Eine flexible Sicherheitsarchitektur für das EJB Framework

Frank Kohmann, TPS-Labs
Michael Weber, Universität Ulm
Achim Botz , TPS-Labs

(frank.kohmann@tps-labs.com)

Überblick

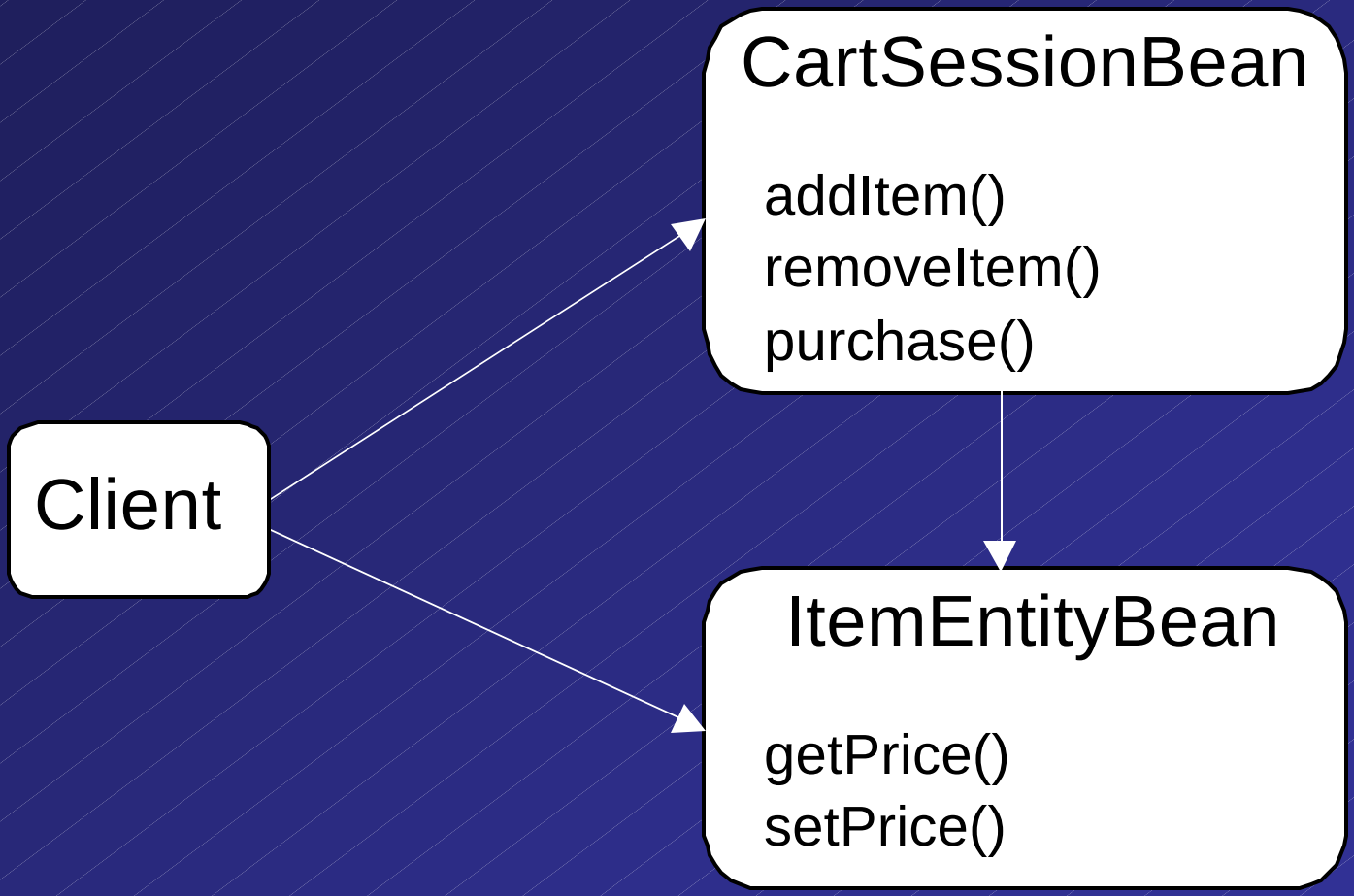
- EJB Security Management
- Neue Architektur
- DeploymentDescriptor
- Funktionalitäten
- Zusammenfassung

