

Identity und Access Management in der Praxis

Meet Swiss Infosec!, 28.01.2010



An der Verkaufsfront nichts Neues

«Mit **SAP** ERP können Sie also nicht nur die Auftragsabwicklung beschleunigen und den Kundenservice verbessern, sondern auch **Umsätze** und Gewinnmargen **erhöhen**, Ihre **Produktivität steigern** und die Gesamtbetriebskosten senken.»

«Durch Konsolidierung und einen Wechsel auf die **Microsoft**-Plattform **senken** Sie Ihre laufenden **IT-Kosten signifikant**. Ziehen Sie aus bereits erworbener Microsoft-Software den **grösstmöglichen Nutzen** für Ihr Unternehmen.»

Mit **Oracle** SCM können Unternehmen die Marktanforderungen prognostizieren, **innovativ auf wechselnde Marktbedingungen** reagieren und ihren operativen Betrieb auf globale Netzwerke abstimmen.

Die **Novell** Compliance Management-Plattform **meldet Probleme nicht nur, sondern behebt sie** auch.

IAM in der Praxis

Etwas Theorie

- ▼ Einführung in die Thematik, wichtigste Definitionen und Begriffe
- ▼ Treiber von IAM

Praxis: Lösungs-Szenarien, Beispiele

- ▼ Im Demosystem eingesetzte Softwarepakete
- ▼ Demo 1: Provisionierung, Synchronisation
- ▼ Demo 2: Approval Workflow, Self Service
- ▼ Demo 3: Strong Authentication

IAM-Projektvorgehen, Kosten- / Nutzenbetrachtung

Anhang

- ▼ Kontakte RECON und Kooperationspartner
- ▼ IAM-Anbieter, -Standards und -Glossar

IAM-Begriffsvielfalt



IAM-Begriffe, Quelle: Siemens

- ▼ Die Begriffsvielfalt ist wie oft bei IT-Themen sehr gross
 - ▼ Es ist nicht einfach einen Überblick zu erhalten
- ➡ siehe auch IAM-Glossar am Ende der Präsentation

IAM-Begriffsdefinition

Das Identity-Management verwaltet die verschiedenen Identitäten, welche die Benutzer gegenüber den Applikationen aufweisen.

Regulatory

Das Access-Management verwaltet die verschiedenen Zugriffsrechte, welche die Benutzer für Applikationen bzw. für Teilapplikationen haben.

Identity

Identity & Access Management

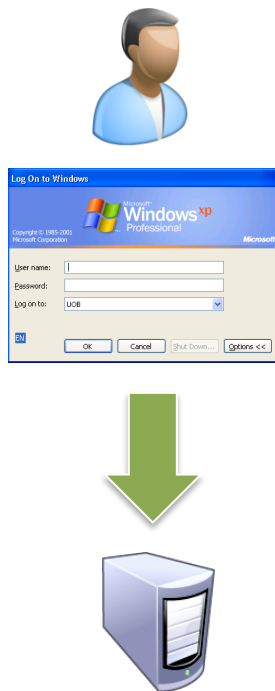
Access

Den richtigen Personen zum richtigen Zeitpunkt die Zugriffsrechte auf Ressourcen erteilen, die diese aufgrund ihrer Aufgaben oder Rollen im Geschäftsprozess benötigen

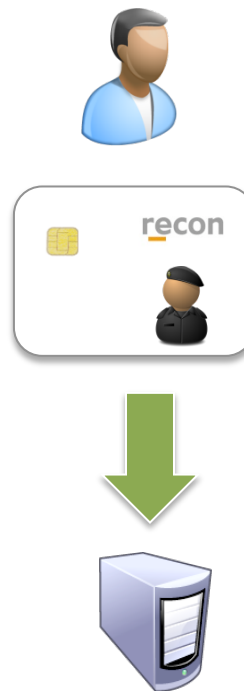
Authentisierungsarten

Das Nachweisen der eigenen Identität gegenüber System, Geräten und Applikationen wird wie folgt klassifiziert:

