Vorlesung Wintersemester 2010/11

Workflow-Management-Systeme

Kapitel 16:
Aktuelle Forschungsthemen

Lehrstuhl für Systeme der Informationsverwaltung, Prof. Böhm
Institut für Programmstrukturen und Datenorganisation (IPD)

Überblick Kapitel 16

Aktuelle Forschungsthemen im Workflow-Bereich

- Aktuelle Forschungsthemen
- Security
- Usability
- Kollaboration

Die Folien 17-19 und 28-36 wurden in der Vorlesung nicht behandelt.
Die Folien zur BP Security Policy wurde nur exemplarisch und sehr kurz behandelt.

Forschungsthemen

Aktuelle Forschungsthemen im Workflow-Bereich

- Sicherheit und Vertrauenswürdigkeit von Workflows in offenen Systemen (siehe unten)
- Adaptive Workflow-Technologie (siehe Kapitel 10)
- Usability / Benutzerunterstützung (siehe unten)
- Data Mining Techniken für Monitoring und Analyse von Workflows (siehe Kapitel 13)
- Workflowchoreographie / Zusammensetzung / semantische Workflows (siehe Kapitel 9)

Forschungsthemen (ff.)

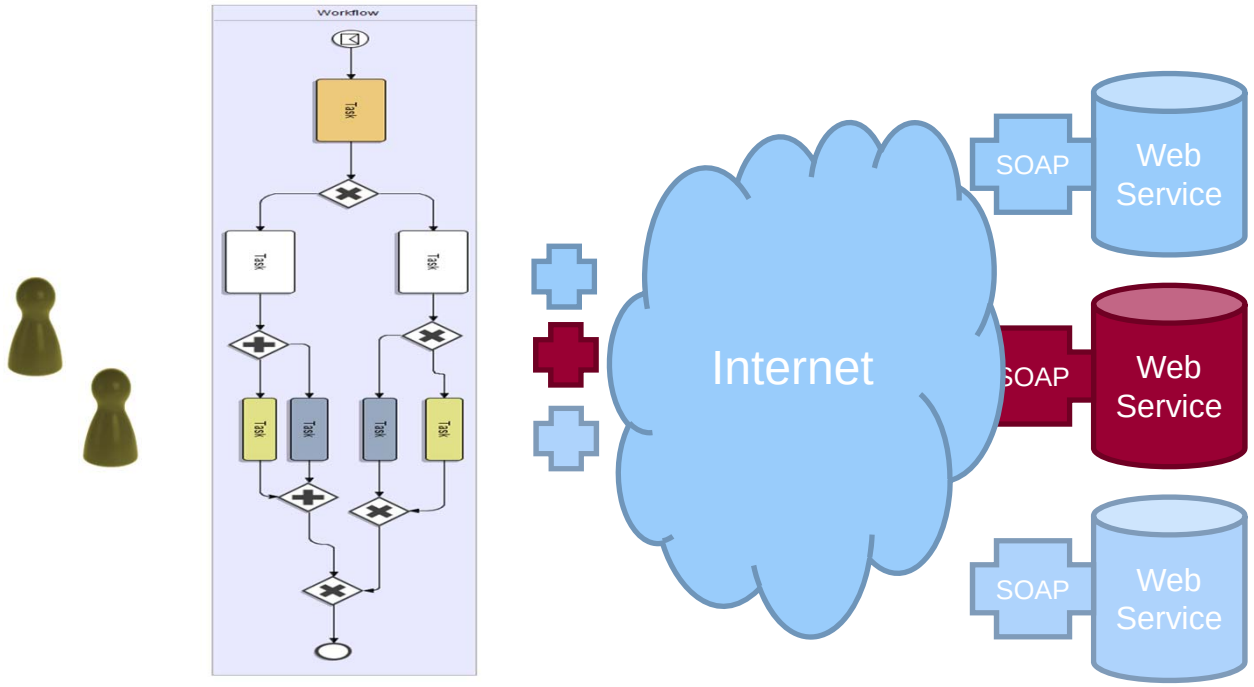
Aktuelle Forschungsthemen im Workflow-Bereich

- Große Datenmengen in Workflows / Scientific Workflows
- Kollaborationsunterstützung - Social BPM
- Event-Processing Systeme – Nutzung für Workflows
- Business Rules – Zusammenspiel mit Workflow-Systemen
- Workflow as a Service

Sicherheit und Vertrauenswürdigkeit von Workflows

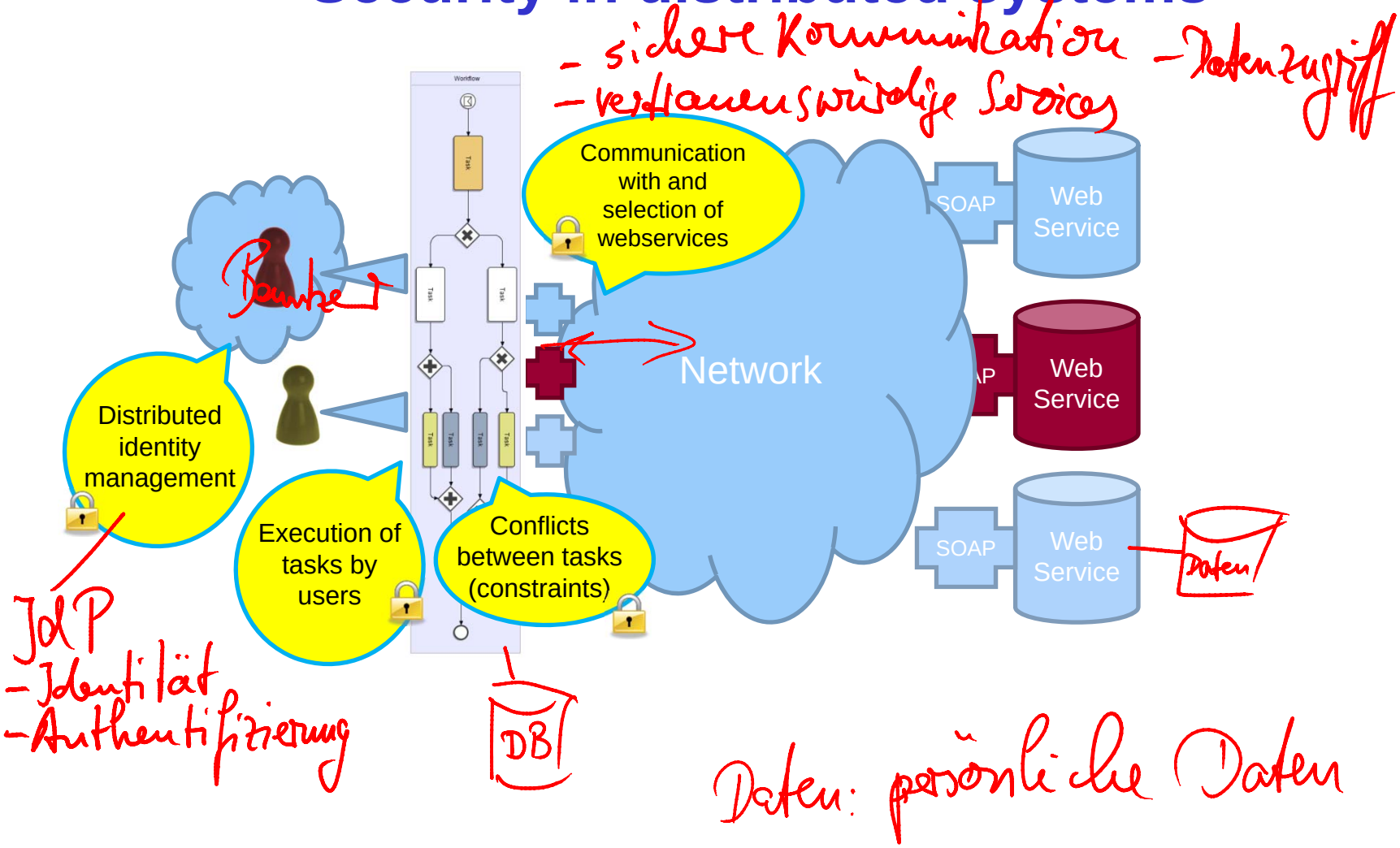
- Sicherheitsarchitektur
- Beispielszenario
- Sichere Workflows
  - Perspektiven
  - Architekturkomponenten
- Konzepte
  - Security Policy
  - Zugriffsüberwachungsanforderungen bei der Workflow-Ausführung
  - Role based Access Control - RBAC
  - (ANSI-Standard für Zugriffsüberwachungsverfahren)
  - Zugriffsüberwachung bei Workflowänderungen

Service-orientierte Architekturen (SOA) und Prozesse



- SOA: lose gekoppelte Services in einem Netzwerk
- Workflow-Management-System (WfMS) koordiniert Prozesse durch Service-Aufrufe
- Interaktive Akteure

Security in distributed systems



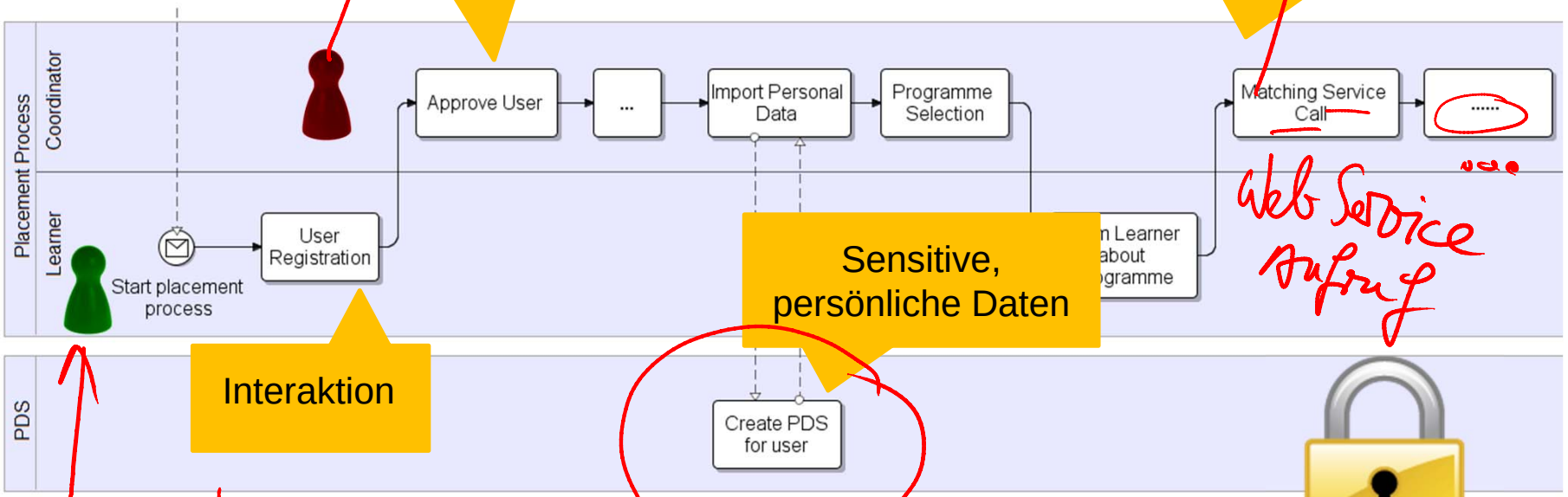
Ausführung – System Architektur

- Sicheres WfMS
  - Erweiterungen eines Open Source WfMS (BPEL-Engine) um Sicherheitskomponenten
  - Abbildung von Sicherheitsarchitekturen

- Einbettung des sicheren WfMS in Sicherheits/Trust-Network
  - Identitätsmanagement über Identity Provider
  - Security- und Trust-Policy-Entscheidungspunkte (PDP)

