

Whitepaper

bi-Cube[®] SSO

Synergien durch die Anbindung eines externen SSO an **bi-Cube[®] IPM**

Technologien Lösungen Trends Erfahrung



Inhalt

| | | |
|------------|---|----------|
| 1 | ZIEL | 3 |
| 2 | FUNKTIONS-KONZEPT | 3 |
| 2.1 | Struktur | 3 |
| 2.1.1 | Indirekte Anbindung | 3 |
| 2.1.2 | Direkte Anbindung | 4 |
| 2.1.3 | Spezielle Anbindung..... | 4 |
| 2.2 | Übergabedaten..... | 5 |
| 2.3 | Abläufe..... | 5 |
| 2.3.1 | Nutzerneuanlage/Deaktivierung | 5 |
| 2.3.2 | Nutzersperrung..... | 5 |
| 2.3.3 | Systemzuweisung/-entzug | 5 |
| 3 | TECHNISCHES LÖSUNGS-KONZEPT..... | 6 |
| 4 | FRAGEN AN DEN HERSTELLER..... | 6 |
| 4.1 | Verzeichnissystem | 6 |
| 4.2 | Programmschnittstelle..... | 6 |
| 4.2.1 | Webservice als Interface | 7 |

1 Ziel

Anwender eines SSO-Systems erkennen sehr schnell die möglichen Synergieeffekte eines mit dem SSO synchronisierten Provisioning Systems. Sowohl das SSO als auch die Identity & Provisioning Management Lösung verwalten die Nutzer des Unternehmens in bestimmten Status und deren Accounts (Benutzername/Kennwort) für die verschiedenen Zielsysteme.

Das SSO erfüllt dabei ausschließlich den Zweck, dem Nutzer die vielen verschiedenen Systemanmeldungen abzunehmen. Das Identity & Provisioning Management greift allerdings deutlich weiter in die gesamten Prozesse der Nutzeradministration ein. Über ein Rollen- und Prozessmodell wird eine deutliche Automatisierung und damit eine wesentliche Erhöhung des Security Niveaus erreicht. Nur durch die Automatisierung der Prozesse und der damit verbundenen Freigabe- und Bestätigungs-Aktionen können die aktuellen Anforderungen aus Sicht der Compliance befriedigt werden. Neben weiteren Synergie-Effekten ist außerdem eine deutliche Reduzierung des personellen Aufwands möglich.

Unternehmen, die z.B. das SSO von Imprivata oder Evidian einsetzen, können mit der Schnittstelle, die **bi-Cube[®] IPM** (IPM = Identity & Provisioning Management) bietet, alle diese Effekte nutzen, ohne dass doppelter Aufwand entsteht.

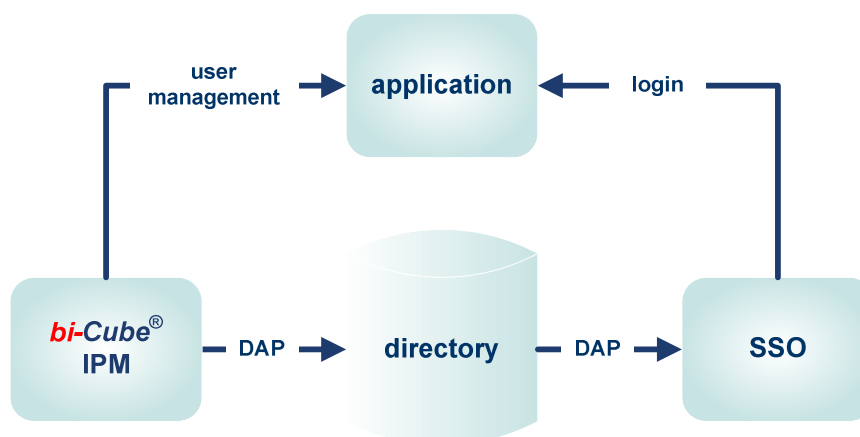
2 Funktions-Konzept

Für die Verwaltung der Nutzer und Berechtigungen übernimmt das Identity & Provisioning Management (IPM) die führende Funktion. Generell bieten sich verschiedene Konzepte für die Anbindung an.

2.1 Struktur

2.1.1 Indirekte Anbindung

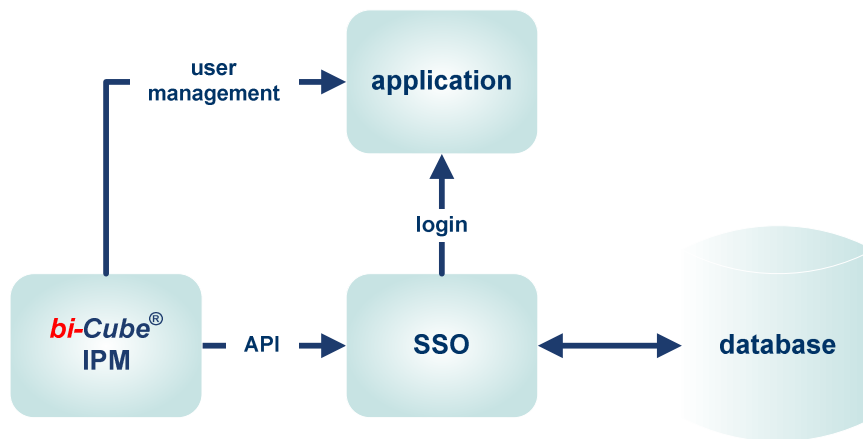
Neben der Pflege des Nutzerkontos in der Zielanwendung übergibt das IPM die notwendigen Informationen in ein Verzeichnissystem. Das SSO liest seinerseits die Informationen aus dem Verzeichnissystem und nimmt die Anmeldung des Nutzers an der Zielanwendung vor.



