UNIVERSITÄT
DUISBURG
ESSEN

ZIM
Zentrum für Informations- und Mediendienste

Identitätsmanagement
an der
Universität Duisburg - Essen

Burkhard.Wald@Uni-DuE.de

Oktober 2009

IM History

1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009

★ DuE ★ HRZ ★ ZIM

AUM	AUM goes IM	AUM 4 DuE	AUM + ITIM	AUM=IM

Projektidee

Abschal-ten ITIM

Erstellung Feinkonzept

Übernahme Schlesiona

Abschluss IBM-Vertrag

Einstieg Wald

Dienstvereinbarung

AUM = Automatisches User Management

SOS-Feed

SVA-Feed

Gründe (Hoffnungen) für den Abschluss der ITIM-Lizenz

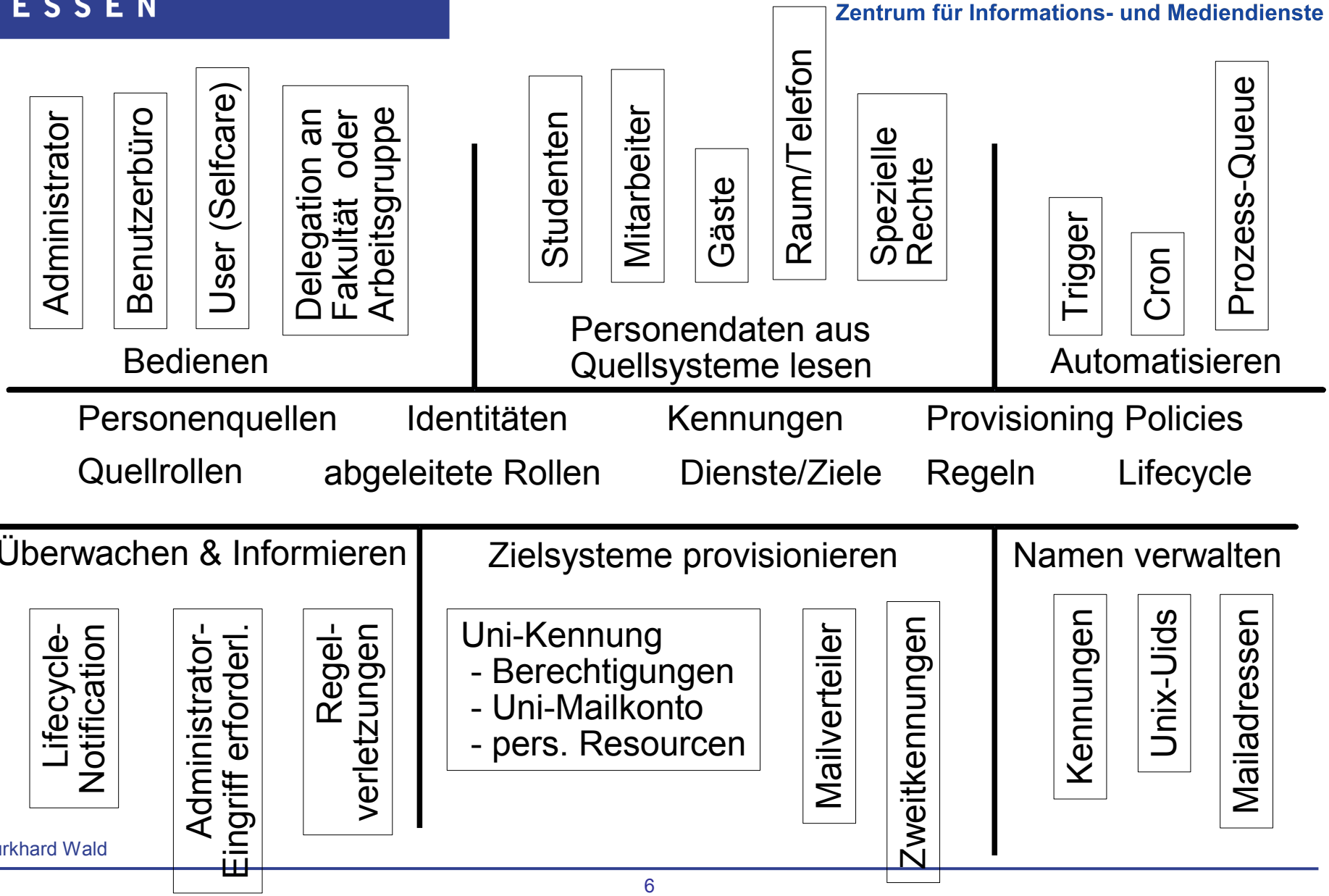
- Kommerzielle Fertiglösung
  - spart Entwicklungsaufwand
  - ist stabiler und leichter zu pflegen
  - bietet im Störungsfall Hersteller-Support
  - ist immer am Stand der Technik
- Gewinn durch gemeinsames Vorgehen in NRW

