

# Business Layer for IdM Systems



## Contents

1	ADDITIONAL REQUIREMENTS FOR IDM SYSTEMS .....	2
2	ACCESS MANAGEMENT IS PART OF EMPLOYEES COMPETENCES .....	2
3	ONLY WITH A BUSINESS LAYER IDM IS FUTURE-PROOF .....	4
4	<i>BI-CUBE</i> <sup>®</sup> IN A MIXED ENVIRONMENT .....	5
5	DIFFERENTIATED REQUIREMENTS .....	6
5.1	IdM requirements of large enterprises / corporate groups .....	6
5.2	IdM requirements of small and medium-sized businesses: .....	7
6	SMB AS THE NEW USER GROUP OF IDM SOLUTIONS .....	7
7	IDM AS MANAGED SERVICES .....	8
7.1	Full service concept .....	8
7.2	IdM outsourcing or Managed services .....	8

# Business Layer for IdM Systems

## 1 Additional Requirements for IdM Systems

During the past two years, the requirements of users regarding IdM<sup>1</sup> solutions have clearly shifted towards the direction of business processes. This development has been geared by the following factors:

1. the raised demands for traceability of not only the direct tasks in the administration but also along the instruction lines (compliance factors)
2. an increasing pressure on secure user self service
3. largely rule-based automation of access management
4. the inclusion of various "lateral processes" with relation to the professional tasks and necessary competences

## 2 Access Management is Part of Employees Competences

In order to fulfill his duties, every employee needs certain competences in the most comprehensive sense of all rights and authorizations, including of course the authorization to use professional applications and their requirements. The following can be linked with the tasks:

- Access rights
- Provision of personal devices (Assets incl. Mobile Device-Management)
- Authorizations to use company facilities (parking, lunchroom, vehicles, ...)
- Process competences, deriving from a leading position (executive)
- Approval processes for models and roles
- Additional areas which use analog processes (e.g. absence or vacation requests)
- SSO
- Internal cost allocation
- License control
- Password self service

All the above (and more) competences can be managed in a rule based role and process model and modification events (such as employee entry, exit or change) widely automated. Within many **bi-Cube**<sup>®</sup> IPM (Identity Management of iSM) installations the broad possibility of process modeling is being used by the companies to integrate processes into the IdM, which are basically pure IT authorizations (Access Management). This has caused a retroactive functional enhancement of **bi-Cube**<sup>®</sup>, considering this trend in the architecture of the solution.

---

<sup>1</sup> IdM = Identity Management

## Business Layer for IdM Systems

As a result, **bi-Cube**<sup>®</sup> - according to its name (*business intelligence cube*) - provides a business layer based on the classical provisioning and being composed of three integrated components:

- A job role model which is clearly separated from system roles (access controls)
- A process engine (workflow technology), closely connected to the job role model which also integrates so called OU competences (leader positions, administrators, ownerships etc.)
- A set of rules which interlinks all properties, roles, positions etc. in relatively free notation and controls the processes. In the extended version of **bi-Cube**<sup>®</sup> V7 even a prolog engine is integrated for this purpose.

In order to significantly shorten the complex implementation so typical for IdM solutions, the following templates have been developed:

- Role reference model
- Generic standard processes (GPM = Generic process models)

Based on a standard configuration, iSM offers a 20 days implementation project ("IdM within 20 days") which is currently unrivaled in the international competition, as far as expenditure and results are concerned.

The project includes the following standard processes:

- Employee entry
- Automatic employee exit to revoke authorizations
- Locking user
- OU change for roles and systems
- Role request procedure
- System request procedure
- Reconfirmation of already allocated authorizations, licenses, users (re-certification, re-licensing, re-validation)
- Request of role change
- Delegation

