



# Workshop cHL-hybrid, MIRO, MOVE, MIAMI

Projekt MIRO

Identitätsmanagement



- **Beschreibung**
- **Begriffe und Definitionen**
- **Ziele und Erwartungen**
- **Architektur, Software**
- **Stand des Projekts**

**„Zu viele Dienste, Anwendungen und Systeme speichern Identitätsinformationen an zu vielen Stellen, ohne die Daten zu integrieren oder wenigstens zu synchronisieren“**

(„Ich-Findung“, Linux Magazin 05/2005)

**„Zur wirksamen Unterstützung von Forschung, Lehre, Studium, Verwaltung und Öffentlichkeitsarbeit soll jedem, der in oder mit der Hochschule zu tun hat, ein einheitlicher, direkter und vollständiger Zugang zu allen Diensten, Informationsquellen und Kommunikationspartnern angeboten werden unter Berücksichtigung der Rolle(n), Aufgaben und persönlichen Berechtigungen eines jeden.“**

(Feinkonzept „Identity Management Universität Duisburg Essen“)

### Identität

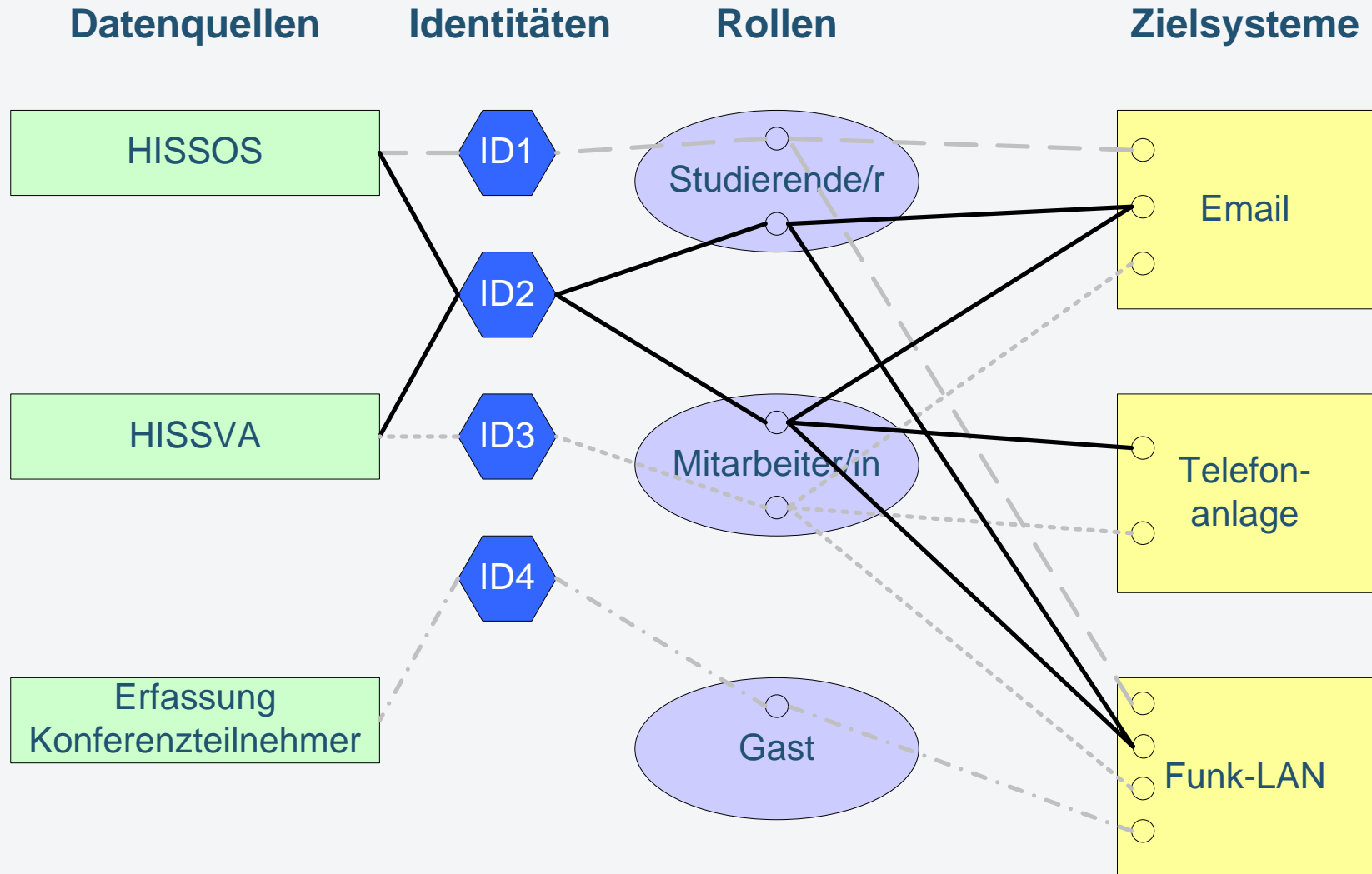
- Summe der Merkmale, anhand derer sich ein Objekt von anderen unterscheidet

