



## Geschäftsorientiertes Provisioning mit Regeln und Rollen

Workshop



Frankfurt am Main, 15. Februar 2005

Dr. Martin Kuhlmann  
Product Line Manager  
Beta Systems Software AG

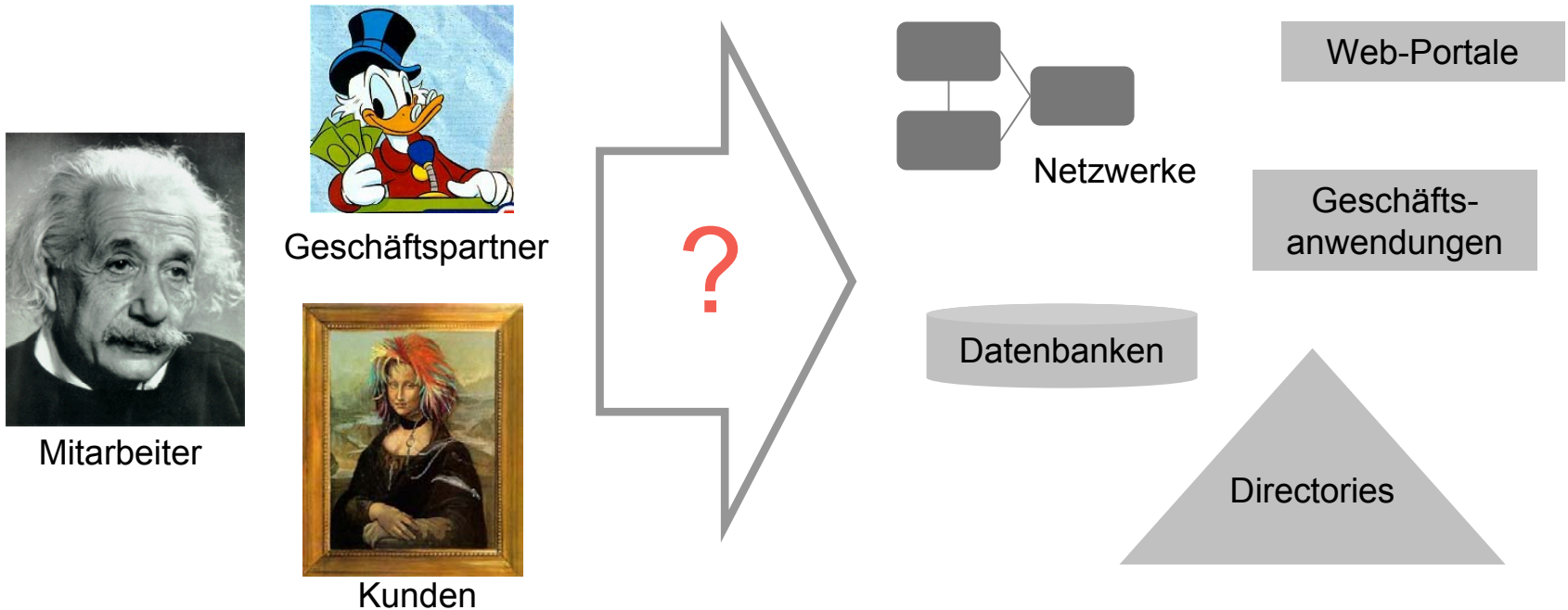
# Agenda

- Rollenbasierte Administration: Die Theorie - RBAC Basics
- Warum rollenbasierter Zugriffsschutz? – Die Vorteile
- Der Weg zum Rollenmodell
  - Grundüberlegungen
  - Praxisbeispiele
  - Top-Down und Bottom Up
- Administration mit Rollen und Regeln
- Role Life-Cycle

# **Rollenbasierte Administration: Die Theorie - RBAC Basics**

# Identity Management braucht ein Administrationskonzept

- Identity Management bringt Menschen die Ressourcen und Werkzeuge, die sie für Ihre Aktivitäten benötigen
- Identity Management Lösungen verwalten den Lebenszyklus eines IT-Benutzers. Sie machen die Administration effizienter und bringen Anwender und Unternehmen höhere Sicherheit
- Welches sind die effizientesten Administrationskonzepte?

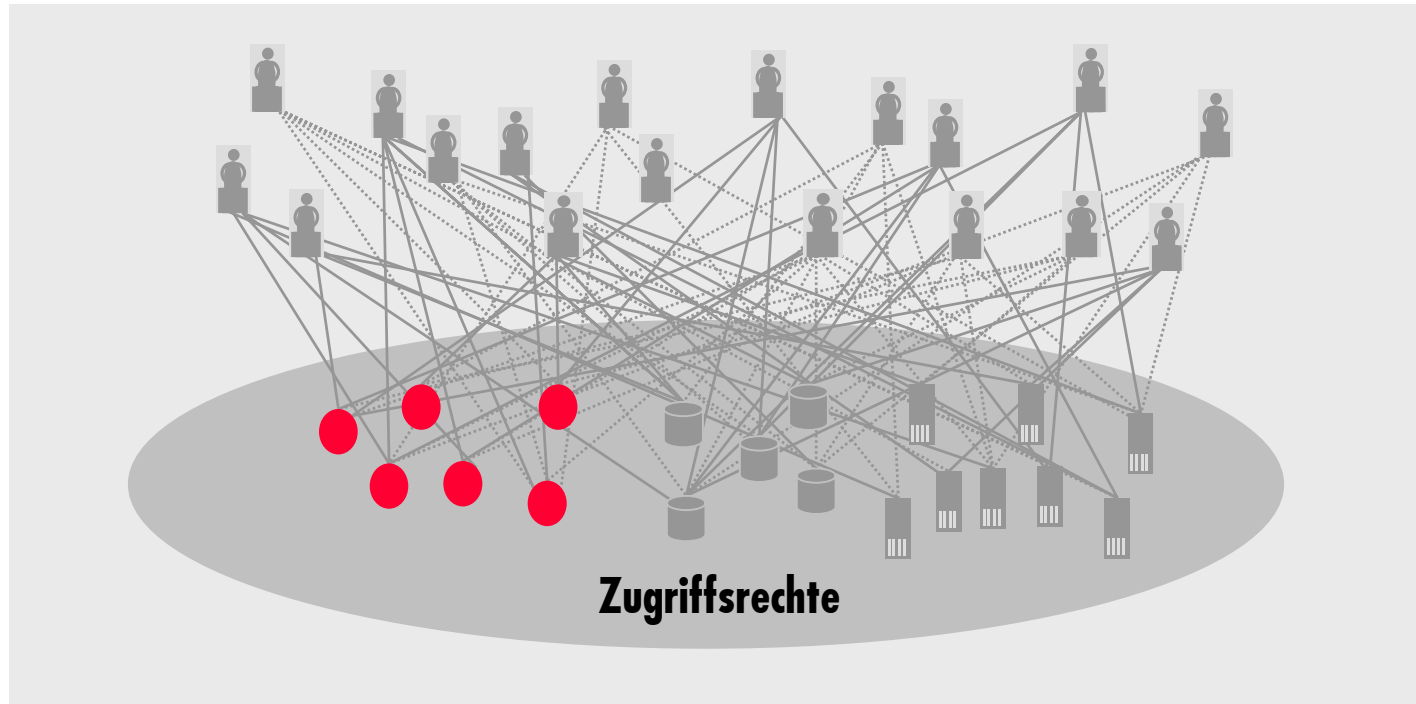


# Übersicht: Zugriffsschutz-Modelle

- Grundlegende Modelle (s. „Orange Book“):
  - Discretionary Access Control (DAC)  
beruht auf expliziter Zugriffsrechtevergabe und Eigentümerparadigma;  
oft in Form von Zugriffskontrollmatrizen;  
„Discretionary“ = „upon discretion of the owner“
  - Mandatory Access Control (MAC)  
beruht auf „Clearance“ und „Classification“;  
vorgeschlagen v.a. für militärische Nutzung
- Weitere Modelle
  - Bell-LaPadula (MAC)
  - Biba (MAC)
  - ...
- Role Based Access Control (RBAC)

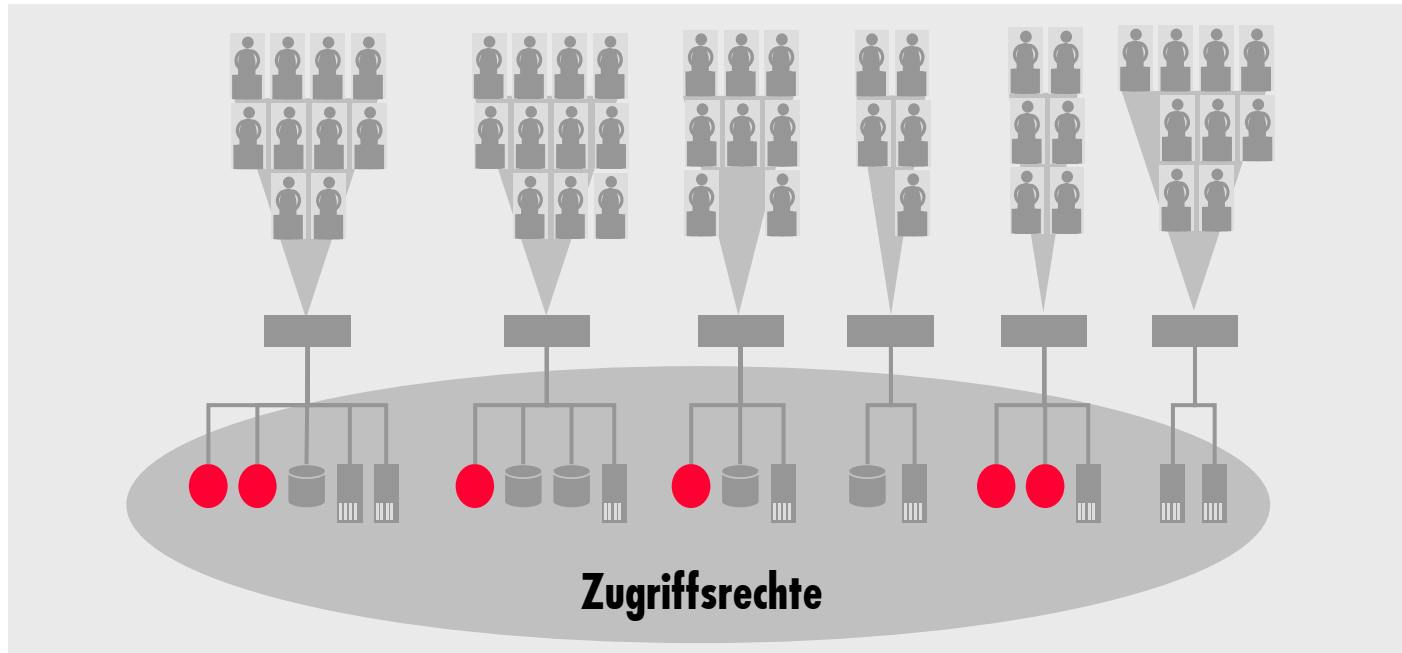
# Rollenbasierte Administration (RBAC)

Die Pflege von Einzelautorisierungen oder plattformspezifischen Gruppen ist keine Lösung ...



