Role-Engineering

Von Funktionen und Gruppen zu Rollen und Rechten

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

Zu meiner Person

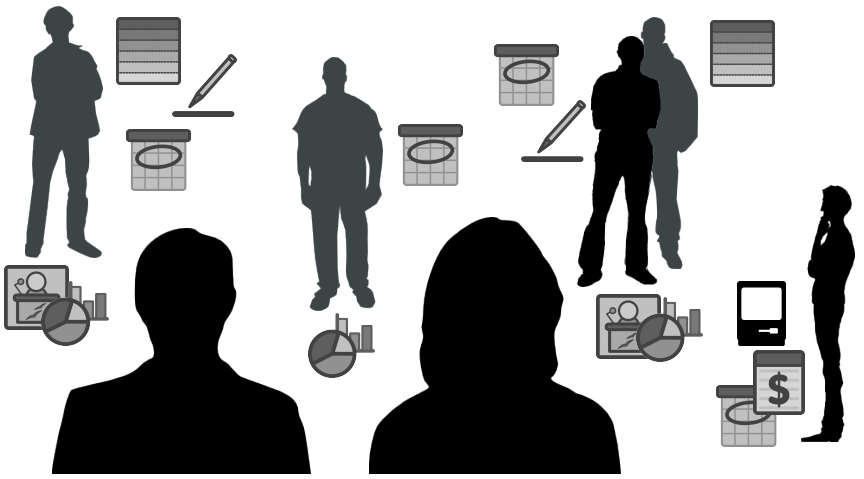
Thomas Hildmann
Technische Universität Berlin
tubIT - IT-Service-Center
Abteilungsleiter: Infrastruktur (Server, Netze)
vormals Abteilung Identity Management

Promotionsthema: Umfassendes Autorisierungsmanagement (RBAC, mehrseitige Sicherheit, Entwicklung des Role Engineeringverfahrens xRE, ...)

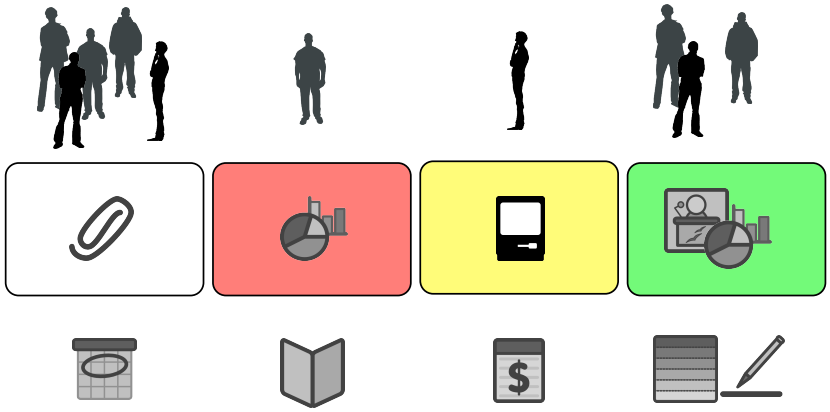
Agenda

- Motivation
- Lösungsansätze
- Role Mining (Bottom-Up)
- Role Engineering (Top-Down)
- Meine Empfehlungen
- Zusammenfassung
- Weiterführende Quellen

