

# Identity Management aus Sicht von Organisation & Technik

UP

UP

**Expert Talk**  
@ devoteam consulting

devoteam  
consulting ↑

# Vorstellung

## ■ Martin Eßlinger

- Ausbildung: Studium an der TU-Wien (technische Physik)
- Zertifizierter IS Manager, BS7799 Auditor und CISSP
- E-mail: Martin.Esslinger at devoteam.at



## ■ Partner bei Devoteam Consulting in Wien

- Seit 10 Jahren im Unternehmen als Berater tätig
- Verantwortlich für das gesamte Produktportfolio von Devoteam Consulting im Bereich der Informationssicherheit
- 15 Jahre Berufserfahrung im IKT-Bereich

## ■ Primäre Arbeitsbereiche der letzten Jahre:

- Management der Informationssicherheit
- Risikomanagement
- Business Continuity Management
- IKT Architektur

# Schlagwort Identity Management

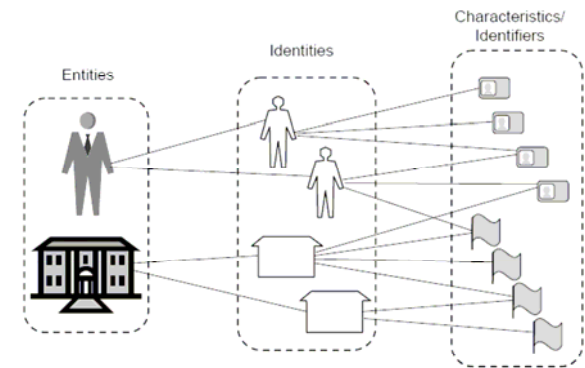
- **Der Identity Management Markt ist durch eine beinahe unüberschaubare Vielfalt geprägt.**
  - Gartner listet für 2007 ca. 20 weltweite Anbieter für „user provisioning“
  - Unterschiedliche Sichtweisen auf die Prioritäten (IT-Themen vs. Organisation und Prozesse)
  - Unterschiedlicher Kontext (Enterpriselösungen vs. Kundenlösungen)
  
- **Wer braucht das?**
  - Regulierte Unternehmen (Finanz, Gesundheit, EVUs)
  - E-Government Bereich
  - Bildungsbereich (Schulen, Universitäten)
  - Industrie (Wartung der Rollen und Rechte in ERP Systemen)
  - Unternehmen mit hoher Mitarbeiterfluktuation (z.B. Handel)
  - Managed IT Service Provider
  - Privatpersonen

# Definitionen

## ■ ISO/IEC: Identity Management (IdM) umfasst:

- die sichere Verwaltung von **Identitäten**
- den Identifikationsprozess einer **Einheit** (inkl. optionaler Authentisierung)
  - Eine „Einheit“ kann alles sein, was eindeutig als solche erkannt werden kann (Person, Tier, Gerät, Objekt, Gruppe, Organisation, etc.)
  - Einheiten können mehrere Identitäten haben, die in verschiedenen Kontexten verwendet werden können.
- die **Information**, die mit der Identifikation bestimmten Kontexts verbunden ist.

Quelle: ISO/IEC JTC 1/SC 27/WG 5 „A framework for IdM“



## ■ ITU-T: Der Begriff IdM wird als Verwaltung von Attributen einer Einheit verstanden (z.B. Kunde, Gerät oder Provider).

- Die Verwaltung digitaler Identitäten ist nicht dazu gedacht, um Personen zu validieren.

Quelle: ITU-T IdM-GSI

# IdM Konzepte

- **Isolierte Benutzer und Berechtigungsnachweise pro Anwendung**
  - Been there, done that...
  
