (“Attribute”) einer Identität

# IdM und Bibliotheken

- viele Dienste von Bibliotheken arbeiten mit Authentifizierung / Personendaten, z.B.:
  - lokale Bibliothekssysteme / Ausleihe
  - Zugriff auf lizensierte Angebote
  - personalisierte Dienste
  - Dokumentserver (Veröffentlichung)
- meist eigene Benutzerverwaltungen in Bibliotheken
- oft eigene Eigenschaften / Attribute: Bibliotheksbenutzernummer, externe Benutzer...

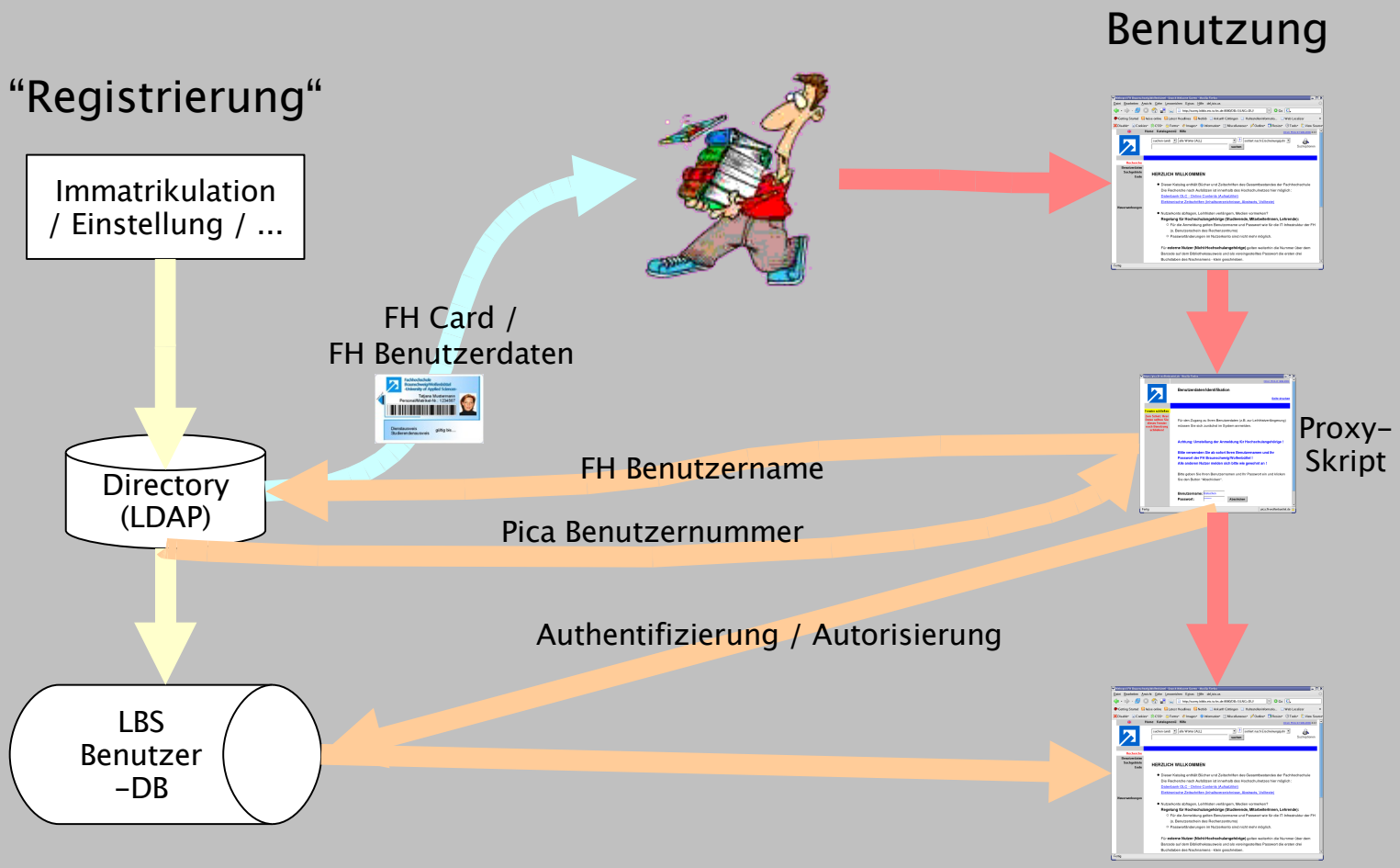
# Probleme bei der Einführung des IdM

- organisatorische: wo sind die Personendaten? wer verwaltet sie? Bereitschaft zur Kooperation? Datenschutz (Aufklärung der Nutzer!) ...
- technische:
  - viele unterschiedliche Systeme mit eigener Nutzerverwaltung
  - oft keine klare Trennung zwischen Anwendung und Nutzerverwaltung, keine definierten Schnittstellen
  - unterschiedliche technische Ansätze für IdM: Metadirectory, “Proxy-Directory”, relationale Datenbanken, föderierte Systeme wie Shibboleth ...
  - viele “Features” im Umfeld: Chip-/Magnetkarten, Single Sign On (SSO), Selbstbedienung ...