Gründe für die Abkehr von der ITIM-Lösung

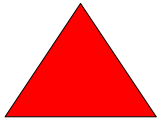
- System-Komplexibilität (Web-Sphere,MQ,LDAP,DB2,....)
- Großer Customizing-Aufwand
- ITIM hat nur geringen Anteil am gesamten IM
- Fehlende Stabilität
- Fehlende Flexibilität
- Kosten

Stattdessen

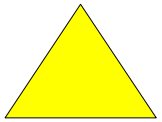
- Weiterentwicklung von AUM
- AUM war Provisionierungssystem mit Konnektoren zu allen HRZ-Diesten
- AUM war im Hause entwickelt auf der Basis von Perl, Perl-CGI, DB2
- AUM-Schema: Kunden <- Kennungen <- Dienste
- Neu erforderlich: Konzept für HR-Feeds


Administrator
Benutzerbüro
User (Selfcare)
Delegation an Fakultät oder Arbeitsgruppe
Bedienen
Studenten
Mitarbeiter
Gäste
Raum/Telefon
Spezielle Rechte
Personendaten aus Quellsysteme lesen
Trigger
Cron
Prozess-Queue
Automatisieren
Personenquellen
Identitäten
Kennungen
Provisioning Policies
Quellrollen
abgeleitete Rollen
Dienste/Ziele
Regeln
Lifecycle
Überwachen & Informieren
Lifecycle-Notification
Administrator-Eingriff erforderl.
Regel-verletzungen
Zielsysteme provisionieren
Uni-Kennung
- Berechtigungen
- Uni-Mailkonto
- pers. Resourcen
Mailverteiler
Zweitkennungen
Namen verwalten
Kennungen
Unix-Uids
Mailadressen

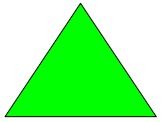
Wahrnehmungen einer Person



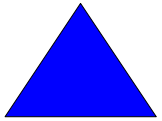
Person aus Fleisch und Blut im direkten Kontakt



