

Zentrale vs. dezentrale Rollenverwaltung und eXtreme Role Engineering als alternatives Verfahren zur Rechteverwaltung

Treffen des Arbeitskreis Verzeichnisdienste des ZKI

Dr.-Ing. Thomas Hildmann
IT Dienstleistungszentrum der TU Berlin



Vorstellung von Person und Einrichtung



Dr.-Ing. Thomas Hildmann
Promotion: Umfassendes
Autorisierungsmanagement

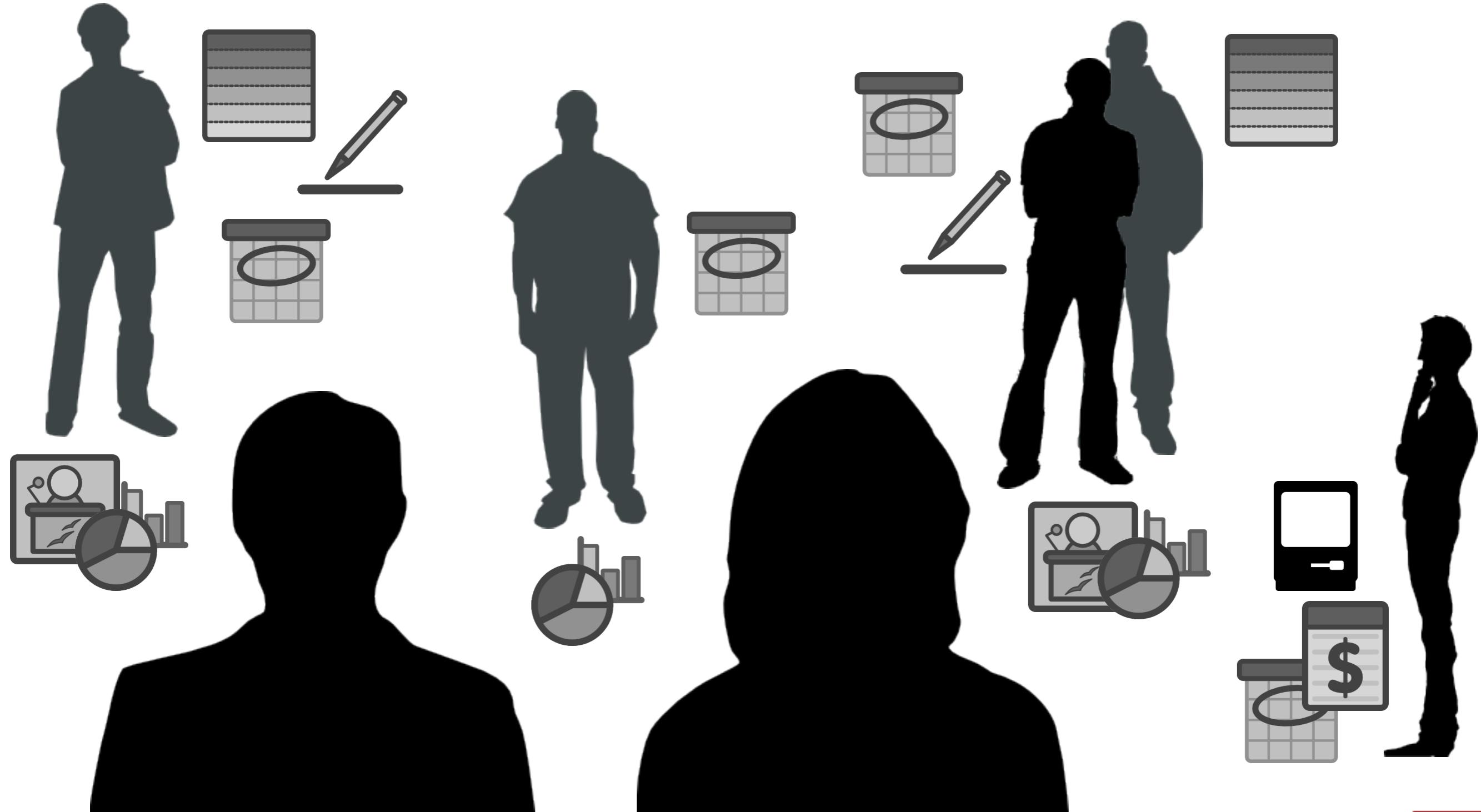
Identity Management
7 Mitarbeiter

tubIT IT-Service-Center
Forschung/Lehre und Verwaltung

Technische Universität Berlin
~30.000 Studierende, ~8.000 Mitarbeiter

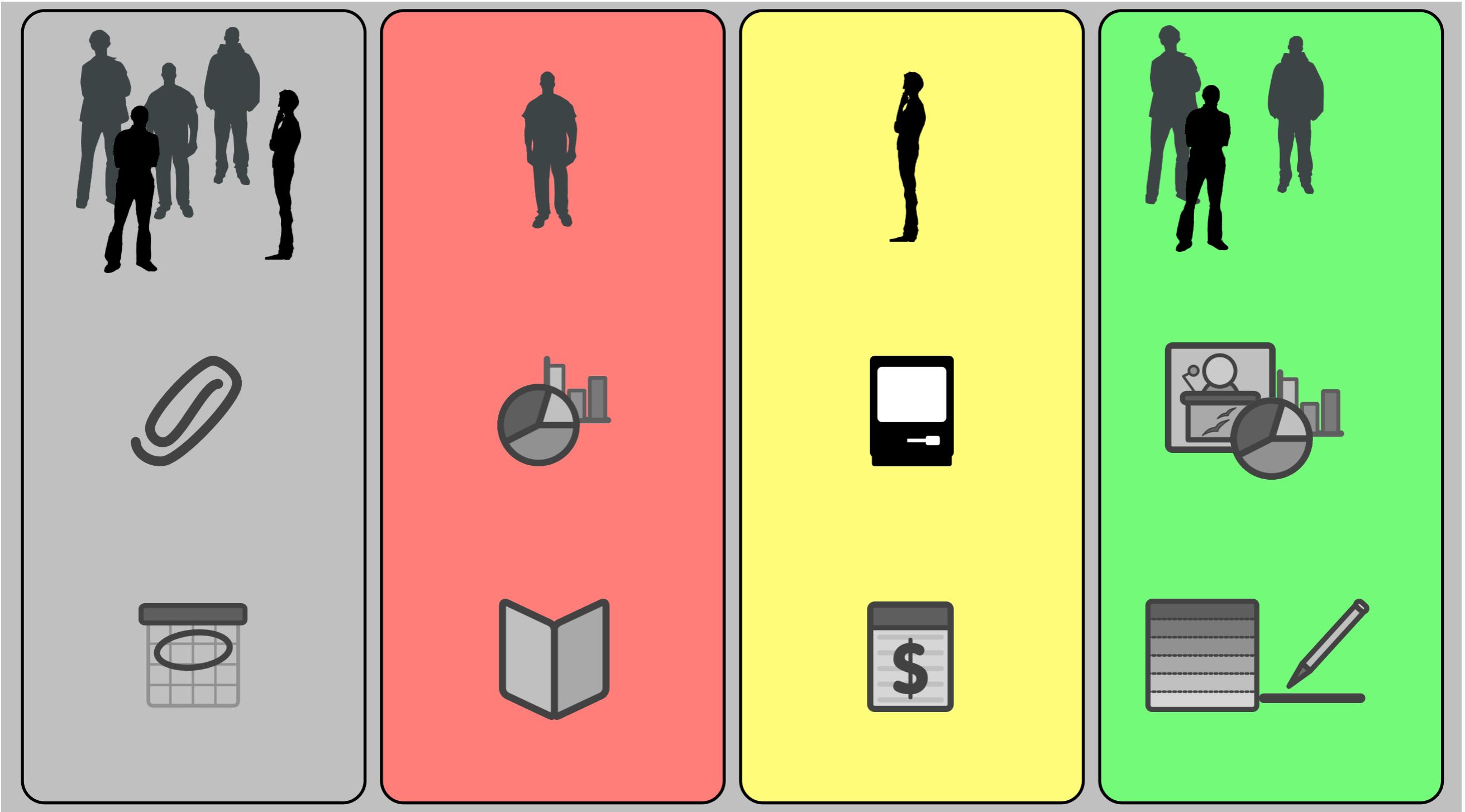
Motivation

Das Fachgebiet

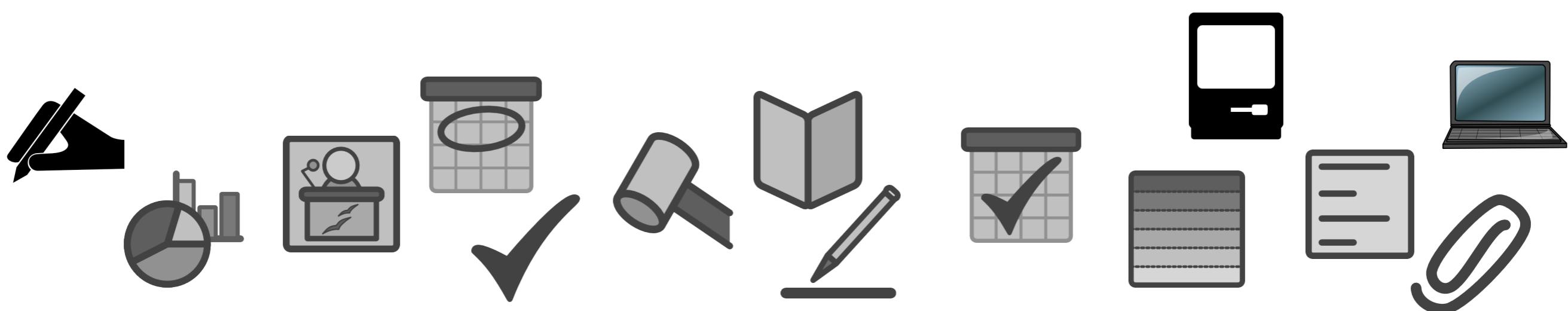
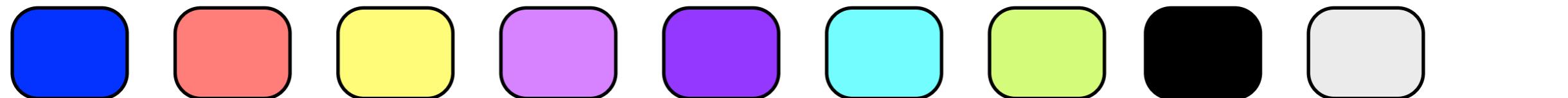
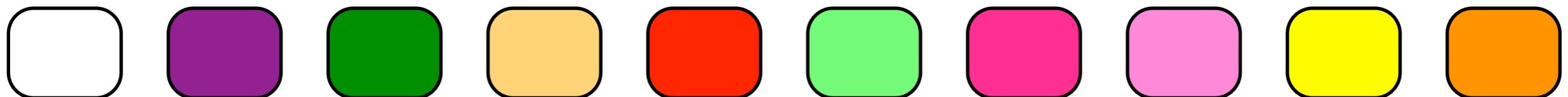


