Die Personen

Begriffe zum

Identity Management

petersen@uni-bonn.de

Welt-Formel

Identity Management

=

META directory

=

LDAP

Welt-Formel

Identity Management

=

META directory

=

LDAP

- Wer?
- Wann?
- Wo?
- Was?
- Wie?
- Warum?

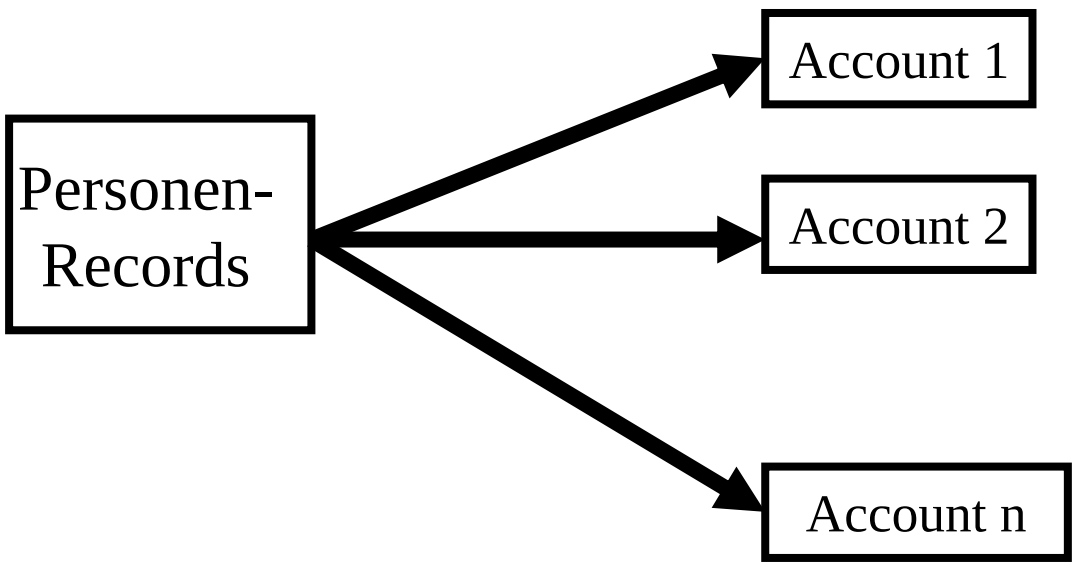
Accounts

- Zugangsrechte
  - Login für Betriebssystem
  - Authentifizierung
- Zugriffsrechte
  - Auf Dateien durch das Betriebssystem
  - Auf Daten durch Anwendungen
    - Datenbanken → Views
    - .htaccess → HTTP-Server
- Audit
- Accounting

- durch das Betriebssystem
  - /etc/passwd
- durch eine Anwendung
  - Kerberos V → Authentifizierung → Key
  - PAM → plugable authentication
  - LDAP (gemeinsames Schema?)
  - Microsoft ADS

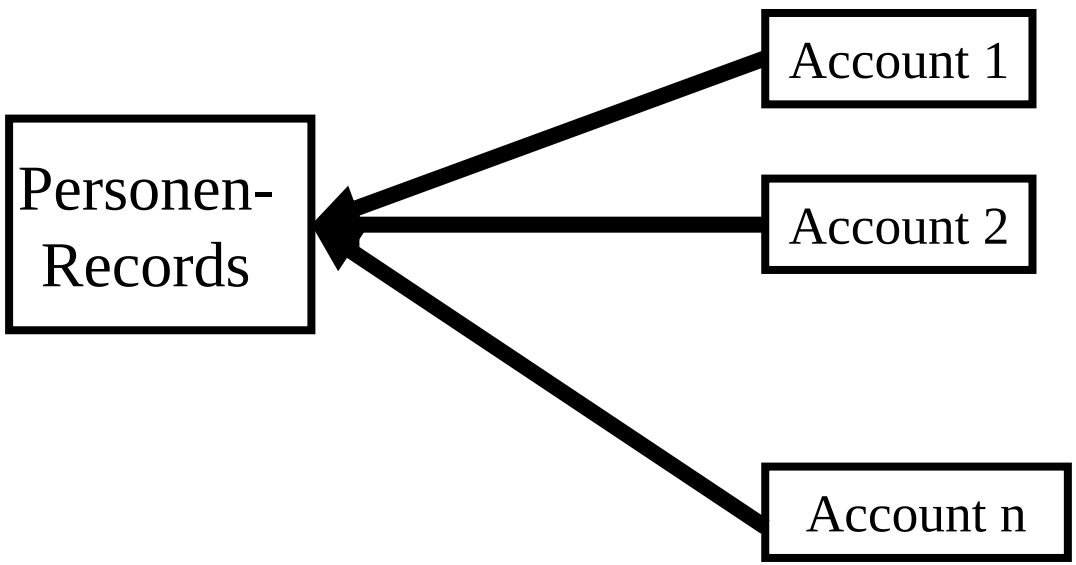
- Personendaten
- Organisationsstruktur
- Funktionen
- Rollen basierende Account-Vergabe
- Workflow
  - Zustimmung, Eskalation
- Life Cycle Management
  - Suspendierung von Accounts
- Zentrales Passwort Management
- Dezentrale Administration

