

IdM-Lösungen in Hochschulen - aktueller Stand, zukünftige Herausforderungen

H. Stenzel

CampusSource & ITMC

TU Dortmund
12.4.2011

IdM tut Not

- Benutzer eines Systems oder einer Anwendung sind zu identifizieren und gezielt zu autorisieren, u.a. für:
 - Eingeschränkte Dienste (Datenschutz, Verträge)
 - Personalisierte Dienste (Portale, Voreinstellungen, Wiedererkennung für CRM oder Statistik)
 - Aufzeichnungspflichten
 - Erhöhung der Sicherheit (Single Sign On, Deprovisionierung)
- „Verzeichnisdienste sind das technische Herz des Informations-Managements in der Hochschule“*

ZKI Arbeitskreis Verzeichnisdienste und Identity Management

- 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
- 1/2-jährliche Treffen, Informationsaustausch und Diskussion:
 - Techniken
 - Projekte, Lösungen
 - Produkte
 - 50 – 60 Teilnehmer pro Sitzung
- Nächste Sitzung: 4.-5. 10. in Jena
- Informationen unter <https://www.zki.de/arbeitskreise/verzeichnisdienste/>

Aktuelle IdM-Projekte

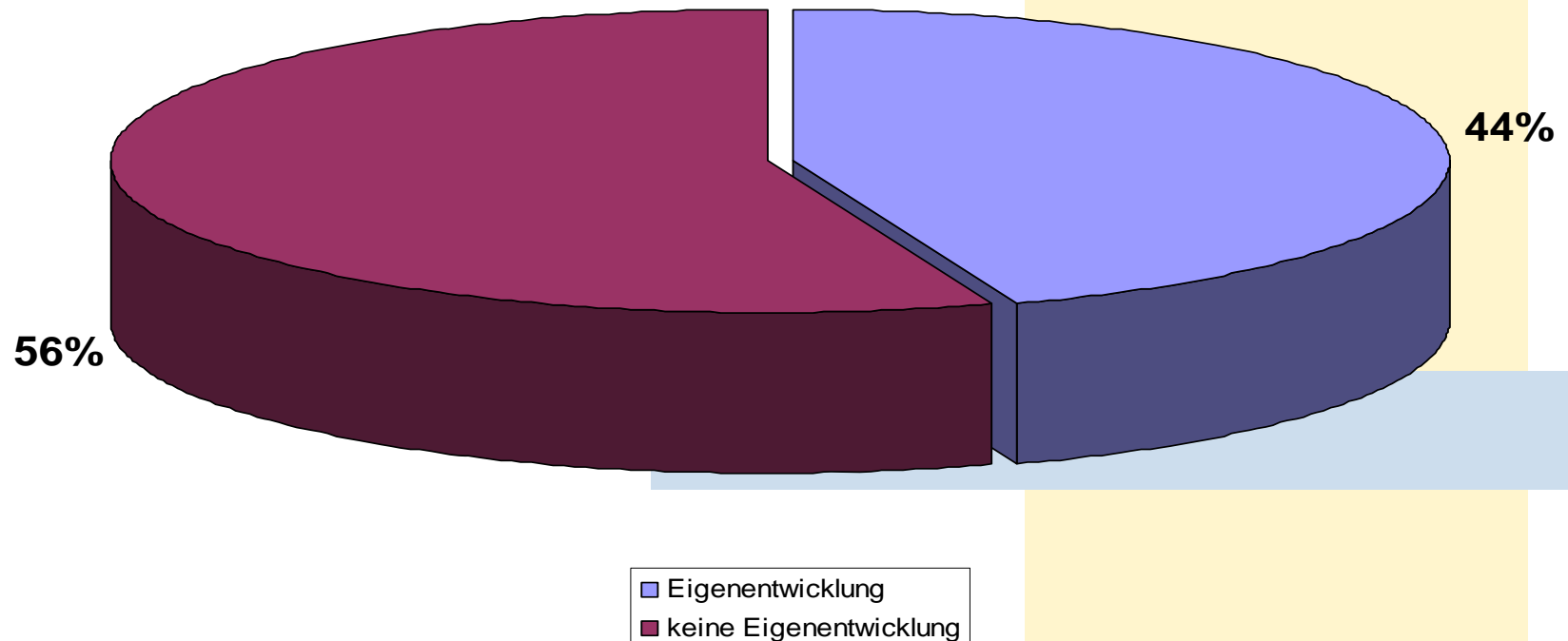
Präsentationen im ZKI-Arbeitskreis „Verzeichnisdienste“ im vergangenen Jahr

