Vorlesung Wintersemester 2011/12

Konzepte und Anwendung von Workflowsystemen

Kapitel 11:
Organisatorischer Aspekt/ Sicherheit & Privatheit

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

Überblick Kapitel 11

Organisatorischer Aspekt / Benutzerzuweisung in Workflow-Management-Systemen

- Motivation
- Überblick Aufgaben eines WfMS (organisatorischer Aspekt)
- Allokation von Ressourcen (Benutzern)

Sicherheit und Privatheit in WfMS

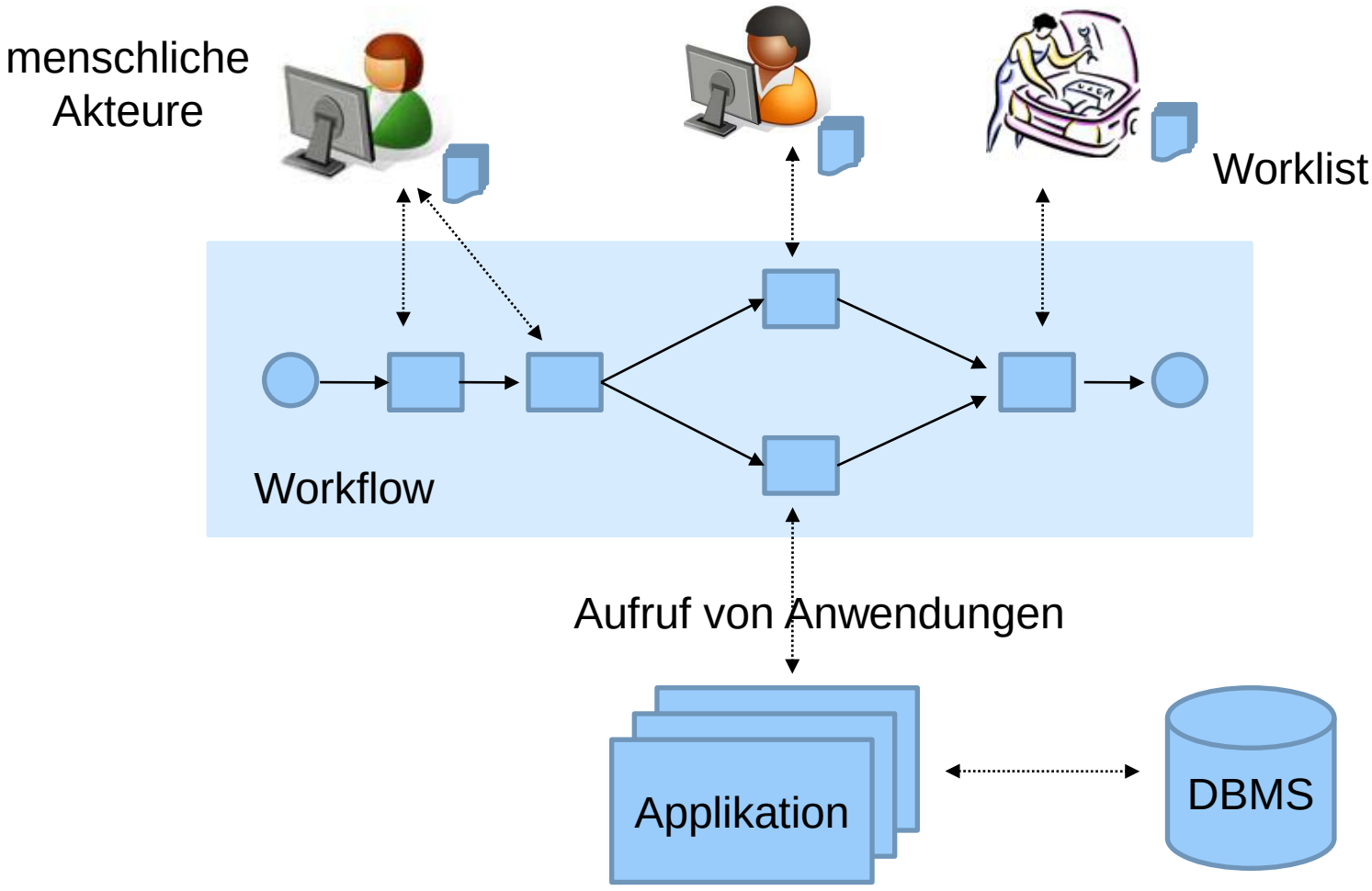
- Motivation
- Sicherheitsaspekte und Privatheit

Motivation

- WfMS Fokus auf Kontrollfluss
  - Welche Aufgaben (funktionaler Aspekt in WfMS) („*which tasks?*“)
  - Einbettung der Aufgaben im Kontrollfluß (verhaltensbezogener Aspekt in WfMS) („*how is the order?*“)

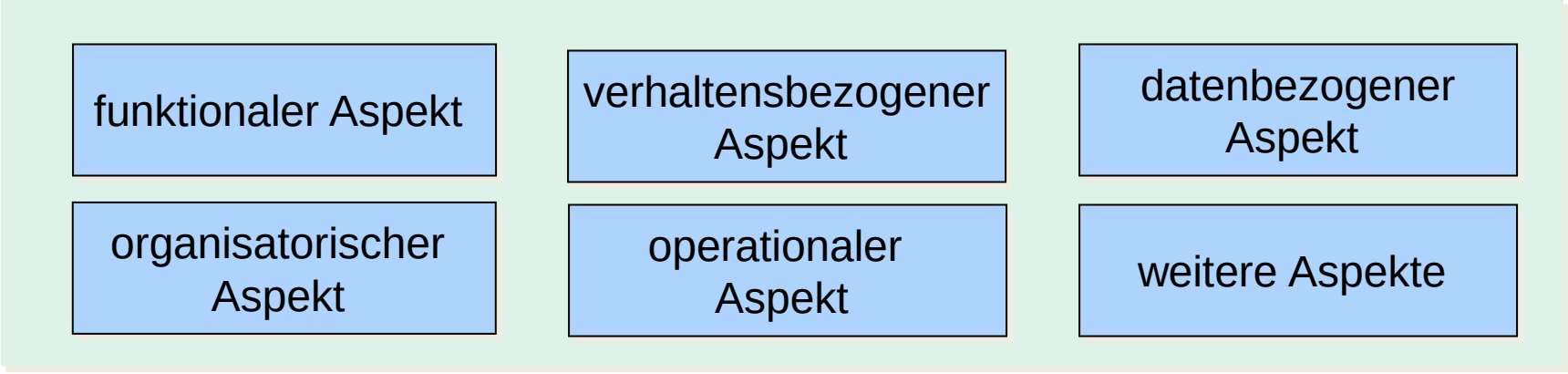
- Fragen in Bezug auf organisatorischen Aspekt in WfMS
  - Wer („*who ?*“) ist für die Ausführung der Aufgaben zuständig
  - Wie erfolgt die Zuordnung von Aufgaben zu Ressourcen
    - Art der Zuordnung beeinflusst Effizienz eines Workflows

Beispiel für Zuordnung



Aspekte von WfMS (Wdh. Kap. 2)

- **Organisations-Aspekt**: beschreibt die organisations-bezogenen Inhalte mit der **Definition von Organisationsstrukturen** und deren **Population**, sowie die Festlegung, **wer** die verschiedenen Operationen eines Workflows **ausführen kann/darf**



- **Organisations-Aspekt**: (erweitert), …… **wer** die verschiedenen Operationen **(Aufgaben)** eines Workflows **unter welchen Bedingungen ausführen kann/darf**

Aufgaben eines WfMS: organis. Aspekt

Koordination der Aufgaben hinsichtlich der verfügbaren Ressourcen

Daraus resultieren folgende Herausforderungen:

- Spezifikation von Ressourcen
- Spezifikation von Organisationsstrukturen und Rollenmodellen sowie deren Population
  - Statisch
  - Dynamisch (z.B. aktuelle Verfügbarkeiten)
- Zuordnung (Allokation) von Ressourcen zu Aufgaben
  - Einsatz einer oder mehrerer Strategien für Zuordnung
  - Rechtemanagement (impliziert durch Zuordnung)

Ressource

- Aufgabenträger, der für die Durchführung der Aufgabe (Task) zuständig ist
- Zeichnet sich durch Fähigkeit aus, diese Aufgabe durchzuführen
- Beispiele:
  - menschliche Akteure (Personen)
  - Sonstige Ressourcen (IT, Lager, Fahrzeuge, etc.)
- Eindeutig identifizierbar
- Limitierte Kapazität
- Ressourcenklasse: Gruppe von Ressourcen mit gleichen Eigenschaften
  - Eine Ressource kann zu mehreren Ressourcenklassen gehören
- Unterscheidung [v.d. Aalst]
  - Rolle: spezifiziert anhand funktionaler Eigenschaften (Qualifikation, „Skills“)
  - Position/Organisationseinheit: in der Organisationsstruktur eines Unternehmens eingegliedert