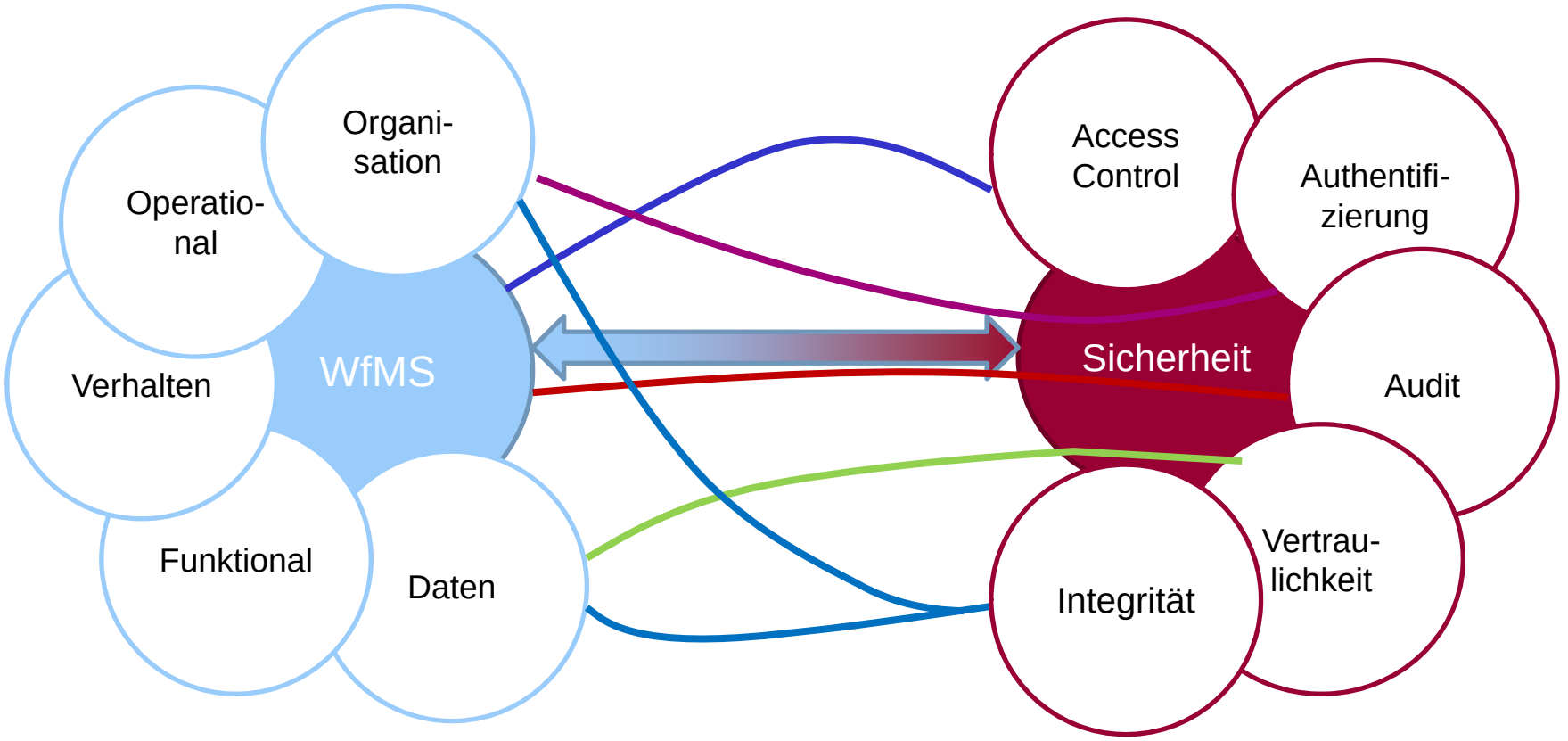
- Demonstratoren für Projekt(TAS^3)-Anwender-Prozesse

Beispielprozess Arbeitsvermittlung



Methodische Anforderungsanalyse

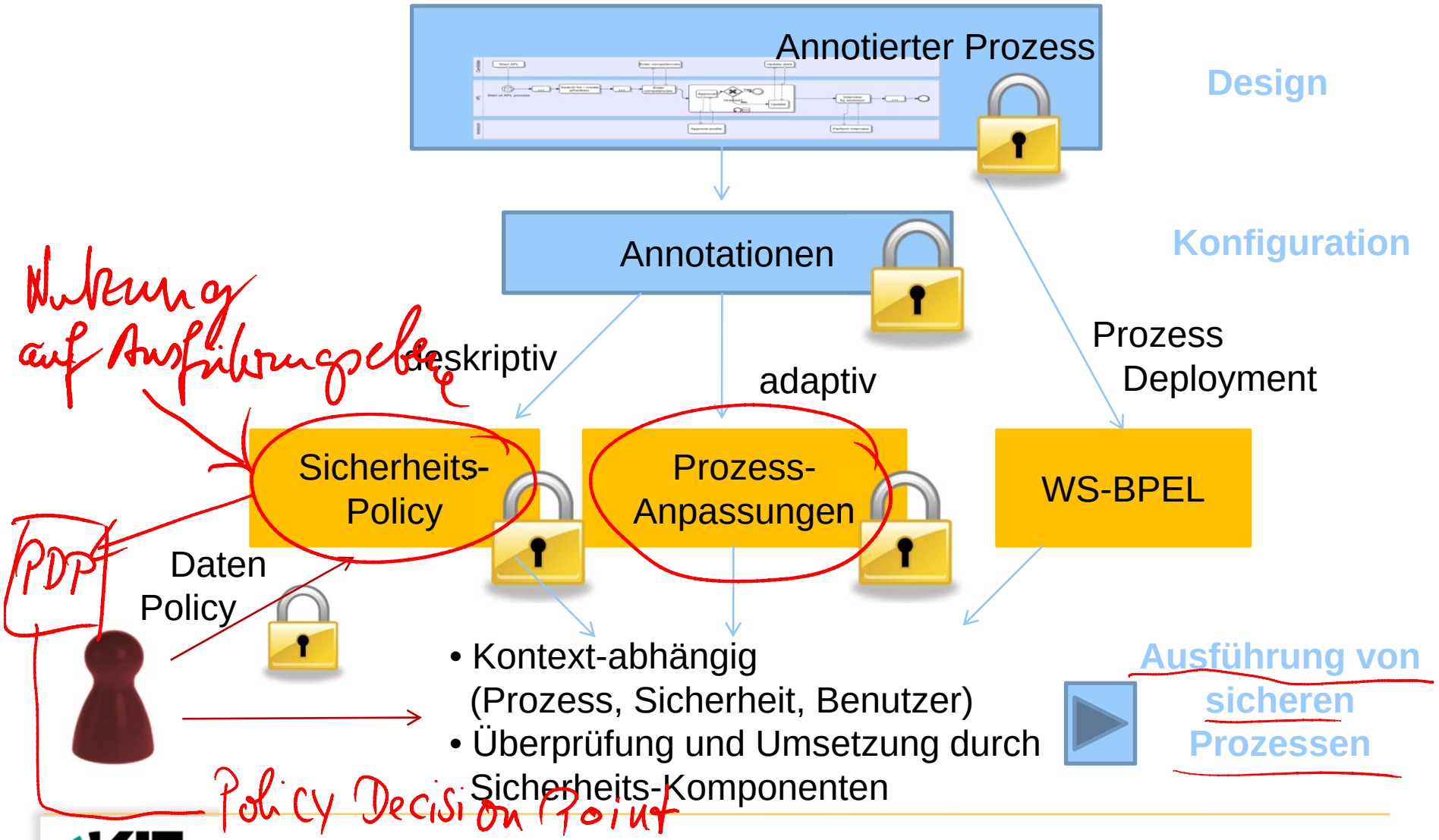
- Analyse einer „realen“ Anwendung



Ergebnis unserer Anforderungsanalyse

- Sicherheitslösungen notwendig für:
  - Zugriffskontrolle (Access Control) für Aktivitäten
  - Daten, die im Prozess involviert sind (insbes. personenbezogene Daten)
  - Kopplung mit externen Services
- Welche Faktoren müssen berücksichtigt werden?
  - Eigenschaften der Benutzer (z.B. Rollen, Zugehörigkeiten)
  - Abhängigkeiten zwischen Aktivitäten
  - Betroffene Prozessinstanz
  - Dynamische Faktoren, z.B. Delegation von Rechten
  - Benutzerpräferenzen, z.B. Auswahlvorgehensweise für W.Services

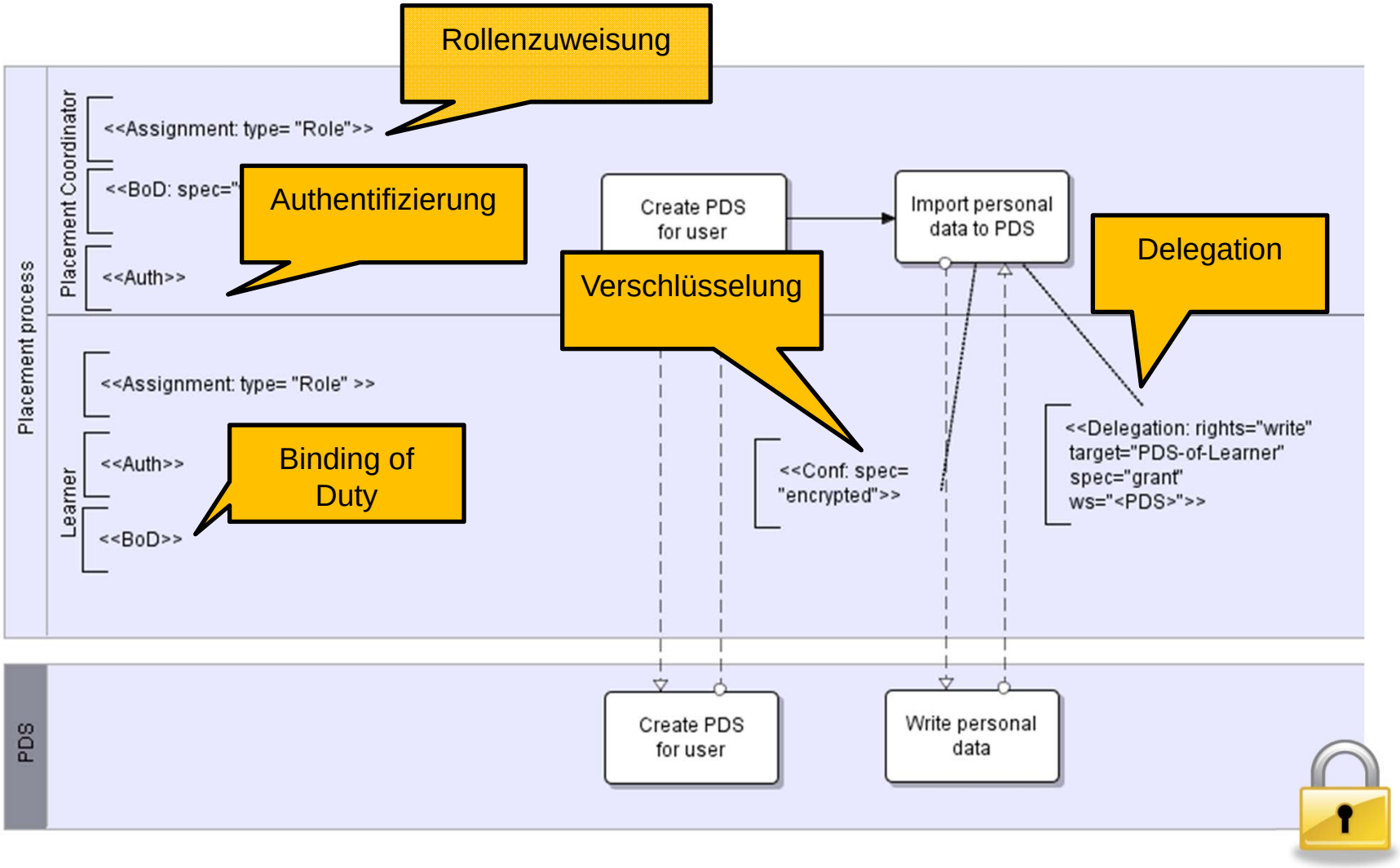
Sicherheit im Lebenszyklus von Prozessen



