OFFIS

OLDENBURGER FORSCHUNGS- UND ENTWICKLUNGSINSTITUT
FÜR INFORMATIK-WERKZEUGE UND -SYSTEME

Berücksichtigung von Berechtigungskonzepten bei der Spezifikation von Fachkomponenten

Holger Jaekel
holger.jaekel@offis.de

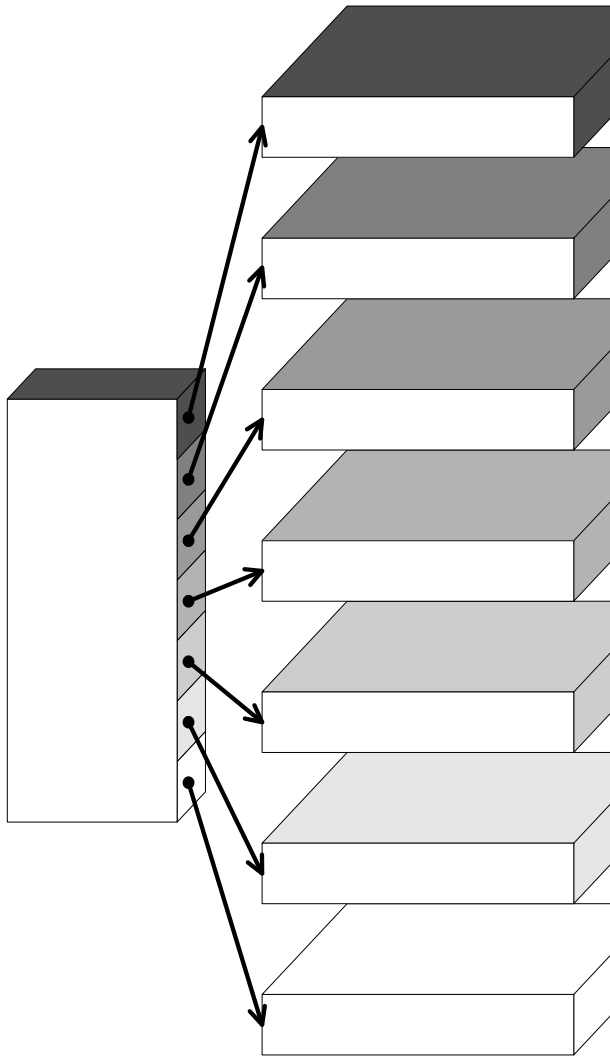
Thorsten Teschke
thorsten.teschke@offis.de

enda

- Motivation: Berechtigungskonzept für Fachkomponenten
- Definition eines Rollenmodells auf der Terminologieebene
- Vergabe von Berechtigungen auf der Aufgabenebene
- Fallstudie: Duke’s Bank Application
- Zusammenfassung

tivation: Berechtigungskonzept für Fachkomponenten

- Fachkomponente
  - Kapselt betriebliche Anwendungslogik
  - Wiederverwendung erfordert Spezifikation
  - Vorschlag: Spezifikation auf sieben Beschreibungsebenen
- Bislang nicht berücksichtigt: Berechtigungskonzepte
  - Definition von Benutzerrollen
  - Zuordnung von Rollen zu Diensten



Beschreibungsebenen nach [ABC+02]

ezifikaton von Sicherheit bei Enterprise JavaBeans

- EJB Deployment Descriptor
  - Definition von *Security Roles*
  - Festlegung von Rechten zur Ausführung von Methoden für eine Rolle
- Deployment
  - Abbildung von Rollen auf Identitäten der Ablaufumgebung
- Einsatz
  - EJB-Container überwacht Zugriff auf Methoden

```
...
<assembly-descriptor>
  <security-role>
    <role-name>BankCustomer</role-name>
  </security-role>
  <security-role>
    <role-name>BankAdmin</role-name>
  </security-role>
  ...
  <method-permission>
    <role-name>BankCustomer</role-name>
    <method>
      <ejb-name>TxControllerEJB</ejb-nam
      <method-intf>Remote</method-intf>
      <method-name>withdraw</method-name
      <method-params>
         ...
      </method-params>
    </method>
  </method-permission>
  ...
</assembly-descriptor>
...
```