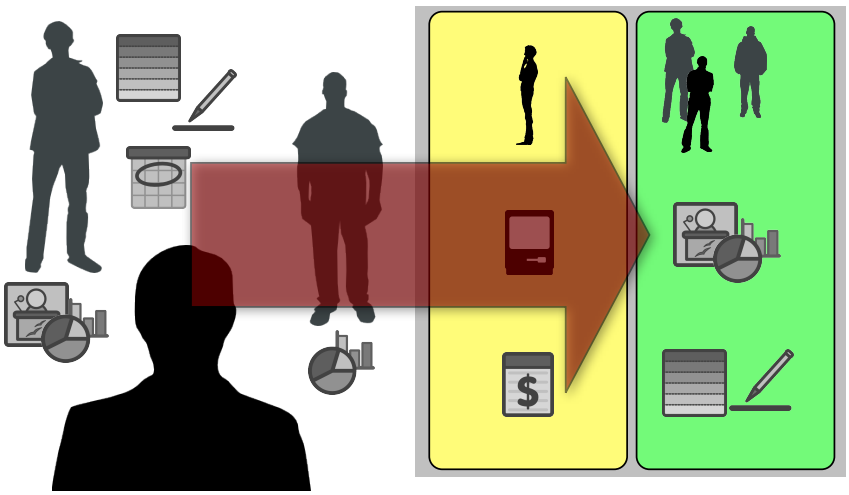
Problemstellung



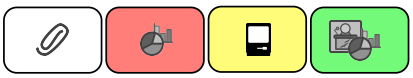
Modellierung über Rollen



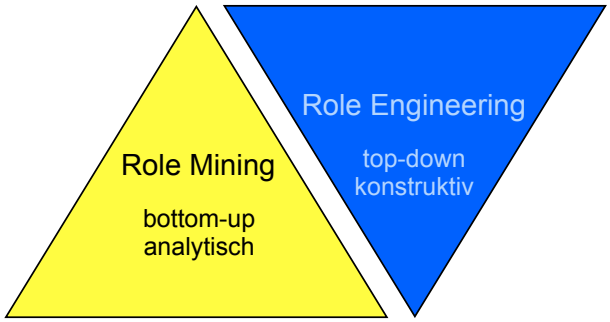
Rollenfindung



Lösungsansätze



Rollen



Personen
und Rechte

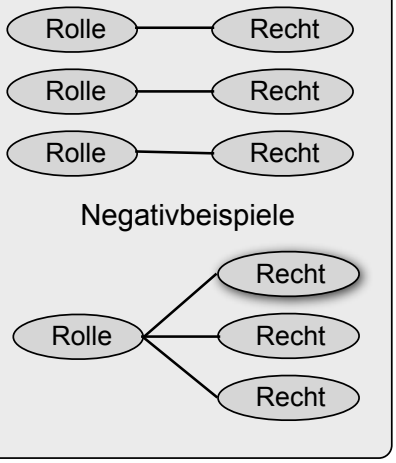
Viele Rechte ≠ wichtiger Mensch
Position ≠ Rolle

Datacenter Berechtigungen

Dr. Thomas Hildmann
Abteilungsleiter

- ☐ xxxx x x xxx
- ☐ xxx xxx xxx
- ☐ xxx xxx xxxxx
- ☐ xxxxxxxxxx
- ☐ xxx xxxxx xx
- ☐ xxxxx xxxxxx
- ☐ xxxx xx xxx
- ☐ xxxx xxx x
- ☐ xxxx
- ☐ xxxxxxx xx
- ☐ xxx xxxxxxx
- ☐ xxxx xxxx

Gute Rollen, schlechte Rollen

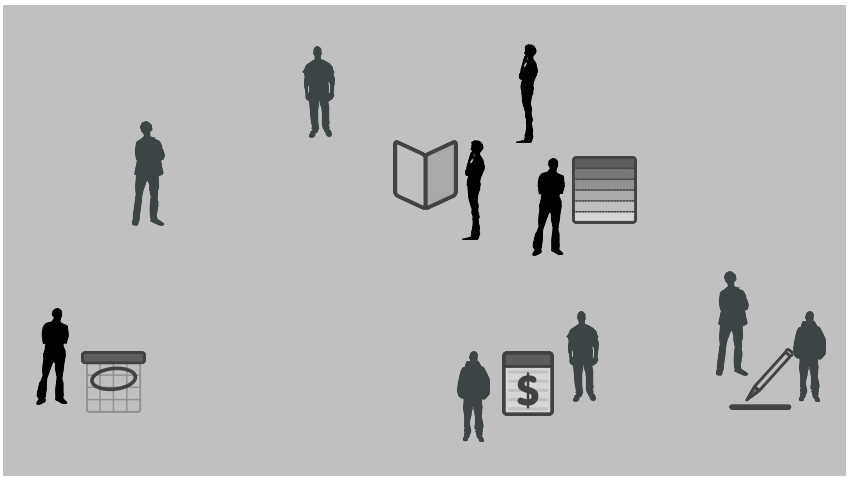


- Gute Rollen sind...
  - leicht zu verstehen
  - setzen Sicherheitspolitik geeignete um
- Gute Rollennamen sind...
  - eindeutig
  - für Rollenzuweiser verständlich
- Rollenhierarchien sind...
  - geeignet, um Abstraktionsniveaus zu modellieren

