

Design und Realisierung von E-Business- und Internet-Anwendungen

„Exkurs“

Identity Management

Dr. Kirsten Bönisch et al.,
Prof. Dr. Heinz-Gerd Hegering
SoSe 2006

Identity Management

Zielsetzung und Gliederung der Vorlesung

Das Identity Management beschäftigt sich mit der Fragestellung „Wie kann sicher gestellt werden, den richtigen Identitäten zum richtigen Zeitpunkt, solange wie nötig, auf eine effiziente und nachvollziehbare Art und Weise berechtigten Zugang zu verschaffen?“

- n Einführung Identity Management
 - Definition und Zielsetzung
 - Schwerpunkte
- n Vertiefung ausgewählte Themenfelder
 - Fachliche Beschreibungen („Fachkonzept“)
 - Rollenmanagement
 - Zulassungsmanagement/eProvisioning
 - Federated Identity Management
- n Praxisbeispiel zur Standardisierung

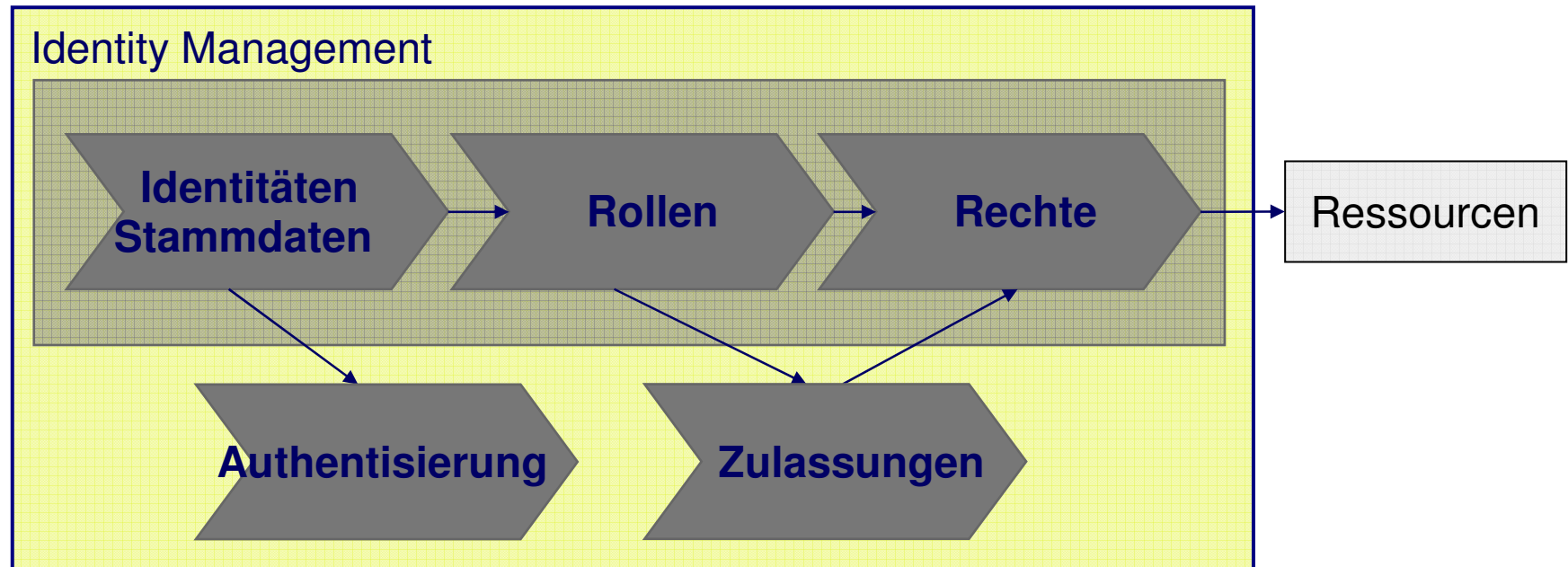
Identity Management Agenda

- n Einführung Identity Management
 - Definition und Zielsetzung
 - Schwerpunkte
- n Vertiefung ausgewählte Themenfelder
 - Fachliche Beschreibungen („Fachkonzept“)
 - Rollenmanagement
 - Zulassungsmanagement/eProvisioning
 - Federated Identity Management
- n Praxisbeispiel zur Standardisierung
 - Der Odette UAM-Standard zum Einsatz von Web Services für unternehmensübergreifendes Benutzermanagement



Einführung Identity Management

Definition und Zielsetzung



Identity Management behandelt

n Identitäten von

- Personen
- Organisationen
- technischen Objekten (Geräten)

einschließlich deren

n Authentisierungs-/Autorisierungsinformationen

d.h.

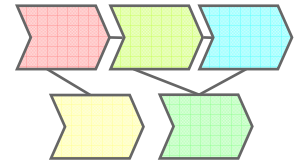
- Stammdaten
- Paßworte, Zertifikate etc.
- Rollen
- Zulassungen
- Rechte

Einführung Identity Management

Aufgabenfelder & Schwerpunktthemen

- n Benutzerverwaltung
- n Rollenmanagement
- n Zulassungsmanagement / e-Provisioning
- n Rechtemanagement
- n Authentisierung
 - Paßwortmanagement
 - Starke Authentisierung (PKI, SecurID, ...)
- n Technische Objekte
- n Auditierbarkeit
- n Standardisierung / Federated Identity Management
- n ...

Einführung Identity Management Prozesse



Aufgeführte fünf „Cluster“ als übergreifender Rahmen für die Modellierung der relevanten Standardprozesse

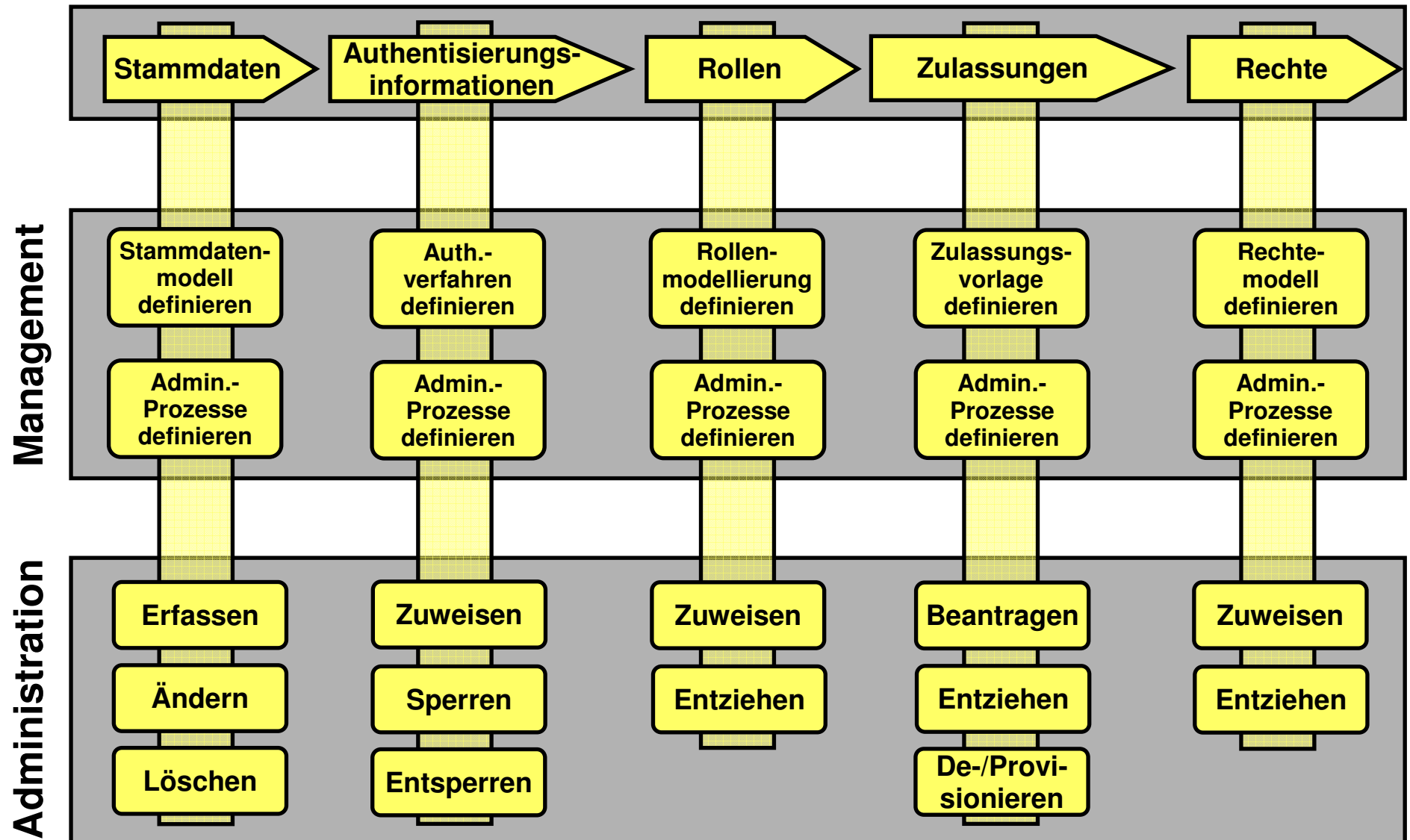
Managementprozesse

- n welche Objekte werden in den Clustern behandelt
- n wie werden die Prozesse für diese Objekte definiert

Administrationsprozesse

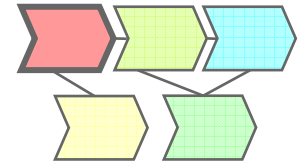
- n Vorgaben zur Verwaltung der Objekte
- n zentrale oder dezentrale Administration
- n Durchführungsverantwortung liegt dann bei den Administratoren!