- **Zentralisierte Benutzerverwaltung**
  1. Single Sign On (SSO) Identitätsdomäne (z.B. Kerberos, .Net Passport)
  2. Meta-Verzeichnisse (Synchronisation von Identitäten über verschiedene Domänen)
  3. Gemeinsame Benutzeridentität/Zertifikat für alle Services (PKI)
  
- **Föderales Model mit einer virtuellen Identitätsdomäne**
  - Trennung des „Identity Service Provider“ vom IT-Service Provider (z.B. SAML, Liberty Alliance, Shibboleth)
  
- **Benutzerzentrierte Modelle**
  - z.B. OpenID, CardSpace, Passwort Stores (virtuelles SSO)
  - Verwendung eines „Personal Authentication Device“ (HW oder SW)

# IdM im Enterprisebereich

## ■ IdM + Access Management = IAM

- Verwaltung und Durchsetzung der Zugangskontrolle auf IKT-Systemen
- Schlagworte: Policy Administration/Enforcement, User-Provisioning

## ■ Typische Funktionsgruppen in IAM-Tools:

- Verwaltung von digitalen Identitäten (Benutzerattribute, Rollen, Berechtigungsnachweise) über Prozesse und Workflows
- Verifikation der Identität (Validierung und Authentisierung inkl. SSO)
- Zugriffsteuerung (Web-Access, OS-Access, Applications, Network Access, Verschlüsselung, DRM, Content Filtering, etc.)
- Audit und Reporting Funktionen

## ■ Basis für IAM-Tools sind meist Verzeichnisdienste

- Meta- oder virtuelle Verzeichnisse
- Integration von heterogenen Verzeichnissen (AD, NDS, X.500)

# IdM im Enterprisebereich

- **Weitergehende Funktionen von IAM-Lösungen erlauben die Administration bzw. automatische Provisionierung von:**
  - Rollen (z.B. „Role Mining“ Funktionen)
  - IT-Ressourcen (z.B. neue Gruppen, neue Laufwerke),
  - Berechtigungsnachweisen (Smartcard, Zertifikat, Passwort, etc.)
  - Nicht IT-bezogene Ressourcen (Schlüssel, Handys, Zutritt, etc.)
- **Kombination von IAM und Security Information and Event Management Tools (SIEM)**
  - Komplementär zu dem in einem IAM System integrierten Funktionen
  - Speziell wichtig für regulierte Unternehmen
  - Kosten für Audit Compliance in die TCO Berechnung für das IAM-System mit einbeziehen!

# Treibende Faktoren für IAM Lösungen

## ■ Wettbewerbsvorteile

- „Self-Service“ Lösungen, personalisierte Portale, Outsourcing-Möglichkeiten, verbesserte Kundenbindung

## ■ Kosteneinsparung

- Personalaufwand (IT/Security Administration, Helpdesk)
- Vereinheitlichte IAM Architektur
- Mitnutzung für nicht IT Themen (el. Zutrittskontrolle, Handys, Karten)

## ■ Operative Exzellenz

- Verbesserte SLAs (z.B. Garantie für die Dauer einer bestimmten Provisionierung nach Eingang des Antrags)
- Verbesserte Produktivität (frühere Nutzbarkeit von Diensten)
- Verbesserte Benutzerfreundlichkeit
- Vereinfachtes Reporting (Security Administration)

# Treibende Faktoren für IAM Lösungen

## ■ IT Risikomanagement

- Vereinfachtes Audit Management
- Zeitnahe Terminierung von Konten bzw. Rechten
- Konsistente Anwendung und Prüfung von Policies
- Bessere Rollentrennung und Granularität („need to know“)
- Breitere Nutzbarkeit von starker Authentisierung
- Bessere Nachvollziehbarkeit von Aktivitäten (Logging/Audit)
- Vorbeugende Risikoerkennung (z.B. Betrug)

## ■ Compliance (regulatorisch, gesetzlich, vertraglich)

- SOX/EuroSOX
- Gesundheitstelematikgesetz, Datenschutzgesetz
- ISO/IEC 27001
- Wirtschaftsprüfer
- Rating Agenturen

# Prozess oder Technologie?

- **Typische Aussagen von Herstellern und IT-Verantwortlichen zu IAM lauten:**
  - „Das ist kein technisches Problem, die Vorgaben auf der organisatorischen Seite fehlen“
  - „IAM ist 80% Prozesse und nur 20% Technik“
- **In der Realität kann derzeit kein am Markt verfügbares IAM-System alle Anforderungen „out-of the box“ abdecken.**
  - Die IAM-Suiten der führenden Hersteller decken den „üblichen“ Bedarf (aus Sicht der großen US-Unternehmen) gut ab.
  - Es gibt viele Anbieter, die spezielle Anforderungen optimal abdecken, und dafür in anderen Bereichen wieder schwächer sind.
  - Wie immer steckt der Teufel im Detail, mit unbegrenztem Budget und perfektem Know-How ist kaum ein IT-Projekt ein Problem...
  - Zuerst das Produkt zu entscheiden und dann über die Anforderungen genauer nachzudenken, ist selten eine gute Idee.

