Westfälische
Wilhelms-Universität
Münster

Workshop c3m-II

Identitätsmanagement

Dr. Gunnar Dietz

Projekt MIRO, Universität Münster

IKM service
ULB • ZIV • UniV

Gliederung

- **Beschreibung**
- **Architektur**
- **Stand des Projekts**
- **Servicecharakter**

Ziel

- Verlässlichen Zugang zu vielfältigen Ressourcen regeln

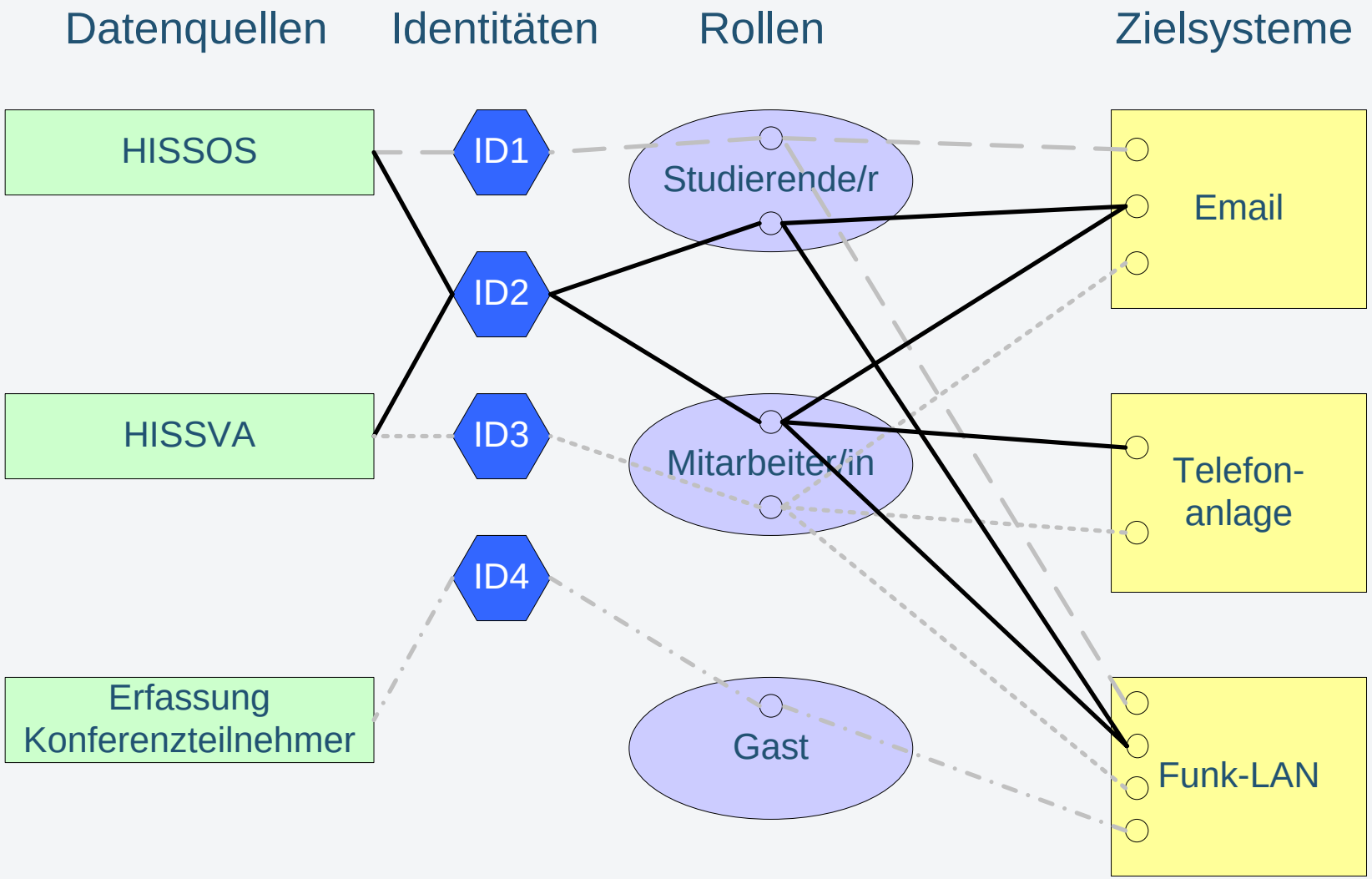
Aufgaben

- Personendaten verwalten, aus versch. Quellen konsolidieren
- Identitäten herausbilden und überprüfen (Authentifizierung)
- 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