Einführung Identity Management Prozesse



IdM Schwerpunktthemen

Identitäten und Stammdaten



n **Stammdaten:**

- eindeutige Beschreibung einer Identität
- wesentliche Grunddaten eines Unternehmens
- bleiben über gewissen Zeitraum unverändert

n **Identität:** selbständig Handelnde

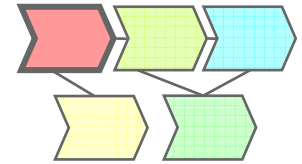
- juristische oder natürliche Person
- technisches Objekt/System (z.B. "Fahrzeuge" oder „Steuergeräte“, die ohne explizite Initiierung mit Anwendungssystemen kommunizieren)
- besteht aus einer Anzahl von Attributen
- Mindestanzahl als Voraussetzung zur Anlage einer Identität

n Natürliche Personen können mehrere Identitäten haben

n Das **Stammdaten-Management** legt fest:

- die Prozesse für das Management der Stammdaten
- welche Stammdaten zu welchem Identitätstypen definiert werden
- das Format der Attribute

Vertiefung: fachliche Beschreibung Anwendungsfälle („Use Cases“)

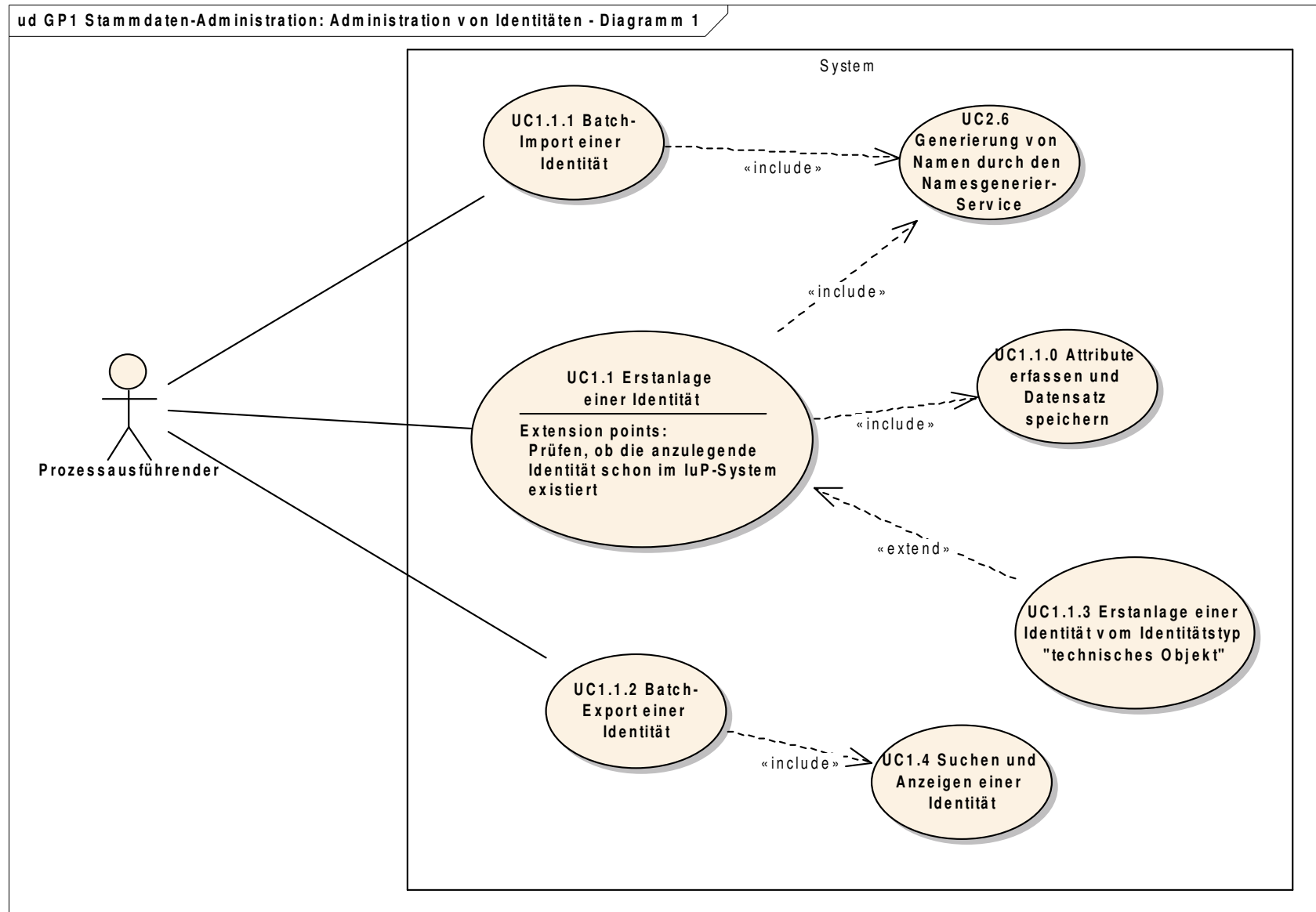


Beispiel: Administration von Identitäten

- UC1.1 Erstanlage einer Identität
 - UC1.1.0 Attribute erfassen und Datensatz speichern
 - UC1.1.1 Batch-Import einer Identität
 - UC1.1.2 Batch-Export einer Identität
 - UC1.1.3 Erstanlage einer Identität v. Identitäts
- UC1.2 Löschen einer Identität
- UC1.3 Modifizieren der Stammdaten / erw. Stan
- UC1.4 Suchen und Anzeigen einer Identität
- UC1.5 temporäres Deaktivieren einer Identität
- UC1.6 Reaktivieren einer temporär deaktivierten Identität
- UC1.7 Vergabe von Berechtigungen zur Administration von Identitäten
- UC1.8 Entzug von Berechtigungen zur Administration von Identitäten
- UC1.9 befristete Aufnahme einer Identität in einen Kontext
- UC1.10 Entfernen einer Identität aus einem Kontext
- UC1.11 Deaktivieren einer Kontextmitgliedschaft
- UC1.12 Reaktiveren einer Kontextmitgliedschaft

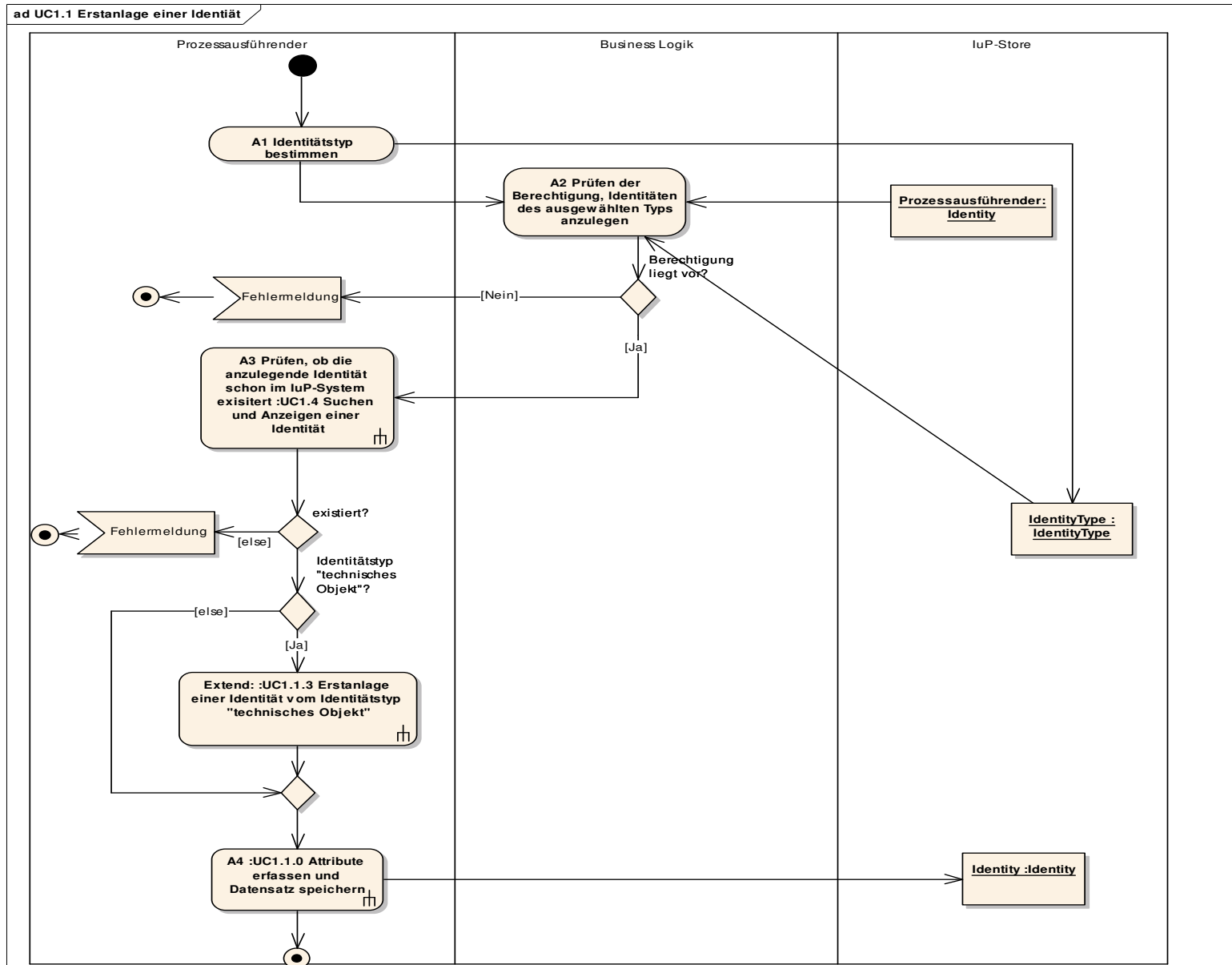
*Kurzbeschreibung
Auslösendes Ereignis
Vorbedingung
Nachbedingung
Aufrufvarianten
Kontrollfluss
Exceptions
Sequenzdiagramm*