### Provisioning

- Prozess der Erstellung, Änderung und Löschung von Benutzerobjekten auf Zielsystemen, automatisiert oder interaktiv
- Hier: Zugang zu Ressourcen herstellen, Personendaten eintragen (**Account**)
- **Rollenbasiert**

# Projekt MIRO – Identitätsmanagement

## Rollenkonzept



### Ziel

- Verlässlichen Zugang zu vielfältigen Ressourcen regeln

### Aufgaben

- Personendaten verwalten, aus versch. Quellen konsolidieren
- Identitäten herausbilden und überprüfen (Authentisierung)
- Zugang zu Ressourcen kontrollieren (Autorisierung)
- Organisationsstruktur abbilden
- Änderungen nachvollziehbar machen (Auditing)
- Single-Sign-On

### Erwartungen an das Identitätsmanagement

- Reduktion des administrativen Aufwandes
  - Nur noch eine zentrale Komponente zu administrieren
  - Automatisierte Workflows
- Wesentlich schnellere Reaktionszeiten
- Selbstadministration und Realisierung der informationellen Selbstbestimmung
- Sicherheitszuwachs
- Zentrales Auditing (Änderungen sind nachvollziehbar)
- Verlässliche Personendaten

### Erfahrungswerte im Identitätsmanagement

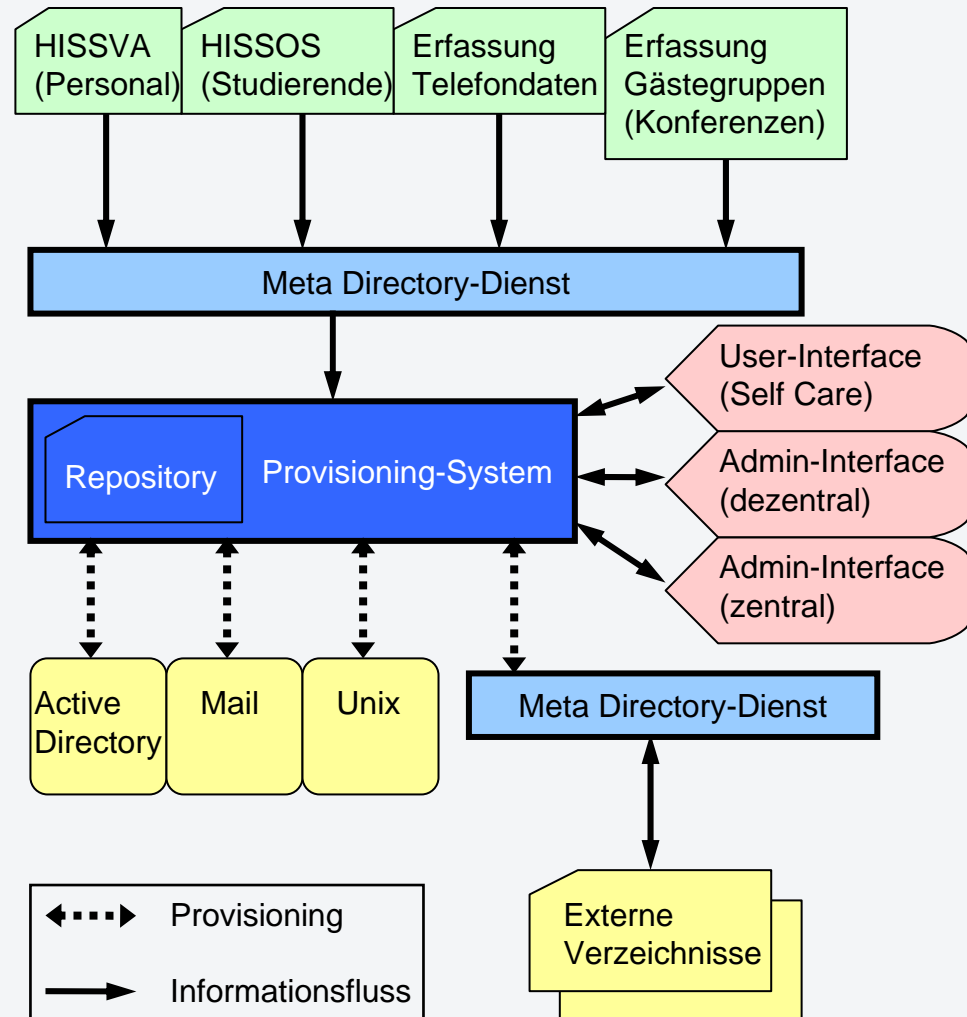
- Ab 3.000 Benutzer kann sich eine Identity Management lohnen
- Ab 10.000 Benutzern amortisiert sich der Aufbau eines automatisierten Identity Management in jedem Fall
- **Ab mehreren 10.000 Benutzern ist das Fehlen eines Identity Managements ein echter Wettbewerbsnachteil für jede Organisation!**

