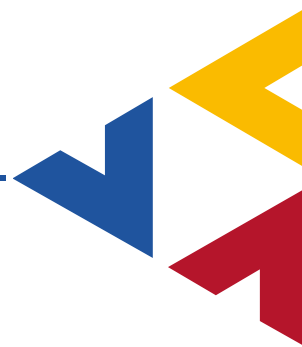


Klinikweites, einheitliches Identitymanagement

Anforderung an Subsysteme

KIS-RIS-PACS und DICOM
Mainz, 3. und 4. Juli 2009

Steffi Druckenmüller, Dipl. Inform. (FH)
Leiterin Zentrum für Informationstechnologie



Eberhard-Karls-Universität
UKT
Universitätsklinikum Tübingen

▶ Problemstellung

- ▶ unterschiedliche Mitarbeiter-Typen im Unternehmen (Festangestellte, MA aus GmbH's, Gastärzte, Gastdozenten, Zivi's, PJ'ler, Praktikanten...)
- ▶ unzureichende Provisionierung von digitalen Identitäten (erstellen, verwalten, deaktivieren, löschen)

▶ Anforderungen

- ▶ funktionstüchtige Infrastruktur für HBA, PKI, Workflowszenarien, Employee-Selfservices
- ▶ Verprobung der Gültigkeit der digitalen Identität gegen das korrespondierende Pendant im Personalsystem

Ziele und Erwartungen an ein IDM



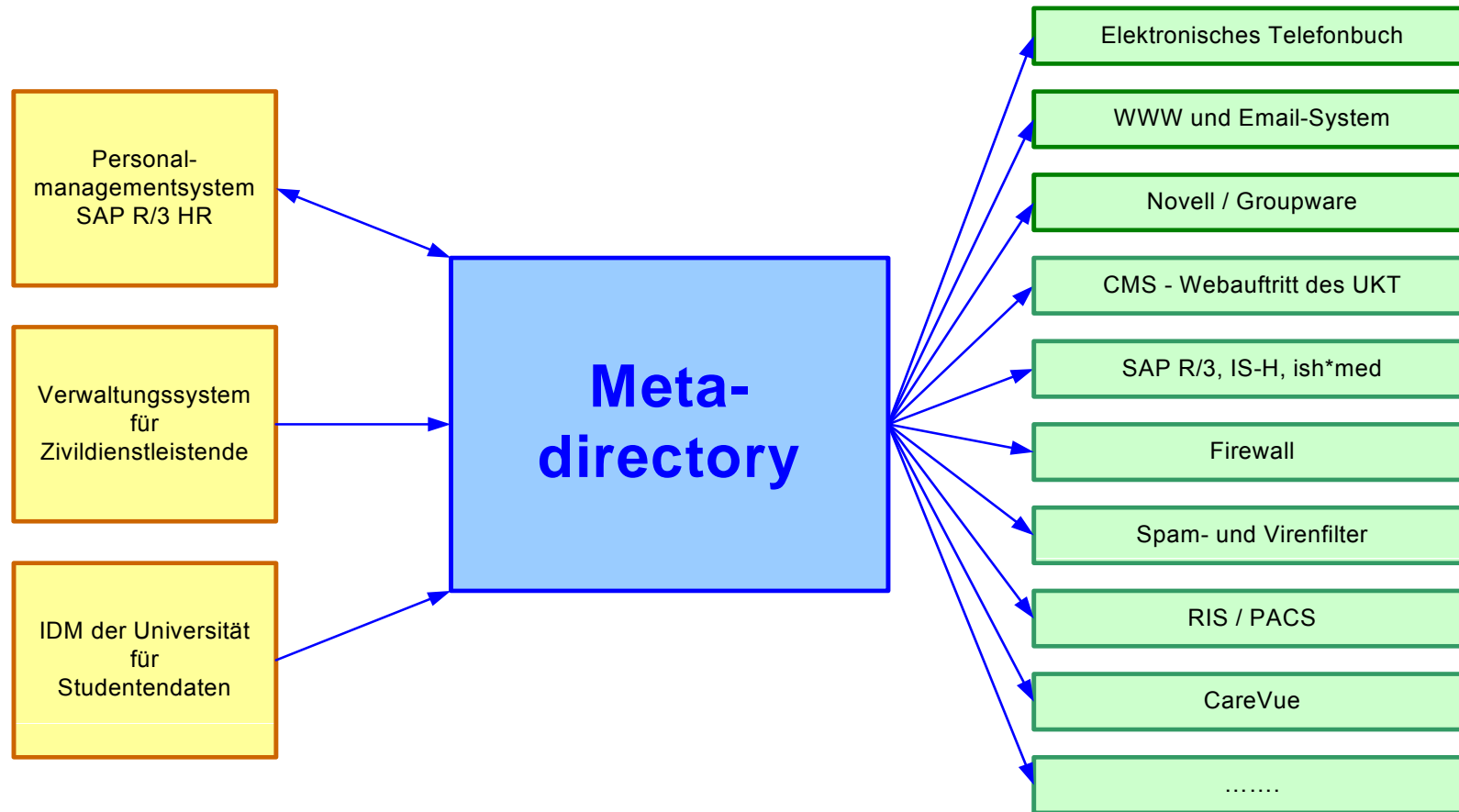
- ▶ unternehmensweit einheitliche Identifikationsverfahren aller Personentypen
- ▶ unternehmensweit eindeutiges Kriterium zur Identifikation aller Personentypen
- ▶ Etablierung einer Infrastruktur:
 - ▶ für Telefon-, dienstliche Anschrift-, E-Mailverzeichnis
 - ▶ durchgängiges elektronisches Antragsverfahren mit Authentifizierung
 - ▶ Passwortsynchronisation
 - ▶ Rechte- und Rollenverwaltung
- ▶ Benutzerkonsolidierung in den Subsystemen
- ▶ Höhere Sicherheit für Zugriffsrechte
- ▶ Synchronisation nur in eine Richtung
- ▶ Anmeldung an einem Subsystem unabhängig von der Verfügbarkeit IDM

