Warum ist Provisioning für Ihr Unternehmen wichtig?

München, 30. März 2004,
Köln 01. April 2004

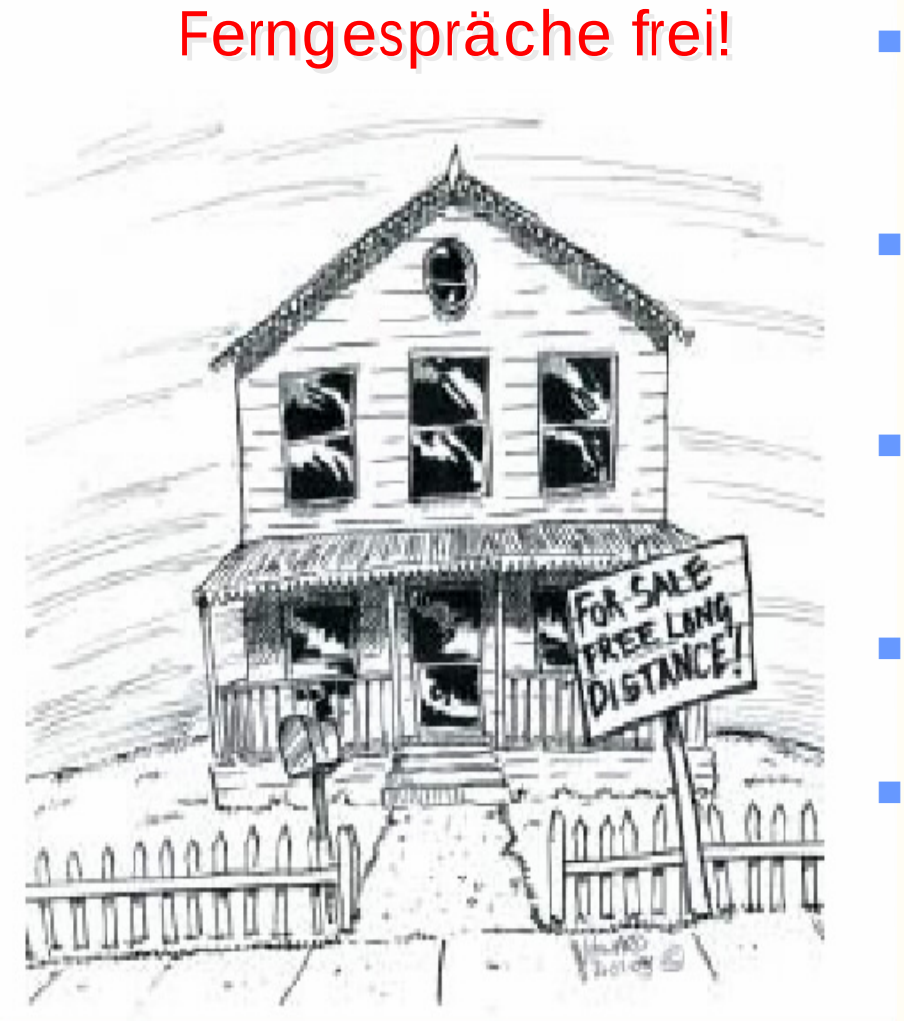
Horst.Walther@Si-G.com

Agenda

- Geschichten die das Leben schrieb
- Provisioning – was ist das?
- Einordnung in das Identity Management
- Ressource Provisioning Prozesse
- Provisioning – warum gerade jetzt?
- Der Markt – Anbieter und Systeme
- Tipps - Was ist zu beachten?

- Anhang
  - Beispiel – Ausgangslage, Ziel, Anforderungen, Kosten, Nutzen
  - Modell des Berechtigungsmanagements, Komponenten, Schnittstellen
  - Checkliste Referenzkundenbesuch
  - Wichtige Standards

Geschichten die das Leben schrieb (1)...



- Ein Top-Manager eines Telekom-Providers zog in ein neues Haus ein.
- Seine Telephonkosten wurden weder ermittelt noch ihm berechnet.
- Als er das Unternehmen verließ, wurde (folgerichtig) vergessen, den Anschluss zu sperren.
- In der Zwischenzeit ging das Haus durch mehrere Hände.
- Schließlich wurde es offen mit dem Vorzug eines freien Telephonanschlusses angeboten.

Geschichten die das Leben schrieb (2)...

Das überzählige Kabel

- Einer meiner Mitarbeiter, ein Novell Administrator, hatte das Unternehmen vor 2 Jahren verlassen und sich selbständig gemacht.
- Etwa 6 Monate später habe ich ein Kabel mit unbekannter Funktion entdeckt.
- Es ließ sich bis in das Büro eines benachbarten Rechtsanwalts verfolgen.
- Dessen Sekretärin loggte sich in unseren Server ein und benutzte unsere Ressourcen.
- Mein Ex-Mitarbeiter stellte Ihr dafür monatlich eine Rechnung.
- Außer meiner Frau habe ich Niemandem je etwas davon erzählt.

Geschichten die das Leben schrieb (3)...

Der Firmenwagen

- Ein Kollege von mir fuhr einen Wagen mit südfranzösischem Nummerschild, lebte aber in Paris.
- Als er sein Vorgänger-unternehmen verlassen hatte, hatte er darum gebeten den Firmenwagen noch solange zu fahren, bis er seine Angelegenheiten geregelt hätte.
- Als sein Chef das Unternehmen auch verließ, wusste Niemand mehr von dieser Abrede.
- Seither wurden alle Kosten noch immer von seinem Ex-Arbeitgeber getragen.

Provisioning – was ist das?

- Provisioning heißt **Versorgung**.
  - Das Deutsche Wort Provision heißt im Englischen *Commission* oder *Kickback*.
- Schon lange ein **militärischer Terminus**: Versorgung der Truppe.
- In der **Telekommunikation** sind Provisioning und De-Provisioning ebenfalls feste Begriffe.
- User-Provisioning, Ressource-Provisioning oder eProvisioning steht für den Lebenszyklus des Managements von **Zugriffsberechtigungen**.

pro·vi·sion (http://dictionary.reference.com/)

noun

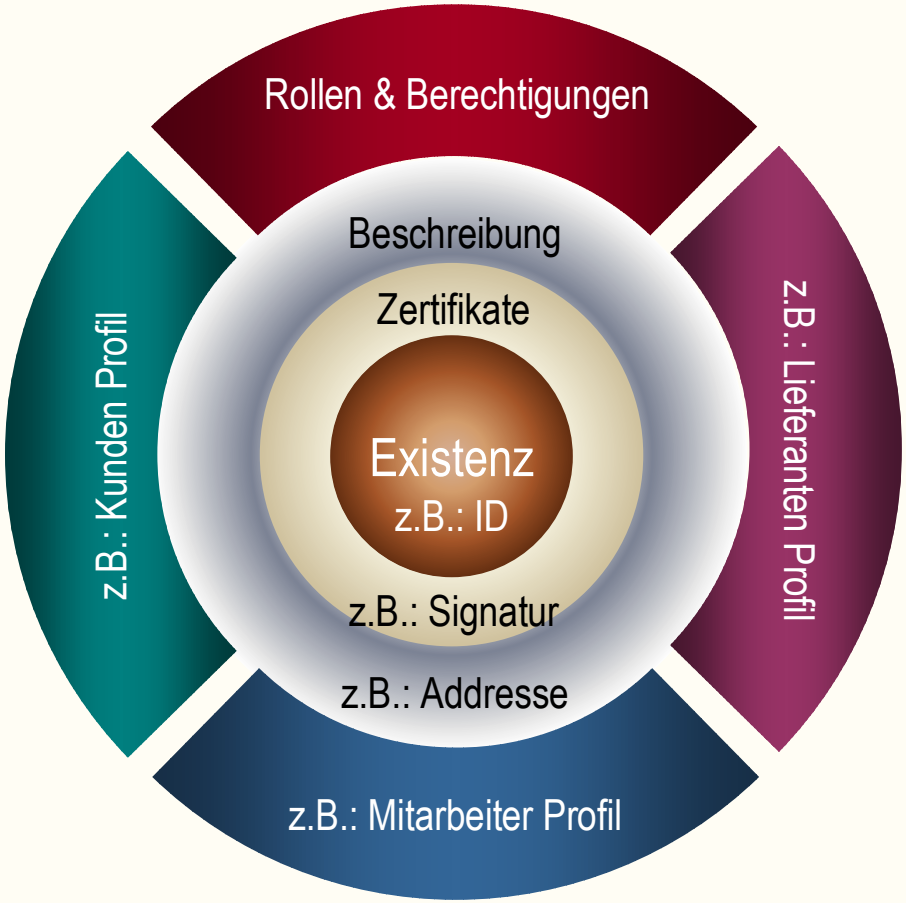
1. The act of supplying or fitting out.
2. Something provided.
3. A preparatory action or measure.
4. **provisions** A stock of necessary supplies, especially food.
5. A stipulation or qualification, especially a clause in a document or agreement.

transitional verb: **pro·vi·sioned, pro·vi·sion·ing, pro·vi·sions**

To supply with provisions.

Die digitale Identität

Die digitale Identität lässt sich gut mit einem Schalenmodell beschreiben.

