

White Paper

bi-Cube[®] SSO

Synergy by Connecting an External SSO to the *bi-Cube[®]* IPM

Technologies Solutions Trends Experience



Table of contents

1	OBJECTIVE	3
2	FUNCTIONS CONCEPT	3
2.1	Structure	3
2.1.1	Indirect Connection	3
2.1.2	Direct Connection	4
2.1.3	Special Connection	4
2.2	Transfer Data	5
2.3	Procedures	5
2.3.1	New User Creation/Deactivation	5
2.3.2	User Locking.....	5
2.3.3	System Assignment/Revocation.....	5

1 Objective

Users of SSO-Systems quickly recognize possible synergy effects of a provisioning system, synchronized with SSO. The SSO as well as the Identity & Provisioning Management solution manage users of companies in a certain status and their accounts (user name/password) for different target systems.

The SSO exclusively serves the purpose to assume the many different system logons of the user. The Identity & Provisioning Management has a more sophisticated function for the entire user administration process. By a role and process model an automatization and with this, a higher security level is achieved. Only by process automatization and the release of action confirmations, the current requirements can be fulfilled from view of the compliance. Besides additional synergy effects a clear reduction of personnel expenditure is possible.

Companies who use SSO from Imprivata or Evidian, may also use with the interface of **bi-Cube[®] IPM** all the effects without double work.

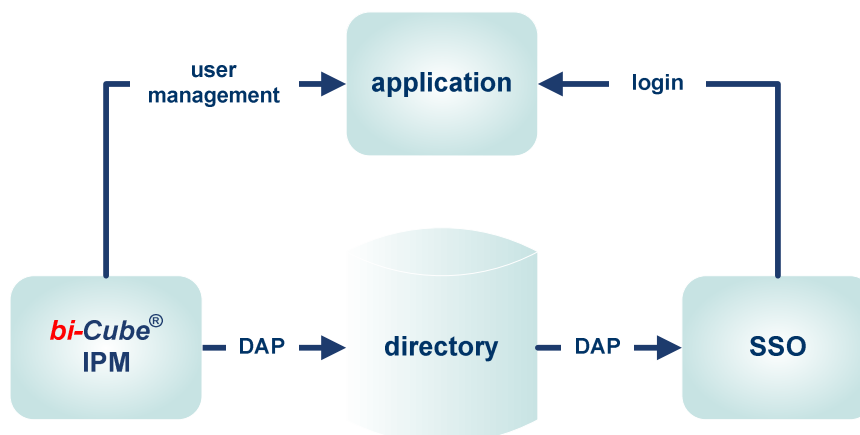
2 Functions Concept

Identity & Provisioning Management (IPM) is the main function for the management of users and authorizations. Generally several concepts are offered for this connection.

2.1 Structure

2.1.1 Indirect Connection

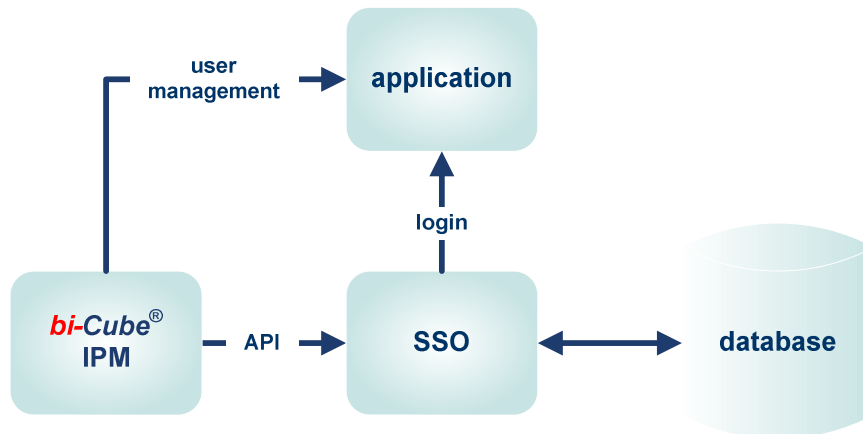
Besides the maintenance of the user account in the target application, IPM transfers the necessary information into a directory system. The SSO reads the information of this directory system and carries out the logon of the user at the target application.