# Rollenbasierte Administration (RBAC)

Administration auf der Basis von unternehmensweiten Rollen ist ein praktikabler Ansatz

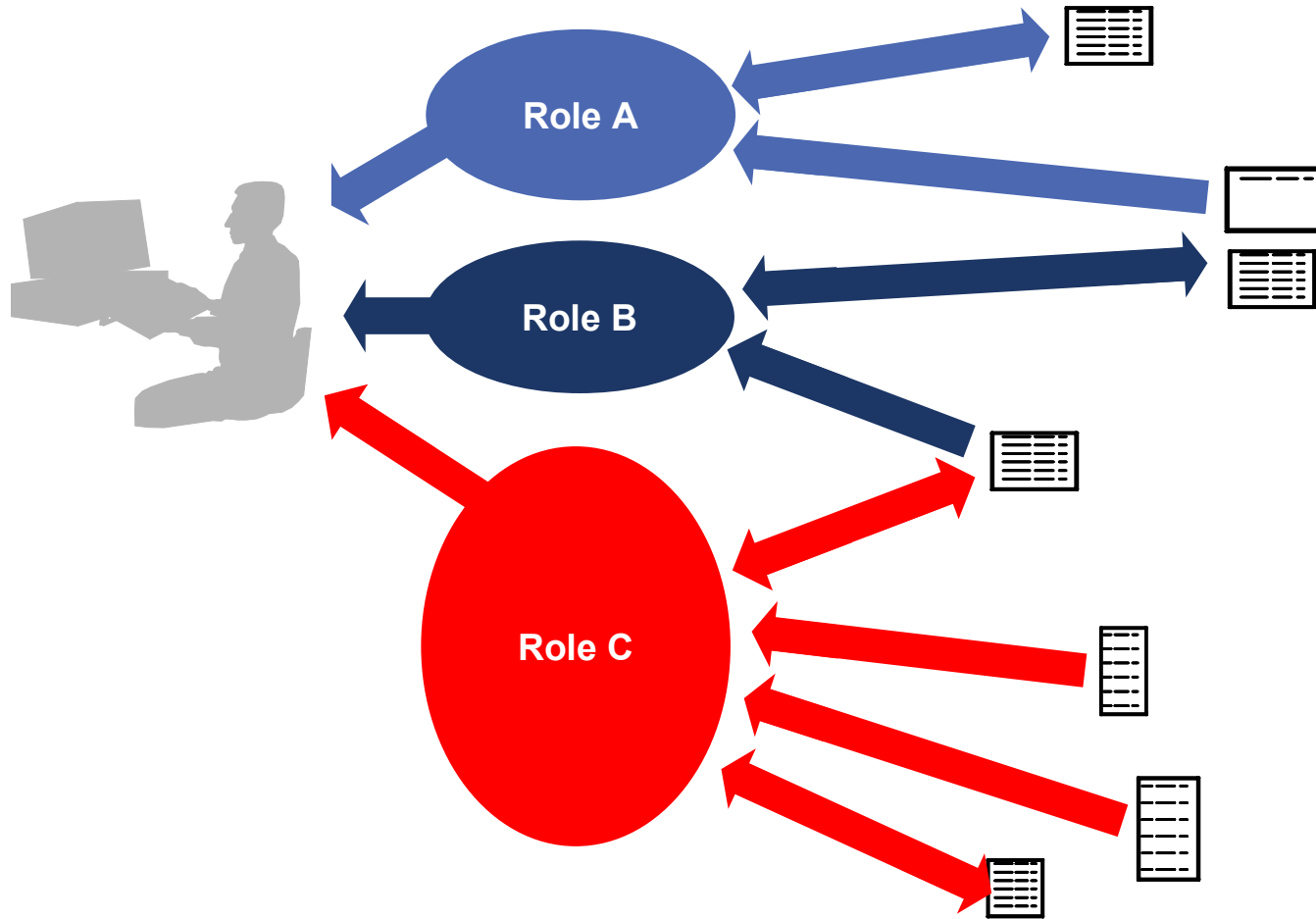


# Role Based Access Control (RBAC) - Definitionen

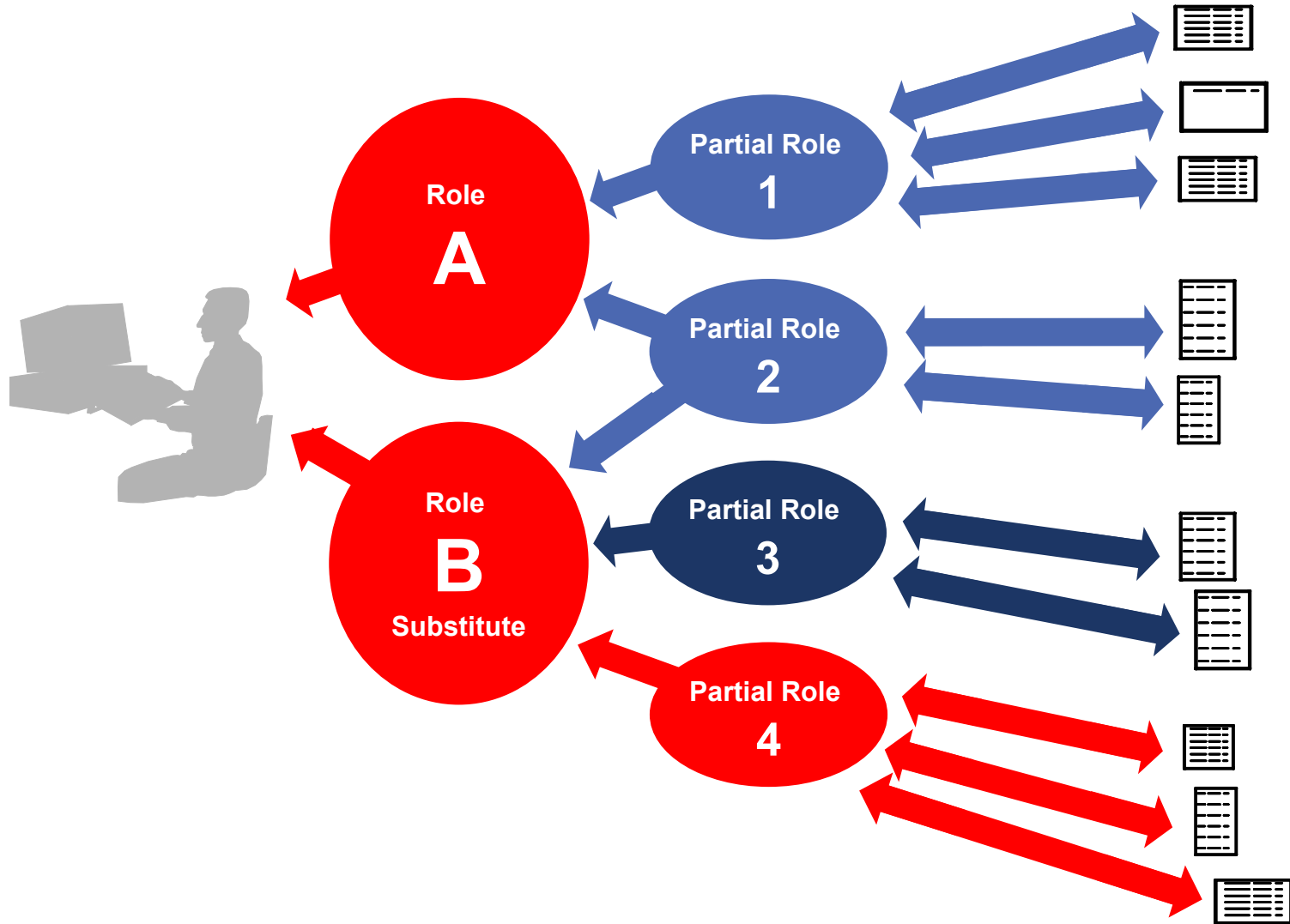
- Eine Security-Rolle ist definiert als ein
  - **Bündel von Transaktionen oder Services, die ein Benutzer oder eine Gruppe von Benutzern im Kontext einer Organisationsstruktur nutzen kann.**
  - Eine Transaktion bzw. ein Service in diesem Sinne ist definiert als ein Datenzugriff inklusive der zugehörigen Ressource.

*(Ferraiolo, Kuhn, 1992)*
- „A role is properly viewed as a semantic construct around which access control policy is formulated. The particular collection of users and permissions brought together by a role is transitory (*vorübergehender Art*). The role is more stable because an organization's activities or functions change less frequently.“  
*(R. Sandhu, Role-based Access Control, 1997)*
- “A role is a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role.”  
*(ANSI 359-2004 Standard)*