Hochschule	Projekt	Status	Produkte/Basis/Plattform
Uni Augsburg (4.10.2010)	ALOIS (Augsburger Leichtgewichtiges Offenes Identity-Management-System)	Im Einsatz	Eigenentwicklung (OpenLDAP, Kerberos, AD)
FU Berlin (10.3.11)	Shibboleth für SSO	Im Einsatz	OpenSource, eigene Erweiterungen
TU Berlin (4.10.2010)	Rollenbasiertes, dezentrales IdM	In Entwicklung	Eigenentwicklung RBAC/J2EE
TU Dresden (4.10.2010)	IdM – Einführung einer Standardsoftware	In Vorbereitung	Wird ausgeschrieben (Eigenentwicklung soll ersetzt werden)
Uni Duisburg-Essen (4.10.2010)	IdM	Im Einsatz / In Entwicklung	IBM TIM / Eigenentwicklung
FH Frankfurt/M (10.3.11)	Digitaler Campus – Vernetzung CM-ERP	Im Einsatz/ In Arbeit	SAP (HCM, geplant SLCM)
HAW Hamburg (10.3.11)	Schnittstelle IdM - CampusNet	Im Einsatz	CIF (kommerzielle Schnittstelle CampusNet – SAP HR)
DSHS Köln (4.10.2010)	IdM	Im Einsatz	IBM TIM/TDI/TDS (+ Radius-LDAP)
Uni Leipzig (10.3.11)	AlmaWeb - integriertes Campus-Management-System	In Vorbereitung	Wird ausgeschrieben (Campus Management: Datenlotsen)
Thüringer HRZ (10.3.11)	Codex IdM 2.0 (redesign) thoska+ (Chipkarte)	Im Einsatz	Novell, eigene Erweiterungen
Uni Ulm (10.3.11)	Benutzermanagement für Bibliotheksverbund	Im Einsatz / in Arbeit	LDAP für aDIS BMS

Historische Folie

Statistik: Eigenentwicklung?