Fachliche Beschreibung von Anwendungsfällen Diagramm/Abhängigkeiten



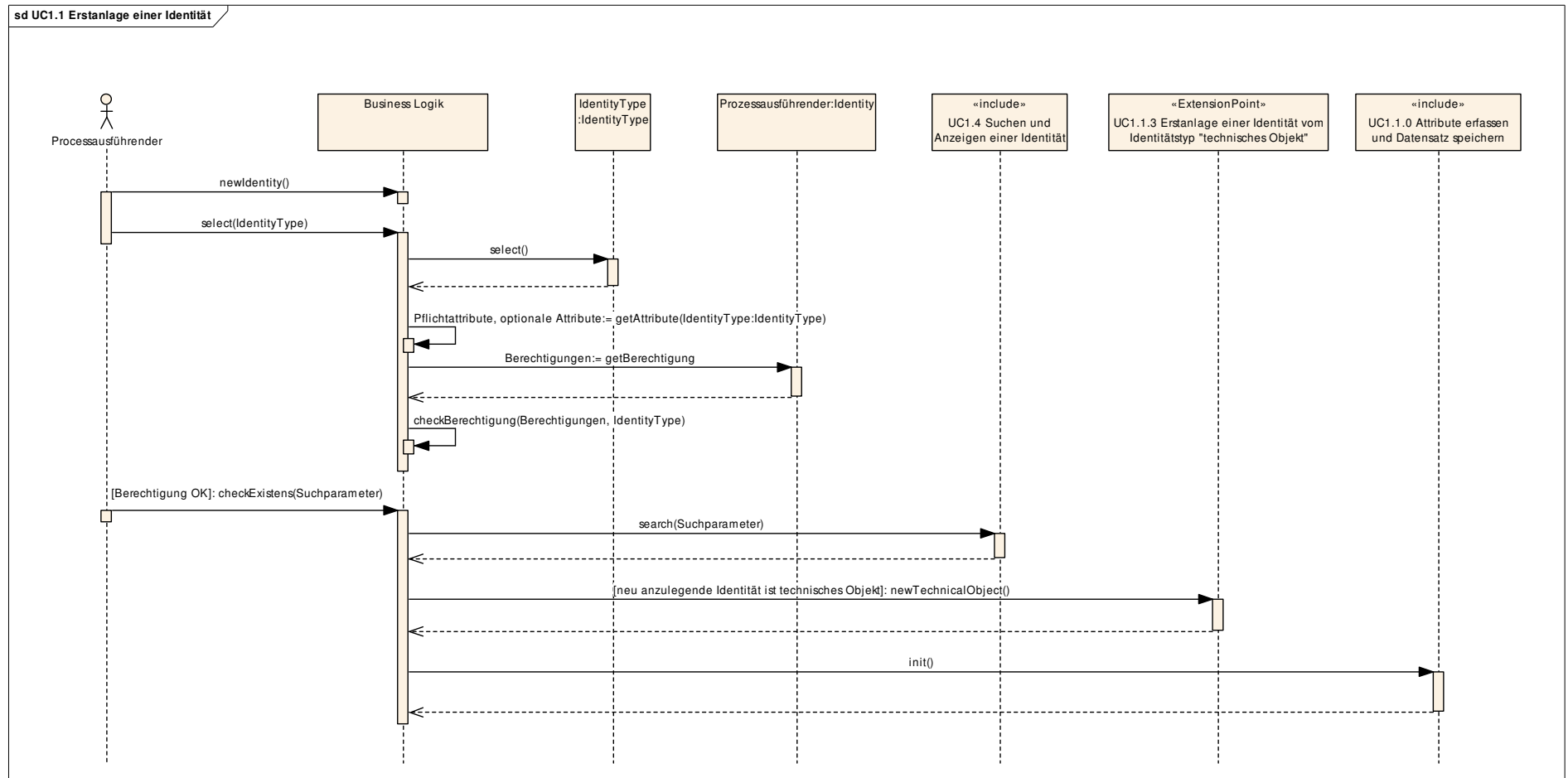
Fachliche Beschreibung von Anwendungsfällen

Kontrollflussdiagramm



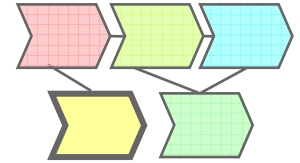
Fachliche Beschreibung von Anwendungsfällen

Sequenzdiagramm



IdM Schwerpunktthemen

Authentisierungsinformationen



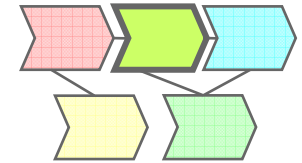
Prozesse für relevante Authentisierungsklassen und –Methoden:

- n Administration von Authentisierungsinformationen
- n Aufbau und Vergabe von Login-/Account-Namen
- n Passwortmanagement
 - inkl. sichere und wirtschaftliche Passwort-Reset-Verfahren
- n Management von Methoden zur starken Authentisierung, Verschlüsselung und Signatur
 - inkl. Notfallprozesse für Sperren und Ersatz
 - Vergabe von (non-User)Zertifikaten für Server-SSL, Code-Signing für sichere Kommunikation, Authentisierung technischer Objekte und für Daten-Signaturstellen (Schutz von Software)

Authentisierungsinformationen und -methoden sind Identitäten (und damit einem Set von Stammdaten dieser Identitäten) zugeordnet

IdM Schwerpunktthemen

Rollen



„Den richtigen Identitäten zum richtigen Zeitpunkt, solange wie nötig, auf eine effiziente und nachvollziehbare Art und Weise, berechtigten Zugang verschaffen“!

Daraus ergibt sich die Forderung nach:

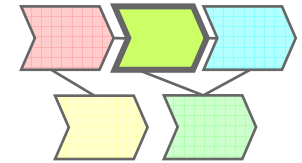
- n einer möglichst hohen Effizienz von administrativen Vorgängen
- n der Nachvollziehbarkeit sicherheitskritischer Aktionen
- n einer unmittelbaren Orientierung an Geschäftsprozessen
- n der Vorgabe von Standardprozessen für IT-Architekturen und -Lösungen

These:

Der Aufbau eines **unternehmensweiten Rollenmanagements** und die daraus resultierende Möglichkeit zur rollenbasierten Vergabe von Zugriffsrechten (→ **eProvisioning**) kann zur Zielerreichung beitragen.

IdM Schwerpunktthemen

Rollen



Zweck: effizientere Administration von Zulassungen & Berechtigungen

- n Gruppierung von (Zulassungen und) Rechten (Permissions)
- n hat darüber hinaus (für die Anwendung) keine Semantik
- n beinhaltet Rechte, die zur Bearbeitung (einer Aufgabe) innerhalb eines Prozesses benötigt werden
- n Anwendungen dürfen nur die Rechte auswerten
- n Unterscheidung: applikationsübergreifend / -spezifisch

"Business Roles“:

- n Bezeichnung betont Definition mit Blick auf die zu unterstützenden Aufgaben / Geschäftsprozesse
- n werden auf Funktionen innerhalb eines definierten Geschäftsprozesses oder Positionen in einer Organisationsstruktur abgebildet
→ fachlicher Bezug

- n Anzustreben sind wenige Rollen
 - ggf. verwendungsspezifisch parametrieren

Vertiefung: Unternehmensweites Rollenmanagement

Rollenmanagement

Rollenmanagement **als unternehmensweiter Prozess**

- n gibt Kriterien zur Unterscheidung von Rollen vor
- n legt Prozesse zur **Modellierung** von Rollen fest
- n gibt Leitlinien für die **Rollenfindung** vor
- n legt Rollentypen fest
(z.B. funktional, organisatorisch, vertraglich, administrativ, ...)
- n gibt Standardprozesse für die Rollen-Administration vor
 - Vergabe
 - Entzug
 - Beantragung von Rollen
 - Anzeige von Rollenzuweisungen
- n legt das Datenmodell für Rollendefinitionen fest
- n Unterstützung der organisatorischen Umsetzung
→ z.B. Aufbau von **Rollen-Clearing** im Unternehmen