Rolle

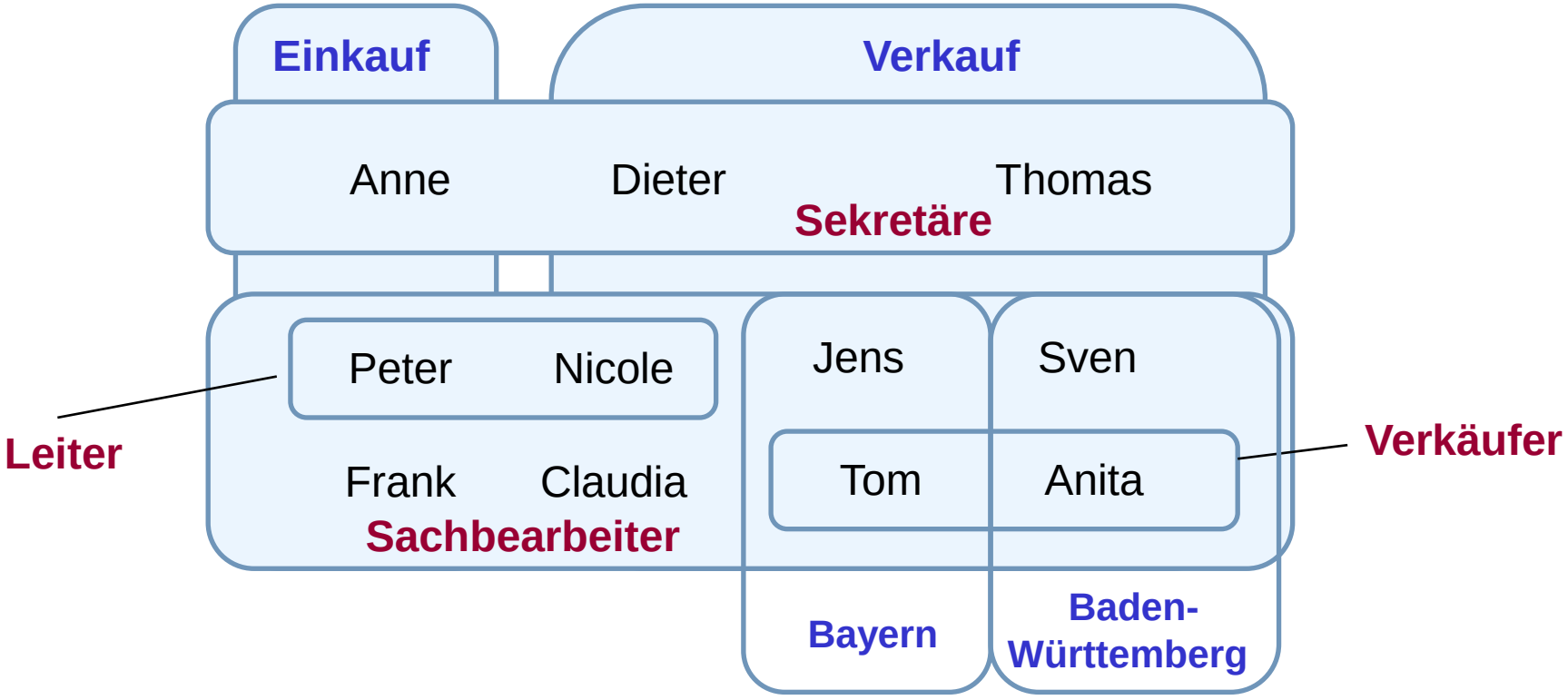
- Ressourcenklasse mit speziellen Fähigkeiten (Skills)
  - Beispiele: Fahrkarten-Verkäufer, Sachbearbeiter zur Schadensregulierung einer Versicherung, Professor, wissenschaftlicher Mitarbeiter, Student, System-Administrator, Assistenzarzt
- In Praxis: Gleichsetzung von Rolle mit Zuständigkeiten

- Durch Zuordnung von Rollen zu Aufgaben ist sowohl **Qualifizierung** als auch **Autorisierung** gewährleistet

Position/ Organisationseinheit

- Personen sind Teil einer/mehrerer Organisationen und sind dort organisatorischen Einheiten zugeteilt; haben üblicherweise dort eine **Position** inne
- Beispiele für organisatorische Einheiten: Einkauf, Produktion, Verkauf, Bereich Bayern, Bereich Baden-Württemberg
- Die Aufgaben und Privilegien dieser Person sind über die Position, nicht über die Person festgelegt
- Unterscheidung von Rollen und Positionen nicht immer möglich bzw. wird in Theorie und Praxis nicht konsequent umgesetzt
- Zuordnung zu Aufgabe (Task) spezifiziert, dass die richtige Organisationseinheit für die Ausführung zuständig ist

Beispiel Rollen und Organisationseinheiten



Organisationseinheiten

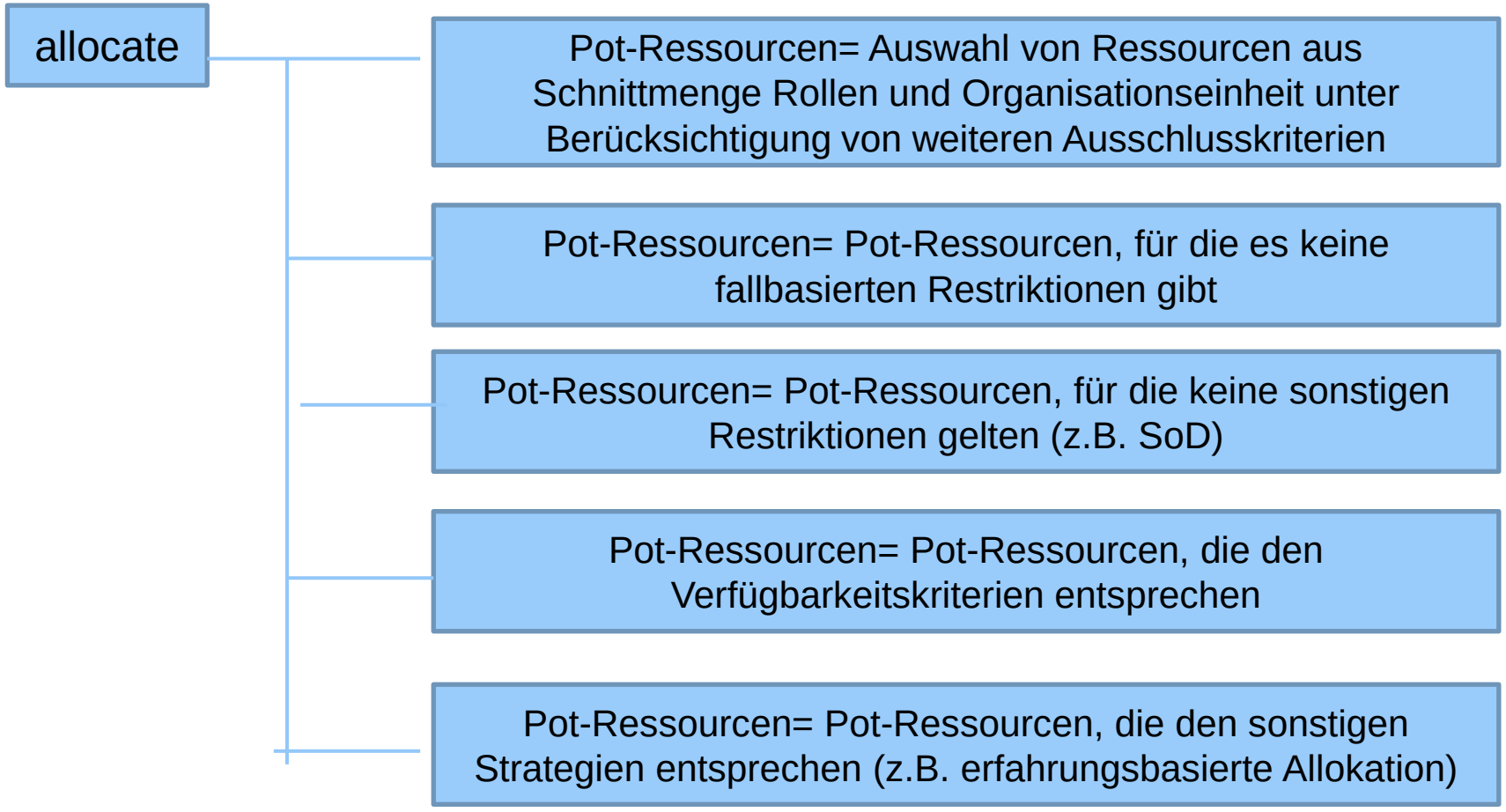
Rollen

Quelle: mod. nach v.d. Aalst

Allokation von Ressourcen

- Aufgabe der Workflow-Engine, die Allokation von Ressourcen (d.h. Auswahl von Prozessbeteiligten) durchzuführen
- Allokations-Prinzip: gewährleistet, dass jede Aufgabe (Task) von einer passenden Ressource umgesetzt wird:
  - Umsetzung von spezifizierten Bedingungen an die Ressource, die im Idealfall sowohl Rollen als auch Organisationseinheiten/ Positionen berücksichtigen
    - Ressource muss Schnittmenge beider sein
    - Komplexere Regeln möglich, z.B. Ausschluss von Organisationseinheiten
  - Potentielle Berücksichtigung von Fall-Attributen (Case)
    - Beispiel (Folie 10): Kundenstandort ist in Bayern, deshalb Auswahl der zuständigen Ressource (Rolle Verkäufer) aus dem Bereich „Bayern“ (-> Tom)
  - Berücksichtigung weiterer Bedingungen: z.B. SoD (Separation of Duties)
  - Je nach Strategie auch Berücksichtigung dynamischer Aspekte: z.B. momentane Arbeitsbelastung, Verfügbarkeit von Personen oder Umsetzung von strategischen Unternehmenszielen

