

Business-Layer für IdM- Systeme

Inhalt

1	ERWEITERTE ANFORDERUNGEN AN IDM-SYSTEME	2
2	ACCESS- MANAGEMENT IST TEIL DER KOMPETENZEN EINES MITARBEITERS	2
3	NUR MIT BUSINESS LAYER IST EIN IDM ZUKUNFTSFÄHIG	4
4	<i>BI-CUBE</i> [®] IN GEMISCHTER UMGEBUNG	5
5	DIFFERENZIERT ANFORDERUNGEN	6
5.1	Anforderungen von Konzernen an ein IdM-Produkt	6
5.2	Anforderungen eines KMU an das IdM-Produkt:	7
6	KMU ALS NEUE ANWENDERGRUPPE FÜR IDM LÖSUNGEN	7
7	IDM ALS MANAGED SERVICES	8
7.1	IdM-Outsourcing oder Managed Services	8

Business-Layer für IdM- Systeme

1 Erweiterte Anforderungen an IdM-Systeme

Die Anforderungen der Anwender an IdM-Lösungen haben sich innerhalb der letzten zwei Jahre deutlich in Richtung der Business-Prozesse verschoben. Getrieben wurde diese Entwicklung insbesondere von folgenden Faktoren:

1. Die erhöhten Anforderungen an die Nachvollziehbarkeit nicht nur der direkten Tätigkeiten in der Administration sondern auch entlang der Weisungslinien (Compliance)
2. Zunehmender Druck auf den gesicherten User Self Service
3. Weitgehende regelbasierte Automatisierung des Access-Managements
4. Die Einbeziehung diverser „nebengelagerter Prozesse“ mit einem Bezug zur fachlichen Tätigkeit und den dafür erforderlichen Kompetenzen

2 Access- Management ist Teil der Kompetenzen eines Mitarbeiters

Jeder Mitarbeiter braucht zur Erfüllung seiner Aufgaben bestimmte Kompetenzen im umfassendsten Sinne aller Rechte und Befugnisse. Dazu gehören natürlich die Berechtigungen auf den Fachapplikationen und deren Voraussetzungen. An die Tätigkeiten lassen sich weiterhin binden:

- Zutrittsrechte
- Ausstattung an persönlichen Geräten (Assets inkl. Mobile Device Management)
- Rechte zur Nutzung unternehmenseigener Einrichtungen (Parkplatz, Kantine, Fuhrpark,...)
- Prozess-Kompetenzen aus einer Führungsposition heraus
- Freigabeprozesse für Modelle und Rollen
- Weitere Bereiche, die analoge Prozesse nutzen (z.B. Abwesenheits- bzw. Urlaubsanträge)
- SSO (Single Sign-On)
- Interne Leistungsverrechnung
- Lizenzkontrolle
- Password-Self-Service

Alle diese (und weitere) Kompetenzen lassen sich in einem regelbasierten Rollen- und Prozessmodell verwalten und vor allem die damit verbundenen Änderungsereignisse (Eintritt- Austritt, Wechsel) weitgehend automatisieren.

In vielen Installationen von **bi-Cube[®] IPM** (Identity Management Lösung des iSM) haben die Anwender die weitgehenden Möglichkeiten der Prozessmodellierung genutzt, um Prozesse in das IdM zu integrieren, die ursächlich reine IT-Berechtigungen (Access-Management) sind. Dies hat rückwirkend zu einer funktionellen Weiterentwicklung von **bi-Cube[®]** geführt, die diesen Trend in der Architektur der Lösung berücksichtigte.

Business-Layer für IdM- Systeme

Im Ergebnis dessen bietet **bi-Cube**[®], seinem Namen entsprechend (*Business Intelligence Cube*), einen Business Layer, der auf das „klassische“ Provisioning aufsetzt und aus drei integrierten Komponenten besteht:

- Ein Fach-Rollenmodell, das eindeutig von den System-Rollen (Access-Controls) getrennt ist
- Eine Prozess Engine (Workflow-Technologie), die eng mit dem Fach-Rollenmodell verbunden ist und auch die OE-Kompetenzen (Führungspositionen, Administratoren, Ownerschaften usw.) integriert
- Ein Regelwerk, das alle Eigenschaften, Rollen, Positionen usw. in relativ freier Notation verbindet und die Prozesse steuert. In der Version 7 ist in der **bi-Cube**[®] Extended Version für diese Aufgabe sogar eine Prolog-Engine integriert.

