

# Whitepaper

**bi-Cube<sup>®</sup> SSO**

**SSO in einer Terminal Umgebung**

Technologien   Lösungen   Trends   Erfahrung



## Inhalt

<b>1</b>	<b>DIE SITUATION.....</b>	<b>3</b>
<b>2</b>	<b>ZIELSTELLUNG.....</b>	<b>4</b>
<b>3</b>	<b>VORAUSSETZUNG .....</b>	<b>5</b>
<b>4</b>	<b>ARCHITEKTUR DER LÖSUNG.....</b>	<b>6</b>
<b>4.1</b>	<b>Biometrische Anmeldung am Terminal Server.....</b>	<b>9</b>
4.1.1	Zusätzliche biometrische Authentifizierung.....	10
<b>5</b>	<b>VORTEILE .....</b>	<b>10</b>

## 1 Die Situation

Die Authentifizierung der Benutzer an der Windows-Anmeldung stellt die erste Stufe der Gewährleistung der Unternehmenssicherheit auf Desktopebene dar. Durch sie wird sichergestellt, dass nur berechnete Personen Zugang zum Rechner und den Daten erhalten. So wird gewährleistet, dass die Benutzer nur die Daten und Programme zur Verfügung gestellt bekommen, für die sie zugelassen sind.

Jedoch liegt genau hier die Schwachstelle des Systems: Kennt ein Unbefugter die Anmeldedaten eines Mitarbeiters, kann er unbemerkt dessen Zugang und damit dessen Daten benutzen. Wird dann noch ein SSO verwendet, stehen dem Eindringling umfangreiche Möglichkeiten zur Verfügung.

Durch ein sinnvolles Kennwortmanagement, welches z.B. Qualität, Länge und Festlegungen zum zyklischen Wechseln der Kennwörter (Kennwortrichtlinien) umfasst, kann ein hohes Maß an Sicherheit erreicht werden.

Welche Ressourcen zur Verfügung stehen und auf welche Art und Weise sie verwendet werden können, wird dabei durch das eingesetzte Kommunikationsprotokoll geregelt.

In den am häufigsten eingesetzten Terminalprotokollen *rdp* bzw. *ica* gibt es jedoch keine Möglichkeit, clientseitig angeschlossene biometrische Geräte mit der Terminalsitzung zu verbinden und zu verwenden.

## 2 Zielstellung

In den IT-Strukturen (vor allem von großen Unternehmen) hat die gesicherte User-Identifikation bei gleichzeitiger Aufwandsreduzierung der Administration und Nutzern eine zunehmende Bedeutung.

Bedingt dies in der zunehmenden Offenheit der IT-Strukturen (Webzugänge, WLAN usw.) und der Vielzahl verschiedener Systeme und Anmeldungen zu Anwendungen oder auch nur bestimmten Funktionen.

Mit Absicherung der User- Authentifikation durch z.B. die Biometrie werden einerseits die Sicherheit und gleichzeitig der Nutzerkomfort erhöht.

In Kombination mit dem **bi-Cube<sup>®</sup> SSO** erübrigt sich für den User die Verwaltung (gelbe Zettel) verschiedener Anmeldedaten zu den von ihm benötigten Anwendungen.

In immer mehr Unternehmen wird bereits die Terminal Server Technologie eingeführt. Durch sie können die Kosten von Hardware und Systemmanagement deutlich reduziert werden.

Die hier beschriebene Lösung zum Thema **bi-Cube<sup>®</sup> SSO** kann im Terminal Umfeld (z.B. Citrix) eingesetzt werden.

Ziel ist es, dass über einen Fat- oder Thin- Client (u.a. embedded XP) die biometrische Anmeldung erfolgt.

Nach erfolgreicher Anmeldung, werden dem User auf dem Terminal Server seine SSO Daten via **bi-Cube<sup>®</sup> SSO Client** bereitgestellt. Die Auswertung der Gültigkeit seiner Daten werden mittels **bi-Cube<sup>®</sup> SSO Client** realisiert. Dazu kommuniziert der **bi-Cube<sup>®</sup> SSO Client** mit dem **bi-Cube<sup>®</sup> Server** und erhält somit einen genauen Überblick über die Anwendungen und Rechte des Users. Somit ist es dem User möglich seine individuellen Anwendungen zu starten.