(Feinkonzept „Identity Management Universität Duisburg Essen“)



# Projekt MIRO – Identitätsmanagement

## Architektur



### IBM Tivoli Produkte

- NRW-Konsortiallizenz
- Produktpalette, bestehend aus:
  - IBM Tivoli Identity Manager (ITIM, TIM)
  - IBM Tivoli Directory Integrator (IDI, TDI)
  - IBM Tivoli Access Manager (TAM)
- Zusätzlich beteiligte Produkte:
  - IBM Directory Server (IDS)
  - IBM DB2
  - IBM WebSphere Application Server, IBM WebSphere MQ

### Zu berücksichtigende Personen im Identitätsmanagement

- Studierende (Ordentliche Studierende, Gast- und Zweithörer/innen, Studierende andere Hochschulen in MS)
- Mitarbeiter/innen
- Ehemalige (Alumni, Emeriti, ehemalige Mitarbeiter)
- Konferenzteilnehmer
- Gäste
- Bürger (Benutzer der ULB)
- Externe (Firmenmitarbeiter, etc.)

### Verzeichnisse an der WWU

- HIS-Anwendungen: HISSOS (Studierende), HISSVA (Mitarbeiter), HISMBS (Organisation), HISLSF (Lehrveranstaltungen), HISPOS (Prüfungsverwaltung)
- Telefon- u. Adressverzeichnis, Telefonanlage
- Schließsysteme
- ULB-Nutzer
- Benutzerverwaltung in versch. Zielsystemen: Unix (DCE, NIS, /etc/passwd), Windows (AD), Mail, BSCW, ...
- Abrechnungssysteme (Print&Pay, uni@home plus)
- WWUBEN

### Alte Benutzerverwaltung: WWUBEN

- Oracle Datenbank
- Zwischen Identitäts- und Account-Management
- 111.000 Nutzer, 43.600 davon aktiv
- 2.342 Benutzergruppen, 1.989 davon aktiv
- Provisioniert u.a. DCE, AD (uni-muenster, nwznet.uni-muenster), Unix-System IVV5, Kerberos (neu)
- Identity-Feed:
  - CSV-Datei aus UniV (HISSOS, HISSVA)
  - Nutzer-ID durch UniV generiert (neu bei Mitarbeitern)

### Vorabuntersuchung Datenschutz

- Abgeseget am 14.11.2005 vom Datenschutzbeauftragten der WWU

### NRW-Projekt Identitätsmanagement

- 10 beteiligte Hochschulen
  - RWTH Aachen, Uni und FH Bielefeld, Uni Bonn, Uni Duisburg Essen, DSH und FH Köln, FH Lippe und Höxter, Uni Münster, Uni Paderborn

