

# Einführung eines IDM-Systems

## Grundlagen und Vorgehensmodell

Michael Silvan  
[silvan@secaron.de](mailto:silvan@secaron.de)

BITKOM Innovationsforum auf der Systems 2008

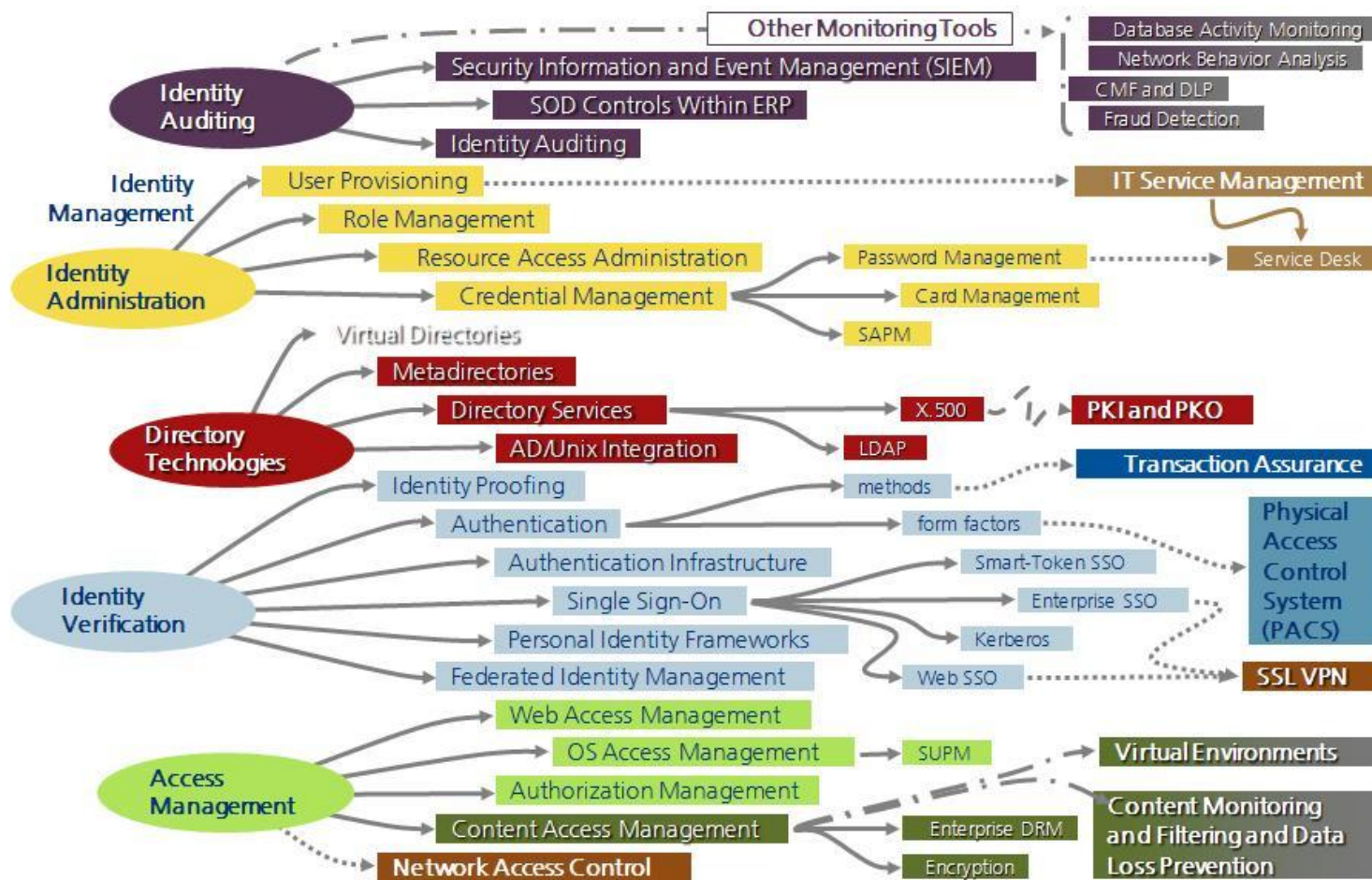
# Agenda

- Treiber und Überblick
- Vorgehensmodell
- Grundlagen
- Identitäten und Rollenkonzept
- Risiken und Erfolgsfaktoren