Vertiefung: Unternehmensweites Rollenmanagement

Rollentypen I

	Reichweite	Inhalt	Ursprung
technisch	Anwendung bzw. Anwendungssystem	Rechte einer spezifischen Anwendung bzw. Anwendungssystems	Anwendungsspezifisches Rechtemanagement
funktional	Externalisiertes, zentralisiertes Autorisierungsmanagement (im wesentlichen Portale und Provisionierung)	Externalisierte technische Rollen, Rechte für Web-Zugriffe (URL-Permissions) und Zulassungen auf Systeme und Ressourcen	Externalisierung
fachlich	Geschäftsprozesse (unternehmensspezifisch und –übergreifend)	Funktionen in einem Geschäftsprozess und Positionen in Aufbau- und Ablauforganisationen, denen technische und funktionale Rollen zugeordnet werden können	Geschäftsprozesse, Aufbau- und Ablauforganisationen

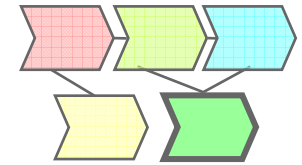
Vertiefung: Unternehmensweites Rollenmanagement

Rollentypen II

	Modellierung	Verwendung	Administration
technisch	Im Rahmen der Anwendungsentwicklung	Ausschließlich innerhalb der Anwendung	Explizite Zuweisung
funktional	Im Rahmen des Integrationsprozesses von Anwendungen in eine Portal- und/oder Provisionierungsinfrastruktur	Innerhalb von einzelnen Anwendungen und von Anwendungsverbänden mit einem externalisierten Rechtemanagement	Explizite Zuweisung sowie Ausstattung über Standardpakete von Rollen und Zulassungen
fachlich	Im Rahmen einer Geschäftsprozessmodellierung und/oder Definition einer Aufbau- oder Ablauforganisation	Innerhalb von Anwendungen, Anwendungsverbänden und grundsätzlich unternehmensweit nutzbar	Zuweisung durch die Instanziierung der Geschäftsprozesse (z.B. Neueinstellung eines MA, Initiieren eines Projekts)

IdM Schwerpunktthemen

Zulassungen



Definition Zulassung/(Anwendungs-)Account:

- n bündelt nutzungsspezifische Einstellungen und Rechte innerhalb einer Anwendung (Ressource)
- n Nutzung setzt ein bestimmtes Recht (LogonPermission) voraus
- n Nutzung erfordert i.d.R. "Berechtigungsnachweis" (Passwort, "Credentials,,)
- n repräsentiert einen (i.d.R.) personenspezifischen Zugang zu einem System
- n ermöglicht Verwaltung "persönlicher" Einstellungen (Default-Werte etc. ...)

Technische Accounts

- n keiner bestimmten Person zugeordnet
- n werden von verschiedenen (ggf. nicht identifizierten) Personen genutzt

Das **Zulassungsmanagement** legt fest

- n welche initialen Rechte und Ressourcen zu einer Zulassung gehören
- n welche Art der Authentisierung für diese Zulassung notwendig ist
- n welche Zugangsarten (Netzwerkebene) für eine Zulassung möglich sind
- n auf welche Art die Zulassung eingerichtet, modifiziert und gelöscht wird (Provisionierung)

Die direkte Zuweisung von Zulassungen an Identitäten ist möglich

Vertiefung: Zulassungsmanagement

Begriffsklärung eProvisioning

Administration auf Unternehmensebene von

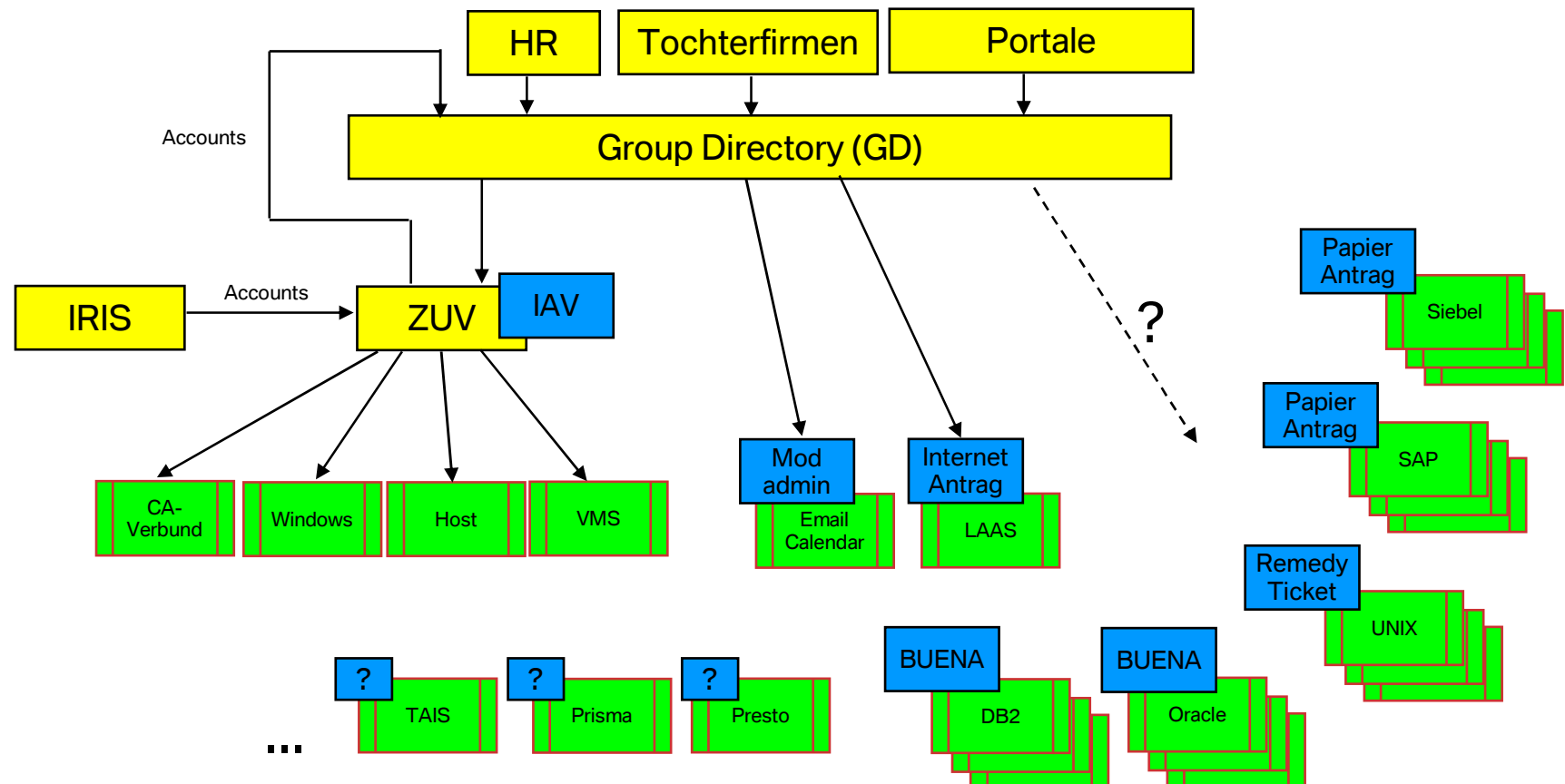
- n Benutzern („User“)
 - HR-Systeme, Verzeichnisse
- n Rollen („Roles“)
 - Unternehmensweite Rollenmodelle (Businessrollen)
- n Zugängen („Accounts“)
 - Ausstatten mit den notwendigen Zugängen
 - User-Self-Service, Workflow
 - Initiale Ausstattung mit Rechten und Ressourcen
- n Rechten („Permission“)
 - Zugriffsmanagement („fein-granular“)
 - Enterprise Access Management, Dienst- und System-spezifische Rechte-Administration

eProvisioning

Vertiefung: Zulassungsmanagement Motivation für eProvisioning

Heutiges zentrales Benutzer- und Zulassungssystem (beispielhaft):

- n historisches, stark gewachsenes System
- n neben der zentralen Zulassungsverwaltung entstanden weitere Zulassungsverfahren
- n keine Gesamtsicht über Zulassungen
- n wichtige Dienste und Systeme werden nicht unterstützt (z.B. SAP, Unix)



Vertiefung: Zulassungsmanagement

Kernaufgaben eines eProvisioning-Systems

Bereitstellung von Diensten für IT-Benutzer und -Administratoren

- n Bereitstellen einer Zulassung („Account“)
- n Löschen einer Zulassung
- n Zulassung ändern (z.B. Abteilungswechsel)
- n Zulassung sperren, freigeben
- n Abgleich der Zulassungen mit den Zielsystemen („Reconciliation“)

User-Self-Service

- n Workflowunterstützung
- n Genehmigungsprozessen

Effiziente Administration

- n Single Point of Administration
- n Rollenunterstützung für Day One/Last Day

Auditing

- n Revisions-Sicherheit

Reporting

- n Linienorganisation
- n Administratoren

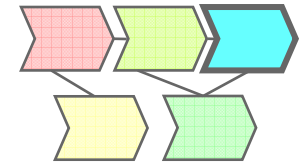
Vertiefung: Zulassungsmanagement

Ziele der Einführung eines eProvisioning-Systems

- n Erhöhung der **Effizienz** der Administration
 - Für IT-Standarddienste und –systeme existieren einheitliche Verfahren für die Benutzerzulassung
 - Dienste und Systemzugänge können auf Basis von Rollen vergeben werden
- n Verbesserung/Erhöhung der **Sicherheit**
 - Über ein Single-Point-of-Administration können Benutzerzulassungen eingesehen und bei Bedarf entzogen werden
 - Es gibt Auditing-Möglichkeiten zur Nachvollziehbarkeit von Zulassungsänderungen
- n Verbesserung der **Benutzerfreundlichkeit**
 - Zügige Bereitstellung der Zugänge auf Dienste / Systeme
 - User-Self-Service
 - Ease-of-Use
- n Möglichkeit der sukzessiven Integration weiterer IT-Dienste

IdM Schwerpunktthemen

Rechte/Permissions



„**das Recht, etwas zu tun oder zu nutzen**“, d.h.