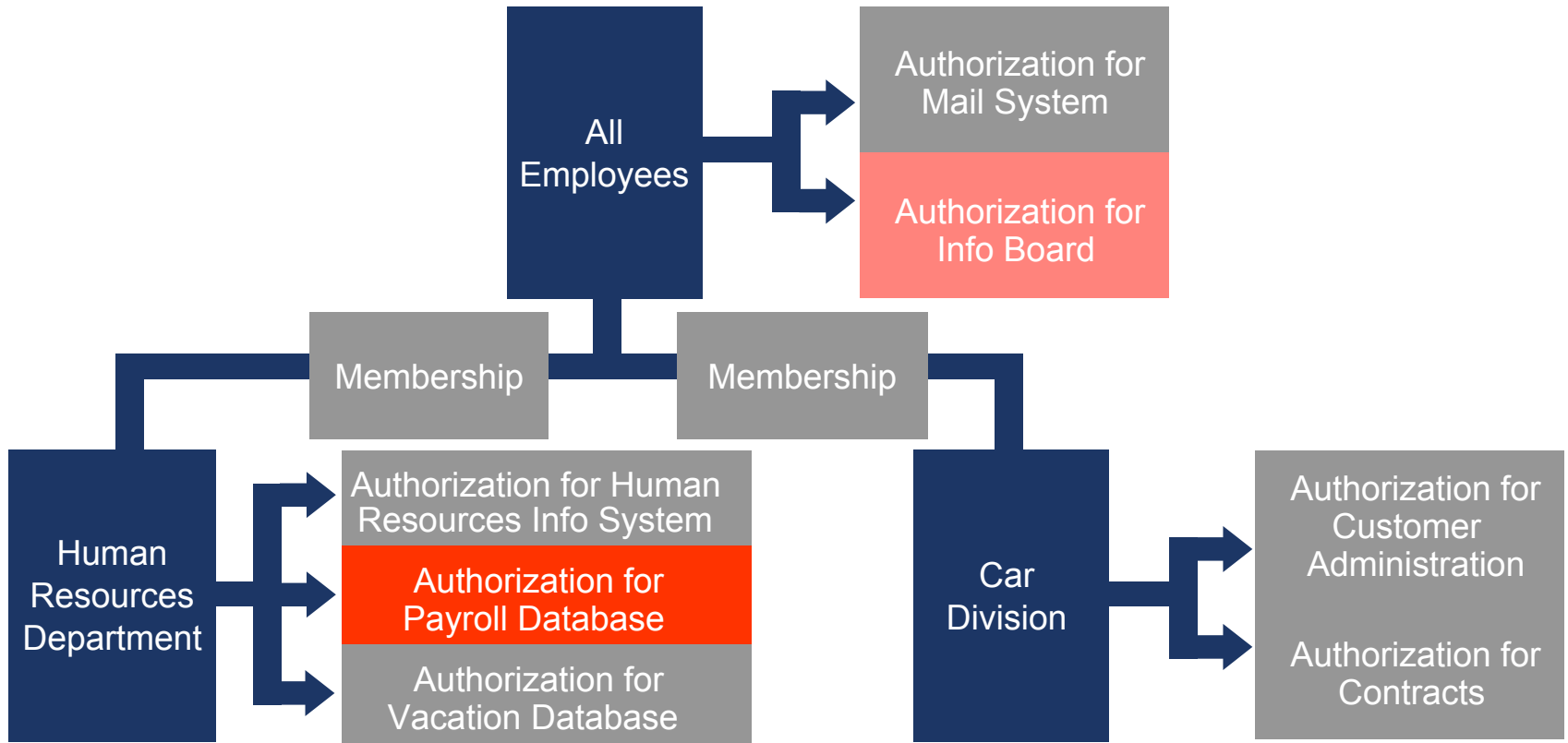
# RBAC : Mehrere Rollen pro Benutzer



# RBAC : Hierarchien von Rollen



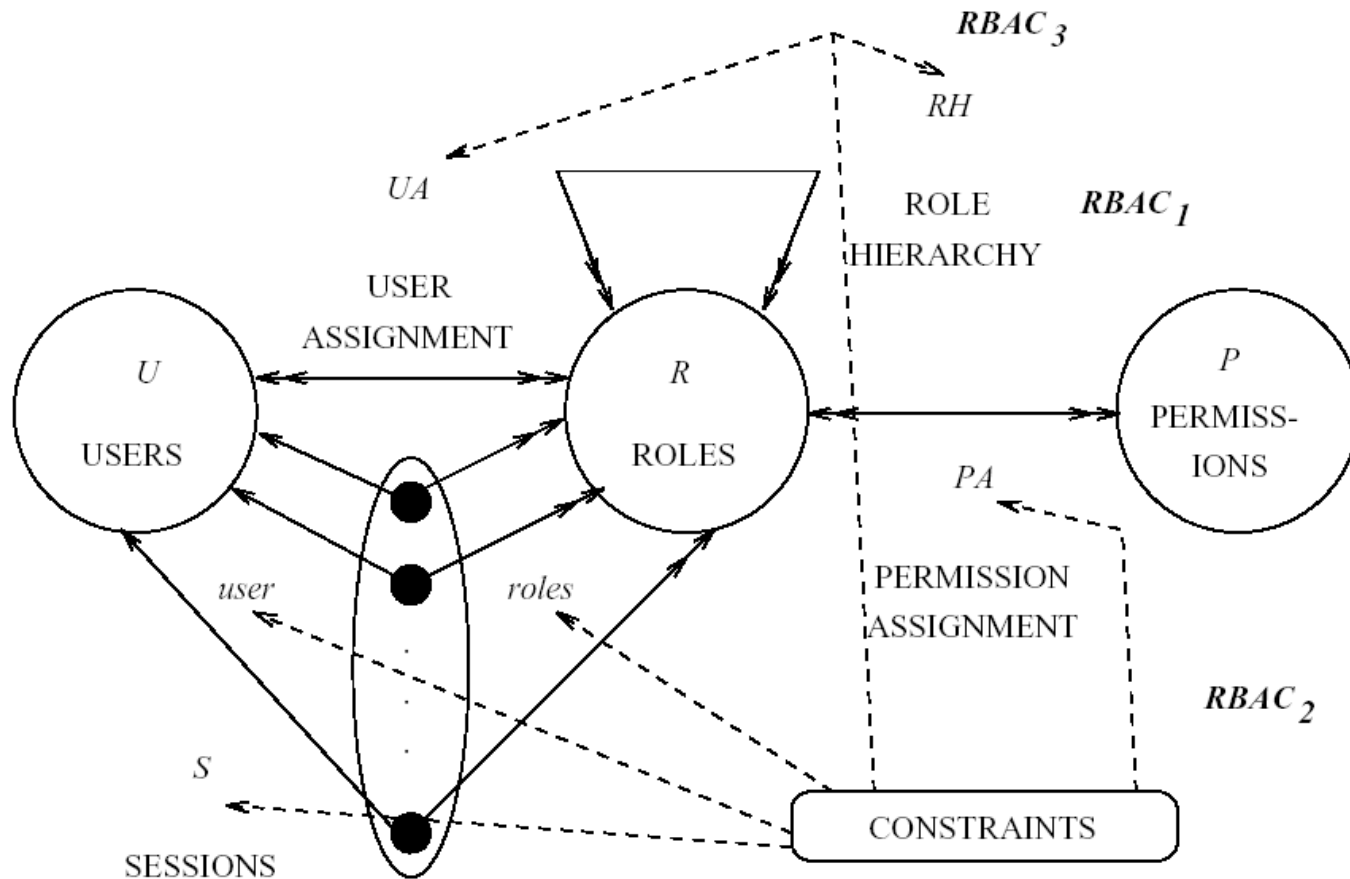
# Beispiel: Organisationseinheiten als Basis für Rollen



# RBAC Historie

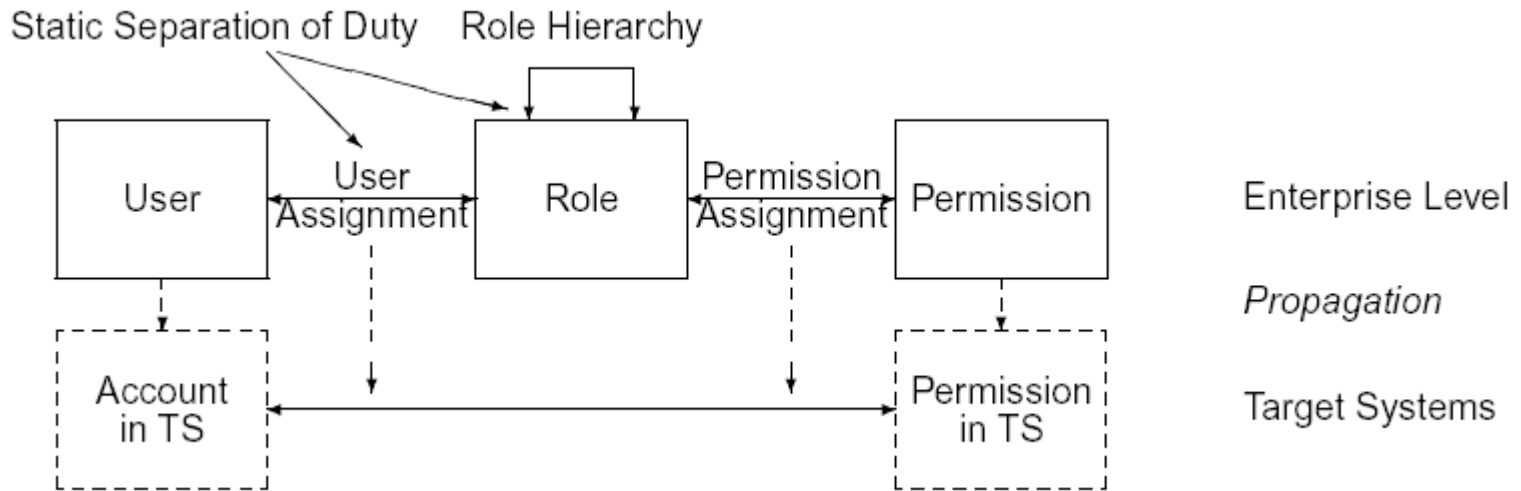
- Nutzung von DAC, MAC und Gruppenkonzepten in kommerziellen Produkten seit den 70er Jahren
- 1992: Grundlegender Artikel “Role-based Access Control” von Ferraiolo und Kuhn
- In den Folgejahren: Grundlagenarbeit in den Konferenzen ACSAC und SACMAT; Entwicklung verschiedener RBAC-Modelle:
  - RBAC<sub>0/1/2/3</sub>
  - ARBAC
  - ERBAC
- 2001: Vorschlag für einen RBAC ANSI-Standard durch NIST
- 2001: Gründung des XACML Technical Committee bei OASIS
- Februar 2004: Verabschiedung ANSI 359-2004 Standard
- Februar 2005: OASIS Standard XACML 2.0 verabschiedet

# RBAC Modelle



Aus: Sandhu/Coyne/Feinstein/Youman, Role-based Access Control Models, 1995

# ERBAC

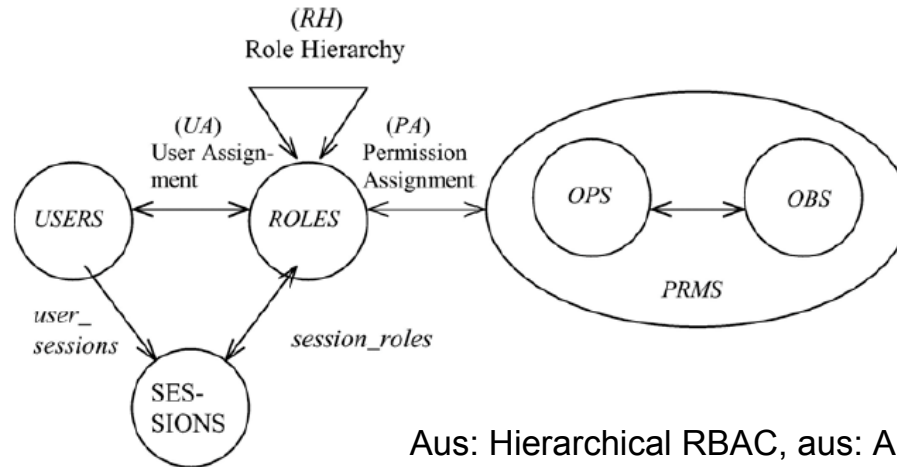


Aus: A. Kern (Beta Systems): Advanced Features for Enterprise-Wide Role-Based Access Control, ACSAC Proceedings, 2003