EJB Security Management

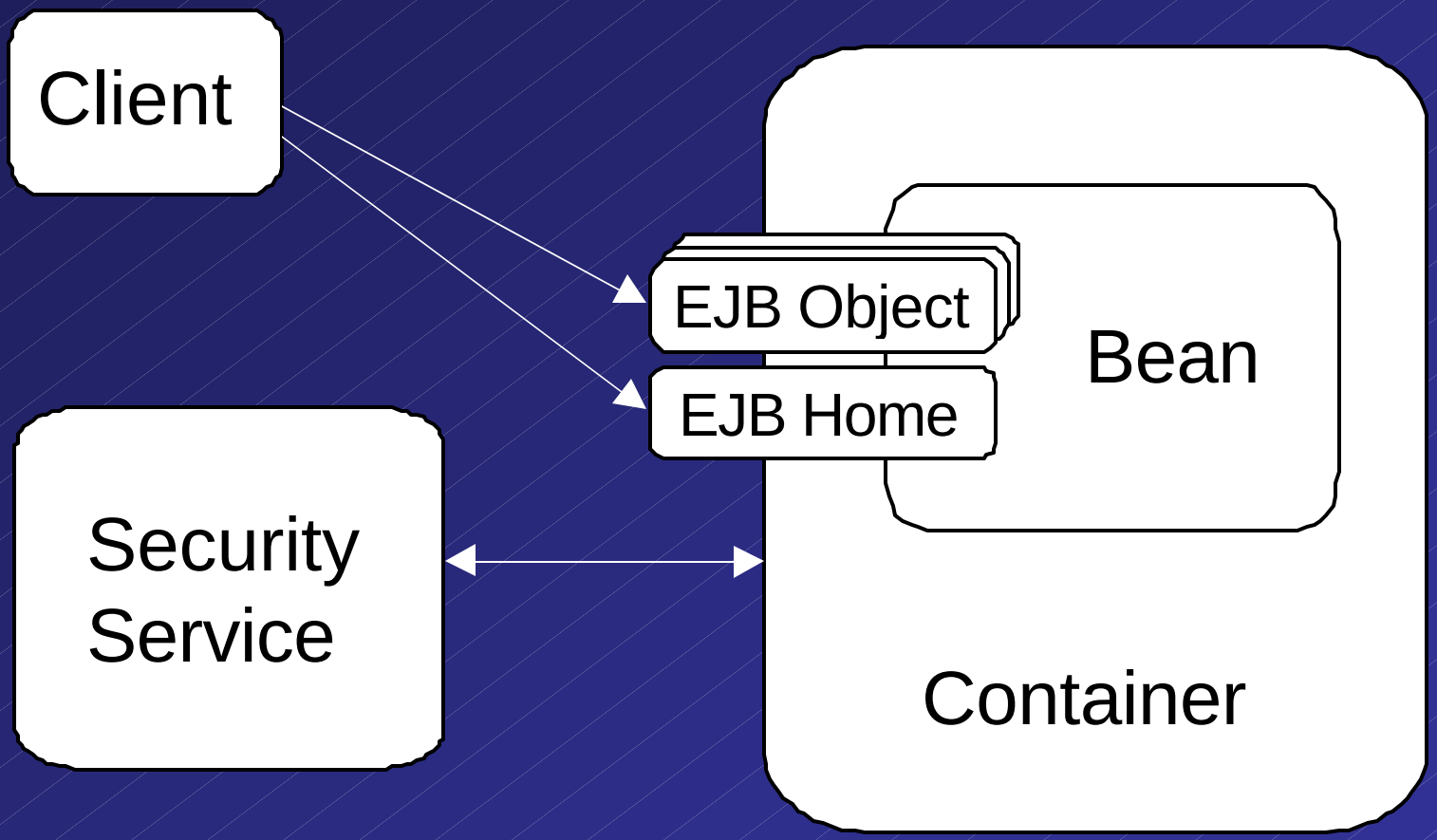
- EJB:
  - server-seitiges Komponenten Modell
  - Server, Container, Beans