Allokationsalgorithmus (vereinfacht)



Anmerkungen zum Algorithmus

- Schritte können teilweise ausgetauscht bzw. ausgelassen werden
- Je nach Strategie und Restriktionen diverse Zusatzaufgaben für das WfMS
  - Beispiele:
    - SoD erfordert Protokollierung der Historie der Allokationen
    - Erfahrungsbasierte Zuordnung erfordert Verwaltung früherer Fälle
- Mit Ergebnis „Pot-Ressourcen“ (Algorithmus) zwei Realisierungsoptionen:
  - 1. Variante: Das Work Item wird allen potentiellen Ressourcen angeboten; sobald eine Person das Work Item auswählt, wird der Verweis bei den anderen Personen gelöscht
  - 2. Variante: Auswahl genau einer Person zur Ausführung dieser Aufgabe (d.h. genau ein Verweis zu einem Work Item wird erzeugt)

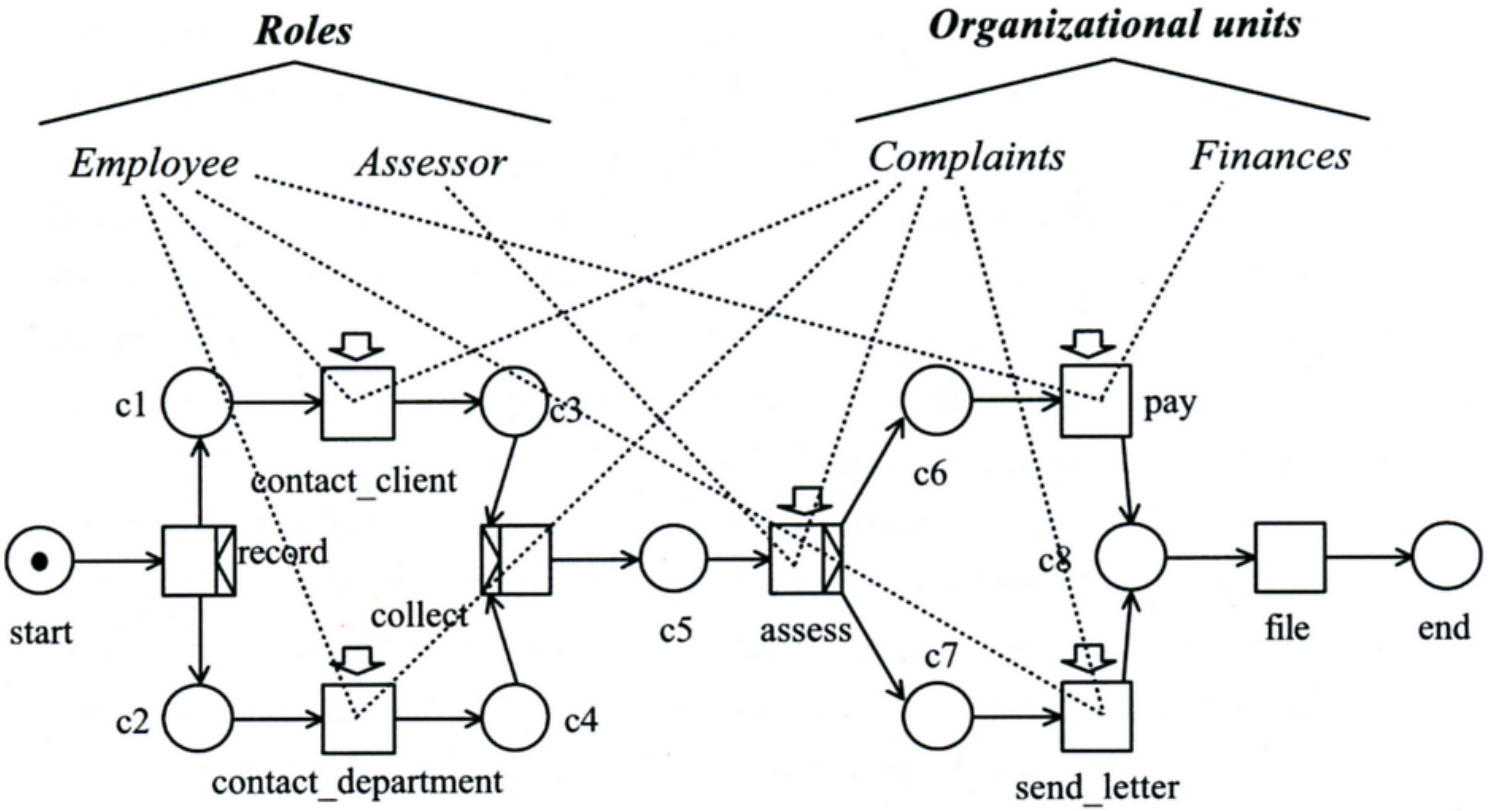
Begriffe (I)

- **Task** (Aufgabe, Arbeitsschritt): entspricht Aktivitäten des Schemas. Zu jeder Task kann eine beliebige Anzahl von Work Items assoziiert sein.
- **Work Item**: Arbeitsschritt einer Instanz, Status: „markiert“ (zur Laufzeit), d.h. kann bearbeitet werden, wird aber noch nicht ausgeführt. Jedes Work Item ist mit genau einer Task assoziiert.
- **Activity**: Ausführung eines Arbeitsschrittes (vorherige Zuordnung einer Ressource). Ein Work Item kann durch Allokation einer Ressource in eine Activity transformiert werden.
- **Work List**: Menge der Aufgaben, die eine Ressource durchzuführen hat (exklusiv oder Allokation an alle)

Begriffe (II)

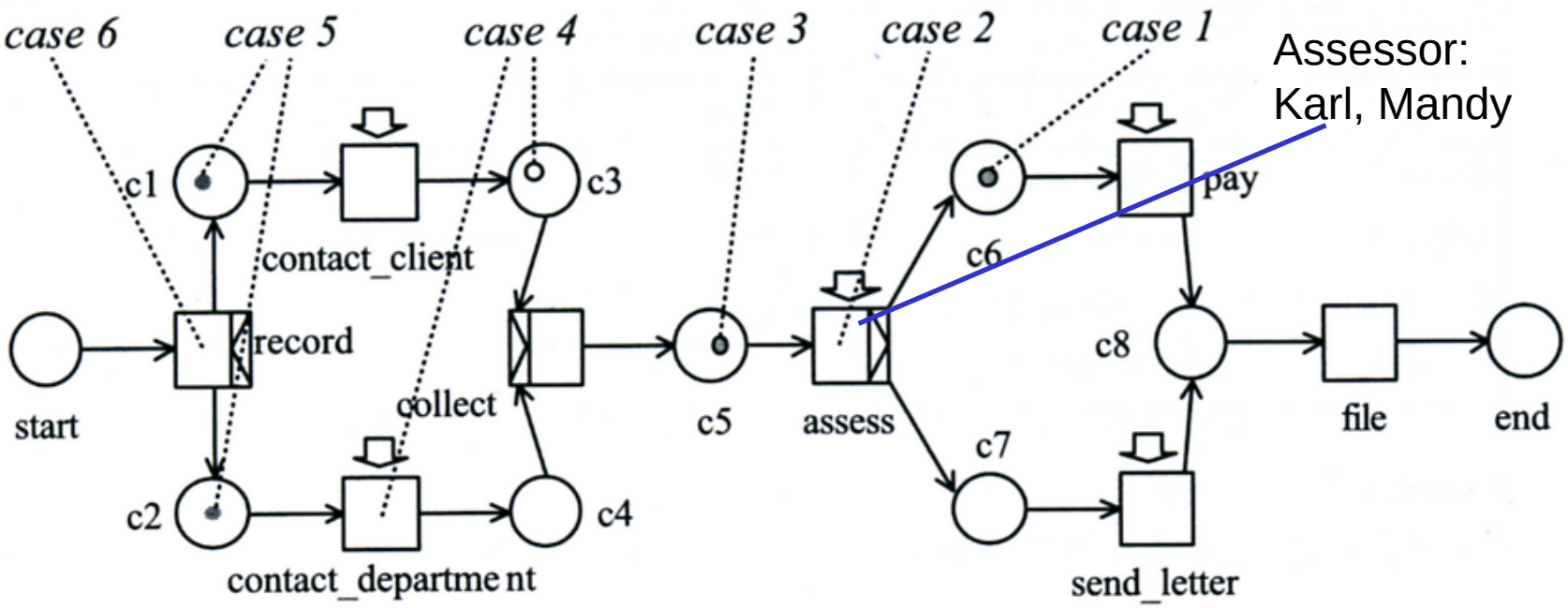
- Ein **Schedule** ist eine Liste von Work Items, für die eine Ressource ihre Zustimmung bezüglich der zukünftigen Abarbeitung gegeben hat.
- Ein **Work Log** (History) ist eine Liste von Work Items, die eine Ressource in der Vergangenheit beendet hat.