# Der NIST Standard

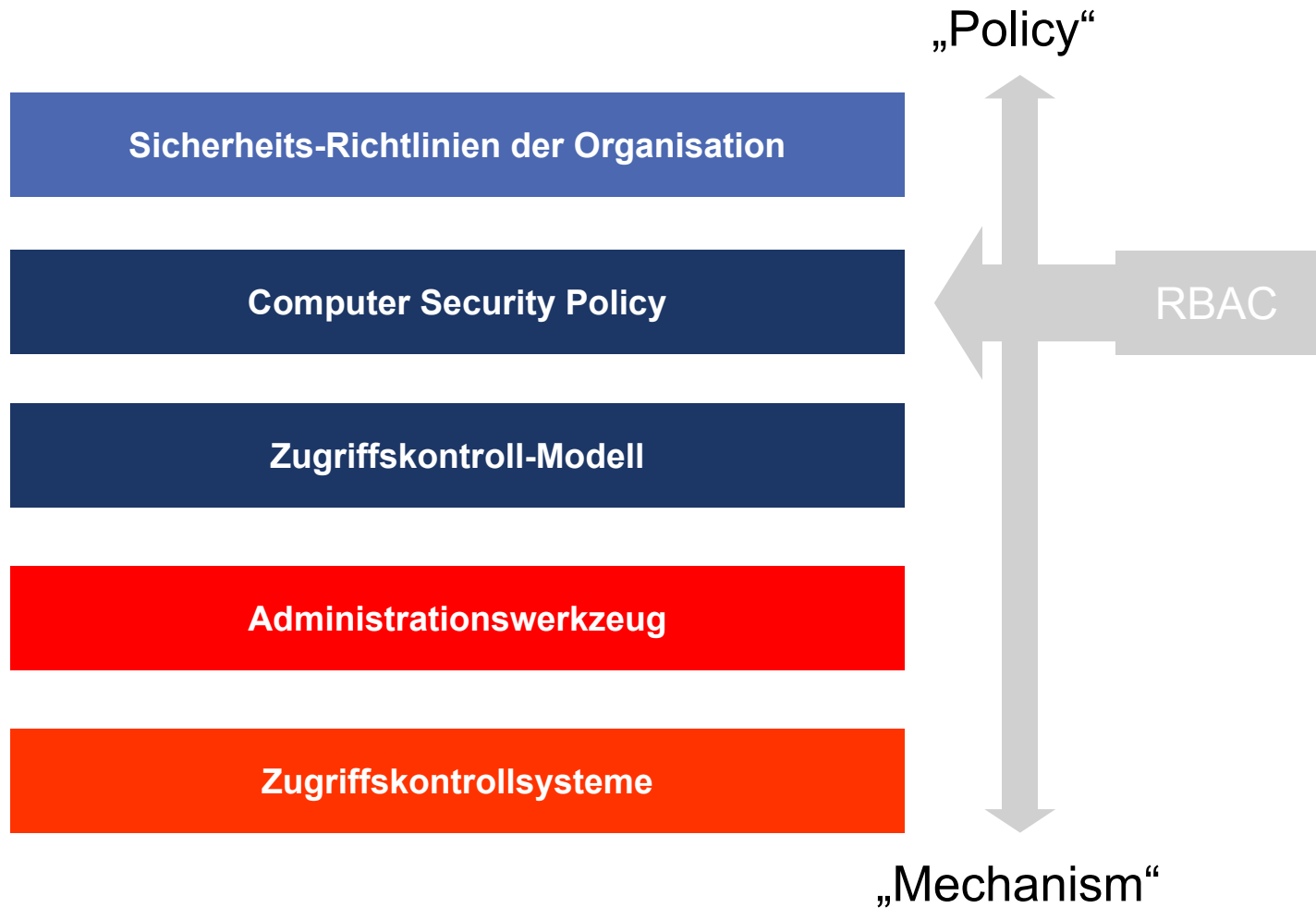
Definiert mehrere Stufen:

- Core RBAC
- Hierarchical RBAC
- Constrained RBAC
- Static Separation of Duty Relations (global constraints)
- Dynamic Separation of Duty Relations (session-based constraints)



Aus: Hierarchical RBAC, aus: ANSI Standard 359-2004

# RBAC-Positionierung

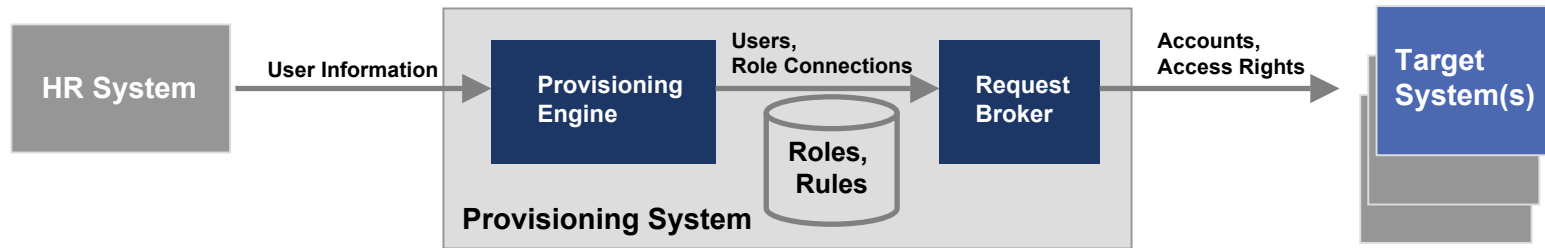


# Warum rollenbasierter Zugriffsschutz? – Die Vorteile

# Warum rollenbasierter Zugriffsschutz?

## Die Vorteile im Überblick (1)

- Leicht zu verstehendes, griffiges Konzept
- Einfachere Administration: Mehr Überblick, weniger Administrationsschritte
- Einfache Definition und Pflege der automatisierten Administration:

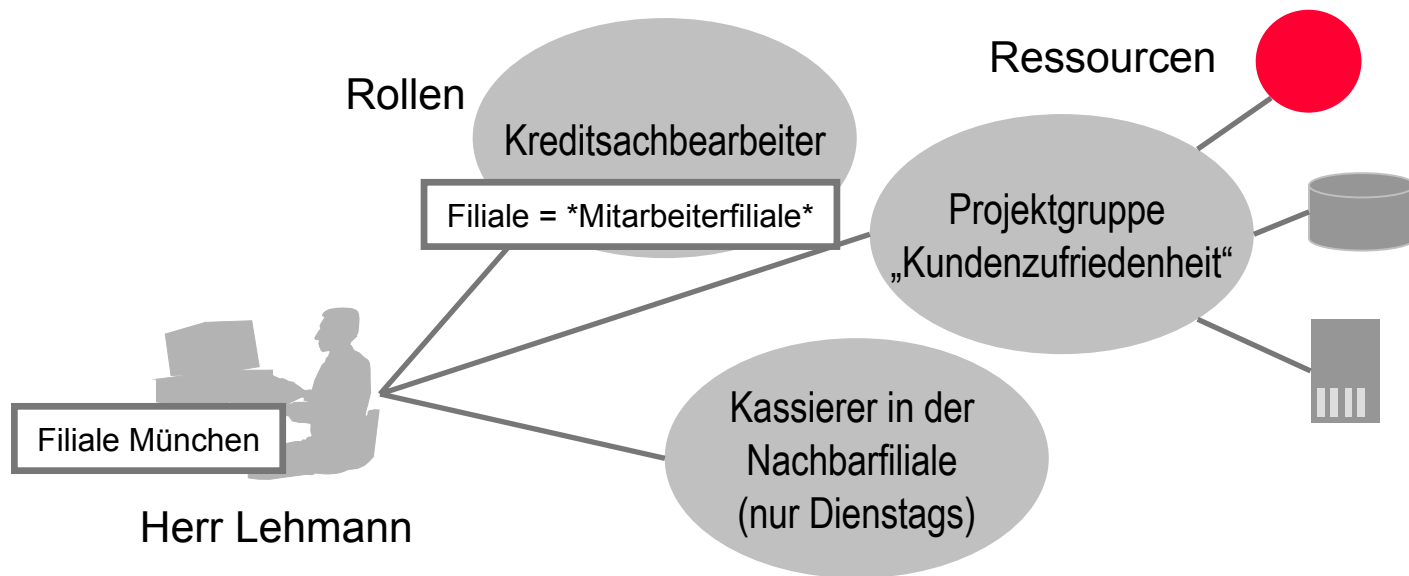


- Rollen ermöglichen eine geschäftsprozessorientierte (nicht-technische) Administration, bilden Organisation und Prozesse gut ab
- Basis für ein einfaches Antragsverfahren für Berechtigungen, Self-Service

# Warum rollenbasierter Zugriffsschutz?

## Die Vorteile im Überblick (2)

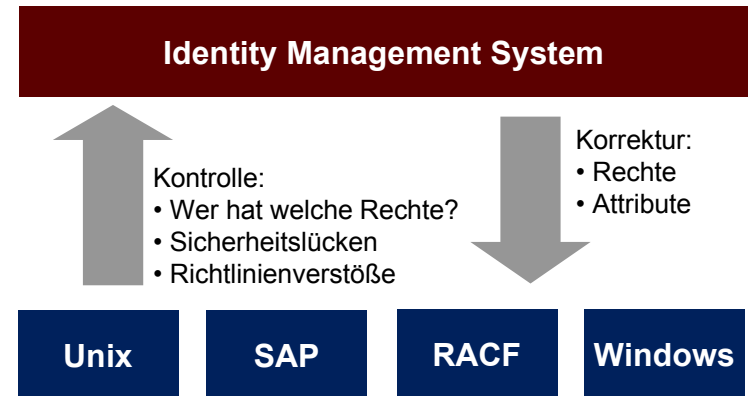
- Verbessertes Sicherheitsniveau, Audit, Regulatory Compliance
- Rollen sind gut zu kontrollieren (Nachvollziehbarkeit/Revision)
- Rollen unterstützen die Zugriffskontrolle für Applikationen
- Rollen sind eine gute Schnittstelle zum Resource Profiling
- Rollen können um regelbasierte dynamische Elemente ergänzt werden (Reduktion der Anzahl der Rollen)



# Warum rollenbasierter Zugriffsschutz?

Verbesserte IT-Sicherheits, Einhaltung von Gesetzen und Standards („Compliance“)

- Motive:
  - Verlässlichkeit/vertraulichkeit von Finanzinformationen (KonTraG, Sarbanes-Oxley, ...)
  - Operative Risikominimierung (Basel II, ISO17799, ...)
  - Schutz personenbezogener Daten (, Europ. Datenschutzdirektive, HIPAA, ...)
- Zu lösende Probleme (u.a.):
  - Korrekte Rechtevergabe
  - Korrektes Ressourcen-Profilung
  - Einhaltung von Sicherheitsrichtlinien
  - Revision und Kontrolle (sensible Benutzerkonten, Rechtekonflikte, ...)
  - Nachvollziehbare Administration
- Vorteile rollenbasierten Zugriffsschutzes:
  - Einfache, korrekte Rechtevergabe und -entzug
  - Rolle hilft bei Profiling
  - Sicherheitsrichtlinien in Rolle abbildbar
  - Abweichungen der Nutzerrechte vom “Soll-Zustand Rolle” leicht zu ermitteln
  - Rollenbasierte Administration leicht nachvollziehbar



# Der Weg zum Rollenmodell

# Der Weg zum Rollenmodell: Grundüberlegungen

- Vision: Plattformübergreifendes Rollenmodell
- Voraussetzungen für die Rollendefinition:
  - Verantwortungsbereiche, Zuständigkeiten und Autorisierungen sind nicht direkt an Personen geknüpft.
  - Es lassen sich formale Kriterien finden, nach denen Zuständigkeiten gegliedert werden können.
- Die Struktur der Security-Rollen reflektiert die „natürliche“ Struktur der Organisation und/oder der Geschäftsprozesse.
- Rollen sind über einen längeren Zeitraum relativ konstant.
- Rollen können mit unterschiedlichem Detaillierungsgrad gebildet werden: eher allgemeingültig oder sehr spezifisch.
- Rollen berücksichtigen nicht jedes Detail an Zugriffsrechten.
- Für die Umstellung auf ein rollenbasiertes Konzept ist in der Regel eine Migrationsstrategie erforderlich

## Der Weg zum Rollenmodell: Einige Kontrollfragen

- Gibt es bereits eine Vorstellung, ob/wie Rollen gemäß Organisationsstruktur oder Geschäftsprozessen gebildet werden sollen?
- Gibt es bereits Systeme im Unternehmen, die Rollen unterstützen?  
Können diese Rollenkonzepte verallgemeinert werden?  
Gibt es mehrere, evt. unvereinbare Rollenmodelle im Unternehmen?
- Gibt es ein Resource Profiling? Kann/soll das eingebunden werden?
- Für welche Bereiche im Unternehmen können Rollenkonzepte am einfachsten eingeführt werden?
- Welche Systeme können eingebunden werden?
- Administrationskonzept für Rollen (Definition, Genehmigung, Pflege, Auditing)?
- Aufwand für Erstellung eines Rollenmodells? Hilfsmittel?