- Unzulänglichkeiten der Spezifikation
  - keine server-unabhängige Authentifizierung
  - keine Autorisierung in Abhängigkeit von Bean Instanzen
  - kein gutes Konzept in Bezug auf Delegation

Beispiel


CartSessionBean
addItem()
removeItem()
purchase()
Client
ItemEntityBean
getPrice()
setPrice()

Die neue Architektur

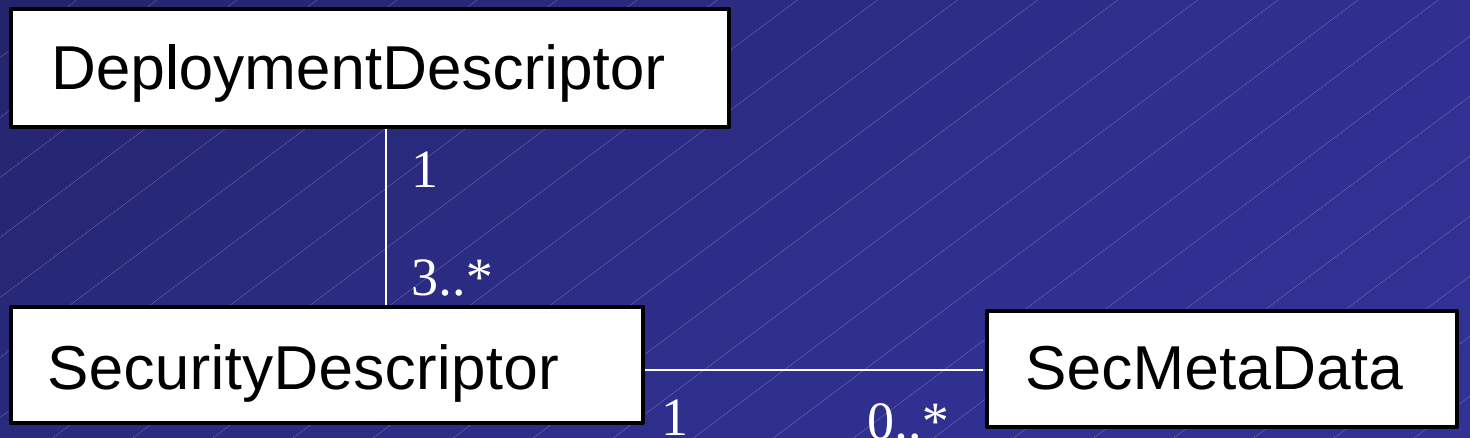


Die neue Architektur

