Seminar "Smarte Objekte und smarte Umgebungen"

Identity Management

Teil1: Einführung und die „ideale Sicht“ – Systeme aus der Forschung (Bettina Polasek)

Teil2: Die angewandte Sicht - Industrielle Systeme

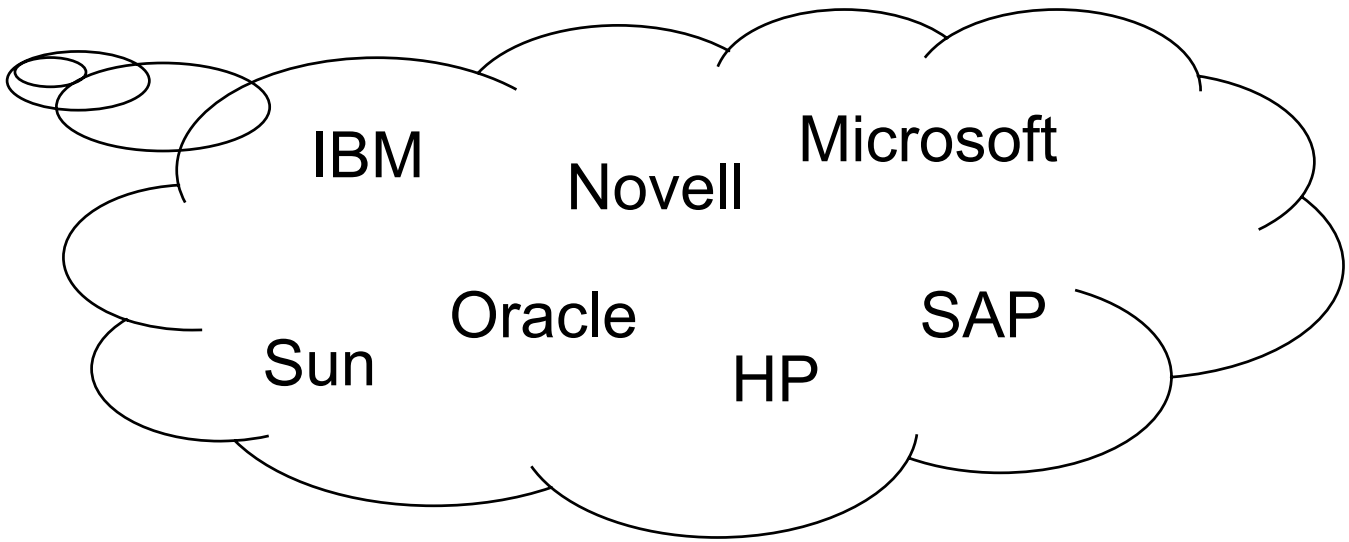
Marcel Beer

IM: Marktüberblick

- Seit einigen Jahren: Verzeichnisdienste
- 1999: Microsoft Passport
- 1999: Meta-Verzeichnisdienste
- 2002/3: Komplette IM Lösungen

IM: Marktüberblick

- Seit einigen Jahren: Verzeichnisdienste
- 1999: Microsoft Passport
- 1999: Meta-Verzeichnisdienste
- 2002/3: Komplette IM Lösungen
- Heute:



Übersicht

- Einleitung:
  - Was versteht die Industrie unter IM?
- Ziele von IM
- Zwei Systeme aus der Industrie
  - Microsoft: „Identity and Access Management“
  - Oracle: „Federated Identity Management“
- Vergleich Forschung-Industrie
- Ausblick

Was ist IM?