- n Erlaubnis, auf eine Ressource (z.B. Dateien, Datensätze, Dienste, Methoden und Transaktionen, Applikationen und Systeme) in definierter Weise zugreifen zu dürfen
- n Semantik wird durch die entsprechende Ressource deklariert, bei der die Wahrnehmung des Rechts erfolgen kann

Rechtemanagement: Festlegungen für den Umgang mit Rechten

- n wie werden Rechteadministrationsprozesse definiert
- n wie werden Rechte gruppiert und in Hierarchien geordnet
- n welche Prozesse werden zentral und welche müssen dezentral durchgeführt werden

Rechteadministration: Durchführung der Rechte-Prozesse

Die direkte Zuweisung von Rechten an Identitäten ist möglich.

Identity Management

Zusammenfassung

Zentrale Objekte des Identity Management sind

n *Identität*

- hat in sog. AuthentisierungsDomänen bestimmte Rechte zur Nutzung von Ressourcen zugeordnet

n *Rollen*

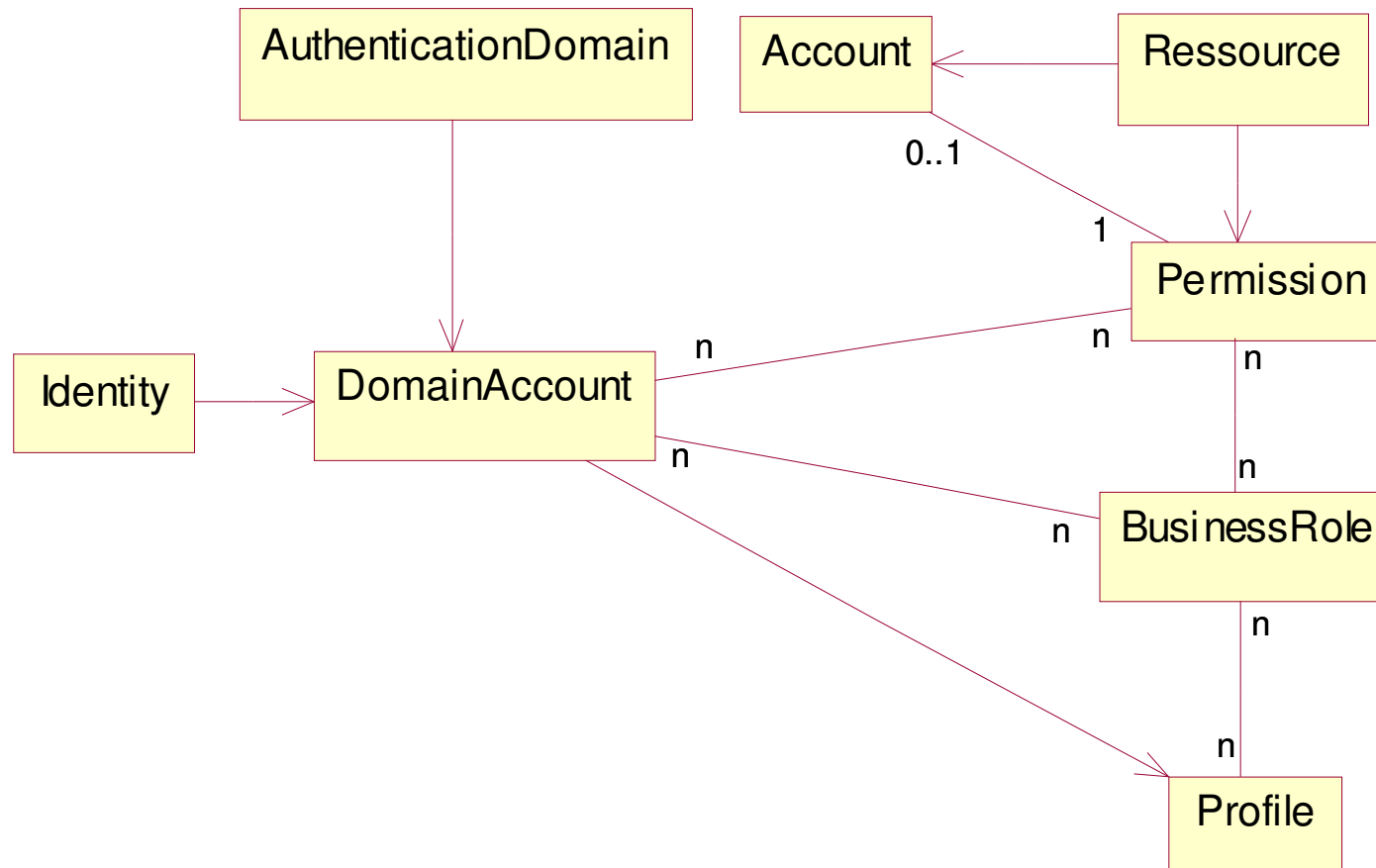
- werden mit Blick auf die zu unterstützenden Geschäftsprozesse definiert

n *Rechte*

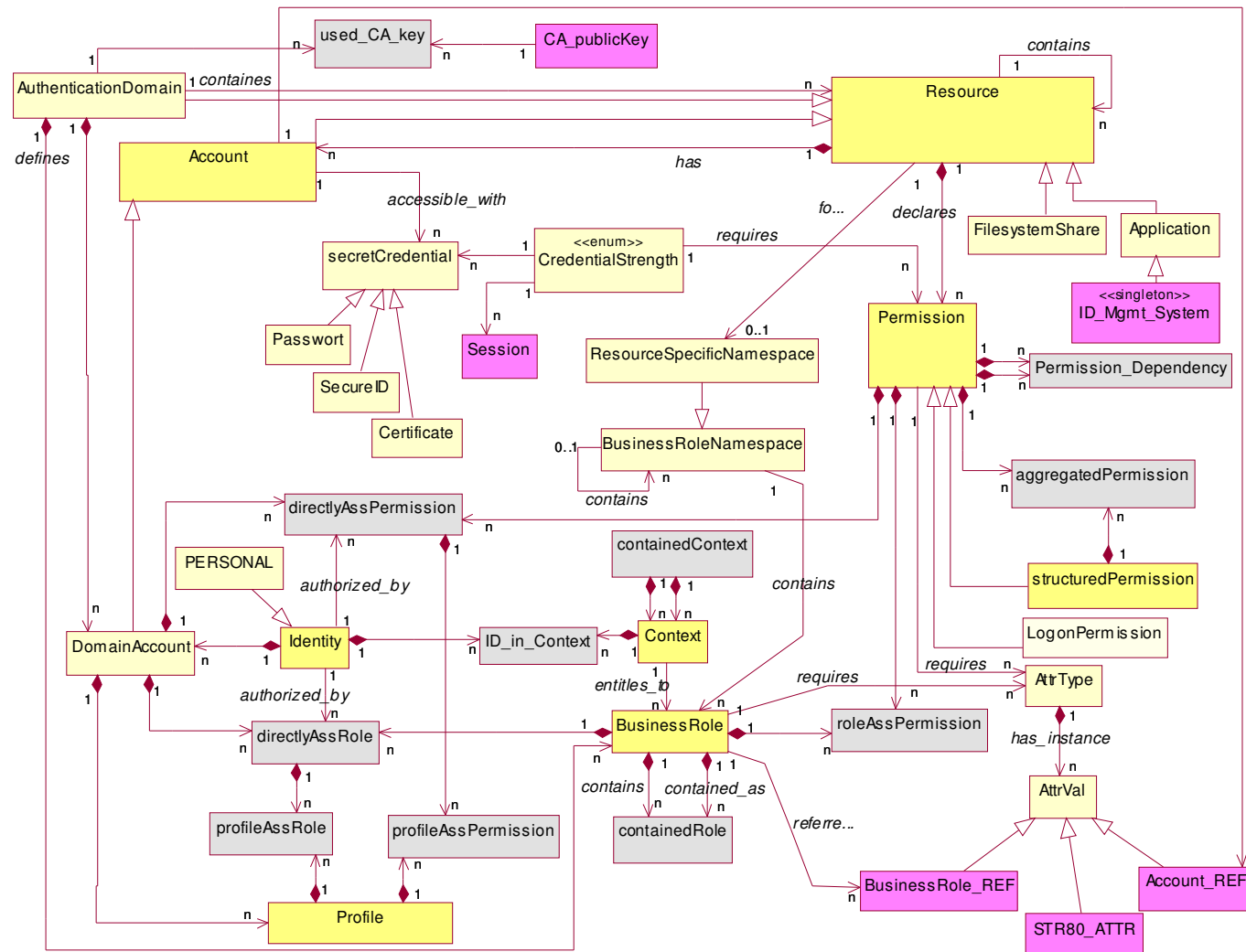
- sind zu Rollen gebündelt, um die Administrierbarkeit der Rechtezuordnung zu unterstützen