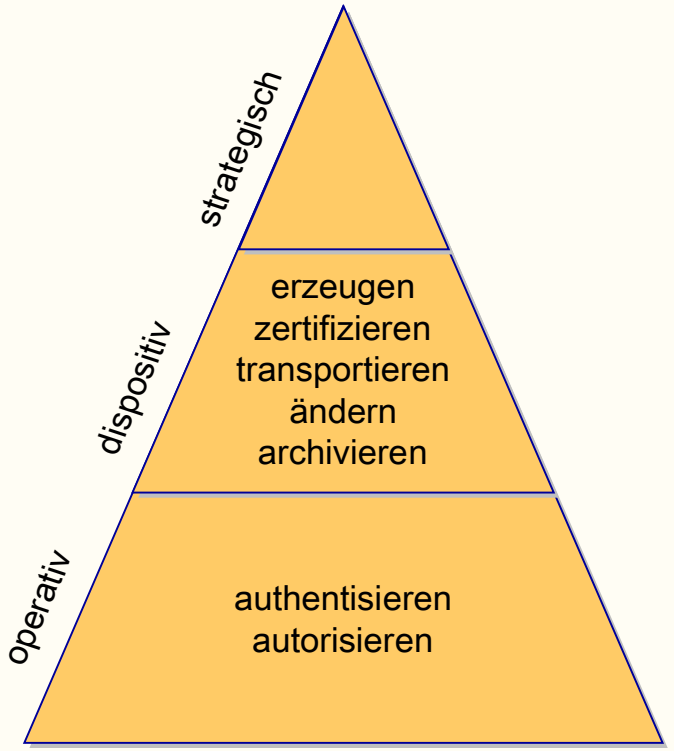


- Der Kern - **Existenz**:
  - eindeutige Identifikation.
  - “ID”, Name, Nummer
  - natürliche oder juristische Person, Anwendung oder Hardwarekomponente.
  - Gleiche Gültigkeit wie Objekt
- Die erste Schale - **Zertifikate**:
  - Zertifikate,
  - unterschiedlich stark
  - Password bis qualifizierte digitale Signatur
- Die zweite Schale - **Beschreibung**:
  - rollenunabhängige gemeinsame Attribute aus,
  - Adressinformationen
  - charakteristische Merkmale.
- Die dritte Schale - **Kontext**:
  - Rolle
  - Berechtigungen

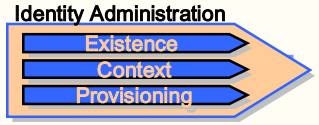
Einordnung in das Identity Management

Die Prozesse des Identity Management lassen sich gruppieren ...

- Nach operativ und dispositiv
  - operativ: authentisieren und autorisieren
  - dispositiv: verwalten digitaler Identitäten
- Nach fachlich und physisch
  - fachlich: verwalten und verwenden
  - physisch: integrieren, transportieren, transformieren und publizieren
- Nach Existenz, Zertifikat und Kontext
  - anlegen, erfassen, ändern, löschen
  - zertifizieren, widerrufen
  - zuweisen, ändern, entfernen von Rollen und Berechtigungen

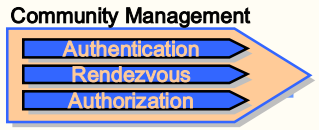


Prozesse des Identity Management (Microsoft)



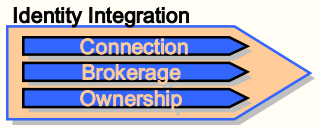
Identity Administration – *die dispositive Seite*

- Verwalten von digitalen Personenidentitäten, ihren Beziehungen zur Organisationseinheit und die Zuweisung von Ressourcen.



Community Management – *die operative Seite*

- Authentisierung, Bereitstellen / Publizieren und Autorisierung von Personen gemäß ihren digitalen Personenidentitäten.



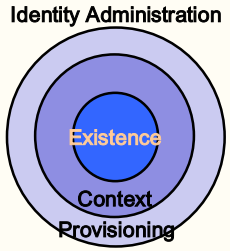
Identity Integration – *die technische Seite*

- Mechanismen für die Aktualisierung und Synchronisation von digitalen Personenidentitäten, die verteilt und teilweise redundant gehalten werden.

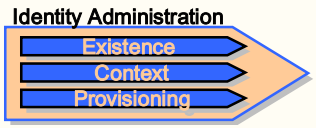
Quelle: Microsoft

Provisioning als Teil von Identity Administration

Verwalten von digitalen Personenidentitäten, ihren Beziehungen zur Organisationseinheit und die Zuweisung von Ressourcen.



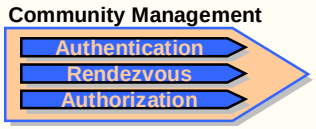
- **Existence**
  - Erzeugen, Verwalten, Synchronisieren von digitalen Personen-Identitäten.
- **Context**
  - Verwalten der Beziehungen von Personen zur Organisation (Rollen) und ihren Ressourcen (Rechte).
- **Provisioning**
  - Versorgen von Personen mit den ihrer Rolle entsprechenden Ressourcen und einbringen der Zugriffsrechte in die Zielsysteme, die die Ressourcenzugriffe steuern.



Community Management

Authentisierung, Bereitstellen / Publizieren und Autorisierung von Personen gemäß ihren digitalen Personenidentitäten.

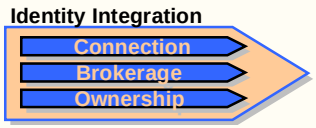
- **Authentication**
  - Authentisierung, ist der Prozess der Verifikation der Identität anhand von Zertifikaten im allgemeinen Sinne.
- **Rendezvous**
  - Der unter Rendezvous zusammengefasste Prozessgruppe, umfasst das Zusammenstellen und **Publizieren** von Adressbüchern, Verzeichnissen, Kalenderfunktionen für Terminvereinbarungen, Online-Meetings und gemeinsamer Ressourcennutzung.
- **Authorization**
  - Autorisierung ist der Prozess, Personen gemäß ihrer digitalen Personenidentität (*Existence*) und der über ihre Rolle im Unternehmen definierten Zugriffsrechte (*Context*) den Zugriff auf Ressourcen zu gestatten oder zu verweigern.



Identity Integration

Mechanismen für die Aktualisierung und Synchronisation von digitalen Personenidentitäten, die verteilt und teilweise redundant gehalten werden.

- **Connection**
  - Mechanismen, die Eigenschaften von Verteilung und Heterogenität überwinden helfen. Technisch sind das **Konnektoren** zum Zugriff auf Standard Verzeichnisse (z.B. LADP, DAP, ANS-SQL) oder Nicht-Standard-Verzeichnisse.
- **Brokerage**
  - Mechanismen, die es gestatten Attribute unterschiedlicher Informationsobjekte **aufeinander abzubilden**. Technisch realisiert über eine Regelmaschine, die auf einem Satz definierter Abbildungsregeln operiert.
- **Ownership**
  - Mechanismen, die bei redundant gespeicherten Informationsobjekten festlegen (und überwachen), in welcher (autoritativen) Quelle bestimmte Attribute führen geändert werden dürfen.

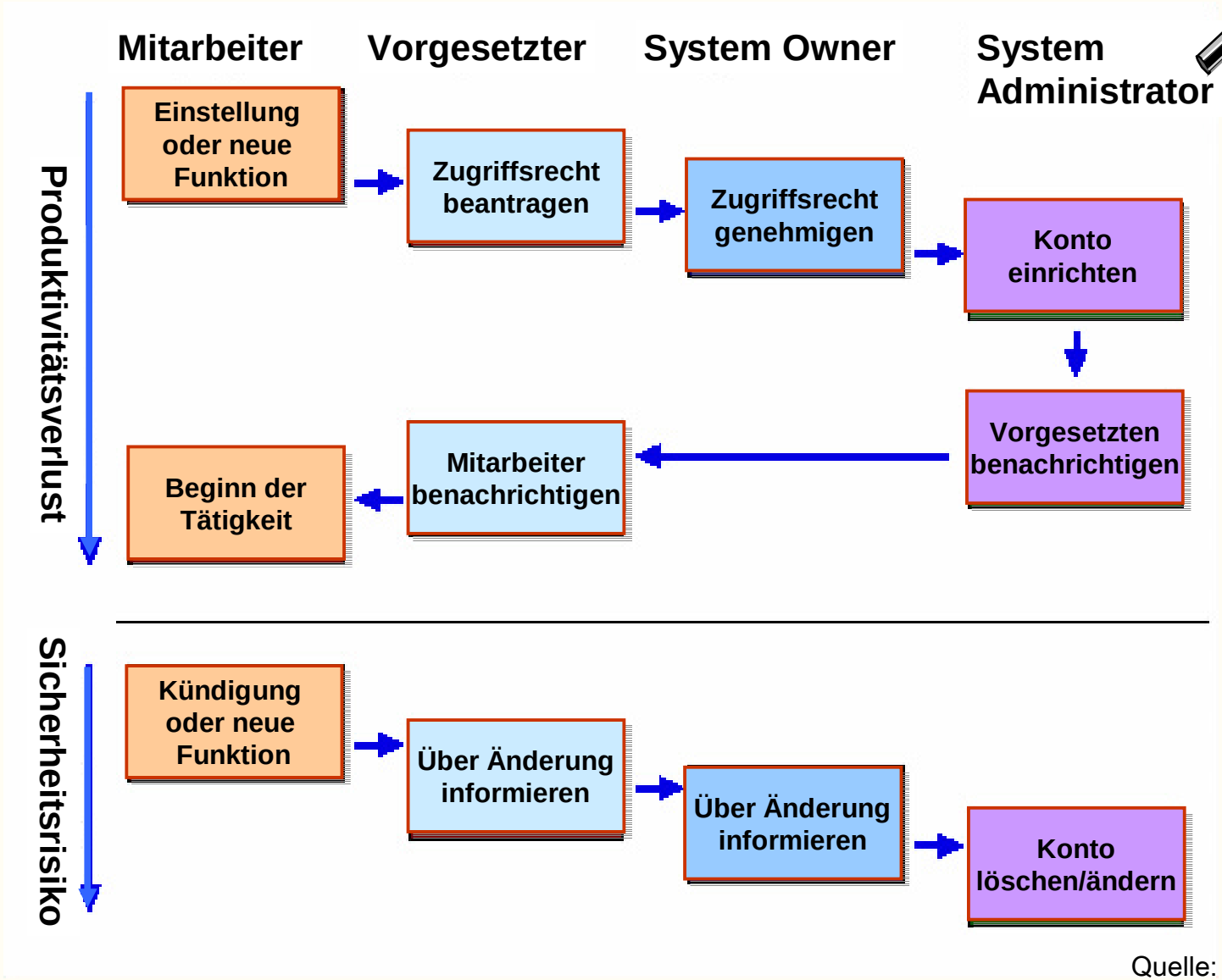


Ressource Provisioning Prozesse

- Provisioning …
  - **Versorgung** mit Ressourcen
  - die automatisierte **Zuweisung** von Berechtigungen zur Systemnutzung.
  - **Änderung** der Geschäftsrolle (Beförderungen, Abteilungswechsel) und Ausscheiden eines Mitarbeiters.
- De-Provisioning ...
  - Unterstützung der Änderung und des Entziehens von Ressourcen.
  - Diese Prozesse sind aus Sicherheitsgründen wichtiger als der eigentliche Provisioningprozess.
- Reverse Provisioning ...
  - Begleitende **Prüfprozesse** Abgleich der tatsächlichen Zugriffsrechte in den Systemen (Ist) mit den vergebenen Rechten (Soll) überein?
- **Manuelle** Beantragung und Vergabe von Einzelrechten ...
  - Die Rechtestruktur eines Unternehmens lässt sich mit vertretbarem Aufwand nicht vollständig über ein Rollenmodell abbilden.
- Die **semiautomatische Versorgung** von Systemen,
  - für die es nicht möglich ist oder sich nicht lohnt, Konnektoren zu erwerben oder zu erstellen.

