



SCIENTIFIC CONSULTING PARTNERS

S-IDM - Identity-Management

“Durch ein konsequentes Identity-Management lassen sich Risikopotentiale deutlich reduzieren und gleichermaßen große Einsparpotentiale realisieren...”

Eckard Vossas
Mitglied des SCOPAR-Beratergremiums



WISSEN - SCHAFFT - NUTZEN

Inhalt

	Seite
Geschäftsprozesse und IdM: Einsatzszenarien	3
Identity-Management und Sicherheit	4
Ausgangssituation	5
Ziel	6
Identity-Management-Lösungen	7
Aspekte, Komponenten	8
Nutzen	9
Nutzen (Kosteneinsparungen)	10
Identity-Management als Basis für IT-Services	11
IdM-Architektur-Komponenten und Lösungsarten	12
Definition einer IdM-Lösung	13
Bausteine einer Identity-Management-Architektur	14
Erfolgsfaktoren	15
Stolpersteine	16
Vorgehen bei der Einführung	17
Prämissen und Ansprüche	18
Identity-Management (Begriffsbestimmung)	19
Digitale Identitäten	20

Geschäftsprozesse und IdM: Einsatzszenarien

- Person wechselt den Nachnamen mit Auswirkungen auf Accounts (z.B. E-Mail)
- Person ändert ihr Passwort (oder Rücksetzung nach Vergessen)
- Person kündigt oder wird entlassen (Erfordernis den Account zu löschen)
- bzw. verlässt das Unternehmen, aber es muss weiterhin auf versch. Accounts oder Accounts zugriffen werden
- Rücksetzung eines Passworts durch einen Administrator
- Sperrung / Aufhebung der Sperrung eines Accounts oder Zugriffsrechts
- Löschung oder Sperrung aller Accounts eines Nutzers
- Übertragung einer Auswahl von Accounts von einem System auf ein anderes
- Änderung einer Zugriffskontrollgruppe mit Auswirkungen auf eine größere Anzahl von Nutzern
- Eintritt einer Person in das Unternehmen und ihre Erfassung/Anlage im HR-System
- Sonderfälle: Freelancer, Praktikanten, Externe (Kunden, Partner)
- Person erhält Accounts, um auf Applikationen oder Systeme zugreifen zu können
- Person erhält Passwörter/Zertifikate, um die Accounts zu nutzen (Authentifikation)
- Person wechselt die Abteilung/Konzernteil mit massenhaften Account-Änderungen
- Person wechselt seine Funktion/Geschäftsaufgabe/ Rolle mit wenigen Account-Modifikationen

mögliche Auslöser für ein
administratives Eingreifen

➤ **Die Einsatzszenarien sind extrem vielfältig und bergen ein enormes Potential an administrativen Kosten, Fehlerquellen und Risiken, aber auch an Optimierungen.**