„was man weiss“



„was man hat“

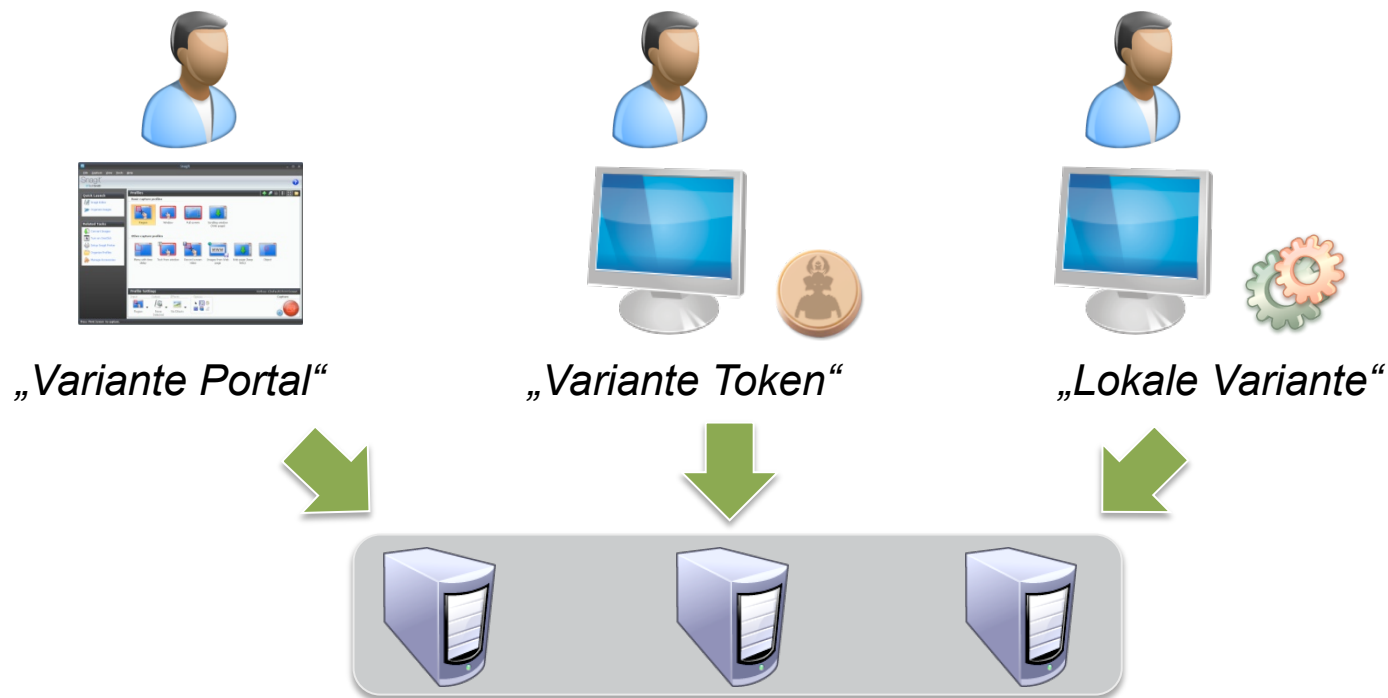


„was man ist“



Single Sign On (SSO)

Single Sign-On bedeutet, dass ein Benutzer nach einer einmaligen Authentifizierung auf alle Rechner und Dienste, für die er berechtigt ist, zugreifen kann, ohne sich jedes Mal neu anzumelden.



Strong Authentication

Digitale Zertifikate stellen die digitale Analogie zu amtlichen Ausweisdokumenten dar. Eine Zertifizierungsstelle bestätigt die Identität einer Person.

Ein digitales Zertifikat ist eine Datenstruktur, die den Namen und den öffentlichen Schlüssel eines Teilnehmers enthält und mit dem privaten Schlüssel einer Zertifizierungsstelle signiert wurde. Die Signatur stellt sicher, dass der öffentliche Schlüssel des Zertifikates zu einer bestimmten Person gehört.



Strong Authentication

Anwendung Digitale Zertifikate

Der Einsatz von digitalen Zertifikaten ermöglicht den Schutz der Vertraulichkeit, Authentizität und Integrität von Daten durch die Anwendung der öffentlichen Schlüssel.

- ▼ elektronische Signaturen (rechtsgültig)
- ▼ Sicherheit im Netzwerk
- ▼ Verschlüsselung von E-Mails und Dokumenten
- ▼ Abwicklung von E-Commerce Geschäften
- ▼ Beleg-Ablage und -Archivierung (MWSt-konform)

Akkreditierte Anbieter

- ▼ Swisscom
- ▼ Die Schweizerische Post
- ▼ Bundesamt für Informatik und Telekommunikation
- ▼ QuoVadis