Beispiel Beschwerdemanagement (I)



Quelle: v.d. Aalst

Beispiel Beschwerdemanagement (II)



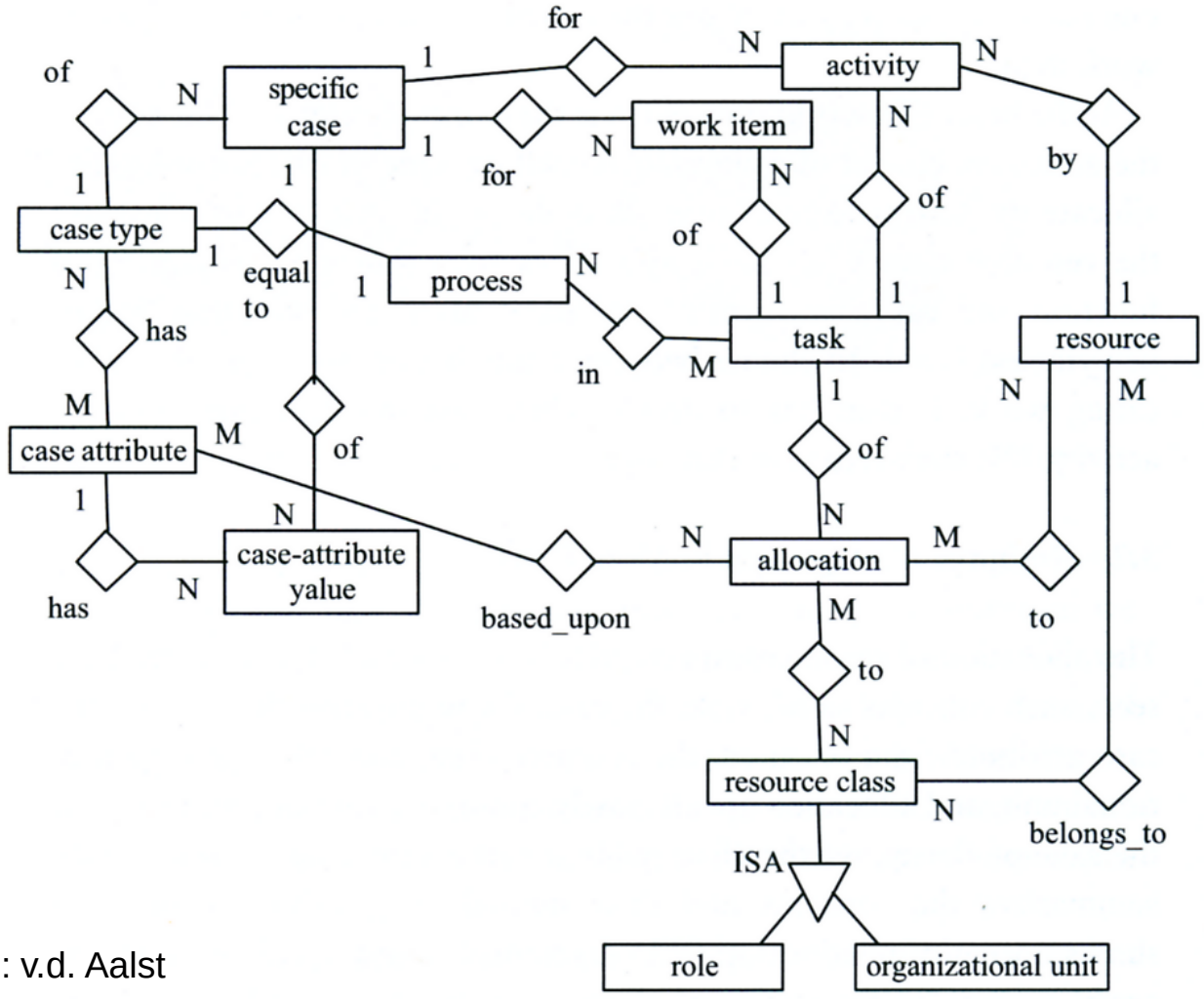
Work items

Case	Task
Case 1	pay
Case 3	**assess**
Case 5	contact_client
Case 5	contact_dept.

Activities

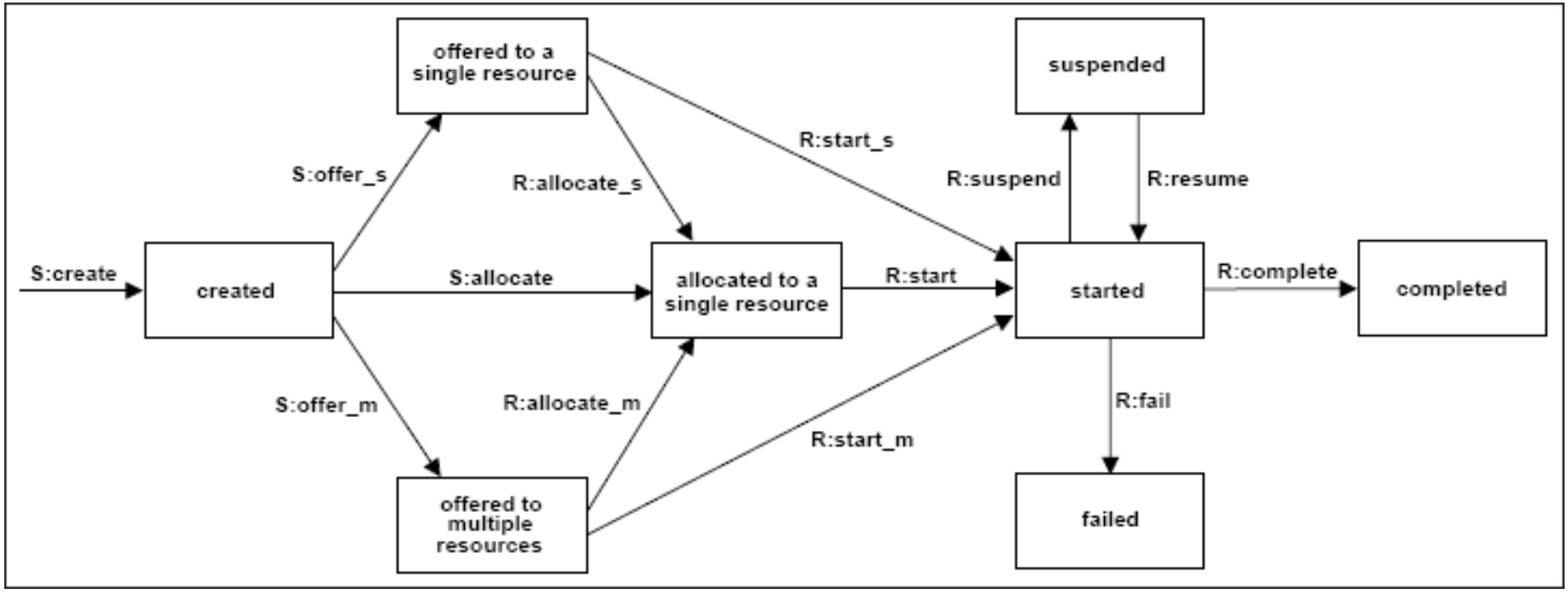
Case	Task	Resource
Case 2	assess	**Mandy**
Case 4	contact_dept.	Jim
Case 6	record	-

Allokation (ER-Diagramm)



Quelle: v.d. Aalst

Lebenszyklus eines Work Items (Zustands-Übergangs-System)



Allokationsmechanismen (I)

- **Direkte Allokation**
  - Zuordnung einer konkreten Person beim Entwurf
  - gleichwertig mit rollen-basierter Allokation, falls nur eine Person diese Rolle inne hat
  - Nachteil: negative Auswirkung auf Flexibilität
    - Anpassungsaufwand
    - Blockierung der Ausführung einer Workflow-Instanz bei Nicht-Verfügbarkeit der Person
  - Vorgehen: http://www.workflowpatterns.com/patterns/resource/creation/wrp1_animation.php
- **Abgeleitete Allokation („Deferred Allocation, Deferred Distribution“)**
  - Spezifikation der Zuordnung beim Entwurf, explizite Auswahl zur Laufzeit
  - Optionen: direkte Allokation oder Berücksichtigung von Rollen
  - Vorgehen: http://www.workflowpatterns.com/patterns/resource/creation/wrp3_animation.php

Allokationsmechanismen (II)

