



Identity-Management - Quo Vadis?

Ein Statement von Eckard Vossas

Zur Strukturierung der Thematik wird im Folgenden die Betrachtung des umfangreichen Gebiets des Identity Managements (IdM) nach folgenden Perspektiven und Kriterien differenziert:

- ✓ Enterprise IdM (IdM innerhalb eines Unternehmens oder Firmenverbunds oder in bilateralen Beziehungen zwischen Unternehmen)
- ✓ IdM im Internet (HTTP-/Web-basierte Anwendungen)
- ✓ Spezialthemen: z.B. IdM für Mobilfunk-Unternehmen (mobile Dienste), neue Medien, staatliche Vorgaben (Gesundheitskarte, Personalausweis)

Natürlich haben diese Bereiche durchaus etwas gemein; es gibt aber auch profunde Unterschiede, die sich bereits in der Analyse über den Grad der Reife bemerkbar machen.

Zur näheren Charakterisierung sollte man die folgenden Fragestellungen zugrunde legen:

- ✓ Status: Wie ist der Stand der Dinge? Wo steht Identity Management aktuell?
- ✓ Ausblick: Wohin bewegt sich Identity Management (Trends, Prognose)? Wohin sollte es sich bewegen (Forderungen)? Welche "Treiber" gibt es?
- ✓ Welches sind die größten Hindernisse und Enttäuschungen in IdM-Projekten?

Identity-Management der Zukunft

- ✓ Die Einführung von Identity Management in Unternehmen wird preiswerter, weniger aufwendig und komplex werden; die Technik bzw. Tools und Produkte zum Identity Management müssen sich dem Reifegrad der Konzepte annähern
- ✓ Customer Identity Management im Internet mit zentralisierter Authentifikation und reduzierter Autorisation sowie Federation-Prozeduren wird Standard
- ✓ Im Enterprise Identity Management wird Autorisation absehbar eine dezentrale Angelegenheit bleiben, komplexe technische Rollen werden weiterhin in Endsystemen verwaltet, Federation wird nur eine geringe Rolle spielen
- ✓ Der Stellenwert von Identity Management in Unternehmen wird (ebenso wie Security-Themen und Datenschutz) eine bessere Awareness und Verankerung im Management sowie in der IT-Governance erhalten

Manche Thesen gehören in mehr als eine Kategorie: gegenwärtige Hindernisse sind zugleich Anforderungen an zukünftige Entwicklungen.

Beurteilung des gegenwärtigen Status des Identity Managements:

Beurteilung hinsichtlich Enterprise IdM:

- ✓ nach Phase der Euphorie im Tal der Ernüchterung
- ✓ auf dem Weg zur Konsolidierung und Standardisierung
- ✓ innerhalb der nächsten fünf Jahre brauchbare Reife bei Abstrichen in den Anforderungen
- ✓ ausgereifte Konzepte und Theorie, aber deutliche Kluft zu adäquater bzw. befriedigender Technik
- ✓ Federation in den Kinderschuhen (mehr offene Fragen als Antworten)

Beurteilung bezogen auf Unternehmen:

- ✓ die Notwendigkeit eines zumindest pragmatisch ausgereiften IdM ist unbestritten, aber es existiert nach wie vor ein enormer Nachholbedarf zur Optimierung des real existierenden IdM
- ✓ viele Projekte sind "überambitioniert"

Beurteilung hinsichtlich Internet IdM (Customer IdM):

- ✓ aufgrund anderer Aufgabenstellung und Anforderungen bereits deutlich ausgereifter als IdM innerhalb von Unternehmen
- ✓ hinsichtlich Authentifikation und reduzierter Autorisation (darf ein Nutzer auf die Web-Applikation zugreifen, was darf er sehen, keine komplexen Rollenkonzepte) bereits gang und gäbe, d.h. Standard
- ✓ Einsatz nutzerbezogener Federation auf dem Weg zum Standard und weit fortgeschritten

Beurteilung hinsichtlich Spezialthemen:

- ✓ hier steht man am Anfang
- ✓ noch nicht einmal ausgereifte Konzepte (geschweige denn Produkte)

Wohin bewegt sich das Identity Management (Trends, Prognose) bzw. wohin sollte es sich bewegen (Forderungen, was fehlt) sowie Meinung zu "Treibern":

