

## Unique Selling Propositions *bi-Cube*<sup>®</sup>

Based on many years of experience of the iSM team in provisioning projects as well as our research projects, the current version 7 of *bi-Cube*<sup>®</sup> could be provided with several essential functions, offering a solution to the customer with which he can reach the currently highest process level 5. For the time being, this is not possible with any other product (e.g. the large vendors IBM, Sun, Oracle etc.)

IPM level	Features	Chances	IPM result
<b>5</b> Dissipative	Integrated role and process model, routine use of standard processes, increasing automation, separation of modelling and administration ICS – self-monitoring	Continuous evolution and automatic adaptation Early alarm function, qualification of the rule system	High productivity, motivation and quality
<b>4</b> Controlled	Use of a central provisioning tool Simple group concept, based on the traditional provisioning	Integrated technological basis, avoidance of problems, integration of more components	
<b>3</b> Standardized	Central manual organisation and documentation, Certain fields partially automated e.g. via the AD	qualitative and structural illustration of processes, problem recognition	
<b>2</b> Regular	Systematization, but different development levels and isolated individual processes	Tests, verifications, standards; recognition of risks and potentialities	
<b>1</b> Ad hoc Situation	Improvisation, rights on call, no documentation	Implementation of operational tools, controlling; qualification of data basis for reports	High risk, frictional loss

In order to reach this process level, functions and architecture approaches as realized in *bi-Cube*<sup>®</sup> are required:

*bi-Cube*<sup>®</sup> USP in brief :

- Integrated technological approach, based on the special ‚Logical Message Processing‘
- SOA = service-oriented architecture: (SDK = software development kit, Web Services)
- Integrated efficient organisation and role model
- Security Classification on all objects and attributes for risk balancing
- Role-oriented workflow system with integration of organizational data
- Efficient set of rules, consisting of model inherent = definitional rules and logic engine = inference machine (internal prolog interpreter)
- Pre-configured best practice applications for request procedures (generic process models)
- Skill Management in connection with the role model
- SoP / self-organising provisioning
- High automation level of administrator job
- Wide range of functions: system-integrated SSO with authentication server
- Integrated privacy concept
- Deep integration of ADS: unique system, which administers the ADS-OU not only through references, but also actively. E.g.: automatic generation of group and dept. filespace
- Integrated USB-Blocker (individual control of USB-ports and all other storage media such as CD, DVD etc.
- Process-integrated Signature Management (PKI = public-key-infrastructure)
- Security-Token (RSA-like)
- Integrated document server with the possibility to attach any documents to objects

## Unique Selling Propositions *bi-Cube*<sup>®</sup>

### Intrinsic safety and Compliance

- Internal Control System (ICS), monitoring security-critical incidents
- Scheduled generating and sending of reports

### Special Services (Accessory processes)

- Additional functions: Entry-Control
- Absence and holiday administration (necessary for process manager)
- Internal cost control
- SLA, associated with transaction-related billing model
- Internal Licence Management
- Freely definable document-based application procedure
- Administration of and application for services, equipment and communication facilities

## 1 Architecture and wide range of functions

Currently there's no other solution provider on the market, achieving the

### High level of the *bi-Cube*<sup>®</sup> IPM architecture and functionality (USP)

- Consistent realization of a modular IPM-specific architecture
- Technology: asynchronous messaging with logic processor
- Open architecture with several interfaces, e.g. SOA-conform Web Services
- Wide range of functions (Identity Management, Provisioning, SSO, Licence and Resources Manager, Internal Cost Allocation, Biometrics ....)
- Intelligent SoP Services (Self-organising Provisioning)
- Efficient Role and Process Management
- Compliance Agents and Internal Control System
- Practical proof of a short and effective introduction phase

### Asynchronous Messaging (USP)

- This principle is a USP of *bi-Cube*<sup>®</sup> and the main aspect for iSM's present technology leadership
- Different from the customary way, the data is not written directly to the data base. Instead, messages are being sent from any system to any other system into a central message room (MR)
- Each target system is connected with the message room through an output connector and is provided with relevant messages (changes of data) by *bi-Cube*<sup>®</sup>. Regular processing is guaranteed by transaction status transfers.
- These messages represent a *bi-Cube*<sup>®</sup> internal protocol
- Before the message processing continues, each message runs through a logic processor which checks the consequences of the messages. As a result of this check, several new messages can be generated, etc.

## 2 Role model and SoP (Self-organising Provisioning) (USP)

The *bi-Cube*<sup>®</sup> process models are the basis of the SoP procedure and the automation of the ICT administration.