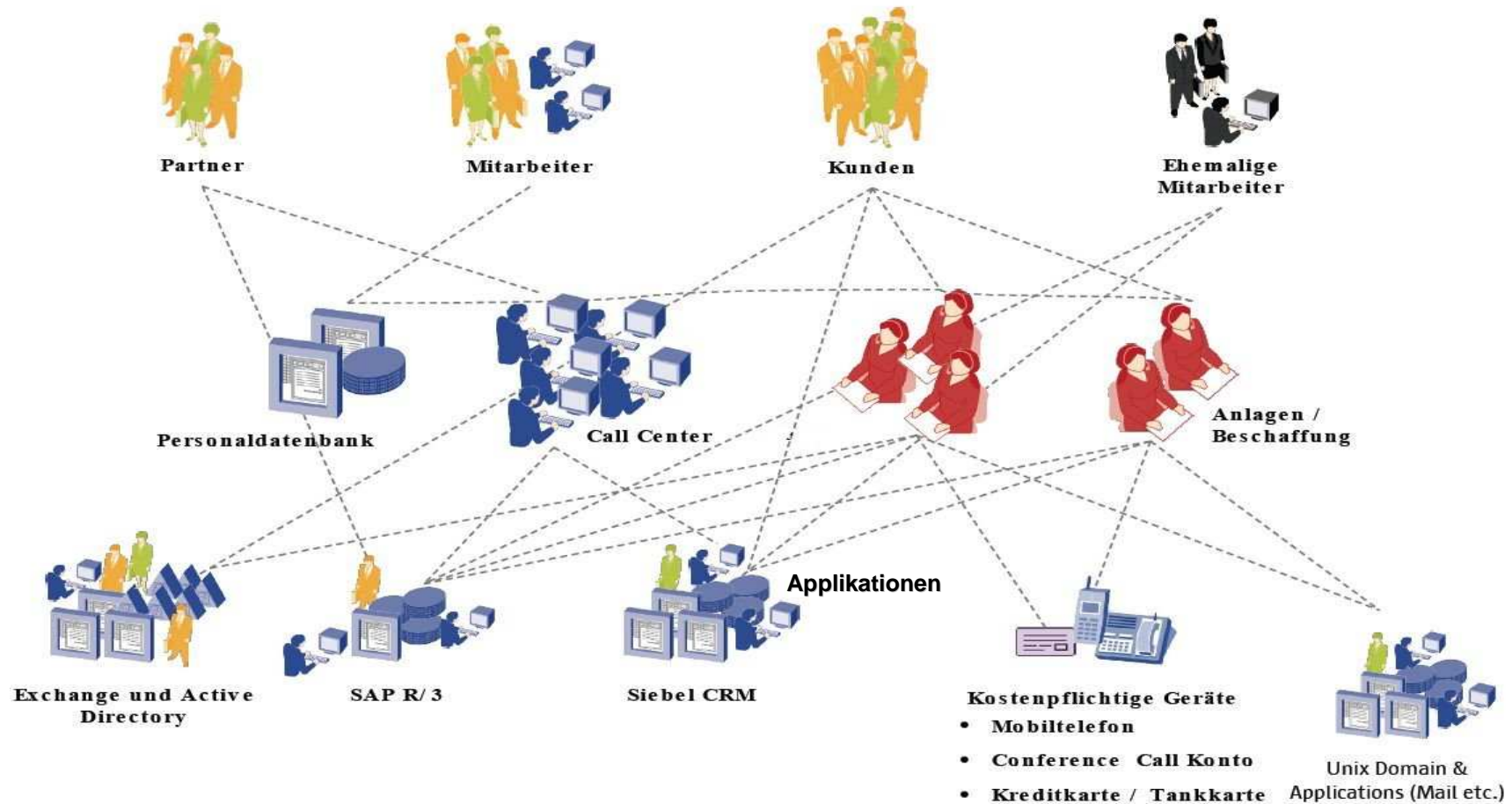
Identity-Management und Sicherheit

Ein auf automatisierten Workflows basierendes, konsolidiertes Identity-Management, dass unternehmensweite Policies verlässlich und effektiv durchsetzt, ist Voraussetzung für:

- Authentifizierung
- Autorisierung
- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Eingabekontrolle
- Weitergabekontrolle
- Protokollierung, Benachrichtigung, Alarmierung
(Auditing, Monitoring)