- **Rollen-basierte Allokation**
  - Wichtigster Ressourcen-Allokations-Mechanismus in WfMS
  - Grundverständnis: alle Personen, die einer bestimmten Rolle zugeordnet sind, sind „funktional“ (*skills*) gleichwertig; alle Rolleninhaber können somit eine Aufgabe (Task) ausführen
  - Vorgehen: jedem Task (Aufgabe) eines Workflow-Schemas wird beim Entwurf eine Rolle zugeordnet
  - **Role Resolution** (zur Laufzeit!): Abbildung der Rollen auf Personen; dabei werden im Idealfall Informationen über Verfügbarkeit von Personen berücksichtigt
  - Vorteile: positive Auswirkung auf Flexibilität
    - keine Anpassung des WF-Schemas bei personellen Wechsel (z.B. Ausscheiden) notwendig
    - Nur verfügbare Personen werden berücksichtigt, keine Blockierung des Ablaufs der Workflow-Instanz
  - Vorgehen: http://www.workflowpatterns.com/patterns/resource/creation/wrp2_animation.php

Allokationsmechanismen (III)

- **Organisatorische Allokation**
  - Nicht Rollen, sondern Positionen innerhalb einer Organisation werden genutzt
  - Beispiele:
    - Krankenhaus: OP wird von HNO-Chirurgen durchgeführt, dieser ist verantwortlich (nicht generell Rolle Arzt)
    - Unternehmen: Leiter einer Abteilung, von der eine Bestellung ausgeht, muss unterschreiben
  - Vorgehen:
    - http://www.workflowpatterns.com/patterns/resource/creation/wrp10_animation.php

Restriktionen bei Zuordnung (I)

- „Separation of Duties“ (SoD) („Separation of Function“)
  - Explizite Trennung der Bearbeitung von Aufgaben innerhalb einer Rolle
  - Ziel: Vermeidung von Missbrauch, Sicherheitskriterien innerhalb eines Prozesses (Vier-Augen-Prinzip)
  - Beispiel: Bearbeitung und Unterschrift eines Antrages
  - Umsetzung: http://www.workflowpatterns.com/patterns/resource/creation/wrp5_animation.php
- Delegation
  - Möglichkeit der potentiellen Übertragung von Ausführungsrechten an andere
  - Flexibilität bei Ausführung (z.B. Aufweichung der „Case Handling“-Bedingung bei lang laufenden Workflow-Instanzen)

Restriktionen bei Zuordnung (II)

- Case Handling
  - Motivation: gewisse Aufgaben, die bearbeitet werden sollen, benötigen ein Gesamtverständnis des Falles
  - (in diesem Kontext:) eine Person bearbeitet alle „Work Items“
  - Vorteile:
    - Fehlervermeidung (durch Kenntnisse des Falles)
    - Reduzierung der Bearbeitungszeit (keine Einarbeitung nötig)
    - Besserer Service zum Kunden
  - Vorgehen: http://www.workflowpatterns.com/patterns/resource/creation/wrp6_animation.php
- Binding of Duties (BoD)
  - Ähnlich wie Case Handling, kann im Ggs. dazu auf Menge von Tasks eingeschränkt werden
  - Motivation u.a.: „retain familiar“ (Binden einer Untermenge der Aufgaben)

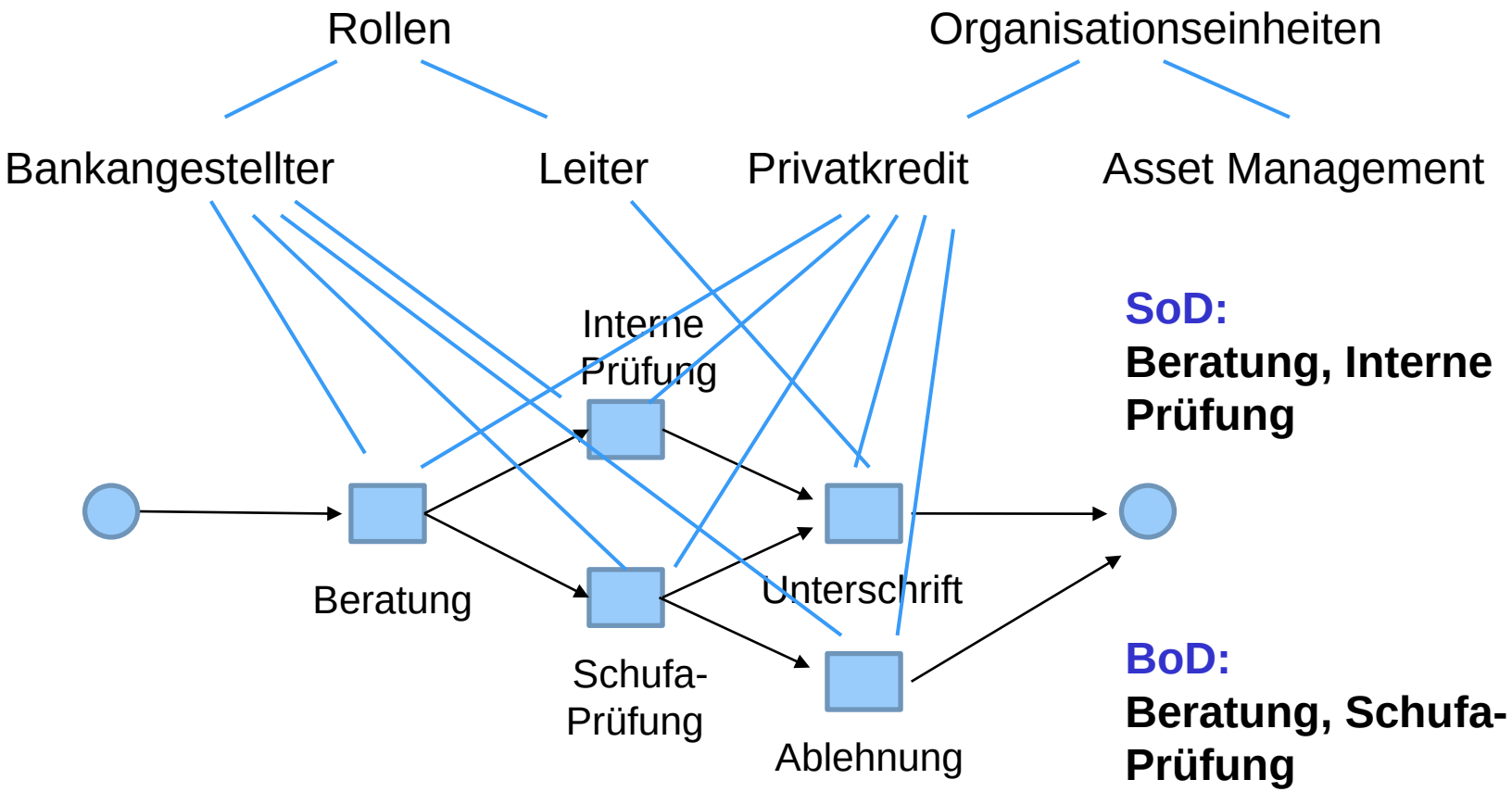
Restriktionen bei Zuordnung (III)

- **Verlaufs-basierte Allokation („History-Based Allocation“)**
  - Idee: Zuordnung einer Ressource zu einem Work Item basiert auf der Ausführungshistorie
  - auch andere Workflow-Instanzen werden hier berücksichtigt
  - Ziel: Allokation anhand beispielsweise persönlicher Erfahrungen und Expertisen, die nicht in Rollen ausgedrückt wird
  - Beispiele:
    - Person, die am längsten eine Task nicht mehr ausgeführt hat
    - Person, die die Task am erfolgreichsten ausgeführt hat
    - Ressource mit der kürzesten Bearbeitungszeit
    - konkrete Ansprechperson, die für die Kommunikation mit einem Kunden verantwortlich ist („one face to the customer“)
  - Notwendigkeit der Repräsentation dieser Information
    - Umsetzung: jede Task hat beispielsweise eine historische Verteilungsfunktion bezüglich der Kriterien
  - Vorgehen: http://www.workflowpatterns.com/patterns/resource/creation/wrp9_animation.php

Beispiele für Unterstützung organisatorischer Aspekte in kommerziellen Systemen

- Staffware (TIBCO)
  - Relativ einfaches Modell von Gruppen und Rollen, starke Einschränkung bei Rollen (jede Rolle kann nur von einer Person belegt sein)
- WebSphere MQ Workflow (IBM)
  - Sowohl Organisationsmodelll als auch Rollenmodell
- FLOWer (Pallas Athena)
  - Nur rollen-basiert (Rollenhierarchie)
- COSA Business Process Management (COSA)
  - Sowohl Organisationsmodell als auch Rollenmodell
- iPlanet (Sun)
  - Eingeschränktes Organisationsmodell
- Details zur Unterstützung der einzelnen Workflow Patterns -> Literaturreferenz

Beispiel für Zuordnung: Kreditantrag bei Bank (I)



Beispiel für Zuordnung: Kreditantrag bei Bank (II)

- 1. Schritt: Bankangestellter UND Abteilung Privatkredit
  - Markus Meier
  - Monika Müller
  - Simone Schmitt
  - Andreas Fischer
- 2. Schritt: fallbasierte Restriktion der Bank: Bei Beratung und Produktabschlüssen dürfen keine familiären Beziehungen zum Kunden bestehen
  - Frau Monika Müller ist Schwägerin vom Kunden Herrn Schultze (Kreditantragsteller)
    -> Frau Müller wird für die Bearbeitung ausgeschlossen
- 3. Schritt: SoD, BoD
  -> Beratung und Schufa-Prüfung kann von Hr. Fischer, Hr. Meier, oder Fr. Schmitt durchgeführt werden