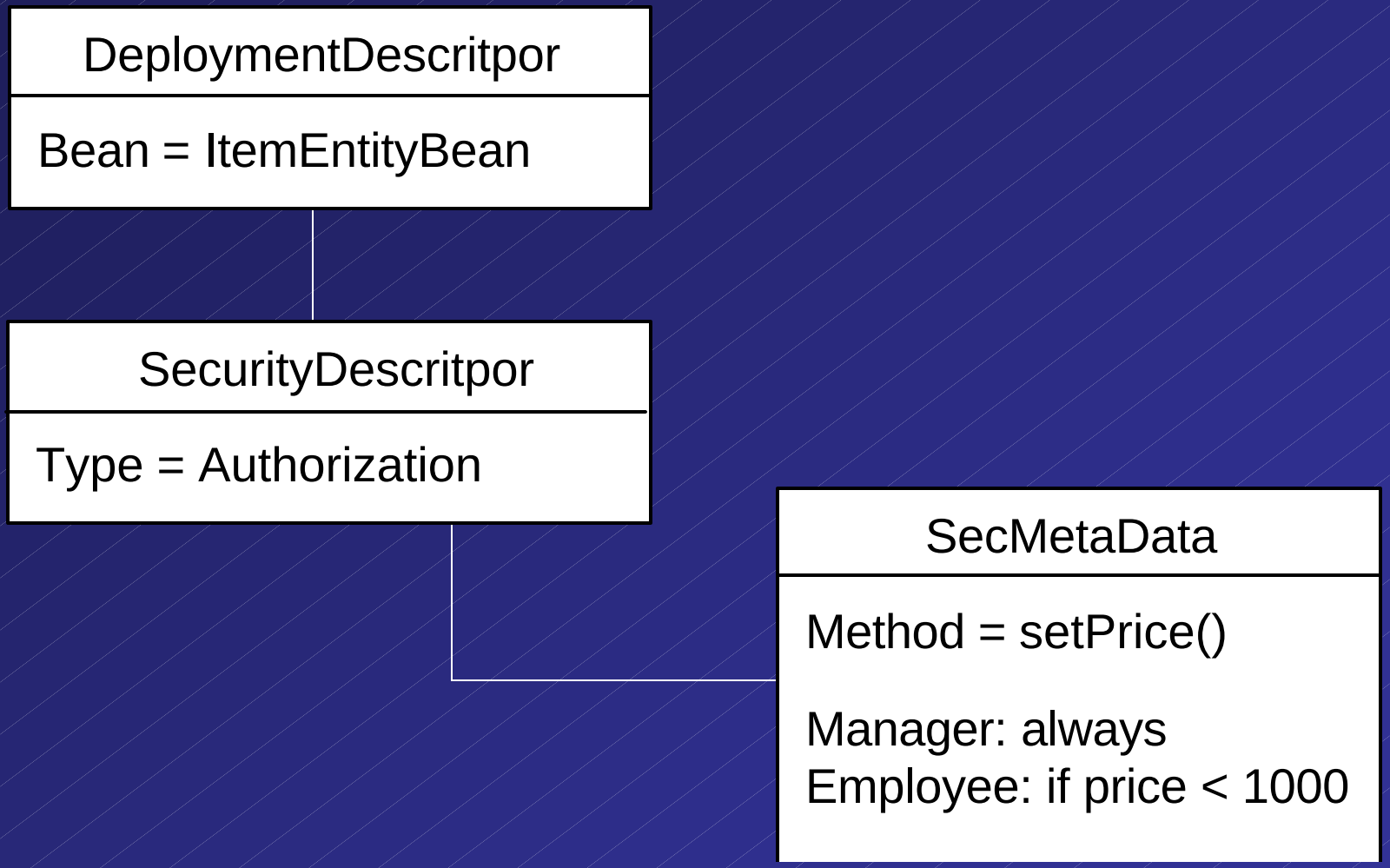
- Einführung eines Domänenkonzeptes
  - Autorisierung
  - Authentifizierung
  - Delegation
  - Domänen verhalten sich gemäß ihrer Policy
  - Zugehörigkeit der Beans zu Domänen

DeploymentDescriptor

- SecurityDescriptor
  - Zugehörigkeit der Bean zu Domänen
  - pro Domäne ein SecurityDescriptor
- SecMetaData:
  - Domänenspezifische Information pro Methode