## Unique Selling Propositions *bi-Cube*<sup>®</sup>

Organisational, job and system roles are allocated as well as withdrawn again, to a large extent automatically, by logical attribute and object references.

Change processes, such as 'Start of employment' - 'End of employment' – 'Change of organisational unit (OU)' – 'Change of OU structure' and 'Change of location' are automatically adopted into the role model.

The automatic processes can be supplemented by approval and information activities at suitable positions.

### Special possibilities in role modelling

In *bi-Cube*<sup>®</sup>, the following technologically efficient functions for role modelling are realized:

- **Synthetic job and system roles (USP)**  
These roles can be directly adopted from the integrated role-mining into the system.
- **Security Classification of roles (SC) (USP)**  
Each object (e.g. the roles) can be attributed to a SC which can be used for process control.
- **Mandator and team roles (USP)**  
Correct management in case of several accounts
- **Trouble-free migration capability from direct to role-based allocation of rights (USP)**
- **Primary Account (USP)**
- **Shadow User (one person in several OUs) (USP)**

### 3 Problems occurring in SoP processes (Self-organising Provisioning) and their solution in *bi-Cube*<sup>®</sup> (USP)

- **Role conflicts (USP)**  
Aggregation or separation of system rights, which are allocated to the user through different roles. Basic rule: the role system dominates direct allocation. Soft migration from direct system allocation to role model
- **Attribute-indexed roles (USP)**  
Free attribute-indexing incl. Boolean logic  
Basis of automation of IPM processes
- **Role references (USP)**  
Basic roles are connected with special roles und allocated automatically
- **Heredity of roles in object structures**  
Roles can be indexed with attributes, referring to hierarchic object structures (e.g. organizational structure, locations, cost centers,..). A role can be configured to be bequeathed to a certain defined depth of the object structure. Control of the change processes, resulting from a probable change of object structures, is most essential in this connection
- **Smooth transition / Change processes (USP)**  
In case of a role change (e.g. change of OU), rights should not change abruptly (possibility of lead and follow-up time and other configurable rules)

- **OU competences**  
This particular construct allows modelling of various views to the organizational structure (OU). Directors, locum tenens, administrators, offices etc. can be freely defined. A director, for example, only sees the users in his OU. An administrator can be assigned to any OU and any depth of the OU structure. He can be assigned to complete branches of the OU structure. In previous versions, these so-called positions with their whole impact were stipulated in the OU. Now the so-called OU competences can be defined freely. Above all, this is necessary for a flexible management of the actors within the process manager.
- **Transaction management (USP)**  
Transactions, being triggered by attribute modifications, have to block certain changes until the transaction is terminated
- **Reduction of role diversity (USP)**  
In connection with the process management, the number of required roles can be significantly reduced. Certain necessary characteristics of role attributes (technical attributes) can remain open in the role definition. These attributes are defined during the allocation process and allocated to the user individually. This is for example a simple and clear method of modelling roles in project and team structures: the rights of a project leader are determined once. Which data view (project documents) he is allowed to have access to, can be determined during allocation of the role.
- **Multi-dimensional management of rights (USP)**  
4 dimensions of rights can be used for modelling and management:
  - Rights / Roles
  - Data views
  - OU competences
  - Security Classification
- **Roles and Teams ( Project organisation) (USP)**  
Aim:
  - Allocation of rights to defined temporary groups of users
  - Central modelling, decentral provisioningRules:
  - The team is provided with a start and expiry date.
  - Team members are assigned to a position (Team leader, locum tenens...)
  - The team leader demands for users for his team, allocates rights and controls the duration of the team
  - Users obtain the team roles on their entrance into the team and lose them on leaving the team.

#### 4 **Model inherent rules and logic engine (inference machine) in process control**

- 4.1 Model inherent rules and logic engine (inference machine)  
The integration of roles and processes requires an efficient rule processing.

## Unique Selling Propositions *bi-Cube*<sup>®</sup>

In IPM products (at least according to the knowledge of the author) there is only a complex of model inherent rules which are defined directly in the GUI to objects, attributes and the basic relations between them.

The further qualification of the processes required more complex rules which could not be controlled anymore by the existent separate model inherent rules. Therefore a rule machine was developed and integrated for the processing of a logic engine (inference machine). This component (*bi-Cube*<sup>®</sup> - Logi) processes simple, complex and also recursive prolog notations. The chosen syntax has been designed in an almost natural language. Thus all occurring logical combinations for the process control can be framed and – after certain practice – be defined also by the operator.