## Business Layer for IdM Systems

### 3 Only with a Business Layer IdM is Future-proof

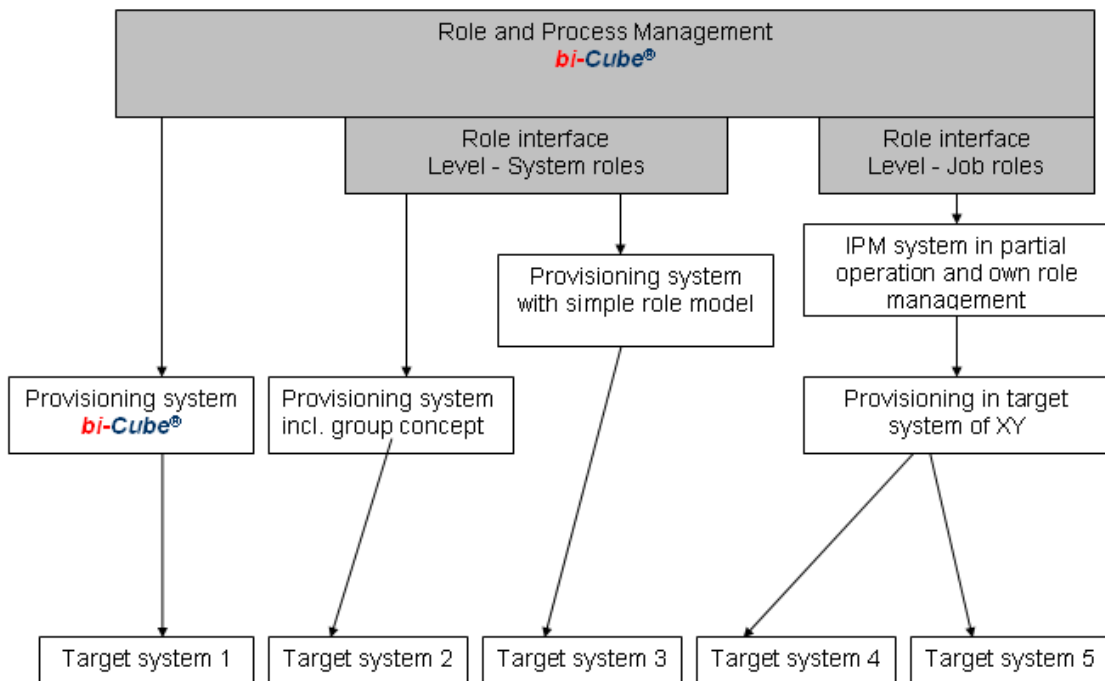
**bi-Cube**<sup>®</sup> IPM has therefore achieved the IPM level 5 of the general process maturity for Identity & Process Management = IPM.

IPM level	Properties of processes	Opportunities	IPM results
<b>5</b> dissipative business layer	Integrated role and process model, routine application of standard processes, increasing automation, separation of modeling and administration ICS - Self monitoring	Continuous evolution and automatic adaption, early warning function, qualification of the rule system	High productivity, motivation and quality
<b>4</b> controlled	Application of a central provisioning tool, simple group concept, based on the conventional provisioning	Integrated technological base, problem avoidance, integration of additional components	
<b>3</b> standardized	Central manual organization and documentation, single areas partially automated e.g. via AD	Qualitative and structural illustration of processes, problem recognition	
<b>2</b> regular	Systematization, but different stages of development and isolated single processes	Check, tests, standards; recognizing risks and potentials	
<b>1</b> Ad hoc situation	Improvisation, authorizations on demand, no documentation	Introduction of operational tools, controlling; data qualification for reports	High risk, friction loss

## Business Layer for IdM Systems

### 4 *bi-Cube*<sup>®</sup> in a Mixed Environment

Other products on the market have none or only rudimentarily developed functionality in the scope of business processes. *bi-Cube*<sup>®</sup> is able to provide 'on-top' business functionality for products like e-Directory, Tivoli, DirX, SAM Jupiter or Active Entry.



## 5 Differentiated Requirements

The goal and motivation to implement an IdM system depends on the size and complexity of the IT environment of each company.

The present system architecture and function of the IdM products available on the market is targeted on the needs of large enterprises – due to the fact that mainly this target group has been affected by a constantly increased pressure regarding compliance, security and rationalization of IT administration processes during the past years.

SMB, on the contrary, have been influenced significantly less or at least delayed by these reasons. Moreover, SMB have a considerably higher demand for the IdM function volume / functionality.

