Westfälische
Wilhelms-Universität
Münster

Gruppenverwaltung im Identitätsmanagement-Kontext

Reinhard Mersch

Zentrum für Informationsverarbeitung (ZIV)

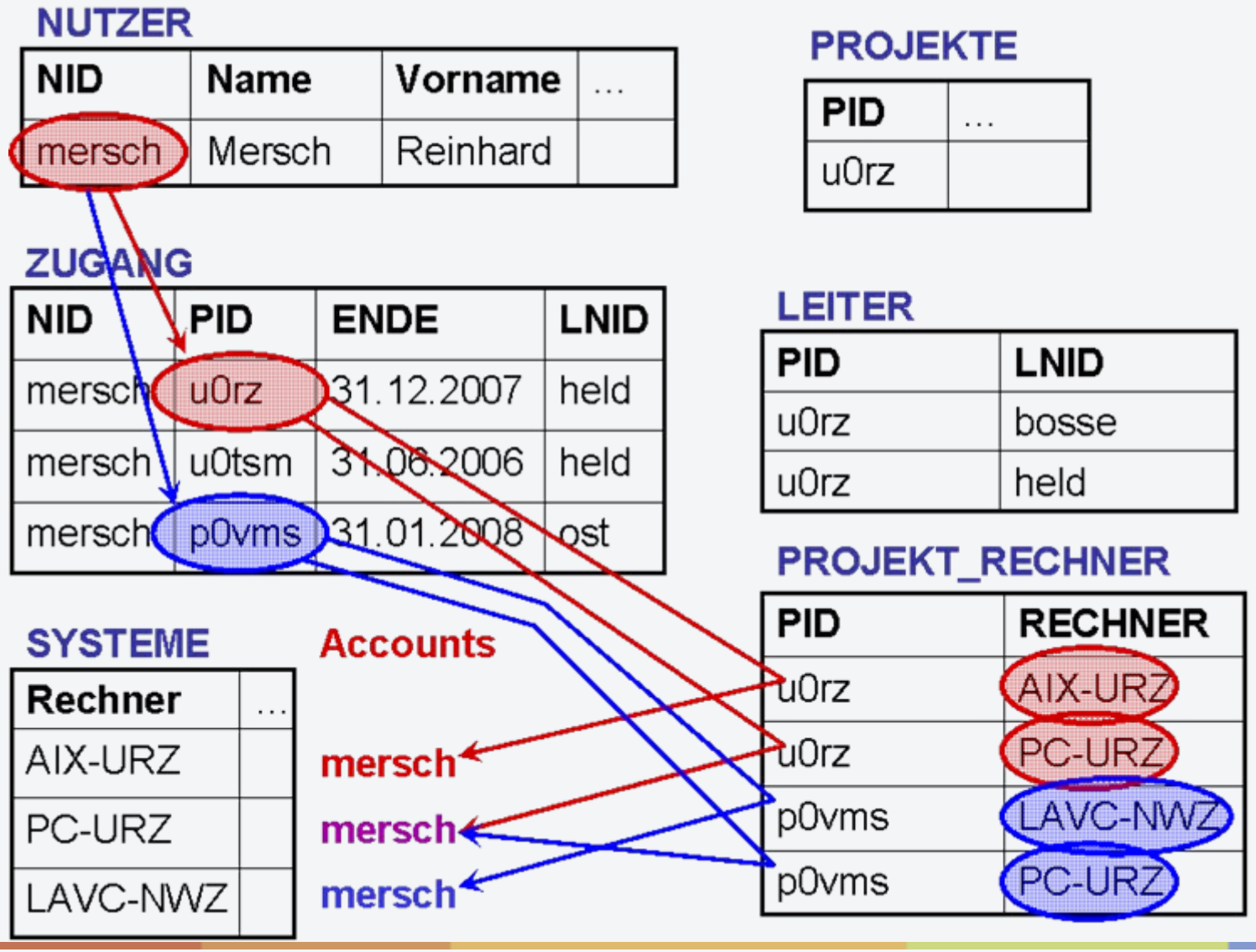
Westfälische Wilhelms-Universität (WWU) Münster

IKM service
ULB • ZIV • UniV

WWUBEN: Nutzer- und Gruppenverwaltung

- Jeder Nutzer ist mindestens einer Gruppe (**Projekt**) zugeordnet (Projekt-**Zugang**).
- Jede Gruppe wirkt auf eine Reihe von Ziel-**Systeme**n.
  - Pro Zielsystem ein Account
  - Alle Accounts eines Nutzer haben dieselbe Kennung.
- Für jede Gruppe gibt es mindestens einen Verantwortlichen (**Leiter**).
- Gruppenzugänge steuern (kumulativ):
  - Zugänge zu Systemen und Ressourcen
  - Spezielle Rechte auf den Zielsystemen
- Vergabe der Gruppenzugänge:
  - einige automatisch (Informationen in den HR-Feeds)
  - sonst manuell (schriftlicher Antrag oder Admin-Oberfläche)
- Projekt-Zugänge sind zeitlich **befristet**.