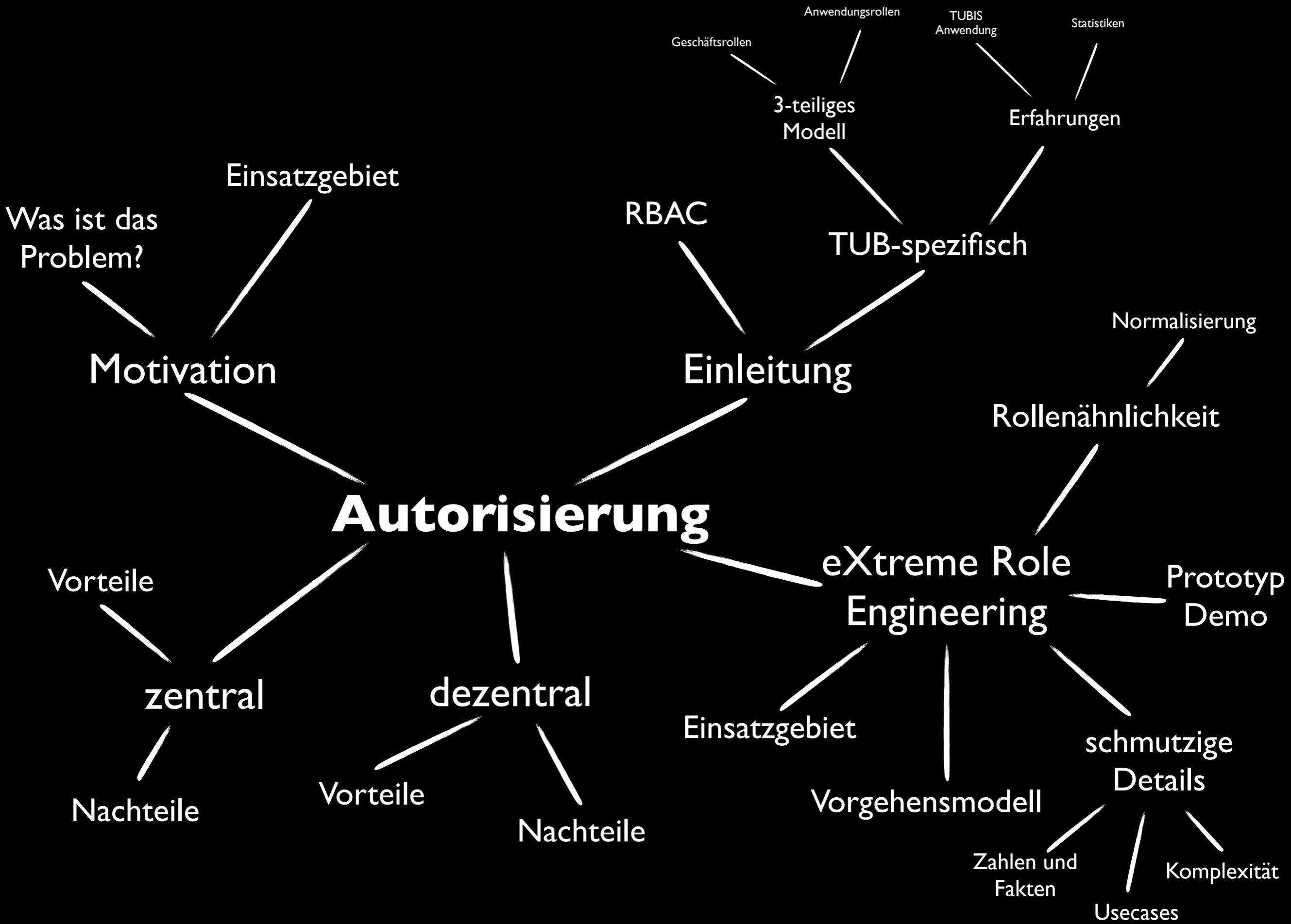
Motivation

Rollen



Die richtige Rollenzahl





ion

Einleit

Autorisierung

ral

dezentral

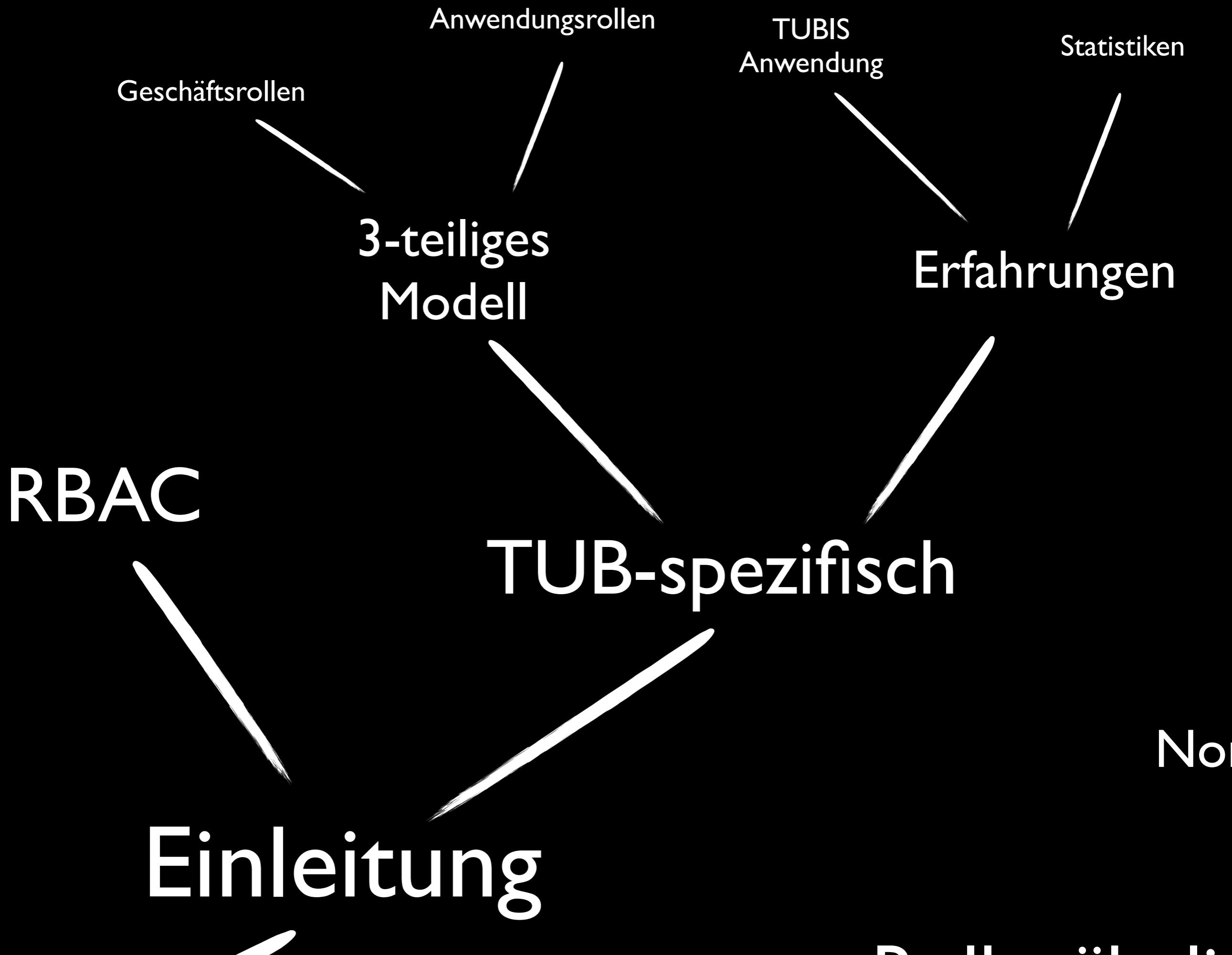
Einsatz

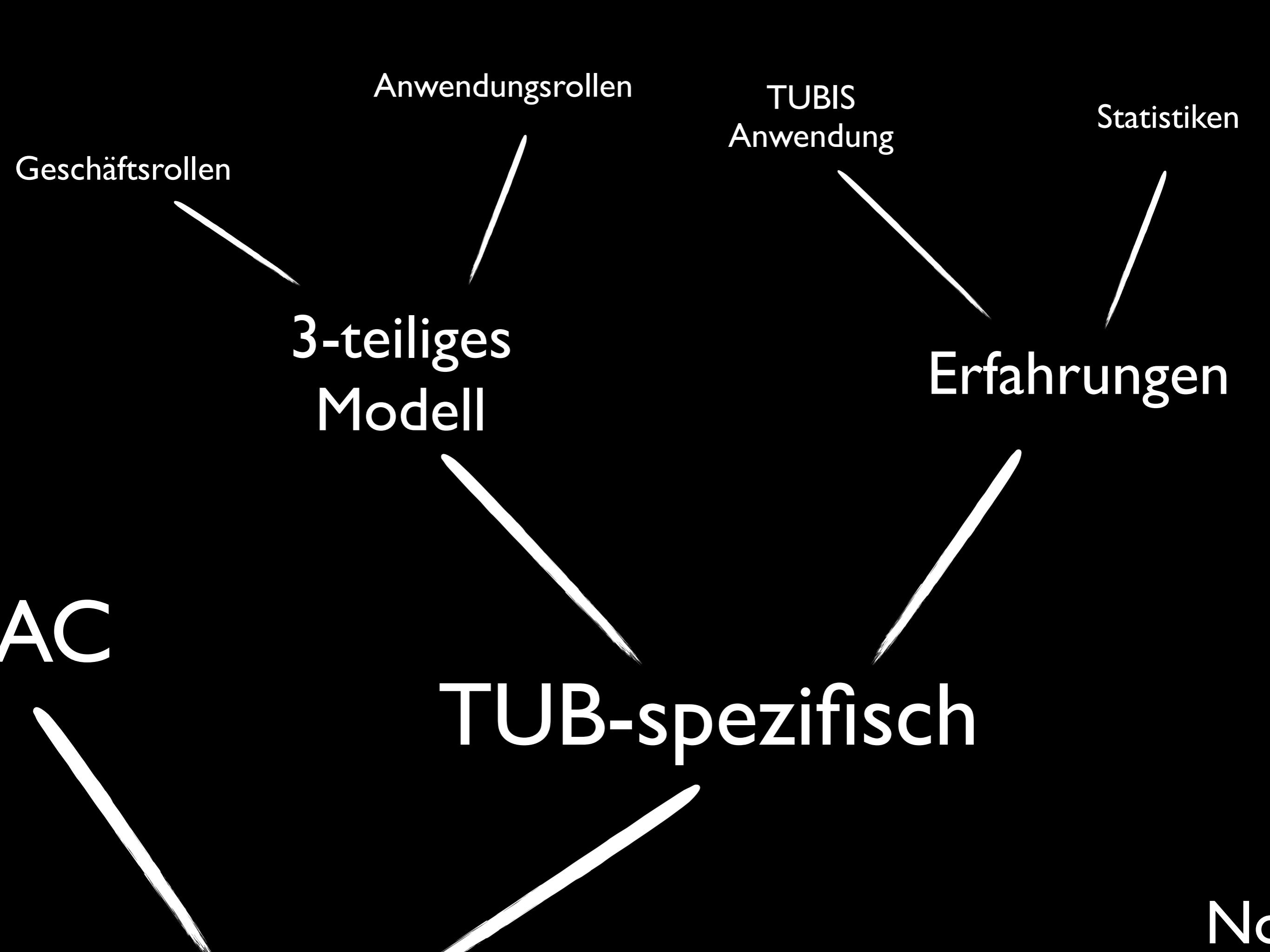
Einsatzgebiet

Was ist das
Problem?