Um die für IdM-Lösungen typisch aufwendige Implementierung deutlich zu verkürzen, wurden folgende Templates entwickelt:

- Rollen- Referenzmodell
- Generische Standard-Prozesse

Im Zusammenwirken mit einer Standard-Konfiguration bietet das iSM ein „20 Tages Projekt“ an, das im internationalen Wettbewerb gemessen am Aufwand und Ergebnis derzeit konkurrenzlos ist.

Es enthält z.B. folgende Standard-Prozesse:

- Mitarbeitereintritt
- Automatischer Mitarbeiter-Austritt zum Entzug der Berechtigungen
- User Sperren
- OE-Wechsel für Rollen und Systeme
- Antragsverfahren Rollen
- Antragsverfahren Systeme
- Wiederholungsfreigaben
- Rollenänderungsantrag
- Delegation

Business-Layer für IdM- Systeme

3 Nur mit Business Layer ist ein IdM zukunftsfähig

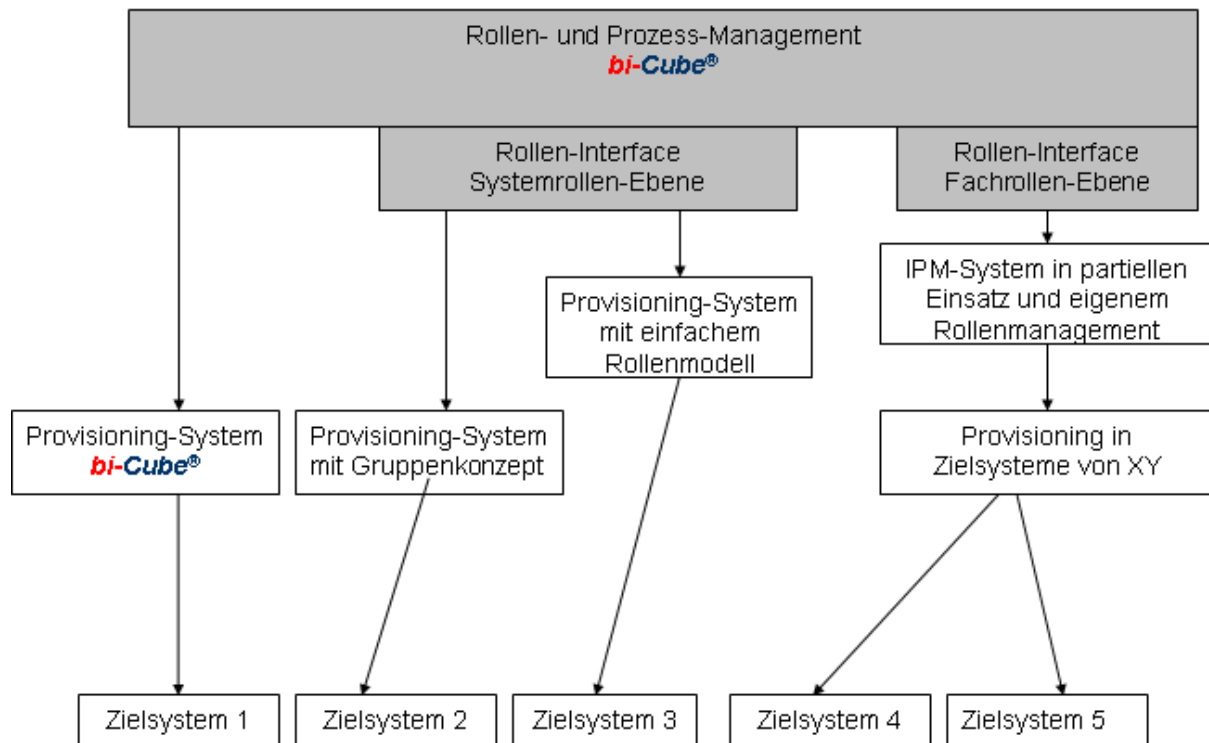
bi-Cube® IPM ist damit in der Lage, die IPM-Stufe 5 der allgemeinen Prozessreife für Identity & Prozess-Management = IPM zu realisieren.