Provisionierung & Synchronisation

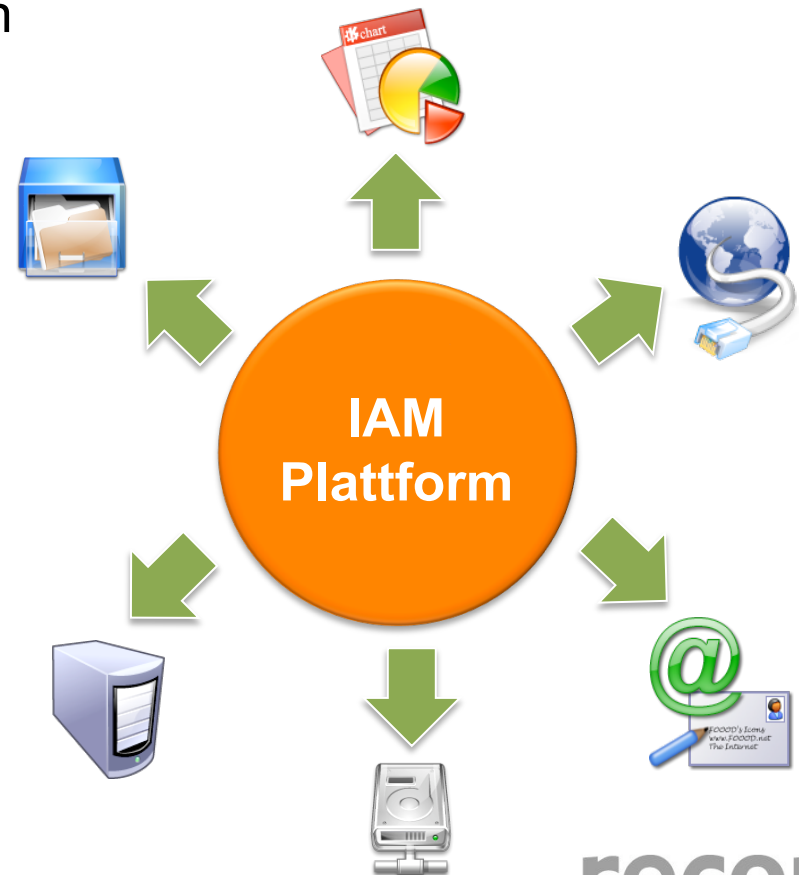
Provisionierung

Unter den Begriff Provisionierung fallen das Management, die Erteilung, Veränderung und Deaktivierung von Zugriffsrechten auf IT-Ressourcen eines Benutzers.

Unter Ressourcen fallen, z.B. Systeme und Daten, Hardware, Applikationen und Portale.

Synchronisation

Man unterscheidet den Begriff in der Art und Weise, dass in der Regel zunächst die Identitäten synchronisiert und anschliessend die Zugriffsrechte provisioniert werden.



Role Based Access Control

Rollen und IAM

- ▼ Identity Management regelt die Zuweisung von Benutzer-identitäten zu Rollen
- ▼ Unter Access Management fällt die Assoziation von Rollen auf Ressourcen



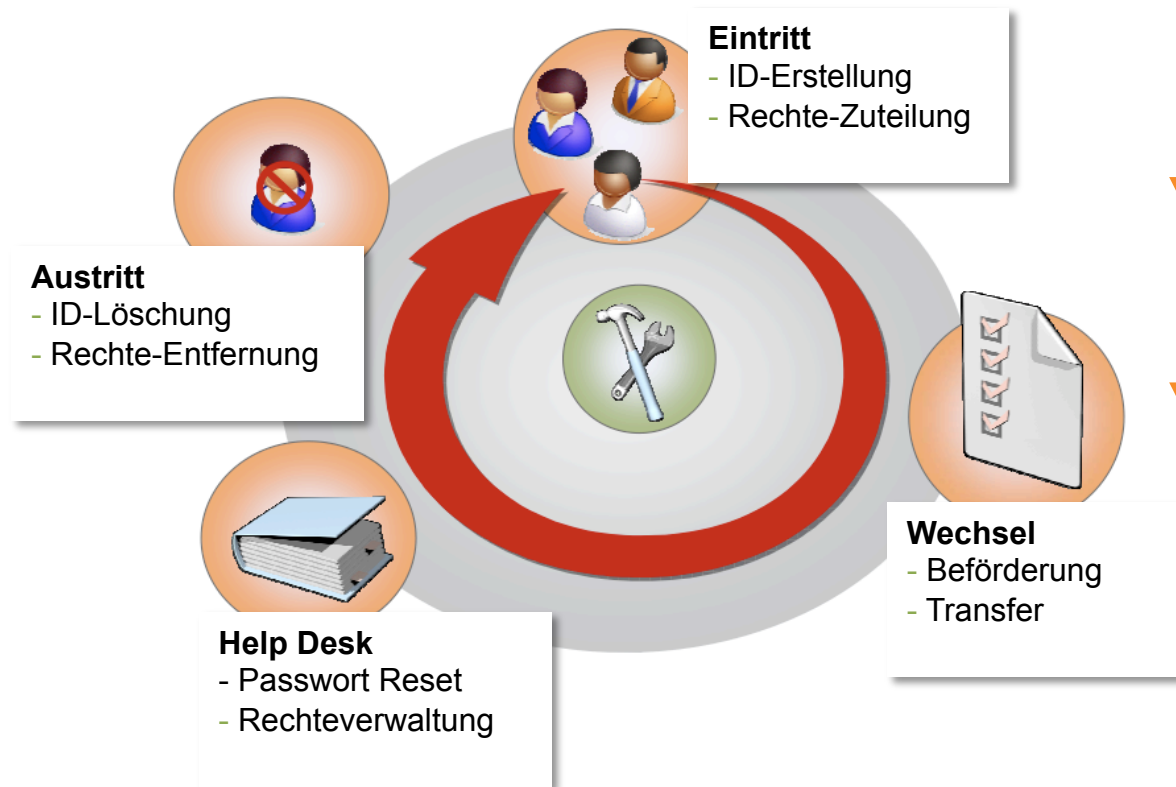
Leitgedanken

- ▼ Das Rollenkonzept soll die Rechte anhand von Arbeitsprozessen abstrahieren
- ▼ In einem IAM-System sollte es weniger Rollen als Benutzer geben
- ▼ Ein Benutzer kann mehrere Rollen umfassen
- ▼ Rollen können Rollen enthalten (Hierarchisches Rollenkonzept)