## Treiber

- Heterogenität: verschiedene Systeme mit einer eigenen Benutzerverwaltung
- Effektivität: Verkürzung der Zeit für die Berechtigungsvergabe
- Mandantenfähigkeit: Trennung der Berechtigungen bzgl. Kunden, Lieferanten
- Compliance: Nachvollziehbarkeit der Berechtigungen (zu jedem Zeitpunkt ,für jeden Mitarbeiter)
- Federation: gesicherter Austausch von Identitäten und Berechtigungen zwischen Unternehmen

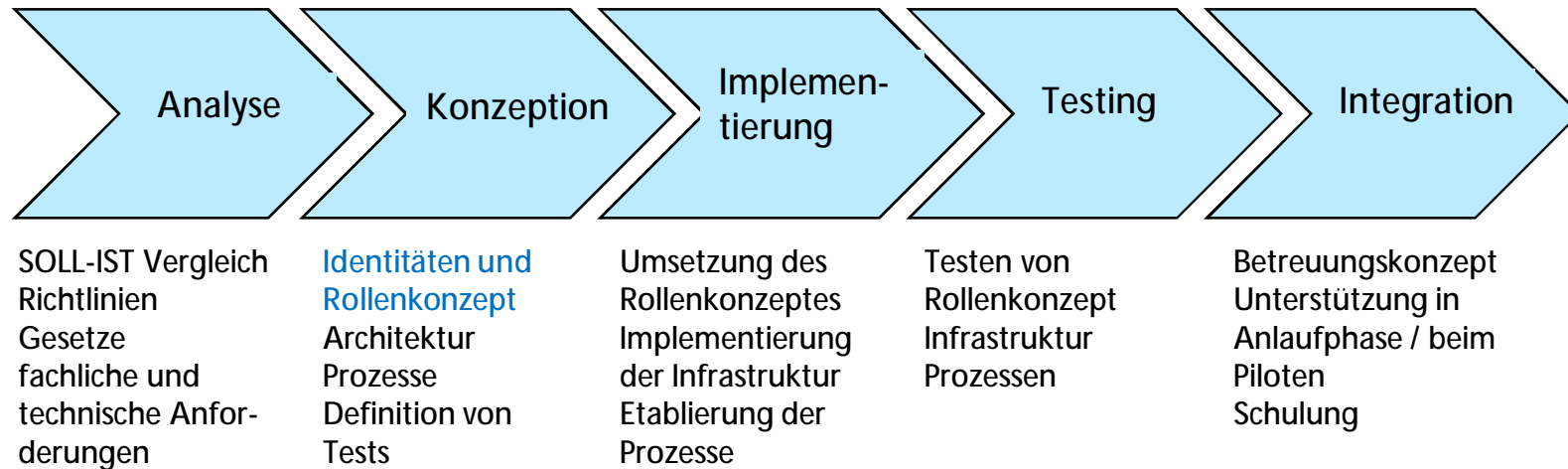
# IDM-Tools: Ein Überblick



Quelle: Gartner

# Einführung eines IDM Systems

## Vorgehensmodell



## Grundlagen: Ebenen des IDM

- Stammdaten  
Qualität der Daten, führende Datenquellen
- Ressourcen  
Art der Ressourcen, Möglichkeiten der Rechtevergabe,  
Hierarchie von Berechtigungen, zentrale oder dezentrale  
Verwaltung, Nachvollziehbarkeit
- Autorisierung (fachliche Rollen)  
Definition der Rollen, Abbildung auf technische Rollen
- Authentisierung  
Authentisierungsmechanismen, Passwort-Richtlinie,  
notwendige Infrastruktur

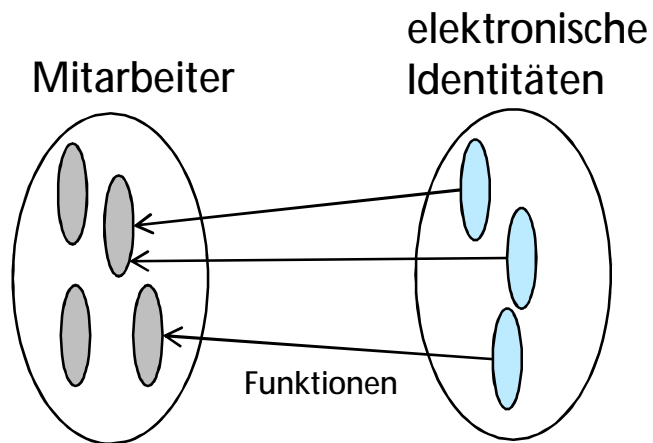
## Grundlagen: Aspekte des IDM

auf allen Ebenen Beachtung der Aspekte:

- Richtlinien  
Vorgaben zur Qualität der Daten
- Prozesse
  - operative: Anlegen eines Accounts
  - administrative: Prüfen der Datenqualität, Anlegen technischer Rollen
  - konzeptionelle: Festlegung führender Datenquellen
- Technik  
Directory, Konnektoren, Synchronisationsmechanismen,  
IDM Tool

# Konzeption: Identitätenkonzept

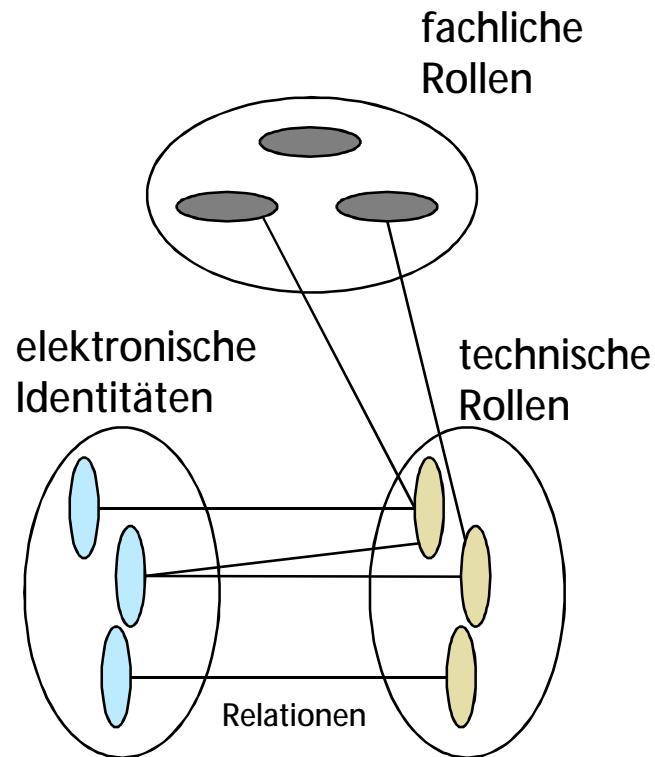
Zuordnung von elektronischen Identitäten zu einem Benutzer



Hauptaufgaben:

- Namenskonvention
- Eindeutigkeit
- Prozess für die Vergabe von elektronischen Identitäten
- technische Beschränkungen