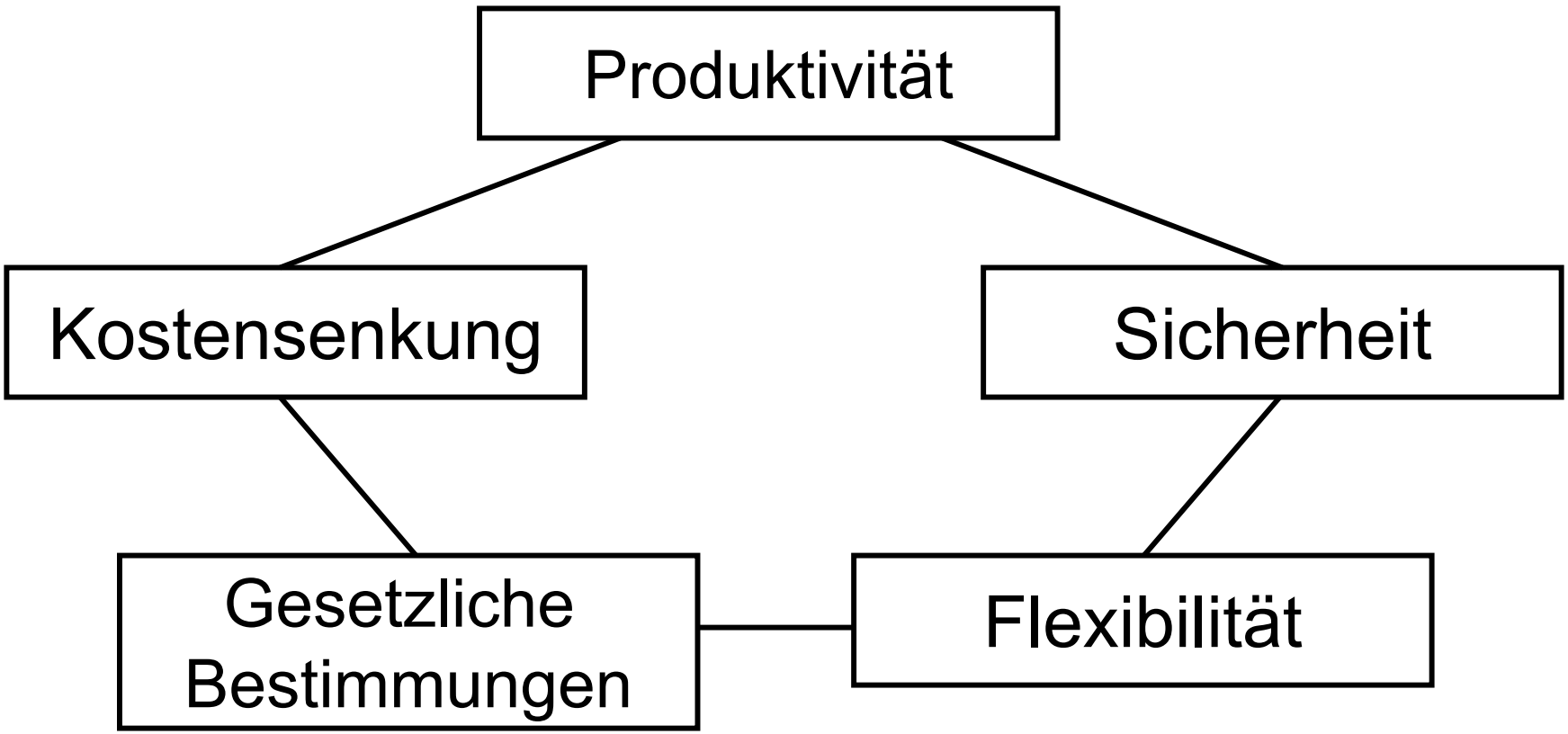
“Identity management is the process by which the complete security lifecycle for end-users and network entities is managed for an organization.” [Oracle]

“Identity and access management combines processes, technologies, and policies to manage digital identities and specify how they are used to access resources.“ [Microsoft]

Status Quo

- ID-Daten auf diverse “Identity-Stores” verteilt
- Anwendungsspezifische Benutzerverwaltung
- Benutzer muss sich mehrere Passwörter merken
- Keine einheitlichen Security-Policies
- Manuelles Erzeugen/Löschen von Accounts
- Austausch von Daten zwischen Firmen / Organisationseinheiten schwierig

Ziele von IM


Produktivität
Kostensenkung
Sicherheit
Gesetzliche Bestimmungen
Flexibilität

Ziele von IM: Produktivität

Produktivität

- Single Sign On
- Weniger vergessene Passwörter
- Automatisches Erstellen/Löschen von Accounts

Kostensenkung

Sicherheit

Gesetzl. Bestimmungen

Flexibilität

Ziele von IM: Sicherheit

Sicherheit

- Einheitliche Authentisierung
- Verwaltung der Benutzer-Rechte
- Zuverlässige Löschung von Accounts
- Bessere Passwort-Policies

Produktivität

Flexibilität

Kostensenkung

Gesetzl. Bestimmungen

Ziele von IM: Flexibilität

Flexibilität

- Vereinfachung der Software-Entwicklung
- Vorteile bei Firmen-Übernahmen / Fusionen
- Bessere Anbindung der Kunden / Partner