Liste der Prozesse

Provisioning - Produktivität und Sicherheit



Quelle: M-Tech

Prozesse (Beispiel 1)

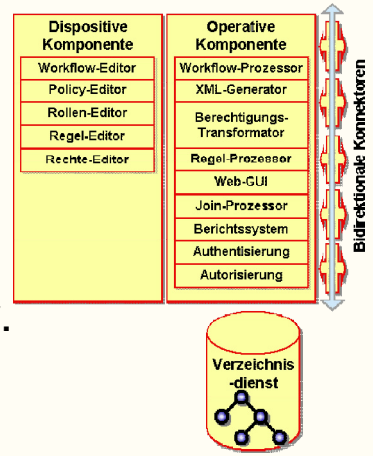
- **Anwender** (Existence)
  - Hinzufügen eines Anwenders
  - Entfernen eines Anwenders
  - Ändern eines Anwenders (Name, Abteilung, Vertragsende)
- **Rolle** (Context)
  - Hinzufügen einer Rolle (und Zuweisen der damit verbundenen Rechte, auch über „Klonen“ oder über Vorlagen / Templates)
  - Entfernen einer Rolle (auf die keine Referenz mehr existiert)
  - Ändern einer Rolle.
  - Prüfen auf Konfliktfreiheit
- **Konto** (Context)
  - Vergeben individueller Rechte,
  - Entziehen individueller Rechte,
  - Zuordnen zu einer Rolle
  - Lösen von einer Rolle
  - Konten unwirksam werden lassen (Ausscheidedatum erreicht)
  - Wiederinkraftsetzen abgelaufener Konten (Ausscheidedatum erreicht) Passwort setzen (Initial-Passwort und Neuvergabe)
- **Regel** (Context)
  - Hinzufügen einer Regel
  - Entfernen einer Regel
  - Ändern einer Regel
- **Genehmigungsstelle** (Provisioning)
  - Hinzufügen einer Freigabeautorität (mit Vertretungsregelung),
  - Entfernen einer Freigabeautorität,
  - Ändern einer Freigabeautorität,
- **Information** (Provisioning)
  - Information des Anwenders über eigene Zugriffsberechtigungen
  - Information des Verantwortlichen über die Zugriffsberechtigungen Dritter (nach Systemen, Organisationseinheiten),
  - Information des Anwenders über den Status eines Antrages auf Rechtevergabe,
- **Abgleich** (Provisioning)
  - Feststellen von Abweichungen der Berechtigungen in den Zielsystemen vom Sollzustand (Hacker, Prozessmängel, Managementfehler, …)
- **Bericht** (Provisioning)
  - Berichten der Rechtestruktur pro System oder Organisationseinheit,

Prozesse (Beispiel 2)

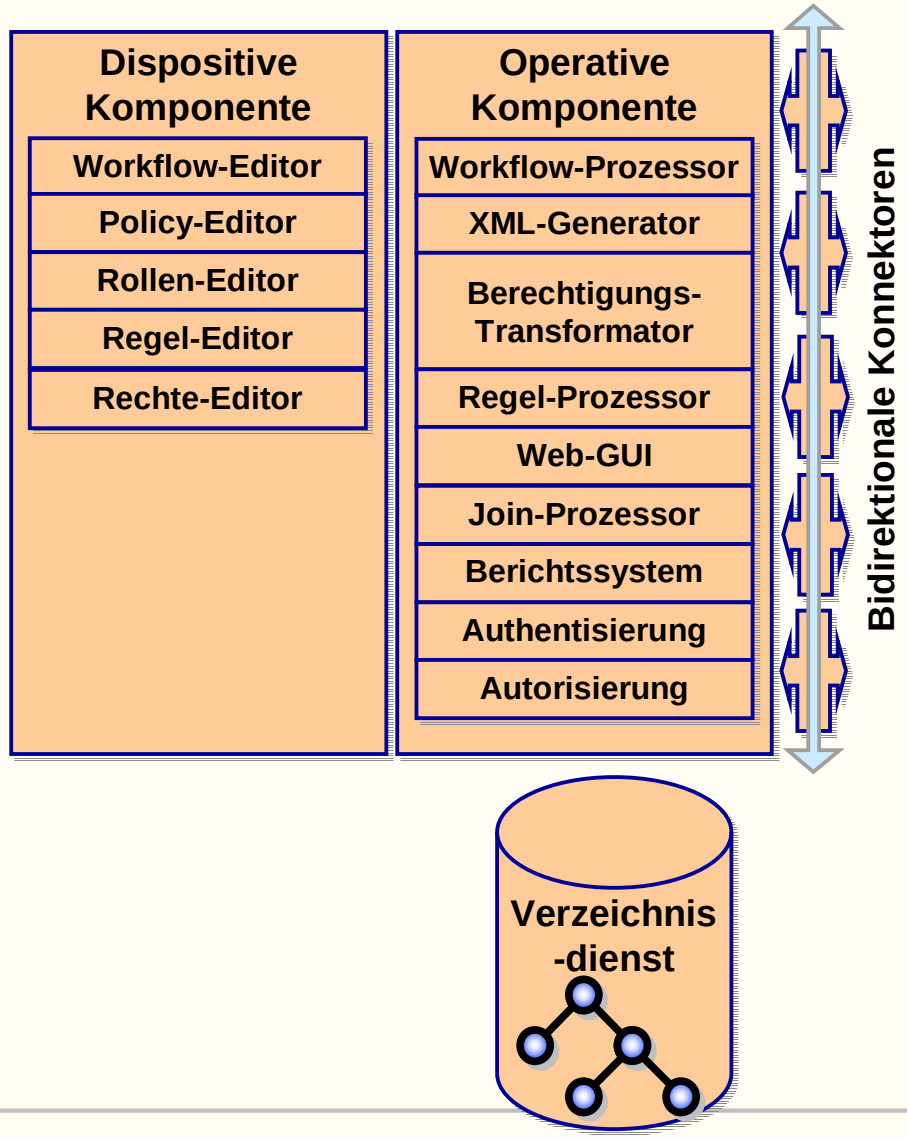
- **Antrag**
  - Antragsdaten (Auswahl, Eingabe, Prüfen)
  - Information der Prozessbeteiligten
  - Genehmigung
    - z.B.: Antragsteller → fachlich Vorgesetzter → Systemverantwortlicher → Administrator
  - Vier-Augen-Prinzip
- **IT-System**
  - Initialer Datenimport
  - Provisioning / De- Provisioning
  - Regelmäßiger Abgleich
- **Mitarbeiter**
  - Neue Mitarbeiter (Laden, Anlegen)
  - Mitarbeiterstammdaten ändern
  - Mitarbeiter sperren
  - Mitarbeiter entsperren
  - Mitarbeiter löschen
- **Berechtigung**
  - Neue Berechtigung
  - Berechtigung ändern
    - Gültigkeitszeitraum,
    - Account-Daten,
    - ...
  - Berechtigung löschen
- **Konto**
  - Account Sperren/Entsperren
  - Neues Passwort
- **Vertreter**
  - Dauerhafte Vertretung,
  - für einen bestimmten Zeitraum
- **Eskalation**
  - Pro Genehmigungsinstanz
  - Zeitraum konfigurierbar
  - Vorgelagerte Information per Email
- **Ausnahmen**
  - Abkürzung des Genehmigungsprozesses
  - Übertragen von Aktivitäten

Architektur von Ressource Provisioning Systemen

- Ein RP-System benötigt die folgenden **Kernkomponenten**:
  - Verzeichnisdienst
  - Workflowsystem
  - Regelsystem,
  - Konnektoren und
  - Optional ein RDBMS oder ein Join-Prozessor.
- **Unterstützende** Komponenten sind ...
  - XML-Generator,
  - Berechtigungstransformator,
  - Internet-fähige graphische Benutzeroberfläche (Web-GUI),
  - Join-Prozessor,
  - Berichtssystem,
  - Authentisierung,
  - Autorisierung



Komponenten eines RP-Systems



Provisioning – warum gerade jetzt?