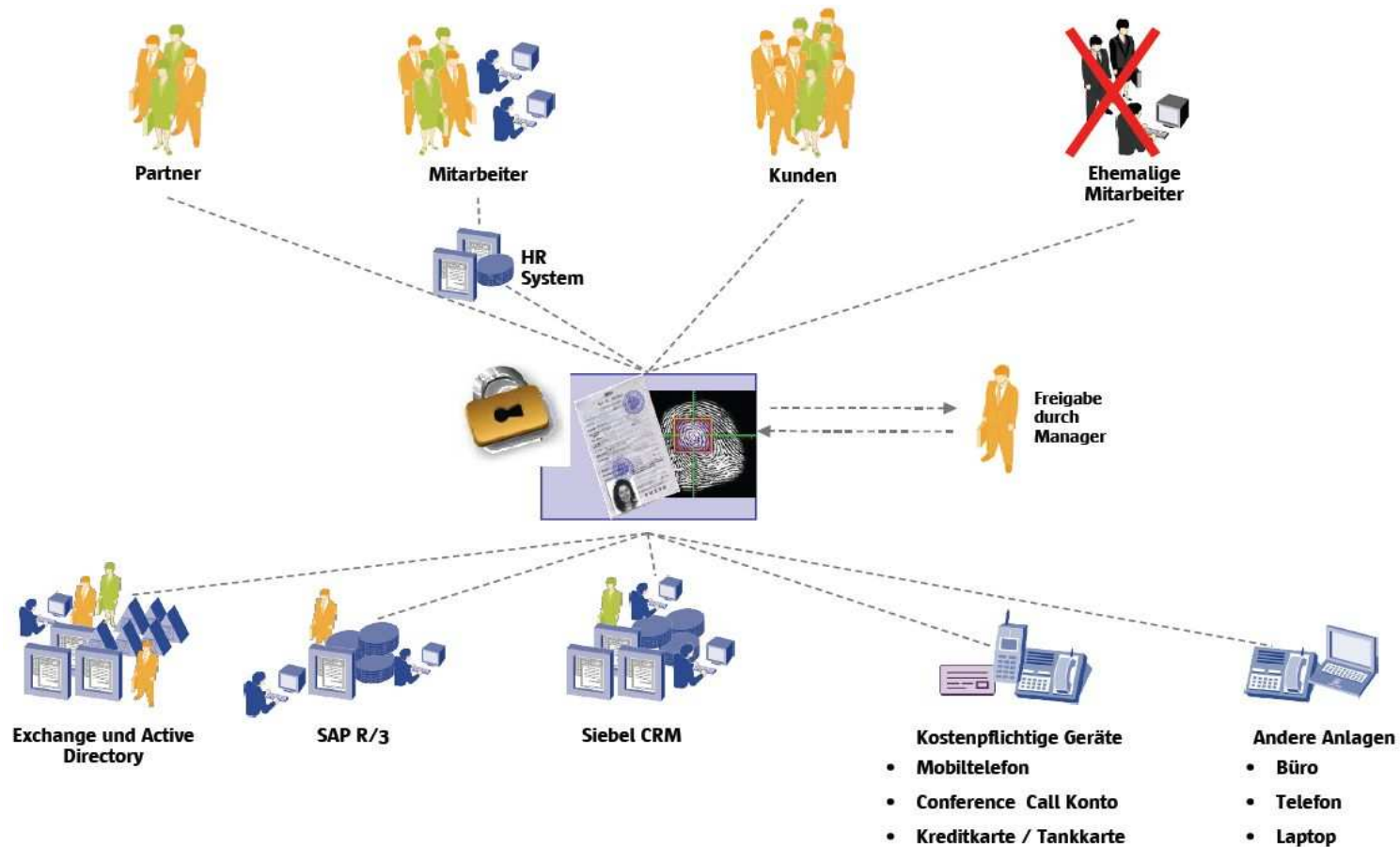
➤ **Sicherheit ist ein zunehmend kritischer Aspekt in Unternehmen, der auch im Sinn der Compliance „groß“ geschrieben werden muss.**

Ausgangssituation



➤ Das User-Management ist häufig unvollständig, unsicher, unsynchronisiert, erfolgt aufwendig und manuell, eine redundante Mehrfachdatenhaltung ist oft anzutreffen.

Ziel



➤ Das Identity-Management sollte einheitlich, effizient, automatisiert und sicher mit konsolidierten und aktuellen Identitätsdaten betrieben werden.

Identity-Management-Lösungen

- zielen darauf ab, eine einheitliche, systemübergreifende Plattform für die Verwaltung von Benutzern, deren Konten und deren Berechtigungen zu schaffen (unter Einbeziehung der relevanten Ressourcen)
- bestehen nicht aus einer einzigen Komponente, sondern betreffen verschiedene Aspekte (nicht nur technischer, sondern auch organisationspolitischer Natur; stehen in Zusammenhang mit Geschäftsprozessen, Geschäftszielen und Corporate Governance)
- Im Mittelpunkt vieler Projekte steht zunächst die Neugestaltung der Benutzer- und Berechtigungsverwaltung (das sog. “user provisioning”; Konsolidierung, Minimierung redundanter oder inkonsistenter Datenhaltung). Hier sind erfahrungsgemäß die größten Kosteneinsparungen zu erzielen