Workflow / Approvals

Identity Lifecycle

- ▼ Rechte-Zuteilung, -Änderung und Entzug benötigen Freigaben



- ▼ Das Recht Freigaben zu erteilen ist selbst wiederum ein Recht
- ▼ Approval-Workflows sind Standard-Workflows
- ▼ Die Komplexität nimmt zu, je länger der Lebenszyklus dauert

Self Service

Zielsetzung: Reduktion der Prozesskosten

Häufigste Support-Fälle im Helpdesk

- ▼ Beantragung und –Erteilung von Rechten
- ▼ Durchführung von Passwort-Resets

Meine Anträge (52) - 0 Erfasst, 0 VG Visierung, 0 SO Visierung, 50 Genehmigt, 0 In Arbeit, 2 Abgelehnt, 0 Fehler, 0 Unbekannt

Zeige 1 bis 10 von 52 << 1 2 3 4 5 6 >>

Art	Typ	Status	AuftragsNr	Recht	Betrifft	Erfasser	Erfassungsdatum	Visiert VG	Visiert Owner	Ausgeführt
🔍	🖥️	🟢 Genehmigt	252746	Unbekannt	Miehling Carsten	Lüscher Daniel		✔️	✔️	🟢
🔍	🖥️	🟢 Genehmigt	523708	G-M-DPSLV	Miehling Carsten	Miehling Carsten		✔️	✔️	🟢
🔍	🖥️	🟢 Genehmigt	432655	G-M-DPTABANKWS	Miehling Carsten	Miehling Carsten				
🔍	🖥️	🟢 Genehmigt	879360	G-M-DPSLVPLATT	Miehling Carsten	Miehling Carsten				
🔍	🖥️	🟢 Genehmigt	799161	G-M-DPBICDBPLU-READ	Miehling Carsten	Miehling Carsten				
🔍	🖥️	🔴 Abgelehnt	254831	Unbekannt	Miehling Carsten	Miehling Carsten				
🔍	🖥️	🟢 Genehmigt	797031	XML SPY (XP)	Miehling Carsten	Miehling Carsten				
🔍	🔑	🟢 Genehmigt	806713	SX Personaleingänge Mo-Fr 6-19Uhr	Miehling Carsten	Miehling Carsten				
🔍	🔑	🟢 Genehmigt	571689	HA Personaleingänge Mo-Fr 6-19Uhr	Miehling Carsten	Miehling Carsten				
🔍	🖥️	🟢 Genehmigt	806686	G-M-DPONBAPRU	Miehling Carsten	Miehling Carsten				

Beispiel: Rechteverwaltung (Sicht eines Anwenders) über Web-Portal

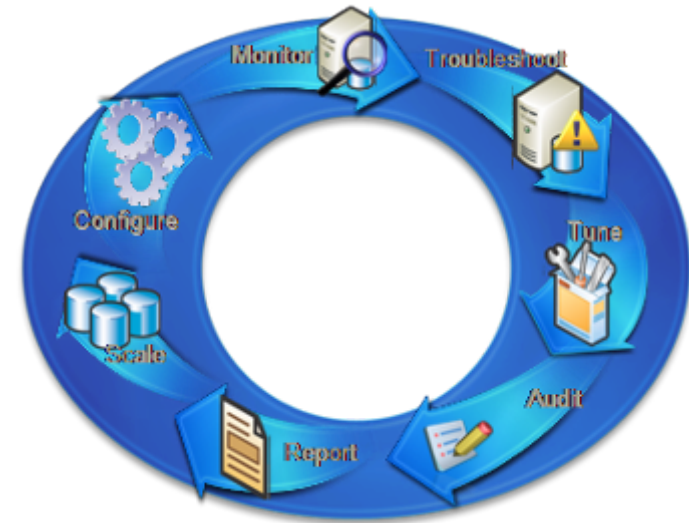


Beispiel: Passwort-Reset

Auditing & Reporting

Ziel 1: Beantwortung der W-Fragen

- ▼ Wer sind meine Benutzer?
- ▼ Welche Berechtigungen haben sie?
- ▼ Warum haben sie diese Berechtigungen?
- ▼ Wer hat sie erteilt, wieder entzogen, respektive genehmigt?
- ▼ Was machen die Benutzer mit den Berechtigungen?



Ziel 2: Nachweis erbringen, dass

- ▼ gesetzliche Vorschriften eingehalten werden
- ▼ die Vorschriftenkonformität sichergestellt ist
- ▼ Sicherheitsstandards eingehalten werden
- ▼ Auditierungs- und Sicherheits-Reports erstellt werden