IPM Stufe	Merkmale	Chancen	IPM-Ergebnis
5 Dissipativ Business-Layer	Integriertes Rollen- und Prozessmodell, Routineeinsatz von Standardprozessen, zunehmende Automatisierung, Trennung von Modellierung und Administration IKS - Selbstüberwachung	Kontinuierliche Evolution und automatische Adaption Frühwarnfunktion, Qualifizierung des Regelsystems	Hohe Produktivität, Motivation und Qualität
4 Gesteuert	Einsatz eines zentralen Provisioning-Tools Einfaches Gruppenkonzept auf der Basis des konventionellen Provisionings	Integrierte technologische Basis, Problemvermeidung, Integration weiterer Komponenten	
3 Standardisiert	Zentrale manuelle Organisation und Dokumentation, Einzelne Bereiche teilautomatisiert z.B. über das AD	Qualitative und strukturelle Darstellung der Prozesse, Problemerkennung	
2 Geordnet	Systematisierung aber unterschiedliche Entwicklungsstufen und isolierte Einzelprozesse	Prüfungen, Tests, Standards; Erkennen von Risiken und Potentialen	
1 Ad hoc Situation	Improvisation, Berechtigungen auf Zuruf, keine Dokumentation	Einführung operativer Tools, Controlling; Qualifizierung der Datenbasis für Reports	Hohes Risiko, Reibungsverluste

Business-Layer für IdM- Systeme

4 *bi-Cube*[®] in gemischter Umgebung

Diverse andere am Markt befindliche Produkte haben keine oder nur rudimentär ausgebildete Funktionalität im Bereich der Business Prozesse. *bi-Cube*[®] ist deshalb in der Lage, für Produkte wie e-Directory, Tivoli, DirX, SAM Jupiter oder Active Entry diese Business-Funktionalität „On Top“ bereit zu stellen.



Business-Layer für IdM- Systeme

5 Differenzierte Anforderungen

Die Ziele und Motivationen zum Einsatz eines IdM-Systems sind von der Größe und der Komplexität der IT-Welt eines Unternehmens abhängig.

Die bisherige Systemarchitektur und Funktion der am Markt verfügbaren IdM-Produkte ist auf die Bedürfnisse von großen Unternehmen ausgerichtet. Die Begründung ist darin zu sehen, da bei diesen Unternehmen der Druck aus Richtung Compliance, Security und Rationalisierung der IT-Administrationsprozesse seit Jahren ständig zugenommen hat. Diese Gründe waren bei KMU deutlich geringer ausgeprägt und wirkten erst mit zeitlicher Verzögerung. Außerdem haben KMU erweiterte Anforderungen an die Funktionalität.

	Große Unternehmen	KMU
Compliance / Nachvollziehbarkeit	Unbedingt erforderlich	Relativ unwichtig
Automatisierung der IT-Administration	Oft erforderlich	Relativ unwichtig
Funktionelle Breite	Enger aber unterschiedlicher Funktionsrahmen	Wichtiger Faktor
Nebengelagerte Prozesse	Nur IdM-Kernfunktionen erforderlich, da für die nebengelagerten Prozesse Spezialsysteme im Einsatz sind	Ergänzende Funktionen von hoher Bedeutung: Lizenzkontrolle, SSO, interne Kostenrechnung, Assets. Interface zur Zutrittskontrolle
HR-Interface	Autom Datenabgleich HR -> IdM	Nicht unbedingt erforderlich In einigen Fällen ist IdM das HR-System
Connectoren	Kernsysteme mit direkten Connectoren	Oft ist Aktion 7* ausreichend
Mandantenfähigkeit	In der Regel notwendig	Selten gefordert

* Aktion 7 = halbautomatischer Prozess

5.1 Anforderungen von Konzernen an ein IdM-Produkt

Große Unternehmen realisieren IdM-Projekte in mehreren Phasen. Zu Beginn konzentrieren sie sich in der Regel auf einen engen Funktionskanal, der durch die Zielvorgaben des Managements bestimmt ist (Compliance, SOX-Audits, Mergers, neue IT-Strategie wie SOA, SaaS usw.)

Business-Layer für IdM- Systeme

5.2 Anforderungen eines KMU an das IdM-Produkt:

- Es wird eine Suite benötigt, die nicht nur IdM „kann“, da beim KMU im Gegensatz zu Großunternehmen korrespondierende Spezialprogramme zumeist fehlen.
- Ein IdM sollte deshalb neben seiner Kernfunktion weiterhin folgende Funktionen bieten:
 - eine einfache Personalverwaltung
 - Rechteverwaltung und Rollenmodell
 - Standorte und Kostenstellen verwalten
 - ein integriertes SSO, Lizenzkontrolle und Kostenverrechnung der IT-Ressourcen
 - einen Authentifikations-Server
 - Eine einfache Software-Verteilung integriert haben (MSI über AD-Gruppen)
 - Ein AD-basiertes rollenintegriertes Ressourcenmanagement
 - Vordefinierte Reports
 - Integrierten Workflow-Manager mit vorkonfigurierten Prozessmodellen
 - Schnittstelle zur Zutrittssteuerung