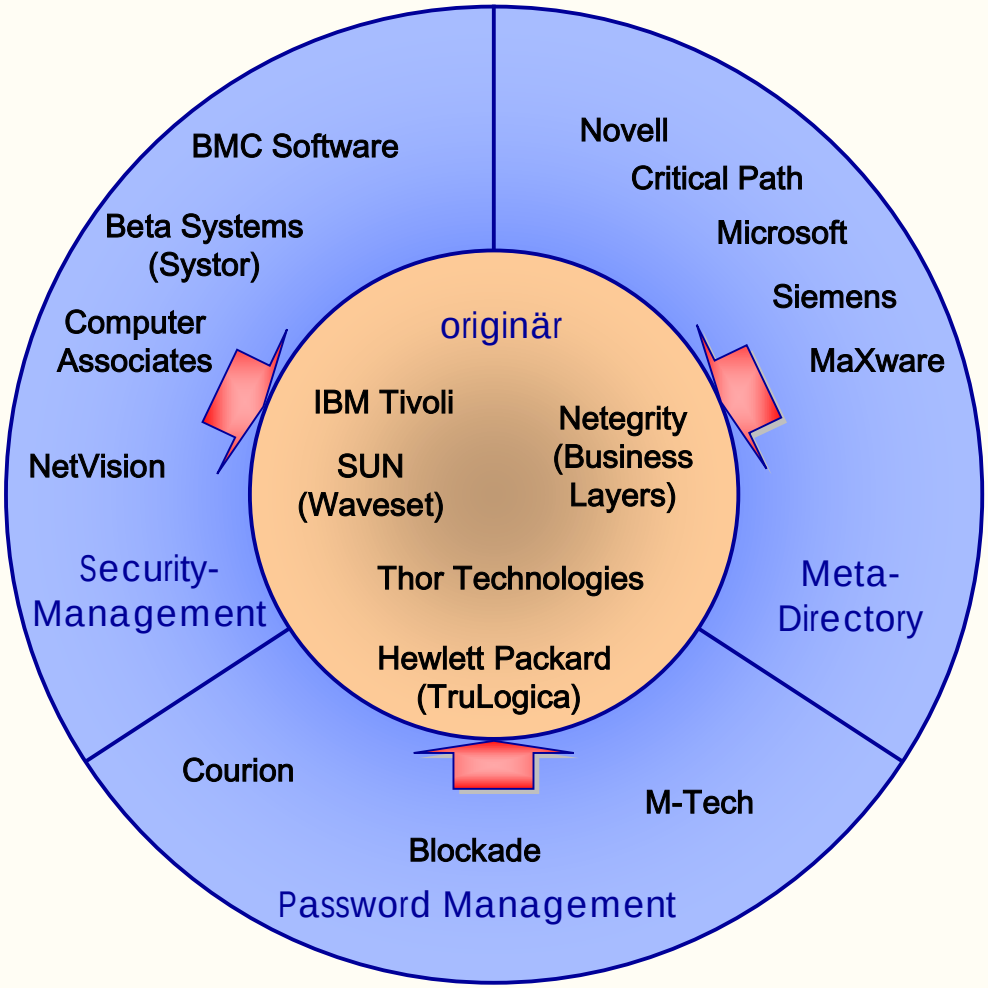
- Denken in kompletten Geschäftsprozessen ...
  - verlangt eine **einheitliche Infrastruktur**.
  - **Isoliert** pro Anwendung definierte Benutzeridentitäten behindern die Implementierung.
- Verschwimmende Grenzen ...
  - Reduktion der **Fertigungstiefe** einzelner Unternehmen
  - zugunsten eines Netzwerkes von **Lieferanten** und Abnehmern
  - Der logischen Vernetzung folgt die elektronische **Vernetzung**.
  - Im e-Business müssen Unternehmen ihr **Inneres nach außen** kehren.
  - **Externe Partner** werden an bisher interne Geschäftsprozesse angeschlossen.
- Unternehmensübergreifende automatisierte Zusammenarbeit ...
  - Lässt sich nicht mit unternehmensweiten technischen Lösungen unterstützen.
  - **Standardisierte** Formate, Protokolle und Verfahren sind erforderlich um
  - Zugriffsrechte verlässlich über Unternehmensgrenzen hinweg weiterzureichen.
- Ressourcenvirtualisierungen (Grid-Computing, Web-Services)...
  - Erfordern eindeutige digitale Identitäten
  - Automatisierte Rechteprüfungen.

Provisioning – warum gerade jetzt?

(Fortsetzung ..)

- Steigende Dynamik
  - Der Wechsel wird zum Normalzustand.
  - Mitarbeiter bleiben für kürzere Zeit mit einer Geschäftsrolle verknüpft.
  - Sie wechseln Abteilungen,
  - Sie arbeiten in Projekten.
  - Sie gehen für einige Wochen zu einer Niederlassung.
  - Zeitweise externe Kräfte benötigen interne Ressourcen.
- Höheres Sicherheitsbewusstsein
  - Erfahrungen mit den Gefahren des Internet,
  - Die hohe IT-Abhängigkeit
  - Das aktuelle Weltgeschehen
  - Ein "Leih' mir 'mal Dein Passwort!" wird heute nicht mehr akzeptiert.
- Externe Auflagen
  - Die elektronische Verkettung von Geschäftsprozessen birgt Risiken.
  - Behördliche Regelungen definieren entsprechende Anforderungen.
  - Banken müssen nach Basel Accord II für die operativen Risiken (operational risks) ihrer internen Abläufe Rückstellungen zu bilden.
  - Nur nachgewiesen geringere Risiken reduzieren diese Kosten.

Der Markt – Anbieter und Systeme



und ihre Herkunft

... und die Liste wird noch länger.

- Oblix,
- Discus Data
- Entact Information Security
- Fischer International
- Open Systems Management
- Voelcker Informatik
- SecuSys
- ...

Quelle: The Burton Group

Tipps - Was ist zu beachten? (1)

Rollen und Berechtigungen

- Die meisten Provisioning Systeme unterstützen Rollenkonzepte
- Wenn keine (von Geschäftsprozessen abgeleiteten) Rollen vorliegen sollte das Projekt auf Rollen verzichten.
- Eine Rollendefinition ist im Einführungsprojekt kaum machbar.

Personalabteilung

- Ihr gehören häufig die autoritativen Personaldaten
- Sie ist es häufig nicht gewöhnt einem IT-Projektleiter zuzuarbeiten.
- Arbeitet häufig nach einem anderen Zeitverständnis.

„Politik“

- Berechtigungssysteme berühren viele Abteilungen
- 20% ist Technik – 80% „Politik“
- Anwender vorher „ins Boot“ holen – oder außen vor lassen.
- „Zwangsbeglückungen“ nur mit Rückhalt im Top-Management.

Tipps - Was ist zu beachten? (2)

Organisatorische Voraussetzungen ...

- Transparenz über das jeweilige **Berechtigungskonzept** der Ziel-Systeme
- Standardisierte **Antragsworkflows** der anzuschließenden IT-Systeme
  - Gleichzeitige Änderung und elektronische Abbildung von Prozessen schafft zusätzliche Risiken
- Unternehmensweit klare und handhabbare **Unterschriftenregelung**
  - inkl. Vertreterregelung, virtuelle Organisationseinheiten z.B. Projekte
- **Akzeptanz** aller Workflow-Beteiligten (Antragsteller, Freigeber, Administrator)
- Hoher Stellenwert des **Einführungskonzeptes**
  - **Marketing**, Kommunikation und Schulung

Technische Voraussetzungen

- Lassen sich die System-Accounts pro Person **automatisiert zuordnen?**
  - fehlender Schlüssel, unterschiedliche Schreibweise → hoher manueller Aufwand
- Konnektoren müssen die vorhandenen technischen Anforderungen der IT-Systeme **vollständig abbilden**
  - z.T. auf Parameterebene

Tipps - Was ist zu beachten? (3)

Verfügbarkeit und Aktualität der benötigten ...

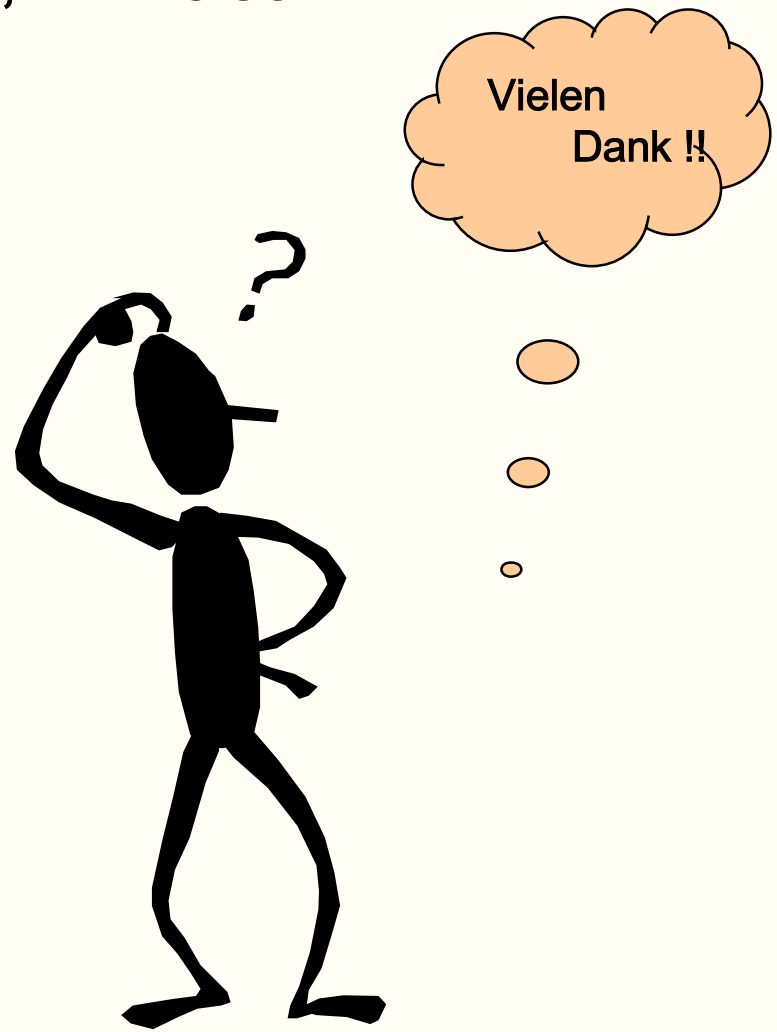
- Personendaten
- Organisationsdaten
- Berechtigungsdaten

Projektumfang/Einführung

Pragmatisches Vorgehen bei der Auswahl der zu realisierenden Funktionalität

- **Stufenweise** Einführung (Antragsverfahren, Reports, Konnektoren)
- Unterstützung von **Standardfälle** (Workflow, Antragstemplates, ...)
- **Sonderfälle** (systemseitig und organisatorisch) weiter manuell durchführen
- Längere Pilotphase mit „**gutwilligen**“ Benutzern vor Start des Roll-Outs

Fragen, Anregungen, Hinweise?



Achtung Anhang

Hier kommen die berüchtigten back-up-Folien ...