Für besonders sicherheitskritische Anwendungen kann vor dem Start eine zusätzliche Authentifizierung angefordert werden. Diese Funktionalität wird zentral am System hinterlegt. Als zusätzliche Authentifizierung können alle derzeit angebotenen Methoden des iSM genutzt werden. Ein Beispiel dazu wäre die Nutzung der biometrischen Authentifikation.



Abbildung 1: biometrische Authentifikation

### 3 Voraussetzung

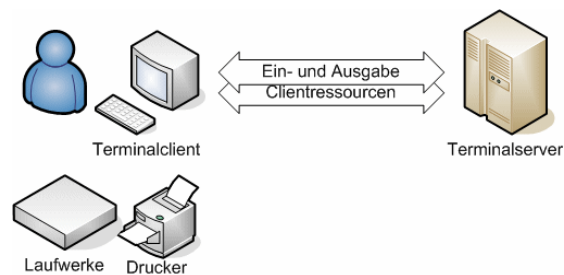
#### Arbeiten in einer Terminal Umgebung

Im Wesentlichen besteht eine Terminalumgebung aus 3 Komponenten:

- Terminalserver
- Terminalclient und
- Kommunikationsprotokoll

Der Terminalclient dient dabei lediglich als Ein- und Ausgabestation. Alle verwendeten Programme werden zentral auf dem Terminalserver ausgeführt. Innerhalb dieser Terminalsitzung können auch Ressourcen des Terminalclients verwendet werden.

Hat beispielsweise ein Benutzer an seinem lokalen Rechner einen Drucker angeschlossen, können Programme, die auf dem Terminalserver ausgeführt werden, diesen wie einen lokalen Drucker verwenden. Auf diese Weise können auch Laufwerke, serielle Anschlüsse und Audioressourcen des Clients verwendet werden.



## 4 Architektur der Lösung

Die Architektur beruht auf der Basis-Architektur von **bi-Cube<sup>®</sup>**. Jedoch kommen nur die erforderlichen Komponenten zum Einsatz.

In der zentralen **bi-Cube<sup>®</sup>** Datenbank werden sowohl die Templates der User als auch deren Logon-Daten, für die Anmeldung der unterschiedlichen Zielsysteme die dem User über den **bi-Cube<sup>®</sup>** SSO Client zur Verfügung gestellt werden, abgelegt. Alle Daten werden mit dem 3DES Verfahren verschlüsselt.