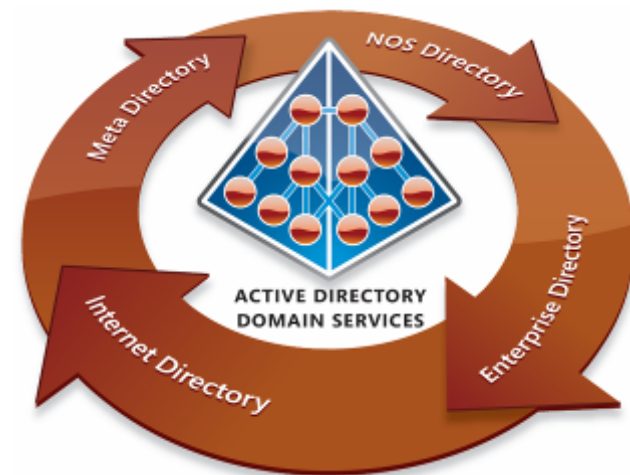
Directory Services

Allgemein

Ein Verzeichnisdienst stellt in einem Netzwerk eine zentrale Sammlung an Daten bestimmter Art zur Verfügung. Die in einer hierarchischen Datenbank gespeicherten Daten können verglichen, gesucht, erstellt, modifiziert und gelöscht werden.

Bekannte Verzeichnisdienste

- ▼ IBM Tivoli Directory
- ▼ Microsoft Active Directory
- ▼ Novell eDirectory (ehemals NDS)
- ▼ OpenLDAP
- ▼ Siemens DirX
- ▼ Sun Directory



IAM-Treiber Medien- und System-Vielfalt

Medien-Vielfalt

- ▼ Aufwändige Verwaltung Identitätsmedien (Hausschlüssel, Schrankschlüssel, Parkkarte, Tankkarte, Kreditkarte, Kantinenkarte, ...)
- ▼ Lückenlose und komplette Übersicht, was ein Mitarbeiter besitzt, ist nur mit hohem manuellem administrativen Aufwand zu erreichen

System-Vielfalt

- ▼ Der Betrieb und Unterhalt von heterogenen und vernetzten Systemlandschaften (Client- und Server-Hardware, Applikationen, Geräte, Kassen, ...) wird zusehendes komplexer und aufwändiger

IAM-Treiber Identitäts- und Zugriffs-Vielfalt

Identitäts-Vielfalt

- ▼ Benutzer mittlerer und grösserer Unternehmungen haben im Durchschnitt 7 – 10 verschiedene Identitäten mit dazugehörigen Logins
- ▼ Passwort Policies sind entsprechend vielfältig und unterschiedlich je Identität

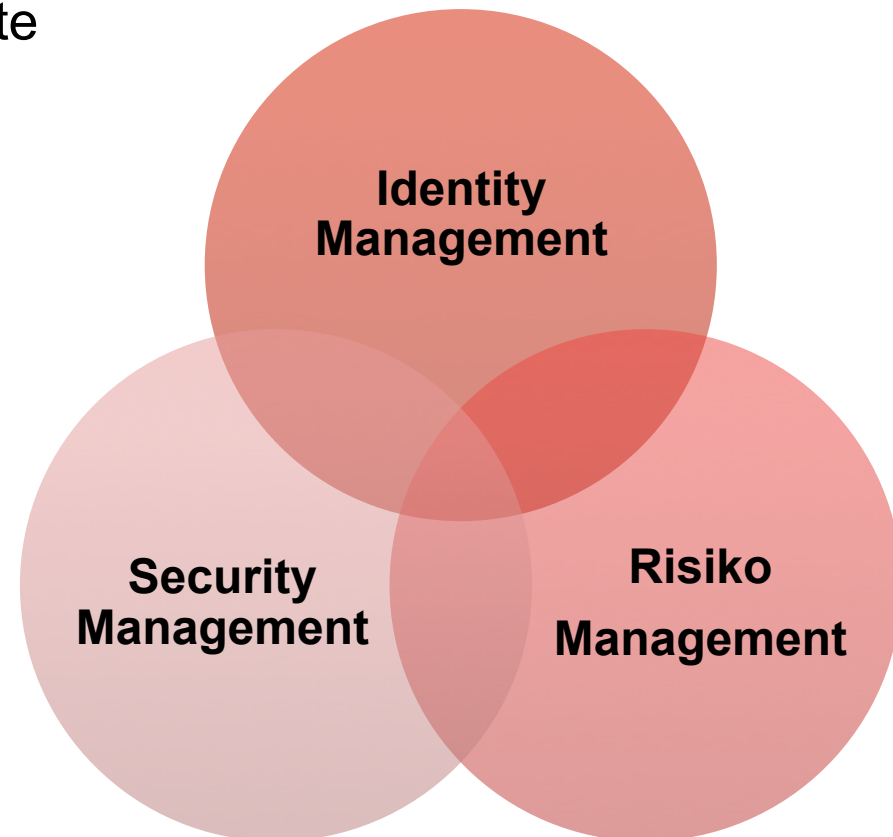
Zugriffs-Vielfalt

- ▼ Zugriffsarten werden zusehends vermischer (Intranet, Extranet, Internet)
- ▼ Trotz gleicher Identität sind physischer und logischer Zugriff heute getrennt behandelt (z.B. Zutritt versus System)

IAM-Treiber Fusion der Disziplinen

Identitäten beeinflussen Sicherheitssysteme

- ▼ Heute in der Regel getrennte Themenfelder
- ▼ Initiant der Vergabe und Änderung von Benutzerrechten ist oftmals die HR-Abteilung
- ▼ „innen = gut“, „aussen = böse“ stimmt nicht mehr
- ▼ Fehler verhindern ist ebenso im Fokus wie Angriffe verhindern