The Active Directory or different LDAP server are possible as directories.

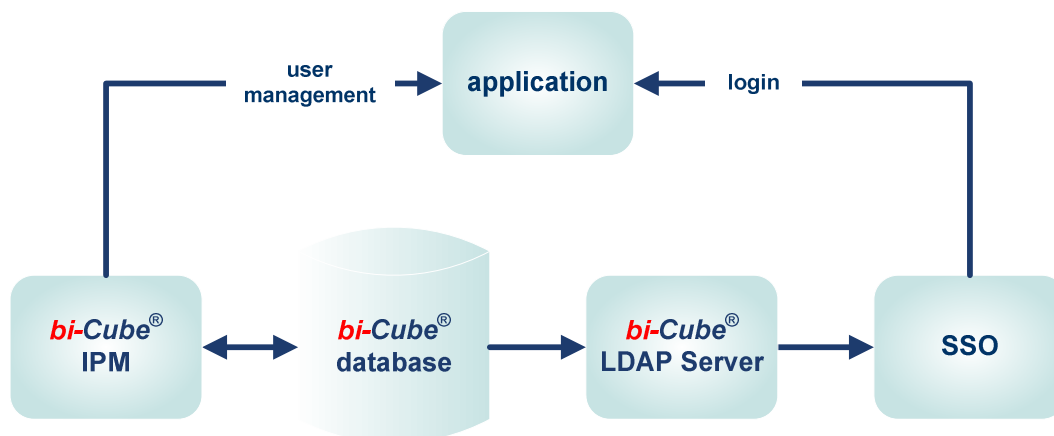
2.1.2 Direct Connection

The SSO is directly connected to the IPM by an API, Web services or similar. SSO manages its own database and directory.



2.1.3 Special Connection

A special connection is a *bi-Cube*[®] database via a SDAP server. Thus, the external SSO can indirectly access the *bi-Cube*[®] database.



2.2 Transfer Data

To keep the integration of both solutions transparent to the customer, a synchronization of user and account data, or the assignment or revocation of an account in a target system is necessary. Current changes of the user status are to be transferred to the external SSO.

Required data for the SSO functionality:

- LAN user name (as identity of the user)
- LAN password (optional)
- User name in the target application
- Password in the target application
- Status of the user

Applications operated by the SSO have to be known to the IPM (subset of target systems managed by IPM)

Relevant data for the IPM like, finger prints, certificate etc. may be exchanged optionally. It is also possible to add additional information of the user, such as post address, telephone number etc.

2.3 Procedures

2.3.1 New User Creation/Deactivation

A new user creation or deactivation is processed in the respective **bi-Cube[®]** target system which is used by SSO for the user data. Is the Active Directory used as SSO directory than the SSO may access the including data. In case other directories or APIs are used then required information may be distributed by a connector.

2.3.2 User Locking

At locking of a user, the user's assigned "access systems" are locked by **bi-Cube[®]**. The user will keep his authorizations, so that after the unlocking he immediately can keep on working. A status information is transferred by **bi-Cube[®]** to the external SSO, that it has to process this information in a manner so that the user cannot use his SSO anymore.

2.3.3 System Assignment/Revocation

At system assignment, an account (user name / password) and corresponding authorizations for the target system is assigned to the user by **bi-Cube[®]** and provisioned by the adequate connector. At the same time the account data of this assignment is transferred to the external SSO by the API, or written in the common directory. Analogously the deletion of an account occurs.

According to the configuration at the IPM, the user will be notified of account changes by e-mail. If the user is manually or automatically informed of SSO applications then the e-mail information can be changed. Herewith an always criticized security problem is eliminated. The user or his supervisor does not need to know the start accounts. They only must be known to the SSO.