Aktiver User in einem System

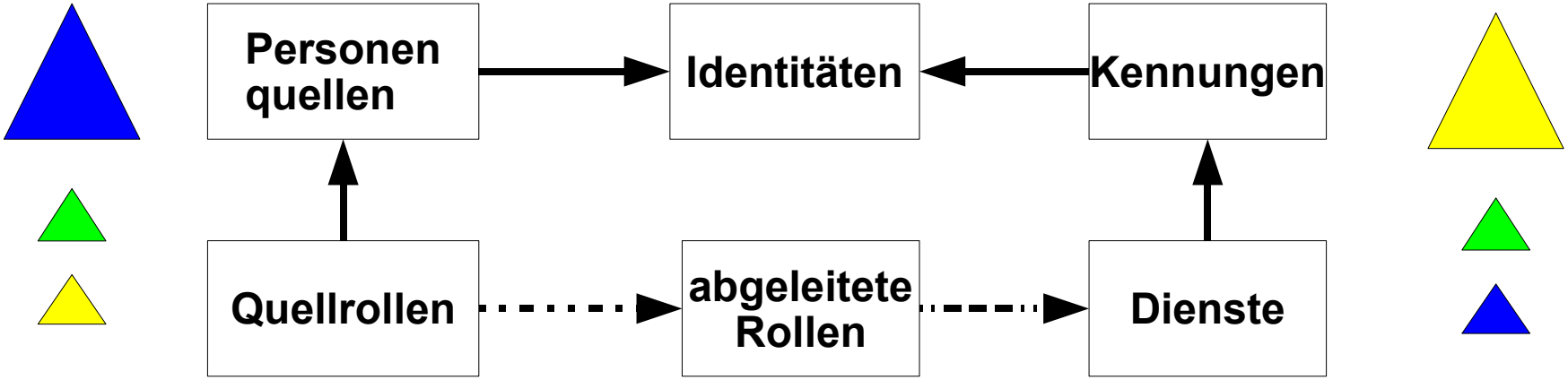


Frei zugägliche Info-Seite im Internet über eine Person



Personeneintrag in einer administrativen Datenbank

IM Kernschema



Personenquellen und Quellrollen

- Personenquellen
  - Quelle (SVA,SOS,LSF,...)
  - Key (Eindeutige ID in der Quelle)
  - Name,Vorname
  - Geburtsname,Geburtsdatum
  - Status (in der Quelle)
  - Änderungsdatum (Quelle)
  - Kundennummer im IM
  - (Uni-Kennung, Passwort)
  - (Mail, Raum, Telefon)
  - Importstatus und Datum

- Quellrollen
  - Quelle
  - Key
  - Nr.
  - Status
  - Periode
  - Bereich
  - Rolle

Status beim Lesen von Personenquellen

- automatisch zugeordnet über Name und Geb.-Datum
- automatisch zugeordnet über Mail-Adresse
- automatisch zugeordnet über Kennung
- automatisch zugeordnet über Bereich
- manuell zugeordnet

- unsicherer Match über Name
- zu häufiger Name
- Name schwierig
- mehrfacher Match
- Match über Mail-Adresse zurückgehalten da Name unstimmig
- Unstimmigkeit bei Kennung
- Sonstige Unstimmigkeit