[zusätzliche Bündelung in Profilen möglich, um beispielsweise administrative und „anwendungsbezogene“ Rechte und Rollen zu trennen]

Modellierung des Identity Management Konzeptionelles Objektmodell (Beispiel)



Modellierung des Identity Management Fachliches Objektmodell (Beispiel)



Umsetzung

Konzeptionelle Sicht auf die Systemlandschaft

Administration & Management
GUI + Workflows



Zentrales Daten-Repository
Identitäten & Rollen

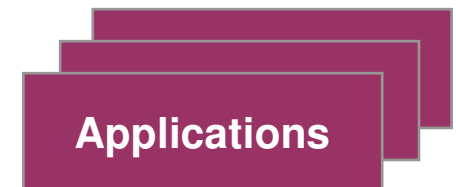


Spezialisierte Directories
Identitäten & Rollen & Policies
Zusätzliche Informationen



Verwendung der Daten
Verschiedene Portale;
diverse Applikationen
innerhalb der Plattformen

Enforcement
Single Sign-On
Authentisierung
Autorisierung



Vertiefung Federated Identity Management

- n Überwindung von Unternehmensgrenzen bzgl. Identity Management
- n Direkte Verbindung zwischen Accounts unterschiedlicher (Partner-) Firmen
- n Vermeidung einer doppelten Anlage und Verwaltung von Accounts
- n Reduziert Verwaltungsmehraufwände durch Schaffung einer Schnittstelle
- n Damit auch Erhöhung der Sicherheit

Alternative Lösungen:

- Liberty Alliance family of standards (SUN, AOL, GM ...)
- WS_Security family of standards (IBM, Microsoft ...)
- OASIS approved standards (z.B. SAML, XACML)

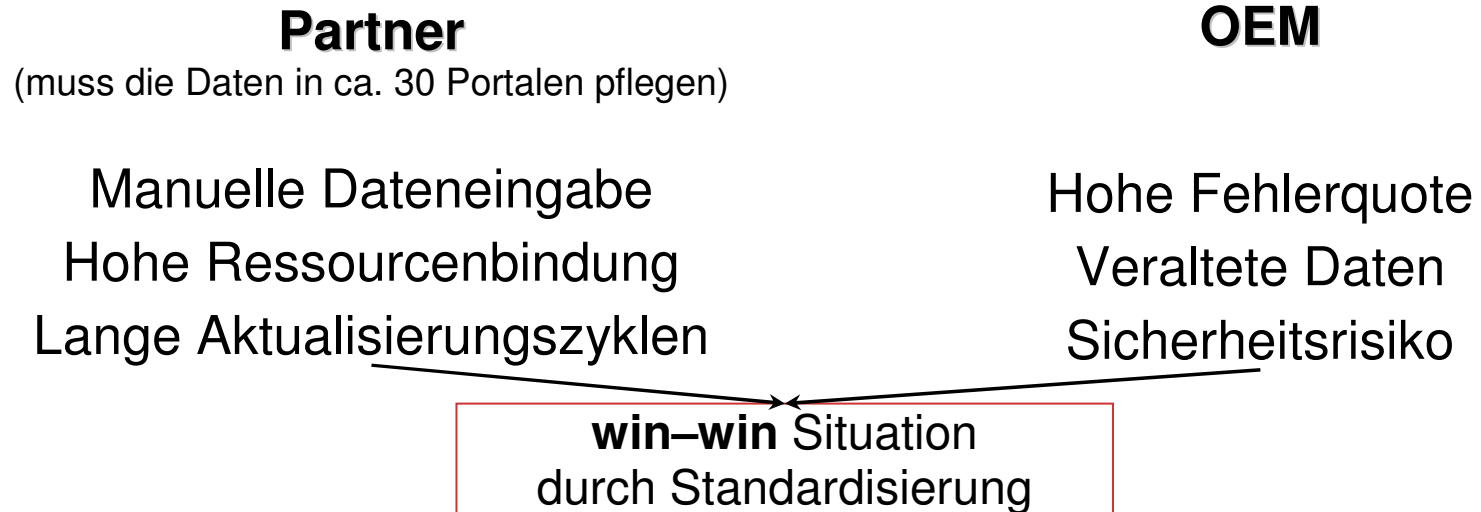
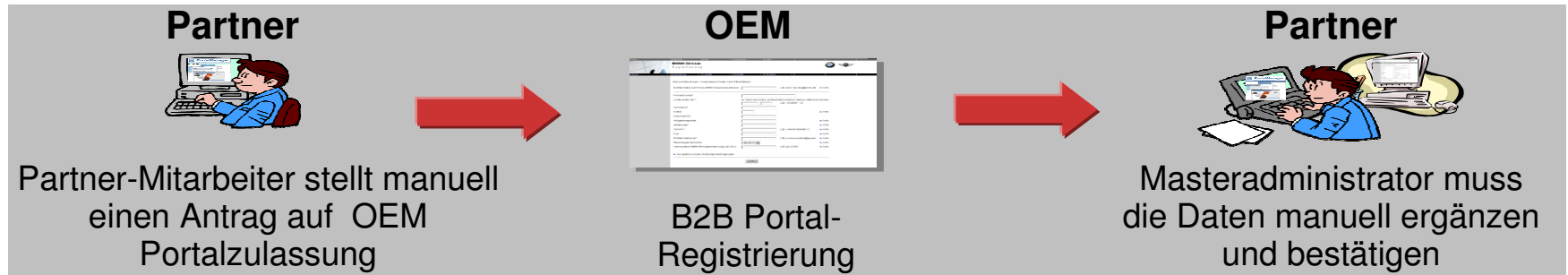
Identity Management Agenda

- n Einführung Identity Management
 - Definition und Zielsetzung
 - Schwerpunkte
- n Vertiefung ausgewählte Themenfelder
 - Rollenmanagement
 - Zulassungsmanagement/eProvisioning
 - Federated Identity Management
- n Praxisbeispiel zur Standardisierung
 - Der Odette UAM-Standard zum Einsatz von Web Services für unternehmensübergreifendes Benutzermanagement



Odette UAM Standard*

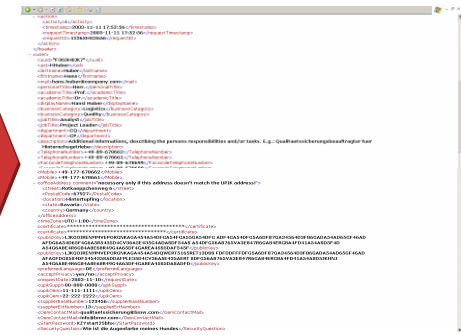
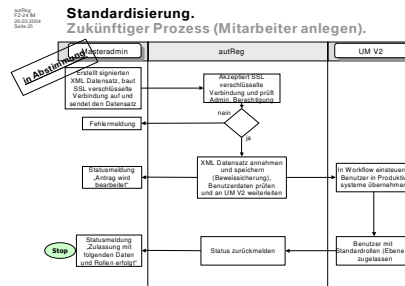
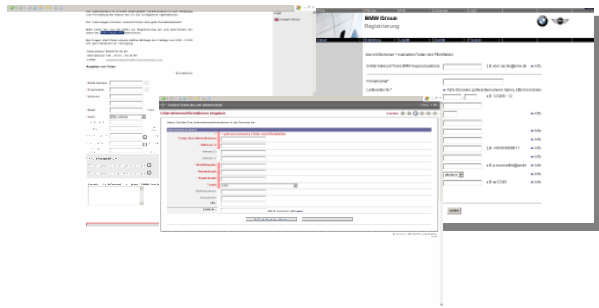
Motivation



* Als E12-Aktivität gestartet, dann aber als Odette-Projekt „User & Access Mgmt.“ initiiert, um europaweite Akzeptanz zu gewährleisten und internationale Resonanz über Zusammenarbeit der Odette mit der AIAG und JAMA/JAPIA zu ermöglichen.

Odette UAM Standard

Vorgehensweise: Standardisierungsschritte



Erster Schritt:

Standardisierung der Daten zur Registrierung von Partnermitarbeitern in OEM Portalen.

Zweiter Schritt:

Standardisierung des Registrierungsprozesses

Dritter Schritt:

Standardisierung der Technologie (WebService, WS Security, XML, usw.)

