Werkzeugunterstützung für sichere Software:

Das CARiSMA Tool

Inhaltsverzeichnis

Motivation

- Modellierung der zu entwickelnden Software:
  - Anforderungen (Anwendungsfalldiagramm)
  - Arbeitsabläufe (Aktivitätsdiagramm)
  - Struktur (Verteilungsdiagramm)

- Unified Modeling Language (UML)
- Business Process Model and Notation (BPMN)

→ Analyse bereits während der Modellierungsphase

→ Analyse durch Werkzeuge

Inhaltsverzeichnis

UMLsec

- Nutzt die Erweiterungsmechanismen der UML
- Modifikation von UML Modellen
- Stereotypes, tagged values, tags

→ Zuweisung von Sicherheitsanforderungen

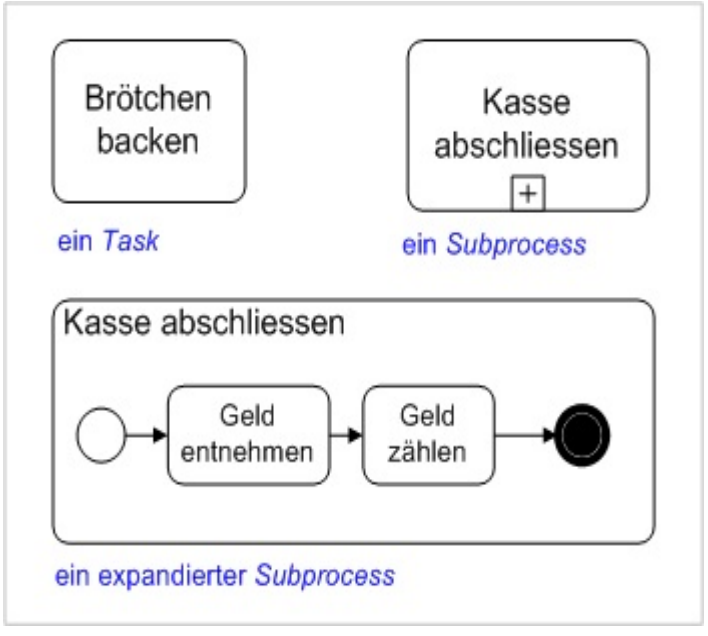
- Spezifikation von Modellen
- Nicht eigenständig zur Modellierung geeignet
- Verknüpfen der Modelle an Bedingungen
  - Body Definition
  - Definition von Operationen und Attributen, die nicht im Modell enthalten sind.
  - Guards
  - Initial and derived values
  - Invariants
  - Pre/Post-Conditions

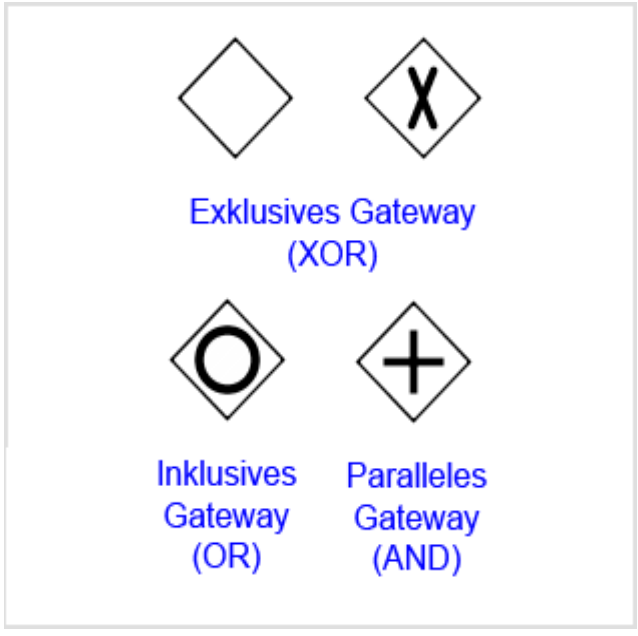
→ Direkter Einfluss auf den zu generierenden Code

BPMN

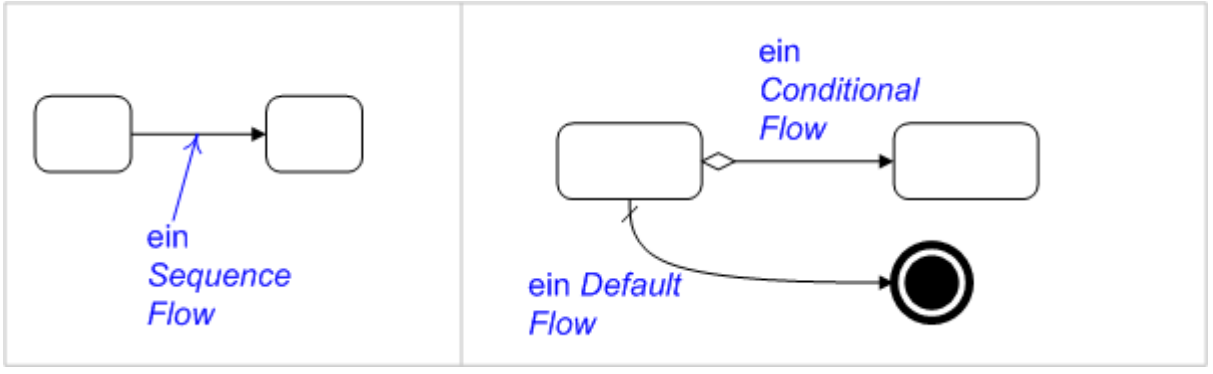
- Modellierungssprache zur Spezifikation von Geschäftsprozessen
- Prozess ist eine Abfolge von Aktivitäten
- Ein Modell besteht aus verschiedenen Basiselementen:
  - Flow Objects: Activities, Gateways und Events
  - Connecting Objects: Sequence Flows, Message Flows
  - Swimlanes, Lanes, Pools
  - Artifacts