➤ **Identity-Management ist ein komplexer Prozess, der einen hohen Nutzen birgt.**

Aspekte, Komponenten

- Aufbau eines zentralen Repository für Benutzer und Berechtigungen (Directory Service)
- automatisierte Geschäftsprozesse für Provisionierung und Deprovisionierung
- Realisierung einer automatischen Datenkonsolidierung (Meta-Directory)
- Verbesserung der Authentifizierung für die Benutzer (z.B. Single Sign-On, zertifikat-basierte Smartcards)
- Konzeption einer unternehmensweit einheitlichen Infrastruktur für die Zugriffskontrolle (Access Management)
- Föderation (Federation)
- Optimierung des zentralen Help Desk (User Self Services z.B. für Passworte)
- Einführung einer einheitlichen Kontrolle über Benutzer und Berechtigungen (Auditing, Monitoring)

➤ **Identity-Management hat viele Facetten, die es zu berücksichtigen gilt.**

Nutzen

- **Kosteneinsparung:** Verringerung der Aufwände für Benutzerverwaltung und User Help Desk
- **Höhere Sicherheit:** bessere Kontrolle über die Benutzerkonten und Berechtigungen, Revisionsicherheit
- **Vereinfachung:** Einführung einheitlicher Administrationsprozesse und -anwendungen für die Benutzerverwaltung
- **Erzielen eines ROI:** Identity-Management-Lösungen führen *langfristig* zu nachweisbaren Kosteneinsparungen
- **Standardisierung:** einheitliche Haltung von Benutzerdaten erleichtert in zukünftigen Projekten die Integration neuer Anwendungen; Erfüllung von Compliance-Anforderungen
- **Voraussetzung** z.B. für SOA, PKI, Unternehmens-Portale

➤ **Identity-Management birgt eine Vielzahl von Nutzenaspekten, von denen das Unternehmen und die IT spürbar profitieren können.**

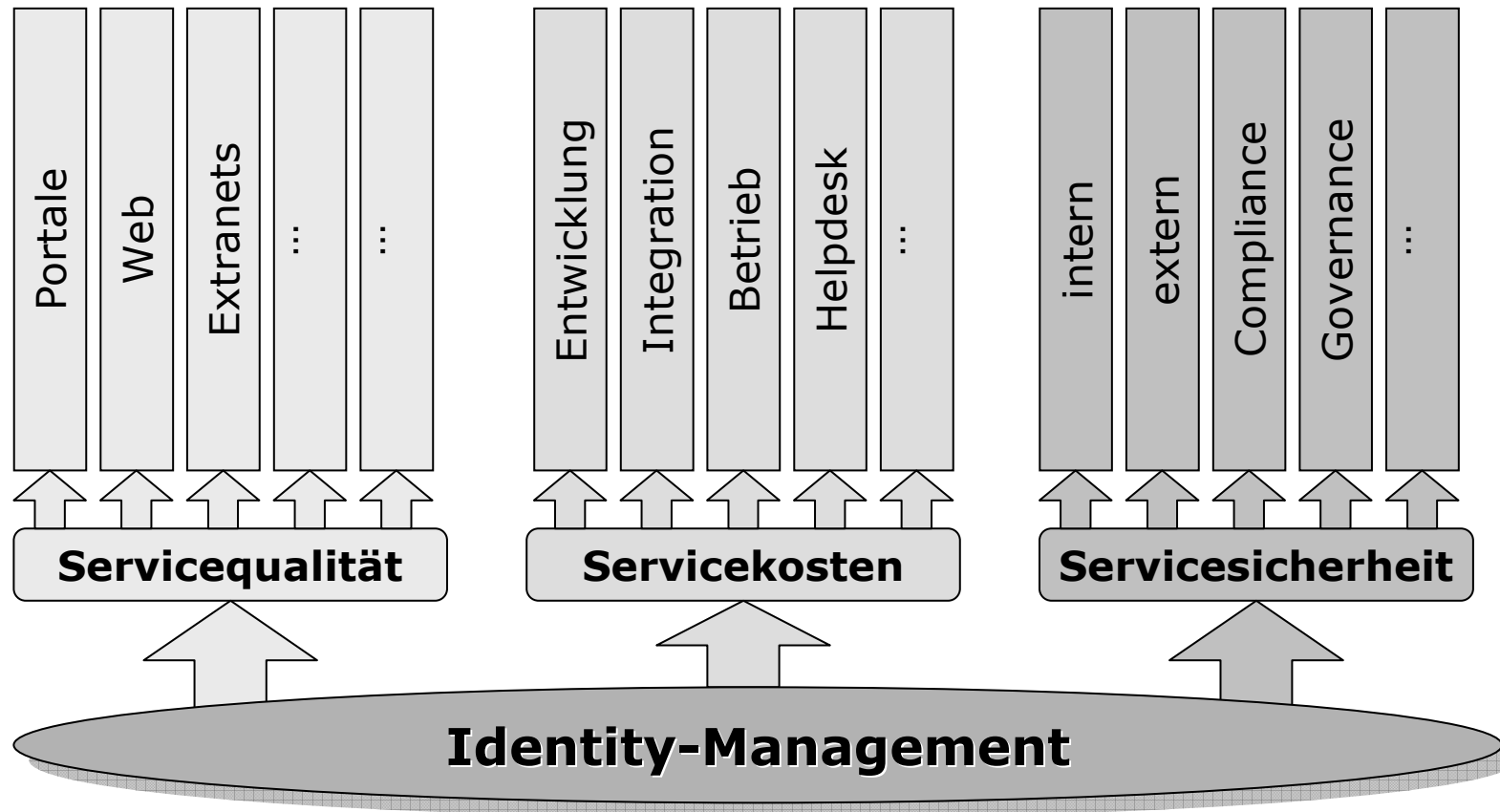
Nutzen (Kosteneinsparungen)