Motivation

Auto



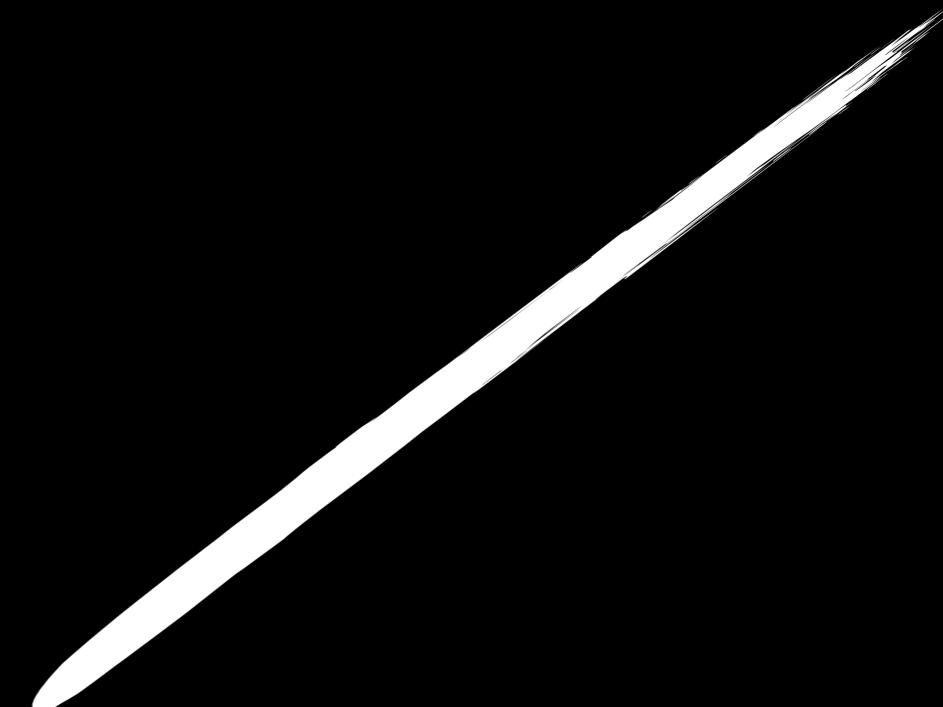


Ein

Autorisierung

dezentral

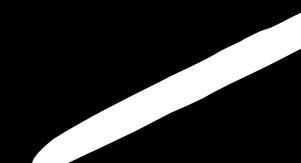
Vorteile



zentral



Nachteile



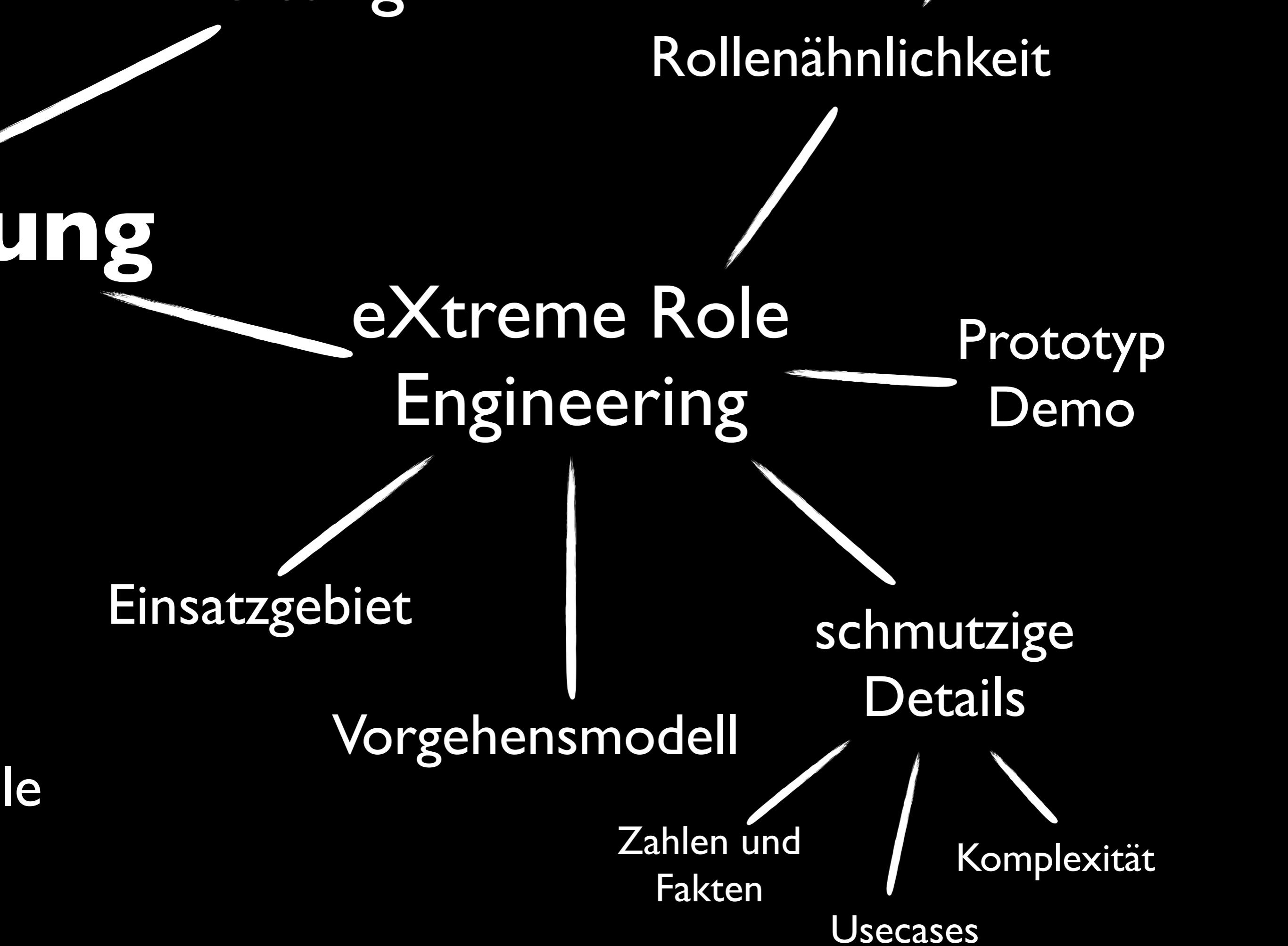
Vorteile

dezentral

Vorteile

Nachteile

Ein:



ng

eXtreme Role Engineering

Einsatzgebiet

Vorgehensmodell

Zahlen und

schm

De

ng

Normalisierung

Rollenähnlichkeit

eXtreme Role
Engineering

Prototyp
Demo

eXtreme Role Engineering

```
graph TD; Central(( )) --> Projekt[Projekt]; Central --> Vorgehensmodell[Vorgehensmodell]; Central --> ZahlenFakten[Zahlen und Fakten]; Central --> Komplexitaet[Komplexität]; Central --> Usecases[Usecases]; Central --> schmutzigeDetails[schmutzige Details]; Central --> Demo[Demo]; Central --> Prototyp[Prototyp];
```