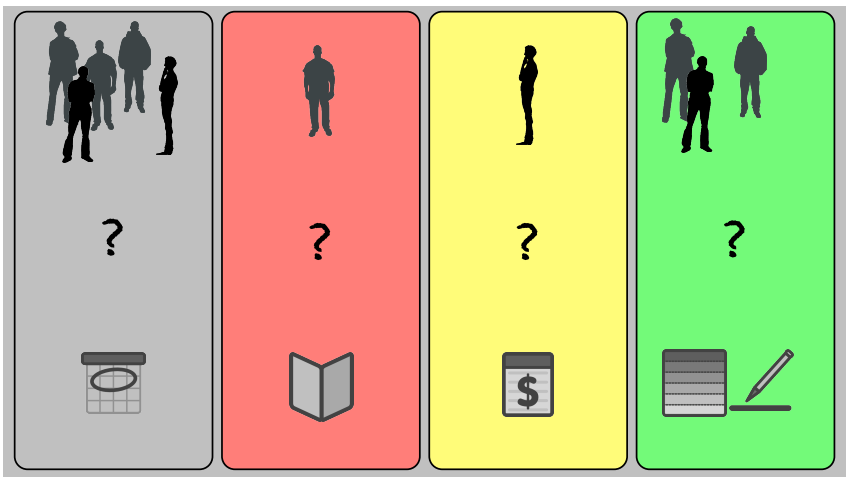
Agenda

- Motivation
- Lösungsansätze
- Role Mining (Bottom-Up)
- Role Engineering (Top-Down)
- Meine Empfehlungen
- Zusammenfassung
- Weiterführende Quellen

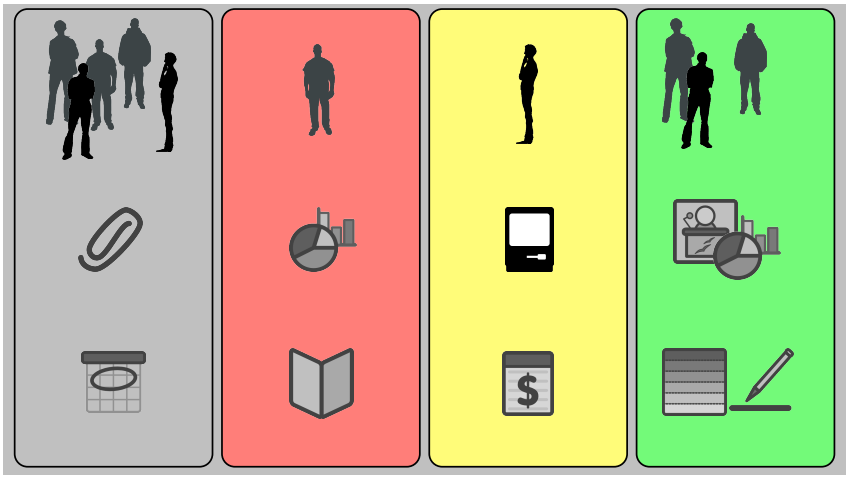
Role-Mining (analytisch)