### 4.2 Skill Management in connection with the role model

By use of the skill management, integrated in *bi-Cube*<sup>®</sup>, role skills can be used for the search of suitable employees or for verification of a role allocation in the application procedure.

### 4.3 Pre-configured best practice applications for request procedures: Generic Process Models (GPM)

For various processes in the provisioning, templates can be defined, reducing this sub-project by 70 to 80% in time and effort. These templates are tested in all parameters and can be used immediately in a productive environment.

In the GPM project of the iSM, a standard set of GPM was defined, explicitly described and realized in *bi-Cube*<sup>®</sup> step by step. Gradually, because this range of GPM is permanently expanded by new ideas, originating from the projects.

The following processes have been identified from the operators' point of view:

1. Application for the allocation of roles
2. Automatic allocation of rights for new employees (start of employment)
3. Confirmation and administration of policies (directives) - separately as well as integrated in the application process
4. Automatic withdrawal of rights of employees leaving the company (end of employment)
5. Immediate blocking of users
6. Consideration of sliding transitions / job change processes
7. Re-entrance into corporate group structures
8. General document-based application process
9. Request for general applications without structuring of rights
10. Support request to URA (user and rights administration )
11. Re-Licensing (regular confirmation of granted licenses)
12. Re-Certification (regular confirmation of granted rights of users)
13. Re-Validation (regular confirmation of the existence of users)
14. Password self-service

Special processes:

- Application for a work place including equipment options
- Application for access rights

## Unique Selling Propositions *bi-Cube*<sup>®</sup>

- Additional functions: Entry Control
- Absence / holiday administration (for control of task-manager)
- SLA in connection with transaction-related billing model
- Freely definable document-based application procedure
- Administration of and application for services, equipment and communication facilities

From these examples the following classification of IPM processes (into which all other processes may be integrated) can be derived:

### Process groups

- Job change processes of users
- Application procedures
- Repeat authorization
- Secondary processes
- Service processes
- Internal processes

## 5 More unique *bi-Cube*<sup>®</sup> features and functions

- Dynamic Filespace Management (USP)
  - Automatic generation of dept. and group file spaces
  - Automatic allocation of dynamic file spaces to users
  - Change processes of OU generate changes of dynamic file spaces
  - Automatic change of dynamic file spaces in case of OU change of user
- Support of Privacy (USP)  
As each attribute can be given a security classification (SC), personnel data worth to be protected, can be treated separately
- More fields of application
  - Licence control (USP?)
  - Integration of USB Blocker (USP)
  - Project controlling in software development (USP)
  - Internal cost control
- PKI in *bi-Cube*<sup>®</sup> IPM environment
  - Only by integration of *bi-Cube*<sup>®</sup> IPM, PKI can be operated economically (USP)
- Compliance and ICS (Internal Control System) (USP)  
Full traceability of all actions and internal monitoring of the system.  
*bi-Cube*<sup>®</sup> can provide information as to which rights a user had at any point of time in the past. Other systems can only report changes from today back to the point of time in question.

## 6 IPM-integrated Single Sign-on

*bi-Cube*<sup>®</sup> is the only product, offering an integrated SSO. Contrary to other vendors, this is not a third party product which has to be integrated by several synchronizing mechanisms and therefore is not subject to the uniform logic and process management.

## Unique Selling Propositions *bi-Cube*<sup>®</sup>

The additional authentication in SSO offers an active authentication on starting applications worth to be protected. In addition to the server-based SSO profile, each user can create his personal SSO profile.

In the password management is effected:

- an automatic password change in target systems if connectors are used
- a Password-Self-Service via the *bi-Cube*<sup>®</sup> web client

In certain application areas the function of a fast user change is required (hospital, shops ...). The Logon Manager takes over other functions in the management of the applications.

The SSO is suitable for the use in a Terminal-Server environment and for integration of biometric authentication.

## 7 Integrated Authentication Server

The *bi-Cube*<sup>®</sup> authentication server provides the following functions:

Dual, secured authentication in several combinations:

- Fingerprint and ID on smart card
- Only user ID on smart card
- Identification of user by fingerprint only
- Biometrically secured token

Both *bi-Cube*<sup>®</sup> tokens (Secu-Token or SMS-Token) can be used by means of radius protocol for secure authentication.

The Token can also be secured by a PIN and therefore be used by external users (e.g. bank or insurance clients...) for secure authentication. These functions:

- Token administration
- Token allocation
- Activation of Certificate Logon
- Token blocking
- FallBack solution for Certificate Logon

provide the close integration of a PKI with an Identity and Provisioning System for the digital certificates.