Projekt

Vorgehensmodell

Zahlen und
Fakten

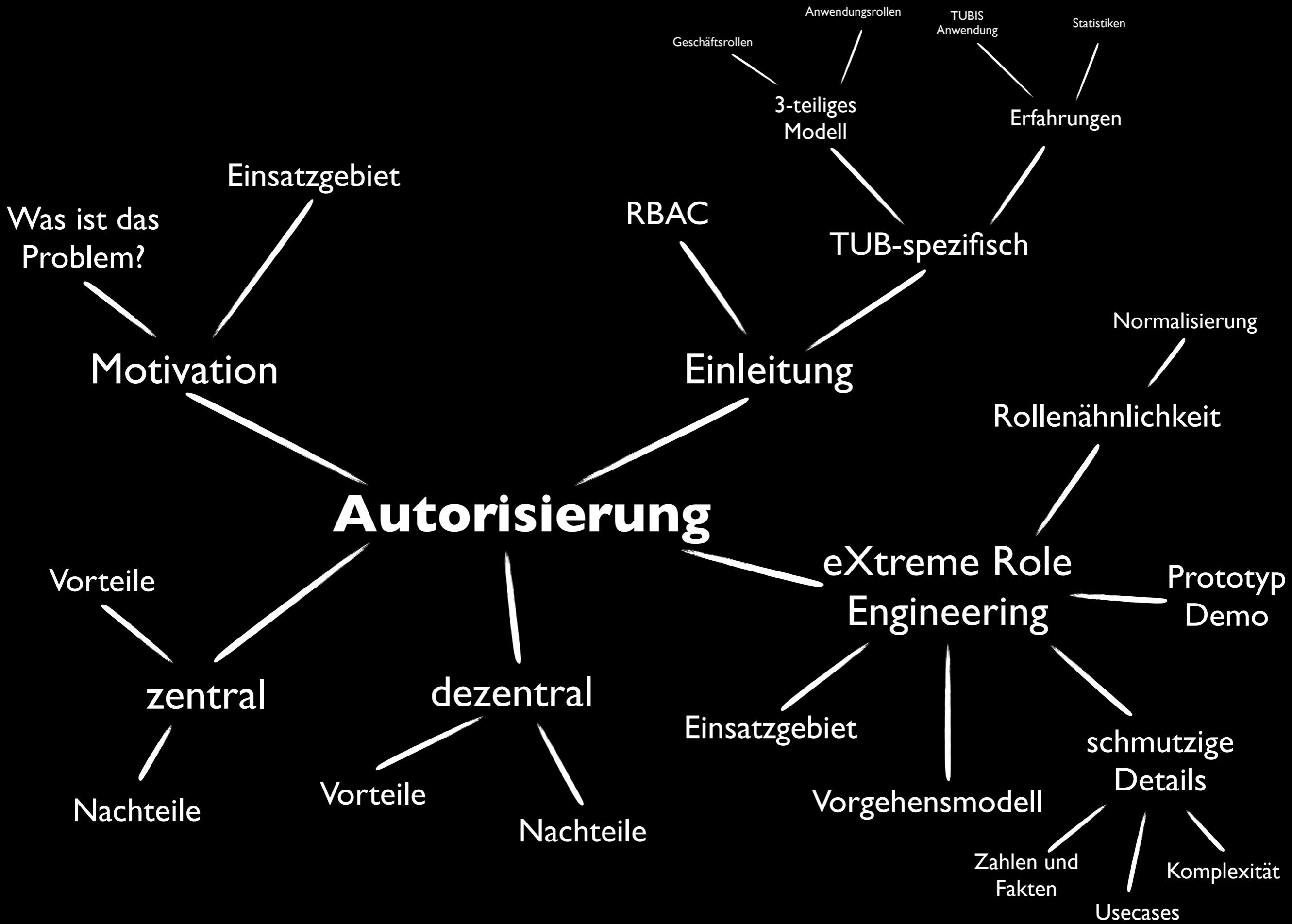
Usecases

schmutzige

Details

Komplexität

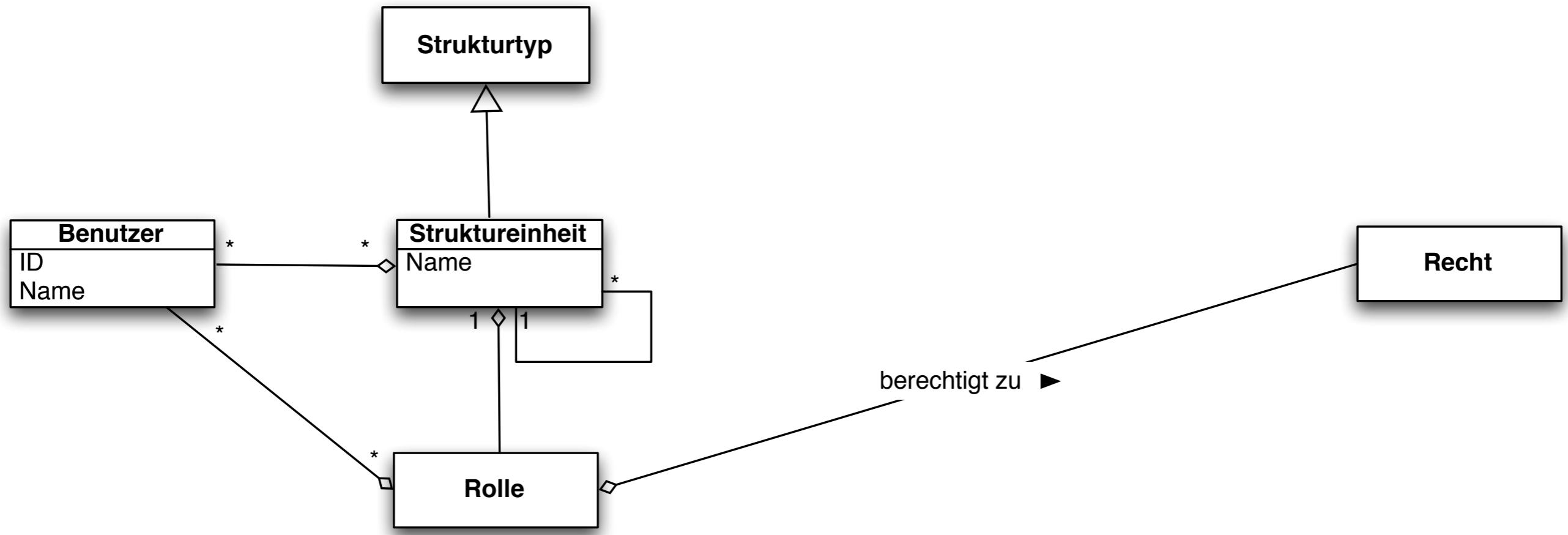
Prototyp
Demo



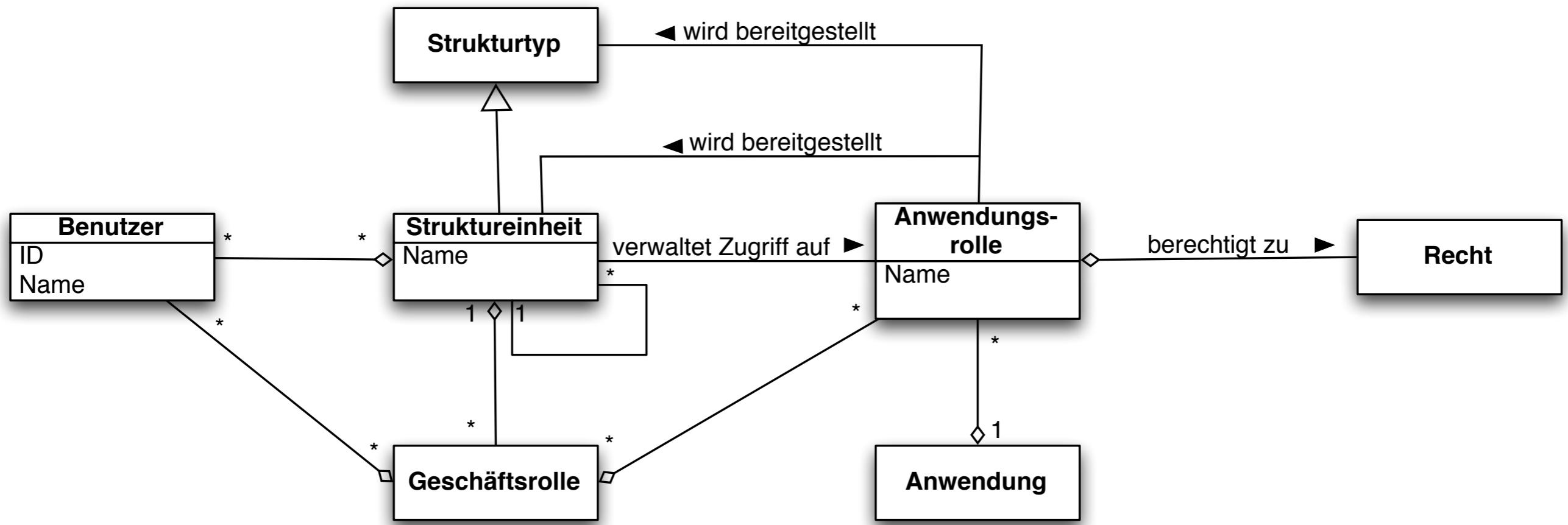
Klassisches RBAC



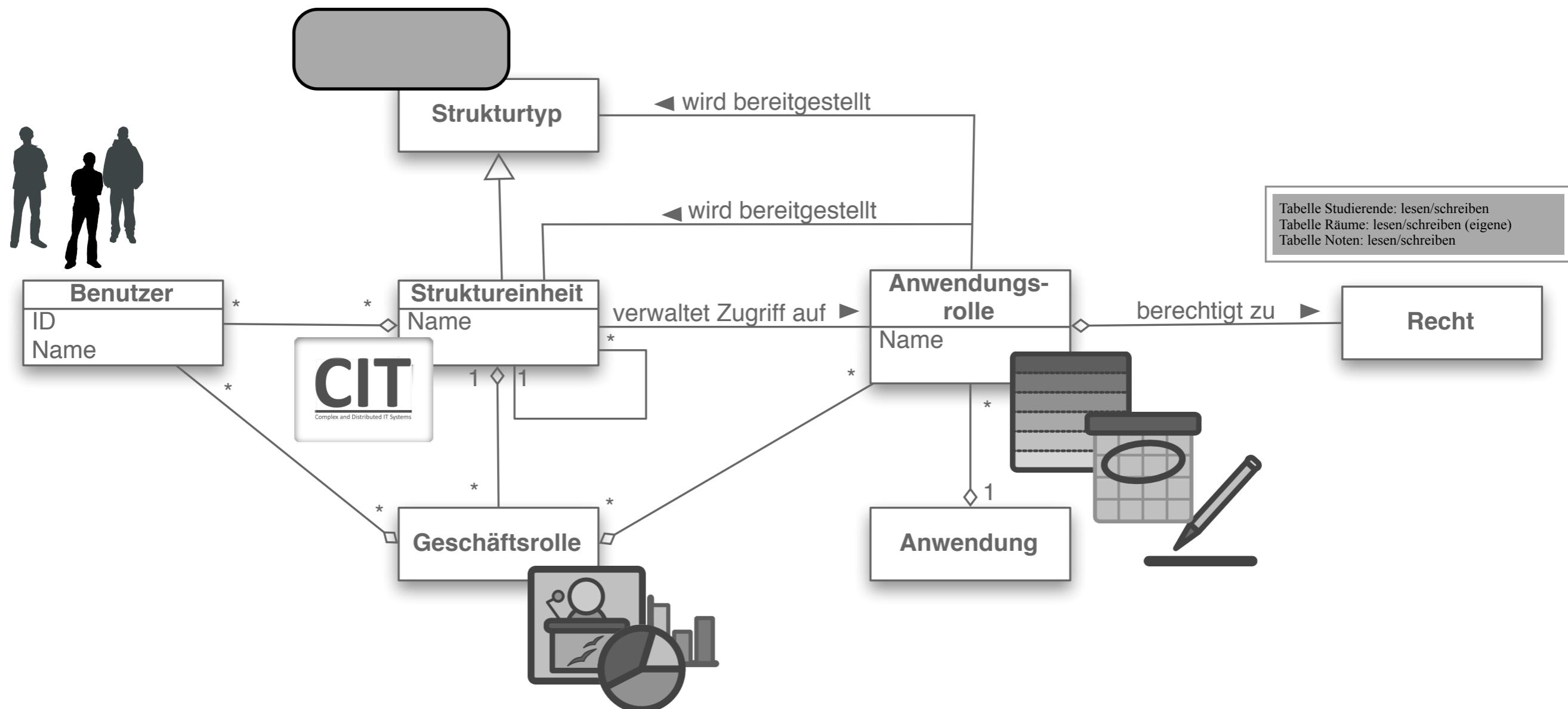
Verteilte Administration



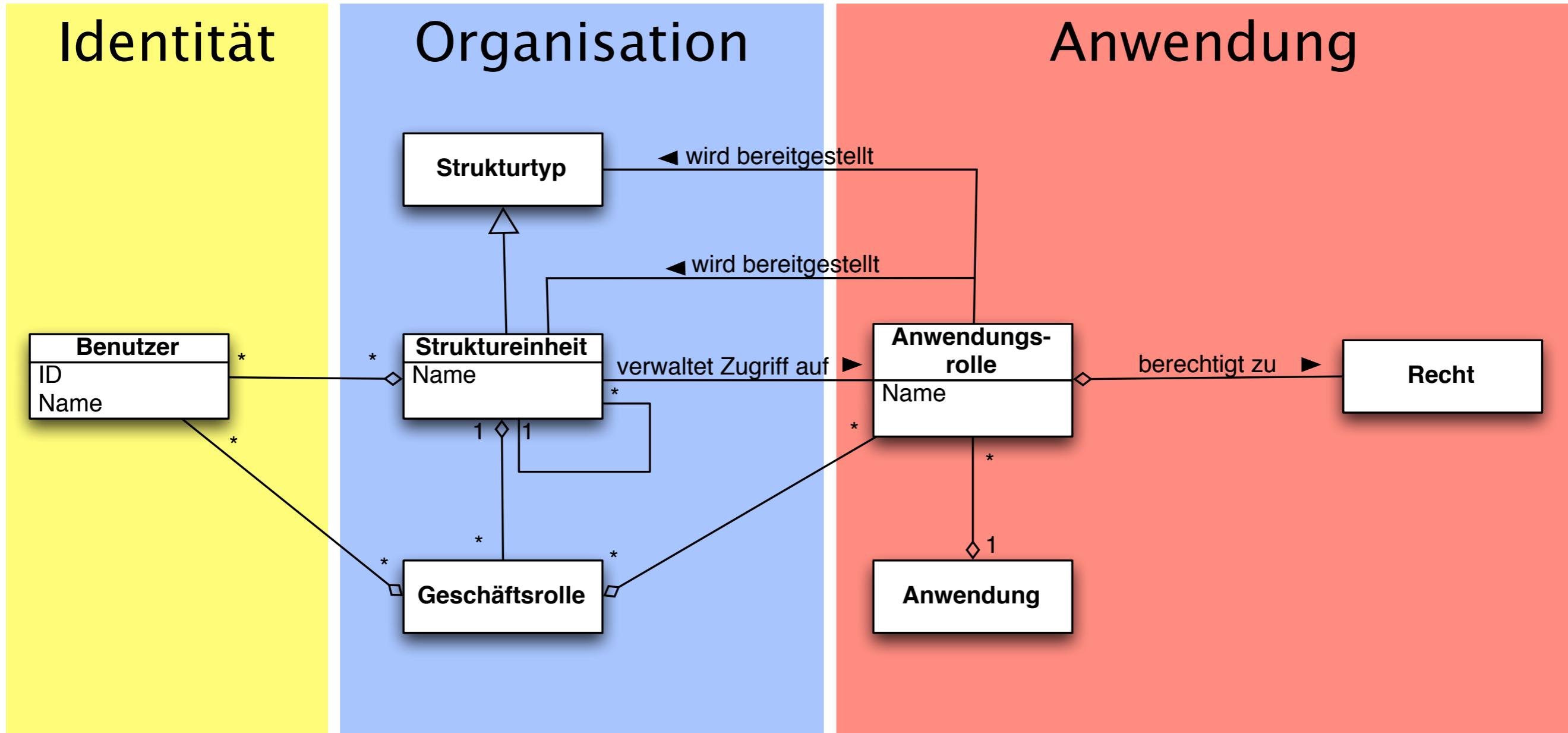
Kapselung der Anwendungsschicht



Eingangsbeispiel im Rollenmodell



3-teiliges Modell mit Views



Erfahrungen im Bereich rollenbasiertes IdM an der TUB

2001 Campuskarte

2007 Webportal mit rollen-basierter
Autorisierung

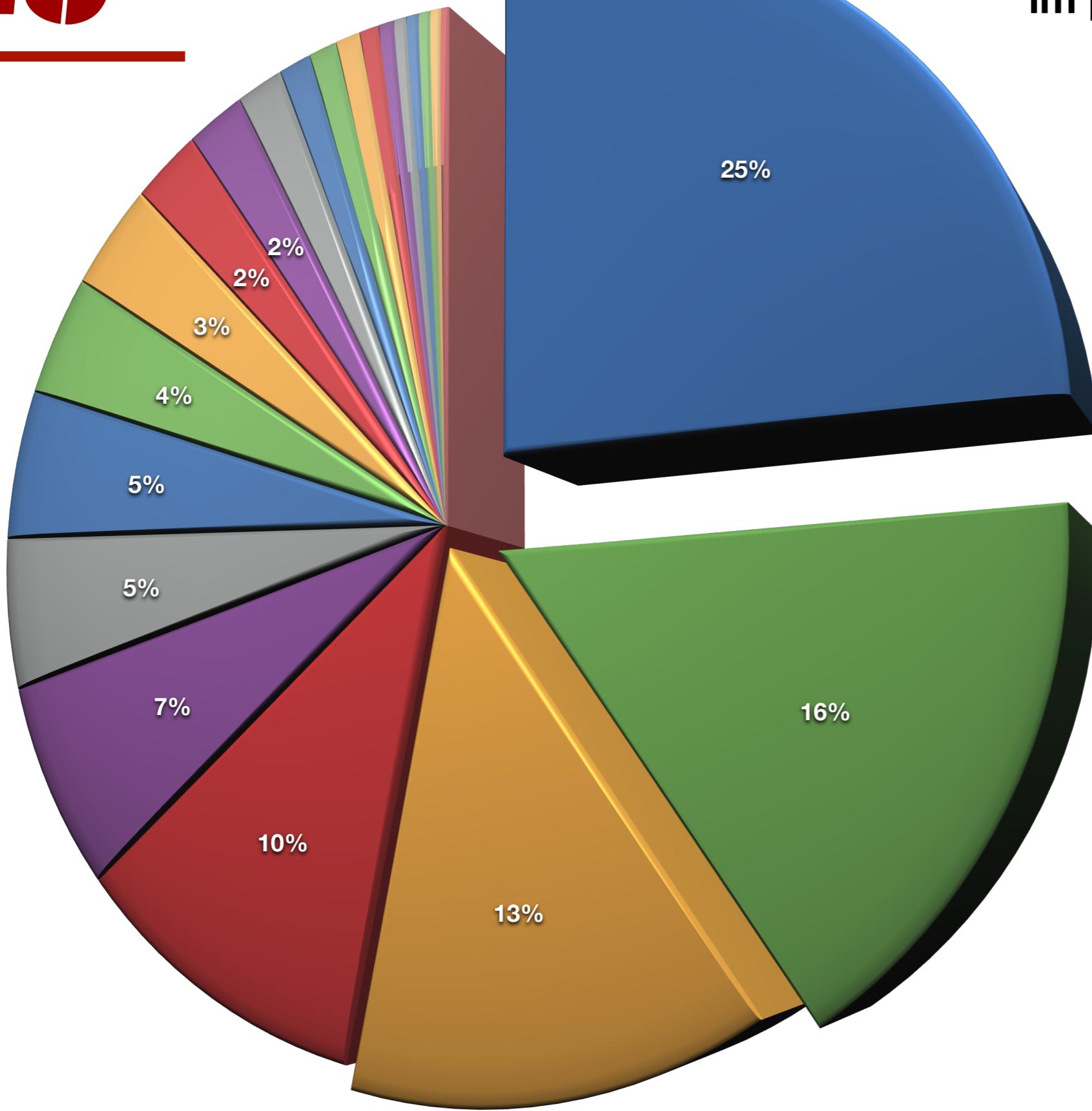
- AA-Gateway: Apache, Jetty/Servlet, PHP
- IdM/RBAC: J2EE Eigenentwicklung
- ~ 50.000 Entitäten im IdM-System
- ~ 30 Anwendungen im Portal
- ~ 500 Einheiten (Fakultät, Institut, Referat...)
- ~ 3000 Rollen / durchschnittl. ~ 6 pro Einheit

TUB-Login

mit Passwort
 mit Campuskarte

IT-Dienste
Rollenverwaltung
Kontenverwaltung
Teamverwaltung
Strukturverwaltung
Orgname-Administration
Softwareportal
Softwareportal (Testphase)
Hardwareportal (Sofort-PC)
Hardwareportal (Mac)
Hardwareportal (Testlogin)
TYPO3 Editierbereich
Campuskarte