Identitätsmanagement
Rollenkonzept



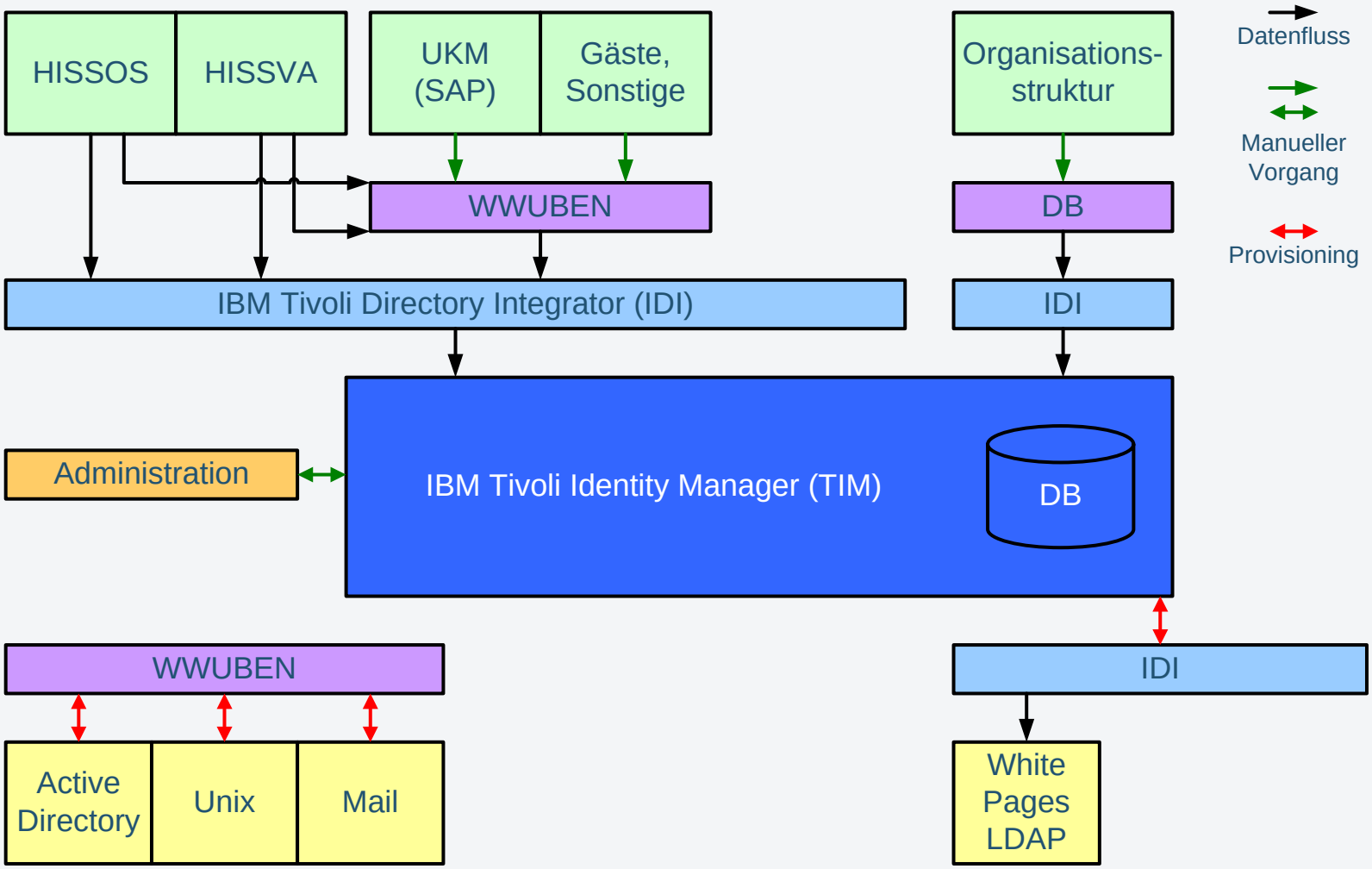
Alte Benutzerverwaltung: WWUBEN

- 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)