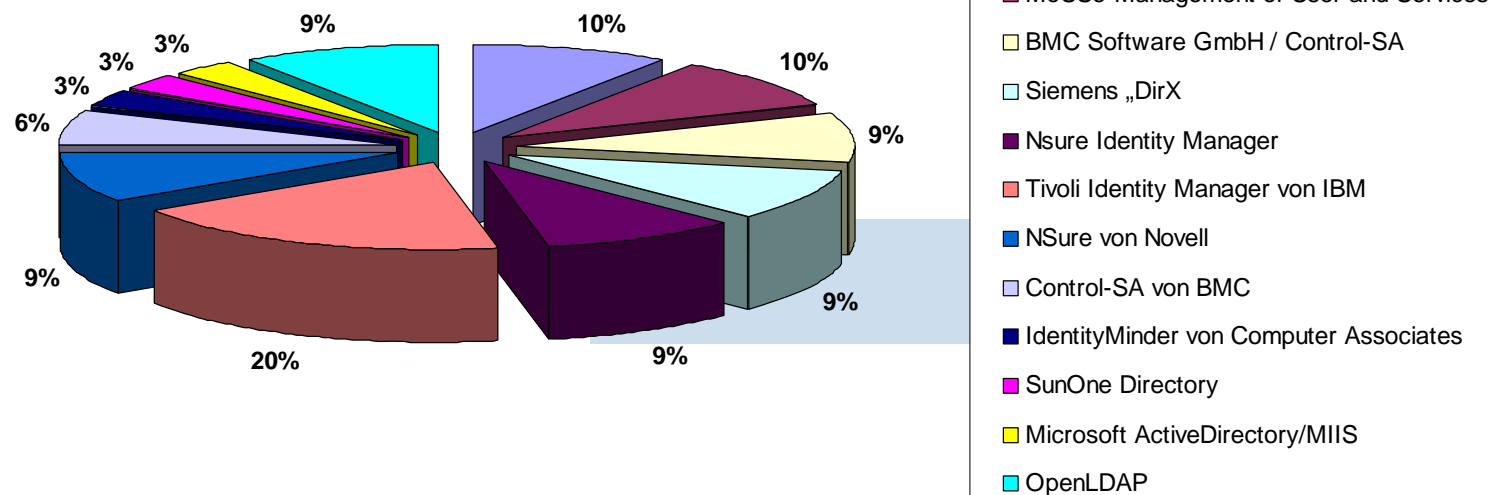
- Oft Eigenentwicklungen auf Basis kommerzieller Systeme
- fast ausgewogen -> Eigenentwicklung / kommerzielles System



Historische Folie

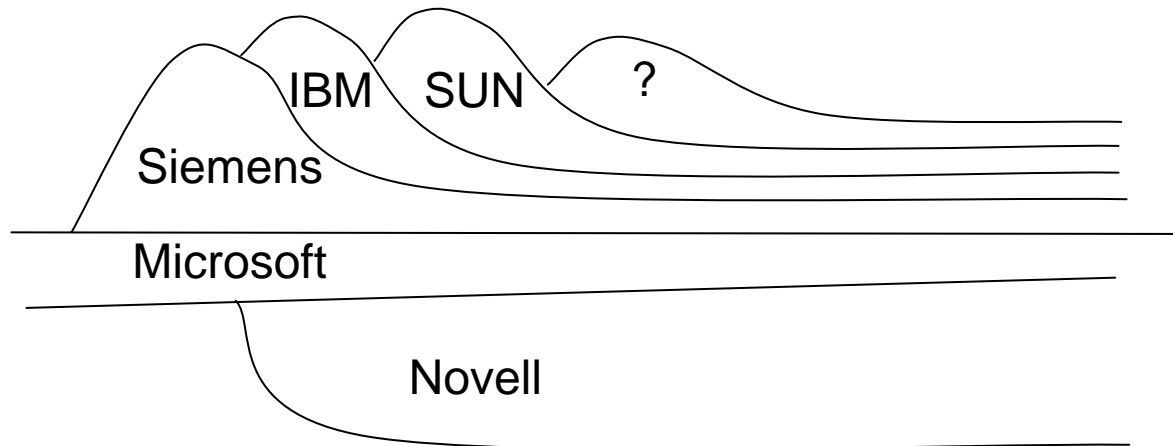
Statistik: Verzeichnissysteme

- Meistgenutztes System ist Tivoli Identity Manager von IBM
- Stark unterschiedliche Verwendung der Systeme