Role-Mining: Clustering



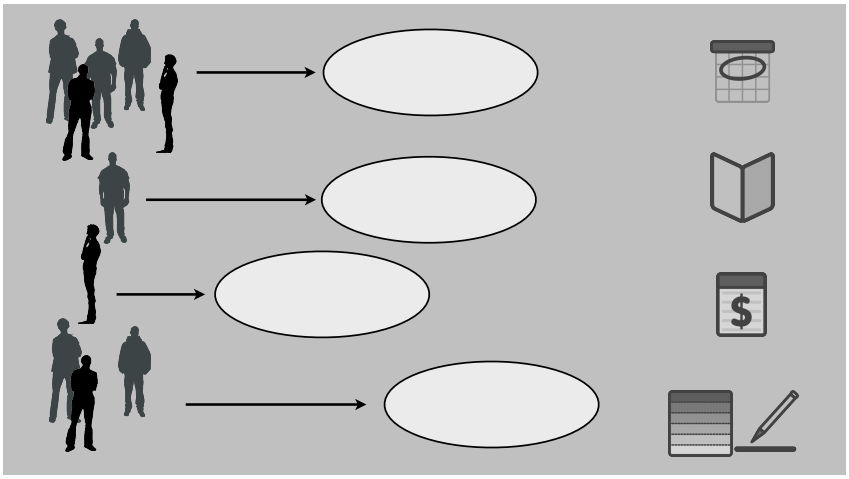
Role-Mining: Clustering



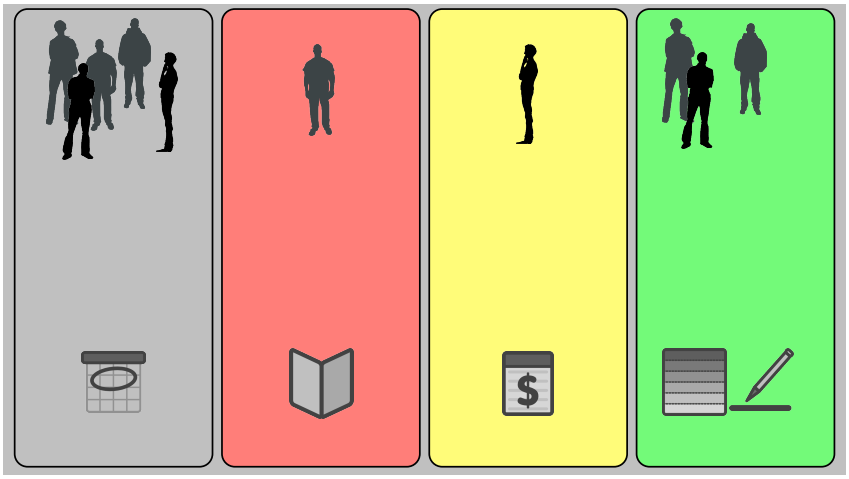
Agenda

- Motivation
- Lösungsansätze
- Role Mining (Bottom-Up)
- Role Engineering (Top-Down)
- Meine Empfehlungen
- Zusammenfassung
- Weiterführende Quellen

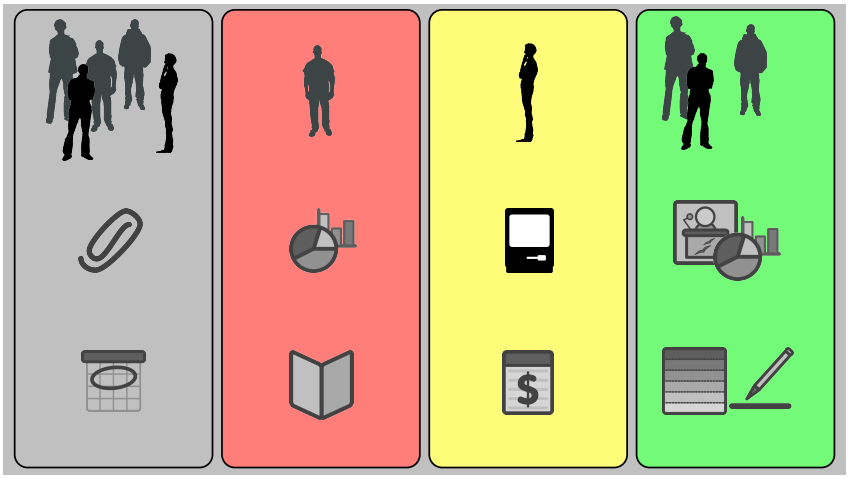
Role Engineering: Anwendungsfälle und Rechte bestimmen