Welches System spielt welche Rolle?



- ▶ Führendes System für Personaldaten
 - ▶ SAP-HR oder andere Personendatensysteme
 - Lieferant von Personenstammdaten und deren Gültigkeit
 - Lieferant des Identifikationskriteriums einer Person
- ▶ Führendes System für digitale Identitäten
 - ▶ Metadirectory
 - Empfänger der Persondaten und deren Gültigkeit
 - Produzent und Lieferant der eindeutigen digitalen User-ID
 - Verwaltung aller digitaler Identitäten
- ▶ Klinische und administrative Subsysteme
 - Empfänger relevanter digitaler Identitäten und deren Gültigkeit
 - Verprobung der Gültigkeit der digitalen Identitäten gegen das Metadirectory
- ▶ Anbindung der Systeme via lizensierter Treiber
 - ▶ HR – Metadirectory
 - ▶ Metadirectory – SAP ...
 - ▶ Metadirectory – MS AD, MS Exchange, Novell, Lotus Notes
 - ▶ Metadirectory – andere LDAP v3-Verzeichnisse

Systemverbund eines IDM



Synchronisation

- ▶ **Personaldatensystem**
 - ▶ erhält eine neue verpflichtende Qualität
 - ▶ verbindliche Anforderungen mit Zeitvorgabe (SLAs)
 - ▶ Grundsteinlegung für das Rollenkonzept
 - ▶ zeitnahe und realistische Abbildung der Aufbauorganisation des Unternehmens

- ▶ **SAP und alle andere Subsystem**
 - ▶ Übernahme eines Identifikationskriteriums
 - ▶ Bereinigung der Benutzerdatenbestände
 - ▶ Implementierung der Synchronisationsszenarien

 - ▶ Definition des spezifischen Rollenkonzeptes

Besten Dank für Ihre Aufmerksamkeit.