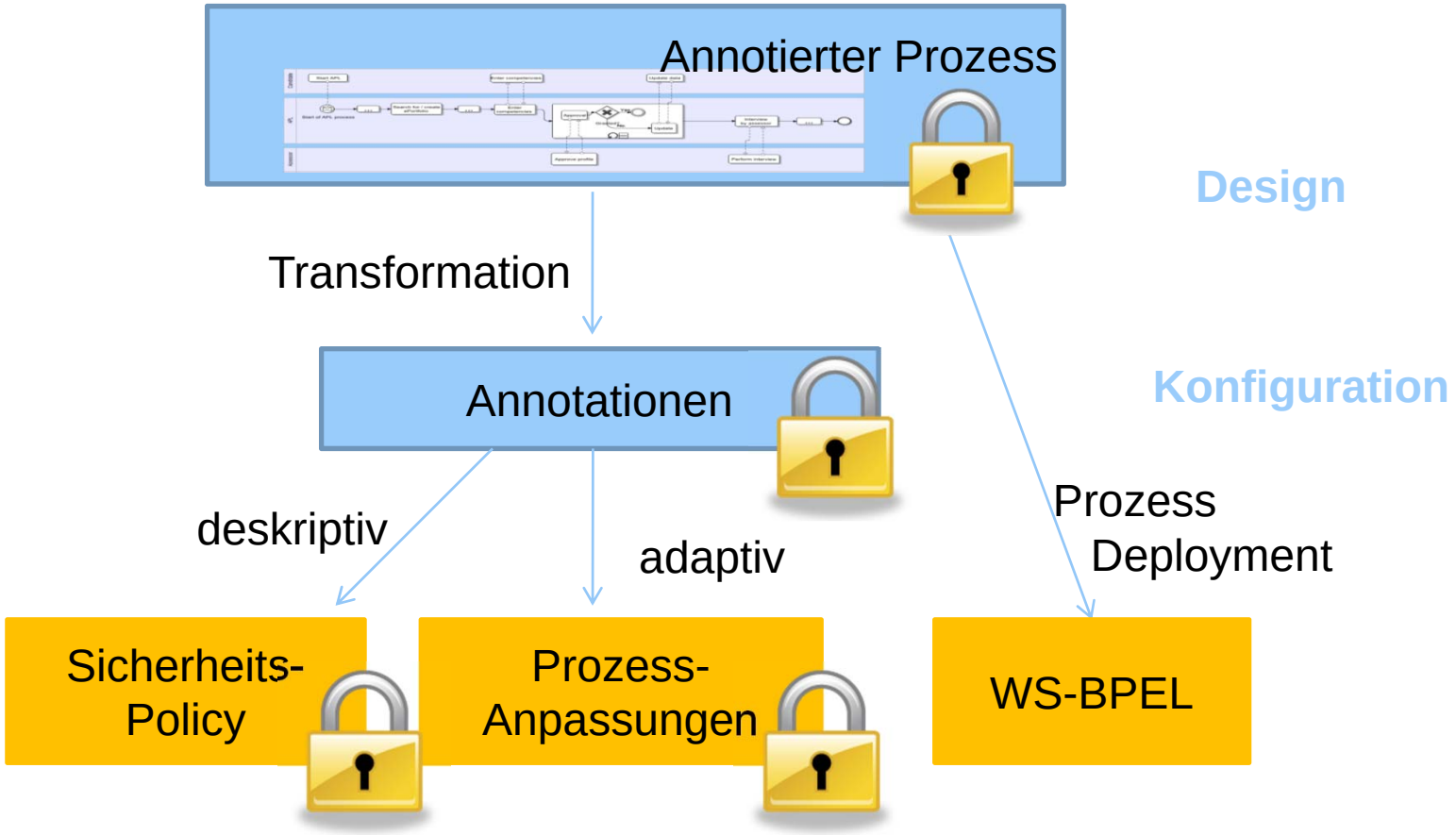
Design

- Entwicklung eines Sicherheits-Vokabulars zur Modellierung
  - Authorisierung, Authentifizierung
  - Pflichtenbindung (BoD (Binding of Duty)), Pflichtentrennung (Separation of Duties (SoD))
  - Verschlüsselung, Signatur
  - …..
- Standard-konform zu BPMN 2.0 (Business Process Model and Notation)
  - Einbindung des Vokabulars als Annotationen
- Neben Sicherheits-Vokabular: „Trust“ und Benutzerinteraktionen, wie beispielsweise
  - Einwilligung zu Geschäftsbedingungen (z.B. Terms & Conditions)
  - Spezifikation der Trust-Parameter beteiligter Services
  - ….

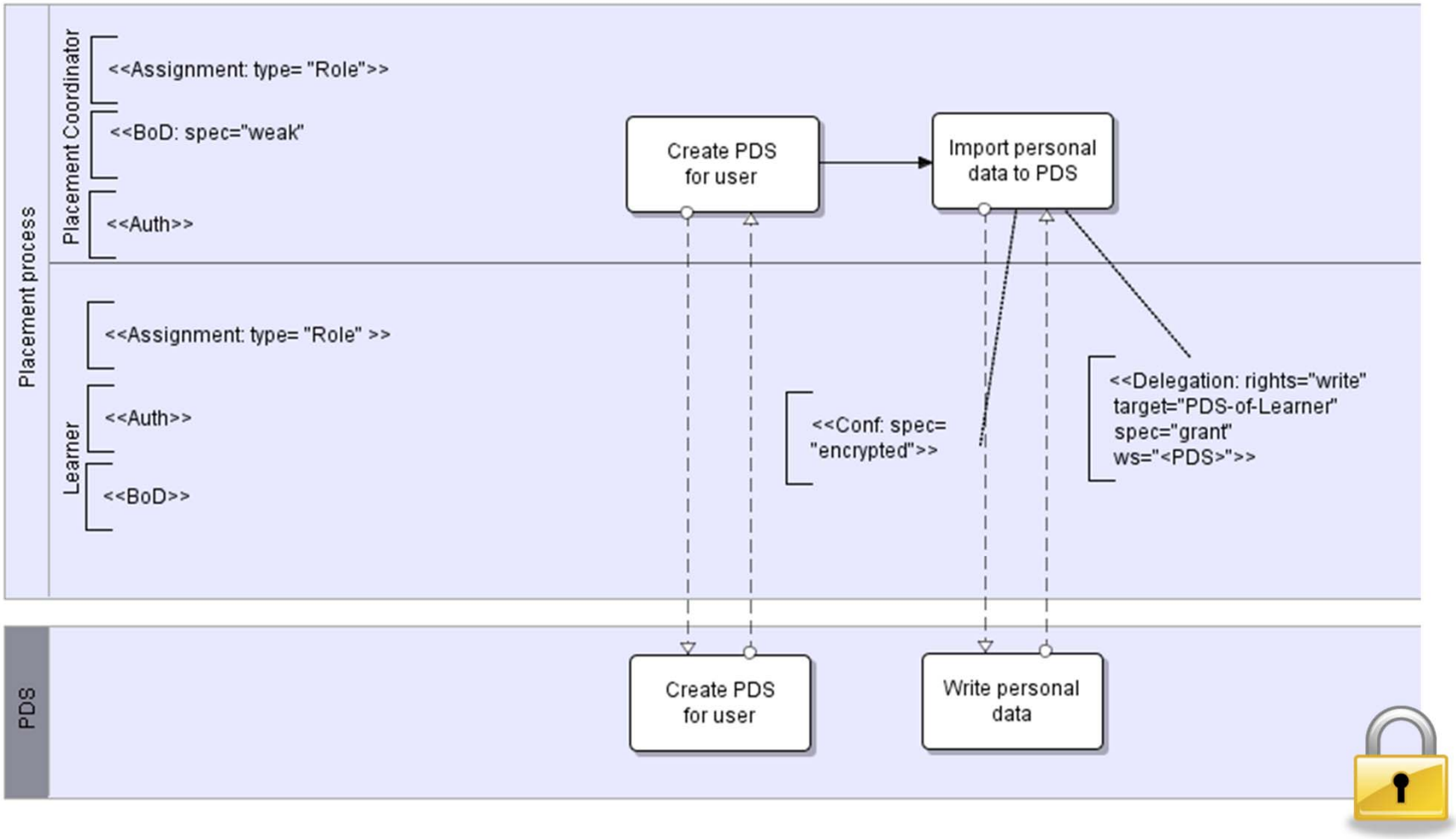
Beispiele Annotationen in BPMN – Sicherheit