Eine Optimierung des Identity-Managements führt zu Kosteneinsparungen durch

- Verringerung des Aufwands für die Benutzerverwaltung
- Verringerung des Aufwands am Service-Desk
- Verringerung des Aufwands bei Neuentwicklungen
- Verringerung der Irrtümer, höhere Korrektheit der Daten
- Verringerung des Aufwands bei der Aufklärung von Sachverhalten
- einheitliche Policies und automatisierte Durchsetzung

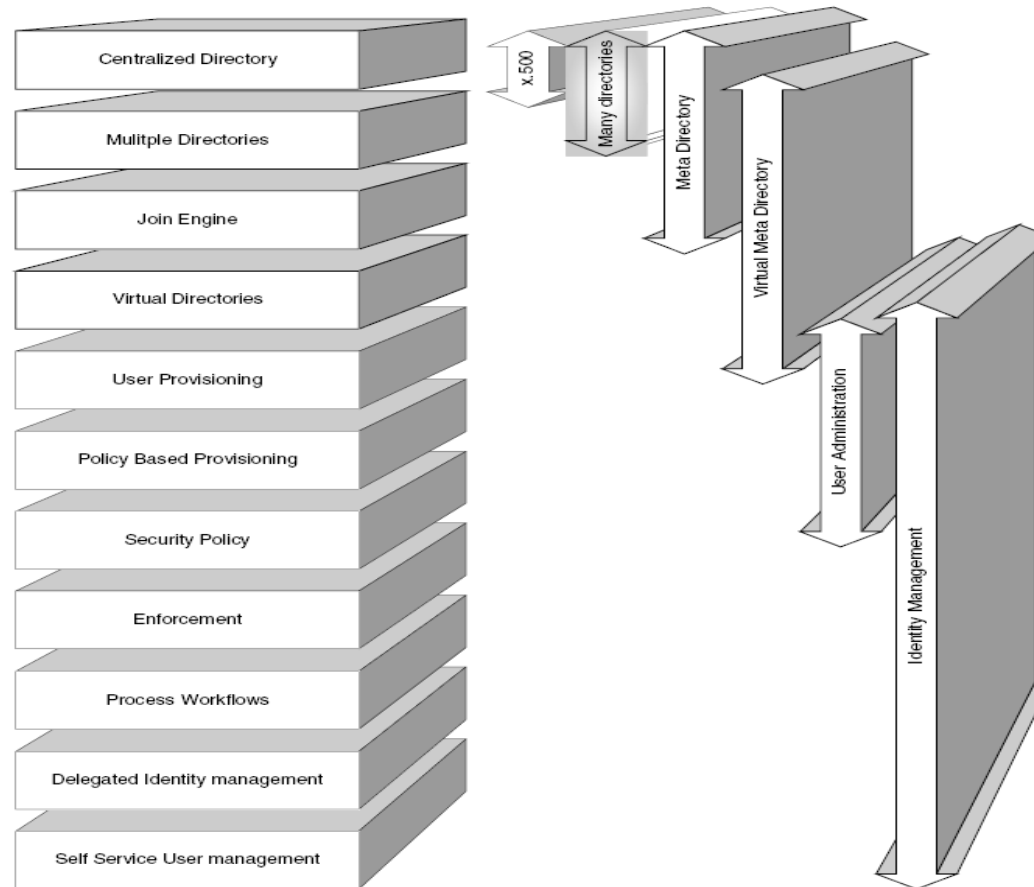
➤ **Es gibt noch andere Arten des Nutzens (neben Sicherheit, Kostenreduktion, Konsolidierung der Administration): neue Chancen für´s Geschäft.**