grenzung Terminologieebene/Aufgabenebene

- Terminologieebene
  - Lexikon aller Begriffe: Kurzdefinition, Langdefinition, Einsatzbeispiele
  - Prädikatorenregeln z.B. für abstraktive/kompositive Beziehungen: $x \in$ Bilanz $\Rightarrow x \in$ Jahresabschluss
  - Konzeptuelle Beziehungen als UML-Klassendiagramm
- Aufgabenebene
  - Unterstützte betriebliche Aufgaben beschrieben durch rekonstruierte Fachsprache
  - Auch hier Spezifikation von abstraktiven/kompositiven Beziehungen

- Vorschlag:
  - Abstraktive/Kompositive Beziehungen ausschließlich auf der Terminologieebene spezifizieren

    (Kompositive Beziehungen im Folgenden nicht weiter betrachtet)

llenmodell auf der Terminologieebene

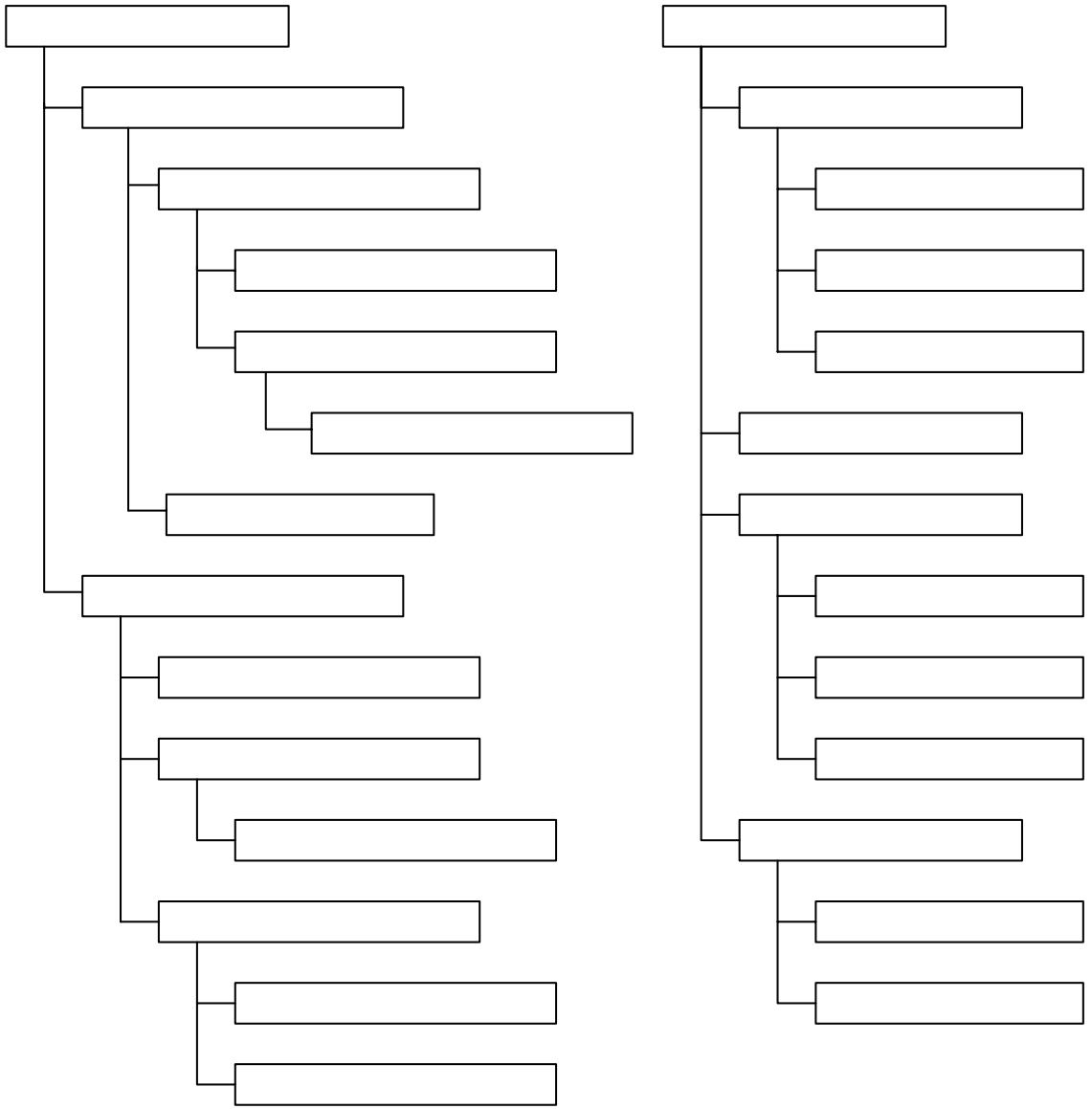
- Satzbauplan für Spezifikation von abstraktiven Beziehungen zwischen Begriffen:

$$[\ N_1 \mid \sqsubset \mid N_2\ ]$$

- Spezifikation des Rollenmodells über abstraktive Beziehungen:

$$\begin{aligned} \text{Buchhalter} &\sqsubset \text{Büroangestellter} \\ \text{Sachbearbeiter} &\sqsubset \text{Büroangestellter} \\ \text{Bilanzbuchhalter} &\sqsubset \text{Buchhalter} \end{aligned}$$

p: Taxonomie mit Definition von Rollen



grenzung Aufgabenebene/Schnittstellenebene

- Schnittstellenebene
  - Angebotene Dienste der Fachkomponente mit IDL
  - Korrespondierende Aufgaben und Dienste in Tabelle
- Aufgabenebene
  - Unterstützte betriebliche Aufgaben beschrieben mit rekonstruierter Fachsprache

- Vorschlag
  - Angebotene Dienste auf der Schnittstellenebene spezifizieren (IDL)
  - Korrespondierende Dienste und Aufgaben auf der Aufgabenebene spezifizieren
  - Aufgaben beschrieben mit rekonstruierter Fachsprache

rgabe von Berechtigungen auf der Aufgabenebene

- Satzbauplan zur Beschreibung der durch einen Dienst unterstützten betrieblichen Aufgabe:

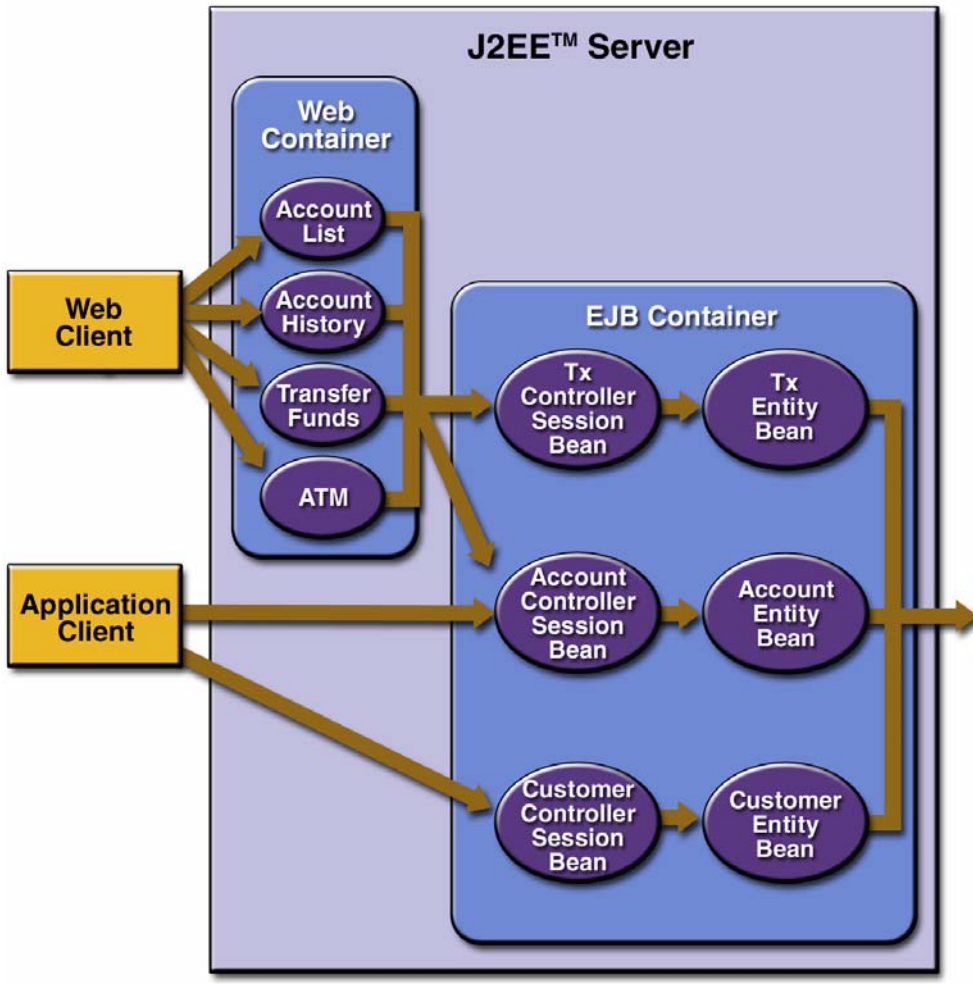
$$[\ N\ |\ \pi\ |\ P\ |\ O_1\ |\ O_2\ |\ \ldots\ ]$$

- Inhaltliche Belegung des Nominators
  - Angabe über Berechtigung, den Dienst zu nutzen
  - Auf der Terminologieebene definierter Rollenbezeicher
  - Spezifikation der minimal erforderlichen Berechtigungsstufe (generellste berechtigte Rolle)

```
[Ein] Buchhalter tut buchen [einen] Zahlungseingang.
[Ein] Bilanzbuchhalter tut erstellen [eine] Bilanz.
```

Istudie: The Duke's Bank Application

- Beispielanwendung zum J2EE Tutorial
  - drei Entity Beans
  - drei Session Beans
  - einige Servlets
- Security Roles:
  - BankCustomer
  - BankAdmin



Architekturübersicht nach [BGH+02]

lstudie: Schnittstellenebene

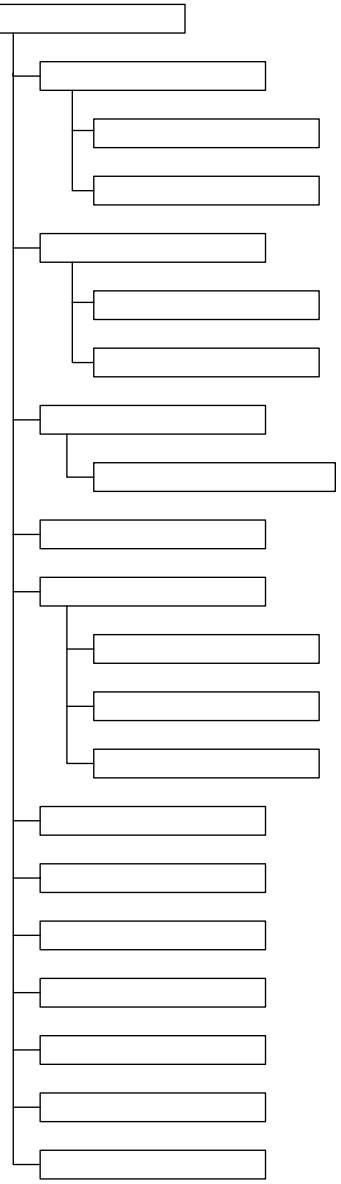
- Module
  - Ein IDL-Modul für jede Session- und Entity-Bean + ein Modul „Extern“
  - In jedem Modul jeweils ein Interface für Home- und Component-Interface der Beans
- Korrespondierende Dienste und Aufgaben jetzt auf der Aufgabenebene