IAM in der Praxis

Etwas Theorie

- ▼ Einführung in die Thematik, wichtigste Definitionen und Begriffe
- ▼ Treiber von IAM

Praxis: Lösungs-Szenarien, Beispiele

- ▼ Im Demosystem eingesetzte Softwarepakete
- ▼ Demo 1: Provisionierung, Synchronisation
- ▼ Demo 2: Approval Workflow, Self Service
- ▼ Demo 3: Strong Authentication

IAM-Projektvorgehen, Kosten- / Nutzenbetrachtung

Anhang

- ▼ Kontakte RECON und Kooperationspartner
- ▼ IAM-Anbieter, -Standards und -Glossar

Softwarepakete Demosystem

IAM-System

- ▼ Windows Server 2008 64 Bit, SQL Server 2008 EE
- ▼ Microsoft Forefront Identity Server 2010

Email-System

- ▼ Microsoft Exchange Server 2010

Personalwesen

- ▼ ABACUS Personalwesen, Version 2009

Directory-System

- ▼ Windows Server 2008 32 Bit mit AD, CA und DNS aktiviert

Clients

- ▼ Windows Vista Business, FIM Passwordreset Add-On
- ▼ Office 2007 Outlook mit FIM Add-On

Demo 1: Provisionierung, Synchronisation

Anwenderfall

- ▼ Mitarbeiter-Eintritt Personalwesen-Applikation
- ▼ Automatische Anlage AD- und Email-Accounts
- ▼ Erfassung Initialpasswort mit Vorbereitung Passwort-Reset

Nutzen

Qualitativer Nutzen

- Keine Papierworkflows
- Keine Laufwege
- Personalwesen legt Grund-Accounts selbständig an
- Keiner Fehler aufgrund Mehrfacherfassung
- Sofortiger Systemzugriff für Benutzer (intern / extern)

Quantitativer Nutzen ¹

- Kostenreduktion Administratoren ca. 28 TCHF für Anlage AD und Email pro Jahr
- Aufwandreduktion Administratoren ca. 120 h für Anpassungen Email pro Jahr
- Aufwandreduktion Administratoren ca. 5 Minuten pro Anpassung

Demo 2: Approval Workflow, Self Service

Anwenderfall

- ▼ Anmeldung und Freigabe Gruppen-Verteilerliste
- ▼ Selbständiges Passwort-Reset

Nutzen

Qualitativer Nutzen

- Keine Papierworkflows
- Keine Laufwege
- Gruppenmitglieder verwalten Listen selbständig
- Anwender setzen Passworte selbständig zurück
- Änderungen sind um vielfaches schneller

Quantitativer Nutzen ²

- Kostenreduktion Administratoren ca. 288 TCHF für Passwortverwaltung pro Jahr
- Aufwandreduktion von 5 Min. pro Passwort-Reset (pro User und Applikation ca. ein Mal pro Jahr)
- Geschätzter Produktivitätsverlust ca. mehrere hundert Tage seitens Anwender pro Jahr

Demo 3: Strong Authentication

Anwenderfall

- ▼ Login mit SmartCard und PIN
- ▼ Automatisches Logout bei Entfernung der SmartCard

Nutzen

Qualitativer Nutzen

- Starke Authentisierung
- Verbesserte Sicherheit am Arbeitsplatz
- Einsatz der SmartCard als Multifunktionskarte (z.B. Zutritt, Catering, Secure Printing)
- Einsatz der SmartCard als Teil von PKI-Lösungen (z.B. Signierung, Encryption)

Quantitativer Nutzen ³

- Durchschnittliche Kosten pro Sicherheitsvorfall ca. 100 TCHF
- Kosteneinsparung für schnelleren und einfacheren Zugriff (logisch und physisch) ca. 350 TCHF pro Jahr
- Reduktion Personalaufwände nach Automation physischer und logischer Zugriff ca. 125 TCHF pro Jahr

IAM in der Praxis

Etwas Theorie

- ▼ Einführung in die Thematik, wichtigste Definitionen und Begriffe
- ▼ Treiber von IAM

Praxis: Lösungs-Szenarien, Beispiele

- ▼ Im Demosystem eingesetzte Softwarepakete
- ▼ Demo 1: Provisionierung, Synchronisation
- ▼ Demo 2: Approval Workflow, Self Service
- ▼ Demo 3: Strong Authentication

IAM-Projektvorgehen, Kosten- / Nutzenbetrachtung

Anhang

- ▼ Kontakte RECON und Kooperationspartner
- ▼ IAM-Anbieter, -Standards und -Glossar

Vorgehen bei IAM-Projekten

Erst laufen lernen, dann fliegen

Multifunktionskarte

- Grobkonzeption MFK / IAM
- Evaluation GU für logischen und physischen Zugriff
- Umsetzung MFK (Karte, Zutritt, allenfalls Catering)
- Grobkonzeption und Einführung Basis Rollenkonzept
- Umsetzung System-Login (Anbindung AD, HR, Zutritt, Exchange)