Deskriptive Konfiguration

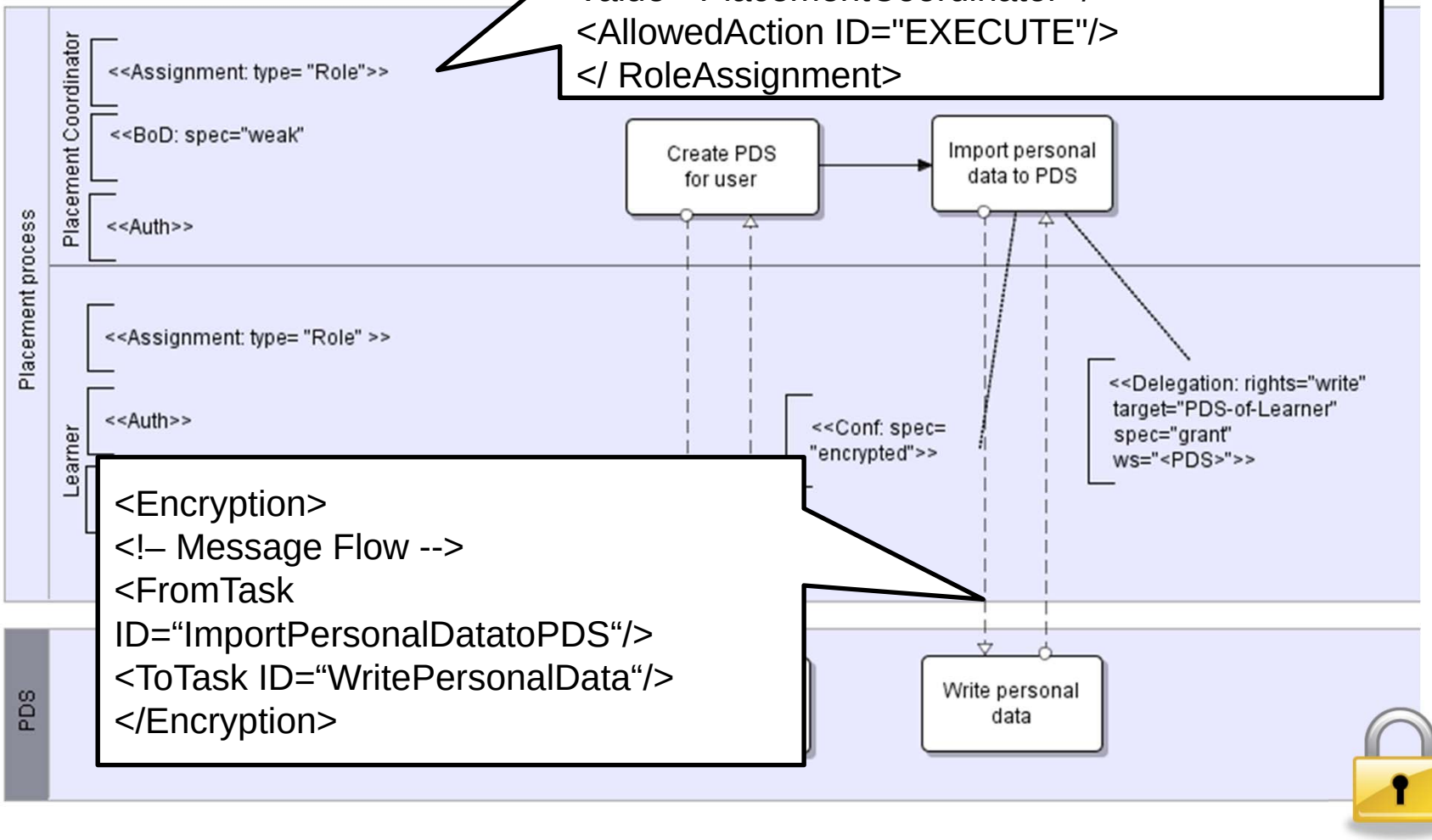


Beispiele Sicherheits-Policy



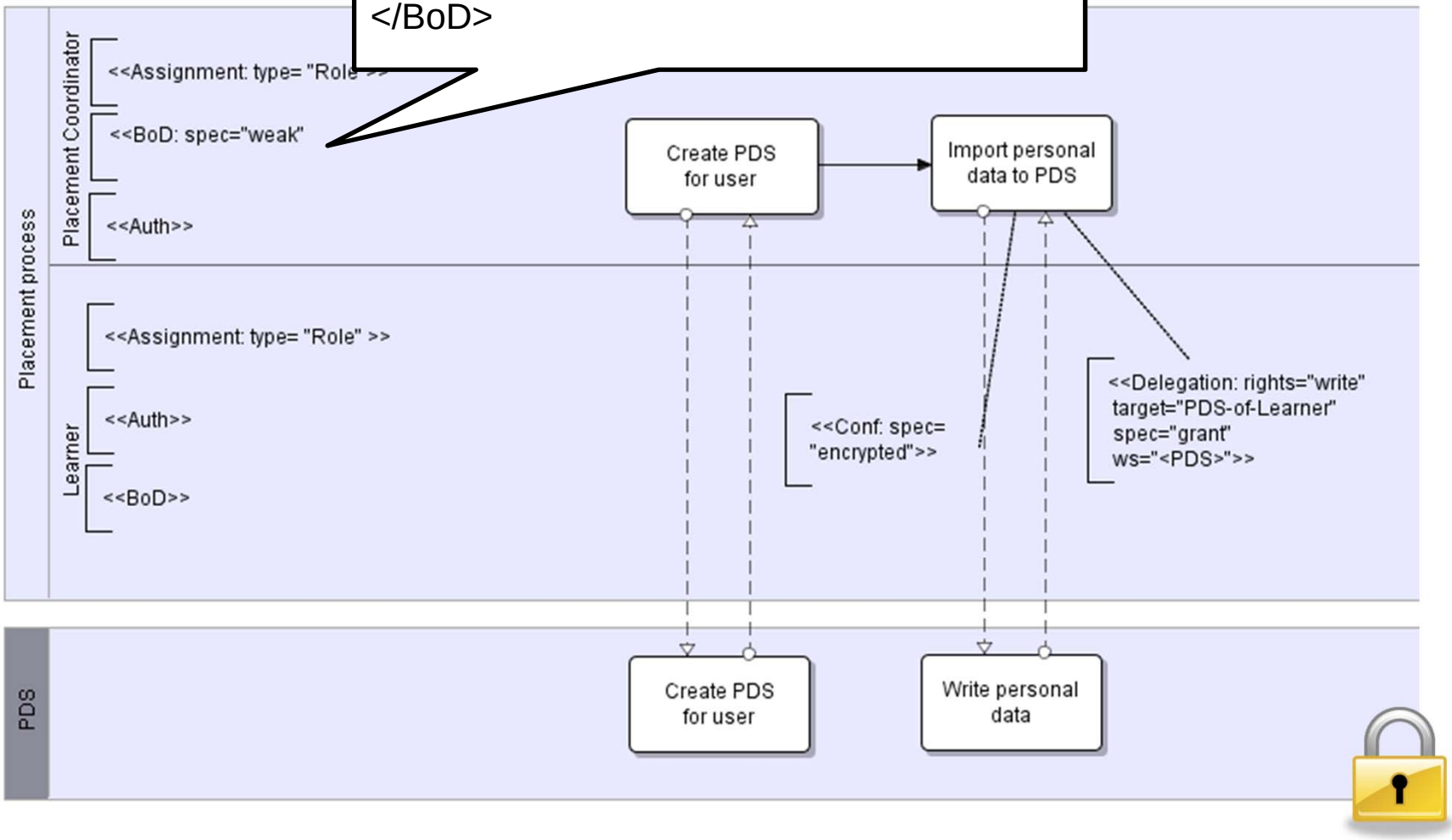
Beispiele

```
<RoleAssignment>
<Task ID="CreatePDSforUser"/>
<Task ID="ImportPersonalDatatoPDS"/>
<Role Type="PlacementProcess"
Value="PlacementCoordinator" />
<AllowedAction ID="EXECUTE"/>
</ RoleAssignment>
```



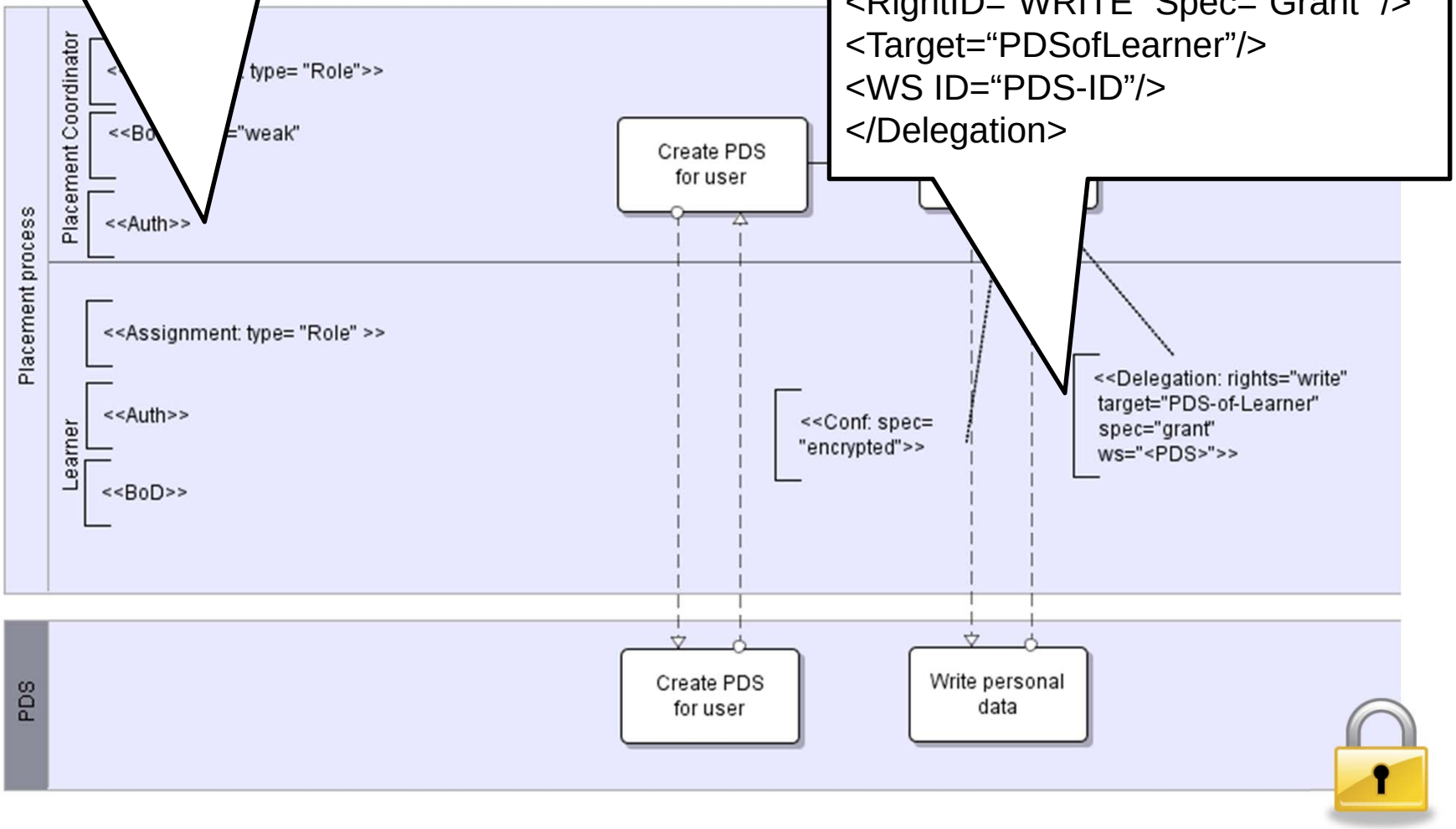

```
<Encryption>
<!– Message Flow -->
<FromTask
ID="ImportPersonalDatatoPDS"/>
<ToTask ID="WritePersonalData"/>
</Encryption>
```

<BoD>
<!– Binding of Duty for set of tasks -->
<Task ID=“CreatePDSforUser“/>
<Task ID=“ImportPersonalDatatoPDS“/>
<SpecType=“weak”/>
</BoD>

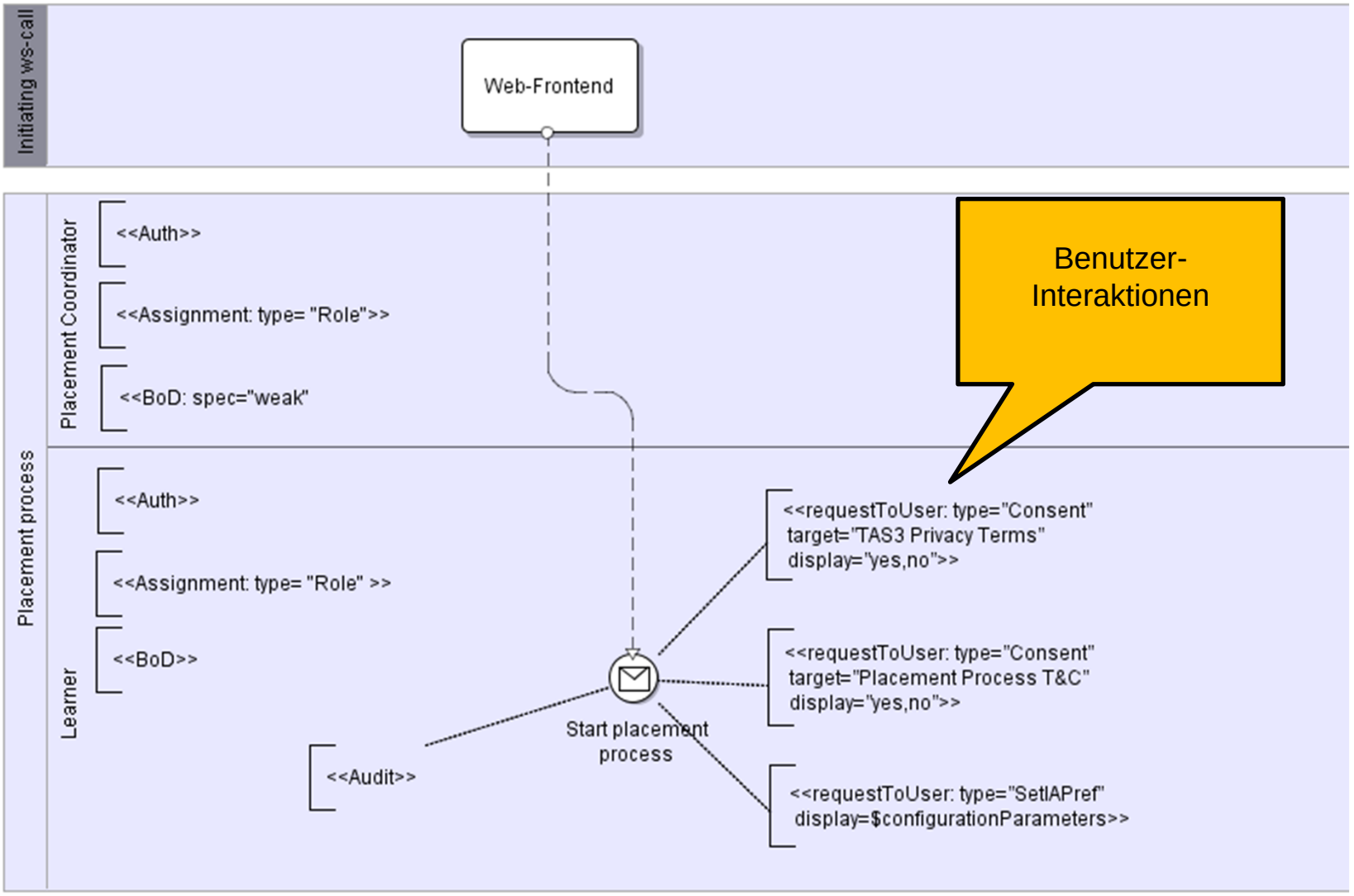


<Authentication>
<Task ID="CreatePDSforUser"/>
<Task ID="ImportPersonalDatatoPDS"/>
</ Authentication >