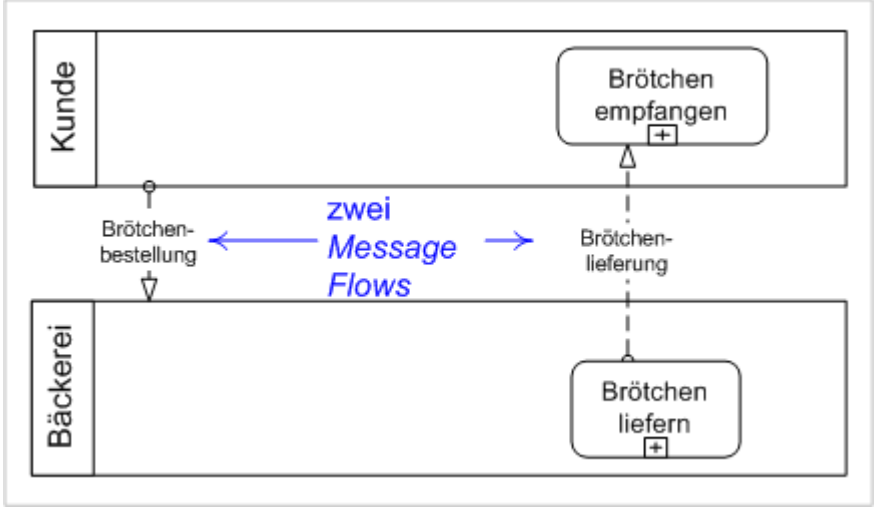
BPMN: Flow Objects



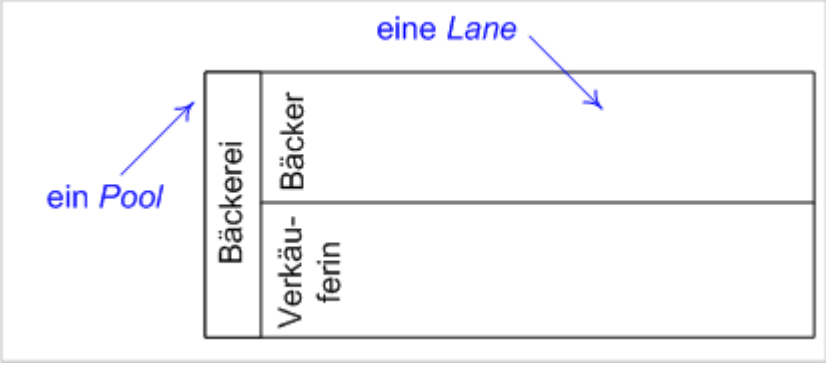


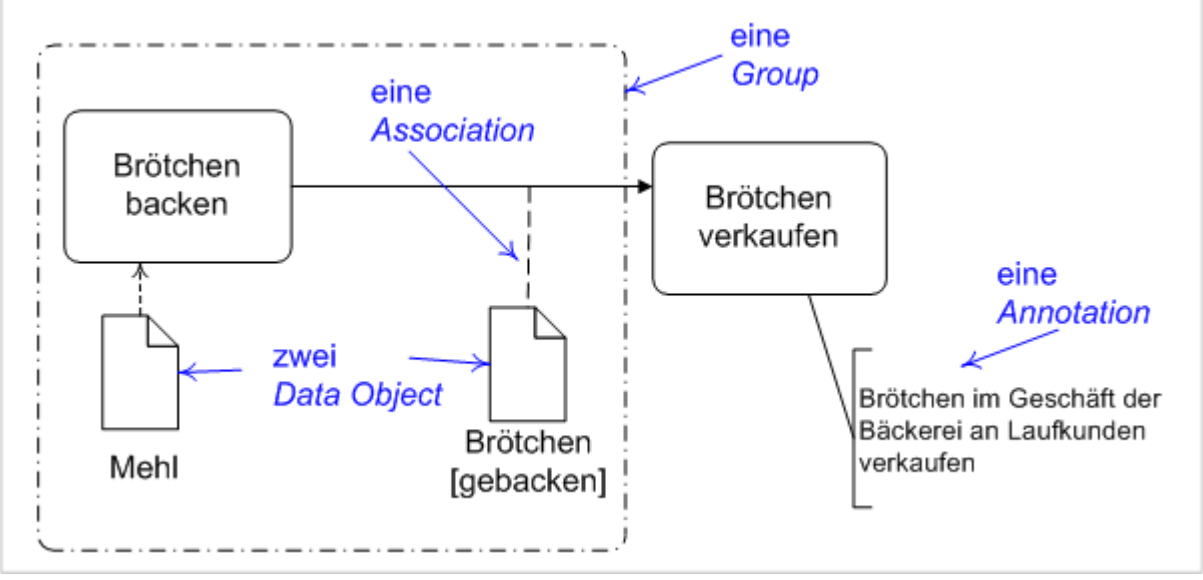
BPMN: Connecting Objects





BPMN: Swimlanes, Artifacts





Inhaltsverzeichnis

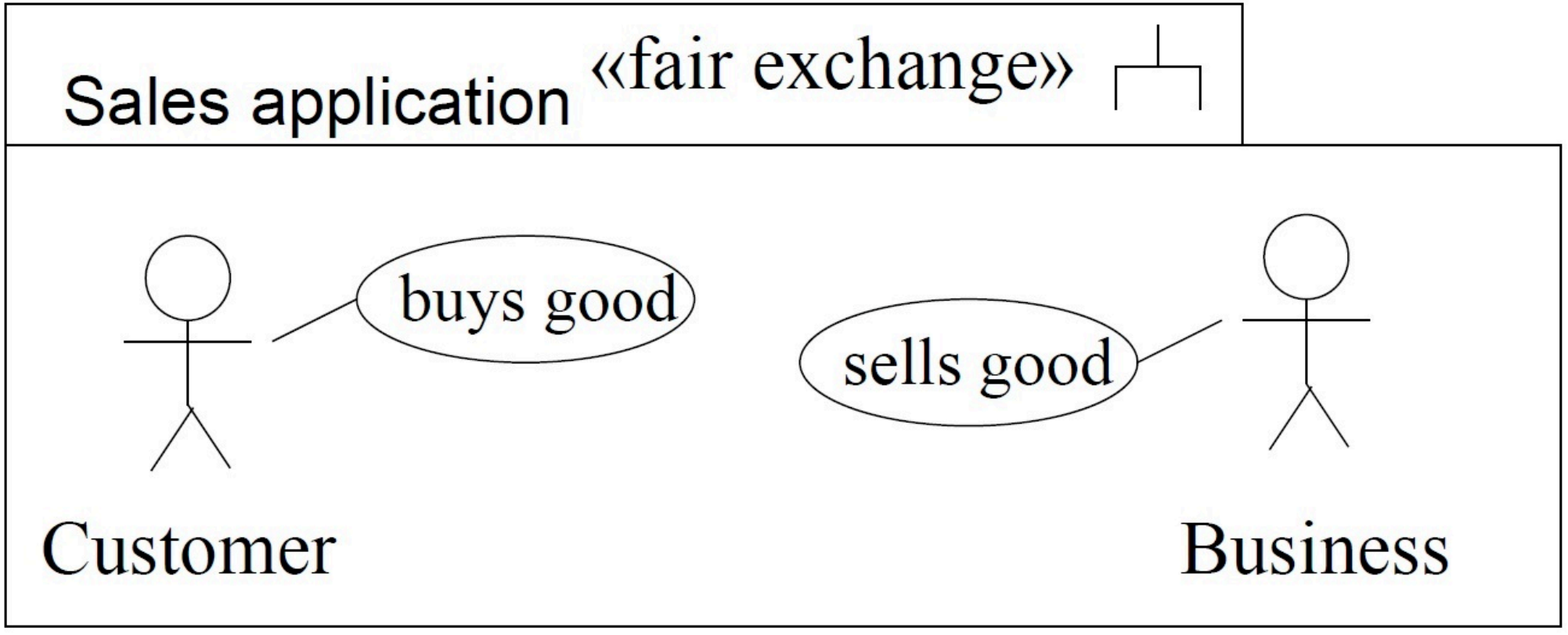
CARiSMA

- Nachfolger des UMLsec-Tool
- Analyse von Modellen auf Einhaltung von Sicherheitsanforderungen
- Baut auf das Eclipse Modeling Framework auf
- Ursprünglich für UML-Modelle konzipiert, jedoch erweiterbar aufgrund der Pluginverwaltung

CARiSMA: Security Checks

- Mehrere Checks bereits als Plugin verfügbar
- Werden in CARiSMA geladen und auf das Modell angewendet
- Static Check auf UML2 Modellen:
  - Fair Exchange
  - Secure Dependency
  - Secure Links
- OCL Check auf BPMN2 Modellen