Odette UAM Standard

Ergebnis

März 2004: Verabschiedung des Standards durch das Technical Committee von Odette

Inhalt:

- XML Guideline zur Benutzerregistrierung (Stammdaten)
- XML Guideline zur Beantragung von Applikationszugriffen
- Beschreibung des Projekts inkl. der Prozesse
- Vorschlag zum Austauschprotokoll und dessen Absicherung

Im Juli 2004 wurde aufgrund eines Änderungswunsches von Renault eine aktualisierte Version verabschiedet

Derzeit Pilotbetrieb der durch den Standard beschriebenen Schnittstelle zwischen BMW und ZF

Feedback aus Pilotierung fließt in Weiterentwicklung des Standards ein

Odette UAM Standard

Funktionalität

Folgende Prozesse werden bei BMW über die Schnittstelle angeboten:

User Management

Neuanlage / Registrierung eines Benutzers

Abfrage der Daten eines Benutzers

Änderung der Stammdaten eines bestehenden Nutzers

Deaktivierung eines Benutzers

Reaktivierung eines Benutzers

Löschen eines Benutzers

Access Management

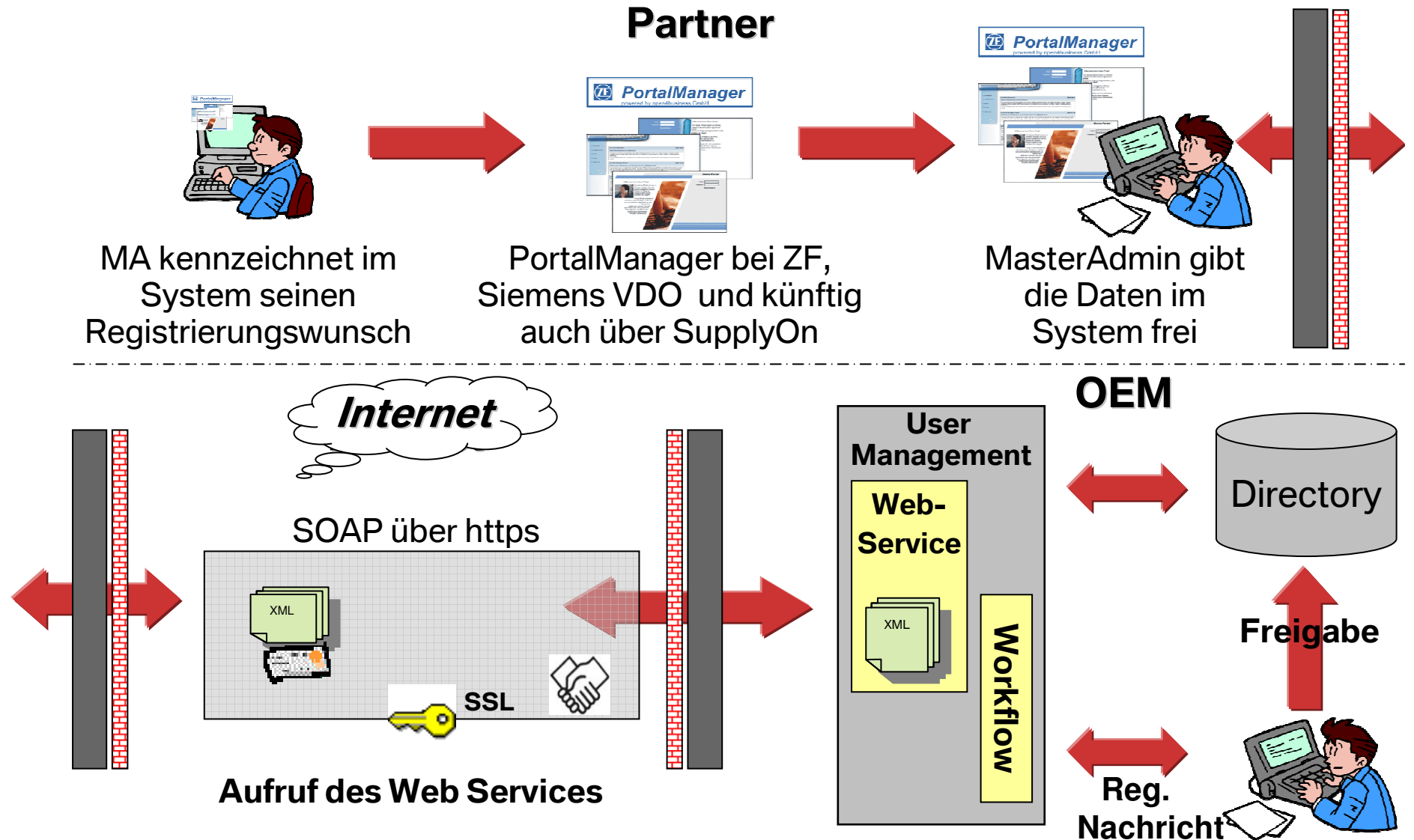
Berechtigungen für einen Nutzer beantragen

Berechtigungen für einen Nutzer entziehen

Zusätzlicher Webservice (aus Piloterfahrung)

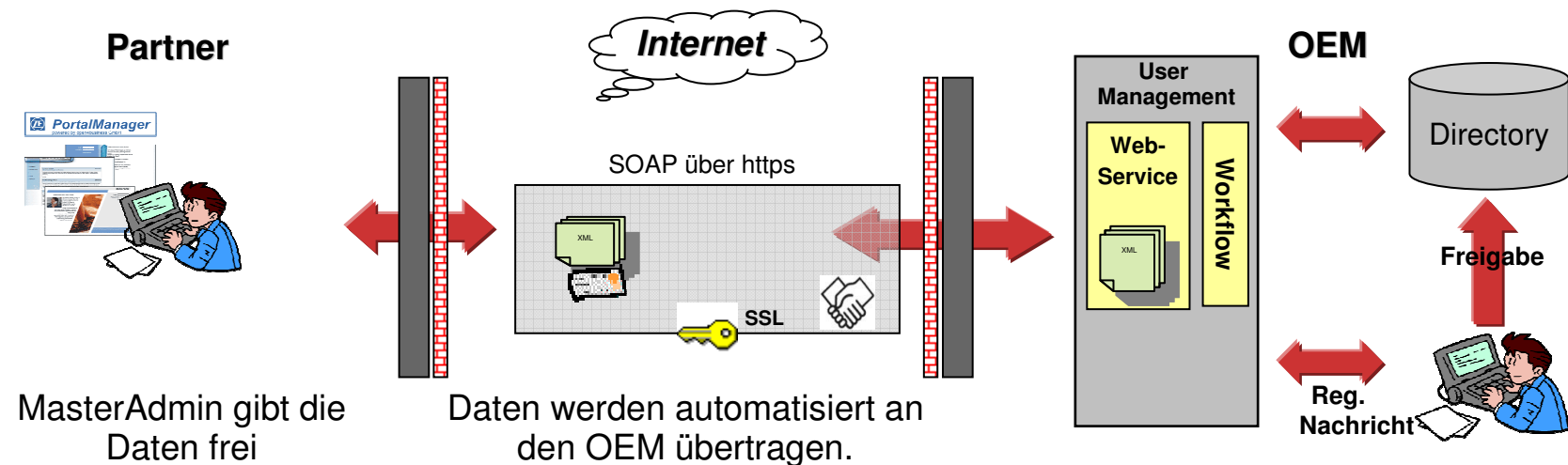
Abfrage der aktuellen Rollen bei BMW

Odette UAM Standard Neuer automatisierter Prozess



WebService-basierter Prozess

Vorteile für den Lieferanten



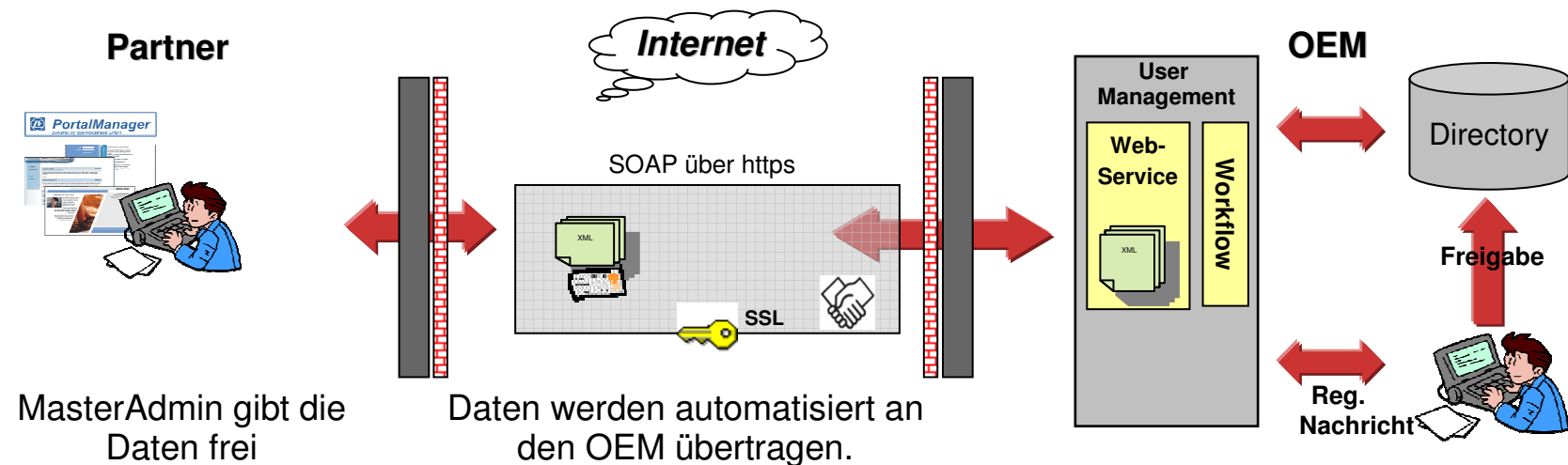
Manuelle Dateneingabe entfällt, da die Daten direkt aus dem Partnersystem genommen werden und an alle (bis zu 30) Portale übermittelt werden können.