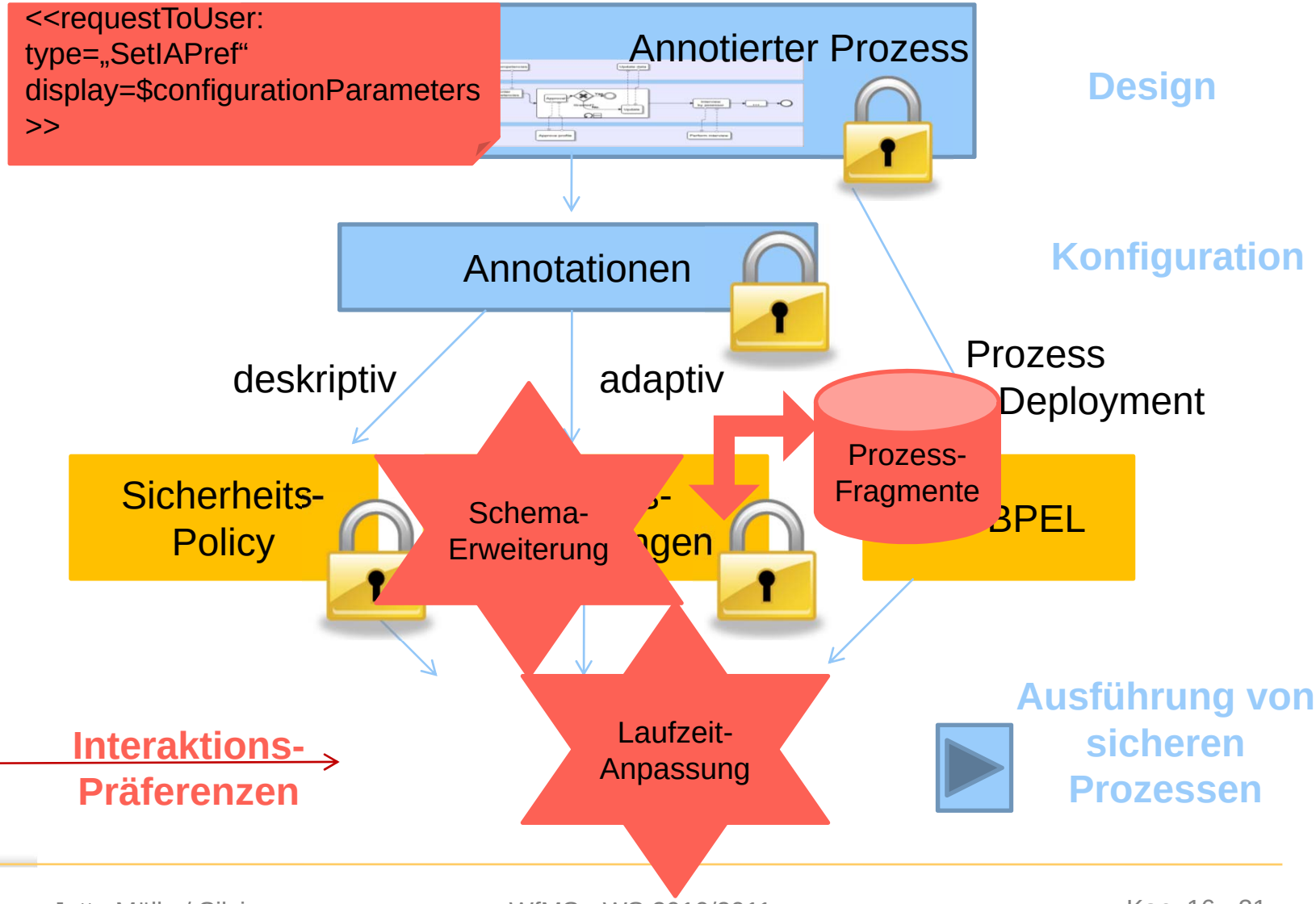
<Delegation>
<!– Transfer of Rights-->
<Task
ID="ImportPersonalDatatoPDS"/>
<RightID="WRITE" Spec="Grant" />
<Target="PDSofLearner"/>
<WS ID="PDS-ID"/>
</Delegation>



Beispiele Annotationen - Benutzerinteraktionen



Adaptive Konfiguration



Sicherheit im Lebenszyklus in WfMS

- Design
  - Annotation von Prozessmodellen
- Konfiguration
  - Transformation der annotierten Sicherheits-Anforderungen
    - Deskriptiv -> Business Process Policy
    - Adaptiv -> Prozess-Erweiterungen (Anpassungen)
- Ausführung von sicheren Workflows
  - Kontext-abhängig (Prozess, Sicherheit, Benutzer)
    - Ggf. adaptiv
  - Überprüfung und Umsetzung mittels Sicherheits-Komponenten
  - (Migration)

Beispiel Security Policy

```
<BusinessProcessPolicy>

<RoleAssignment>
<Task ID=“CreatePDSforUser“/>
<Task ID=“ImportPersonalDatatoPDS“/>
<Role Type=“CoordinatioEntitlement"
     Value=“staff" />
<AllowedAction ID="EXECUTE"/>
</ RoleAssignment >

<Authentication>
<Task ID=“CreatePDSforUser“/>
<Task ID=“ImportPersonalDatatoPDS“/>
</ Authentication >

<BoD>
<!– Binding of Duty for set of tasks  -->
<Task ID=“CreatePDSforUser“/>
<Task ID=“ImportPersonalDatatoPDS“/>
</BoD>

<Encryption>
<!– Message Flow -->
<FromTask ID=“ImportPersonalDatatoPDS“/>
<ToTask ID=“WritePersonalData“/>
</Encryption>

<Delegation>
<!– Transfer of Rights-->
<Task ID=“ImportPersonalDatatoPDS“/>
<RightID=“WRITE” Spec=“Grant” />
<Target=“PDSofLearner”/>
<WS ID=“PDS-ID”/>
</Delegation>

</BusinessProcessPolicy>
```

Komponenten einer BP Security Policy

- Regeln zum Ausführen von Tasks, z.B. Rollen (Access Control ?)
- Zuordnungsstrategie (bei mehreren Optionen)
- Direkte Zuordnungen
- Spezifikation von Rollenhierarchien (warum in Bpolicy?) -> soll vom annotierten Prozessmodell extrahiert werden, sofern möglich;
- Authentifizierung
- Restriktionen für BoD und SoD
- Delegation
- Verschlüsselung/Signaturen für Nachrichtenflüsse
- Data Access
  - (im TAS-3 Umfeld von extern (z.B. generische Data Policies der Nutzer) und muss an BP angepasst werden)
  - Oder spezifisch für den BP, vom Benutzer über User Interactions festgelegt;
- Trust Policies für Web Service Aufrufe

Beispiel BP Security Policy

```
<DataItemList>
<!-- Data items on which permissions are transferred. -->
<!-- The mechanism for transferring the permission
needs to be determined. -->
<DataItem ID="data-itemID1" type="urn:tas3:E-Portfolio"
ownerref="JobSeekerTasks"/>
<DataItem ID="data-itemID2" type="urn:tas3:CV"
ownerref="JobSeekerTasks"/>
</DataItemList>

<AccessSpecification>
<Right Type="read,write" DataItemID="data-itemID1"
AllowedFor="PlacementProviderTasks"/>
<!-- Allow the user assigned to PlacementProviderTasks
read and write access on data-itemID1
(of type urn:tas3:E-Portfolio, defined above) -->
</AccessSpecification>


</BusinessProcessPolicy>
```

Hier dann Beispiel Auditing

Umsetzung von User Requests (1)

- Idee: Dynamische, benutzer- und sicherheits-kontext-abhängige Einbindung von a priori spezifizierten Prozess-Pattern
- Beispiel:
  - Interaktionspräferenzen eines Benutzers zur Handhabung seiner persönlichen Daten

Umsetzung von User Requests (2)

- Annotation impliziert folgende Schritte
  - Modifikation des Prozess-Schemas, Hinzufügen von Prozessfragmenten (a priori und zur Laufzeit)
    - A priori: Einfügen von Benutzerinteraktionen
    - Zur Laufzeit: abhängig von Benutzer- und Sicherheitskontext (z.B. Interaktionspräferenzen für Zugriff auf persönliche Daten)
  - Anpassung der Prozesskonfiguration (z.B. Trust-Parameter für Web Service Aufruf)
  - Migration von Instanzen (falls nötig)

Zugriffskontrollanforderungen I

Anforderungen an Kontext-sensitive Zugriffskontrolle:

- Order of events
- Strict least Privilege
- Separation of duty

Order of events:

- Gewähren bestimmter Zugriffsrechte hängt von der erfolgreichen Beendigung anderer Tasks ab
- Z.B. Kann der Schadensfall nicht anerkannt werden, wenn nicht das Kundenprofil vervollständigt wurde
- Der Mechanismus sollte daher in der Lage sein zu erkennen, an welchem Punkt bei der Bearbeitung des Schadensfalls er sich befindet.

Zugriffskontrollanforderungen II

Strict least Privilege:

- **Least Privilege:** Ein Benutzer bekommt minimale Rechte, die nötig sind, um seine Arbeit zu verrichten**, d**.h. er bekommt Rechte auf Tasks, die er zu irgendeinem Zeitpunkt während seiner Arbeit ausführen muss
- **Strict Least Privilege:** Rechte werden weiter eingeschränkt auf die minimalen Rechte, die *zu einem bestimmten Zeitpunkt für eine bestimmte Task* benötigt werden. Z.B. sollte ein Manager, der den Schadensfall-Ablaufplan inizialisiert, nur die Sachbearbeiter-Rechte erhalten, die nötig sind um die Task auszuführen, nicht aber die Rechte, um den Schadensfall zu genehmigen oder zu verweigern

