

# Identitätsverwaltung und Single Sign-On an der MLU Halle-Wittenberg

-- ein Zwischenbericht --

Michael Schaarschmidt  
ZKI Arbeitskreis Verzeichnisdienste  
Herbsttreffen 2011



# Die Uni im Überblick

- 20.000 Studierende
- 20.000 Bewerber
- 4.000 Mitarbeiter ohne Medizinischer Bereich
- 4.300 Mitarbeiter Medizinischer Bereich
- 37.000 Mitglieder Bibliothek



2005

2006

2007

2008

2009

2010

2011

2012

2013

- SyBase-DB mit 2 Tabellen (Accounts, Gruppen)
- Gruppen-Tabelle: 300 Einträge (Gruppenname, Gruppenkennzeichen, gid, Gruppen-Ansprechpartner, Adresse, ...)
- Account-Tabelle: 28.000 Einträge (Name, Vorname, Geburtsdatum, uid, gid, Mail-Adresse, ...)



2005

2006

2007

2008

2009

2010

2011

2012

2013

- 21.000 Accounts ohne Zuordnung (Müll-Accounts)
- 5-Stelliger Account-Name: z.B. nmaef
- Gefühlte Trennung zwischen Mitarbeiter-Studenten, Gast- und Funktional-Accounts
- 10 Dienste provisioniert (Mail, Radius / WLAN, Parallel-Rechner, Cluster, ...), Mail, Zettel, ...



2005

2006

2007

2008

2009

2010

2011

2012

2013

- Anforderung: zentrale Generierung und Verwaltung von Studenten-Accounts!
- Entwurf eines relationalen DB-Modells (3. NF), mit dem Ziel, zentraler Account und Zugangsverwaltung zu zentralen Diensten
- prototypische Umsetzung auf Oracle-DB (XE), Web-GUI in PHP



2005

2006

2007

2008

2009

2010

2011

2012

2013

- Synchronisation der Daten aus und in HIS-SOS per DB-Abgleich
- Information an Studierenden per Willkommensbrief mit Imma-Unterlagen
- Automatische Verabschiedung der Studenten per Mail.
- Provisionierung studentischer Daten in LDAP





2005 2006 **2007** 2008 2009 2010 2011 2012 2013

- automatische Übernahme der Mitarbeiter-Daten (Uni) aus HIS-SVA
- Vollständige Generierung der Mitarbeiter-Accounts
- Provisionierung in LDAPs dezentrale Dienste



2005 2006 **2007** 2008 2009 2010 2011 2012 2013



- praktische Einführung von Gast- und Funktional-Accounts
- Account-Laufzeiten, automatische Informierung bei Ablauf
- Generierung Kommunikationsverzeichnis





2005 2006 2007 **2008** 2009 2010 2011 2012 2013

- automatische Übernahme der Mitarbeiter-Daten (Medizin) aus SAP-R3
- Anforderung: automatisch generierte Mailverteiler!





2005 2006 2007 2008 **2009** 2010 2011 2012 2013

- Umstellung der Accountgenerierung für Studierende auf Web Services
- Anforderung: Einführung Shibboleth für Web-basierte Bibliotheksdienste (nicht PICA-basierte Dienste)



A horizontal timeline arrow pointing to the right, with a green gradient and a dark green outline. It contains a series of years from 2005 to 2013. The year 2010 is highlighted in blue.

2005 2006 2007 2008 2009 **2010** 2011 2012 2013

- Erster Prototyp zu Shibboleth für die Bibliothek mit simpleSAMLphp
- Zweiter Prototyp zu Shibboleth für die Bibliothek mit Shibboleth (Java)



2005 2006 2007 2008 2009 2010 2011 2012 2013



- Schulung adm. Mitarbeiter zu Themen wie LDAP, Kerberos, Active Directory
- Einführung Single LogOn: Kerberos+LDAP - Active Directory - Cross Realm Trusts
- Einführung Shibboleth für Bibliothekszugänge
- Planung: Account-Vergabe für Bewerber
- prov. Einf. Chipkarten-basierte Authorisierung



2005 2006 2007 2008 2009 2010 **2011** 2012 2013

### System-Status

Gesamtanzahl Personen:	47637
Gesamtanzahl Accounts:	40766
Studenten-Accounts:	28682 ( <b>8981</b> )
privilegierte Studenten Accounts:	585
Mitarbeiter-Accounts:	3934
Mediziner-Accounts:	2275
Gast-Accounts:	1274 ( <b>668</b> )
Funktionale Accounts:	1242
Müll-Accounts:	2774





2005 2006 2007 2008 2009 2010 2011 **2012** 2013

- Umstellung auf genau einen Account pro Person
- Entkoppelung von Account und Account Typ
- Kopplung der Ressourcen an Rollen
- Kopplung Shibboleth + Kerberos
- Planung der Einführung einer Komm. IdM-Lösung