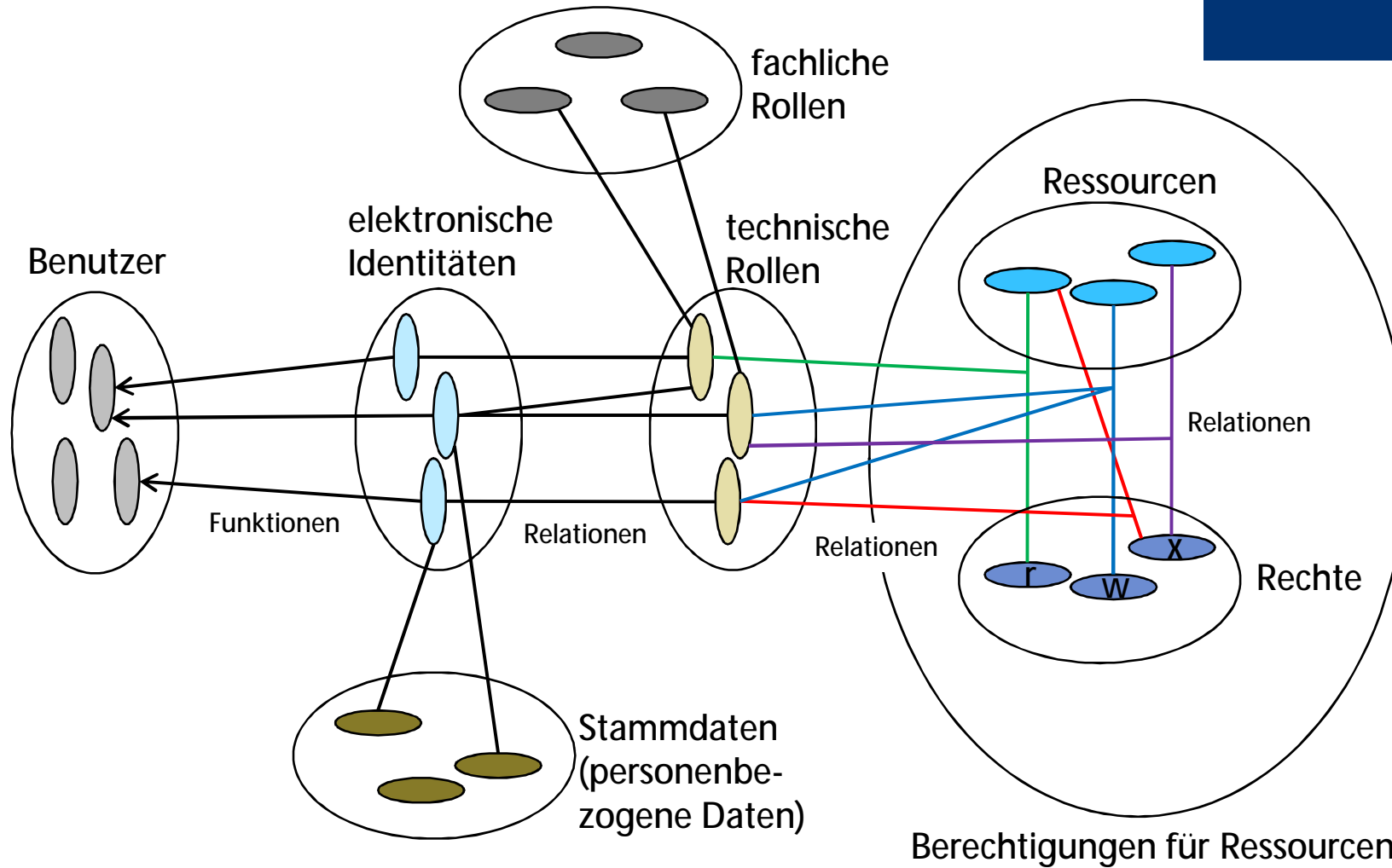
# Konzeption: Rollenkonzept



## Hauptaufgaben:

- Definition von fachlichen Rollen (Funktionen)
- Zuordnung von fachlichen Rollen zu technischen Rollen gemäß least privilege Prinzip
- u.U. Definition einer Hierarchie von technischen Rollen:  
technische Sammelrolle **B** → Funktion  
technische Einzelrolle **B** → Aufgaben

# Konzeption: Role Based Access Control (RBAC)



# Rollenkonzept: Aufgaben/Funktionen Matrix

Funktion	Vertrieb	BackOffice	Controlling
<b>Aufgaben</b>			
Angebotserstellung	X		
Kunden verwalten	X		
Protokollierung im CRM	X		
Aufgaben „normaler Benutzer“	X	X	X
Reports FI analysieren			X
Reports CO erstellen			X

# Rollenkonzept: Aufgaben/Funktionen Matrix

	Vertrieb	BackOffice	Controller
<b>Aufgaben</b>			
Angebotserstellung	J2EE DB lesen, schreiben		
Kunden verwalten	CRM Verwaltungs- rechte		
Protokollierung im CRM	CRM lesen, schreiben		
Aufgaben „normaler Benutzer“	Berechtigungen „ADS normal“	Berechtigungen „ADS normal“	Berechtigungen „ADS normal“
Reports FI analysieren			SAP FI lesen
Reports CO erstellen			SAP CO lesen, schreiben

Einzelrolle  
IT-Rolle ADS normal

Sammelrolle  
Business-Rolle Vertrieb

## Risiken

- Schwache Anforderungsanalyse
- Zu große erste Projektphase
- Übersehen von Stakeholdern
- Fehlende Prozesse & Datenmodelle
- Fehlendes Rollenkonzept
- Fehlendes technisches Know- How
- Datenqualität

## Best Practises

### Erfolgreiche Projekte:

- gehen iterativ und inkrementell vor
  - Projekte, die alles auf einmal erreichen wollen, scheitern
  - Große IAM Projekte dauern: Technik, Prozesse, Akzeptanz
- machen Nutzen durch Quick-Wins sichtbar
- haben klar definierte Etappenziele
- verlieren das Fernziel nicht aus den Augen

## Kontakt

Secaron AG  
Ludwigstr. 45  
D-85399 Hallbergmoos  
Tel. +49 811- 9594 - 122  
Fax +49 811- 9594 - 220  
[www.secaron.de](http://www.secaron.de)  
Ansprechpartner:  
Michael Silvan  
E-Mail: [silvan@secaron.de](mailto:silvan@secaron.de)



19.10.2008

» | secaron

Vielen Dank für  
Ihre Aufmerksamkeit!

e.security solutions

Seite 15