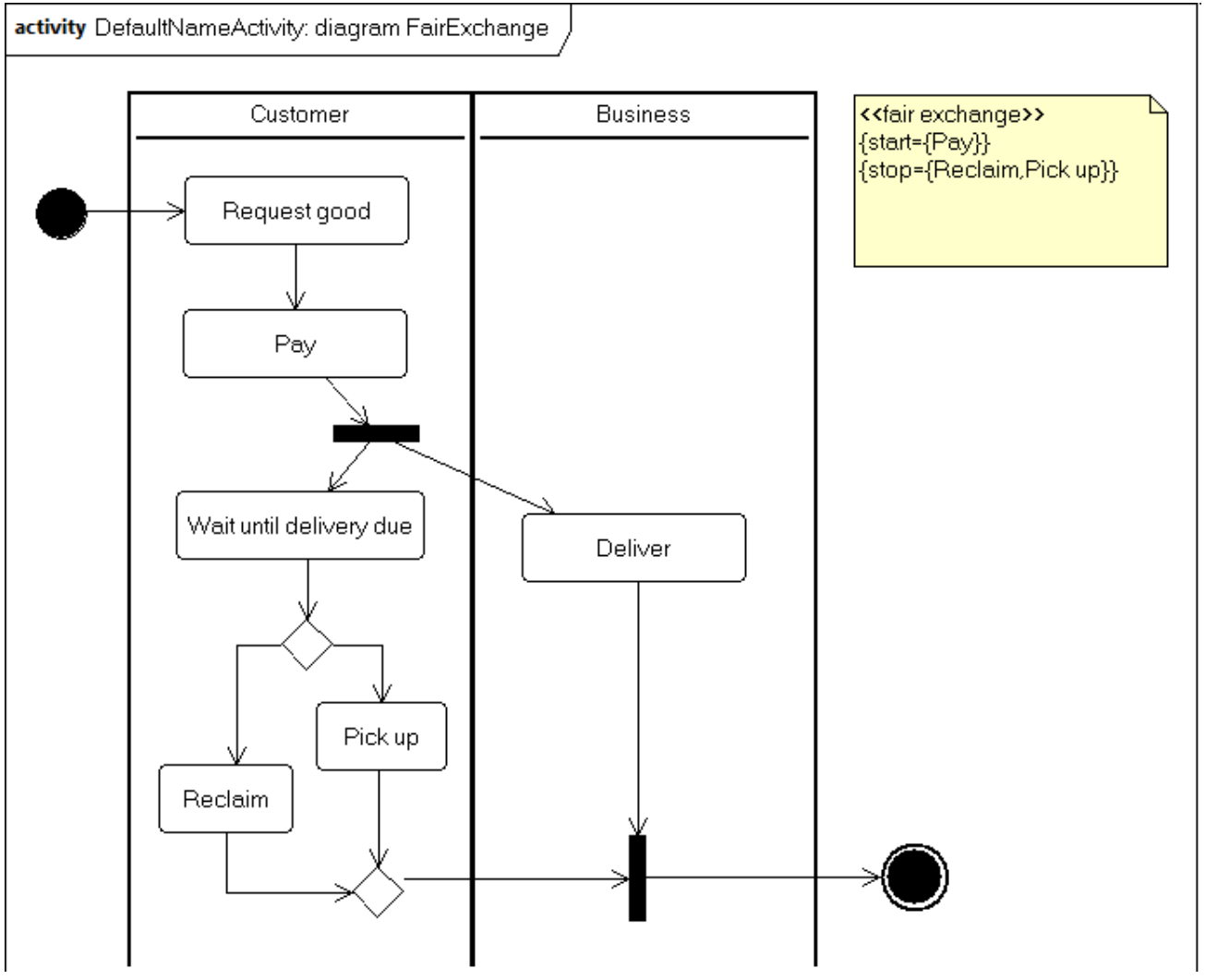
CARiSMA: Fair Exchange



CARiSMA: Fair Exchange

- Anforderungen an einen Handel:
  - Käufer erhält Ware, Verkäufer erhält Zahlung
  - Käufer behält Zahlung, Verkäufer behält Ware
- Handel erst abgeschlossen, wenn einer der beiden Fälle eintritt