Anhang

- Beispiel
  - Ausgangslage & Ziel
  - Anforderungen
  - Nutzenkomponenten
  - Kostenkomponenten
- Modell
  - Regelkreis des Access Rights Management
  - Komponenten des Regelkreises
  - Schnittstellen des Regelkreises
- Checkliste Referenzkundenbesuch
  - Workflowkomponente
  - Maskenbearbeitung
  - Agenten und Schnittstellen
  - Rollen- und Berechtigungsstruktur
  - Performance – Reporting – Sicherheit - Aufwände
- Standards
  - SPML - Services Provisioning Markup Language
  - SAML - Security Assertion Markup Language
  - XACML - eXtensible Access Control Markup Language
  - XKMS - XML Key Management Specification
  - WS-Security

Beispiel

- Ausgangslage & Ziel
- Anforderungen
- Nutzenkomponenten
- Kostenkomponenten

Beispiel – Ausgangslage & Ziel

- Typische Ausgangssituation:
  - hohe IT-Durchdringung im Unternehmen
  - große Anzahl an IT-Systemen mit unterschiedlichen Benutzerzahlen
  - Heterogenes Berechtigungsmanagement
  - gewachsene Strukturen und Verantwortlichkeiten
  - unterschiedliche Antragsverfahren und Genehmigungsprozesse
  - unterschiedliche Rechtestrukturen
    - Gruppen, Rollen ...
  - unterschiedliche Namenkonventionen
    - Benutzerkennung, Rechte ...
  - unterschiedliche Administrationsverfahren
  - unterschiedliche Auswertungs- und Kontrollmöglichkeiten

- Ziel (?)
  - Steuerung, Administration und Kontrolle der Zugriffsrechte ...
    - von **allen** IT-Benutzern
    - für **alle** IT-Ressourcen
    - auf **allen** IT-Systemen (des Unternehmens)

Beispiel - Anforderungen (1)

- Informationsobjekte
  - Datenmodell – Berechtigungskonzept
  - Berechtigungsdaten (Rolle, Berechtigung, Account, ...)
  - Antragsdaten
  - Mitarbeiter – und Organisationsdaten
- Berechtigungskonzept
  - Beschreibung der Funktionen/Dialoge
  - Beschreibung der Rollen (inkl. Regeln)
  - Zuordnung von Funktionen und Rechten zu Rollen
  - Provisioning/De-Provisioning
- Verwaltung von Mitarbeiter- und Organisationsdaten
  - Unternehmen, Abteilungen (laden, abgleichen, anlegen, ändern, löschen)
  - Mitarbeiter (laden, abgleichen, anlegen, ändern, sperren, löschen)
  - Zuordnung (Unternehmen <-> Abteilung, Abteilung <-> Mitarbeiter, ...)
- Verwaltung von Berechtigungsdaten
  - Rollen, Berechtigungen, Zielsysteme, Accounts, Regeln (anlegen, ändern, löschen)

Beispiel - Anforderungen (2)

- Prozesse/Workflow
  - Manuell <-> automatisch initiierte Prozesse
- Information der Prozessbeteiligten
  - Neue Aktivität zur Bearbeitung
  - Antrag – Statusinformationen
  - Eskalation
  - Änderung von Mitarbeiter- und Organisationsdaten
- GUI-Konventionen
  - Design-Vorgaben, Ergonomie, Maskenaufbau pro Funktion/Dialog
- Anbindung der IT-Systeme (inkl. des Systems selbst)
  - Art der Anbindung (manuell, automatisiert)
  - Prozessdaten (Account, Rechte, Rollen, Antragsdaten, ...)
  - Initialer Datenimport
  - Antragsverfahren
  - Provisioning
  - Abgleiche/Auswertungen

Beispiel - Anforderungen (3)

- Anbindung von Konnektoren
  - Generelle Voraussetzungen
  - Spezifikation des Agenten je Zielsystem (Eigenschaften, Funktionalität, technische Angaben)
  - Ohne Agenten auf dem Zielsystem?
- Auswertungen/Reports/Historie
  - Aktuelle Accounts und Rechte (eigenen, fachl. Vorgesetzter, Systemverantwortlicher ...)
  - Antragsstatus (Antragssteller, Antragsbetroffener, Genehmiger)
  - Abgleiche (**Soll <-> Ist**, Mitarbeiter <-> Ist, ...)
  - Nicht zugeordnete Accounts
  - Sicherheitskritische Ereignisse
- Logging/Audit
  - Systemmeldungen, Fehlermeldungen, Transaktionen, Tracing, Audit
- Sicherheitsanforderungen
  - Account-Konventionen, Passwort, Zustellung, Neuanforderung, Verschlüsselung ...
- Performance

Beispiel - Nutzenkomponenten (1)

Quantitativer Nutzen

- Reduktion von **Lizenzkosten** durch die Löschung überflüssiger Accounts
- Reduktion des **Archivierungsaufwands** für Administratoren
- Reduktion des **Revisionsaufwands** bei Systemprüfungen
- Reduktion des Klärungs- bzw. **Kontrollaufwands** für Administratoren
- Reduktion des **Administrationsaufwands** (Agenten, PW-Self-Service)
- Reduktion der **Wartezeit** für Antragsbetroffene
- Reduktion des Aufwand zur Klärung des **Antragsstatus**

< Sollte als Basis der Projektverrechnung dienen ! >
< Nicht immer direkt zurechenbar ! >
< Beidseitige schriftliche Bestätigung notwendig ! >

→ Die Automatisierung des User Provisioning führt zu - teilweise erheblichen - Produktivitätssteigerungen.

→ Die typische Amortisations-Zeit liegt bei 1,5 Jahren

Beispiel - Nutzenkomponenten (2)

- Qualitativer Nutzen/Sicherheitsgewinn
  - Steigerung der **Antragsqualität** (Standardisierung und Validierung)
  - Minimierung von **Administrationsfehlern**
  - Entlastung von **Routine-Tätigkeiten**
  - Reduzierung der Anzahl **ungenutzter Accounts** (potentielle Angriffsquelle)
  - Reduzierung der Missbrauchs- bzw. Angriffsmöglichkeiten durch transparente „**doppelte Buchführung**“ (**Soll <-> Ist**)
  - **Eindeutige Verknüpfung** zwischen Unternehmensmitarbeiter und IT-Benutzer
  - Auswertungen als Basis zur effizienten **Kontrolle** und ggf. Korrektur von Berechtigungen (Mitarbeiterstamm, **Soll**, **Ist**, Historie, Audit)

< Steigende externe Anforderungen, z.B. Basel II, §25aKWG, KonTraG ! >
< Steigende interne Anforderungen: Revision, Datenschutz, IT-Security ! >

Beispiel - Kostenkomponenten (1)

- Projektkosten
  - Projektmanagement/Kommunikation (15%)
  - Vorstudie (5%)
  - Anforderungsdefinition (10%)
  - Marktanalyse/Produktauswahl (5%)
  - Lizenzkosten/Hardwarekosten (10%)
  - Feinkonzept/IT-Konzept (10%)
  - Entwicklung/Konfiguration/Test (30%)
  - Implementierung/Pilot (7,5%)
  - Dokumentation/Schulung (7,5%)

< Hoher Kommunikationsaufwand ! >
< Trotz Standardprodukt hoher Anteil der Entwicklungskosten ! >
< Keine Schulung der „normalen“ Benutzer ! >

Beispiel - Kostenkomponenten (2)

- Anschlusskosten (Roll-Out)
  - Fachliche Anwendungsbetreuung (30%)
    - Koordination und Kommunikation
    - Abschluss Leistungsvereinbarung (inkl. Take-On-Template)
    - Funktionaler Test
    - Funktionale Dokumentation
  - Technische Anwendungsbetreuung (30%)
    - Durchführung der Anbindung
    - Test der Anbindung
    - Technische Dokumentation
  - Systemverantwortlicher IT-System (40%)
    - Abschluss Leistungsvereinbarung
    - Lieferung Systemdaten
    - Funktionaler Test, Abnahme

< Abhängig von Anbindungsart, Komplexität der Rechtestruktur und des Workflows (10-40 PT pro System) ! >

Beispiel - Kostenkomponenten (3)

- Laufende Kosten
  - Anwendungsbetreuung funktional (20%)
    - Funktionale Pflege und Weiterentwicklung
    - Generelle funktionale Fragen und Probleme
    - Kontrollfunktion, spezielle Auswertungen
  - Anwendungsbetreuung technisch (20%)
    - Wartung und Betreuung
    - Technische Fragen und Probleme
  - Systemadministration (30%)
    - Interne Systemadministration
    - Fragen und Probleme Systembenutzer
  - Hardwarekosten (15%)
    - Entwicklungs-, Test- und Produktionsumgebung
  - Softwarekosten (15%)
    - Lizenzgebühren, Professional Service

< Ohne Anschlusskosten, diese wurden bereits separat berücksichtigt ! >

Beispiel - Kostenkomponenten (4)

- Refinanzierung
  - Projektkosten
    - IT-Dienstleister/Anwendungsverantwortlicher per Umlage
    - Hauptnutzerträger per Verrechnung des Nutzens
  - Anschlusskosten (Roll-Out)
    - Standard: Jede Partei trägt den eigenen Aufwand
    - Non-Standard: Zusatzleistungen müssen separat vereinbart und vom Systemverantwortlichen des IT-Systems getragen werden
  - Laufende Kosten
    - IT-Dienstleister/Anwendungsverantwortlicher per Umlage