Zugriffskontrollanforderungen III

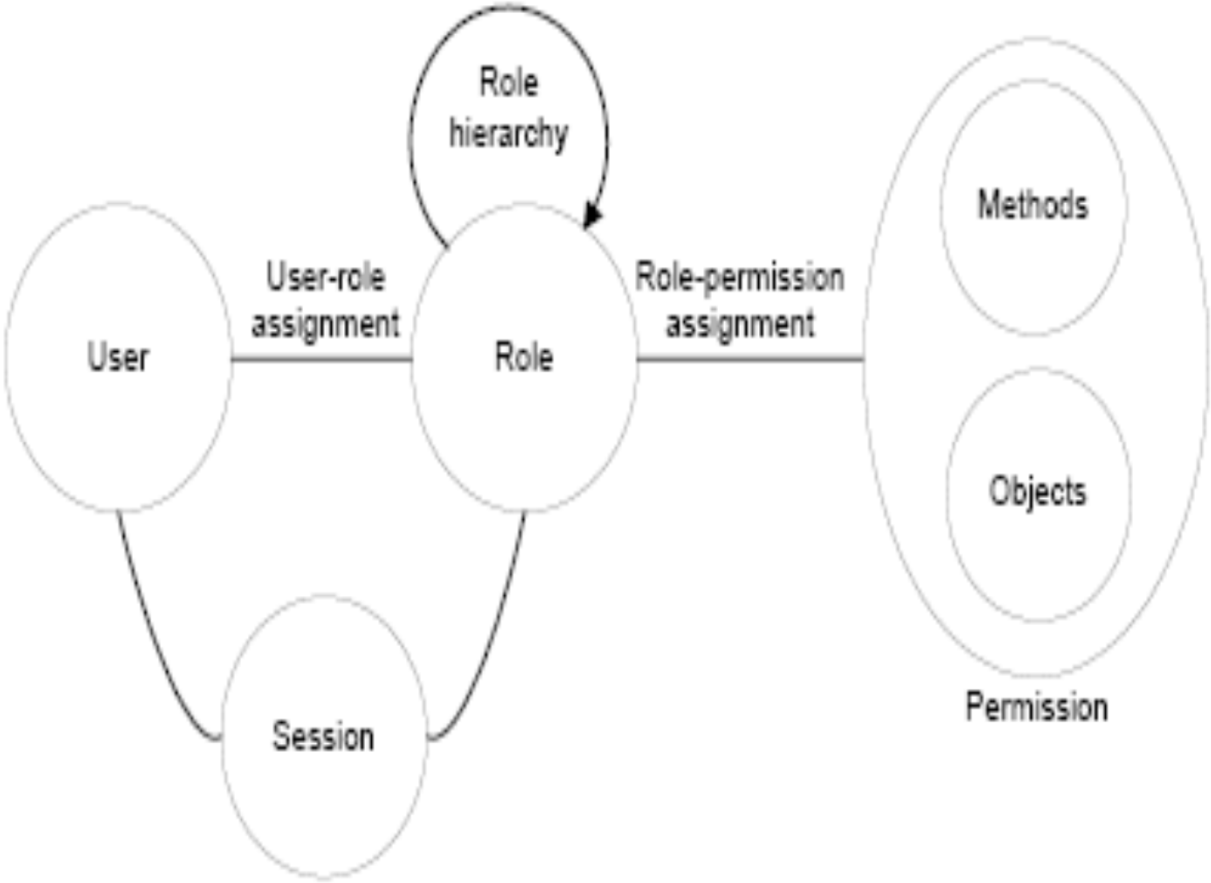
Separation of duty:

- Verlangt zwei oder mehr verschiedene Personen, die für den Abschluss eines Geschäftsprozesses verantwortlich sind
- Erschwert Betrug, da dafür eine Verschwörung nötig ist und dadurch erhöhtes Risiko der Betrüger
- Z.B. sollten Schadensgutachter (assessor) und Manager disjunkte Rechte haben. Außerdem müssen laut Prozess-Definition beide beteiligt sein
- Separation-of-duty-Anforderungen werden häufig als Geschäftsregeln formuliert, z.B. „Ein Scheck benötigt zwei verschiedene Unterschriften“

Autorisierung mit RBAC

- Zur Festlegung von Ausführungs- und Zugriffsberechtigungen dienen in WfMS *rollenbasierte* Zugriffskonzepte
- Aufgaben-orientierte Rechtevergabe durch Rollen
- Eine *Rolle* ist eine Sammlung von *Privilegien* (Rechten), die *Benutzern* zugewiesen werden.
- RBAC konzentriert sich auf die Unterstützung folgender Konzepte :
  - Gruppierung von Benutzern
  - Gruppierung von Berechtigungen
  - Aufgabentrennung (Separation of Duty)

Role-based Access Control (RBAC) I



Role-based Access Control (RBAC) II

- **Benutzern** (U) werden **Rollen** (R) durch eine Benutzer-Rollen-Zuweisungsrelation (UA) zugewiesen
- Die **Zugriffsrechte** (P), die in Verbindung stehen mit einer Rolle, werden in der Rollen-Zugriffsrechte-Zuweisungsrelation (PA) wiedergegeben
- Die Zugriffsrechteabstraktion (P) wird in diesem Modell wiedergegeben als die für ein **Objekt** (O) verfügbaren **Methoden** (M)

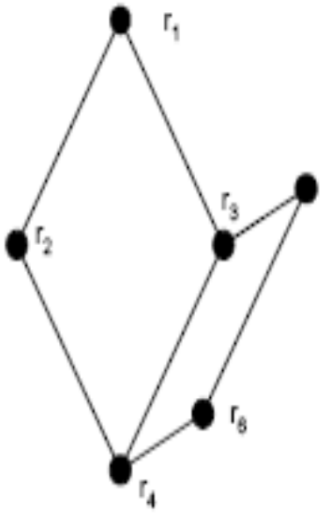
Role-based Access Control (RBAC) III

- Z.B. könnte ein Benutzer das Recht erhalten die „Schadensfall-Genehmigen“-Methode für ein „Schadensfall-Formular“-Objekt auszuführen
- Ein Benutzer erhält die Zugriffsrechte verbunden mit den Rollen, die er für die **Session** (S) einnimmt
- Eine Session ist ein zeitgebundenes Konstrukt, um Benutzer, Rollen und Zugriffsrechte miteinander zu verbinden

Role-based Access Control (RBAC) IV

Vererbung durch Rollenhierarchie:

- Rollen sind untereinander partiell geordnet
- Rollen erben die Rechte derjenigen Rollen, die in der partiellen Ordnung kleiner sind als sie selbst.



- Rolle r1 ist den Rollen r2 und r3 übergeordnet, die wiederum sind r4 übergeordnet
- r1 erbt die Rechte, die mit r2 und r3 verbunden sind
- r1 und r5 stehen durch die Rollenhierarchie nicht miteinander in Verbindung

RBAC und Kontext

RBAC unterstützt Prinzipien wie „Separation of duty“ oder „least privilege“, aber erzwingt sie nicht

Separation of duty:

- Kann erreicht werden, indem die Mitgliedschaft zweier Rollen sich gegenseitig ausschließt durch **disjunkte Rollenhierarchien**
- Im Beispiel sind dann Schadensgutachter und Manager in verschiedenen Rollenhierarchien, die Rechte von Schadensgutachter und Manager sind disjunkt

Least Privilege:

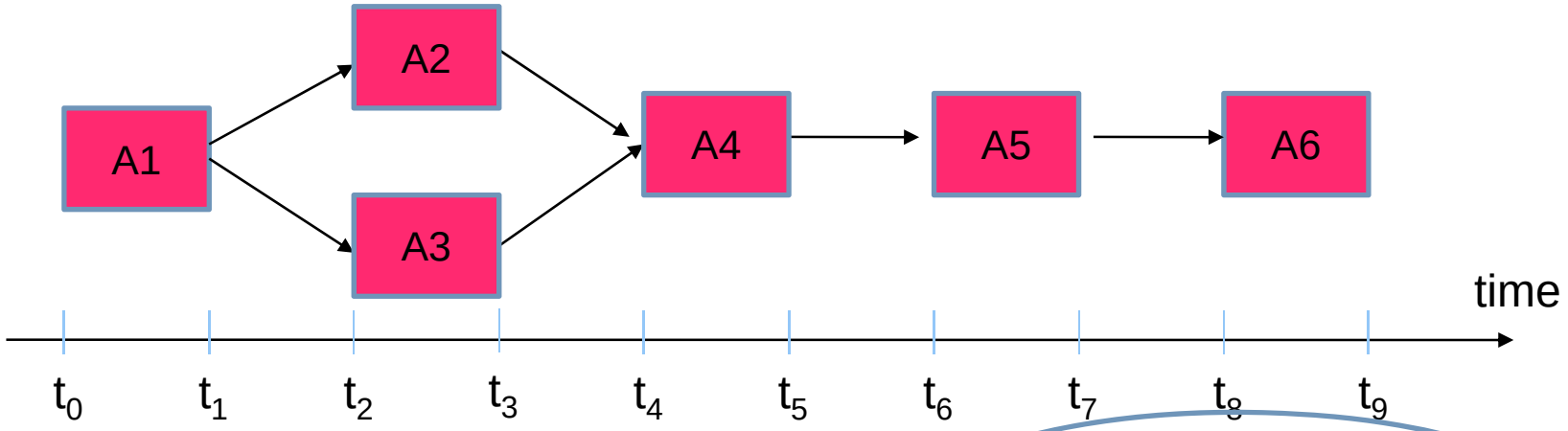
- RBAC erlaubt einem Benutzer, eine Rolle einzunehmen, die weniger Rechte hat, als er bekommen könnte

Usability/Benutzerunterstützung in Workflow-Systemen

- Teilnehmer am Workflow Lebenszyklus: Prozessmodellierer, Teilnehmer am Prozess, Administrator / Fall-Verantwortlicher

- Usability Aspekte
  - Visualisierung des Zustands einer Workflowinstanz
  - Security Policy für Workflows
  - Zuordnung von Akteuren im Workflow (z.B., Benutzer zu Rolle, Re-Assignments (z.B. Benutzer im Urlaub))
  - Modellierungs-Werkzeug
  - Prozessadaptionen

Business Process Visualizer and BP Policy (I)

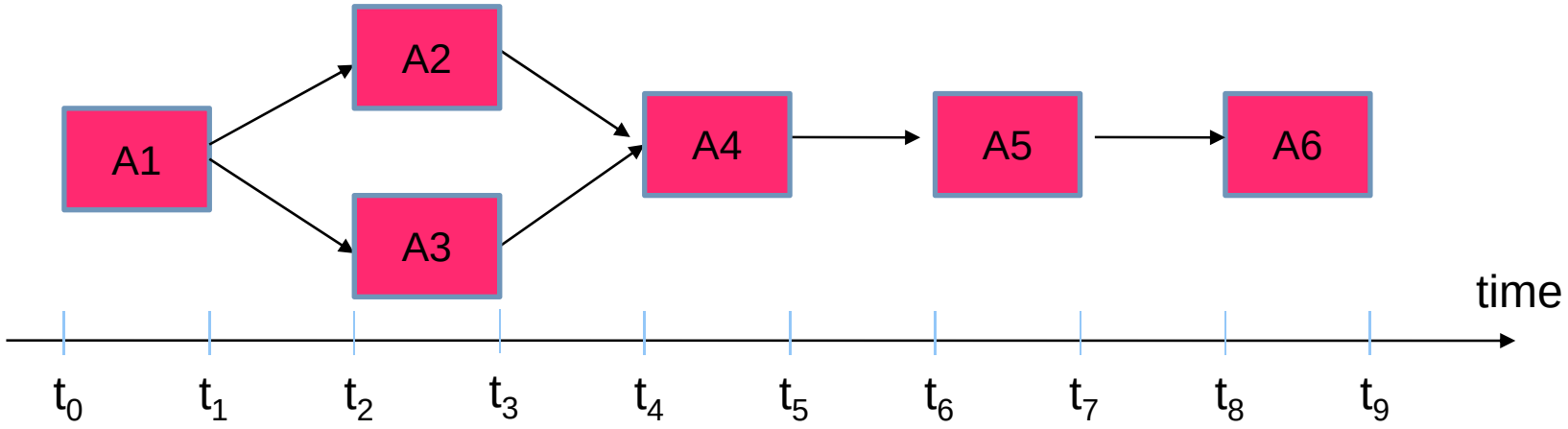


? **WHO will** access **WHICH** of my personal data in which way

persönliche Daten

[t_2,t_3]: Role: Coach, User:Smith, PII: mahara profile
[t_2,t_3]: Role: Clerk, User:Muelle, PII: affiliation (mahara profile)