Als Verzeichnisse kommen dabei z.B. das Active Directory oder verschiedene LDAP-Server in Frage.

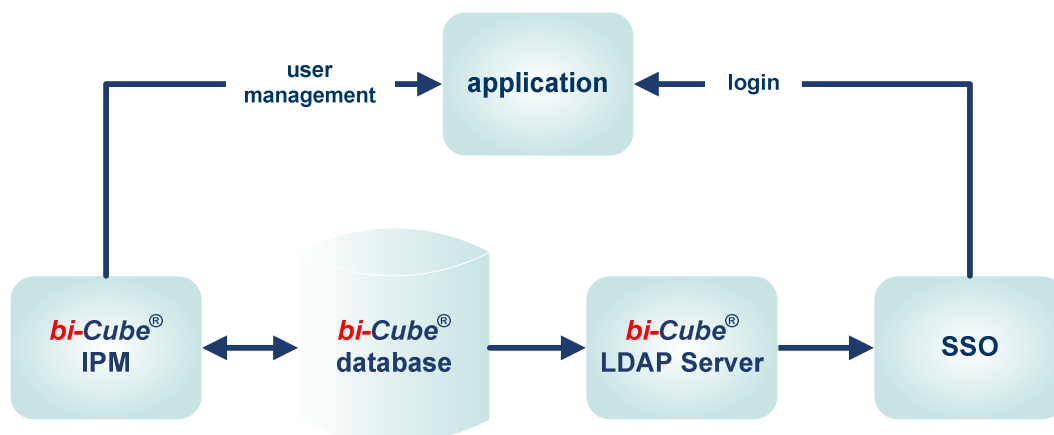
2.1.2 Direkte Anbindung

Das SSO wird über eine API, Webservices o. dgl. direkt an das IPM angebunden. Das SSO verwaltet seine Datenbank bzw. sein Verzeichnis selbst.



2.1.3 Spezielle Anbindung

Eine spezielle Anbindung stellt die Abbildung der **bi-Cube[®]** Datenbank über einen LDAP-Server dar. Damit könnte das externe SSO mittelbar auf die **bi-Cube[®]** Datenbank zugreifen.



2.2 Übergabedaten

Um die Integration beider Lösungen für den Kunden transparent zu halten, ist ein Abgleich der Nutzer- und Accountdaten bzw. der Zuteilung oder des Entzugs eines Accounts in einem Zielsystem erforderlich. Aktuelle Änderungen im Nutzerstatus sind ebenfalls an das externe SSO durchzureichen.

Die notwendigen Daten für die SSO-Funktionalität sind:

- LAN-Benutzername (als Identität des Nutzers)
- LAN-Kennwort (optional)
- Benutzername in der Zielanwendung
- Kennwort in der Zielanwendung
- Status des Nutzers

Dem IPM müssen alle Applikationen bekannt sein, die durch das SSO bedient werden (Teilmenge der durch das IPM verwalteten Zielsysteme)

Optional können weitere für das IPM relevante Daten wie Fingerprints u.ä. ausgetauscht werden. Ebenso ist es möglich, zusätzliche Informationen zu den Nutzern wie Mailadressen, Telefonnummern o. dgl. zu übergeben.

2.3 Abläufe

2.3.1 Nutzerneuanlage/Deaktivierung

Bei Neuanlage bzw. Deaktivierung eines Nutzers wird dies von **bi-Cube[®]** im jeweiligen Zielsystem, das vom SSO für die Nutzerdaten genutzt wird, vorgenommen. Wird das AD als SSO-Verzeichnis genutzt, kann damit das SSO auf diese Informationen zugreifen. Bei Nutzung anderer Verzeichnisse oder einer API werden die notwendigen Informationen über einen Connector verteilt.

2.3.2 Nutzersperrung

Bei der Sperrung eines Nutzers werden durch **bi-Cube[®]** die dem Nutzer zugeteilten „Zugangssysteme“ gesperrt. Er behält aber seine Berechtigungen, so dass er nach dem Entsperren umgehend wieder arbeitsfähig ist. Von **bi-Cube[®]** geht eine Statusinformation an das externe SSO, das diese Information in der Weise verarbeiten muss, dass der Nutzer sein SSO nicht mehr nutzen kann.