< Direkt zurechenbare Kosten sollten verrechnet werden ! >

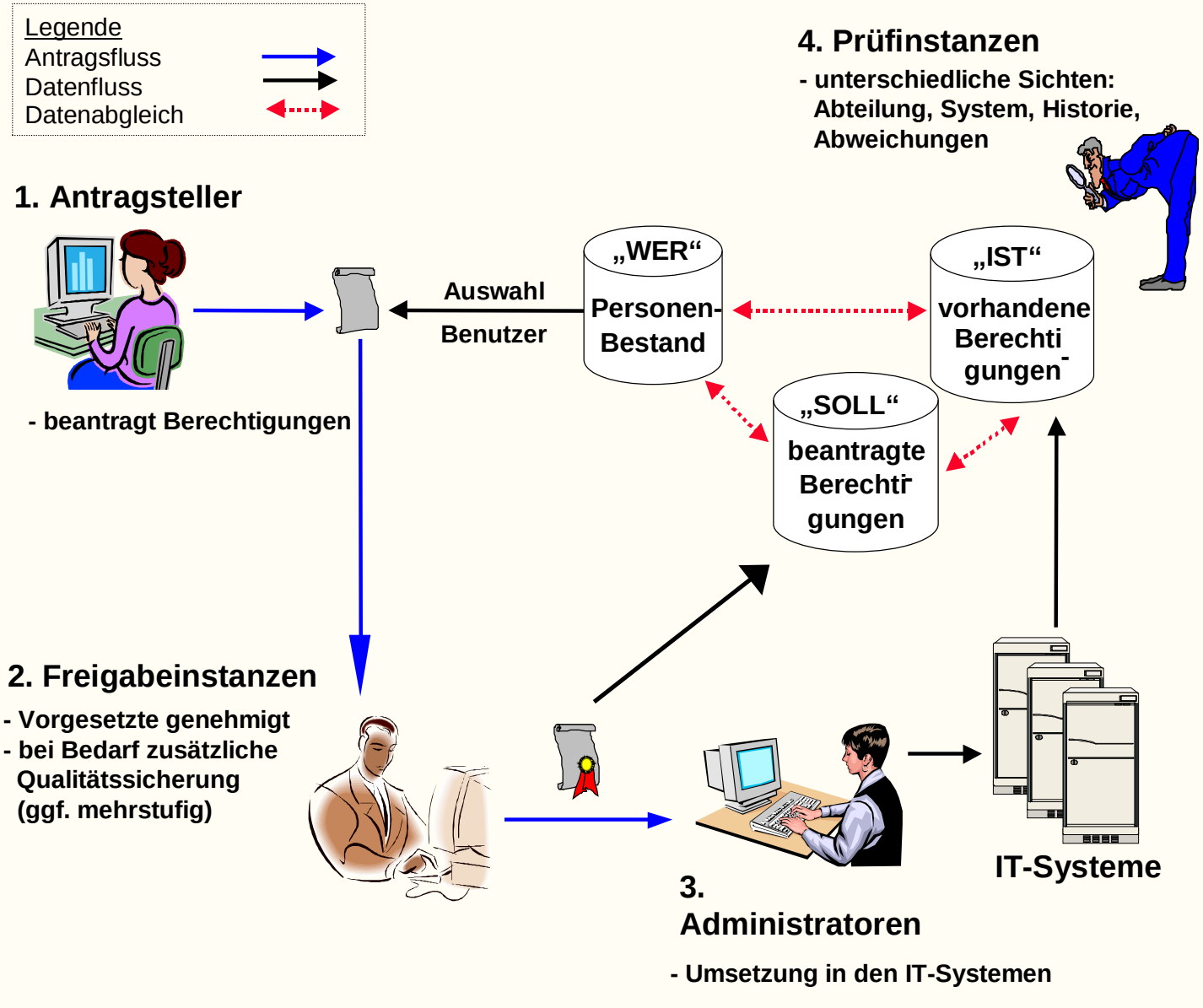
< Beidseitige Bestätigung als Voraussetzung ! >

< Umlageverfahren meist leichter durchzusetzen ! >

Modell

- Regelkreis des Access Rights Management
- Komponenten des Regelkreises
- Schnittstellen des Regelkreises

Modell – Regelkreis des Access Rights Management



Modell – Komponenten des Regelkreises (1)

1. Antragsverfahren
   - Elektronisch unterstütztes Antragsverfahren
   - Auswahl des Antragsbetroffenen aus Mitarbeiterstamm
   - Systemspezifische Antragstemplates (möglichst standardisiert)
     - Einrichtung, Änderung und Löschung von Benutzern und Rechten
     - Validierung der Input-Daten
   - Möglichkeit zur Antragsverfolgung
   - Elektronische Archivierung
2. Genehmigungsprozess
   - Systemspezifischer Genehmigungsworkflow (Änderung Regelwerk)
   - Möglichst flächendeckenden Standardworkflow festlegen
     - Fachlich Vorgesetzter als erste Prüfinstanz (personelle Verantwortung)
     - Systemverantwortlicher als weitere Prüfinstanz (Systemverantwortung)
   - Ggf. weitere Prüfinstanzen für Sonderfälle
     - Revision, Datenschutz ...
   - Nur autorisierte Personen dürfen als Genehmiger zugelassen sein

Modell – Komponenten des Regelkreises (2)

3. Administration
   - Möglichkeit zur Automatisierung mittels Agenten
   - Schnittstelle für manuelle Administration
   - Berechtigungsprüfung erfolgt weiterhin durch die Zugriffssteuerungssysteme der IT-Systeme
4. Berechtigungsevidenz
   - Globale Evidenz über Benutzer und Rechte
     - **Ist**: durch regelmäßigen Input aus den IT-Systemen
     - **Soll**: die komplett genehmigten Anträge stellen das Soll dar
   - Kontroll- und Auswertungsmöglichkeiten
     - **Ist <-> Soll**: Administrationsfehler, Hacker
     - Mitarbeiterstamm **<-> Ist**: Ausscheiden, Abteilungswechsel (WF-Trigger)
   - Unterschiedliche Sichten und Anforderungen
     - Abteilungssicht (fachlich Vorgesetzter)
     - Systemsicht (Systemverantwortlicher)
     - Abweichungen, kritische Rechte, Historie (Revision, Datenschutz)
   - Kann als Grundlage zur Bildung von Geschäftsrollen dienen

Modell – Schnittstellen des Regelkreises

- Mitarbeiter-/Organisationsdaten
  - Anbindung an die Personalverwaltung zur eindeutigen Verknüpfung zwischen dem Unternehmensmitarbeiter und dem IT-Benutzer
  - Redundanzkontrolle der Mitarbeiterstammdaten in den Berechtigungsdaten
  - Anträge nur für aktive Unternehmensmitarbeiter (intern und extern) möglich
  - Organisatorische Änderungen als automatischer WF-Trigger
    - Ausscheiden MA -> Sperrung bzw. Löschung Accounts
    - Neuer MA -> Einrichtung Standardrechte
    - Abteilungswechsel -> Entzug von Abteilungsrechten
  - Beziehung MA <-> fachlich Vorgesetzter
    - Sicherheit im Genehmigungsverfahren
    - Abteilungssicht in Auswertungen
- IT-Systeme
  - Manuelle oder automatisierte Administrationsschnittstelle
  - Regelmäßiger Abgleich der IST-Daten (Accounts, Rechte, Rollen)

Checkliste Referenzkundenbesuch

- Workflowkomponente
- Maskenbearbeitung
- Agenten und Schnittstellen
- Rollen- und Berechtigungsstruktur
- Performance
- Reporting
- Sicherheit
- Aufwände
- Weitere Problempunkte

Checkliste Referenzkundenbesuch (1)

- Workflowkomponente
  - Oberfläche und Flexibilität des Prozessmodellierungstools
  - Definition von Eskalationswegen
  - Mailanbindung, Arbeitskorbdefinition oder anderweitige Benachrichtigungen sowie Sicherstellung der Mailzustellung
  - Monitoring- und Workflow-Administrations-Funktionen (Suspend-, Restart- und Rollbackmöglichkeiten bei auftretenden Fehlern)
  - Schleifen, Varianten und Rücksprünge innerhalb von Prozessen (Kategorisierung von Prozessvarianten abhängig von IT-Ressource oder Organisationseinheiten) und parallele Abarbeitung von Workflow-Aktivitäten
  - Zeitversetzt startende, ereignisgesteuerte und zyklische Prozesse (z.B. Überprüfen des Ablaufens von Gültigkeiten)
  - (mehrstufige) Vertreter- und Abwesenheitsregelungen und Übertragung von Aktivitäten zur Laufzeit (z.B. bei Abwesenheiten)
  - Festlegung von Workflow-Rollen (vorgegeben, frei festzulegen - abhängig von IT-Ressource, Organisationseinheit) zur Prozesslaufzeit
  - automatisches Anstoßen eines Prozesses durch einen anderen (keine Subprozesses)
  - Definition von Bedingungen

Checkliste Referenzkundenbesuch (2)

- Workflowkomponente
  - Festlegung von Gültigkeitszeiträume (von Accounts, Benutzern etc.) und davon abhängigen Regeln
  - Konsistenzprüfungen innerhalb der Prozesse (relevant für Stammdatenänderung zur Laufzeit) wie zum Beispiel Behandlung von Genehmigeränderung während Prozesslaufzeit
  - Loggingmöglichkeiten, Revisionsinformationen
  - mehrfach nutzbare Prozesse / Prozessblöcke
  - Prozess-Synchronisation (Behandlung voneinander abhängiger Anträge, z.B. bei Löschen eines Antrags)
  - Anzahl und Art der benötigten Workflow-Prozesse (Subprozesse, mehrfach verwendbare etc.)