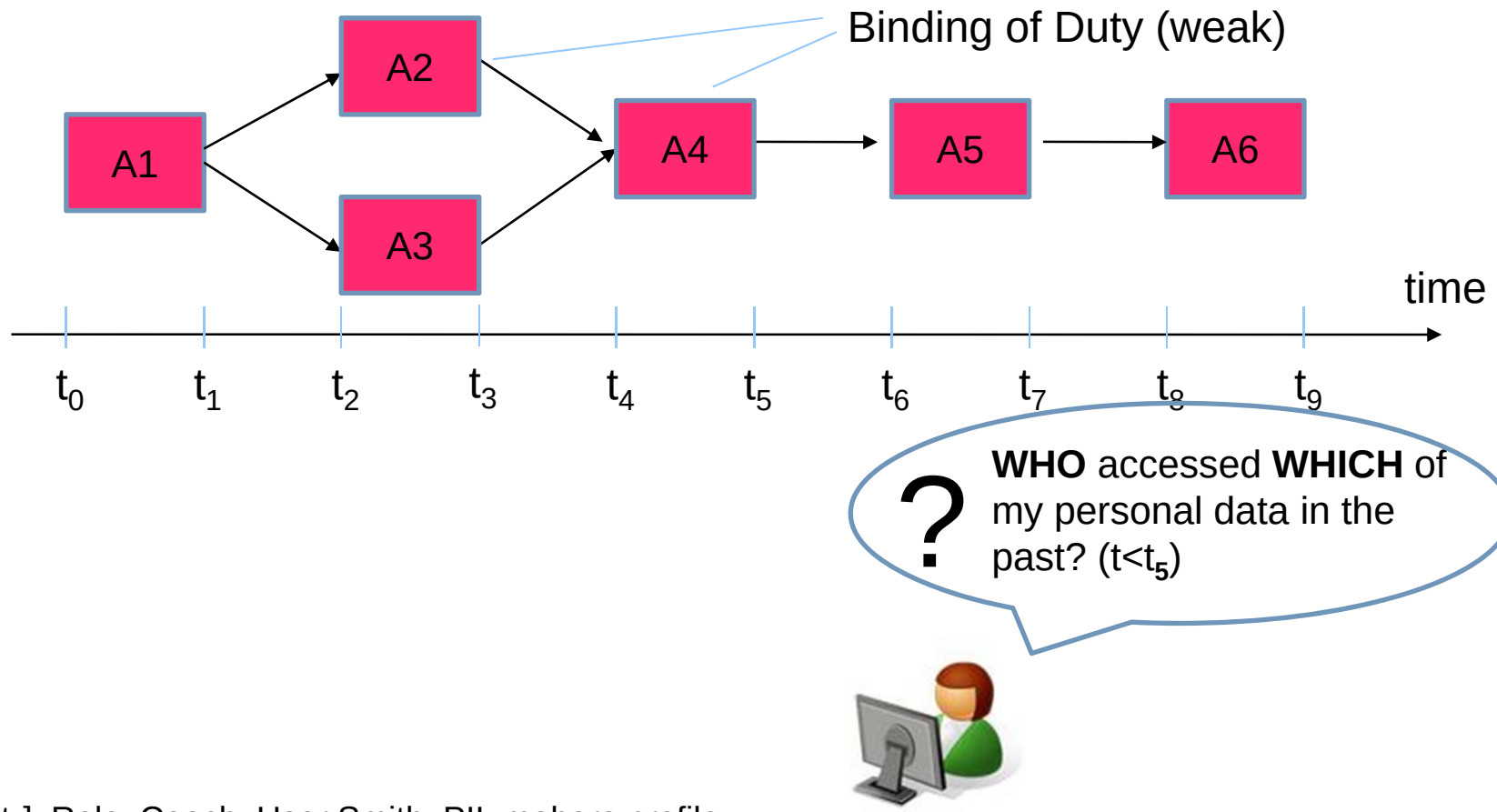
Business Process Visualizer and BP Policy (II)



? **WHO** will access **WHICH** of my personal data in the future? ($t>t_4$)

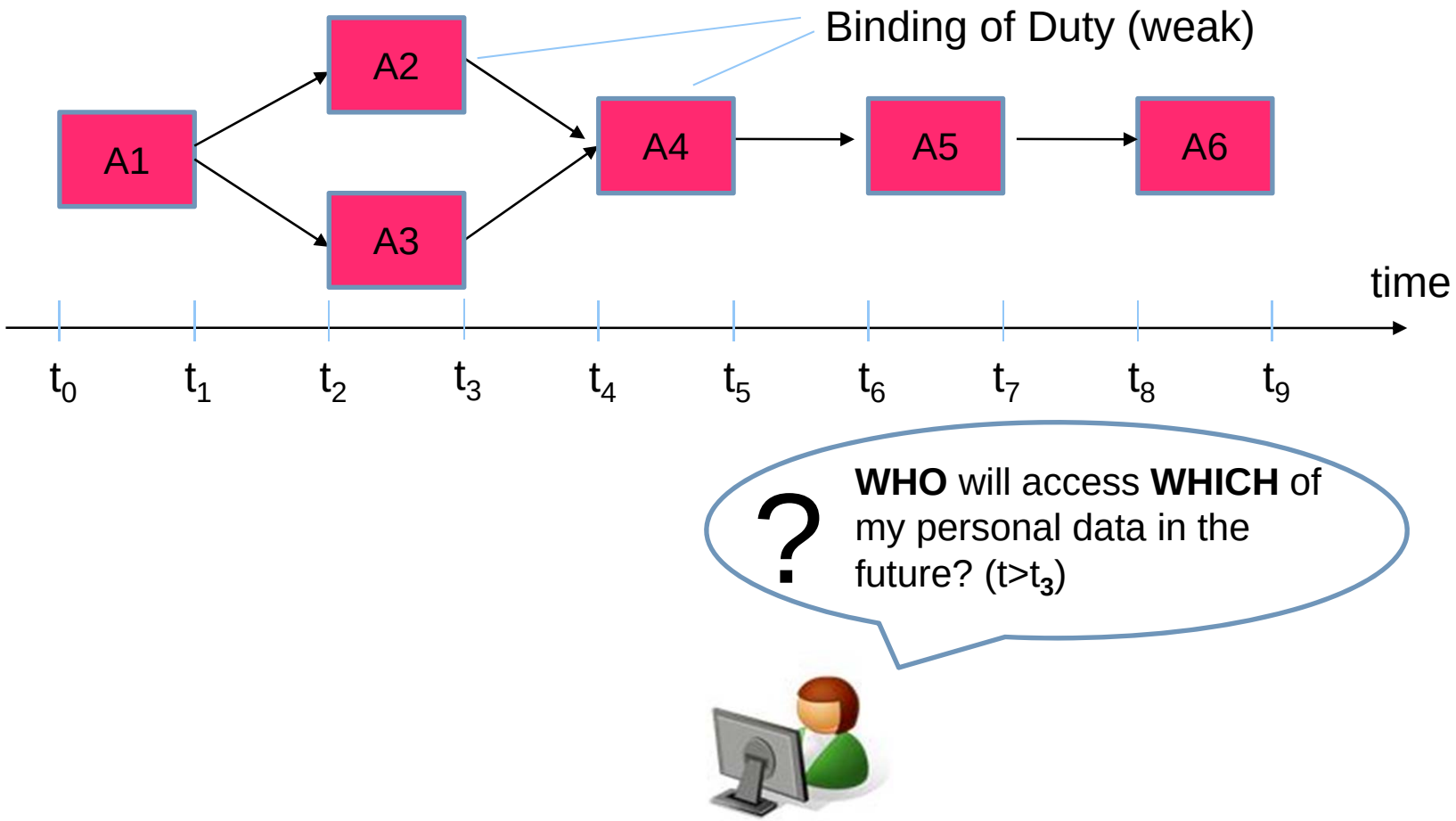
$[t_4,t_5]$: Role: Coach, User:Smith, PII: mahara profile
$[t_6,t_7]$: Role: Coach,delegation to Webservice „Matching“, rights: read; PII: certificates (mahara profile)

Business Process Visualizer and BP Policy (I)



$[t_2,t_3]$: Role: Coach, User:Smith, PII: mahara profile
$[t_2,t_3]$: Role: Clerk, User:Muelle, PII: affiliation (mahara profile)
$[t_4,t_5]$: Role: Coach, User:Hook, **Re-Assignment (Smith->Hook)**, PII: mahara profile

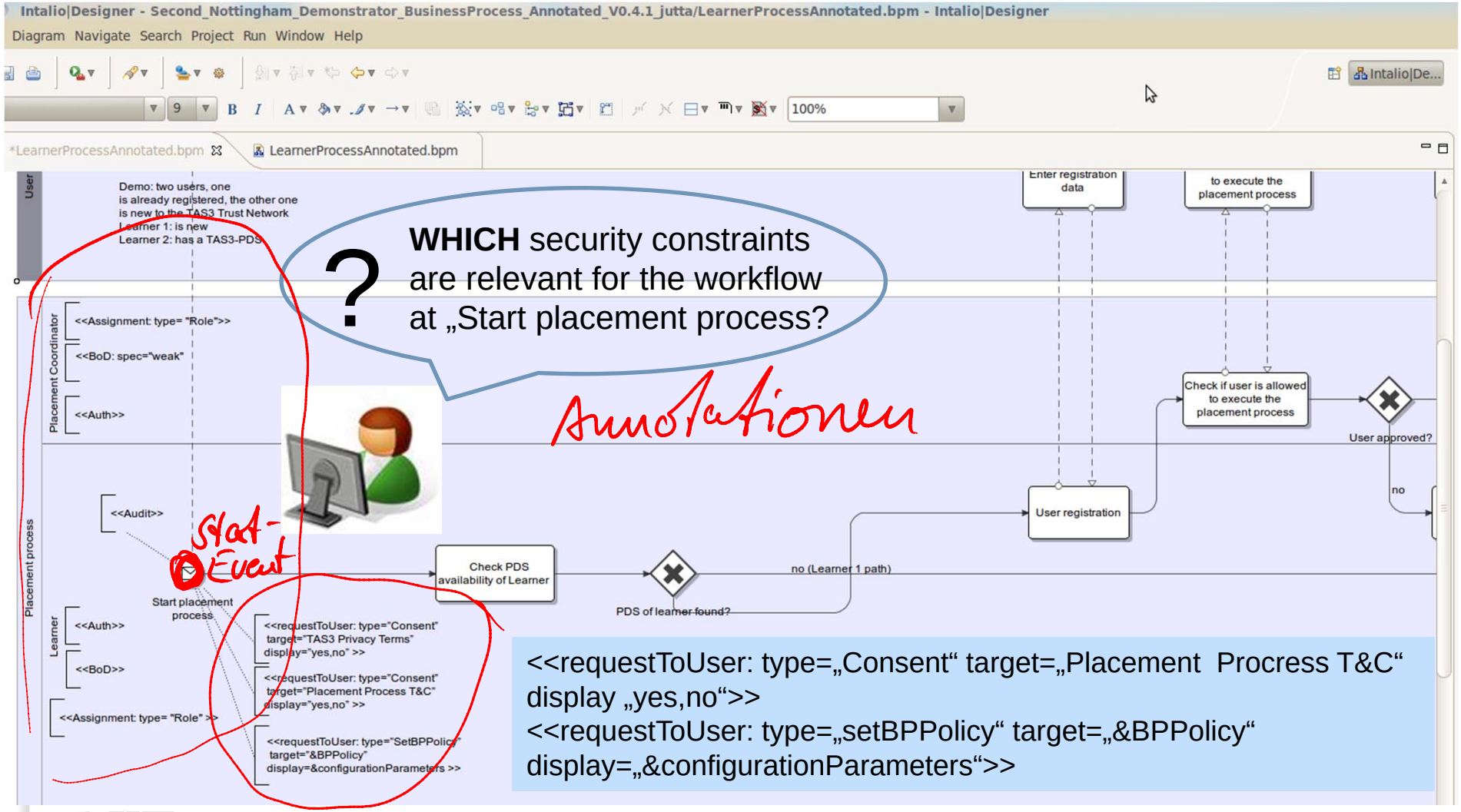
Business Process Visualizer and BP Policy (III)