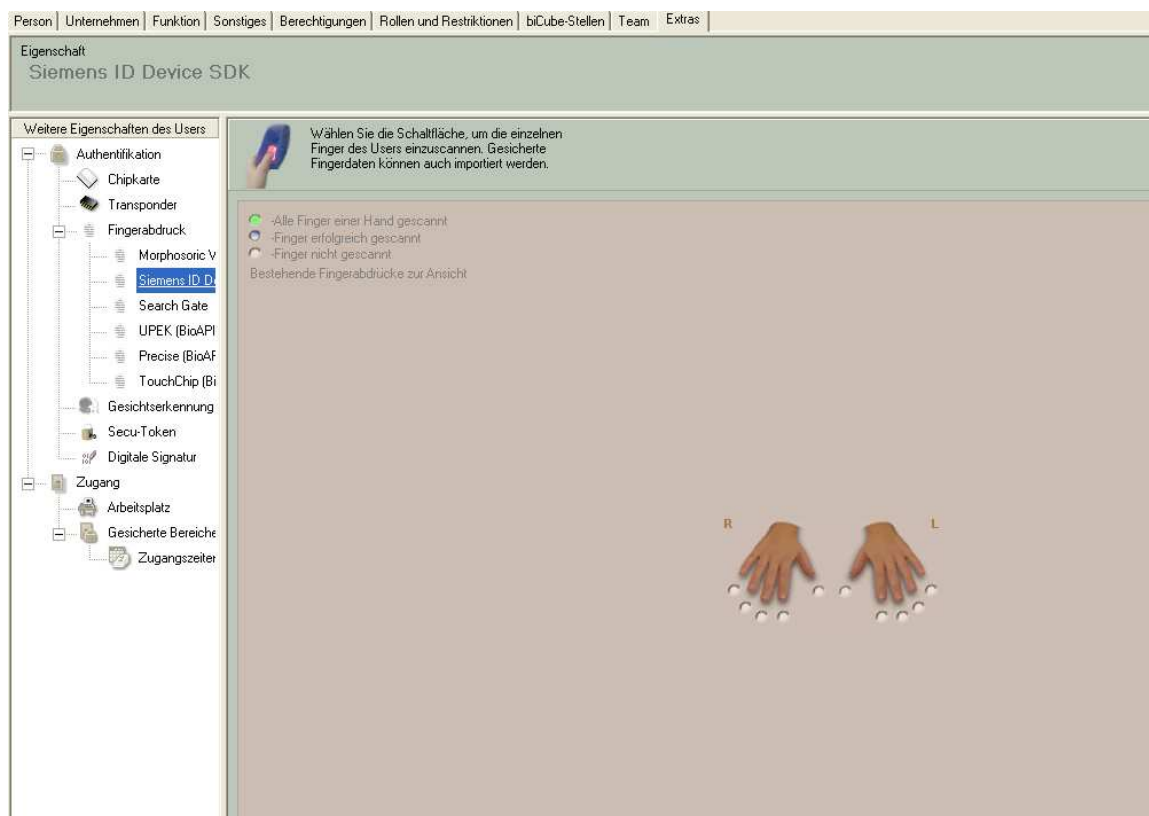


Abbildung 2: **bi-Cube<sup>®</sup>** User Manager im Register Extras

Der **bi-Cube<sup>®</sup>** Server stellt auf Anforderung die benötigten Anmeldedaten aller am Terminal Server angemeldeten bzw. die Anmeldung anfordernden User zur Verfügung.