Checkliste Referenzkundenbesuch (3)

- Maskenbearbeitung
  - Definitionsumgebung für Masken (Beurteilung der grafischen Oberfläche und Skripterstellung: Flexibilität und Komfortabilität, Programmiersprache, Erstellungsprozess, Hinterlegung der Masken in Datenbank oder als Datei, Layoutanpassbarkeit)
  - Anpassbarkeit / Flexibilität der Nutzung von Datenbankfeldern (fest vorgegeben oder als Maskenfelder frei definierbar, z.B. für die Ablage von Projektdaten für im Rahmen von Projekten gestellte Anträge)
  - Integrierbarkeit von Feldtypprüfungen und anderen logischen (semantischen und syntaktischen) Prüfungen in Masken
  - Aufgabenaufteilung Client / Server (clientseitige Prüfungen, Hinterlegung von Cookies, Laden von Anwendungskomponenten auf dem Client bei Start)
  - rollenabhängige Masken (Datenverantwortlicher, Administrator, Vorgesetzter)
  - (kontextsensitive) Hilfe
  - zur Verfügung gestellte Maskenelemente (DropDown-Listen, Checkboxen etc.)
  - integrierte Such- und Sortierfunktion
  - Definitionsmöglichkeit für Pop-up-Fenster (für Bestätigungen, Sicherheitsabfragen, Hinweise)

Checkliste Referenzkundenbesuch (4)

- Agenten und Schnittstellen
  - Komfortlabilität der Entwicklungsumgebung für Agenten (verfügbare Tools, Testmöglichkeiten, erforderliche Programmiersprachen)
  - Konfiguration von Standardagenten und Erstellung von Agenten für Eigenanwendungen
  - Funktionsweise und Konfiguration des Deltaabgleichs mit Zielsystemen
  - Berechtigungs- und Rollenkonzept (Abstraktionsgrad / Behandlung der unterschiedlichen Berechtigungsstrukturen der verschiedenen IT-Ressourcen)
  - User- und Organisationsdatenabgleich (welche Schnittstelle, wie oft, batch/online/ manuell, was passiert bei kurzfristigen Datenänderungen, z.B. ein Nutzer wechselt die Abteilung)
  - Notwendige Schnittstellenarbeiten seitens des Zielsystems (Datenimport, bidirektionaler Abgleich, Schnittstellenvereinbarungen, Konfigurationen)

Checkliste Referenzkundenbesuch (5)

- Rollen- und Berechtigungsstruktur
  - Festlegung von Rollen für spezifische GUIs und Rechte bei Beantragungsprozessen für das System selbst
  - von der Abteilungs- bzw. Unternehmenszugehörigkeit abhängige Sichten und Rechte
  - Administrationsrolle und -berechtigungen für das System
  - Abbildung der Rollen/Rechte aus den Zielsystemen
  - Rollenconstraints für die Zielsysteme
- Performance
  - Erfahrungen hinsichtlich Performance (Datenabgleich, Lasttest, Antragabarbeitung)
  - Performance der Nutzeroberfläche (Geschwindigkeit beim Laden der Masken, Datenbankabfragen)
  - Beispielhaft Dauer für Generierung eines Standardreports (alle Anträge mit Status für einen Benutzer)

Checkliste Referenzkundenbesuch (6)

- Reporting
  - Definition von Standardberichten (Benutzer, Genehmiger, Administrator)
  - Historisierung (Revisionsberichte, Audittrail) der Antragsdaten in den Zielsystemen
  - Reports zu Schnittstellen und zum Deltaabgleich
  - Anzeigen von Eskalationsvorgängen für einzelne Anträge
  - individuell zur Laufzeit definierte Berichte
  - weitere rollenabhängige Berichte
- Sicherheit
  - Auswirkungen von Inkonsistenzen (z.B. bei Stammdatenimporten) auf das Gesamtsystem
  - Mitteilung von Accounts und Passwörtern
  - Sicherheitsrestriktionen bei der Anbindung von Zielsystemen bzw. für den Anschluss der Personendaten (HR-System)
  - verschlüsselte Kommunikation und abgeschottete Server

Checkliste Referenzkundenbesuch (7)

- Aufwände und andere Problempunkte
  - Aufwand für Initialdatenimporte von Personal- und Organisationsdaten und dabei auftretende Probleme
  - Aufwand und Probleme bezüglich Berechtigungsinformationen der Zielsysteme
  - Aufwand für Agentenerstellung und Anschluss einer Ressource inkl. Schnittstellenvereinbarung
  - Aufwand für Definition und Implementierung der Prozesse
  - Aufwand für Testphase und Fehlerbehebung
  - Aufwand für Schulung und Einarbeitung
  - Benötigtes Know-how (bestimmte Programmiersprachen, Architektur, Entwicklungsumgebungen)
  - Anzahl und Art der tatsächlich angebundenen IT-Ressourcen
  - Nutzerzahlen (als Nutzer verwaltet, selbst aktiver Nutzer des Tools)
  - Aufwand zum Erstellen der GUIs (Zeit pro Maske bzw. pro Prozess)
  - Aufwand zur Realisierung eigener Reports
  - Umgang der auftretenden Dateninkonsistenten
  - Aufwand Betriebsführung (Anzahl Personen, Art der Rollen)

Checkliste Referenzkundenbesuch (8)

- Aufwände und andere Problematiken
  - Ausführlichkeit und Verständlichkeit der mitgelieferten Dokumentation
  - Erfahrungen mit Produktupdates (Konfigurationsmanagement) und Aufwand (Zeit, Personen, Datenumstellung, Test)
  - Erfahrungen mit Nutzerfreundlichkeit und Maßnahmen zur Nutzerakzeptanz
  - Erfahrungen mit Helpdesk/Unterstützung des Herstellers
  - Am stärksten unterschätzte Aufwände!!

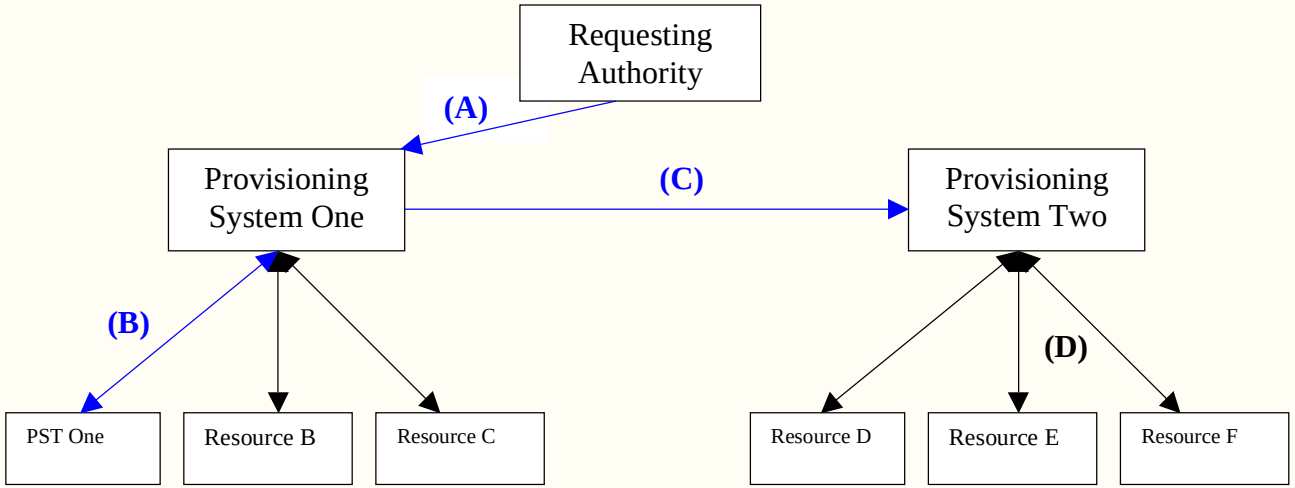
Standards

- SPML - Services Provisioning Markup Language
- SAML - Security Assertion Markup Language
- XACML - eXtensible Access Control Markup Language
- XKMS - XML Key Management Specification
- WS-Security

SPML - Services Provisioning Markup Language

- Die *Organization for the Advancement of Structured Information Standards* (OASIS) definiert ein Austauschformate für Provisioning-Daten.
- *Services Provisioning Markup Language* (SPML).
- Sie soll die Vergabe von Zugriffsrechten an elektronische System automatisieren zu helfen.
- Diese Initiative berücksichtigt die Ergebnisse von ...
  - Active Digital Profile (**ADPr**),
  - eXtensible Resource Provisioning Management (**XRPM**) und
  - Information Technology Markup Language (**ITML**),
- Die Freigabe als Standard durch die OASIS Mitglieder steht unmittelbar bevor.

SPML



- A high-level schematic of the operational components of an SPML model system.
- In SPML request flow A the Requesting Authority (client) construct an SPML document subscribing to a pre-defined service offered by Provisioning System One.
- System One takes the data passed in this SPML document, constructs it's own SPML document and sends it to PST One (SPML request flow B).
- PST One represents an independent resource that provides an SPML compliant service interface.
- In order to fully service the initial Requesting Authorities request, Provisioning System One then forwards a provisioning request (SPML request flow C) to a second network service called Provisioning System Two.
- System Two is autonomously offering a provisioning service it refers to as Resource E.
- In this case Resource E is a relational database within which System Two creates some data set.
- Having successfully received Provisioning System One's request, Provisioning System Two carries out the implementation of its service by opening a JDBC connection to Resource E and adding the relevant data.
- In this example, the SPML document flows follow a simple request/response protocol flow that supports both synchronous and asynchronous operations.
- Importantly, these SPML flows are initiated unidirectional.
- When System One made a request of System two, it assumed the role of a Requesting Authority and initiated it's own request/response flow with it's chosen service point.
- When System Two implemented its service at Resource E, it did not use an SPML protocol message as Resource E does not support SPML.