	Large companies	SMB
Compliance / traceability	essential	relatively insignificant
Automation of IT-administration	often required	relatively insignificant
Functional width	Close but different functional framework	Important factor
Lateral processes	Only IdM core functions required, since special systems are used for lateral processes	Additional features are of high significance: license control, SSO, internal cost allocation, assets. Interface to access control
HR interface	Automatic data synchronization HR > IdM	Not necessarily required In some cases IdM assumes the function of the HR system
Connectors	Core systems with direct connectors	Often action 7* is sufficient (semiautomatic process)
Client capability (Multitenancy)	Usually necessary	Rarely required

### 5.1 IdM requirements of large enterprises / corporate groups

Large enterprises implement IdM projects in several phases. At the beginning the focus is usually on a narrow function channel defined by the management targets (Compliance, SOX-audits, mergers, new IT strategy such as SOA, SaaS etc.)

## Business Layer for IdM Systems

### 5.2 IdM requirements of small and medium-sized businesses:

- A suite is required which should not only provide IPM but also affiliated functions, since special corresponding programs are usually not available at small and medium businesses, unlike in large corporations.
- Therefore an IdM - besides its core functions - should also offer the following:
  - a simple personnel administration
  - administration of credentials and role model
  - administration of locations and cost centers
  - an integrated SSO, license control and cost allocation of IT resources
  - an authentication server
  - the integration of a simple SW distribution (MSI by AD groups)
  - an AD based role integrated management of resources
  - predefined reports
  - an integrated workflow manager with pre-configured process models
  - an interface to access control

## 6 SMB as the New User Group of IdM Solutions

Conditions on which a small or medium-sized business should consider an IPM solution:

- If the business has approx. 300 user and an IT environment of medium complexity
- If the company has a very complex IT environment of different system platforms
- If the company manages data which represent the ideational assets of the enterprise
- If the company is a sub-supplier for finalists, and the finalist imposes its compliance requirements on the sub-supplier (e.g. SOX).

Requirements of the SMB to the IdM vendor:

- It should also be a SMB to guarantee sufficient problem understanding of an IdM prospect.
- It should be located in the same country to avoid language misunderstandings or time zone delays.
- A SMB-vendor is able (and also ready) to come to terms with certain special demands of the SMB-customer at short notice.
- The solution should have been developed in the same country since it must be focused on country specifications and laws.
- The product should have reached a certain maturity to offer satisfying stability.
- Usually a SMB does not have specific IPM specialists. Therefore full service up to the outsourced management of the solution by the IdM-vendor should be offered.
- The IdM product should represent the strategic product of the vendor to guarantee the SMB safety of its investment.
- Most favorable and cost saving for the customer is direct delivery, maintenance and support by the software manufacturer.

## 7 IdM as Managed Services

For enterprises in the upper SMB segment, the problems of the expert and skilled maintenance of the system arises after the productive implementation. Although the IdM system can actually be serviced by the current user administrators, the profile of qualification is now completely different. Their job specification now comprises logical modeling, consideration of organizational issues as well as comprehension of and the work with role and process models. This cannot be just a side job for e.g. the AD-administrator.

This problem has to be solved in order to pave the way for IdM in the SMB sector.

### 7.1 Full service concept

IdM systems often exceed own skills and capacities of small and medium-sized businesses. Although their IT infrastructure can be as complex as those in large enterprises, SMB often do not have qualified IT administrators and cannot or don't want to bind scarce personnel resources with the necessary expertise to manage an IdM solution. Contrariwise they wish or need the possibility to use an IdM or Single Sign-on.

For this specific situation, iSM offers a flexible modular support for the **bi-Cube**<sup>®</sup> SMB solution.

The full service concept includes a broad customer support, assisting the customer in designing, modeling and operating the IdM solution (which is installed in the infrastructure of the customer).

### 7.2 IdM outsourcing or Managed services

In logical further consequence of the full service, the service provider also offers operation of the IdM system. Connected with this service, several technical and business organizational issues may occur, resulting in high security requirements:

- The customer communicates with the IdM system via Web only (Security)
- The services and connectors, however, are running at the customer's site, since they must have direct access to the target systems of the IdM.
- The modeling (roles, processes etc....) is made by means of separate request procedures.
- The service provider must work with a so-called secured operational concept.
- The service provider must commit himself to specific IdM SLAs
- The service provider must offer a transaction related pricing model

In connection with Managed Service, technical approaches like SOA and SaaS have been considered in view of their usability and application maturity and concrete solutions have already been developed.