- Kein Match, automatisch neu aufgenommen

- Kein Match, Neuaufnahme zurückgehalten

- manuell neu aufgenommen

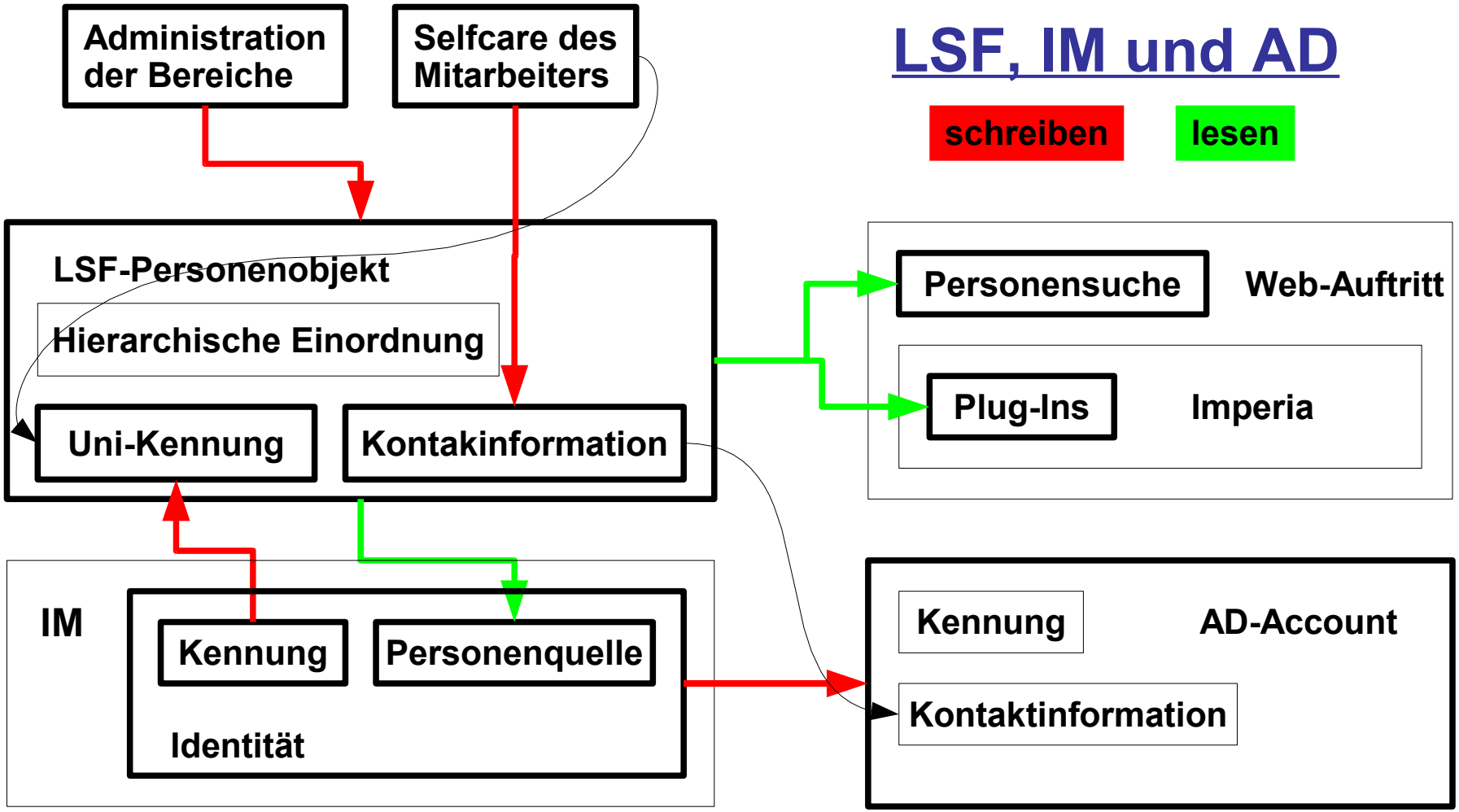
Abgeleitete Rollen

- Hinter einem Namen steht ein SQL-Select über Personenquellen und Quellrollen.
- Regelmäßig werden alle Rollen aller Personen geprüft
- Das Ergebnis wird in die Datenbank gesschrieben
- Dadurch ist es möglich „Gewinn“ oder „Verlust“ einer Rolle zu bemerken
- Die Ereignisse „Gewinn“ oder „Verlust“ einer Rolle können Prozesse auslösen. (definiertes Skript kommt in Job-Queue)
- Provisionierungsskripte werten die Rollen aus. Aus der Rolle wird so ein Flag oder eine Gruppenmitgliedschaft in AD oder LDAP (z.B. für Shibboleth)

Kontaktdaten aus LSF lesen

- LSF bildet Selfcare für öffentliche Kontaktinformation und die Administration durch Sekretariate ab.
- LSF ist integriert in den Web-Auftritt (Online-Personensuche), Imperia bietet Plugins.
- LSF ist Quellsystem für Kontaktdaten (Telefon, Raum, Kontakt-Mail-Adresse)
- IM liest LSF aus und ordnet diese einer Identität zu
- Zugeordnete Kontaktinformation kann z.B. ins AD geschrieben werden (globales Adressbuch für Exchange)
- Zugeornete Uni-Kennung kann ins LSF geschrieben werden (für Selfcare)

LSF, IM und AD


schreiben
lesen
Administration der Bereiche
Selfcare des Mitarbeiters
LSF-Personenobjekt
Hierarchische Einordnung
Uni-Kennung
Kontakinformation
Personensuche
Web-Auftritt
Plug-Ins
Imperia
IM
Kennung
Personenquelle
Identität
Kennung
AD-Account
Kontaktinformation

FSV und IM

- FSV = Finanzbuchhaltung von HIS
- Etwa 1000 Eingetragene Nutzer
- Wie kommen sie darein ?
- Wie kommen sie wieder heraus ?
- Welche Rolle übernimmt IM ?
- FSV nicht als IM-Ziel sehen sondern als IM-Quelle
- Neue FSV-Quellen werden im IM zugeordnet
- FSV-User bekommen die abgeleitete Rolle „fsv_user“
- Im IM wird Regel definiert: „fsv_user => mitarbeiter“
- Regelverletzung wird an FSV-Administratoren gemeldet