Sicherheit

Gesetzl. Bestimmungen

Produktivität

Kostensenkung

Ziele von IM: Gesetzliches

Gesetzliche Bestimmungen

- Einfachere Umsetzung von neuen Richtlinien
  - Datenschutz
  - Archivierung
  - Auskunftspflicht

Flexibilität

Kostensenkung

Sicherheit

Produktivität

Ziele von IM: Kostensenkung

Kostensenkung

- Konsolidierung der ID-Stores
- Automatisierung der Adminstration
- Zeitersparnis für Angestellte/Helpdesk

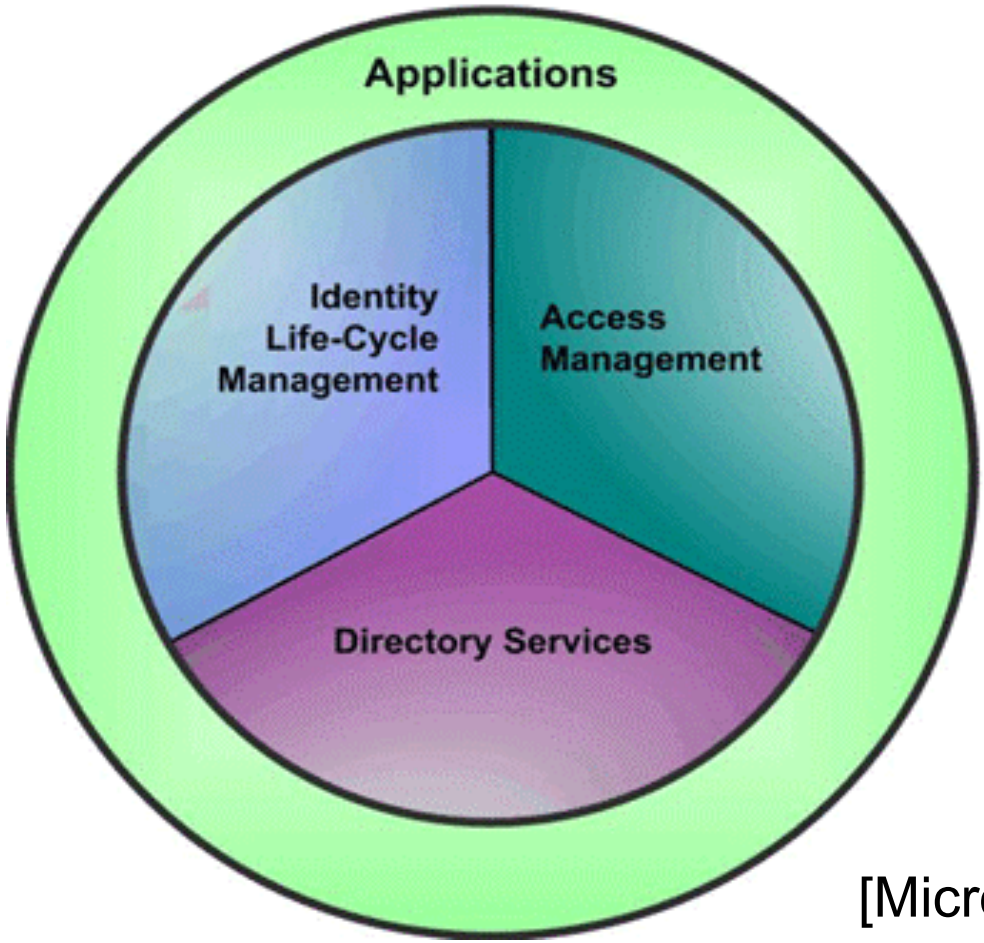
Gesetzl. Bestimmungen

Produktivität

Flexibilität

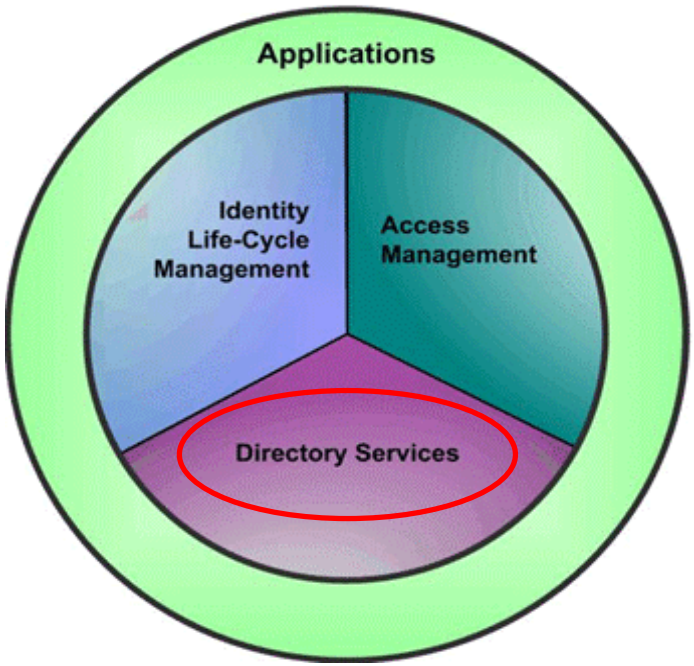
Sicherheit

Microsoft IM Framework



[Microsoft]

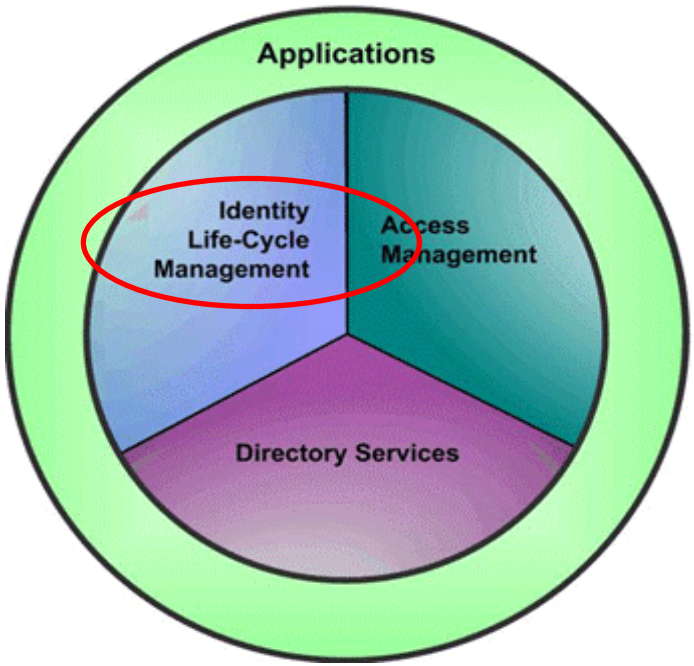
MS: Directory Services



"Active Directory" verwaltet:

- Benutzerprofile
- Rechte
- Passwörter
- Zertifikate

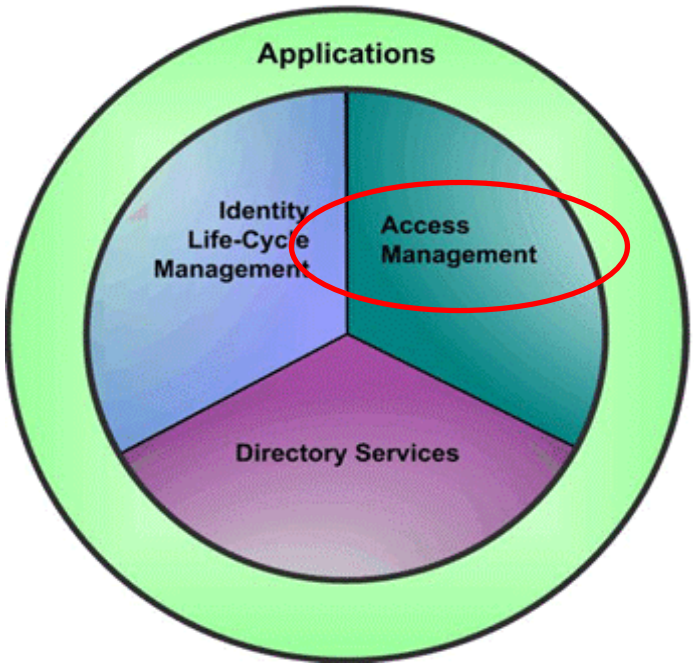
MS: Lifecycle Management



"Identity Aggregation & Synchronization":