Passwort-Rücksetzung
ABR-Infotool
Liste der Rollenverwalter und IT-Betreuer
UB-Datenexport
IT-Anträge
Externen-Accounts
IP-Adresse
Gast-Accounts
TYPO3-Auftritt
Webauftritt
Mailingliste

Nutzungshäufigkeit von Diensten im persönlichen Portal für 2009





Rollenverwaltung

TUBIS-Rollenverwaltung: Zentrales IT-Dienstleistungszentrum der Technischen Universität Berlin (tubIT)
Ihre Rolle: Verwalter TU-Berlin



Organisationseinheit auswählen

Organisationseinheiten

1 Ebene anzeigen 2 Ebenen anzeigen 3 Ebenen anzeigen

Geschlossene Organisationseinheiten anzeigen

[Organisationseinheiten neu aufbauen](#)

47 Zentrales IT-Dienstleistungszentrum der Technischen Universität B ...

4700 Zentrales IT-Dienstleistungszentrum der Technischen Universität ...

47001100 IT-Service-Center TU Berlin (tubIT)

47008100 tubIT-Laden

Informationen der ausgewählten Organisationseinheit

Name:	Zentrales IT-Dienstleistungszentrum der Technischen Universität Berlin (tubIT)
Kostenstelle:	47
Status:	aktiv
Kategorie:	Zentraleinrichtung
Genehmigte Kurzbezeichnung (OrgName):	tubit
Beantragte Kurzbezeichnung:	tubit
Beschreibung:	Zentrales IT-Dienstleistungszentrum der Technischen Universität Berlin (tubIT)