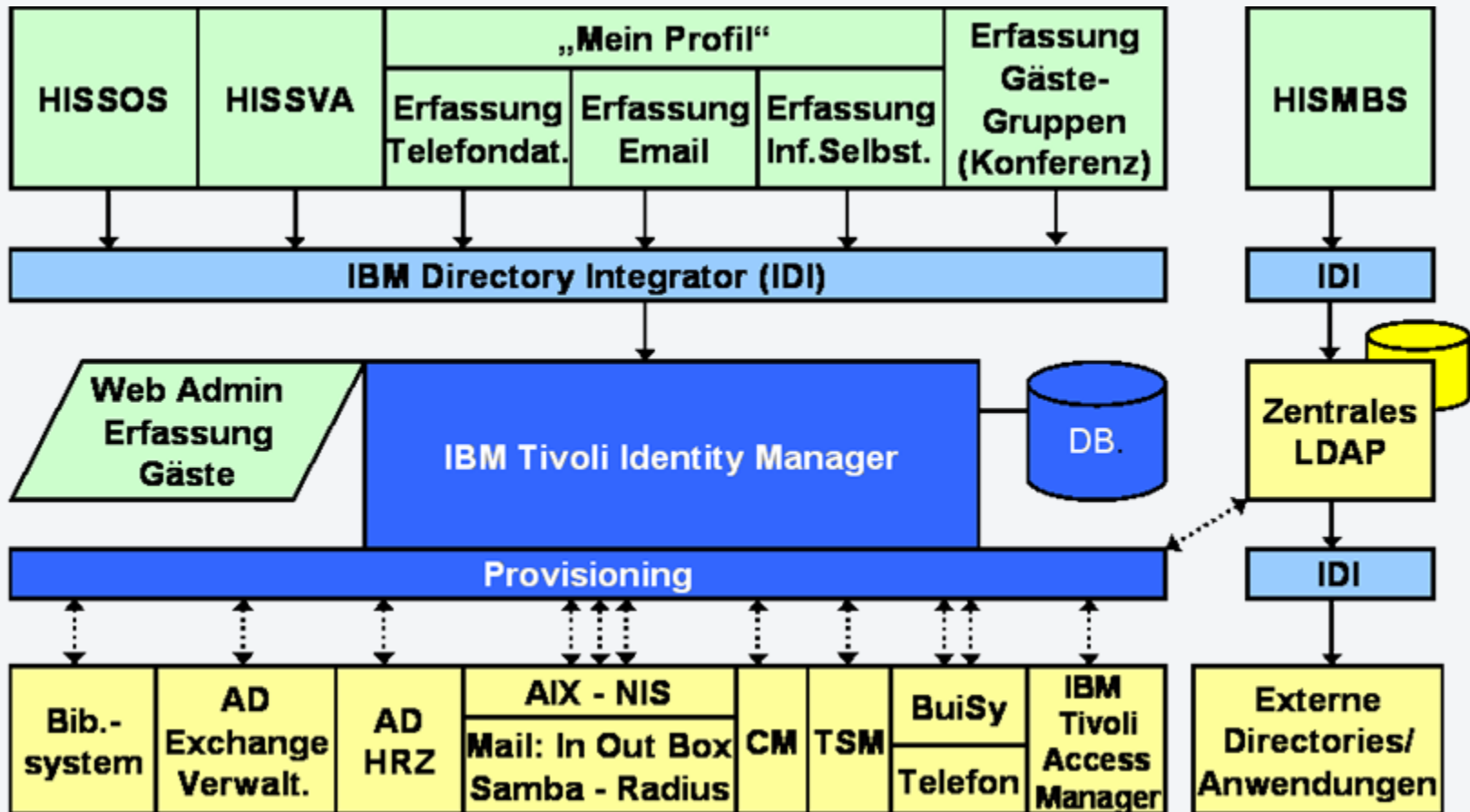
### Prototyp

- Entwickelt durch die Universität Duisburg Essen und IBM

# Projekt MIRO – Identitätsmanagement

## Prototyp

### Feinkonzept Universität Duisburg-Essen



**Vielen Dank  
für  
Ihre Aufmerksamkeit!**



## Backup

AP6-1: Einarbeitung in das vorhandene Produkt

AP6-2: Installation der Software und Einspeisung von Identitäten

AP6-3: Anschluss von Ressourcen an das Identitätsmanagement

AP6-4: Rollen und Rechte im Provisioning-System

AP6-5: Einrichtung der Profil- und Selbstadministrationsdienste

AP6-6: Einrichtung der Organisationsstruktur in LDAP

AP6-7: Public-Key-Infrastrukturen in LDAP

AP6-8: Einbringung von besonderen Identitäten

AP6-9: Besonderheiten für den Einsatz im Informationsmanagement

AP6-10: Identitätsmanagement für Sachen

# Projekt MIRO – Identitätsmanagement

## Arbeitsplan

### Arbeitsplan wie zunächst im Projektantrag vorgesehen

Projektjahr	PM	2005		2006				2007				2008				2009				2010		
		III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	
AP6-1: Einarbeitung in Produkt	6	■	■																			
AP6-2: Software u. Identitäten	12		■	■	■	■																
AP6-3: Anschluss Ressourcen	21	■	■	■	■	■																
AP6-4: Rollen u. Rechte	15							■	■	■	■											
AP6-5: Profil- u. Selbstadministration	12		■	■	■	■																
AP6-6: Organisationsstruktur in LDAP	9							■	■	■												
AP6-7: PKI in LDAP	9														■	■	■	■				
AP6-8: Besondere Identitäten	12											■	■	■	■							
AP6-9: Besonderheiten im Einsatz	21			■	■	■	■	■	■													
AP6-10: ID-Management für Sachen	9														■	■	■					
Summe	126																					