Studenten Lifecycle: Immatrikulation

- Einschreibung
  - Student gibt eigene Mail-Adresse an
- Unikennung mit Initalpassword wird mitgeteilt
- Student kommt durch „abgeleitet Rollen“ bereits auf automatische Mailverteiler
- Student schaltet die Kennung frei
  - Anmeldung an QIS-POS und LSF möglich (Rückmeldung, Belegung, etc)
  - Auch Moodle und BSCW
  - Uni-Mail-Adresse wir zugeteilt
  - Weiterleitung an private Adresse ist Defaulteinstellung

Studenten-Lifecycle: Exmatrikulation

- Exmatrikulation
- nach 2 Wochen: Verlust der abgeleiteten Rolle „Student“
  - Studentenattribut im LDAP verschwindet
- nach 6 Wochen: Student erhält eine Mail
  - Student kann Mail-Weiterleitung setzen.
- nach 6 Wochen: Kennung wird (bis auf Mail-Adresse mit Weiterleitung) gesperrt.
- Nach 12 Wochen: Alle Resourcen werden gelöscht, (Mail-Weiterleitung bleibt erhalten)

Herausforderung Exmatrikulation

- Wie ist die Rolle „Student“ genau definiert
- Gibt es einen anderen Status z.B. Mitarbeiter
- Hohe Dynamik im SOS
- Noch am Ende des Semesters kommt Rückmeldung für dieses Semester
- Deaktivierung muss dann rückgängig gemacht werden. (erneute Mail muss verschickt werden)
- Herausgehende Mail dürfen nicht mehrfach geschickt werden, und dürfen sich nicht widersprechen.
- Das ganze Hin und Herr muss protokolliert werden und muss für das Benutzerbüro nachvollziehbar sein. (Call-Bearbeitungen)

Neuer Mitarbeiter

- Wo erscheint neuer Mitarbeiter als erstes?
  - idealerweise im SVA-Feed
    - wird automatische gematched
    - Oder händisch gematched
    - Oder händisch neu angelegt
      - Brief mit Zugangsdaten per Hauspost
  - manchmal LSF-Feed
  - manchmal im Benutzerbüro
- Mitarbeiter erhält Uni-Kennung und Mail-Adresse
  - Kennung muss freigeschltet werden
  - Mail wird aber schon vorher zugestellt.
  - Zugang zu WLAN, Uni-Intern, VPN von außen

Weitere Herausforderungen: Mitarbeiter

- Managment von Kontaktinformationen
  - Siehe oben (LSF)
- Automatische Mailverteiler
  - wie bei Studenten
- Zugriffsberechtigungen (oder Verteiler) auf Grund von Zugehörigkeit zu Gruppen und Bereichen
  - Daten aus SVA für die Praxis nur eingeschränkt nutzbar
  - Einsatz von „Grouper“ geplant
- Ausscheiden von Mitarbeitern
  - Siehe FSV
  - Siehe Exmatrikulation

Thema Gäste : bleibt schwierig

- Allgemeines Gästeproblem
  - Gast muss Status nachweisen
  - Dienstleister muss Status verifizieren
- Spezielles Gästeproblem
  - Was dürfen und bekommen die Gäste
    - Finanzielle Aspekte
    - Lizenzrechtliche Aspekte
    - Aspekte bzgl. Außendarstellung
    - Administrative Aspekte (Prüfungen, Abstimmungen)
    - Aspekte bzgl. Vertraulichkeit

Online Registrierungsanwendung für Gäste

- Registrierung, Einladung und Bestätigung
- Kein weiteres Personenverzeichnis, bildet nur einen Bestätigungsworkflow ab
- Administratoren in den Bereichen
- Das ist nur auf Lehrstuhlebene möglich
- Gibt es überhaupt Gäste?
  - Lehrbeauftragte und SHKs stehen im SVA
  - Promotionsstudenten stehen im SOS
- Keine qualitativ wertvollen Dienste für Gäste

Handlungsfelder 2010

- Nutzbarmachen von Kontaktinformationen
- Automatische Mailverteiler für Mitarbeiter etablieren
- Grouper zum Einsatz bringen
- Mehr für den Prozess „Mitarbeiter scheidet aus“ tun
- Shibboleth und/oder CAS vermehrt intern zum Einsatz bringen.
- Datenabgleich mit Klinikum
- Gesamtkunstwerk Identitymanagment für Hochschule und ZIM durchschaubarer machen. (Prozesshandbuch, Betriebshandbuch)