# Prozess und Technologie!

- **IAM umfasst den gesamten Lebenszyklus der IAM-Information**
  - Einrichtung, Modifikation, Suspendierung, Terminierung und Archivierung
  - Informationen (Attribute) der Identität verändert sich mit der Zeit und müssen daher sorgfältig verwaltet und geschützt werden
- **IAM ist kein IT-Projekt – ein strategischer und prozessorientierter Ansatz ist jedenfalls erforderlich**
  - Einführung kann nicht einfach an die IT delegiert werden
  - IAM Systeme stellen Technologien zur Unterstützung des prozessorientierten Ansatzes dar
- **Der individuelle Reifegrad der Organisation bestimmt das Verhältnis zwischen Organisation und Technik**
  - Teure IAM-Komplettlösungen in einem „chaotischen“ Umfeld?
  - Best Practice Standardlösungen für spezielle Anforderungen?

# Praktische Empfehlungen

- **Revisionsfunktionen inklusive Datenschutz vorab planen**
  - Wer hat vor 12 Monaten auf diese Datei Zugriff gehabt?
  - Nachträgliche Auswertung differentieller Änderungen fast unmöglich
- **Internes Kontrollsystem des IAM Systems vorher planen**
  - z.B. Alarm, wenn jemand Admin-Rollen anhäuft oder wenn Admin Rechte in der Nacht nur für kurze Zeit vergeben werden
  - Nur Auswertung der Logs im nachhinein problematisch
- **Betriebskonzept für das IAM System erstellen**
  - IAM stellt kritische Funktionen bereit, die entsprechende Skills erfordern (z.B. Umgang mit Rollendesign und Regeleditor)
  - Kleine Änderungen können großen Schaden anrichten
  - Trennung von Entwicklung/Test und Produktion gilt auch hier!
- **Anforderungen an die Eigensicherheit des Systems festlegen**
  - Reicht einem Prüfer ein nicht revisionssicheres System?
  - Analoge Problematik wie bei FiBu Systemen

# Praktische Empfehlungen

## ■ Planung der Prozesse und Rollen

- Kurze Implementierung und dann stetige Migration als Teil der IdM Prozesse („Tag X“ Migrationen funktionieren nicht)
- Von Beginn an alle Quellen für Identitäten berücksichtigen
  - Die heutige Unternehmensrealität umfasst mehr als nur Angestellte aus dem SAP HR System
- Das Rad muss nicht neu erfunden werden - auch im Bereich der Prozesse gibt es generische Vorlagen („GenericIAM“)
- Mischung von Rollen und individuellen Rechten (80/20) als Teil des Designs zulassen
- Zentrales mehrdimensionales Rollendesign aus geschäftlicher Sicht, z.B.
  - Rolle im Unternehmen (angestellt, nicht angestellt), Geschäftliche Rolle in der Geschäftseinheit/Bereich, Kompetenz Rolle bei der Genehmigung, etc.
- Trennung der geschäftlichen Rollen von der Berechtigung auf Ressourcenebene (technische Rolle)
- Gutes Rollendesign ermöglicht eine Rollenzahl von ca. 10% der Benutzerzahl

# Praktische Empfehlungen

## ■ Weitere Tipps (ohne jeden Anspruch auf Vollständigkeit):

- „Schattenbenutzer“ statt spezielle Rollen verwenden, wenn diese in mehreren Prozessen oder Rollen tätig sind
  - Vereinfachung der Rollendesigns
- Antrag für den Entzug einer Rolle vorsehen
  - Dem User steht ein Recht zu, er will oder braucht es nicht auszuüben
  - Kostenreduktion, wenn z.B. eine Applikation nicht benötigt wird.
  - Vereinfachung der Rollendesigns
- Erteilung von Rechten mit der Zustimmung zu Richtlinien verknüpfen
  - Abgeschaut von den shrink-wrap EULAs
- Bedarf nach Revalidierung berücksichtigen
  - Recht muss zum Stichtag, nach einem Intervall oder nach Inaktivität automatisch zur erneuten Prüfung vorgelegt werden (z.B. Forderung aus SOX)
- Workflow-Schritte gruppieren, nicht für jedes Ereignis ein eigene Benachrichtigung schicken