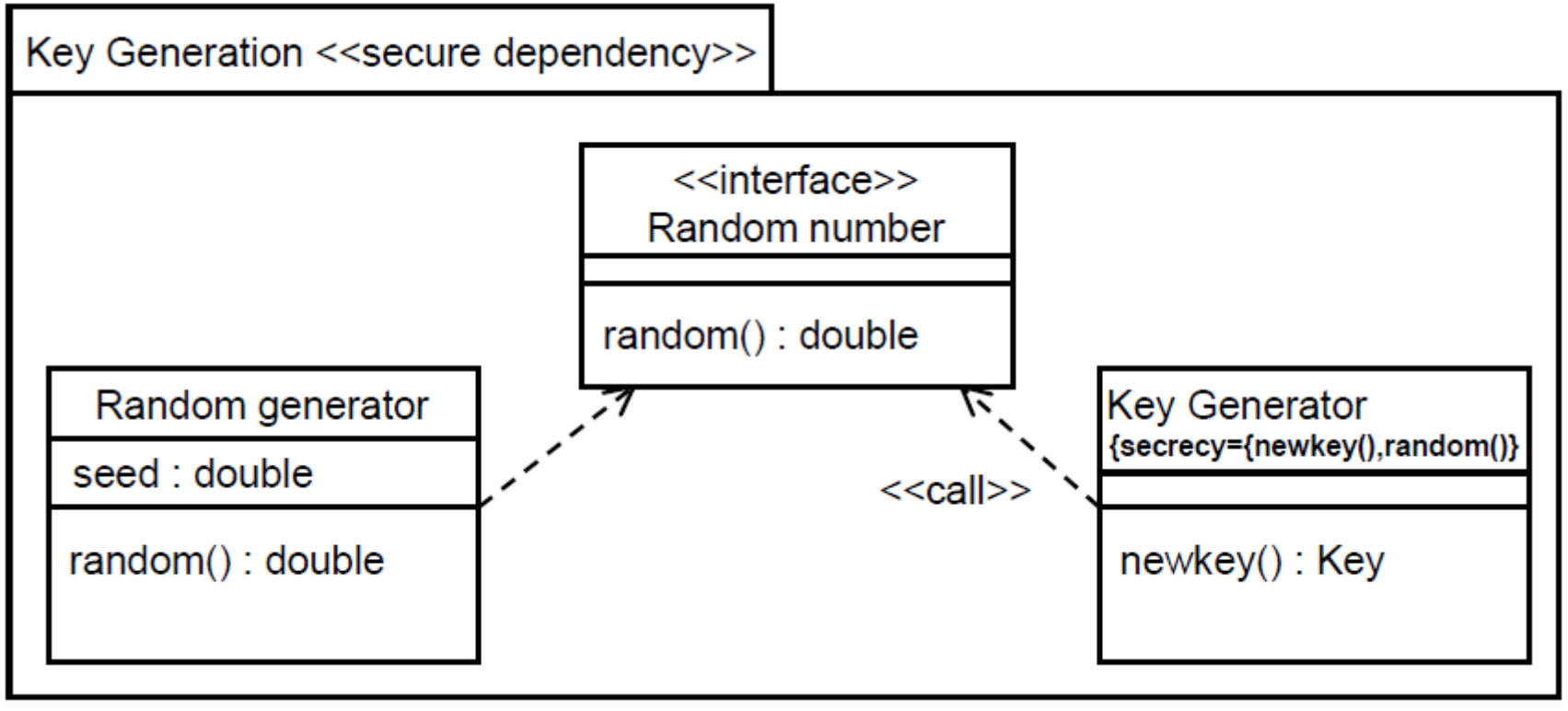
CARiSMA: Fair Exchange



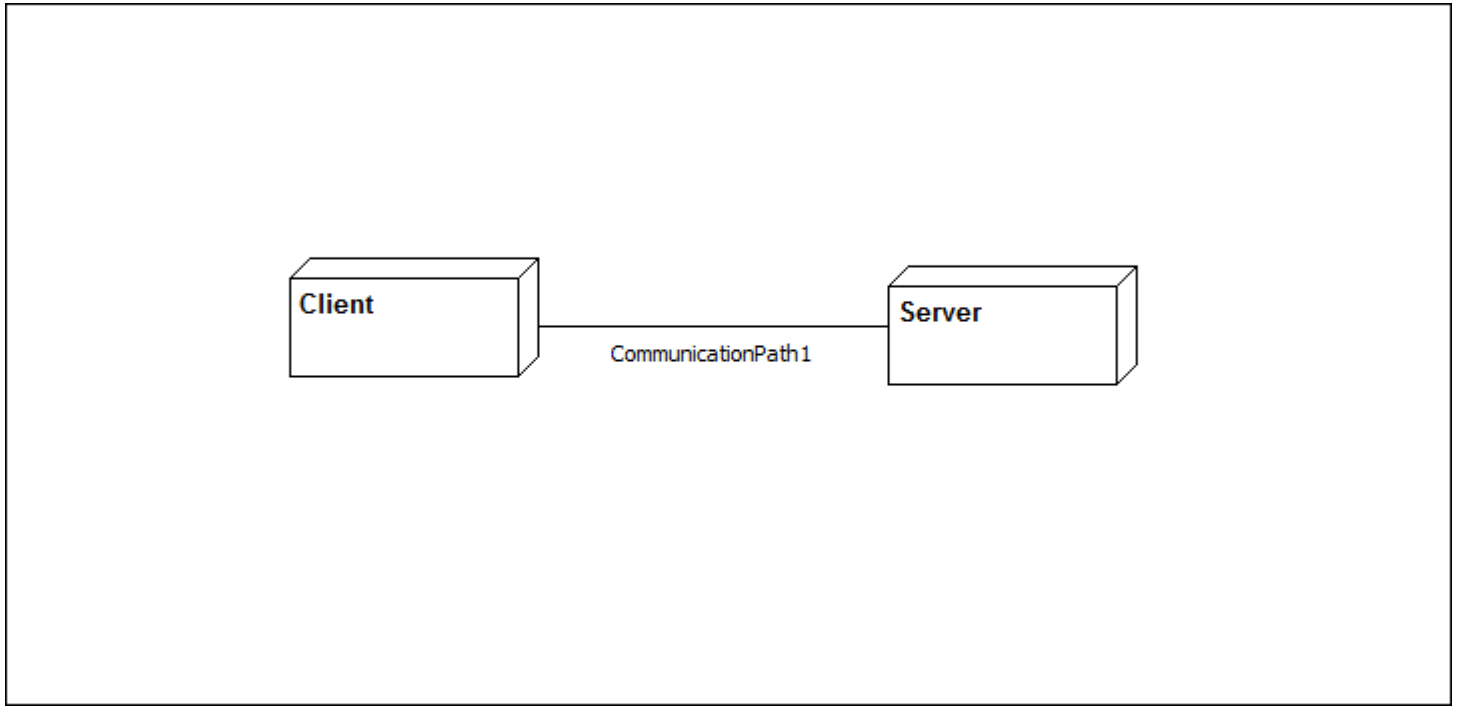
CARiSMA: Secure Dependency

- Seien C und D zwei Systeme, die Daten austauschen.
- An die Daten können Anforderungen gestellt werden:
  - {secrecy}, {integrity}
- Secure Dependency ist genau dann erfüllt, wenn Anforderung in C und D erfüllt.