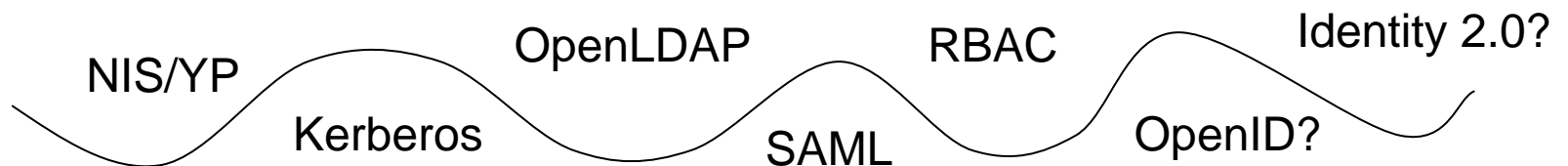


Proprietär vs. RYO

- Kommerzielle Metadirectories -> IdM-Systeme



- Eigenentwicklung: RZ-User-Management + DB
offene Standards



Kommerziell vs. RYO

- Kommerzielle Systeme:
 - Reich an Funktionen
 - Komplex
 - Steile Lernkurve
 - Selten vollständig
 - Hohe Einstiegskosten
 - Nachhaltig
- Eigenentwicklungen:
 - Schlank
 - Angepasst
 - Schnellere Erfolge
 - Schrittweises Wachstum
 - Betreuungsaufwändig
 - Personalabhängig
 - Externer Support ist möglich

IdM und Chipkarten

- Frühe Hochschulen:, z.B.:
 - Uni Bochum (Rubicon)
 - FH Braunschweig/Wolfenbüttel
 - TU Chemnitz
- In IdM-Planungen berücksichtigt: z.B.
 - IntegraTum (TUM, LRZ)
 - Uni Tübingen
 - Uni Rostock
- I.d.R. Link auf Chipkarten-ID im Benutzerverzeichnis
- Aktuell z.B.:
 - Thüringen (Codex): Thoska+
 - Uni FFM: Goethe-Card
 - Hochschulverbände = Studentenwerk
 - Zukunft:
 - Baden-Württemberg ?
 - Rheinland-Pfalz ?
 - Hamburg ?
- Eine Person – eine Identität – eine Chipkarte

IdM und Kooperationen

- Problem:
 - Zugriff auf geschützte Ressourcen gewähren, ohne selber alle (fremden) Identitäten verwalten zu müssen
- Lösung:
 - IdM-Föderationen, vertrauensvolle Zusammenarbeit zwischen Institutionen
- Technische Basis z.Zt.:
 - SAML2
 - Shibboleth

Hochschul-übergreifende IdM-Lösungen

Ausgehend von:

- Anwender-Gruppen, insbes.
 - Bibliotheken und Verlage,
 - Lehr-Verbünde und E-Learning,
 - Grid
- Organisationen
 - Hochschul-Allianzen
 - Landes-Initiativen