Hohe Ressourcenbindung wird entschärft, da die Administratoren die Daten überspielen können und nicht mehr manuell einpflegen müssen.

Aktualisierungszyklen werden aufgrund der direkten Verbindung zwischen den Systemen wesentlich verringert.

WebService-basierter Prozess

Vorteile für den Hersteller/OEM



Fehlerquote wird deutlich geringer, da die Daten direkt aus den Partnersystemen kommen und übertragen werden können (keine manuelle Eingabe).

Die Aktualisierung der Daten wird wesentlich einfacher und die Aktualisierungsrate kann dementsprechend erhöht werden.

Das Sicherheitsrisiko wird minimiert, da die Aktualisierungsprozesse zeitnah und automatisiert vom Lieferanten angestoßen werden können.

Odette UAM Standard

Weitere Schritte

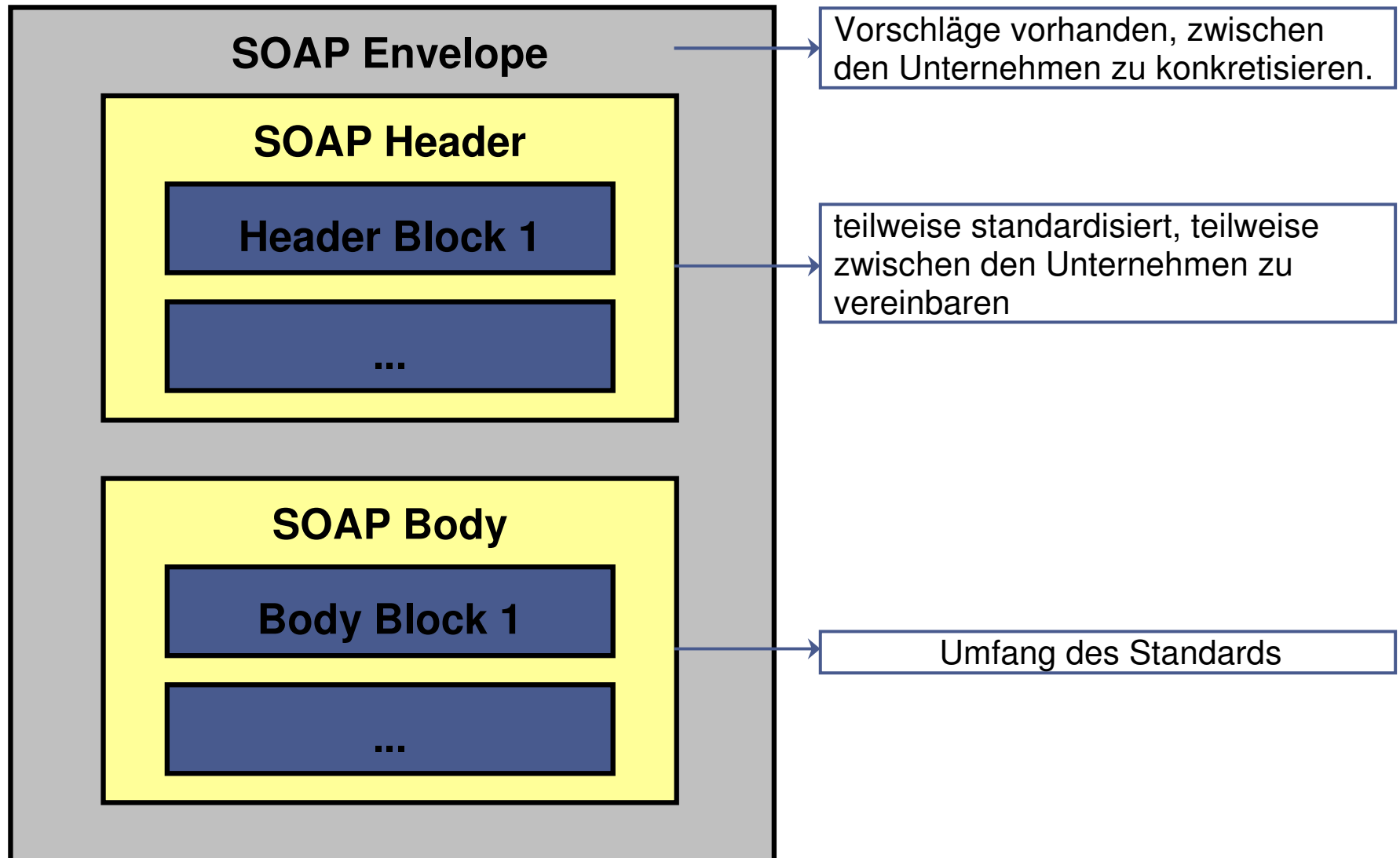
- n Aufbau der durch den Standard beschriebenen Schnittstelle als erster Pilot zwischen BMW und ZF
- n Erfahrungen aus der Pilotierung in Dokumentation des Standards integriert und im Juni 2005 an Odette zurückgemeldet
- n Nach der erfolgreichen Pilotierung muss die Schnittstelle vom Pilotstatus zu einer Lösung weiterentwickelt werden
- n Anbindung weiterer Partner (Siemens VDO, Webasto, ...)

Weiterführende internationale Standardisierung:



Odette UAM Standard

Aufbau SOAP Nachricht



Odette UAM Standard

Beispiel XML

```
<?xml version="1.0" encoding="UTF-8" ?>
- <od31:UserAdministration xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:od31="http://www.odette.org/core/usradm"
  xmlns:core="http://www.odette.org/core/core" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.odette.org/core/usradm usradm.xsd">
  <IssueDate>2004-03-01</IssueDate>
  <DocumentID>20040301-0001</DocumentID>
  <DocumentTypeCode>405</DocumentTypeCode>
  <AgencyCode />
  <SubsetID>A31011</SubsetID>
- <UserAdministrationEntity>
  <PartyID>01-234-5678</PartyID>
  <AgencyCode>16</AgencyCode>
  <Name>Autoparts International INC.</Name>
- <Address>
  <Street>Automotive Avenue 1</Street>
  <City>Supplier City</City>
  <PostCode>123456789</PostCode>
  <SubCountryCode />
  <CountryCode>US</CountryCode>
  <AddressLineText />
  </Address>
  <BusinessEntityAdministratorID>5968b3ce679311d88ce200300543ac56</BusinessEntityAdministratorID>
- <AdditionalPartyID>
  <PartyID>123456</PartyID>
  <AgencyCode>X04</AgencyCode>
  </AdditionalPartyID>
  </UserAdministrationEntity>
- <AdministrationAction>
  <AdministrationActionCode>1</AdministrationActionCode>
  <!-- create -->
- <ActionRequestText>
  <TextLine>This is a sample XML message to demonstrate how a working user management message to create a new user could look like.</TextLine>
  <LanguageCode>en</LanguageCode>
  </ActionRequestText>
  </AdministrationAction>
- <User>
  <UserUUID>547f5e9f2fb04879a4c017f0a38e9f7c</UserUUID>
  <LanguageCode>en</LanguageCode>
- <PersonalInformation>
  <LastName>Doe</LastName>
  <FirstName>John</FirstName>
  <DisplayName>John Doe, Autoparts Intl. INC.</DisplayName>
  <PersonalTitle>Mr.</PersonalTitle>
  <GenderCode>1</GenderCode>
  <AcademicTitle />
  <Photo />
  <PreferredLanguageCode>DE</PreferredLanguageCode>
  <PreferredLanguageCode>EN</PreferredLanguageCode>
  <PreferredLanguageCode>FR</PreferredLanguageCode>
  <PreferredLanguageCode>ES</PreferredLanguageCode>
  <PreferredLanguageCode>ITX</PreferredLanguageCode>
  </PersonalInformation>
- <JobInformation>
  <DepartmentName>CQ</DepartmentName>
  <BusinessArea>User</BusinessArea>
```


Das wärs für heute...

- n Fragen / Diskussion

- n Verbesserungsvorschläge

- n Die Folien sind bereits auf die Web-Seite der Vorlesung:
<http://www.nm.ifi.lmu.de>

- n Nächste Woche:
Beginn des zweiteiligen Vorlesungsteils über IT-Prozesse
(Dr. Igor Radisic)