CARiSMA: Secure Dependency



CARiSMA: Secure Links

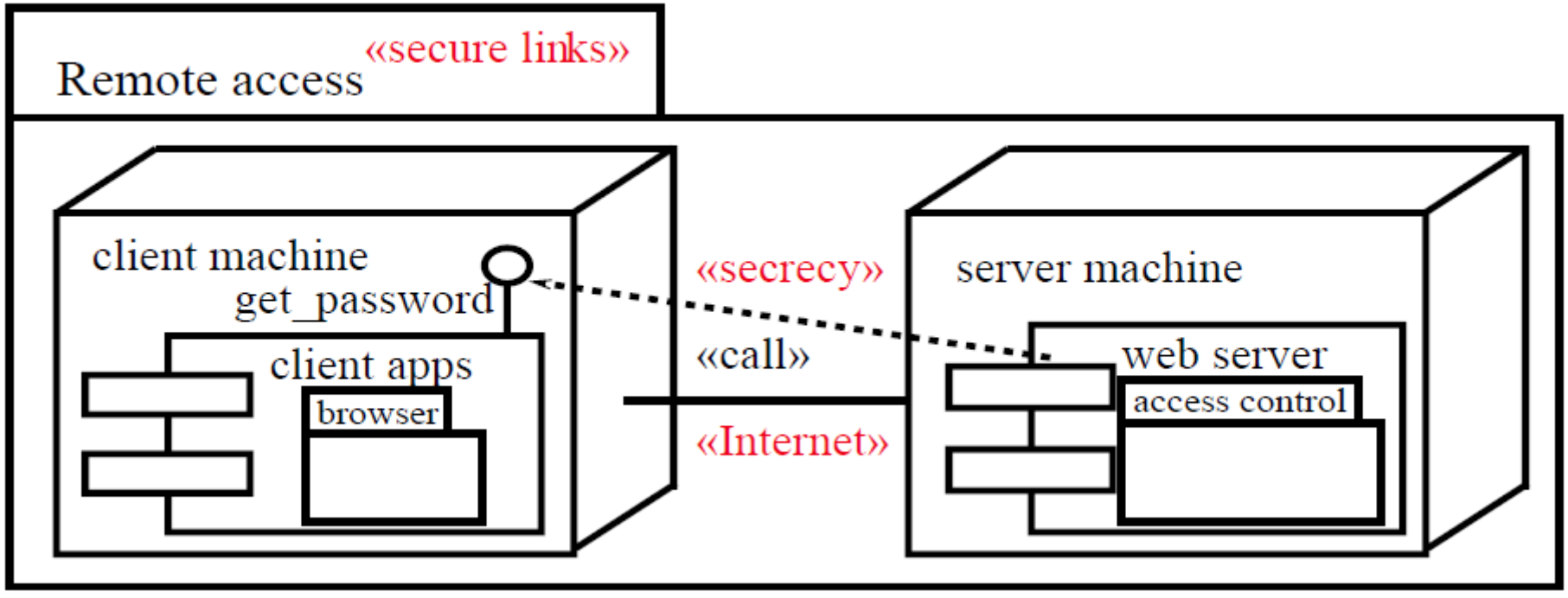


CARiSMA: Secure Links

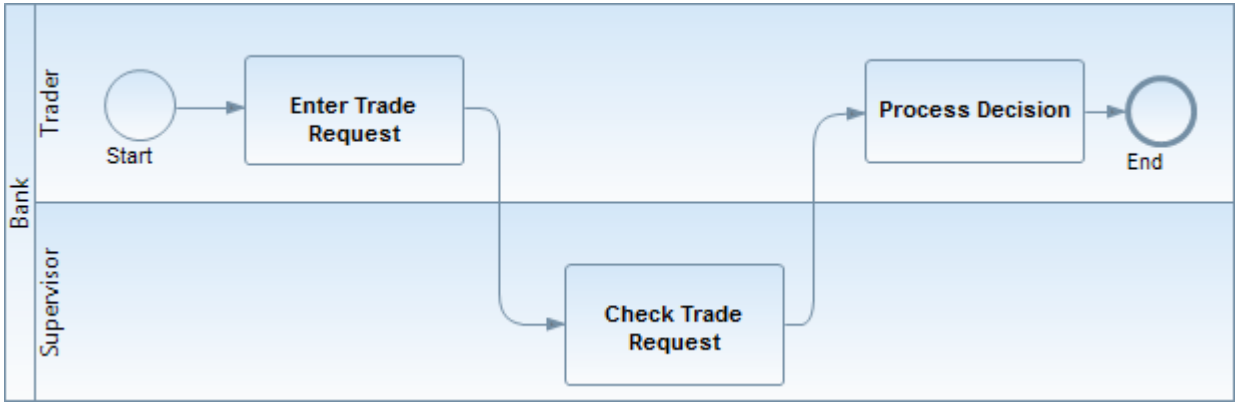
- Es existieren Kommunikationstypen s mit