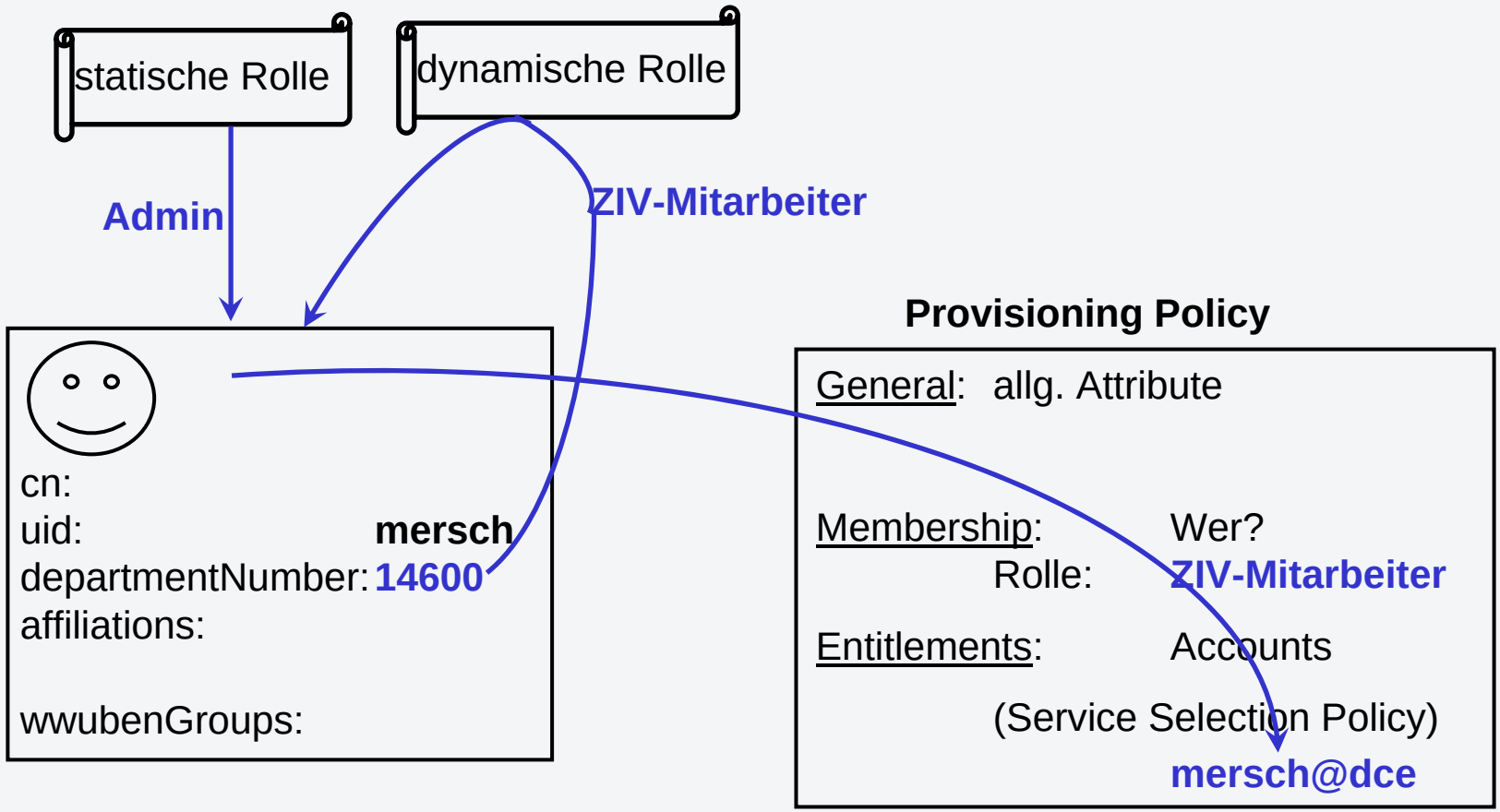
WWUBEN: Nutzer- und Gruppenverwaltung



WWUBEN: Gruppenübersicht

- 1556 aktive Projekte (Gruppen)
- 50236 Primär-Zugänge
- 36866 zusätzliche Zugänge
  - 2500 automatisch vergeben an MitarbeiterInnen
  - 11000 automatisch vergeben an Studierende
- 61 automatisch zugewiesene Projekte
- Projekt-Typen:
  - Institut (354 Projekte)
  - Arbeitsgruppe (362)
  - Zusatz (meist Admin) (177)
  - Info-Anbieter / Imperia-Rolle (592)
  - Externe (58)