6 KMU als neue Anwendergruppe für IdM Lösungen

Unter welchen Bedingungen sollte sich ein mittelständisches Unternehmen für eine IPM-Lösung interessieren sollte:

- Das Unternehmen hat ca. 300 User und eine IT-Landschaft mittlerer Komplexität
- Das Unternehmen hat eine hochkomplexe IT-Landschaft verschiedener Systemplattformen
- Im Unternehmen werden Daten verwaltet, die das ideelle Vermögen des Unternehmens ausmachen
- Das Unternehmen ist mit wesentlichen Teilen seiner Produktion als Zulieferer für Finalisten tätig, die Compliance-Anforderungen genügen müssen (z.B. SOX) und diese Anforderungen dann auch auf die Zulieferer ausdehnen.

Welche Anforderungen hat ein KMU an den Lieferanten:

- Es sollte ebenfalls ein KMU sein, um hinreichendes Problemverständnis des Lieferanten erwarten zu können.
- Es sollte seinen Sitz im Lande haben, um keine Sprach- oder Zeitzoneprobleme aufkommen zu lassen.
- Ein KMU als Lieferant ist kurzfristig in der Lage (und vor allem auch bereit), auf gewisse spezielle Anforderungen des Kunden einzugehen.
- Die Lösung sollte im Lande entwickelt worden sein, da ein IdM stark auf landestypische gesetzliche Vorgaben usw. ausgerichtet sein muss
- Das Produkt muss eine gewisse Reife haben, um hinreichende Stabilität erwarten zu können.
- Da ein KMU in der Regel keine IdM-Spezialisten vorhalten kann, ist möglichst ein Full Service bis hin zum Outsourcing anzubieten.
- Das IdM-Produkt sollte beim Lieferanten das strategische Produkt darstellen, um Investitionssicherheit zu haben.
- Am günstigste für den Kunden ist, wenn er direkt vom Hersteller beliefert und betreut wird.

Business-Layer für IdM- Systeme

7 IdM als Managed Services

IdM- Systeme überfordern vielfach die eigenen Skills und Kapazitäten mittelständischer Unternehmen. Obwohl deren IT - Infrastruktur vor denselben Herausforderungen steht wie die großer Konzerne, verfügen sie vielfach nicht über einen Stab qualifizierter IT – Administratoren und können bzw. wollen keine knappe personelle Ressourcen mit der erforderlichen umfassenden Fachkompetenz für eine IdM-Lösung binden. Andererseits besteht der Wunsch bzw. die Notwendigkeit, die funktionellen Möglichkeiten eines IdM oder Single Sign-On zu nutzen.

Genau auf diese spezifische Situation mittlerer Unternehmen geht das iSM mit einem passgenauen, modular aufgebauten Betreuungsangebot für die **bi-Cube**[®] KMU-Lösung ein.

Das Full-Service Konzept realisiert eine weitgehende Betreuung des Kunden im Design und Betrieb seiner IdM-Lösung, wobei diese in der Infrastruktur des Kunden installiert ist.

7.1 IdM-Outsourcing oder Managed Services

In logischer Konsequenz des Full-Service übernimmt ein Service-Provider auch den Betrieb des IdM-Systems. Bei diesem Service ergeben sich diverse technische, beriebsorganisatorische Probleme, die dann noch durch hohe Security Anforderungen ergänzt werden.

- Der Kunde kommuniziert mit dem IdM-System nur noch über das Web (Security)
- Die Services und Connectoren laufen aber beim Kunden, da sie den direkten Zugang zu den Zielsystemen des IdM haben müssen
- Die Modellierungen (Rollen, Prozesse usw.) erfolgen in separaten Antragsverfahren
- Vom Service-Provider muss ein sog. Gesichertes Betriebskonzept realisiert werden.
- Der Service-Provider muss sich zu IdM-spezifischen SLA verpflichten
- Der Service-Provider muss in der Regel ein transaktionsbezogenes Abrechnungsmodell anbieten

Im Bereich des Managed Service wurden insbesondere technische Ansätze wie SOA und SaaS auf ihre Verwendbarkeit und Einsatzreife betrachtet und konkrete Lösungen erarbeitet.