  s ∈ {<<Internet>>, <<encrypted>>, <<LAN>>}
- Für einen Standard-Angreifer gilt:
  - $Threats_{default}$(Internet) = {delete, read, insert}
  - $Threats_{default}$(encrypted) = {delete}
  - $Threats_{default}$(LAN) = {}
- Es existieren Anforderungen {<<secrecy>>,<<integrity>>}
  - <<secrecy>> ist erfüllt gdw. read ∉ $Threats_A$(s)
  - <<integrity>> ist erfüllt gdw. insert ∉ $Threats_A$(s)

CARiSMA: Secure Links

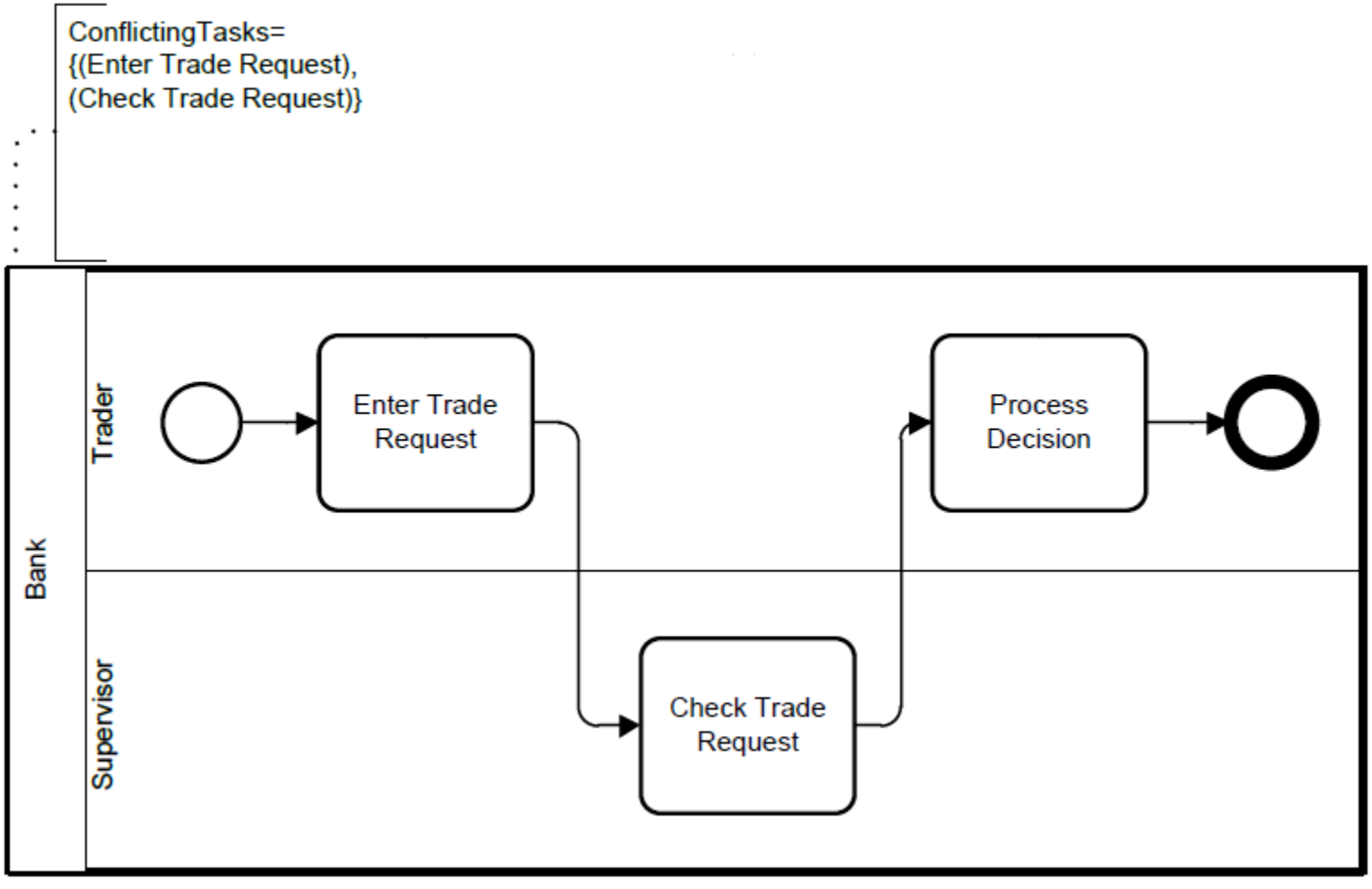


CARiSMA: BPMN2 OCL Check

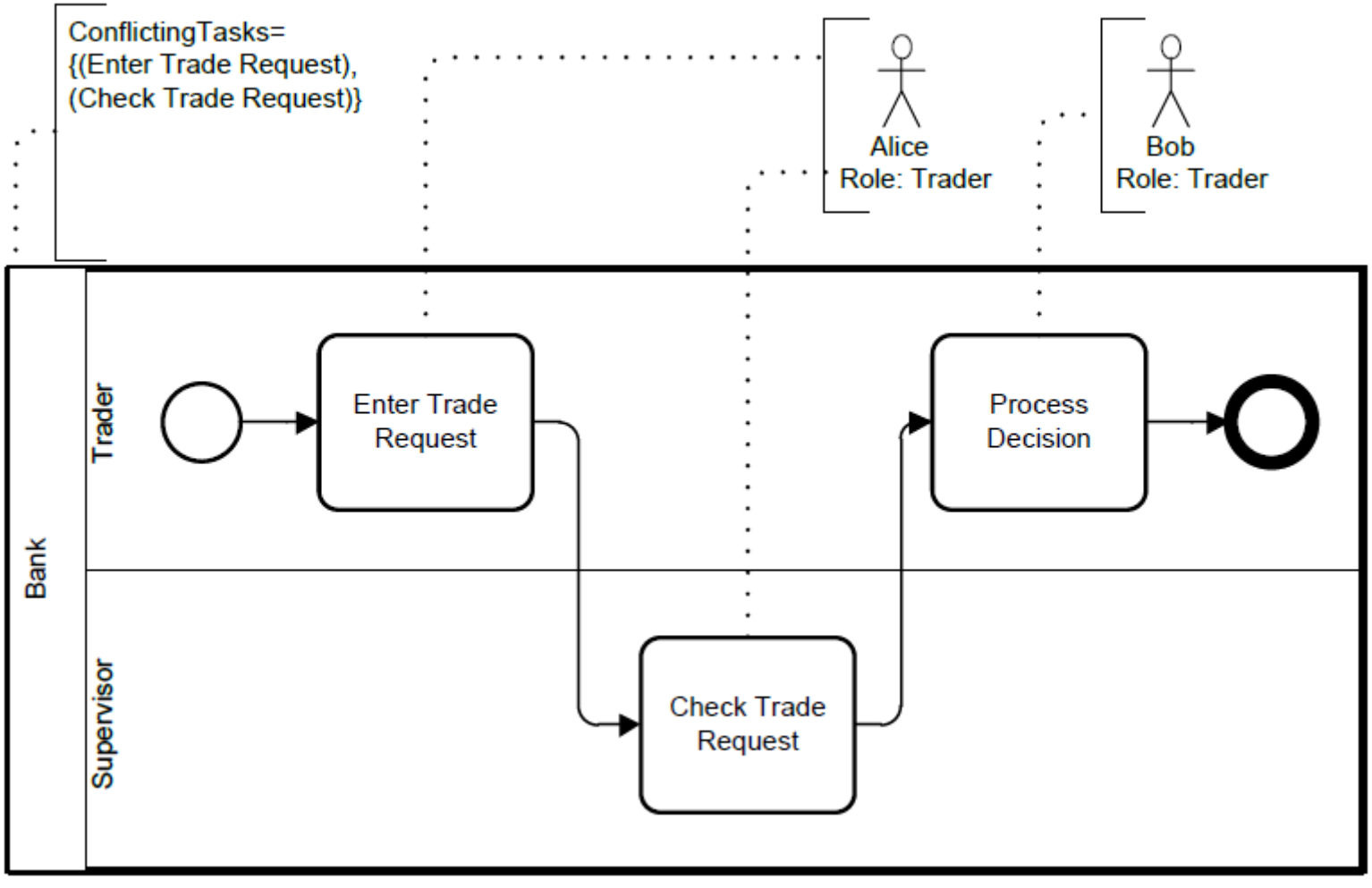


LEHRSTUHL 14
SOFTWARE ENGINEERING

CARiSMA: BPMN2 OCL Check



CARiSMA: BPMN2 OCL Check



CARiSMA: BPMN2 OCL Check

```
Context: Conflict
inv: self.conflictingTasks -> forAll(x,y | x <> y
        implies x.workItem.performer ->
        forAll(z | y.workItem.performer -> excludes(z)))
```

Fragen bisher?

Weiter mit: Praxis!

Literatur

- Jan Jürjens Secure Systems Development with UML
- Dev Team CARiSMA Dokumentation
  http://vm4a003.itmc.tudortmund.de/carisma/web/doku.php
- Object Management Group OCL Documents associated with Object Constraint Language, Version 2.3.1 http://www.omg.org/spec/OCL/2.3.1/
- Grafiken, teilweise modifiziert, aus Wikipedia Artikel zu BPMN 2.0
  http://de.wikipedia.org/wiki/Business Process Model and Notation
- Object Management Group UML Unified Modeling Language
- Object Management Group BPMN Business Process Model and Notation
  http://www.omg.org/spec/BPMN/2.0/
- Eclipse Modeling Framework http://www.eclipse.org/modeling/emf/
- Sven Wenzel The UMLsec2 Tool - Development Guide
  Interne Entwicklerdokumentation zum UMLsecTool