Beispiel für Zuordnung: Kreditantrag bei Bank (III)

- 4. Schritt: keine Einschränkungen bzgl. der Verfügbarkeitskriterien
- 5. Schritt: Bankstrategie zur Allokation: der erfolgreichste Berater (d.h. derjenige mit den meisten Kreditabschlüssen) soll bei der Allokation bevorzugt werden

  -> Frau Schmitt wird als erfolgreichste Bankangestellte für die Beratung allokiert (und für Schufa-Prüfung, BoD)

  -> das Work Item Beratung wird Frau Schmitt zugeteilt

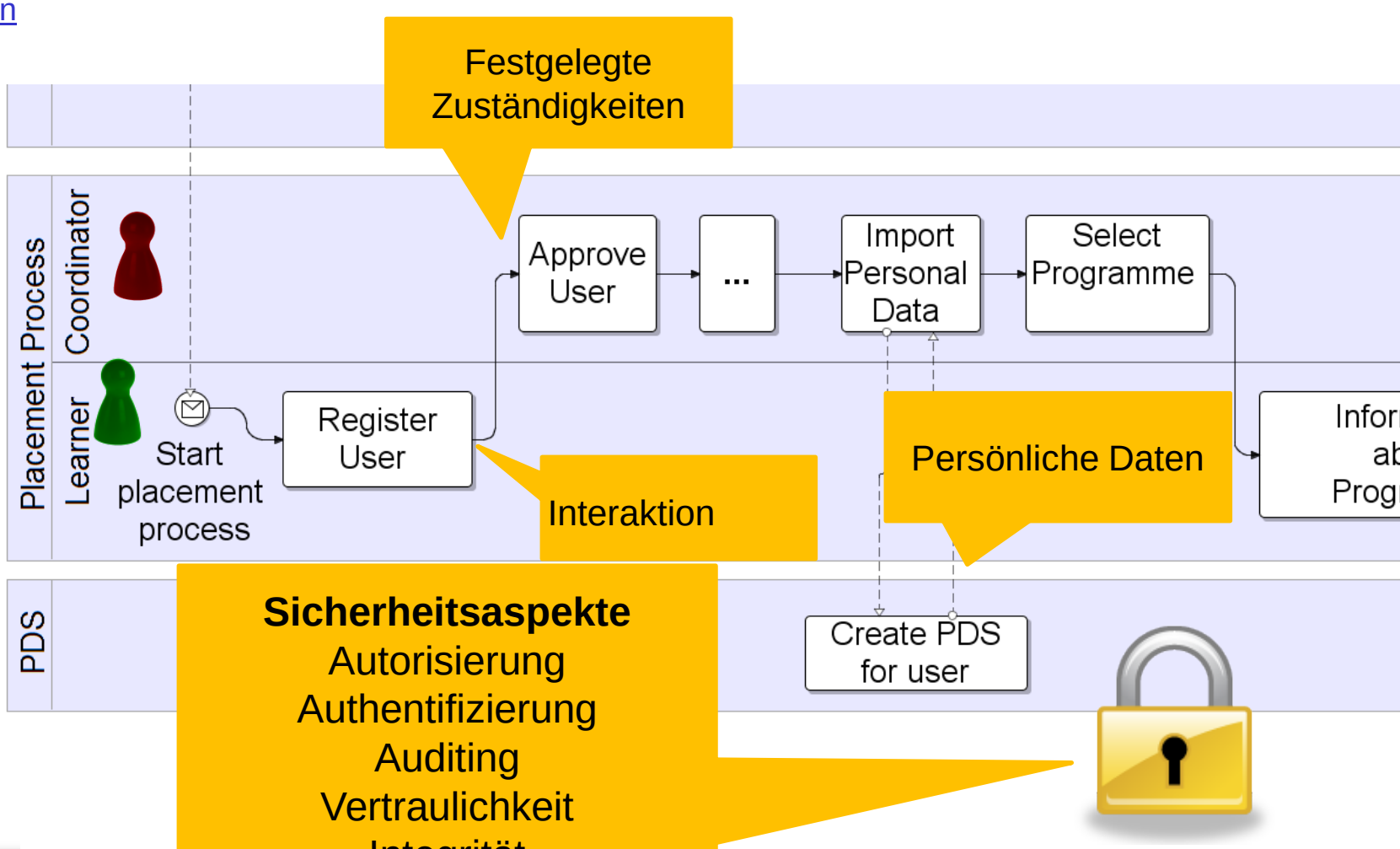
  -> Hr. Meier oder Hr. Fischer sind somit für die Prüfung zuständig (SoD)

  -> Sobald Frau Schmitt mit der Beratung fertig ist, wird u.a. das Work Item Prüfung aktiviert.

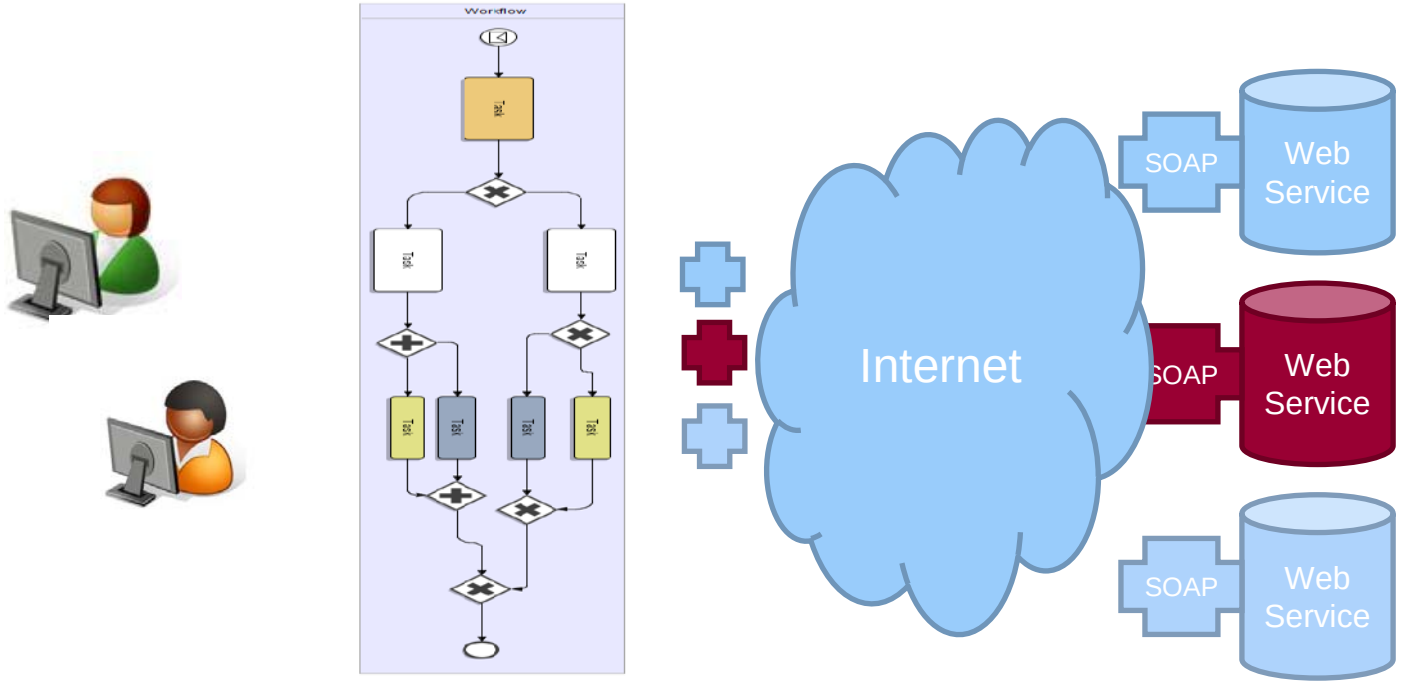
  -> Hr. Meier und Hr. Fischer wird das Work Item „Prüfung Kreditvergabe“ zugeteilt. Hr. Fischer selektiert das Work Item und führt den Arbeitsschritt durch. Durch die Zustimmung von Hr. Fischer wird das Work Item bei Hr. Meier entfernt

  -> …….