Adresse:	EN 50 Einsteinufer 17, 10587 Berlin
Telefon:	22703
Fax:	21060
E-mail:	tubit@tu-berlin.de
Homepage:	www.tubit.tu-berlin.de
Rollenverwalter:	Herr Klaus Nagel, Tel: 314-25786

[Selektierte Organisationseinheit auswählen](#) [Eine Ebene höher](#) [Übersicht](#)

Rollenverwaltung

TUBIS-Rollenverwaltung: IT-Service-Center TU Berlin (tubIT)

Ihre Rolle: Verwalter TU-Berlin



Organisationseinheit auswählen : Organisationseinheit verwalten : Geschäftsrollen-Übersicht

Alle Geschäftsrollen dieser Organisationseinheit

Bestell Tester
DNS-Administrator
DNS-Verwalter
Gast-Verwalter
Leiter/in Bereich - 47001100 (n.v.)
Mitarbeiter/in Zentraleinrichtung - 47001100
Modulverwalter/in
PERS Büroleitung - 47001100 (nicht delegierbar)
POS Tester
Prüfer/in
PW-Verwalter
t3admin
TUBIS-Master
tubIT-Anwendungsverwalter
tuBV-Verwalter
Typo3 Antrag
Typo3 Chefredakteur
Typo3 Entwickler
Typo3 Redakteur
Typo3 Verwalter

n.v.: (nicht vergeben) - Dieser Rolle wurden noch keine Positionen zugewiesen

- [Geschäftsrolle bearbeiten](#)
- [Geschäftsrolle entfernen](#)
- [Geschäftsrolle hinzufügen](#)
- [Mitglieder anzeigen](#)