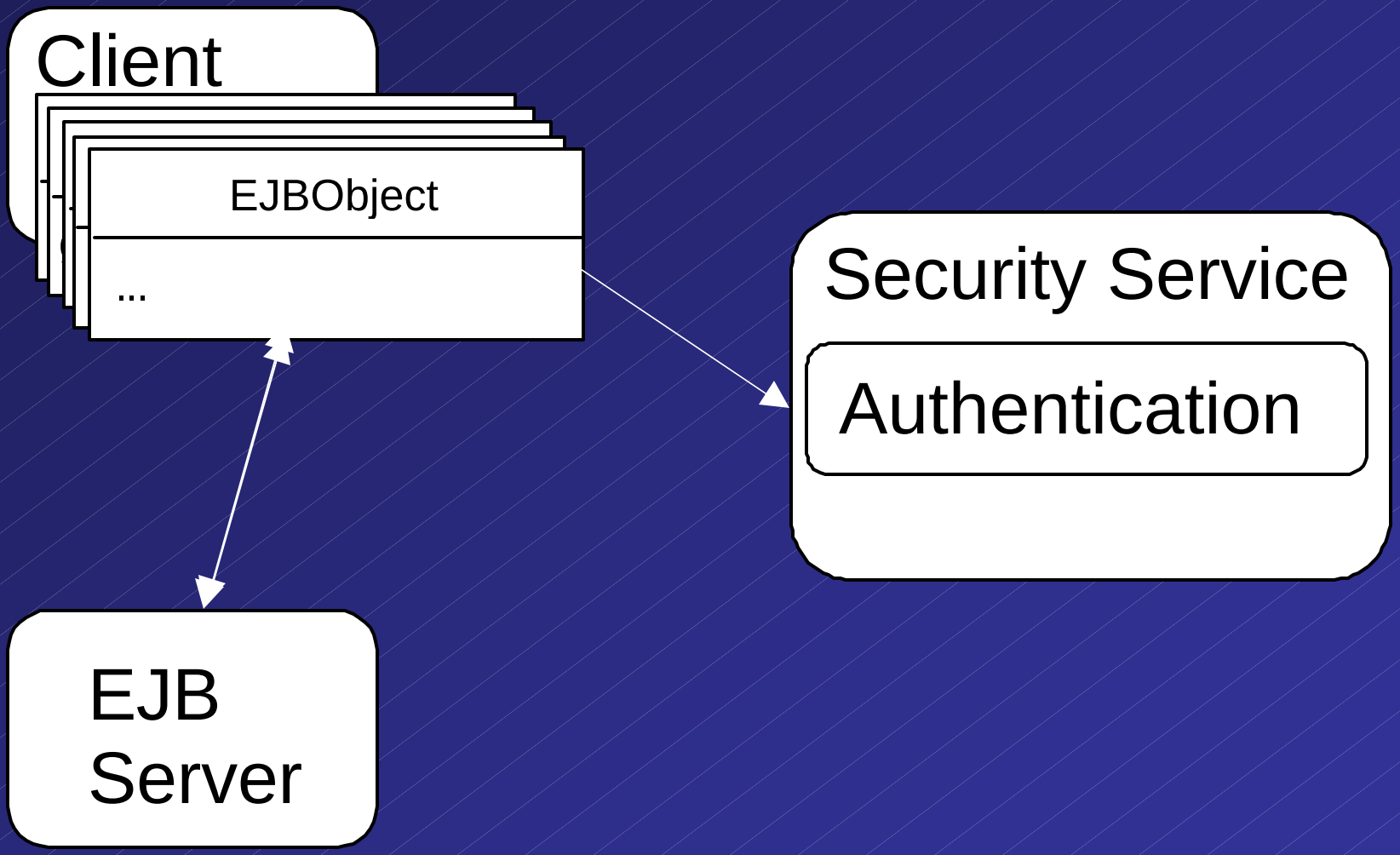
DeploymentDescriptor



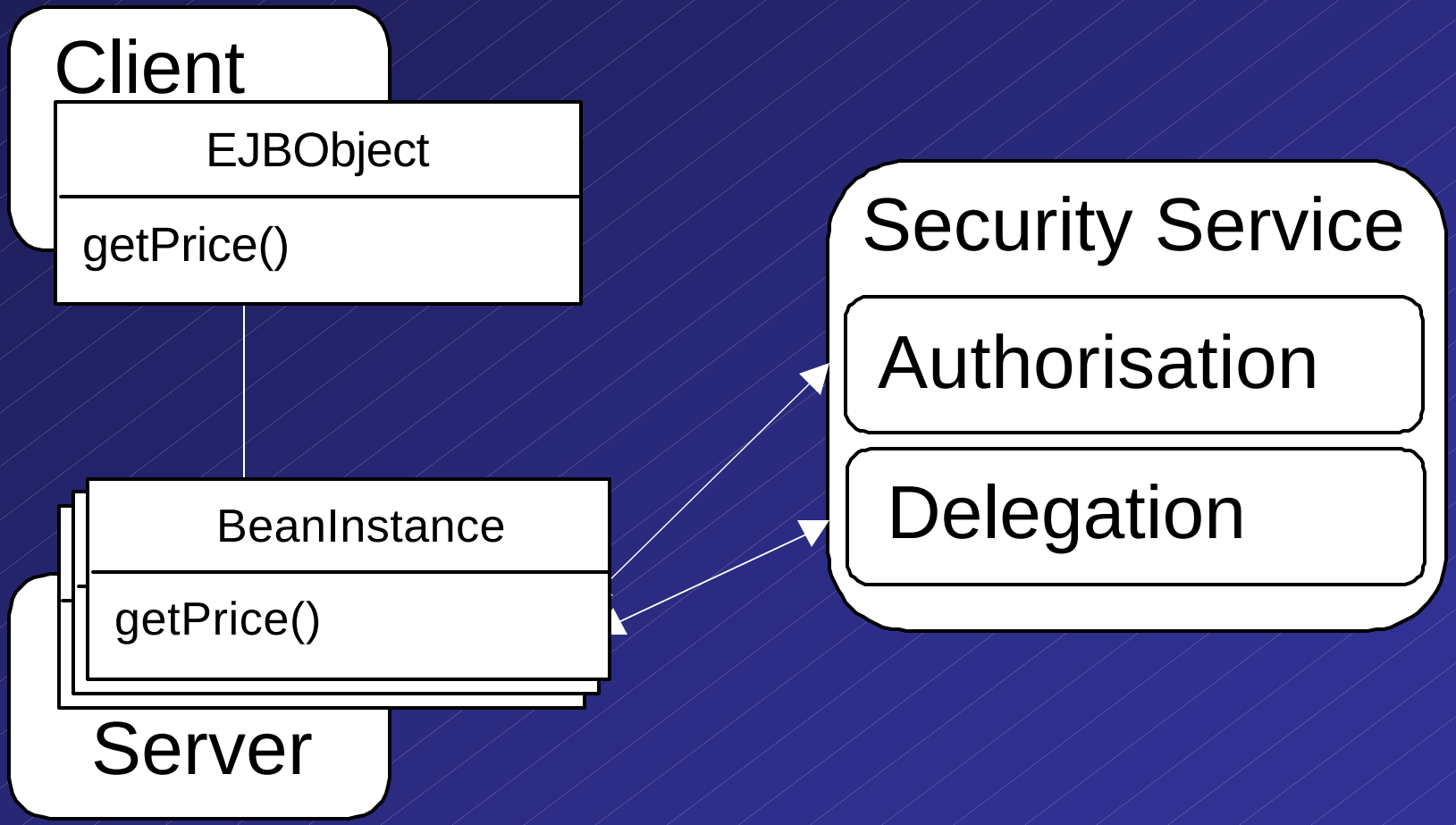
Authentifizierung

- Zuordnung sicherheits-relevanter Attribute durch die Erzeugung eines Credential
- Beans
  - automatisch durch Container
- Client
  - auf 5 verschiedenen Ebenen:
    - Runtime, ThreadGroup, Thread
    - EJBHome, EJBObject

Authentifizierung



Autorisierung / Delegation



Zusammenfassung

- Security Service (unabhängig vom Container)
- neue Pflichtenverteilung zwischen Container und Security Service
- Einführung eines Domänen Konzeptes

→ flexible Autorisierung (auch auf Instanzebene)

→ Delegation wird möglich

→ server-unabhängige Authentifizierung

Aber: Änderung der Spezifikation nötig