# Der Weg zum Rollenmodell: Praktische Kriterien

- Änderungsfaktoren und -häufigkeiten sind wichtige Kriterien für ein Rollenmodell:
  - Individuelle Faktoren
  - Globale Faktoren
- Mögliche Merkmale für Basisberechtigungen:
  - Fachfunktion
  - Führungsfunktion
  - Abteilung
  - Gesellschaft
  - Projekt
  - Delegation
  - Kostenstelle
- Basisrollen sind i.d.R. auch die Träger für zielsystemspezifische Attribute (Logon-Times, HomeDir, ...)
- Zudem können Rollen existieren für
  - Allgemeine Rechte
  - Sonderrechte
  - Obige Gruppen ergänzende Rechte
- Rollenzuordnungen erfahren Einschränkungen:
  - Datenräume
  - Userspezifische Einschränkungen
  - Rollenspezifische Einschränkungen

# Rollenkonzept - SAM Mengengerüste

<b>Versicherung A</b>	<b>17.000 Benutzer</b>
	<b>120 Rollen</b>
<b>Bank A</b>	<b>30.000 Benutzer</b>
	<b>400 Rollen</b>
	<b>ca. 10 Rollen pro Benutzer</b>
<b>Bank B</b>	<b>31.000 Benutzer</b>
	<b>450 Rollen</b>
	<b>ca. 1 Rolle pro Benutzer</b>

## Rollenkonzept - Burton Group Survey 2003

- Umfrage bei 6 Organisationen
- 4 Unternehmen haben unternehmensweiten Ansatz, 2 einen begrenzten Ansatz
- Budget zwischen 90.000\$ und mehreren Mio. \$, ca. 1.70\$ pro User
- Projektdauer von 2-3 Monaten bis 18-36 Monate (36 Monate nicht erfolgreich)
- Anzahl Rollen pro Unternehmen: 25-28 bis >1500

Aus: K. Kampman, G. Gebel, Enterprise Experiences with Roles, Burton Group, 2003

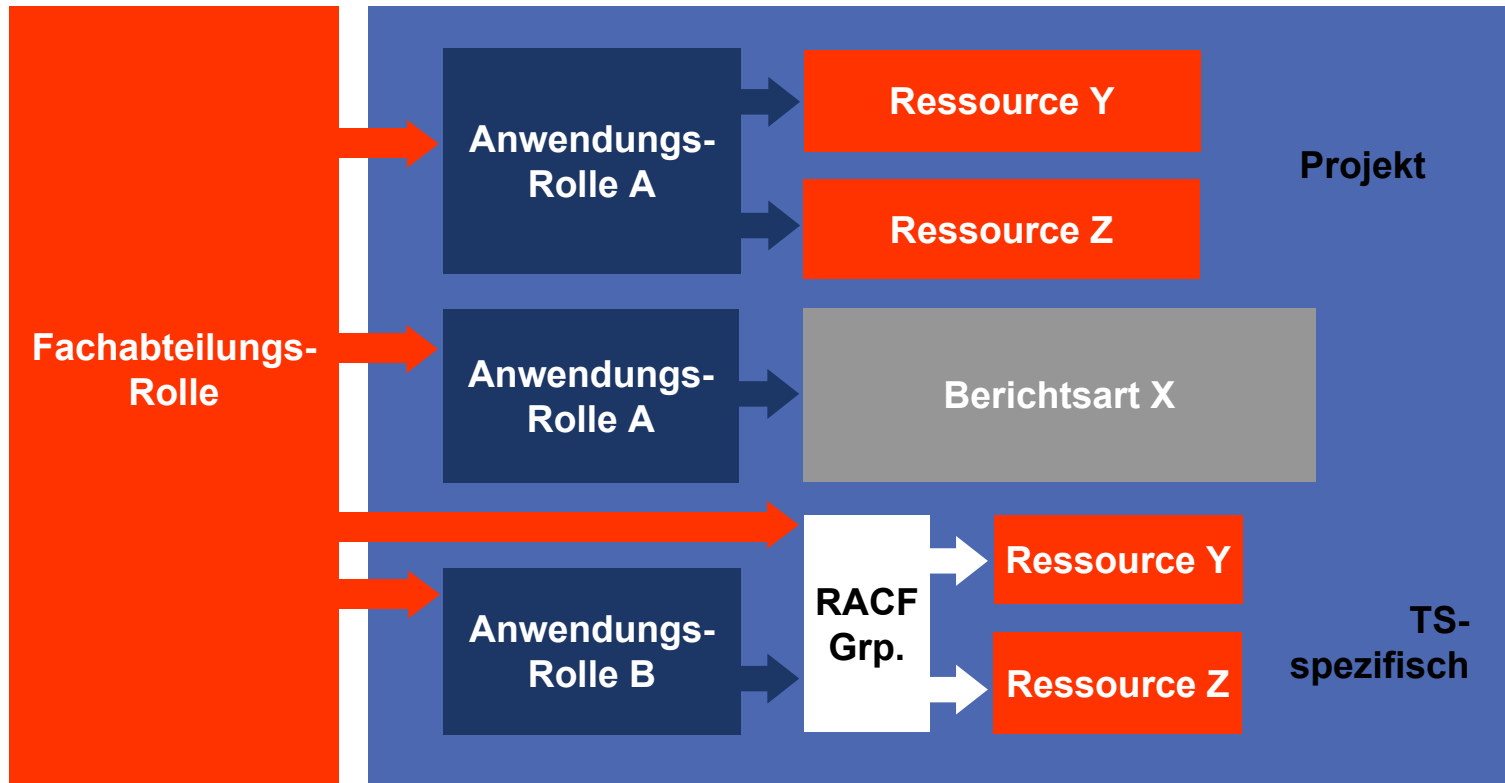
# Praxisbeispiel 1: RBAC-Modell

- Kundenprofil: Großbank,  
ca. 130.000 User IDs werden mit SAM verwaltet  
30 RACF-Systeme  
Windows  
Administration über Antragsverfahren
- Filialbereich:
  - IMS-/CICS-Anwendungen
  - OS/2, Safeguard Desktop
- Zentrale Fachabteilungen, DV-Bereich:
  - RACF
  - Listen-/Berichtswesen

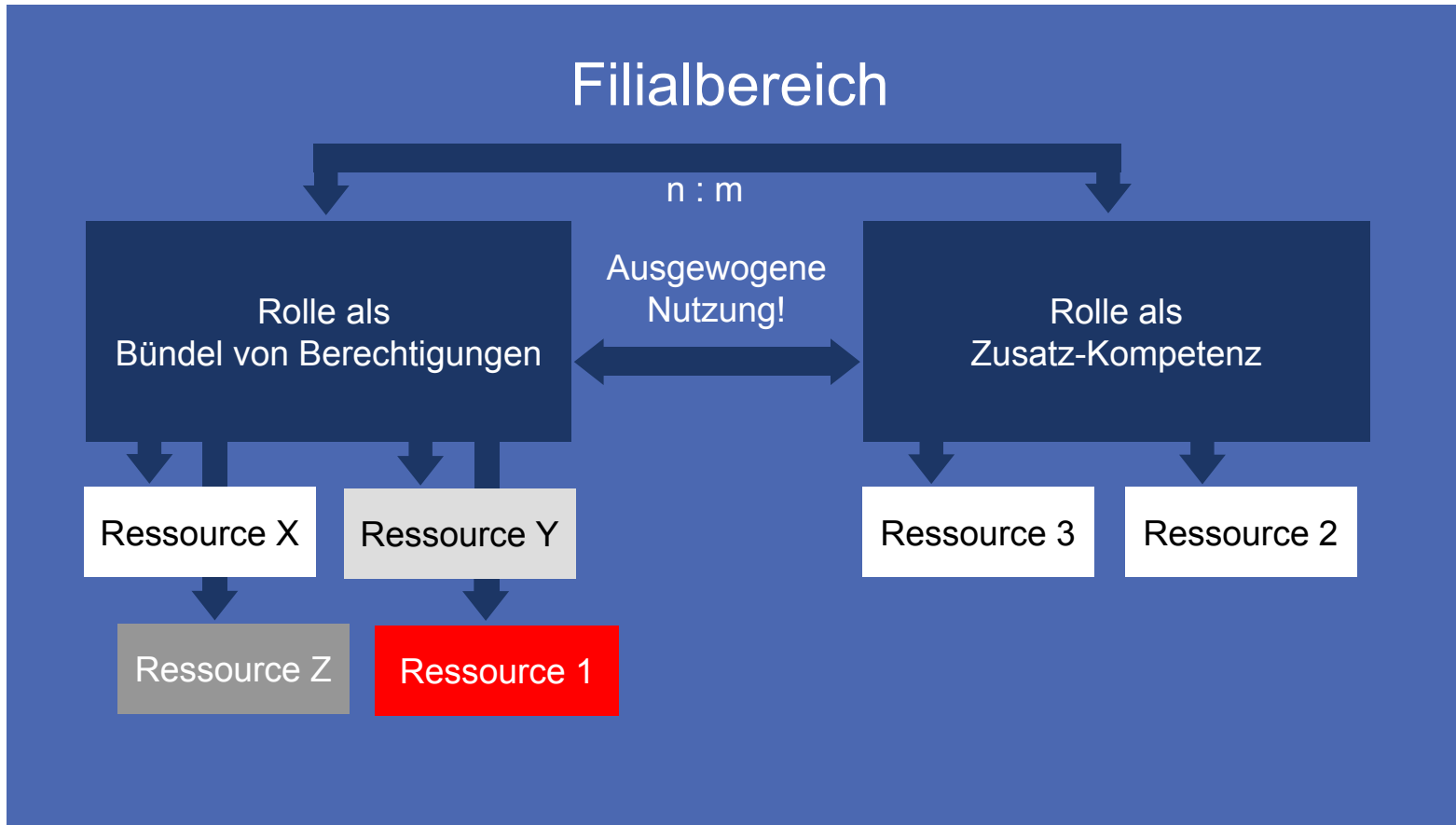
# Praxisbeispiel 1: RBAC-Modell

Antragsverfahren

Zentrale Fachabteilungen [SAM]