# IdM an der FH Braunschweig / Wolfenbüttel

- Zusammenfassung aller Personendaten in einem zentralen IdM-System beim Rechenzentrum
- Ziele:
  - Abgleich der diversen Personendatenbestände in der Hochschule
  - Personendaten sollen nur noch an einer Stelle verwaltet werden
  - Einheitliches Login für Nutzung aller elektronischer Angebote der Hochschule (Email, Computerbenutzung, Anmeldung zu Prüfungen/Veranstaltungen, WLAN, Bibliothek ...)
  - Einführung einer FH-Card

# FH Wolfenbüttel



# Organisationsübergreifendes IdM ("federated IdM")

- derzeit vor allem IdM innerhalb von Organisationen
- Bedarf für organisationsübergreifendes IdM: Mobiltelefonbenutzer will auch im Ausland telefonieren, Tagungsteilnehmer will WLAN am Tagungsort nutzen, Student von Hochschule A will E-Learning-Angebot bei Hochschule B nutzen, Wissenschaftler von Einrichtung A will Angebot von Bibliothek B nutzen usw.
- einige Projekte im Hochschulbereich in Deutschland
  - auf Länderebene: SOI in Niedersachsen, SAXIS in Sachsen, eCampus in Hamburg, ReDI/AAR in Baden-Württemberg, CODEX in Thüringen ...
  - deutschlandweit: DFN AAI

# Beispiel: Nationallizenzen / DFN AAI

- Nationallizenzen:
  - viele Angebote von vielen Anbietern
  - Nutzer aus vielen Einrichtungen
  - Einzelnutzer, die keiner Einrichtung zugerechnet werden können
- pragmatische Lösung:
  - Zugangskontrolle bei den Anbietern über IP-Adressen der Einrichtungen
  - Einzelnutzer greifen über Proxies bei berechtigten Einrichtungen zu (z.B. mittels HAN-Server)
- Ziel: Umstieg auf verteilte Authentifizierung und Autorisierung mittels Shibboleth, Einzelnutzerverwaltung für Nationallizenzen bei der VZG als Mitglied von DFN AAI

# Shibboleth

- Middleware zur verteilten Authentifizierung und Autorisierung
- Zwei Rollen:
  - Identity Provider (IP): Authentifizieren Nutzer
  - Service Provider (SP): Anbieter von Diensten, die eine Authentifizierung und Autorisierung erfordern
- IPs und SPs schließen sich in Föderationen zusammen und können ihre Dienste untereinander nutzen
- Grundlage von Föderationen: Vertrauensverhältnis zwischen den Teilnehmern auf Grundlage von Vereinbarungen
- Voraussetzung zur Teilnahme: Identity Management bei IPs, Anerkennung der Vereinbarungen

# DFN AAI

- hervorgegangen aus dem AAR-Projekt der UB Freiburg und UB Regensburg im Rahmen von Vascoda
- deutschlandweite Föderation zur Authentifizierung und Autorisierung
- DFN als Betreiber der Infrastruktur der Föderation (anerkannter Dienstleister für die Wissenschaft, Erfahrung im Bereich Zertifizierung/Kryptographie)

# “Virtual Home Organization“ für Einzelnutzer

- derzeit (noch wenige Tage): Einzelnutzer der Nationallizenzen müssen sich bei mehreren Bibliotheken, die den Zugang zu den Verlagsangeboten via Proxy bereitstellen, anmelden
- VZG hostet www.nationallizenzen.de und betreibt die Systeme für die Registrierung der nutzenden Einrichtungen und (bald) der Einzelnutzer
- erster Schrittt: Einzelnutzer werden in IdM-System verwaltet (schlicht: OpenLDAP), Benutzerdaten werden zu den Bibliotheken, die den Zugang bereitstellen, repliziert
- zweiter Schritt: Umstieg auf Shibboleth, IdM der VZG als Identity Provider, Proxies der Bibliotheken oder Verlage als Service Provider