# Praktische Empfehlungen

## ■ Tipps zur Technologie

- Buy not make!
  - Die Marktreife ist vorhanden, eine Inhouse/Individual Programmierung nur in wenigen Spezialfällen konkurrenzfähig
- Provisionierungsfunktionen und Rollentrennung im Bereich der Virtualisierung berücksichtigen
- Trennen von Enterprise Directory und Identity Management System
  - Ausprägung des Enterprise Directory als (unsichtbare) Middleware
  - Wo sich AD als primäres System aufdrängt, ist meist keine gar keine zusätzliche IAM Lösung erforderlich.
- Unterstützung für Serviceorientierung (SOA) berücksichtigen
  - Derzeit nicht Mainstream in IAM-Systemen, Schnittstellen proprietär
- Flexibilität der Lösung beim Rollenmanagement sicherstellen
  - Unterstützung des gesamten Lebenszyklus eine Rolle
  - Hohe Prozessautomatisierung in der Administration anstreben
  - 4000 Rollen mit 10-stelligen Namenskodierungen für 5000 Benutzer sind nicht Stand der Technik...

# Praktische Empfehlungen

- **Speziell beim Access Management relativiert sich oft die Aussage, dass die Technik von IAM Systemen „kein Problem“ ist.**
  - Berechtigungen und Ressourcen werden meist asynchron provisioniert
    - Erwünschtes Verhalten wenn Abweichung Soll-Ist vorhanden?
    - Erwünschtes Verhalten wenn die Ressource knapp oder überlastet ist?
  - Kontextabhängige Berechtigungen können nicht über das IAM-System abgedeckt werden sondern müssen in der Applikation konfiguriert werden.
  - Zugriffskontrollen können nur dann in Echtzeit vom IAM abgefragt werden, wenn die Applikation speziell auf das IAM abgestimmt wurde
  
- **Sorgfältige Abwägung des Kosten-Nutzen Faktors der IAM-Integration einer Applikation erforderlich**
  - Priorisierung vornehmen und schrittweise umsetzen
  - Nicht mit Gewalt eine vollständige Einbindung aller Applikationen fordern

# Ausblick

- **Differenzierende Faktoren für IAM Lösungen in den nächsten Jahren:**
  - Innovationen im Bereich der Architektur einer Serviceschicht (SOA).
    - Standards für eine Interoperabilität in diesem Bereich sind allerdings nicht vor 2010 zu erwarten.
  - Access Management in föderierten Umgebungen (Intranet und Extranet)
  - Verbesserungen und Erweiterungen im Bereich des Reporting, um Governance und Risikomanagement Anforderungen abzudecken
  - Granulares Rollen- und Autorisierungsmanagement für ERP Applikationen
  - Integrierte Funktionen für das Monitoring in Echtzeit und für forensische Analysen

# Impressum



devoteam  
consulting ↑

© Devoteam Consulting GmbH

This document has been prepared by Devoteam Consulting GmbH. It is not to be copied or reproduced in any way without Devoteam Consulting's express permission. Copies of this document must be accompanied by title, date and this copyright notice.

## Devoteam Consulting GmbH Business Unit Austria

Tel.: +43 (0) 1 715 0000-0  
FAX: +43 (0) 1 715 0000-150  
Anschrift: Palais der Schönen Künste  
Löwengasse 47  
A-1030 Wien  
Österreich

E-mail: [office@devoteam.at](mailto:office@devoteam.at)

[www.devoteam.at](http://www.devoteam.at)

Autor:	Martin Eßlinger
Versionsdatum:	2007-10-18
Dateiname:	Expert-Talk_20071018_DC-AT.ppt

### Devoteam Group Business Units:

ALGERIA, AUSTRIA, BELGIUM, CZECH REPUBLIC, DENMARK, FRANCE, ITALY,  
LUXEMBOURG, NETHERLANDS, NORWAY, MAROKKO, POLAND, SPAIN, SWEDEN,  
SWITZERLAND, UNITED KINGDOM, UNITED ARAB EMIRATES and SAUDI ARABIA



GROUP  
DEVOTEAM