Arbeitsweise von IDM



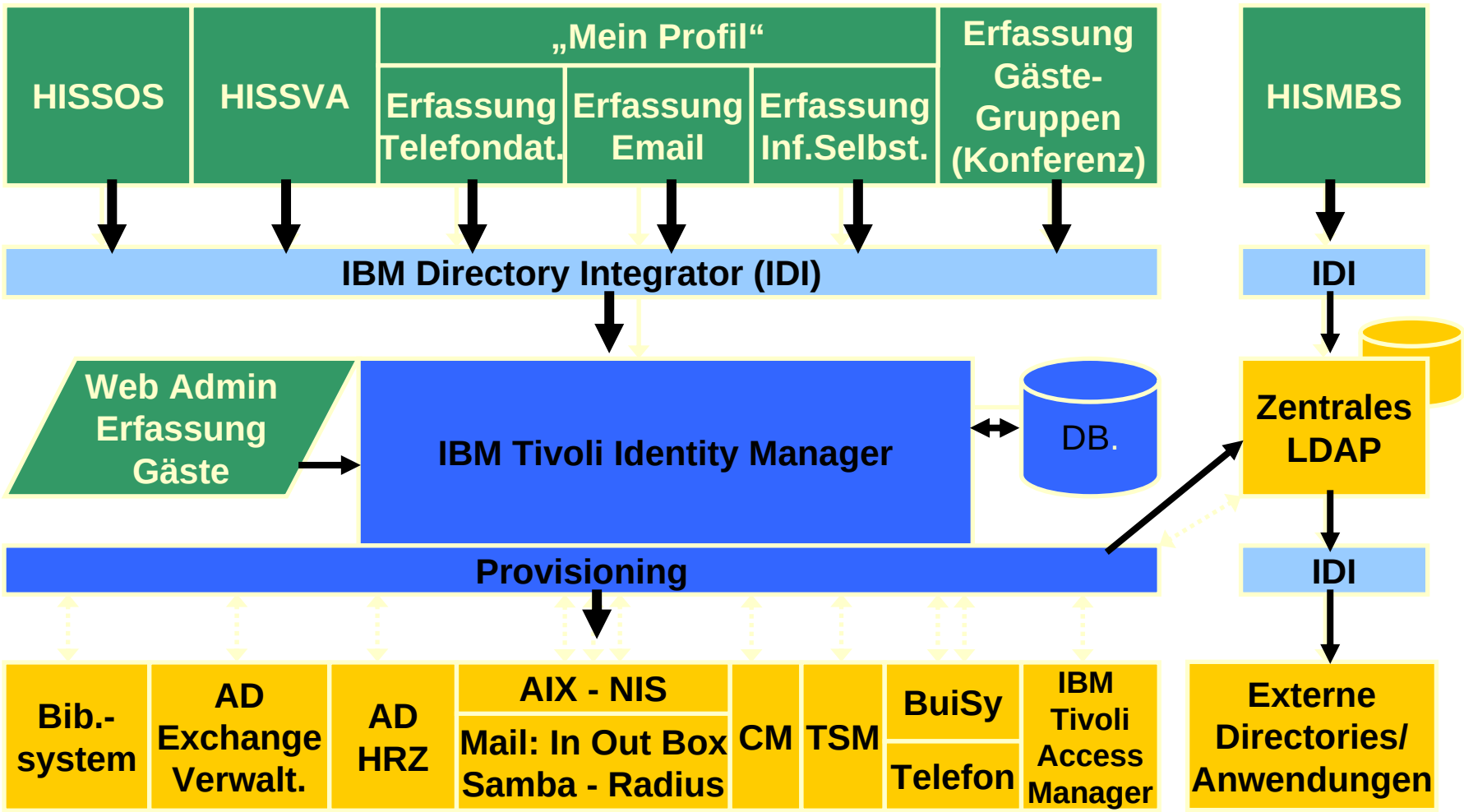
Provisionierung

Arbeitsweise von IDM



Reconciliation

IBM Tivoli Identity Manager
Architektur für Duisburg-Essen



Authentifizierung vs. Identifizierung

- Authentifizierung
  - Gemeinsames Geheimnis
  - Benutzerkennung und Passwort
  - PIN/TAN
- Zertifikate
  - Verteilung von Zertifikaten
  - Personen-Identifizierung (Wo? Wie?)
  - Verschlüsselung von Information (Schlüssel-Eigentümer kann nur entschlüsseln)

Single Sign On

- Betriebssystem
  - z.B. rsh, ssh
- Anwendungen/Portale
  - Vertrauen auf die erste Anmeldung
  - Technik:
    - Reverse Proxy
    - Weitergabe der Session Parameter
- WebSphere Application Server
  - 6 Schichten von Sicherheit (Authentifizierung)

- Password Policies
  - Länge, Dauer, Änderungen
- Accounts
  - nur aktiv wenn in Gebrauch
  - sperren
  - löschen
    - Daten löschen
    - Daten weitergeben
  - Rollenwechsel der Person
- Auditing
  - Wer hat wann was geändert?

- www.redbook.ibm.com
  - Enterprise Security Architecture with Tivoli Products