Identity-Management als Basis für IT-Services



- Identity-Management ist ein zentraler Bestandteil der IT.

IdM-Architektur-Komponenten und Lösungsarten



➤ Identity-Management ist ein vielschichtiger Prozess.

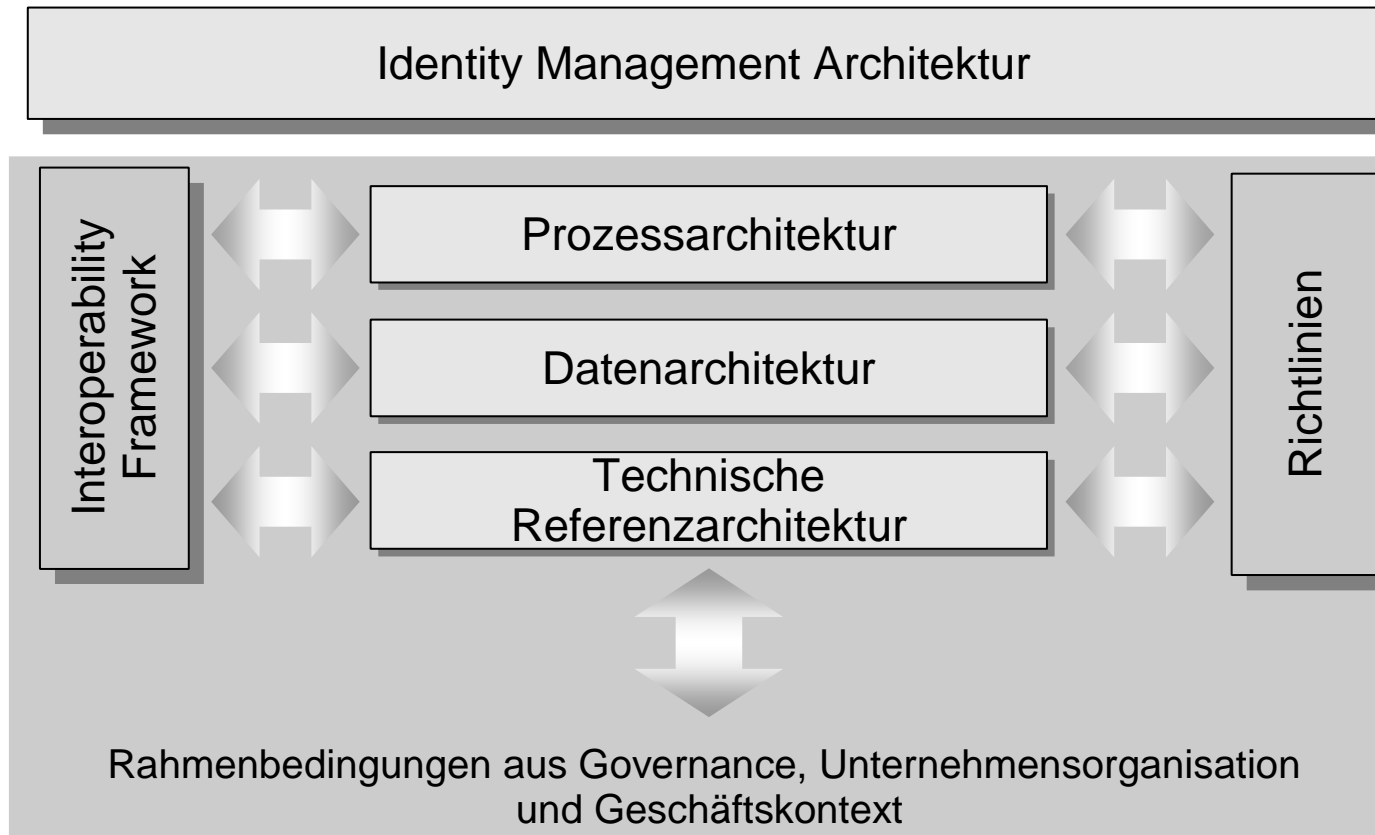
Definition einer IdM-Lösung

Relevante Bereiche des Identity-Managements, die bei der Schaffung von optimierten Lösungen betrachtet werden müssen:

- Nutzerverwaltung (Prozeduren)
- Password-Management (Prozeduren)
- Access Control Management (Prozeduren)
- Sicherheitsrichtlinien
- Zielsysteme
- Schnittstellen und Standards
- Auditing und Reporting (Prozeduren)
- technische Anforderungen

➤ **In der Definitionsphase wird das Projekt unter Berücksichtigung der aktuellen Umgebung, Aufgabenstellung und Anforderungen an die Lösung spezifiziert.**

Bausteine einer Identity-Management-Architektur



- **Erfolgreich ist, wer alle Bausteine des Identity-Managements kennt und beherrscht.**

Erfolgsfaktoren

- Das Unternehmensmanagement (inkl. der Geschäftsführung) ist sich der Notwendigkeit eines Identity-Managements bewusst, erkennt den Benefit (an), der für das Unternehmen daraus erwachsen wird, und hat seine Rollen und Verantwortlichkeiten akzeptiert
- Ressourcen für die Entwicklung der Architektur sind verbindlich zugesichert
- Das IT-Personal in der Organisation, unabhängig davon, wo es organisatorisch angesiedelt und wie es organisiert ist, versteht und akzeptiert das Erfordernis eines klar strukturierten und koordinierten Identity-Managements mit automatisierten Workflows