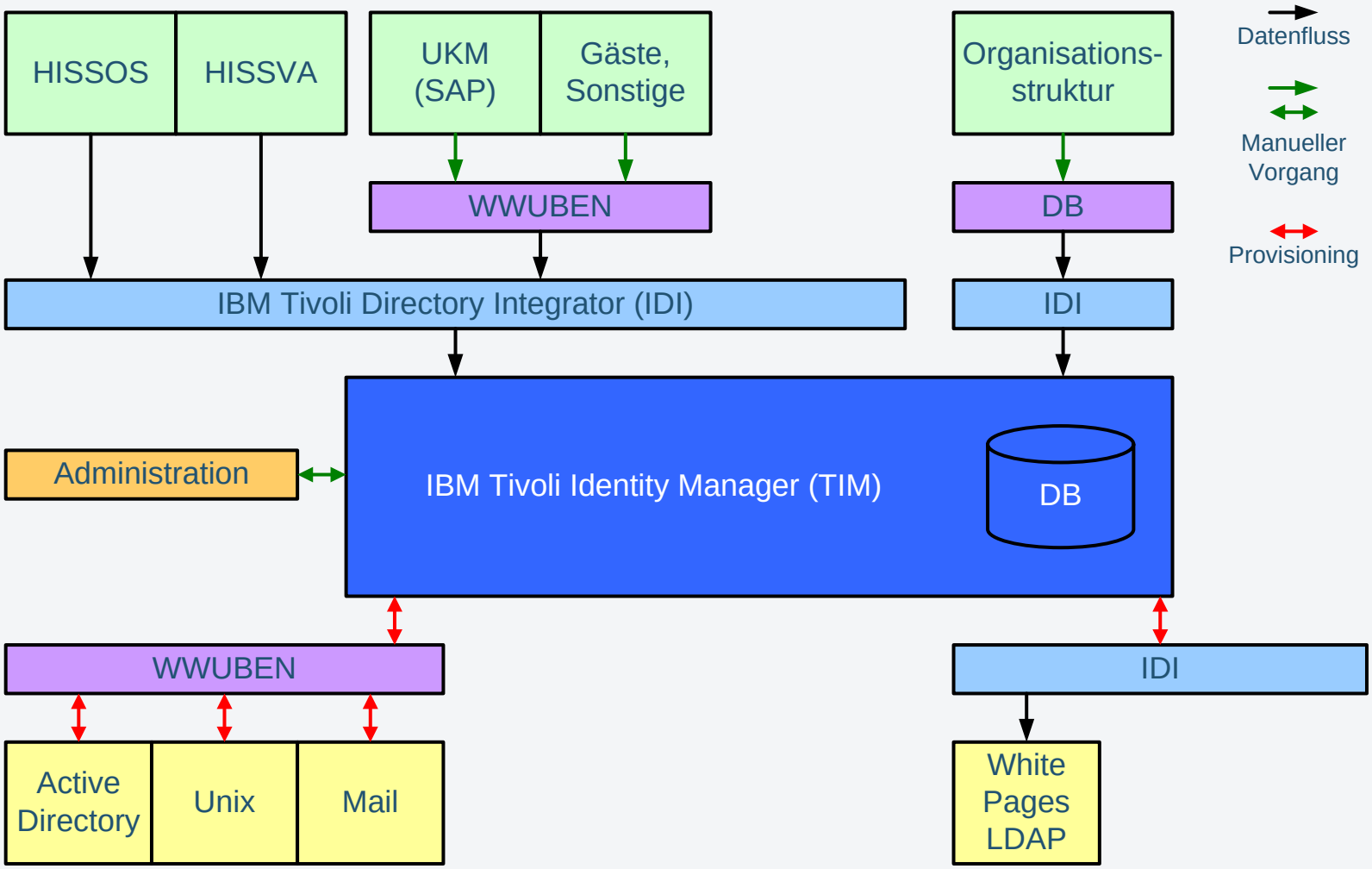
IBM Tivoli Produkte

- 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

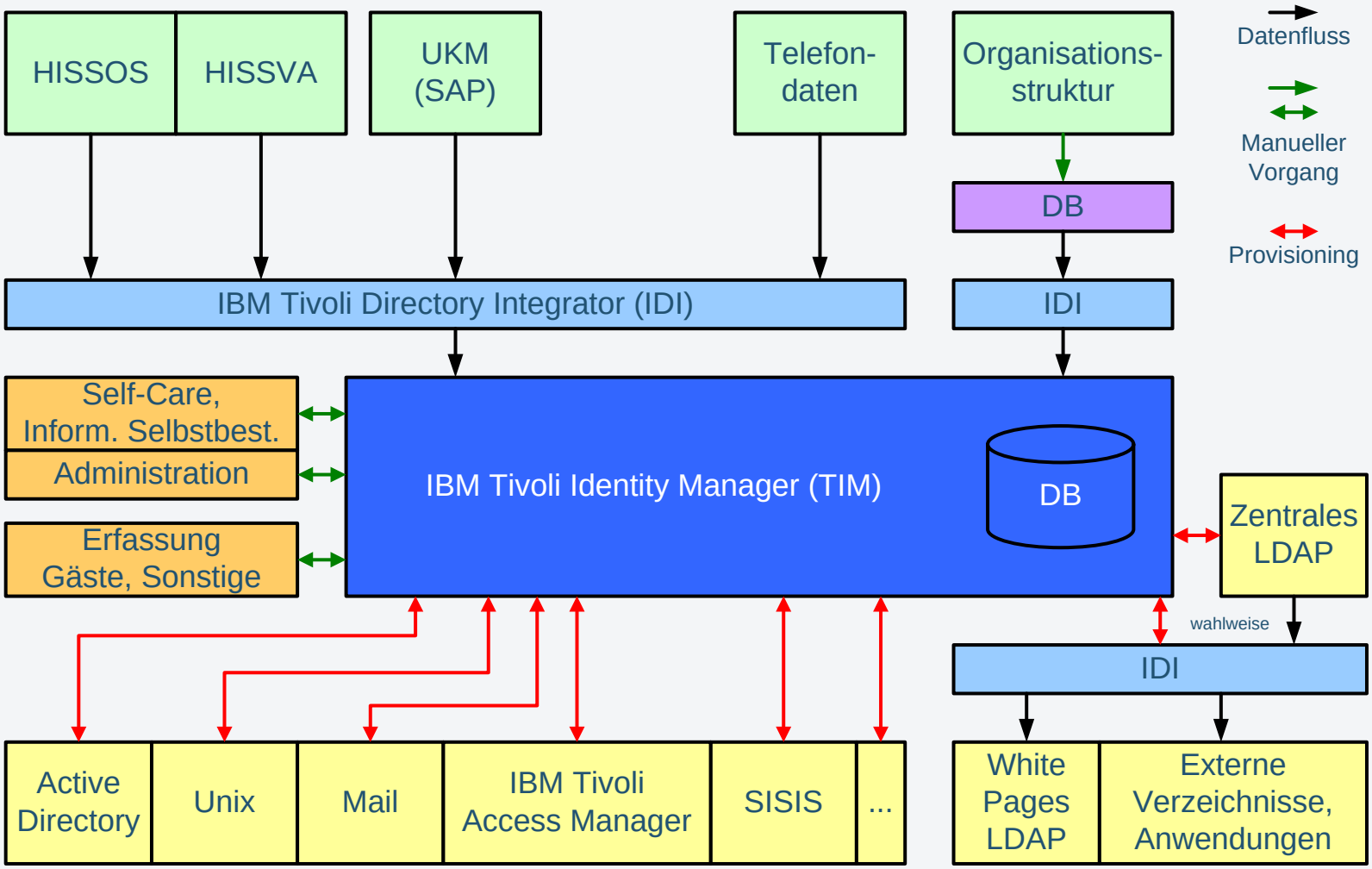
Identitätsmanagement
Architektur, aktueller Stand



Identitätsmanagement
Architektur, nächster Schritt



Identitätsmanagement
Architektur, Ziel



Stand des Projekts

- IdM-NRW (technische und konzeptionelle Kooperation)
  - Feinkonzepte (Uni DuE, Uni Bi, RWTH Ac)
  - IBM Prototyp
- Datenschutz-Vorabkontrolle

- Referenz-Installation des Prototypen
- Neu-Installation ohne Prototyp

- HR-Feeds implementiert
- Erstes Zielsystem provisioniert (LDAP)

Weiteres Vorgehen

- Realisierung des Gruppenkonzepts
  - Bestandsaufnahme der Gruppen und Konsolidierung
  - Gespräche mit IVVen und Fachbereichen durch MIRO-AP 4
- Performance und Ausfallsicherheit
- Provisionierung weiterer Zielsysteme
  - u.a.: Anbindung Bibliothek (SISIS)
- Self-Care GUIs
  - u.a.: Realisierung der Informationellen Selbstbestimmung
- Realisierung des Mappings
- Administrations-Konzept
- Erstellung eines (Fein-)Konzepts

Provisionierung von Zielsystemen als Service

- Beispiel: Provisionierung eines LDAPs für Authentifizierung und Autorisierung in einer Anwendung
  - inetOrgPerson oder beliebiges Schema
  - Provisionierung erfolgt automatisch, Änderungen werden sofort an das Zielsystem weitergegeben
  - Vorteil: Aktuelle Benutzerdaten
  - Reconcilation: Änderungen im Zielsystem können an das Identitätsmanagement zurückübertragen werden.

- Wichtig: Vorgang muss klar geregelt sein, Abstimmung mit den Hoheitsträgern der Daten nötig (UniV) -> Verfahren entwickeln.

60000 Personen

2000 Rollen

1 Identitäts-Management

Vielen Dank

für

Ihre Aufmerksamkeit!