Passwortmanagement

- Umsetzung Passwortmanagement Applikationen mit Prio 1
- Umsetzung Selfservice-Workflows für Passwort-Reset
- Umsetzung spezifische Zusatzfunktionen (PKI, Verschlüsselung, etc.)
- Analyse und Detailkonzeption nächste IAM-Ausbaustufe

Federated Identity und Zusätze

- Anbindung externe Partner und Systeme
- Ausbau und Umsetzung Rollen- und Zugriffskonzept
- Ausbau Selfservice-Workflows (Anträge und Freigaben)
- Umsetzung spezifische Zusatzfunktionen (Audit & Reporting)

Kosten- / Nutzenbetrachtung

Punktueeller Einsatz (Anwenderfälle aus Demo)

- ▼ Die Automatisierung einfacher Workflows bringt bereits nachweislichen qualitativen und quantitativen Nutzen
- ▼ Die gezeigten Beispiele resultieren in einem ROI von weniger als zwei Jahren (bei gleichzeitig erhöhter Sicherheit)

Umsetzung einer umfassenden IAM-Strategie

- ▼ Vorgehensweise in Etappen (siehe vorangehende Folie) bedingt langfristige Investitionsrechnung und Finanzierung
- ▼ Je grösser die Anzahl Mitarbeiter und Systeme, je wichtiger ist die Konzeptionsphase und die Evaluation des richtigen IAM-Systems und –Anbieters
- ▼ IAM-Projekte eignen sich auch für KMUs (siehe Anwenderfälle aus Demo mit Investitionskosten kleiner 100 TCHF)

IAM in der Praxis

Etwas Theorie

- ▼ Einführung in die Thematik, wichtigste Definitionen und Begriffe
- ▼ Treiber von IAM

Praxis: Lösungs-Szenarien, Beispiele

- ▼ Im Demosystem eingesetzte Softwarepakete
- ▼ Demo 1: Provisionierung, Synchronisation
- ▼ Demo 2: Approval Workflow, Self Service
- ▼ Demo 3: Strong Authentication

IAM-Projektvorgehen, Kosten- / Nutzenbetrachtung

Anhang

- ▼ Kontakte RECON und Kooperationspartner
- ▼ IAM-Anbieter, -Standards und -Glossar

IAM-Experten RECON - Kontakte

IT-Strategie und -Beratung



Carsten Miehling

RECON IT Services GmbH
Gubelstrasse 5
CH-6301 Zug

Tel. +41 (0)41 720 45 70
Fax +41 (0)41 720 45 79
Mobile +41 (0)79 687 62 94
miehling@recon-is.ch
www.recon-is.ch

Identity und Access Management



Ronald Aregger

RECON IT Services GmbH
Gubelstrasse 5
CH-6301 Zug

Tel. +41 (0)41 720 45 70
Fax +41 (0)41 720 45 79
Mobile +41 (0)79 828 94 67
aregger@recon-is.ch
www.recon-is.ch

Kooperationspartner - Kontakte

Microsoft Forefront



Christian Jäggli

Microsoft Schweiz GmbH
Richtistrasse 3
CH-8304 Wallisellen

Tel. +41 848 224 488
cjaggli@microsoft.com
www.microsoft.com

Physische Sicherheit Multifunktionskarten



Christian Künzler

Securiton AG
Alpenstrasse 20
CH-3052 Zollikofen

Tel. +41 (0)31 910 17 53
christian.kuenzler@securiton.ch
www.securiton.ch

ABACUS Personalwesen



Joachim Vetter

ABACUS Research AG
Ziegeleistrasse 12
CH-9302 Kronbühl

Tel. +41 (0)71 292 25 25
joachim.vetter@abacus.ch
www.abacus.ch

IAM-Anbieter – Übersicht

- BMC Identity Access Management Suite www.bmc.com/identitymanagement
- CA Identity & Access Management Suite www.ca.com/us/identity-access-management.aspx
- Entrust Identity Management and PKI www.entrust.com/identity-management-pki
- IBM Identity Management www-01.ibm.com/software/tivoli/solutions/identity-mgmt
- Novell Solutions for Security & Identity www.novell.com/identityandsecurity
- Microsoft Identity Lifecycle Management www.microsoft.com/windowsserver2008/en/us/ida-home.aspx
- Oracle Identity Management www.oracle.com/technology/products/id_mgmt/index.html
- Siemens DirX-Identity www.siemens.de/enterprise/security
- Sun Microsystems Identity & Access Management www.sun.com/software/products/identity_mgr/index.xml

IAM-Standards

OASIS

Organization for the Advancement of Structured Information Standards. Internationale Non-Profit Organisation definiert Industrie-übergreifende und offene E-Business und Web-Service-Standards.

WS-Federation

Web-Service-Federation. Spezifikation für Identity Federation. Darin sind Mechanismen beschrieben, mit welchen unterschiedliche Sicherheitsdomänen Informationen über Identitäten und Authentisierungen austauschen können.