Motivation Sicherheit in Workflows
Beispiel Praktikumsvermittlung



Service-orientierte Architekturen (SOA) und Workflows



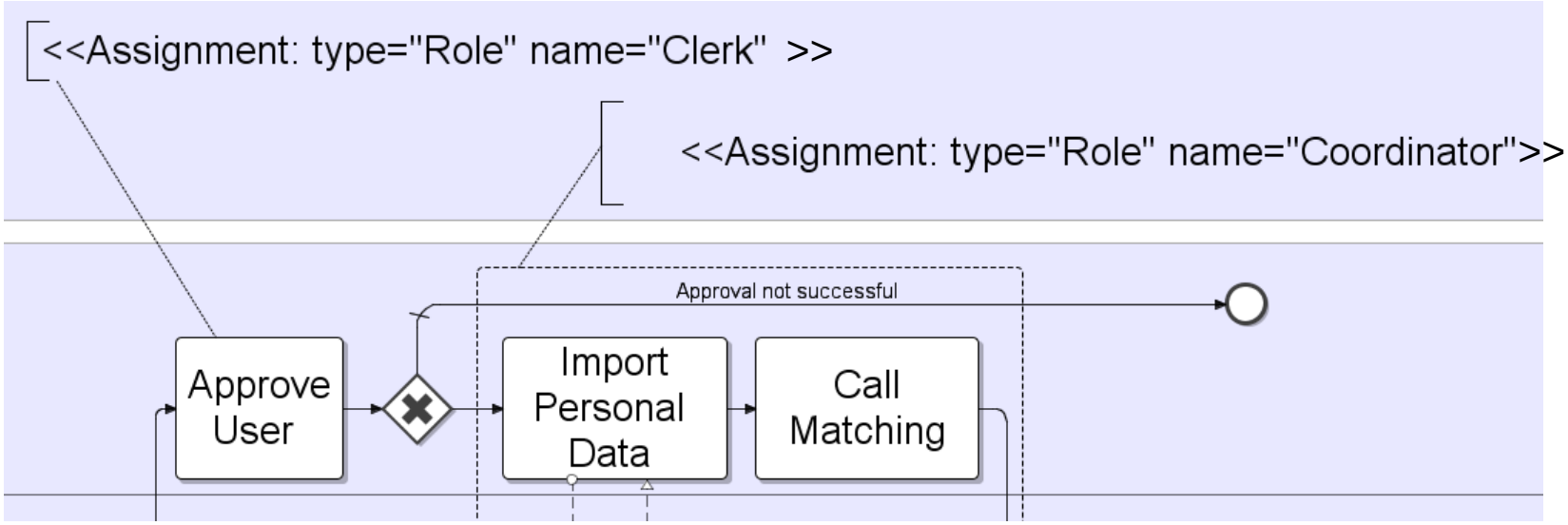
- SOA: lose gekoppelte Services in einem Netzwerk
- Workflow-Management-System (WfMS) koordiniert Prozesse durch Service-Aufrufe
- Interaktionen mit Akteuren

Sicherheits-Facetten in SOA

Autorisierung (I)

- Rechtevergabe an Akteure oder Web Services zur Durchführung von Aufgaben (Aktivitäten) bzw. zum Zugriff auf Daten
- -> siehe Organisatorischer Aspekt (wer kann/**darf** Aufgabe durchführen)
- Role Assignment“ (Rollenzuweisung)
  - Autorisierung von Rolleninhabern zur Ausführung einer Aufgabe
- „Assignment Mechanism“ (Allokationsmechanismus)
  - Zuordnung der Aufgaben an Rolleninhaber (z.B. Erfahrungsgrad, Kundenbetreuer)
- „User Assignment“
  - Direkte Zuordnung eines Benutzers

Beispiel Spezifikation „Role Assignment“



Mögliche Umsetzung: Darstellung von Sicherheitsbedingungen im WF-Modell

- Autorisierung von Aufgabe „Approve User“ durch Rolleninhaber von „Clerk“
- Analog Gruppe von Aufgaben („Import Personal Data, „Call Matching“) durch Rolleninhaber von „Coordinator“

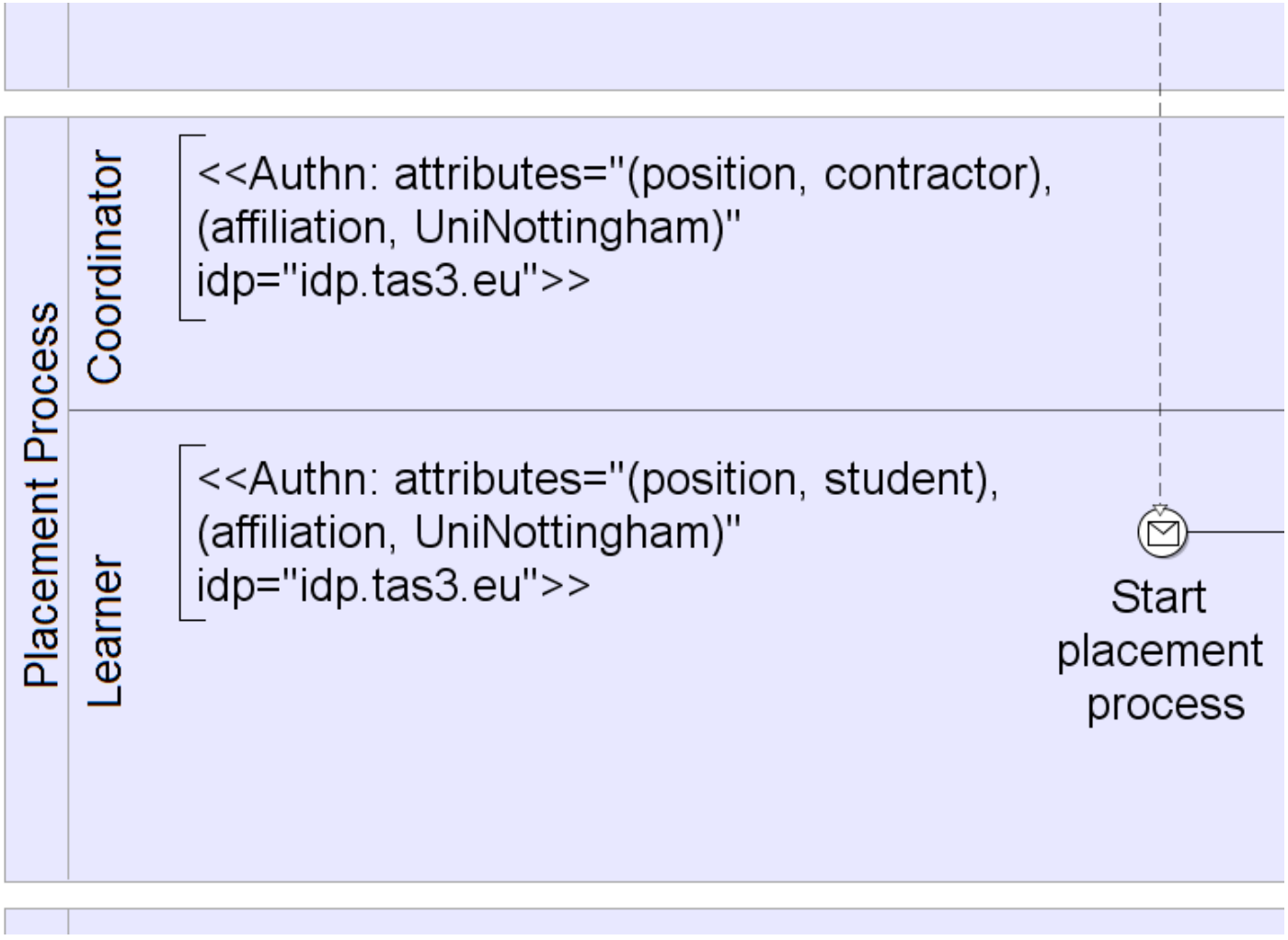
Autorisierung (II)

- Workflow-spezifische Einschränkungen
  - „Separation of Duty“ (Pflichtentrennung)
    - Aufgaben müssen von **unterschiedlichen** Benutzern durchgeführt werden
    - Motivation oft zusätzliche Sicherheit (z.B. 4-Augen-Prinzip)
  - „Binding of Duty“ (Pflichtenbindung)
    - Aufgaben müssen vom **gleichen** Benutzer durchgeführt werden
- Delegation von Rechten
  - Für Zugriffe auf Daten
    - Grundverständnis: Ausführungsrechte von Aufgaben implizieren Zugriff auf Daten
    - Sonderfälle: externe Dienste (Web Services), explizite Zugriffsbeschränkungen auf Daten
  - zur Ausführung von Aufgaben