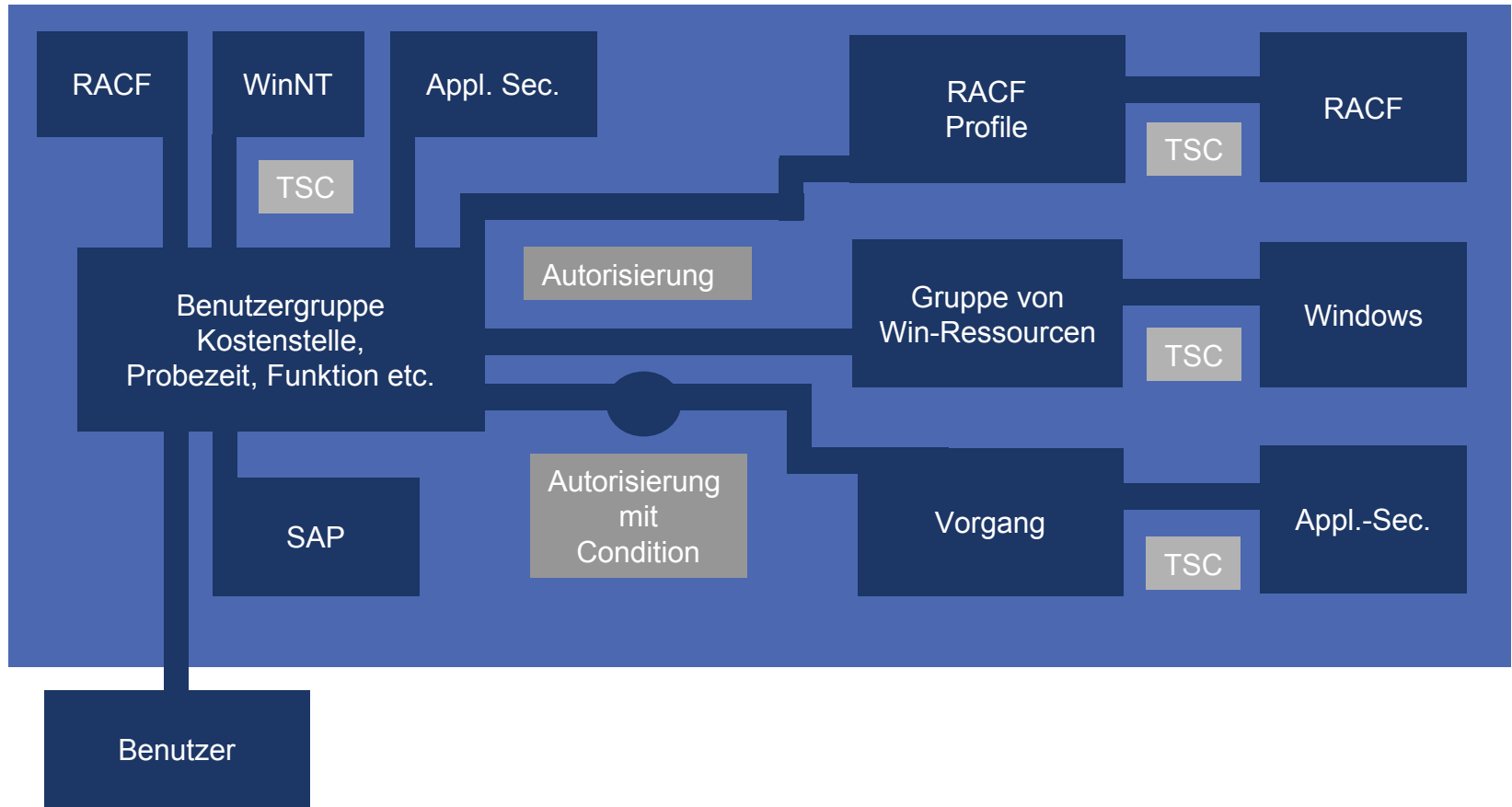
# Praxisbeispiel 1: RBAC-Modell



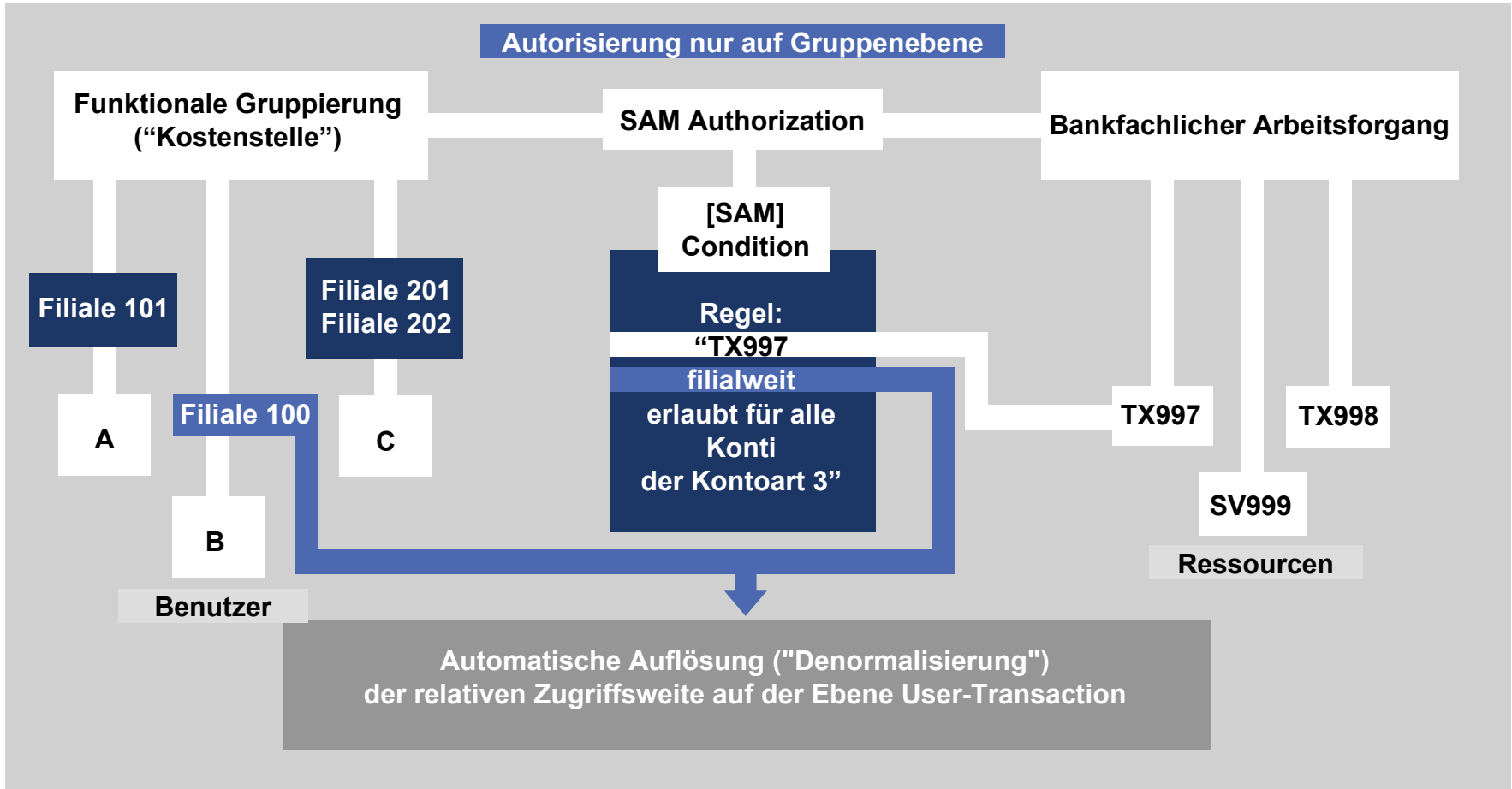
## Praxisbeispiel 2: Provisioning mit RBAC

- Kundenprofil: Große Geschäftsbank,  
40.000 Benutzer werden mit SAM von Beta Systems verwaltet  
Systeme: 3 RACF, 7 Domains Windows NT/2003 , 3 SAP-Systeme,  
2 zentrale u. 2 dezentrale Bankapplikationssysteme,  
Host-Benutzerverwaltung, Unix-Applikation ESS-Space.,  
Directory mit Zugriffskontrolldaten für Anwendungen
- Ca. 1000 Basis- und Zusatzrollen, flexibel parametrisiert
- Vererbung von Berechtigungen über mehrere Ebenen
- Ca. 2-7 Rollen pro Person
- Die SAM Provisioning Engine automatisiert Rechteverwaltung via HR-Anbindung
- Jeder Anwender nutzt durchschnittlich 4 Systeme
- Änderungen bei Rollenzuordnungen und Parameter-Änderungen summieren sich auf ca. 12.000 vollautomatisierte Rechteänderungen pro Woche (inkl. Sperren bei längeren Abwesenheiten, Azubi-Standortwechsel, etc.)
- Durchschnittlich 600 Rechteänderungen pro Woche werden manuell administriert
  
- **Fazit: 95% Automation der Sicherheitsadministration**
- **Erheblicher Einspareffekt ist nachweisbar**

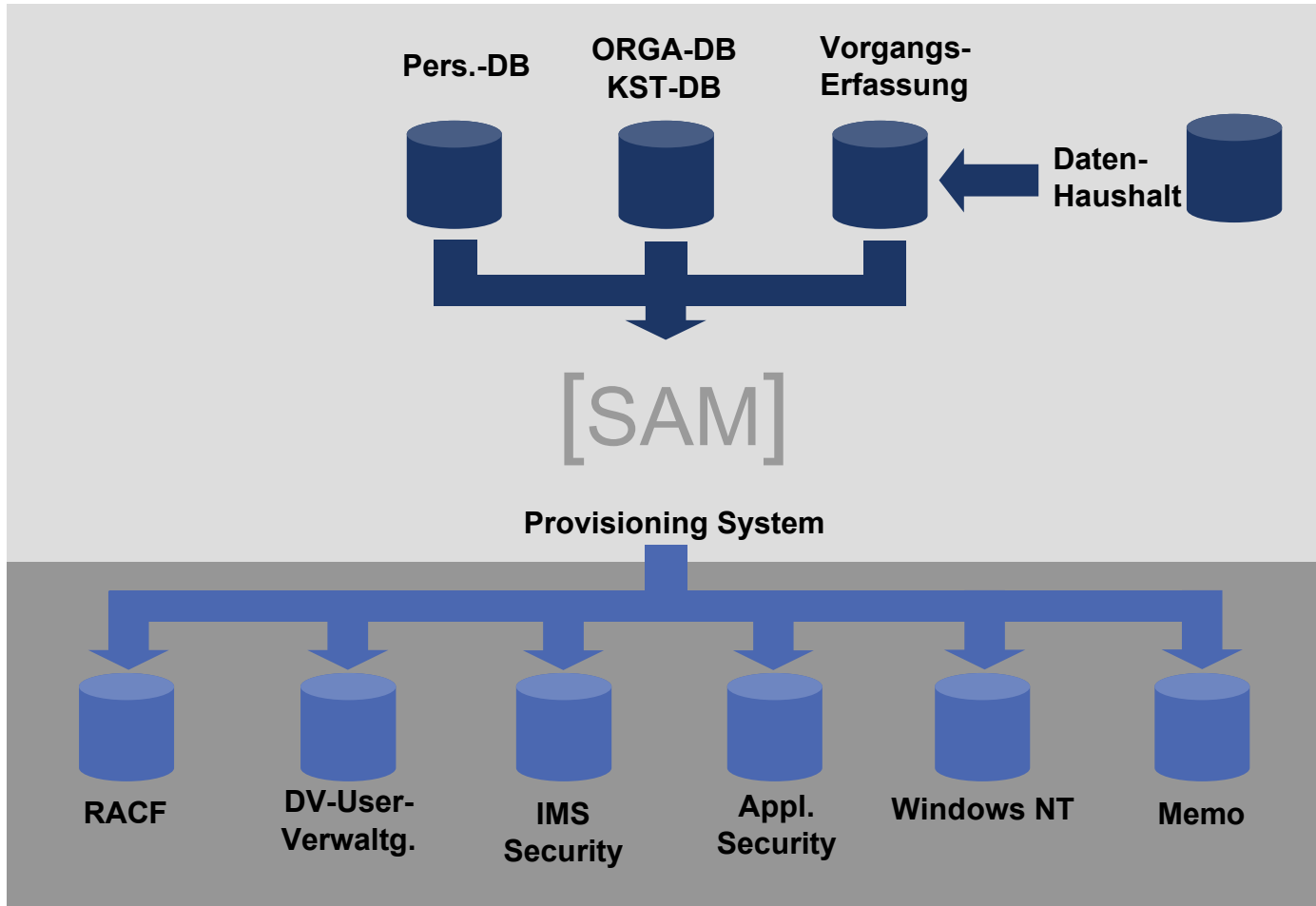
# Praxisbeispiel 2: Provisioning mit RBAC