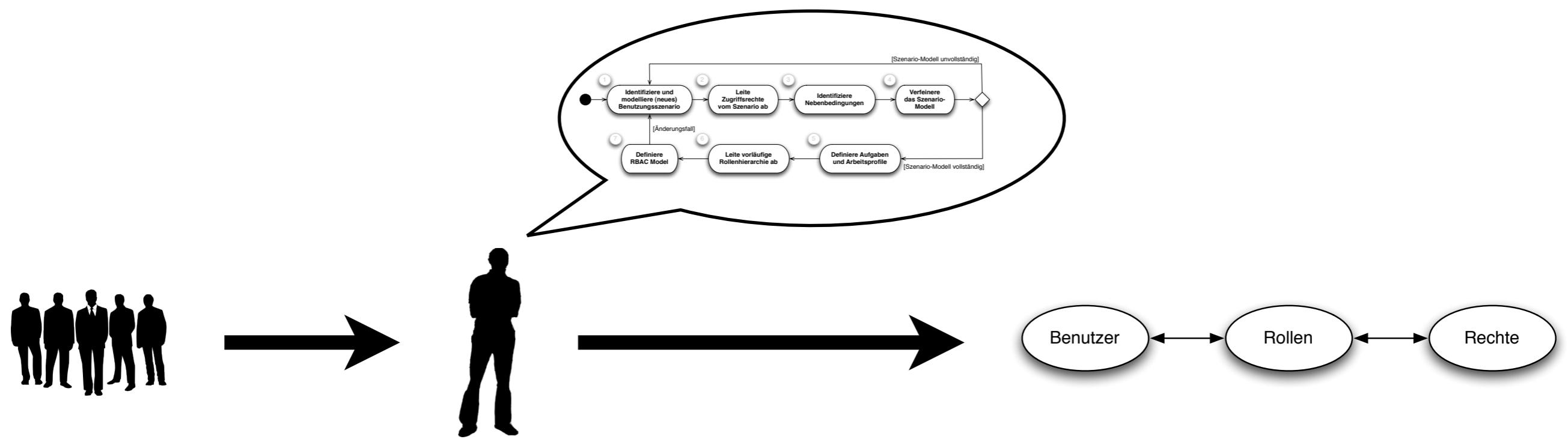
Mitglieder der ausgewählten Geschäftsrolle

Gehrcke, Hans-Christian Sonstige Angestellte (47001100)
Schmidt, Martin Handw./Facharbeiter/in (47001100)
Kwiatkowski, Manfred Sonstige Angestellte (47001100)
Rieger, Timo Ang. i.d. Maschinenbedienung (Maschinensaal) (47001100)
Nagel, Klaus Wissenschaftliche/r Angestellte/r (47001100)
Gebhardt, Thomas Sonstige Angestellte (47001100)

[Mitglied bearbeiten](#)

Zentrale Lösung

Was verstehе ich darunter?

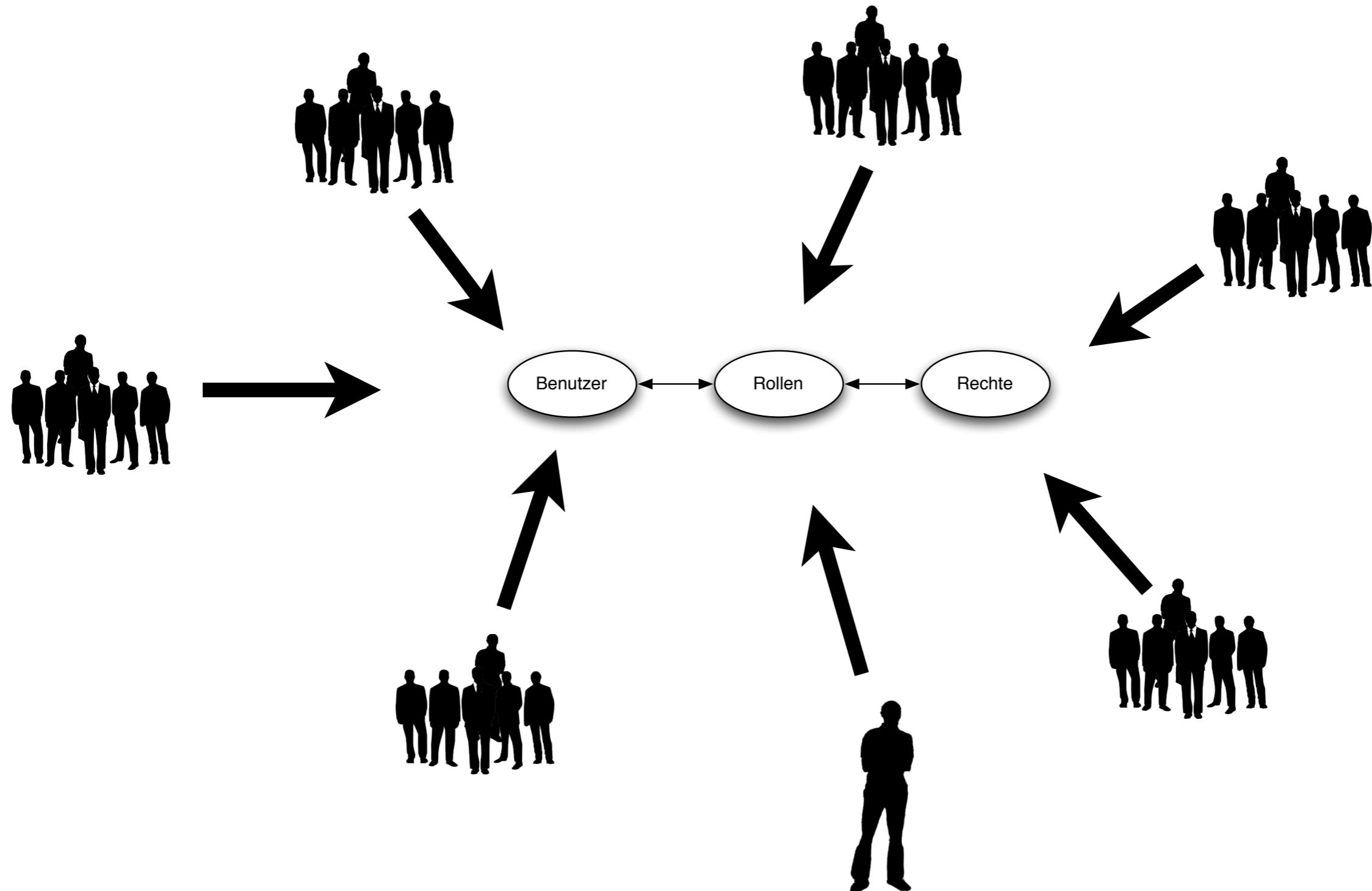


Vorteile einer zentralen Lösung

- Klassischer RBAC-Ansatz: Verteilung der Verantwortung
- Es existieren Role-Engineering Methoden für eine zentrale Lösung, die zu strukturierten Modellen führen
- Know-How über Autorisierungsmodell gebündelt
- Überblick über das gesamte System
- IT-Dienstleister = Rollendienstleister (Service)
- Klassischer Weg: Anforderung, Analyse, Implementierung
- Rollenadministratoren können beraten und prüfen
- flache Lernkurve als Einstieg für Nicht-Experten
- Constraints können organisatorisch umgesetzt werden
- Vertretungsregelungen bei Admins durch Dienstleister

Dezentrale Lösung

Was verstehе ich darunter?



Erfahrungen im Bereich rollenbasiertes IdM an der TUB

- Kein Bittstellergefühl
- Reduzierung der Bearbeitungszeit
- Backuprollen in übergeordneten Einheiten
- Rollenvertretungen von jedem verwaltbar
- Flexible selbst gestaltete Struktur
- Transparenz
- Verteilung der Verantwortlichkeiten
- Entlastung der Administratoren
- Fehlinterpretation durch dritte entfällt
- Fehler sind lokal beschränkt
- Sehr guter Überblick über die verwaltete Einheit