Role Engineering: Zusammenfassen



Role Engineering: Rollen verfeinern

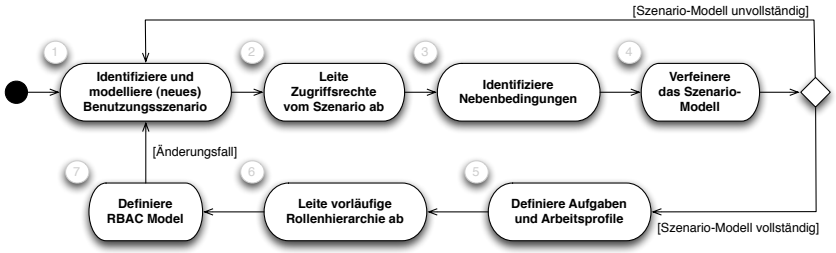


Role-Engineering

1. Erstellen oder Übernehmen von Szenarios aus den Arbeitsprozessen (z.B. Neue Benutzer hinzufügen)
2. Ermitteln der Akteure, Aktionen und Objekte
   Akteure werden Rollen
   Aktionen auf Objekte werden Zugriffsrechte
3. Gemeinsam mit Experten für die Anwendung passende Zugriffsrechte für die Arbeitsprozesse definieren
4. Zugriffsrechte entsprechend der Prozesse zusammenfassen (z.B. Hinzufügen, Ändern, Löschen)
5. Benennung der Prozesse entsprechend der Akteure, die die Zugriffsrechte nutzen werden (z.B. Kontenverwalter)

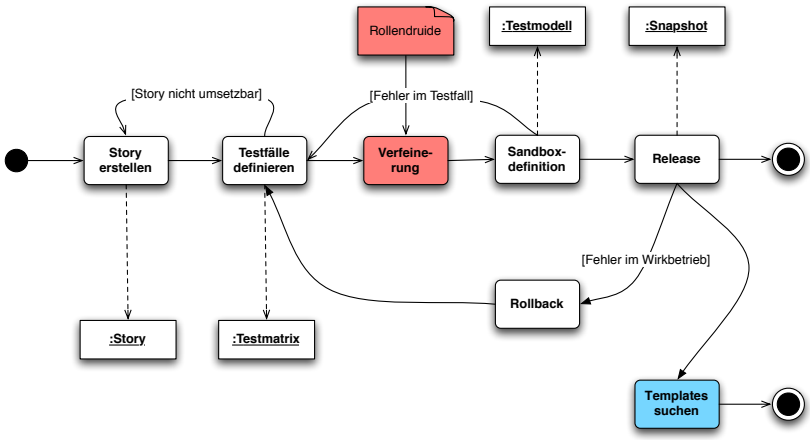
Coyne and Davis: Role Engineering, Artech House, Norwood, MA 2008

Szenario-basiertes RE

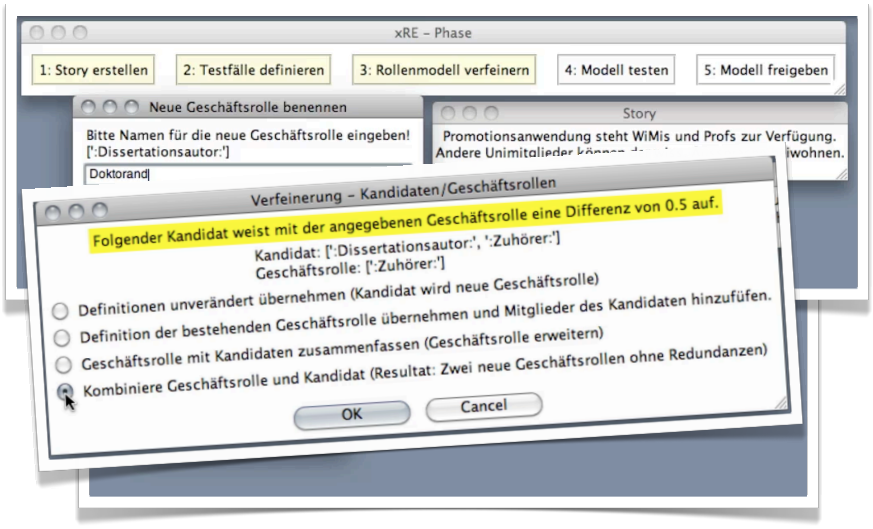


Gustaf Neumann and Mark Strembeck. 2002. A scenario-driven role engineering process for functional RBAC roles. In *Proceedings of the seventh ACM symposium on Access control models and technologies* (SACMAT '02).