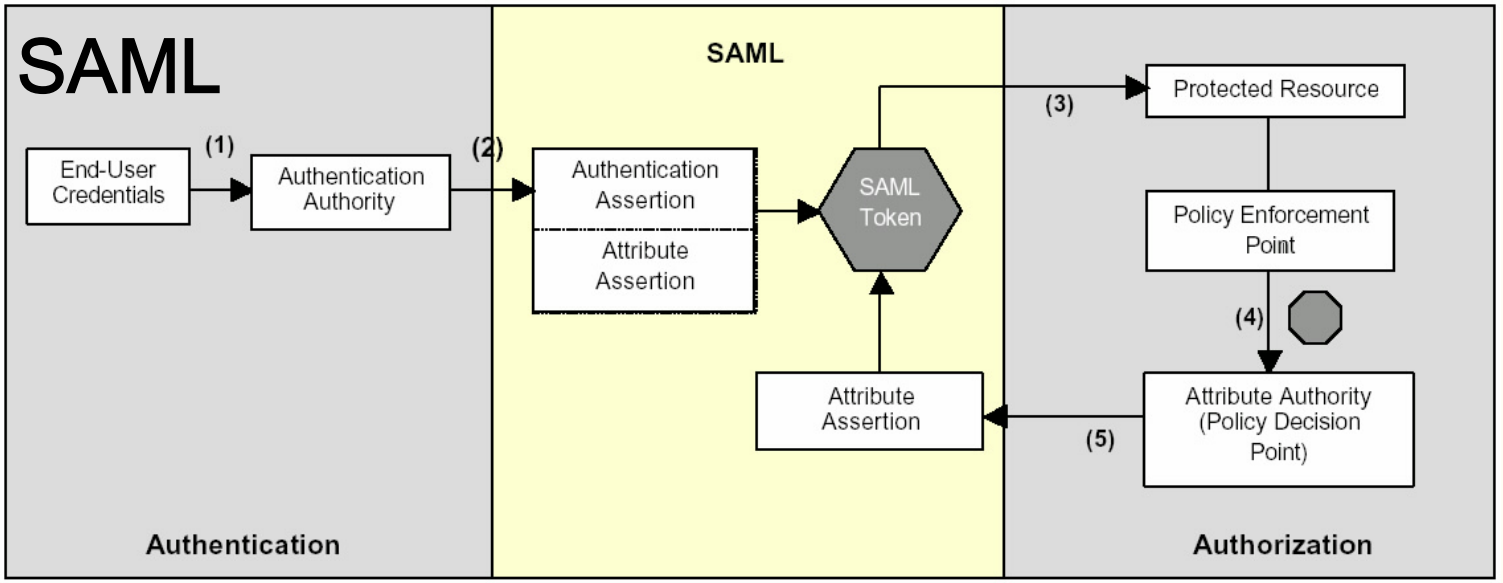
SPML – Beispiel: Laden von Massendaten

```
<?xml version="1.0" encoding="utf-8"?>
<batchRequest xmlns ="urn:oasis:names:tc:SPML:1:0:req" xmlns:spml="urn:oasis:names:tc:SPML:1:0:core">
  <spml:addRequest>
    <spml:identifier type="urn:oasis:names:tc:SPML:1.0:core#GUID">
      <spml:id>584D268K</spml:id>
    </spml:identifier>
    <spml:attributes>
      <attr name="objectclass" xmlns="urn:oasis:names:tc:DSML:2:0:core">
        <value>BasicAccount</value>
      </attr>
      <attr name="id" xmlns="urn:oasis:names:tc:DSML:2:0:core">
        <value>584D268K</value>
      </attr>
      <attr name="firstname" xmlns="urn:oasis:names:tc:DSML:2:0:core">
        <value>Jane</value>
      </attr>
      <attr name="lastname" xmlns="urn:oasis:names:tc:DSML:2:0:core">
        <value>Doe</value>
      </attr>
    </spml:attributes>
  </spml:addRequest>
  …
```

SAML - Security Assertion Markup Language

SAML - Security Assertion Markup Language ist …

- Ein ***Framework*** für den Austausch von Sicherheitsinformationen, sog. *Assertions* (Feststellungen)
- Diese Assertions der **Authentisierung** und **Autorisierung** werden in XML-Dokumenten ausgedrückt.
- SAML bietet Lösungen für ...
  - *Identity Federation*
    - Eine Technologie, die es Unternehmen ermöglicht seine Lieferanten und Kunden als sicher als Anwender seiner Systeme zu berechtigen.
  - Eine feinkörnige Authentisierung
    - Anwender können von einer Stelle authentisiert werden und von einer anderen autorisiert werden.
- SAML Profile beschreiben die Arbeitsweise ...
  - Ein Web Browser Profil für ein Single-Sign On
    - Ist Teil von SAML 1.0
  - Ein WS-Security Profil für die Absicherung von Web-Services
    - Ist Teil von SAML 2.0



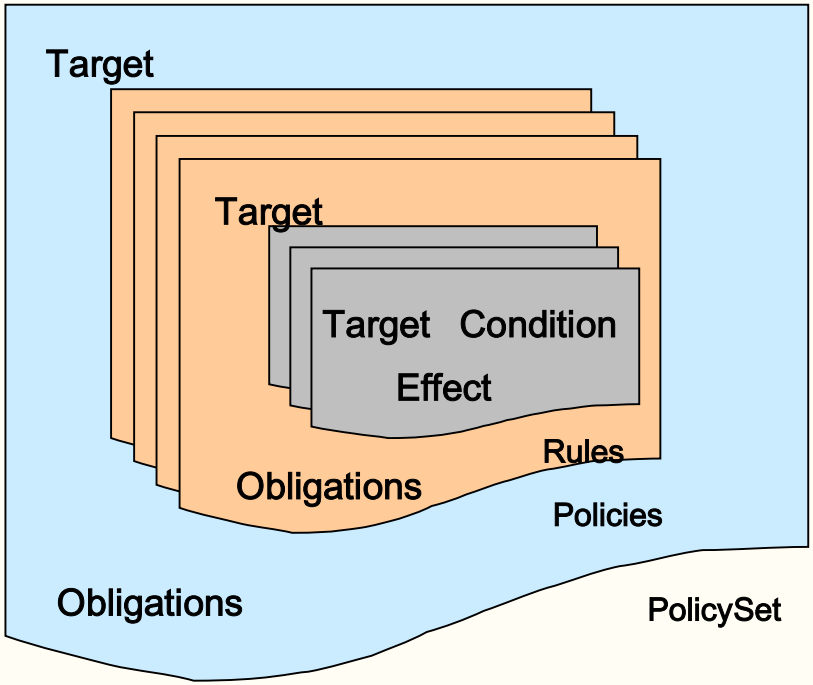
1. Der Benutzer reicht Zertifikate an die *Authentication Authority* ein (eine Security Engine oder SAML-bereite Fachanwendung).
2. Die *Authentication Authority* bestätigt die Benutzerzertifikate an Hand des Ben-utzerverzeichnisses und erstellt eine *Authentication Assertion* und with eine oder mehr *Attribute Assertions* (d.h., eine Rolle oder eine anderes Benutzer-profil). End-User ist nun authentisiert und identifiziert und *SAML Assertions* in einem *Token* zusammengestellt.
3. End-user will nun damit auf eine geschützte Ressource zugreifen.
4. Der *Policy Enforcement Point (PEP)* fängt seine Anfrage ab und reicht End-Users *SAML-Token* (*Authentication Assertion*) an die *Attribute Authority* weiter. (oder eine SAML-bereite Sich-erheits-Engine oder Fachanwendung.
5. *Attribute Authority* oder *Policy Decision Point (PDP)* entscheiden nach ihren Richtlinien. Bei Genehmigung erstellt er eine, an den *SAML-Token* angehängt, *Attribute Assertion*. End-User kann sich mit dem *SAML-Token* gegenüber allen beteiligten Geschäfts-partnern ausweisen..

XACML - eXtensible Access Control Markup Language

- Die *eXtensible Access Control Markup Language* (XACML) ist eine vom *Technical Committee* der OASIS definierte Regelsprache zur automatisiert auswertbaren Dokumentation von Policies.
- **Policies** sind Geschäftsregeln, die Berechtigungen und Zuständigkeiten festlegen und die zugehörigen Gültigkeitsbedingungen definieren.
- Beispiel: „*Ein Mitarbeiter von Human Ressources (HR) darf Lohnkonten von Angestellten des Hauses unterhalb der Vorstandsebene einsehen und verändern, ausgenommen sein eigenes*“.
- XACML wird in XML abgebildet und verwendet **SAML** (Security Assertions Markup Language) für den Austausch von Authentisierungs- und Autorisierungsinformation.

XACML-Konzepte

Die XACML-Begriffswelt dreht sich um eine Formalisierung des Autorisierungsprozesses.



- **Policy & PolicySet** – anwendbare Grundregeln.
- **Target** – Index-Tabelle, um schnell anwendbare Regln zu finden.
- **Conditions** – Beliebige logische Ausdrücke (+ arithmetische & Zeichenkettenoperationen)
- **Effect** – “Permit” oder “Deny”
- **Obligations** – weitere erforderliche Operationen.

SAML und XACML

- OASIS hat die *Extensible Access Control Markup Language* (XACML) Version 1.0 herausgegeben.
- Mit XACML soll ein XML soll ein Schema für die Darstellung von Berechtigungen bereit stehen.
- XACML soll damit SAML (Schwerpunkt: Authentisierung) ergänzen.
- Fachleute sehen jedoch funktionale Überlappungen zwischen SAML und XACML (in der aktuellen Version).
- Zwischen beiden OASIS-Arbeitsgruppen besteht noch Abstimmungsbedarf.
  - OASIS: <http://www.oasis-open.org/>
  - Liberty Alliance Project: <http://www.projectliberty.org/>

XKMS - XML Key Management Specification

- *XML Key Management Specification* (XKMS) ermöglicht die Behandlung öffentlicher Schlüssel in Anwendungen.
- XKMS soll damit XML-basierten Clients PKI -Funktionen verfügbar machen.
- Verlagert die Behandlung vieler operativer PKI-Funktionen vom Client zu einem Back-End-Server
  - Die mächtigen Funktionen ermöglichen einfachere Clients
- Kapselt die traditionelle PKI
- Erfordert SOAP und UDDI
- Eine bestehende PKI ist damit Voraussetzung.
- Das Konzept der *Public-Key Infrastructure* ist jedoch noch nicht flächendeckend umgesetzt.
- Vermutlich sich werden beide in einer Ko-Evolution entwickeln.
- Web Services benötigen die Unterstützung von ...
  - XKMS public-key management
  - SAML,
  - XML encryption (XML Enc),
  - XML signing (XML Dig Sig) und
  - WS-Security

WS-Security

- Initiatoren
  - IBM, VeriSign, Microsoft, Sun
- Generische Spezification zum Schutz von SOAP-Nachrichten, incl. SAML
- Die Sicherheitserweiterungen im SOAP-Header betreffen …
  - Integrität
  - Verschlüsselung
  - Authentisierung
- Verwendet vorhandene XML-Standards (Verschlüsselung, Digitale Signature)
- Sicherheits-Tokens: unterstützen ..
  - Name / Passwort,
  - X.509 und
  - Kerberos tickets

Wichtige XML-Standards für Web Services

Im Rahmen der Verwendung von Web Services können weiter wichtig sein …

- SOAP (Simple Object Access Protocol)
  - RPC and Message passing protocol
- WSDL (Web Services Definition Language)
  - interface definition language
- UDDI (Universal Description, Discovery & Integration)
  - protocol for finding services and resources
- ebXML
  - eBusiness standard from U.N + OASIS