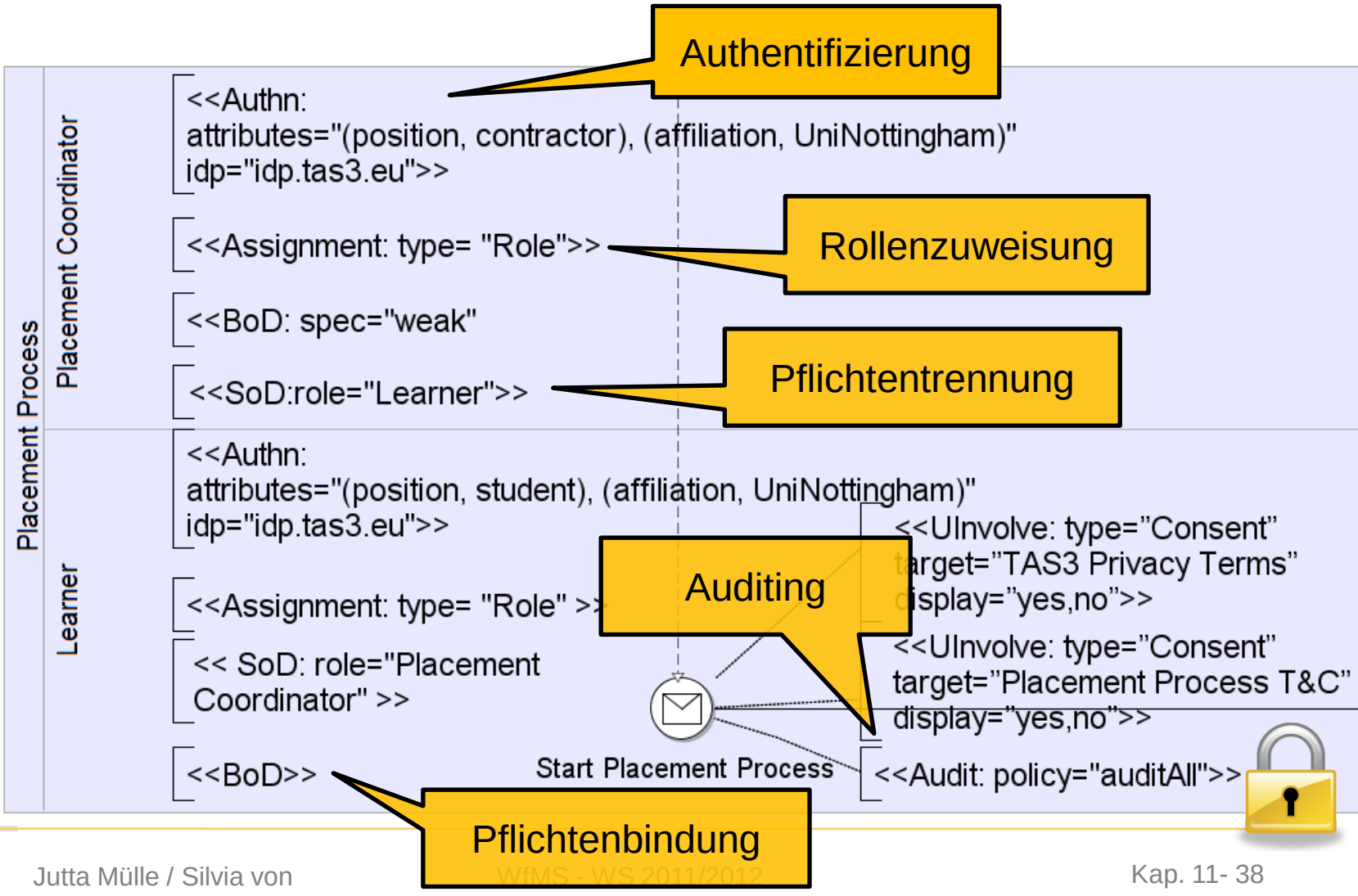
Weitere Sicherheitsfacetten in Workflows

- Authentifizierung
  - Identifikation von Beteiligten
    - Attribut/Werte-Paare
    - Bestätigung durch Identity-Provider
- Vertraulichkeit von Datenflüssen
  - Verschlüsselung/ Signatur
- Datenintegrität
  - Korrektheit und Schutz vor unberechtigter Manipulation der Daten
- Auditing
  - Motivation: Nachvollziehbarkeit der Workflow-Ausführung (gesetzliche Bestimmungen)
  - Protokollierung (Logging)

Beispiel Spezifikation Authentifizierung



Beispiel zur Spezifikation von Sicherheit Annotationen im WF-Modell



Umsetzung von Sicherheit in WfMS

- Basismechanismen in WfMS verfügbar
  - Rollenkonzepte zur Autorisierung
- Nicht hinreichend unterstützt
  - Eingeschränkte Autorisierungen (z.B. für Bereiche des Workflows)
  - Separation of Duty (SoD), Binding of Duty (BoD)
  - Rechtemanagement für Daten
- Umsetzung von Sicherheitsaspekten durch proprietäre Software-Erweiterungen
  - aufwändig, kostspielig

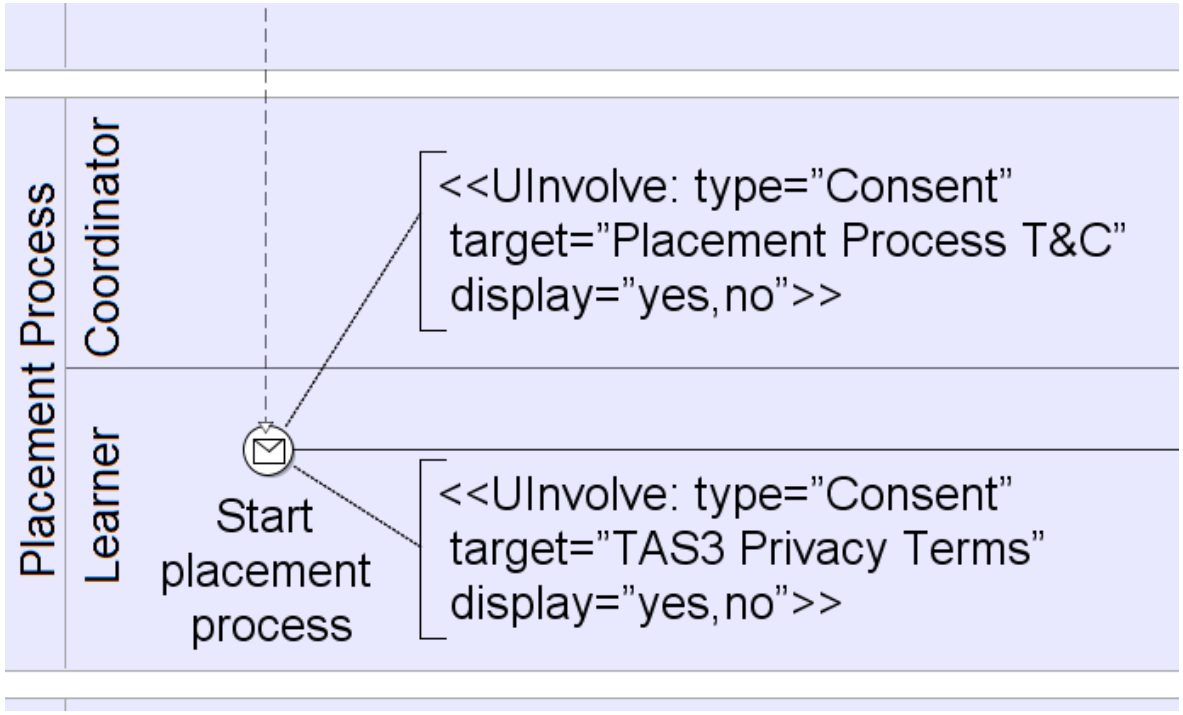
„Privacy“ und „Trust“ in Workflows (I)

- Personenbezogene Daten
  - Beispiele: Einkaufsverhalten, sensible Daten (medizinische Daten, Zeugnisse)
  - Schutz vor unberechtigtem Zugriff auf Daten
  - Rechtliche Rahmenbedingungen (z.B. Zustimmungen, Nachverfolgung → Auditing)
  - Trust (Reputation) von beteiligten Web Services, die Zugriff auf personenbezogene Daten haben bzw. die diese verarbeiten

„Privacy“ und „Trust“ in Workflows (II)

- Einbeziehung der sog. „Betroffenen“
  - Berücksichtigung persönlicher Präferenzen
    - Regelungen für Datenzugriffe
    - Informationspolitik (Notifikationen) bzgl. Umsetzung von Richtlinien
    - Auswahl von Services zur Speicherung personenbezogener Daten anhand der Reputation (Trust-Level)
    - Feedback von Web Services
  - Trust-Feedback nach Nutzung von Services
  - Einwilligung zu Geschäftsbedingungen (z.B. Terms & Conditions)

Beispiel Spezifikation „Consent“



Mögliche Umsetzung von Privatheitsaspekten (Zustimmungen):

Darstellung von Spezifikationen der Betroffenen im WF-Modell

Exemplarische Fragen zu Kapitel 11

- Welche Aufgaben umfasst der Organisationsaspekt eines WfMS?
- Was versteht man unter Work Items? Beschreiben Sie kurz den Lebenszyklus von Work Items.
- Beschreiben Sie rollenbasierte Allokation.
- Diskutieren Sie vergangenheits-basierte Allokationsmechanismen hinsichtlich der Umsetzung von strategischen Unternehmenszielen.
- Beschreiben Sie kurz Sicherheits- und Privatheitsaspekte in WfMS.
- Was versteht man unter SoD und BoD?

Ergänzende Literatur zu Kapitel 11

- Will van der Aalst und Kees van Hee: Workflow Management: Models, Methods, and Systems, 2002 (Kapitel 3)
- Mathias Weske: Business Process Management: Concepts, Languages, Architectures, 2007 (Kapitel 3.8)
- Workflow Resource Patterns
  - http://www.workflowpatterns.com/patterns/resource/
  - http://www.workflowpatterns.com/documentation/documents/Resource%20Patterns%20BETA%20TR.pdf