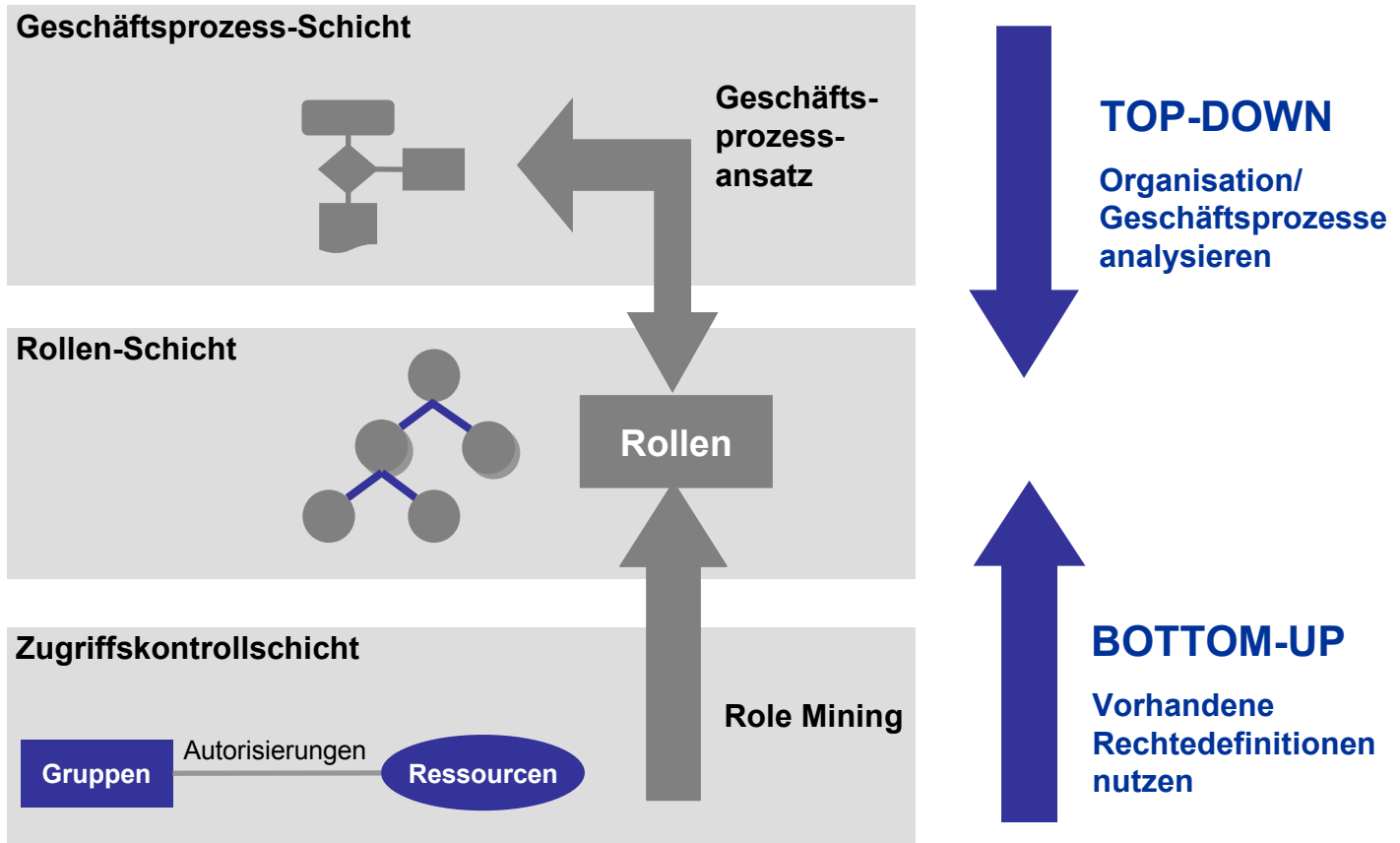
# Praxisbeispiel 2: Provisioning mit RBAC



## Praxisbeispiel 2: Provisioning mit RBAC

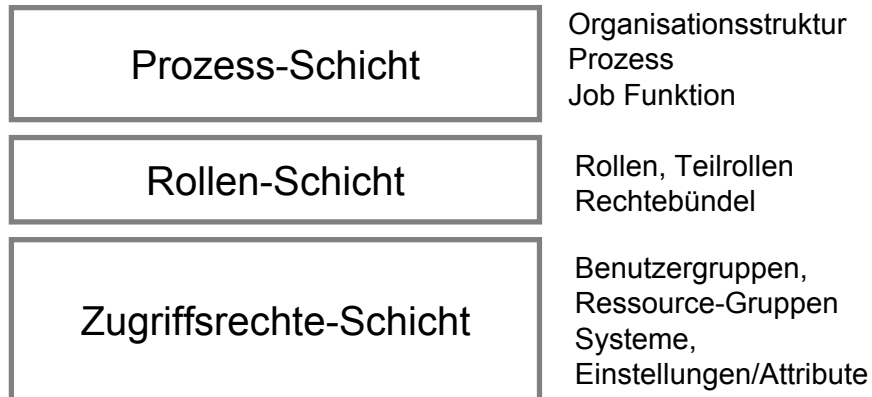


# Der Weg zum Rollenmodell: Top-Down oder Bottom-Up?



# Überlegungen zum Top-Down-Ansatz

- Falls Geschäftsprozessmodell vorhanden und Prozesse/Ressourcen elektronisch verfügbar: Evtl. Rollen aus Prozessen ableiten.
- Management Attention sicherstellen
- Zusammenarbeit mit Fachabteilungen ist erforderlich:
  - Verantwortliche in Fachbereichen finden
  - Fachbereich bei Auswertungen unterstützen: Wer darf was?
- Vorgehensweise für das Rollenmodell festlegen:



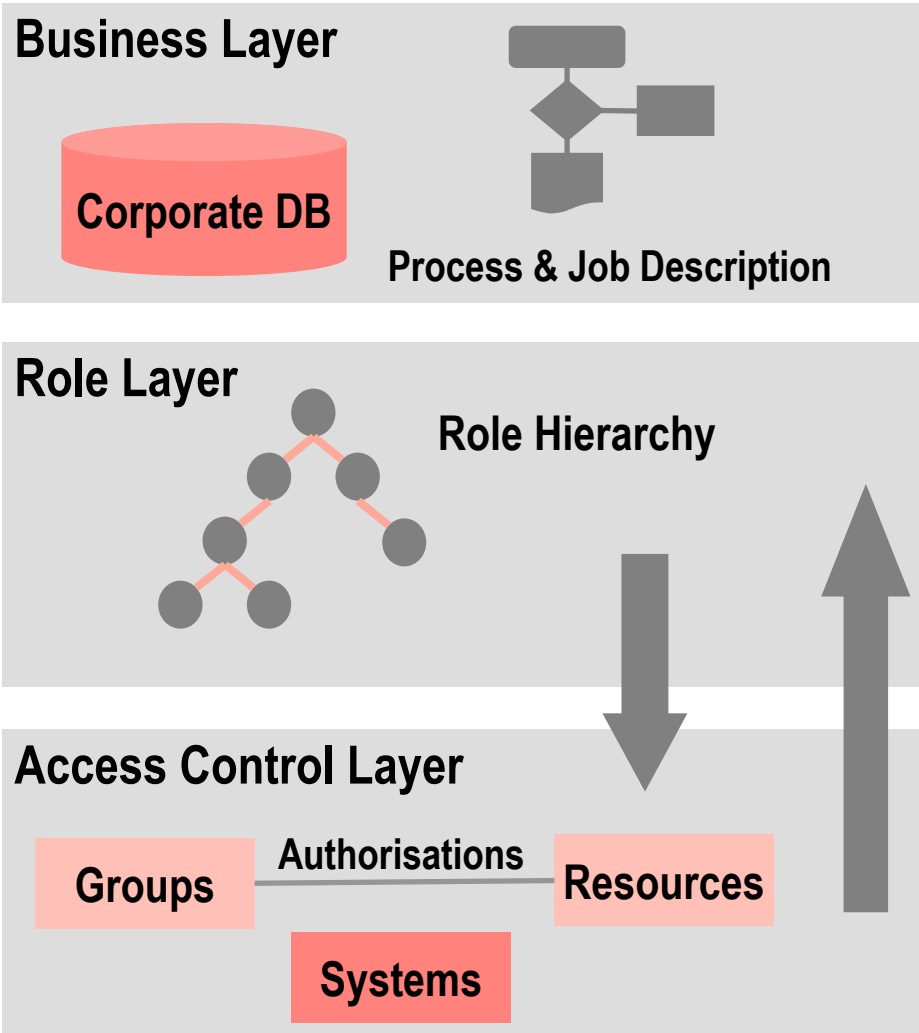
# Top-Down Ansatz: Realisierung des “Need-to-Know” Prinzip

- Für eine korrekte Rechtevergabe ist eine Analyse der Zugriffsrechte vorteilhaft:
  - Risikoanalyse für Ressourcen und Gruppierung in Building Blocks (Resource Profiling)
    - Datenklassifizierung
    - Transaktionen und ihre Zugriffsarten
  - Gruppierung der Benutzer nach operativen Kriterien (“Wer tut was?”)
    - Funktion
    - Vertrauenslevel
  - Aufstellen einer “Enablement Matrix”
- Rollen können die Gruppierung der Benutzer und die Enablement Matrix abbilden.