$[t_4,t_5]$: Role: Coach, User:Smith (weak Binding of Duty), PII: mahara profile
$[t_6,t_7]$: Role: Coach,delegation to Webservice „Matching“, rights: read; PII: certificates (mahara profile)

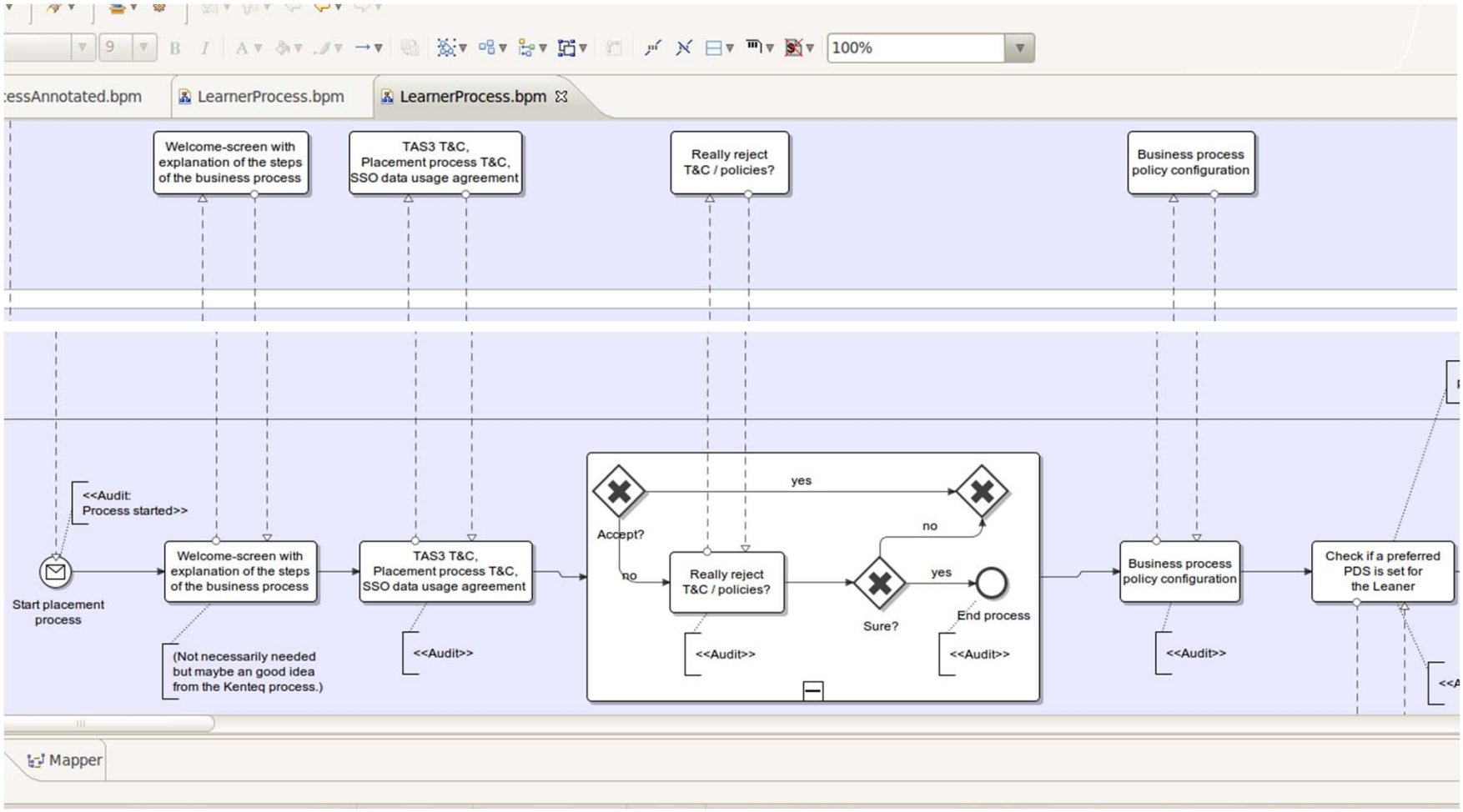
Business Process Modelling and Adaptation (I)

User: Business Process Modeller, Security Annotations of the Process Model



Business Process Modelling and Adaptation (II)

Transformation of Security Annotations: adapted business process



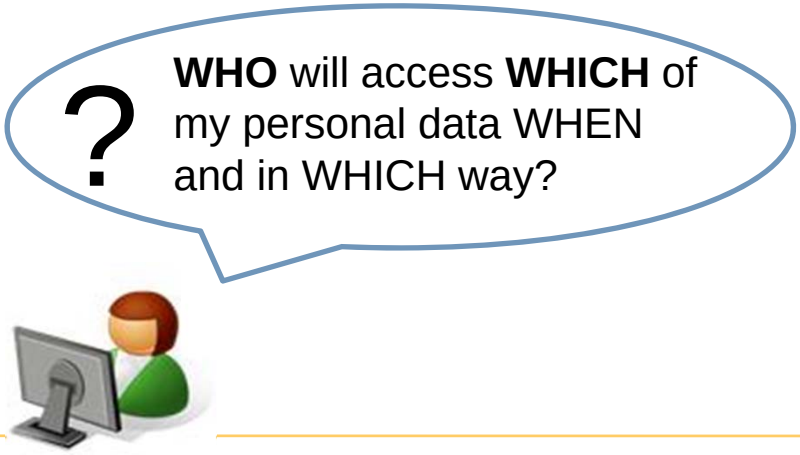
Business Process Modelling and Adaptation (IV)

Security Annotations allow to descriptively specify security constraints.

We support the modeller with an ontology using an adequate common vocabulary.

The result is

an adapted business process with user interactions and calls to the security framework,
and a business process security policy which provides a basis for informing the end-user about the relevant security constraints



WF Management für Wissenschaftliche Anwendungen

- Workflow Modell ist von Natur aus unvollständig
  - Konzepte sind nicht stabil
  - Prozesse sind häufig nicht im Vorhinein bekannt, z.B. Experimente.
- Notwendigkeit für dynamische Änderungen
  - Vorbereitete dynamische Änderungen (im Modellierungstool unterstützt).
  - Ad-Hoc dynamische Änderungen, unvorhergesehene Änderung und nicht vorbestimmbarer Zeitpunkt (häufig!).
- Haben meist keine API für Workflow-Kontrolle.
- Datenbank-basierte Verwaltung der Ablaufdaten.

Workflows um Kollaborationsmechanismen erweitert

- Beispiel klinischer Workflow
- Bei ärztlicher Untersuchung im Klinik-Workflow ergeben sich besondere Umstände. Der Arzt entscheidet sich zur (nicht vorgesehenen) Kooperation/Kollaboration mit einem Spezialisten an anderer Klinik.
- Danach Rückkehr zum ursprünglichen Klinik-Workflow und Anpassung an die neuen durch die Kollaboration erzielten Erkenntnisse.

Zusammenspiel Koordination und Kollaboration

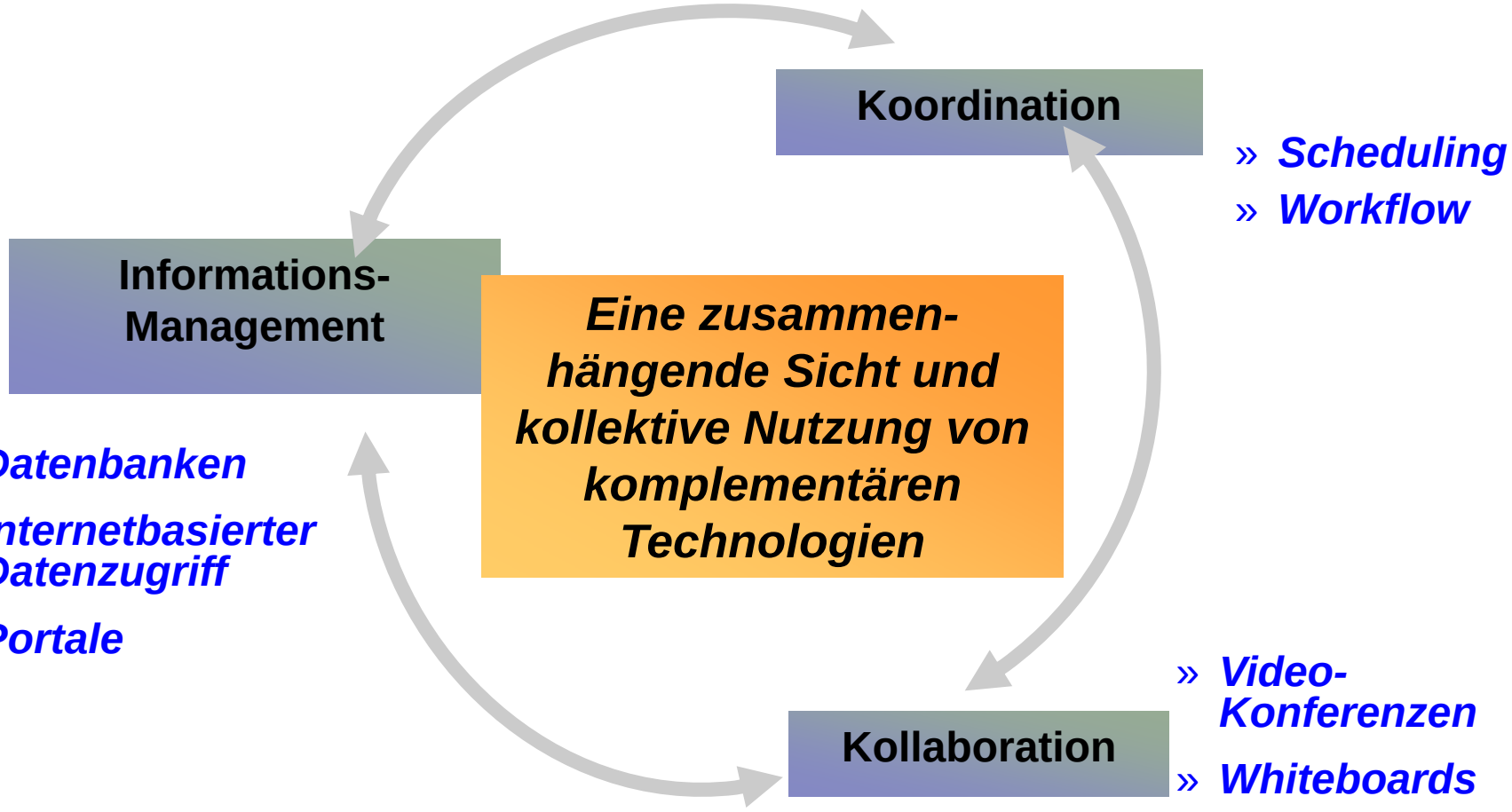
Interessante Fragestellungen:

- Wie könnte ein einheitliches Modell aussehen, um viele alle Formen der Kooperation zu unterstützen?
- Wie erfasst man die Ergebnisse einer Kollaboration? Wie kann man diese weiter (im Workflow) nutzen?

Formen der Verknüpfung von Kollaboration & Koordination

- Unterstützung der Zusammenarbeit vor dem koordinierten Ablauf
- Kollaborationsunterstützung in Workflows
- adaptive durch Koordination hervor gerufene Kollaboration

Vision


Koordination
» Scheduling
» Workflow
Informations-Management
» Datenbanken
» Internetbasierter Datenzugriff
» Portale
Eine zusammen-hängende Sicht und kollektive Nutzung von komplementären Technologien
Kollaboration
» Video-Konferenzen
» Whiteboards
» Applikations-Sharing

Exemplarische Fragen zu Kapitel 16

- Was sind Beispiele für aktuelle Forschungsthemen im Workflow-Bereich?
- Nennen Sie Zugriffsmechanismen, die wichtig sind im Zusammenhang mit WFMS?
- Was sind Aspekte der Benutzerunterstützung im Workflowmanagement?