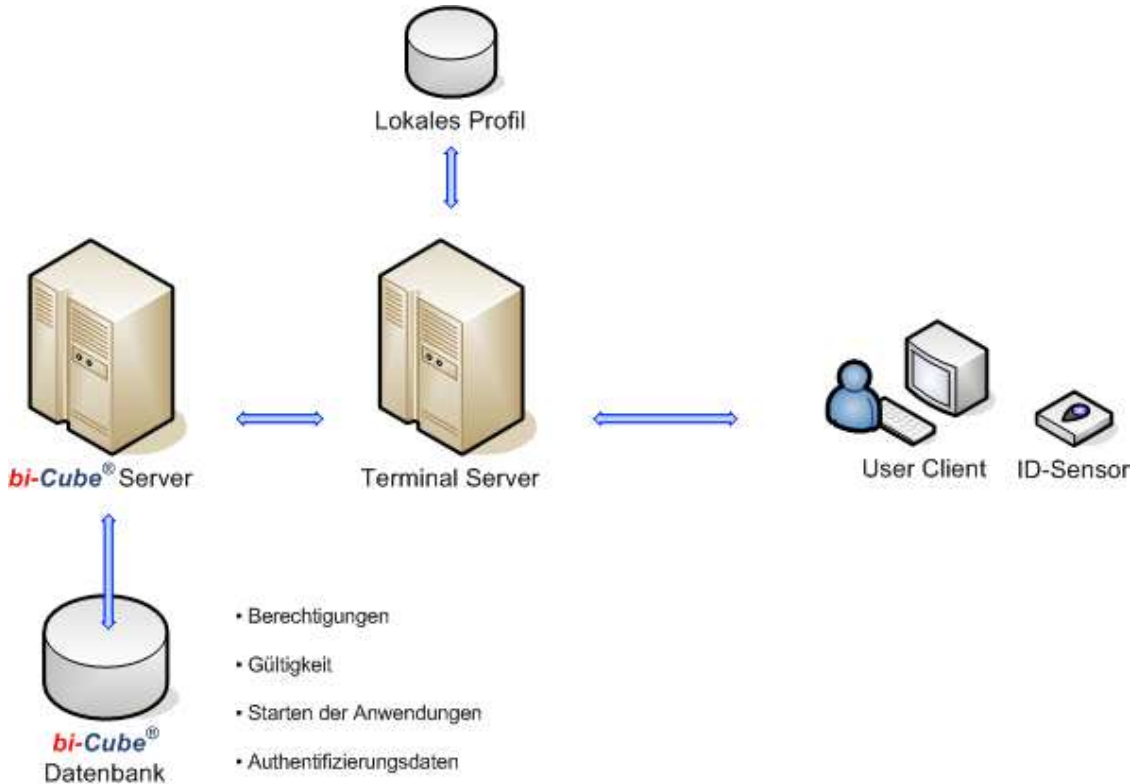
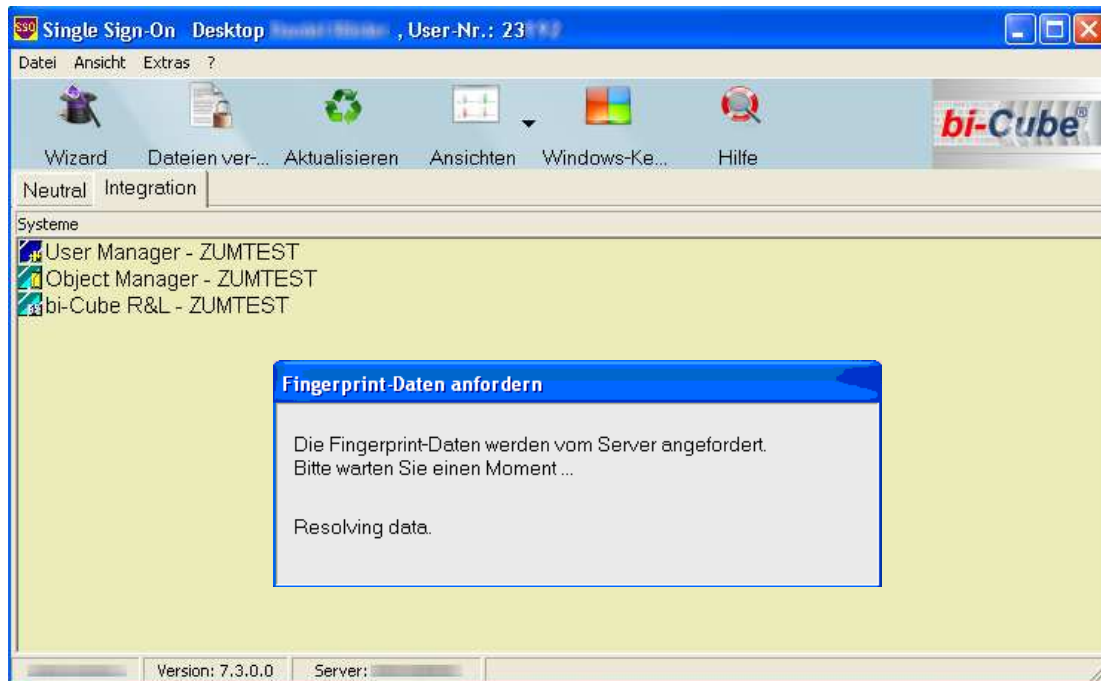


Abbildung 3: **bi-Cube<sup>®</sup>** SSO im Terminal

Dieses sog. SAD-File (secure access data) wird auf dem **bi-Cube<sup>®</sup>** Server gebildet, verschlüsselt und ebenso auf dem Terminal-Server abgelegt. Es wird bei Useranmeldung bzw. Systemstart automatisch (wenn konfiguriert) angefordert bzw. kann bei Änderung der Anmeldedaten oder bei Änderung der Rechte am User aktualisiert werden. Ein automatischer Abgleich des Profils kann auch im laufenden Betrieb organisiert werden, wenn konfiguriert.



**Abbildung 4:** **bi-Cube<sup>®</sup>** SSO Client beim aktualisieren des Profils und der Fingerprint Daten

Die richtige Zuordnung zum User erfolgt durch einen speziellen **bi-Cube<sup>®</sup>** Service auf dem Terminal Server, der über die IP- Adresse des Clients das richtige SAD-File dem konkreten User zuordnet.

## 4.1 Biometrische Anmeldung am Terminal Server

Mit Hilfe eines speziellen Verfahrens, ist es möglich sich mittels Fingerabdruck am Terminal Server anzumelden. Auf dem Terminal Server muss dazu die iSM GINA vor die MS GINA gelegt werden. Dieses Verfahren wird als GINA Chaining bezeichnet. Auf dem Fat- oder Thin- Client sowie auf dem Terminal Server muss ein spezieller Dienst (**bi-Cube<sup>®</sup> Logon Manager**) installiert werden der die biometrische Anmeldung ermöglicht.