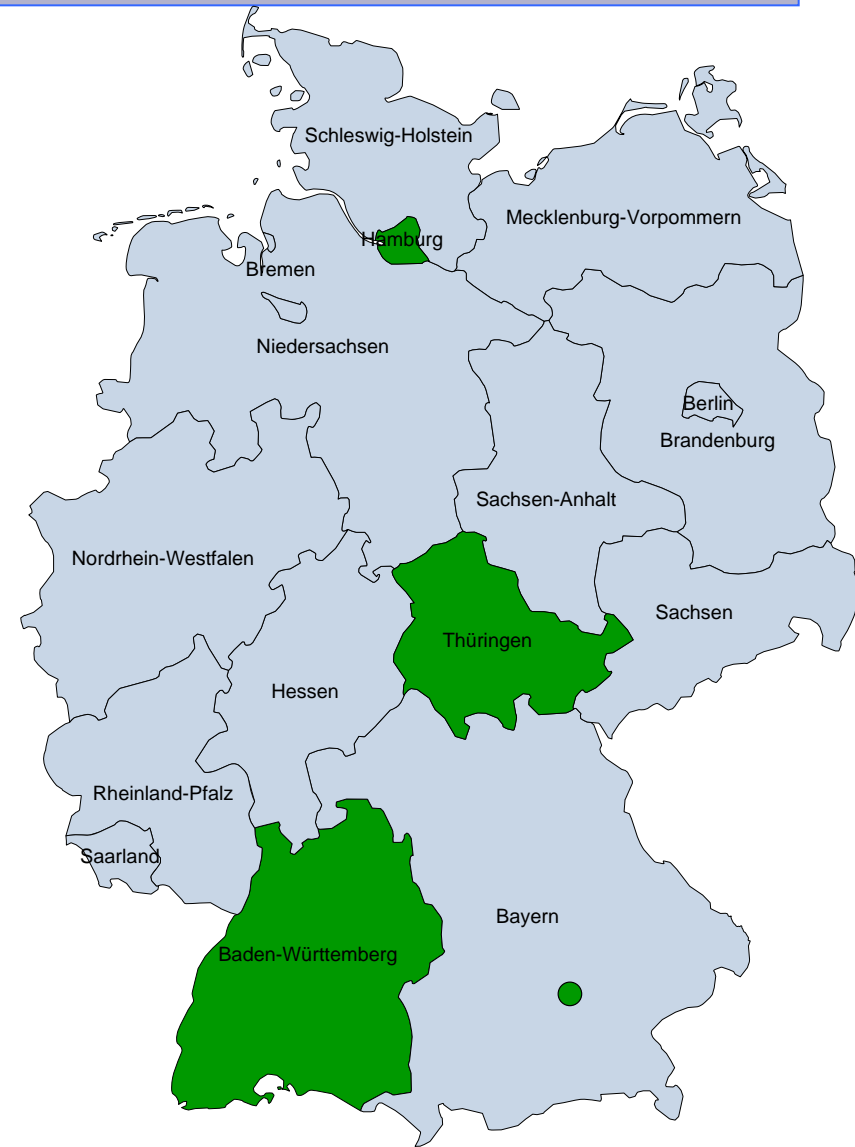
Verbünde für Anwendungen

- **Baden-Württemberg:**
Bibliotheken
- **Bayern:**
Bibliotheken, Virtuelle HS
- **Brandenburg:**
Bibliotheken (i.A.)
- **Niedersachsen:**
E-Learning, als Keimzelle
- **Rheinland-Pfalz:**
Virtueller Campus (SSO i.A.)
- **Sachsen:**
E-Learning



Verbünde der Einrichtungen

- **Münchner Raum:**
LRZ-zentriert (auf ca. 15 Studiengänge begrenzt)
- **Hamburg:**
Senat erwirkt zentrales IdM aller Hochschulen
- **Thüringen:**
alle HS-Rechenzentren erarbeiten gemeinsam lokale IdM-Lösung, Föderation und Bibliotheksanbindungen stehen noch aus
- **Baden-Württemberg:**
Ministerium macht Vorgaben für IdM-Nutzung



Wünsche an die Zukunft?

- Hochschulen (Ministerien, Hochschulangehörige) geben IdM das nötige Gewicht
- Alle Hochschulen nehmen an AAI und DFN-Roaming teil
- Anwendungen werden IdM-*aware*
- Anwendungsunabhängige Rollen- und Rechte-Verwaltung
- Stärkere Authentisierung mit Besitz und Geheimnis
- Benutzer-zentriertes IdM, jenseits SAML 2. Identity 2.0?

Schlussbemerkungen

Es besteht kein klares Bild, aber:

- Technische Voraussetzungen und Support für IdM und Föderationen sind vorhanden (User-Groups, ZKI-AK Verzeichnis-Dienste, DFN-AAI)
- Bewältigung interner organisatorischer Aufgaben ist wesentlicher als Lösung technische Probleme
- Ständige Herausforderung: Einfangen technischer und organisatorischer Inseln
- Gesichertes IdM ist Voraussetzung für moderne, integrierte Services
- Gesichertes internes IdM ist Voraussetzung für Föderationen mit externen Partnern
- Bedarf für Kooperationen kann Auslöser für interne IdM-Aktivitäten sein
- Von Anwendungen getriebenen Lösungen wirken i.d.R. nicht integrierend für gesamte Hochschulen (z.B. Bibliotheken, Grid)
- Zentralisiert koordinierte Ressourcen sind offenbar Voraussetzung für Erfolg bei übergreifenden Strukturen

Wir sind noch am Anfang eines Weges