- ein Governance-Prozess zur Festlegung von Rollen und Verantwortlichkeiten, zur Erstellung von Richtlinien und zur Durchsetzung derselben wurde aufgesetzt und funktioniert
- alle Beteiligten (Player), das Management eingeschlossen, haben realistische (vereinbarte) Erwartungen hinsichtlich kurzfristiger Kosten und Benefits
- die Unternehmenskultur zeichnet sich aus durch Eigenschaften wie: vorausschauendes, zukunftsgerichtetes Agieren, Akzeptanz von Änderungen und den Willen, ein gewisses Maß an Risiken auf sich zu nehmen

➤ **Die SCOPAR-Experten haben umfassende Erfahrung im Bereich des Identity-Managements und wissen worauf es ankommt.**

Stolpersteine

- Misstrauen und Angst vor Veränderungen
- Furcht vor Verlust der Kontrolle (Macht)
- Unerfahrenheit oder Mangel an Fortbildung
- Zwang zur Überplanung oder perfektionistische Suche nach der "besten" Methode
- Ernste und chronische Ressourcen-Knappheit
- Arroganz seitens der IT-Abteilung – die "wir wissen es am besten"-Mentalität
- Unternehmenspolitik, - kultur und Player mit anderen Motiven
- Fixierung auf kurzfristigen ROI
- Akzeptanz des Status Quo (selbstgefälliges Zurücklehnen)
- Kürzliches sichtbares Scheitern in der IT-Planung
- IT-Abteilungen: mangelnde Ausrichtung ihrer Arbeit an den Geschäftserfordernissen ihrer Unternehmen
- Silodenken herrscht vor
- überlastete Helpdesk-Mitarbeiter und IT-Spezialisten können über aktuelle Problemfälle hinaus nicht handeln und planen