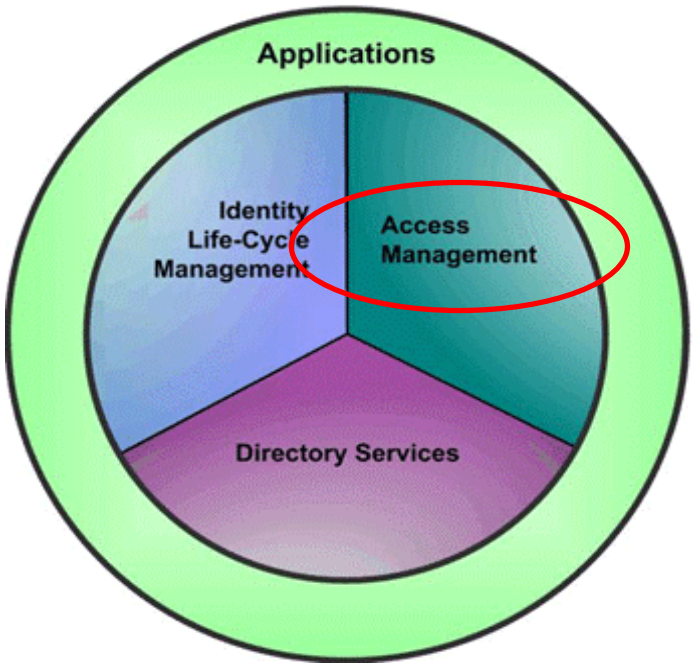
- Zusammenfassen
- Synchronisieren
- Erstellen
- Migrieren
- Löschen

MS: Access Management



- Intranet Zugriff (B2E)
  - Single Sign On (SSO)
  - VPN
- Extranet Zugriff
  - B2E, B2C, B2B
  - Web SSO
- Vertrauensbeziehungen und Federations

MS: Access Management



- Authentisierung
  - Benutzername & Passwort
  - Digitale Zertifikate
  - Biometrische Merkmale
  - Smartcards
  - Kerberos-Tickets
- Autorisierung
  - Access Control Lists
  - Rollenbasiert

Oracle: Federated IM

- Innerhalb einer Firma:
  - Verbinden verschiedener Abteilungen
- Firmenübergreifend:
  - Sichere B2B Handelsbeziehungen
  - Partner, Zulieferer, Outsourcing
- Vertrauensverhältnisse:
  - Vertraglich abgesichert
  - Beidseitig “kündbar”
- Federated Single Sign On für Benutzer

Oracle: Federated IM

Vielfältige Anwendungsbereiche: [Oracle]

- E-Government
  - Datenaustausch zwischen Behörden
- Gesundheitswesen
  - Datenaustausch vs. Privatsphäre
- Bildungswesen
  - Departements-/Universitätsübergreifende Ressourcen und Dienste
- Telekommunikation
  - Ortsabhängige aber anonyme Dienste

Liberty Alliance

- 2001 gegründet von 33 “Big Players”
- Heute über 160 Mitglieder
- Offene Standards für Federated IM & -Services

Resultate:

- Technische Spezifikation die einfaches SSO innerhalb von Federations ermöglicht
- Interface Spezifikationen, Privatsphären- und Sicherheits-Richtlinien für ID-basierte WS
- Richtlinien für Federated IM mit mobilen Geräten

Forschung vs. Industrie

- Forschungssysteme:
  - Endbenutzer im Mittelpunkt
- Industrielle Systeme:
  - IM-Prozesse im Unternehmen verbessern
- Aber: Federated Identity Management - Firma als Endbenutzer: [vom 1. Teil:]
  - Benutzer-Kontrolle
  - Teilidentitäten
  - Privatsphäre, Vertrauen

Marktpotential

- *„Alle Analysten, vor allem aber IDC, sagen uns, dass dieser Markt abheben wird. IDC verspricht bis 2007 ein Marktvolumen von vier Milliarden Dollar“*
  [Frank Issing , Sun Microsystems]

- *„Federated Identity Management is economically inevitable“*
  [Burton Group, Market Analyst]

Schwierigkeit

- Komplexität:

„Identity and access management initiatives tend to be more complex than the majority of IT projects...“

„...Because of the Diversity of identity stores and protocols, encryption mechanisms, policies need to work together“ [Microsoft]

Fazit

- IM heute:
  - Entwicklung läuft auf Hochtouren
  - Einführung/Umsetzung erst am anlaufen
- IM morgen:
  - (Federated) IM hat Zukunft
  - IM nicht nur für Personen sondern auch für Smarte Objekte

Quellen

- www.microsoft.com/technet/security/topics/identitymanagement/idmanage/default.mspx
- www.oracle.com/technology/products/id_mgmt/
- www.projectliberty.org/
- Malcolm Crompton
  „Proof of ID Required? Getting Identity Management Right.“