# Geschäftsvorfälle als Basis für Rollen

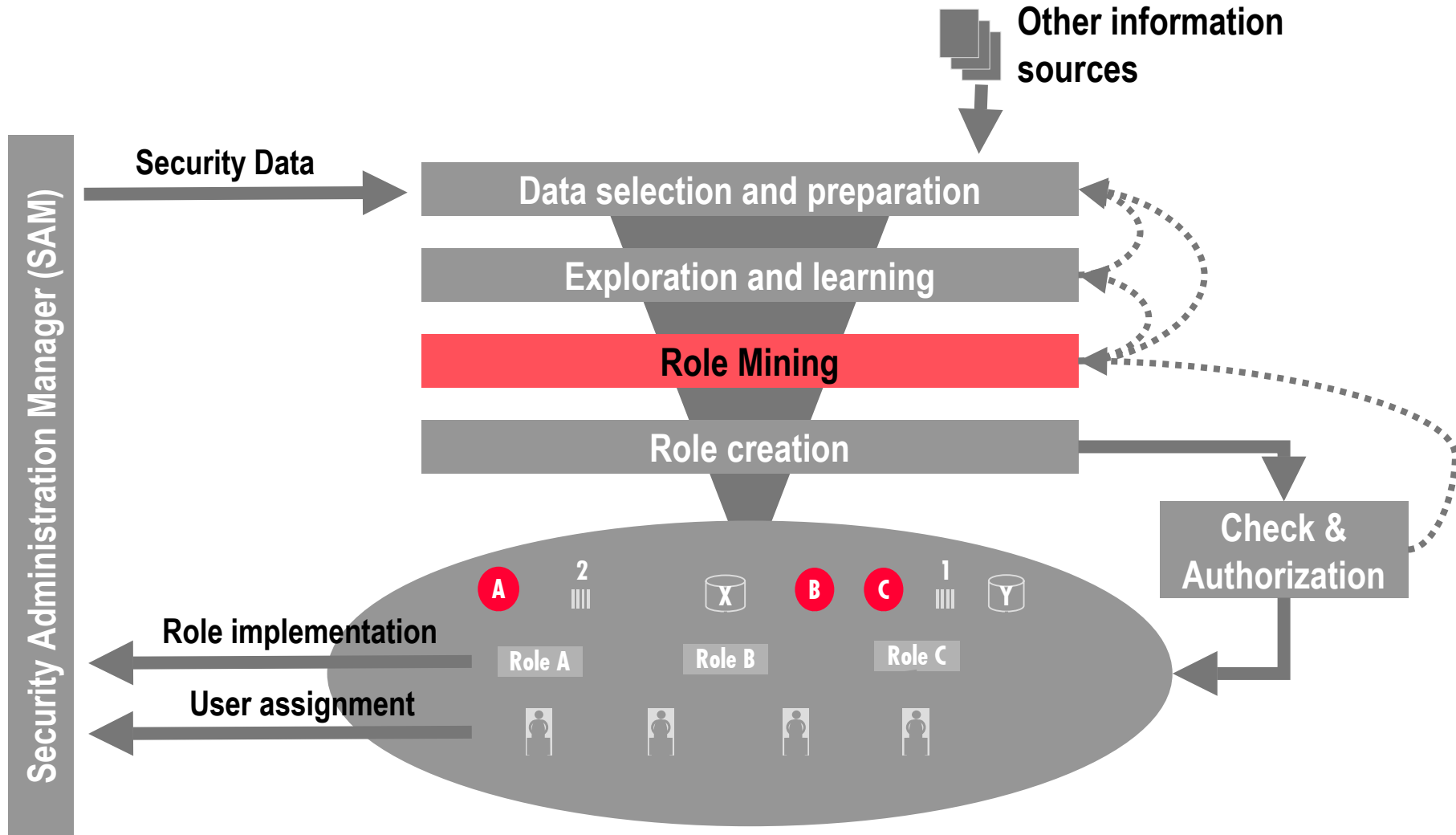
Ereignis	Aktion	Ressource	Operation	Funktion	Zugriffs Recht
Schadens- meldung	Annahme  Zuordnung Sachbearbeiter  Regulierung	Briefe	Lesen	Sekretär	PERMIT GRANT CONNECT  ...
		Offene Anfragen	Einfügen	Sekretär	
		Offene Anfragen Kundenstamm	Lesen Verändern	Manager	
		Schadensreport	Lesen Verändern	Schadens- sachbearbeiter	
Entscheidung	Rabatt reduzieren  Zahlungs- anweisung	Kundenstamm	Verändern	Vertrags- sachbearbeiter	
		Kundenverträge	Einfügen	Schadens- sachbearbeiter	
Brief an Kunden	Brief schreiben	Briefe	Einfügen	Sekretär	

# Role Mining – Die Idee



- Die Berechtigungen sind bereits vorhanden!  
–Untersuchung der vorhandenen Zugriffskontrolldaten
- Suche nach Mustern in den Berechtigungsdaten
- Ableitung von Rollen, Abgleich mit Geschäftsprozessen, Restrukturierung der Zugriffsrechte

# Role Mining – Vorgehensweise SAM Role Miner



# Administration mit Rollen und Regeln

# IM Konzepte – keine Frage der Religion

## Rollen, Regeln, Policies

Es gibt doch auch noch „Regeln“ und „Policies“ – welchem Paradigma soll ich folgen?



- Rollen, Regeln und Policies sind allesamt Hilfsmittel für eine effizientere und automatisierte Administration
- Regelbeispiel:  
„Wenn ein Benutzer auf einem Windows-Server in Köln-Niehl arbeitet, dann wird sein Home Directory auf dem Kölner Zentralserver eingerichtet“
- Beispiele für Policy oder Richtlinie:  
„Kein Benutzer darf Sonntags arbeiten“  
„Kassierer dürfen auf ihre eigenen Konten nicht zugreifen“
- Der Unterschied zwischen Regeln und Policies schwimmt hin und wieder
- Ein Provisioning-System sollte idealerweise Rollen, Regeln und Policies unterstützen die Ansätze produktiv und gemeinsam nutzen.

# Regelbasierte Administration

## **Administrative Regeln**

„If USER\_OU = APPROVER\_OU  
then  
APPROVE\_REQUEST is allowed“

## **Provisioning-Regeln**

„If USER\_JOB\_FCT is TELLER  
then  
assign USER to Role  
TELLER\_<USER\_LOCATION>“

**Workflow,  
Delegated  
Administration**

**Provisioning  
Engine  
(Automation)**

**Business Administration Logic**

„If USER\_TYPE = MANAGER  
then  
MAILBOX\_PUBLIC\_READ\_ACCESS  
= NO“

## **Trigger-Regeln**

**Target Systems**

## **Zugriffskontrollregeln**

„If USER\_LOCATION =  
CONTRACT\_DEPARTMENT and  
CONTRACT\_TYPE is not VIP then  
allow CONTRACT\_CHANGE “

# Vorteile regelbasierter Administration

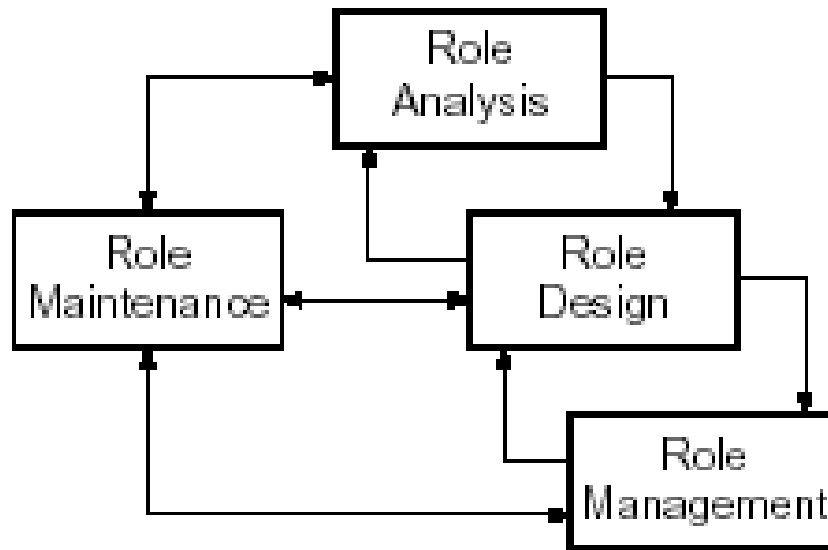
- Provisioning-Regeln ...
  - sorgen für die einfache Umsetzung der zu automatisierenden Prozesse
  - sind die Basis für Automation als bedeutenden ROI Faktor
- Trigger-Regeln ...
  - Stellen Parameter korrekt ein
  - vereinfachen und beschleunigen die Administration
- Administrative Regeln ...
  - bieten die Möglichkeit, Administrationskonzepte schnell zu konfigurieren
  - spart Implementierungsaufwand
- Zugriffskontrollregeln ...
  - Bieten eine übersichtliche, geschäftsprozessorientierte Administrationsmöglichkeit

# Administrationskonzept mit Rollen und Regeln

- Rollen sind eher statisch, Regeln eher dynamisch
- Wie setze ich Rollen ein, wie Regeln? – Einige Hinweise:
  - Basisparameter für Rollen sollten relativ geringer Änderungshäufigkeit unterliegen
  - Mittels Regeln sollte die Anzahl der Rollen minimiert werden
  - Nutzung von Rollen vereinfacht Revisionsfähigkeit/Nachvollziehbarkeit
  - Rollen erlauben Policy Enforcement:
    - Rollen definieren einen Sollzustand für Berechtigungen und Attribute der zugeordneten Benutzer.
    - Bei Wahl einer geeigneten Provisioning-Software kann dieser geprüft und ggf. in den Zielsystemen durchgesetzt werden
  - Wo möglich, sollten Rollen statt Trigger-Regeln eingesetzt werden
  - Regeln sollten nicht zu komplex sein, damit Übersichtlichkeit gewahrt bleibt
  - Kaskadierende Regeln und große Rollenhierarchien sind problematisch

# Life Cycle Management für Rollen und Regeln

- Für Rollen und Regeln muss ein Pflegeprozess eingerichtet werden:
  - „Role Engineering“ als iteratives Vorgehen
    - Role Management: Routineänderungen bei Rollen (z.B. Löschen einer Ressourcenberechtigung)
    - Role Maintenance: Änderungen des Rollenkonzeptes
  - Pflege von Regeln setzt Detailkenntnisse über das Regelwerk voraus



# Ausblick

# Ausblick

- Die grundsätzlichen Vorteile von RBAC sind heute akzeptiert, RBAC ist nach anfänglicher Skepsis wieder ein Thema
- “Rollen und Regeln” sind - ausgewogen genutzt - ein idealer Ansatz
- Die Kenntnisse im Bereich RBAC haben spürbar zugenommen; daher sind zahlreiche weitere Implementierungen zu erwarten
- Federated Identity Management:
  - Beim Austausch von Berechtigungsinformationen ist die Einigung auf semantische Rolleninhalte noch ein Problem
  - SPML behandelt derzeit keine Rollen
  - XACML beinhaltet Rollendefinitionen

## RBAC Literatur und Links (Auswahl)

- D.F. Ferraiolo, D.R. Kuhn, R. Chandramouli, Role Based Access Control, Artech House, 2003  
(Buch zu RBAC)
- R. Sandhu, Role-based Access control, G. Mason university, 1997  
(Überblicksartikel)
- <http://csrc.nist.gov/rbac/>  
(RBAC-Seite des NIST mit vielen weiterführenden Links)
- D.F. Ferraiolo und D.R. Kuhn, Role Based Access Control, 15th National Computer Security Conference, 1992  
(der Grundlagenartikel)
- <http://docs.oasis-open.org/xacml/cd-xacml-rbac-profile-01.pdf>  
(XACML profile, includes RBAC definitions)
- Kern, Advanced Features for Enterprise-Wide Role-Based Access Control, ACSAC 2002
- Kern, Kuhlmann, Moffet, Schaad, Observations on the Role Life-Cycle in the Context of Enterprise Security Management, Proceedings of SACMAT 2002
- K. Kampman, G. Gebel, Enterprise Experiences with Roles, Burton Group, 2003  
(Survey on Role Implementation)
- G. Gebel, Roles and Access Management: Seeking a Balance Between Roles and Rules, Burton Group, 2003
- Kuhlmann, Schimpf, Shohat, Role Mining - Revealing Business Roles for Security Administration using Data Mining Technology, Proceedings of SACMAT 2003
- <http://www.acm.org/sigs/sigsac/sacmat/>  
(SACMAT Homepage)

**-betasystems**

**Vielen Dank für Ihre Aufmerksamkeit!**

[martin.kuhlmann@betasystems.com](mailto:martin.kuhlmann@betasystems.com)