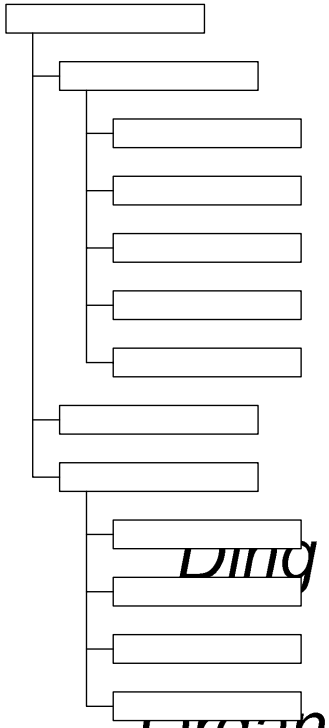
```
module AccountControllerBean {

 interface AccountControllerHome {
  AccountController create()
   raises (CreateException);
 }

 interface AccountController {
  string createAccount(...)
   raises (...);
  void remove(in string accountId)
   raises (...);
  void addCustomerToAccount(in str
   customerId, in string accountID
   raises (...);
 }
}
```

lstudie: Terminologieebene





Ding

Organisationseinheit

Bankadministrator

KONTO

Kurzdefinition: KONTO =$_{DF}$ die von einer Bank geführte Rechnung über den Zahlungsverkehr ihres Kunden.

Langdefinition: KONTO =$_{DF}$ Ein KONTO ist die laufende Abrechnung, in der alle Zahlungsvorgänge und daraus resultierenden Forderungen und Verbindlichkeiten aus der Geschäftsverbindung zwischen Kreditinstitut und Kunden registriert werden.

Einsatzbeispiele: SPARKONTO, GIROKONTO, TERMINKONTO, DEPOTKONTO, WÄHRUNGSKONTO

GIROKONTO

Kurzdefinition: GIROKONTO =$_{DF}$ ...

Kunde

lstudie: Aufgabenebene

ten-)Typ	(Fach-)Begriff
stomer	Kunde
count	Konto
	Buchung
nkCustomer	Kunde
nkAdmin	Bankadministrator

nst	Aufgabe
ring createAccount(...) raises (...);	Bankadministrator tut erzeugen Konto.
id removeAccount(in string accountID) raises (...);	Bankadministrator tut löschen Konto.
id addCustomerToAccount(in string customerID, in string countID) raises (...);	Bankadministrator tut hinzufügen Kunde mi Konto.
countDetails getDetails(string accountID) raises (...);	Organisationseinheit t ermitteln Kontodaten mit Konto.

sammenfassung

- Spezifikation von Berechtigungskonzepten
  - Integration in bisherige Beschreibungsebenen
  - Spezifikation von Rollen auf Terminologieebene
  - Normsprachlicher Ansatz für Spezifikation von Berechtigungen auf der Aufgabenebene

- Zuordnung von zu spezifizierenden Sachverhalten zu Beschreibungsebenen
  - Abstraktive/Kompositive Beziehungen ausschließlich auf der Terminologieebene spezifizieren
  - Korrespondierende Datentypen/Fachbegriffe und Dienste/Aufgaben auf der Aufgabenebene spezifizieren