2.3.3 Systemzuweisung/-entzug

Bei Systemzuweisungen werden in **bi-Cube[®]** dem Nutzer der Account (Benutzername / Kennwort) und die spezifischen Berechtigungen für das Zielsystem zugeteilt und über den entsprechenden Connector provisioniert. Parallel dazu werden die Accountdaten dieser Zuteilung entweder über die API an das externe SSO übergeben oder in das gemeinsame Verzeichnis geschrieben. Analog erfolgt die Löschung eines Accounts.

Je nach Konfiguration im IPM wird der Nutzer per Mail über Kontenänderungen benachrichtigt. Werden die SSO-Anwendungen ihm manuell oder automatisch bekannt gemacht, können die Mailinformationen für SSO-Anwendungen abgeändert werden. Hiermit wird ein immer wieder kritisiertes Security Problem eindeutig eliminiert. Dem Nutzer (bzw. seinem Vorgesetzten) brauchen keine Start-Accounts zur Kenntnis gegeben werden, da diese nur dem SSO bekannt sein müssen.

3 Technisches Lösungs-Konzept

Für die technische Umsetzung ist als Erstes festzulegen, ob ein gemeinsames Verzeichnis (AD, Novell NDS, IBM Tivoli, SUN One, Oracle Internet Directory o. a.) oder ob eine Schnittstelle (C-API, Webservice) verwendet werden soll.

Vorzugsweise sollte das AD benutzt werden. Darin erfolgt notwendigerweise die Anlage des Nutzers und das AD wird z.B. schon für Gruppenmitgliedschaften (der zugeteilten Applikationen) bedient.

In diesem Fall ist die Struktur der relevanten Daten festzulegen.

Für eine Schnittstelle muss eine Beschreibung bzw. eine Definition vorliegen.

Von **bi-Cube[®] IPM** wird ein Standard-Connector SSO-OC (ASCII) angeboten, der alle SSO-relevanten Daten enthält.

In der internen Steuerung des **bi-Cube[®]** ist zu beachten, dass der SSO-OC zumindest für die Neuanlage von Accounts sequentiell nach den direkten Connectoren für die Zielsysteme arbeitet. Es muss gesichert werden, dass im Zielsystem der Useraccount angelegt ist, bevor das SSO den Zugang zu diesem Zielsystem anbietet.

4 Fragen an den Hersteller

4.1 Verzeichnissystem

- Wie sieht die Datenstruktur bzw. das Schema des Verzeichnisses aus?
- Ist auch ein beliebiger LDAP-Server, z.B. OpenLDAP, verwendbar, wenn das Verzeichnis entsprechend konfiguriert wird?
- Speichert das SSO eigene Informationen, z.B. die Anwendungsdefinitionen im Verzeichnis, d.h. muss das SSO im Verzeichnis schreiben können?
- Werden die Kontoinformationen im SSO zwischengespeichert und wie wird die Aktualisierung ausgelöst?

4.2 Programmschnittstelle

Von **bi-Cube[®] IPM** werden folgende Informationen bereitgestellt:

| Funktion | Parameter | Bemerkung |
|--------------|--|--|
| User-New | Verw-ID User-ID_SSO User-Attribute | Verw-ID zur eindeutigen Zuordnung im bi-Cube IPM User-ID_SSO = ID des Users im SSO bzw. des userdaten-verwaltenden Zielsystems (z.B. AD) In bi-Cube referenzierte User-Attribute |
| User-Disable | Verw-ID User-ID_SSO User-ID | |
| User-Enable | Verw-ID User-ID_SSO User-ID | |
| User-Update | Verw-ID User-ID_SSO User-Attribute | Geänderte User-Attribute |

| | | |
|-------------|---|--|
| Account-New | VerwID User-ID_SSO User-ID / PW | User-ID und PW des Users im Zielsystem |
| Account-Del | VerwID User-ID_SSO User-ID | User-ID des Users im Zielsystem |
| PW-Change | VerwID User-ID_SSO User-ID PW-old / PW_new | |

Für die Datenübergabe per Datei wird das **bi-Cube[®]** Standardformat angewendet:

datum;uhrzeit;system;aktion;verwid;logon;passw;[attributname;attributwert;]

Dabei bedeuten:

| | |
|--------------|---|
| datum | das Datum der Datenübergabe |
| uhrzeit | die Uhrzeit der Datenübergabe |
| system | die betroffene Anwendung |
| aktion | die auszuführende Aktion (siehe oben) |
| verwid | die bi-Cube[®] Verwaltungs-ID des betroffenen Nutzers |
| logon | die Nutzerkennung in der jeweiligen Anwendung |
| passw | das entsprechende Kennwort des Nutzers in der Anwendung |
| attributname | der Name des Attributs |
| attributwert | der Wert des Attributs |

4.2.1 Webservice als Interface

Diese Daten können auch durch einen Webservice bereitgestellt werden, die dann von der aufrufenden Komponente abgefragt und selbständig verarbeitet werden.
Ein weiterer Webservice nimmt vom SSP den RC entgegen und setzt den Status der übergebenen Daten auf erledigt bzw. meldet einen Fehlercode.