Nachteile einer dezentralen Lösung und Maßnahmen

Nachteil für lokalen Admin

Fehlender Überblick über Rollenmodell

Fehlendes Wissen um neue Anwendungen

Folgenabschätzung und Konsequenzen

Abwesenheit des lokalen Rollenadministrators

Fehlendes Anwendungswissen

Hohe Komplexität des Modells

Maßnahmen

Mehrteiliges Modell
Anwendungs-, dezentrale/zentrale Rollenadmins

Informationspolitik
Support

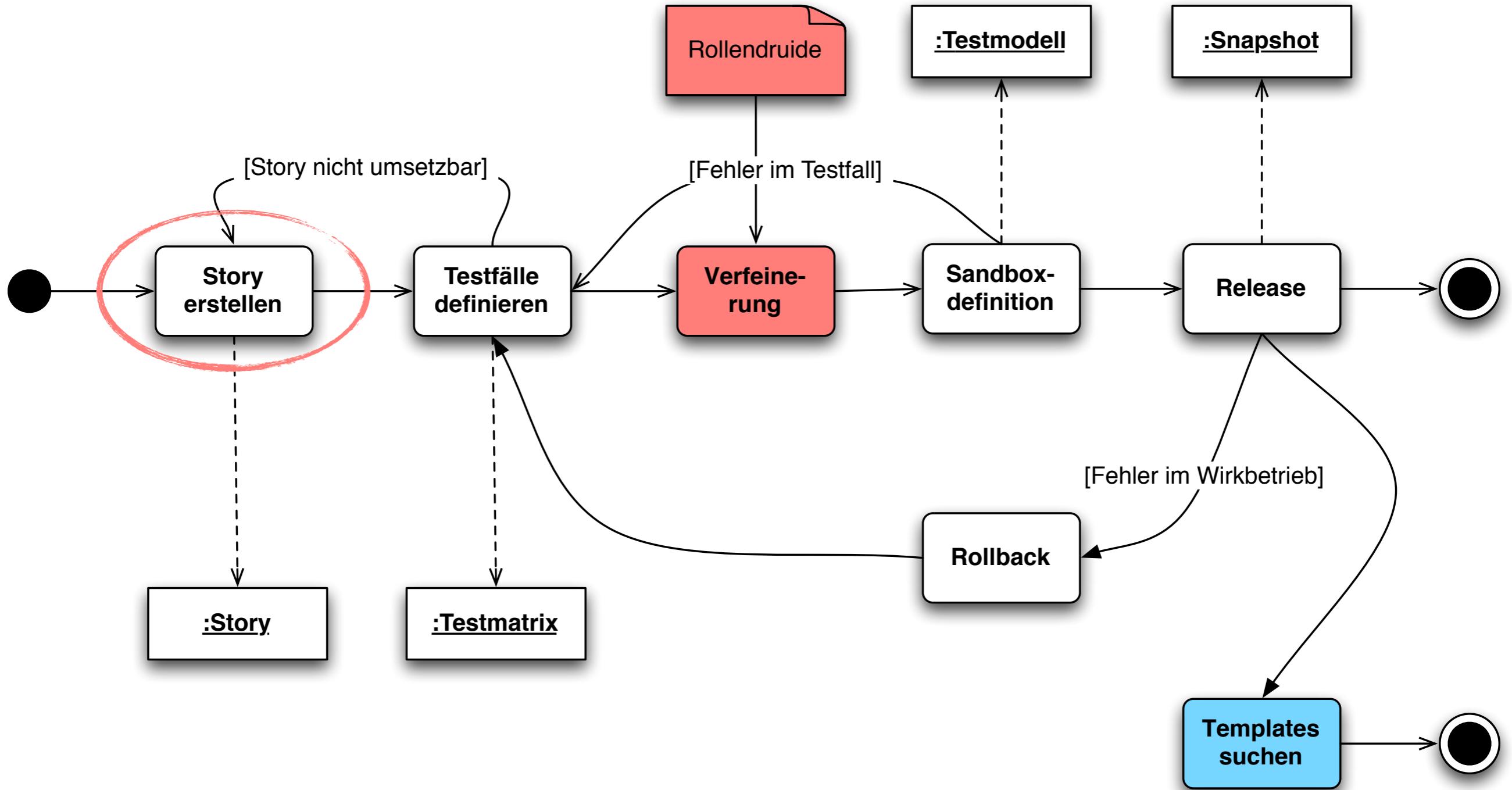
Schulungen, Informationen
Support

Selbst definierte Vertretungen
Backuprollen, zentrale Rollenadmins

Informationen
Anwendungsrollen vordefiniert / Templates

Schulung und Support
Werkzeuge: GUIs, eXtreme Role Engineering

eXtreme Role Engineering



Ähnlichkeit von Rollen

	P_1	P_2	P_3	P_4	C_1	C_2	C_3
read	1	1	1	0	1	1	1
write	1	0	1	0	0	1	0
edit	1	0	0	0	0	1	0
delete	1	0	0	1	0	0	1

$$d(x, y) =_{def} \sum_{i=1}^n |x_i - y_i|$$

x / y	P_1	P_2	P_3	P_4
C_1	3	0	1	2
C_2	1	2	1	4
C_3	2	1	2	1

Normalisierung des Abstands

$$dn(x, y) = \frac{\sum_{i=1}^n |x_1 - y_i|}{n}$$

0.0 ... 0.5 ... 1.0

gleich

unterschiedlich

Python Ablage Bearbeiten Hilfe



xRE - Phase

1: Story erstellen

2: Testfälle definieren

3: Rollenmodell verfeinern

4: Modell testen

5: Modell freigeben

Komplexität

begrüßung() $\{O(1)\}$

modellLaden() $\{O(p)\}$

storyDefinieren() $\{O(1)\}$

testmatrixErstellen() $\{O_{kandidatenErstellen} + O_{vereinigeGleicheKandidaten} = O(2no^2)\}$

verfeinerung() $\{O_{verfeinerung} = O(opn)\}$

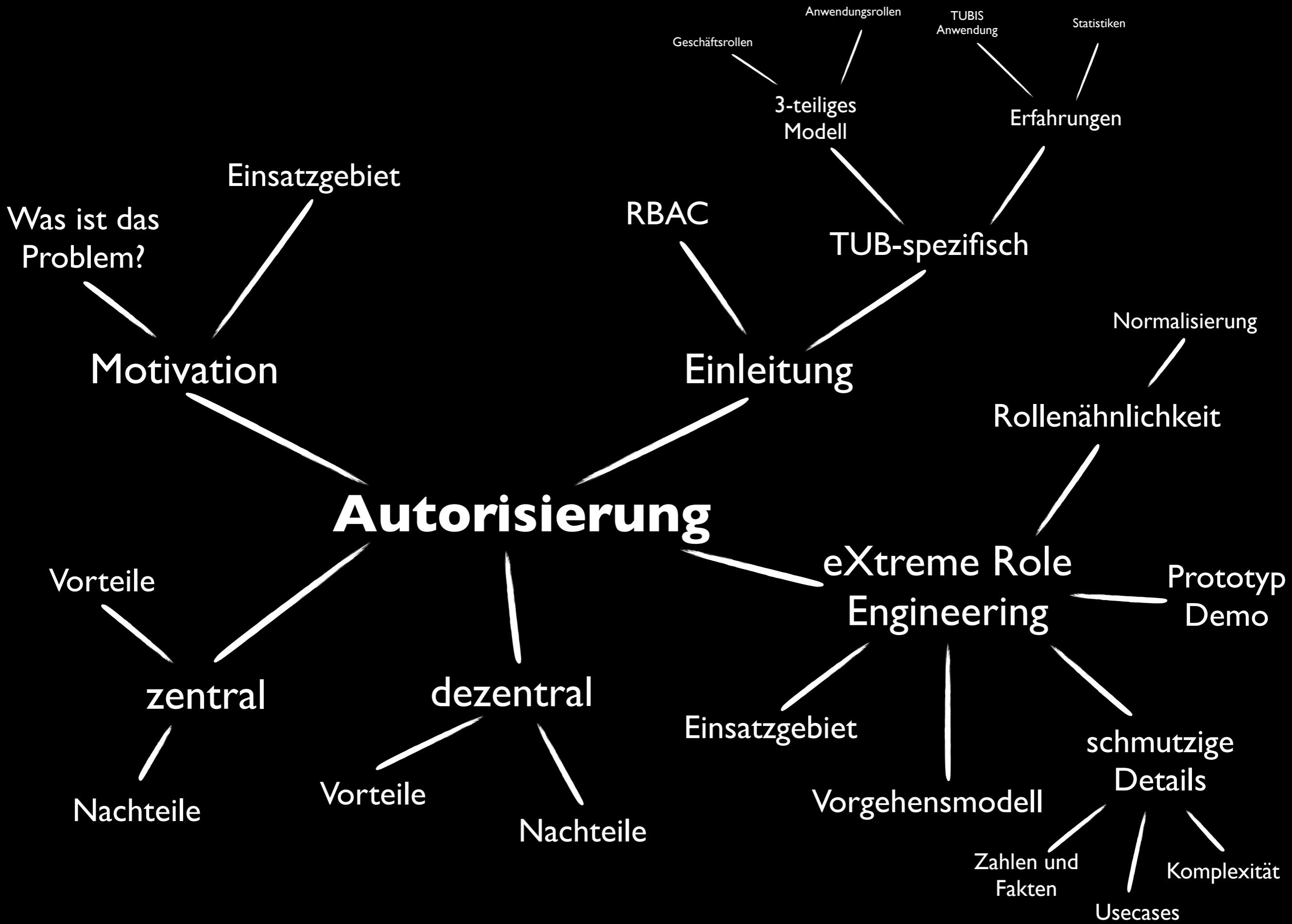
sandboxTest() $\{O(1)\}$

modellSpeichern() $\{O(p)\}$

$$\begin{aligned} O_{xREprozess} &= O(\max(O(no^2), O(opn))) \\ &\Rightarrow O(opn) \text{ für } p \geq o \end{aligned}$$

Erfolgreiche Tests

- xRE: Prototyp, Tests mit „Echtdaten“, eine Testperson, Vergleich mit „Handarbeit“
- xRE ermöglicht „intelligentes“ Hinzufügen von Rollen für „kleine“ Organisationseinheiten



Zusammenfassung

- **Erfahrungen** an der TU Berlin zeigen **Eignung** des **dezentralen** Identitätsmanagements.
- Anfänglich hoher Schulungsaufwand und Kritik.
Inzwischen hohes Maß an **Transparenz**, **Flexibilität** und **Selbstbestimmung**.
- Fehler und Lücken sind auf Werkzeuge zurückzuführen.
Daher **Verbesserung** und Erweiterung von **Methoden** und **Werkzeugen**.
- Nächster entscheidender Schritt: **eXtreme Role Engineering**

Quellen und Kontaktdaten

thomas.hildmann@tu-berlin.de

<http://www.user.tu-berlin.de/hildcatf/>