- **Die SCOPAR-Experten kennen die Stolpersteine bei der Durchführung von Projekten im Umfeld des Identity-Managements.**
- **Orientierung an praxiserprobten Abläufen (Best Practices) bewirkt eine engere Verschränkung von IT-Alltag und Geschäftszielen.**

Vorgehen bei der Einführung

- Richtlinien (bestehende analysieren, neue schaffen)
- Nutzer- und Berechtigungskonzept (meistens regel- und rollenbasiert)
- Analyse der bestehenden Repositories mit Daten über digitale Identitäten (ADS, Datenbanken, SAP HR, SAP ZBV, ...)
- Bestandsaufnahme der Objekte/Ressourcen (Intranet, Dokumente, File-Services, Zugangs-Credentials, ...)
- Analyse und Konzeption der zugehörigen Geschäftsprozesse, Implementierung entsprechender, weitgehend automatisierter Workflows
- Bestehende Nutzer, Gruppen, Berechtigungen, Accounts (UNIX, Windows, Firewall, VPN ...)

➤ **Ein zielorientiertes und strukturiertes Vorgehen ist Voraussetzung für ein erfolgreiches und nachhaltiges Identity-Management.**

Prämissen und Ansprüche

Prämissen für Projekte

- An erster Stelle steht die Konzeption und Planung
- Erst wenn die optimale Lösung für die Anforderungen gefunden ist, werden die „realen“ Produkte zu deren Erfüllung gewählt
- und nicht umgekehrt: die Anforderungen sollen nicht von den Leistungsmerkmalen der Produkte abgeleitet werden

Anspruch an Projekte

- Sie erfordern die Zusammenarbeit verschiedener Fachabteilungen und der IT-Abteilung
- Sie betreffen die Geschäftsprozesse des Unternehmens und verändern diese gegebenenfalls
- Sie werfen einen kritischen Blick auf die Informationssysteme und Datenspeicher des Unternehmens – mit dem Ziel, diese nach fachlichen Anforderungen zu integrieren
- Sie erfordern ein Projektteam, das viele verschiedene fachliche und technische Themengebiete abdecken muss
- Sie erfordern Management-Attention

➤ **Identity-Management ist nicht nur eine technische, sondern vor allem auch eine organisatorische Anstrengung.**

Identity Management (Begriffsbestimmung)

IdM umfasst den automatisierten, policy-gesteuerten Umgang mit den elektronischen Daten, die zu einer Entität gehören, z.B.

- zum Zweck der E-Mail-Adressierung, der Authentifikation oder der Autorisierung
- aber auch zur Ausstattung mit Arbeitsmitteln, zur Bearbeitung von Support-Anfragen o.ä.

IdM bezeichnet den kompletten Verarbeitungsprozess dieser Identitäts-informationen – von der Erhebung, Erfassung und Speicherung über die Verarbeitung und Nutzung bis zur Vernichtung – unter Berücksichtigung von Geschäftsstrukturen und –aufgaben

- Management der Repositories zum Speichern dieser Daten
- Strukturierung der Daten
- Geschäftsprozesse, Unternehmenskontext, Policies

➤ **Digitale Identitäten sind die Ausgangsbasis für IdM**

Digitale Identitäten

digitale Identität: Sammlung von digital gespeicherten Daten über ein *Subjekt* (charakteristische Merkmale, Präferenzen, Attribute)

Subjekt/Entität: Person, Organisationstruktur, Firma (Kunde, Lieferant, Partner), Applikation, Maschine oder anderes, *Zugriff auf eine Ressource anfordernd*

Ressourcen: z.B. Web-Seiten, Daten in einer Datenbank, Account auf einem Rechner, Services, Applikationen, E-Mail, Transaktion über eine Kreditkarte, Zugang zu einem Gebäude ...

Noch Fragen?



SCIENTIFIC CONSULTING PARTNERS

SCOPAR - Scientific Consulting Partners
Maximilianstraße 35a
D - 80539 München

Fon: +49 - 89 - 958 98 065
Fax: +49 - 89 - 958 98 066
E-Mail: info@scopar.de

WISSEN - SCHAFFT - NUTZEN