Der installierte **bi-Cube<sup>®</sup> Logon Manager** clientseitig fordert vom **bi-Cube<sup>®</sup> Server** die notwendigen Daten für die Anmeldung des Users am Terminal Server an. Können diese erfolgreich ausgewertet werden, erfolgt „OK“ an den **bi-Cube<sup>®</sup> Logon Manager** serverseitig und die Anmeldung wird durchgeführt.

Es erfolgt also eine Verifikation anhand der User-ID und dem dazu gehörenden Fingerprint Templates.

Dieses Verfahren wird für alle verfügbaren Authentifizierungsmethoden des iSM angeboten.

Eine Identifikation der User ist auch möglich. Hierbei spielt die Anzahl der User eine große Rolle. Die Größe eines biometrischen Teams sollte nicht zu groß gewählt werden, da es sonst zu Performance Problemen kommen kann. Maximal 100 User pro Team, sollte hier als Richtwert genommen werden.

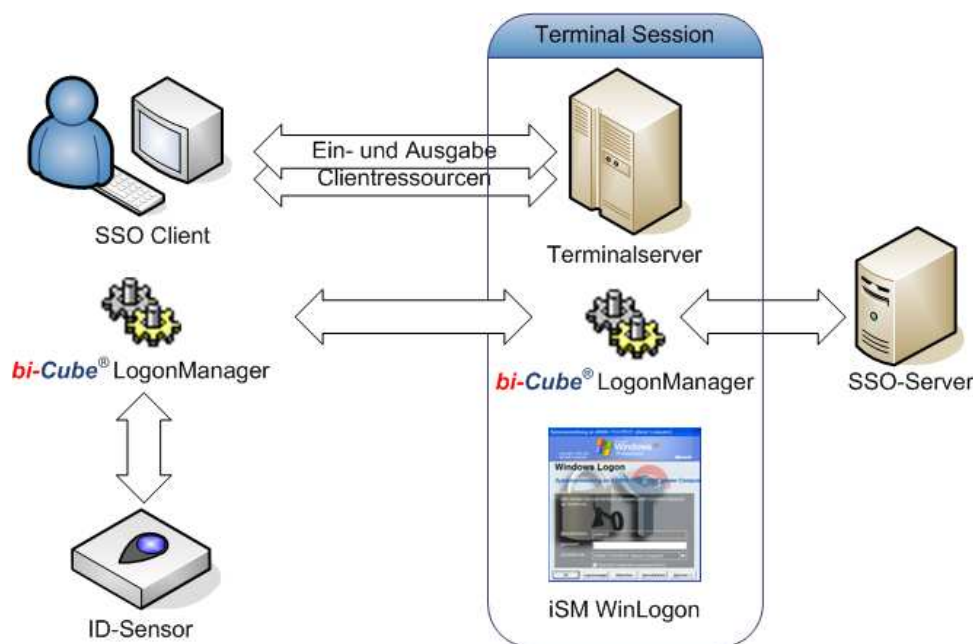


Abbildung 5: **bi-Cube<sup>®</sup> Logon Manager** im Terminal

#### 4.1.1 Zusätzliche biometrische Authentifizierung

Um Anwendungen mit einem sicherheitskritische Anwendungen besser abzusichern, wird bei deren Start durch den SSO-Client nochmals vorher die biometrische Authentifikation angefordert. Um diese spezielle Methode der zusätzlichen Authentifizierung nutzen zu können, muss dies am System im Object Manager konfiguriert sein.



Abbildung 6: **bi-Cube<sup>®</sup>** SSO Client mit der biometrischen Zusatzauthentifizierung

## 5 Vorteile

Es erfolgt technologisch bedingt kein Eingriff in das verwendete Terminalprotokoll. Weil es keinen Eingriff in die zu sichernden Anwendungen gibt, kann praktisch jede beliebige Applikation mit einer zusätzlichen Authentifizierungsmethode z.B.

- Biometrie (Fingerabdruck)
- Speicher-/RFID Karten
- Windows Kennwort
- Token

gesichert werden.