eXtreme Role-Engineering



Rollendruide



Agenda

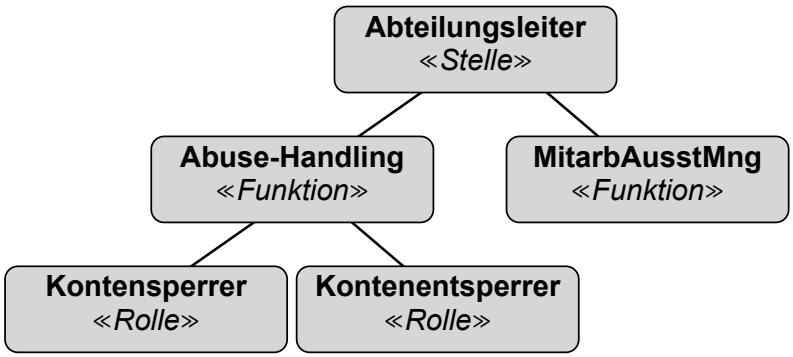
- Motivation
- Lösungsansätze
- Role Mining (Bottom-Up)
- Role Engineering (Top-Down)
- Meine Empfehlungen
- Zusammenfassung
- Weiterführende Quellen

Funktionen ≠ Stellen ≠ Rollen

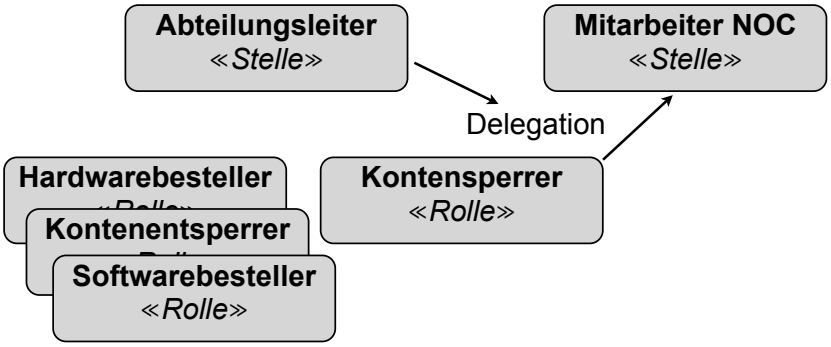
Abteilungsleiter «*Stelle*»	**Abuse-Handling** «*Funktion*»	**Kontensperrer** «*Rolle*»
Professor «*Stelle*»	**Prüfer** «*Funktion*»	**Prüfer** «*Rolle*»
Sysadmin «*Stelle*»	**Sysadmin** «*Funktion*»	**Sysadmin** «*Rolle*»

- Zuordnung erfolgt jeweils über den Anwendungsfall
- Bei sauberem Role Engineering ist Zuordnung klar

Abstraktionsniveaus und Hierarchien



Rollenzuweisung dezentralisieren



Meine Empfehlungen

- Wenn möglich: Start von der Grünen Wiese
  - Eine Anwendung nach der anderen, ein Szenario nach dem anderen
  - Schrittweise Aufbau des Rollenmodells jeweils mit Verfeinerung
  - eXtreme Role Engineering könnte helfen / ist in Arbeit
- Bei Start aus existierendem System: Hybrides Modell
  - Start mit minimaler Zahl an Rechtemodellen und Role Mining
  - den Rest via Szenarios und Role Engineering hinzufügen
  - am besten mit Rollenexperten arbeiten sonst mit Tools
- Klein und einfach halten!
  - Vereinfachung in den Prozessen beginnen.
  - Ausnahmen vermeiden! Intelligenz in Prozessen nicht in Modellen!
- Role Engineering aus der Cloud?
  - Datenschutz und Datensicherheit im Auge behalten!

Die Wahrheit...

- Role Engineering ist ein Engineering-Prozess.
- Das modellierte Rollenmodell ist nur so gut, wie die Prozesse aus denen es hervor ging.
- Es gibt keine Software mit ~~„Do what I want"~~ ~~„Do what I mean"~~ „Do what I should mean"-Knopf.
- Rollenmodelle haben einen Lebenszyklus wie Software.
- Der Lebenszyklus beinhaltet auch das Finden und Beseitigen von Fehlern.
- Refactoring ist auch in Rollenmodellen eine Option

Zusammenfassung

- Ableitung von Rollen aus Funktionen und Rechten ist fast so alt, wie Rollenbasierte Zugriffskontrolle selbst
- Zwei grundsätzlich verschiedene Ansätze:
  1. Role Mining: Bottom-Up (analytisch)
  2. Role Engineering: Top-Down (konstruktiv)
- Als Hilfsmittel stehen zur Verfügung:
  - Literatur
  - Software
  - Experten

Umfassendes Autorisierungsmanagement

thomas.hildmann@tu-berlin.de

http://www.user.tu-berlin.de/hildcatf/promotion.html