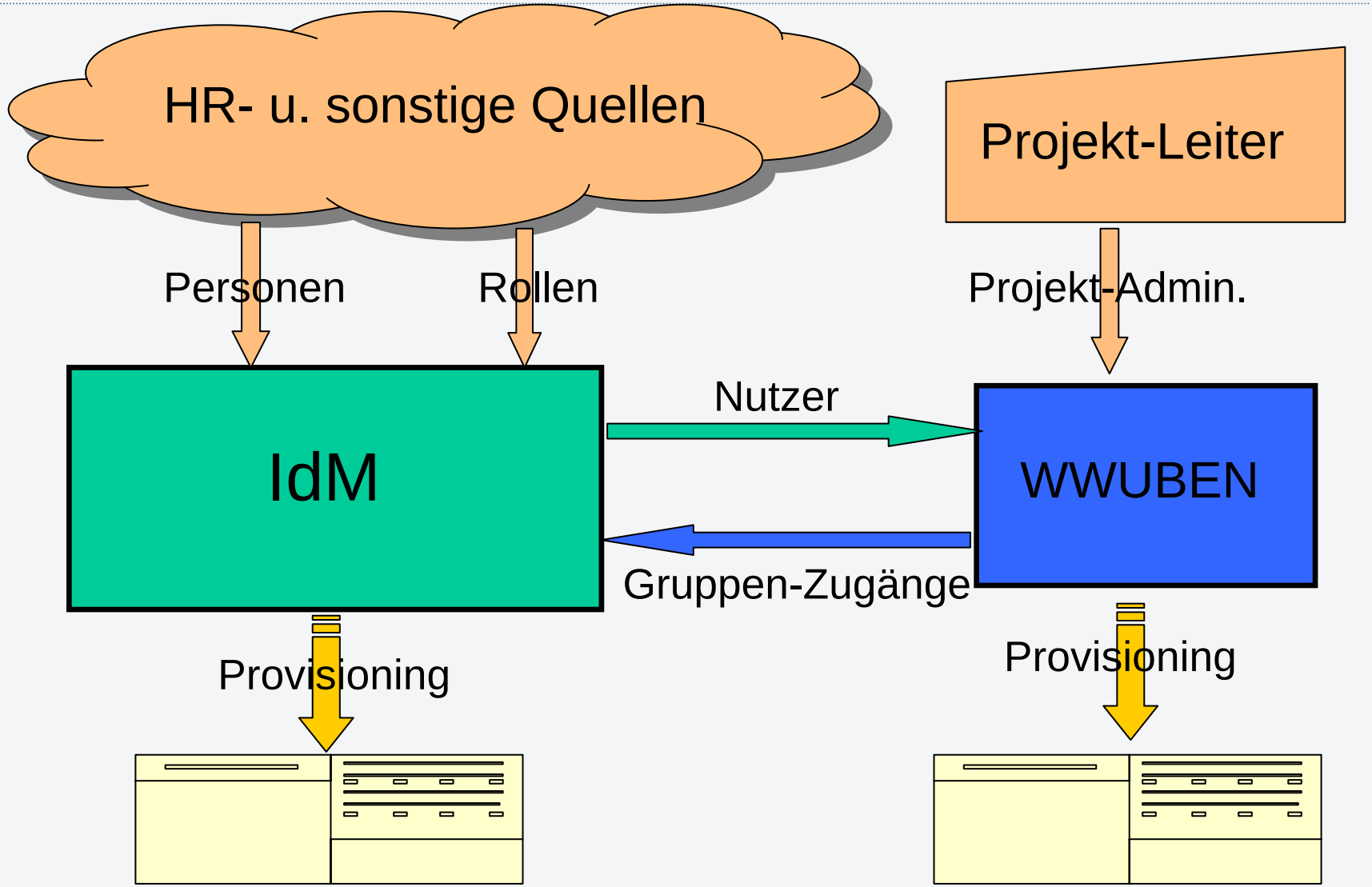
Rollen-Basiertes Provisioning im IdM



Gruppen vs. Rollen im Identitätsmanagement (TIM)

- Gruppen / Rollen im IdM:
  - Gruppen an Accounts gebunden
    - Verwaltung Zielsystem-spezifisch
  - Rollen an Identitäten gebunden
    - Wirken auf alle Accounts einer Person/Identität
- Migrationsprobleme WWUBEN → IdM:
  - Gruppen an Nutzer (i.e. Teilmenge der Accounts einer Person) gebunden
  - Expiration
  - Delegation und Administration
- Orthogonale Konzepte? (vs. RBAC)
  - Gruppe zur Implementierung von Rollen?
  - Ansatz: Rolle global / Gruppe lokal

Interimslösung: Gruppenverwaltung bleibt in WWUBEN



Nutzer-Konzept im IdM der WWU