XACML

eXtensible Access Control Markup Language. Standardisiertes XML-Schema, welche die Darstellung und Verarbeitung von Autorisationsrichtlinien festlegt.

XCBF

eXtensible Common Biometric Format. Ermöglicht die normierte Übertragung von Daten mit biometrischen Identitäten (z.B. Retina Scans, Gesichtsgeometrie und Fingerabdrücke)

SAML

Standard Security Assertion Markup Language. Für den Austausch von Authentisierungs- und Autorisierungsdaten zwischen zwei Systemen.

DSML

Directory Service Markup Language. Beschreibt Informationen aus LDAP-basierten Verzeichnisdiensten im XML-Format. Erlaubt Abfragen und Mutationen mittels XML.

SPML

Service Provisioning Markup Language. Fokussiert Übertragung von Benutzer- und Ressourcen-Provisionierungsdaten. Die Provisionierung umfasst Automatisierung der Verwaltung von Benutzer- und System-Zugriffsberechtigungen.

UDDI

Universal Description, Discovery and Integration. Bezeichnet einen standardisierten Verzeichnisdienst. Wird häufig mit serviceorientierter Architektur (SOA) in Verbindung gebracht.



Bei der Produkte-Evaluation auf Standards achten

IAM-Glossar

Authentisierung (Authentication)

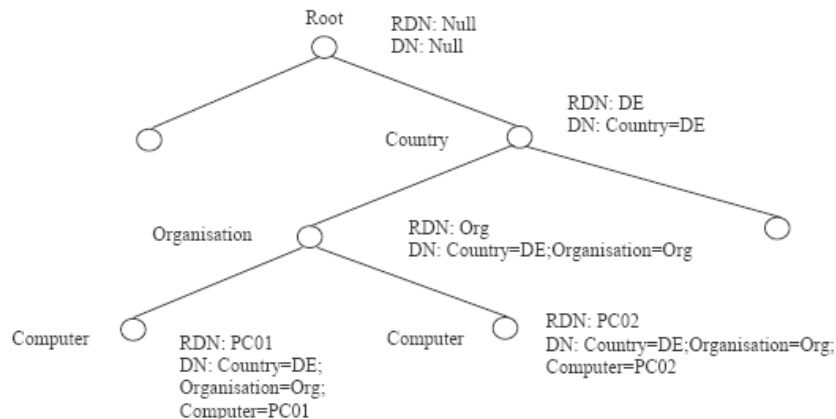
Nachweisen der eigenen Identität gegenüber einem IT-System

Autorisierung (Access Management)

Zugriffssteuerung auf Applikationen

Baumstruktur des Verzeichnis (Directory Information Tree DIT)

Aufbau des Verzeichnisdienstes nach X.500 Standard



Benutzer Provisionierung (User Provisioning)

Ursprung aus dem Militärjargon; meint das rechtzeitige bereitstellen der kriegsrelevanten Utensilien (Waffen, Munition, Proviant, Uniformen etc.). Es ist ein anderes Wort für User Management

Deprovisionierung (Deprovisioning)

Automatischer Entzug von Zugriffsrechten, aber auch Änderungen der Zugriffsrechte für Benutzer.

Distinguished Name (DN)

Pfad des Eintrages ab dem Root: z.B. Country = CH, Organisation = Axpo_Holding, Organisation Unit = CKW_AG.

Identität (Identity)

Benutzername und Passwort können für IT – Systeme Identitätsnachweise für Benutzer sein.

Identitäts-Verwaltung (Identity Management)

Verwalten der digitalen Identitäten der Benutzer in einem IT - System

IAM-Glossar

Konnektoren oder Agenten (Connectors or Agents)

Schnittstellen zwischen dem Meta Verzeichnis und dem User Managementsystem der Applikationen

Lightweight Directory Access Protokol (LDAP)

Protokoll, welches Zugriff auf ein X.500 Verzeichnis gewährt

Meta Verzeichnis (Meta Directory)

Einheitliche und zugängliche Informationsressource welche die isolierten Verzeichnisse einer Unternehmung verknüpft. Die Verzeichnisse werden dabei nicht ersetzt, sondern zusammengeführt

Passwortrichtlinien (Password Policies)

Anforderungen an Benutzerpasswörter: Komplexität, Gültigkeitsdauer, Verhalten nach fehlgeschlagenen Login-Versuchen, etc.

Provisionierung (Provisioning)

Automatische Zuweisungen von Zugriffsrechten zur Benutzung von IT-Systemen.

Relativ Distinguished Name (RDN)

Speziell ausgezeichnetes Attribut, welches den Namen jeden Eintrages gibt

Reverse Provisionierung

Ermöglicht den Status der Zugriffsrechte aktuell wie auch in der Vergangenheit zu ermitteln.

Rollen

Eine Sammlung von Benutzern und von Zugriffsrechten, abgeleitet von Benutzergruppen

Rollen basierte Zugriffskontrolle (Role based access Control RBAC)

Über Rollen definierte Zugriffskontrolle.

Single Sign On (SSO)

Einmaliges autorisieren gegenüber einem IT System, um zu den zugewiesenen Ressourcen zu gelangen.