- ✓ Konsolidierung von Identitätsdaten, zentralisierte Authentifikation, Unterstützung eines sicheren SSO (mit Mehr-Faktor-Authentifikation)
- ✓ Autorisation wird absehbar eine dezentrale Angelegenheit bleiben, komplexe technische Rollen werden weiterhin in Endsystemen/Ressourcen verwaltet werden
- ✓ Produkte, Tools und Implementierung müssen deutlich preiswerter werden
- ✓ die Einführung von IdM-Systemen muss weniger aufwendig und komplex werden, die Technik muss -- um das geeignet unterstützen zu können -- dahingehend verbessert werden
- ✓ der Stellenwert von IdM in Unternehmen muss eine besserer Awareness innerhalb des Managements bzw. der IT-Governance erhalten
- ✓ die Fähigkeiten der Technik und Implementierung muss mit den Möglichkeiten der Konzepte und den Erwartungen der Anwender bzw. Entscheider Schritt halten
- ✓ Reduktion von Komplexität in beispielsweise Workflows oder Rollenkonzepte durch vermehrten nutzerzentrierten Ansatz und größere Abstraktion/Strukturierung
- ✓ user centric approach führt auch im Internet zu höherer Akzeptanz

Treiber:

- ✓ Compliance wird zwar zunehmend wichtiger, wird aber dennoch nur in bestimmten Branchen (Banken, Versicherungen, großen Beratungs- und Rechtsanwaltsunternehmen) eine bestimmende Rolle spielen; sonst nicht
- ✓ Konsolidierung disparater, verteilter, isolierter, historisch gewachsener Nutzerverwaltungen
- ✓ Enabler für brauchbare (automatisierte) Workflows und Prozesse
- ✓ Monitoring und Revision (Fragestellungen wie: Wer hat warum auf welche Ressourcen welche Zugriffe? Welche Zugriffe habe ich als Nutzer in welchem Umfang auf welche Ressourcen?)
- ✓ Security-Themen, SSO, User Self Service

Welches sind die größten Hindernisse/Enttäuschungen (z.B. bei der praktischen Umsetzung, Einführung):

- ✓ mangelnde Verankerung von IdM-Projekten in IT- und Unternehmens-Governance
- ✓ selbst wenn man vorher darlegt, dass IdM-Projekte sich nur zu 30% mit purer Technik, aber zu 70% mit Prozess- und Organisationsevoluton befassen, gibt es dennoch hinterher im Umfeld der Geschäftsprozesse und Organisationskompetenzen größte Widerstände (Widerstand von Applikations- oder Fachverantwortlichen; die Windows-Administratoren können sich nicht vorstellen, dass man Automatismen außerhalb Ihrer eingefahrenen Praktiken zulassen darf; die SAP-Verantwortlichen lassen niemanden in ihre "selbstgestrickten" Implementierungen blicken ...)
- ✓ die existierenden Produkte sind oft nicht in der Lage, in einfacher Art und Weise den Konzepten zu folgen; es gibt kein System und keine Lösung "Out-of-the-Box"

- ✓ Performance-Probleme, zu hohe Komplexität der Implementierungen, zu großer Aufwand bei der Einführung
- ✓ "überambitionierte" Projektziele im Verlauf: auf einmal werden hochkomplizierte Workflows konstruiert, die mit herkömmlichen Mitteln niemand konzipiert hätte bzw. die so vorher nie existiert haben; Unfähigkeit, Rollen zu abstrahieren; die Erwartung, dass Technik alles lösen kann; der Unwille, eingefahrene aber untaugliche Prozesse zu reformieren
- ✓ aus Sicht der Budget-Verantwortlichen: warum soll man eine hohe Investition ohne kurzfristigen ROI für ein IT-internes Werkzeug bewilligen, dass zwar die Sicherheit und interne Abläufe verbessert, aber nach Außen keine großartig "sichtbaren" Resultate zeigen?
- ✓ aus Sicht der IT: warum soll man eingestehen, dass man gewisse Dinge und Abläufe nicht im Griff hat?
- ✓ für Anwender und Manager sichtbar sind: SSO und User Self Service: das ist aber nur ein Bruchteil von IdM

SCOPAR-Experte:

Eckard Vossas
Mitglied des SCOPAR-
Beratergremiums

Beratungsschwerpunkte:

IT-Architekturen, IT-Strategien, Directory Services, Access & Identity Management, IT-Sicherheit, Kryptographie, IT-Integrationen, Mail- & Messaging-Systeme, Web-Systeme.

Kontakt:

SCOPAR - Scientific Consulting Partners
Maximilianstraße 35a, 80539 München
Fon: +49 - 89 - 958 98 065
Fax: +49 - 89 - 958 98 066
E-Mail: info@scopar.de
Web: www.SCOPAR.de