

# White Paper

## **bi-Cube<sup>®</sup> SSO** **SSO in a Terminal Environment**

Technologies Solutions Trends Experience



## Table of contents

<b>1</b>	<b>THE SITUATION .....</b>	<b>3</b>
<b>2</b>	<b>OBJECTIVE.....</b>	<b>4</b>
<b>3</b>	<b>REQUIREMENT .....</b>	<b>5</b>
<b>4</b>	<b>ARCHITECTURE OF THE SOLUTION.....</b>	<b>6</b>
<b>4.1</b>	<b>Biometric Logon to the Terminal Server .....</b>	<b>9</b>
4.1.1	Additional Biometric Authentication.....	10
<b>5</b>	<b>ADVANTAGES.....</b>	<b>10</b>

## 1 The Situation

The first step of company security at desktop level is demonstrated with the user authentication at the Windows logon. This ensures that only authorized personnel have access to computers and contained data. Thus, only the data and programs which are authorized to the user are available.

However, this is the weak point of the system. For example, if a stranger knows the employee's credentials he can easily have access to the user's data, and if a SSO is used then extensive opportunities are available to the intruder.

With a well designed password management, establishing the quality, the length and the validity of passwords (Password policy), a high level of security can be achieved.

What resources are available and in what way they can be used is regulated by the communication protocol.

In the most terminal protocols *rdp* or *ica* there is no possibility to (client wise) link connected biometric devices with the terminal session.

## 2 Objective

Secure user identification within the IT structure (mostly in large companies) while reducing administration and user expenditures becomes increasingly important. This is because of increasingly open IT structures (e. g. Web accessibility, wireless, etc.) and the multiplicity of systems and logon to applications or even specific functions. The security and user comfort is increased by securing the user authentication via biometrics,. By combining the **bi-Cube<sup>®</sup> SSO** there is no need for the user to manage (remember) logon data to required applications.

In more and more companies the terminal server technology is introduced. Thus hardware and system management costs are significantly reduced.

The here described solution to the subject **bi-Cube<sup>®</sup> SSO** can be used in the terminal environment (e.g. Citrix).

The goal is to execute the biometric logon via a fat or thin client (also embedded XP).

After a successful logon, all SSO data are provided to the user through the **bi-Cube<sup>®</sup> SSO Client** to his terminal sever. The analysis of data validity is executed by the **bi-Cube<sup>®</sup> SSO Client**. The **bi-Cube<sup>®</sup> SSO Client** communicates with the **bi-Cube<sup>®</sup> Server** and obtains an exact overview of the user's programs and rights. Thus, the user may activate his individual application.

For special critical applications an additional authentication can be demanded prior to the start. This functionality is centrally stored in the system. All currently available additional authentication options of iSM may be used (e.g. the biometric authentication).



Picture 1: Biometric authentication

### 3 Requirement

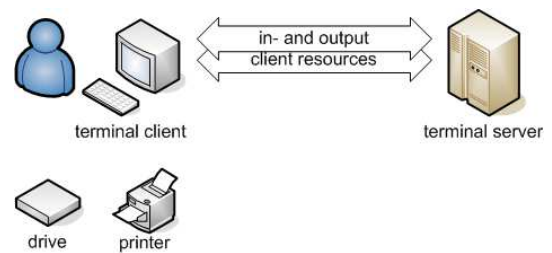
#### Working in the terminal environment

The terminal environment mainly consists of 3 components:

- Terminal server
- Terminal client and
- Communication protocol

The terminal client serves only as the input and output station. All used programs are centrally executed in the terminal server. Also resources of the terminal client can be used within this terminal session.

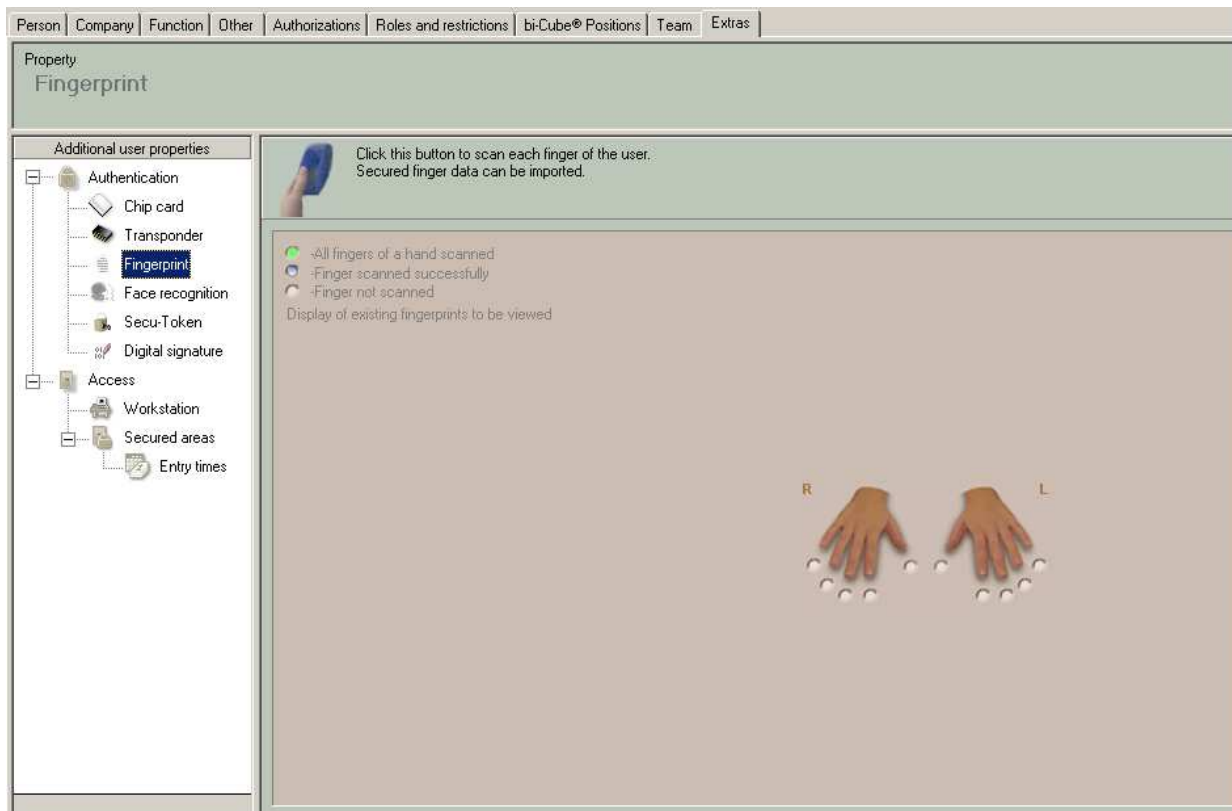
For example, if a user's local computer is connected to a printer, then programs which run on the terminal server can use this printer as local printer. This way, also drives, serial ports and audio resources of clients are used.



## 4 Architecture of the Solution

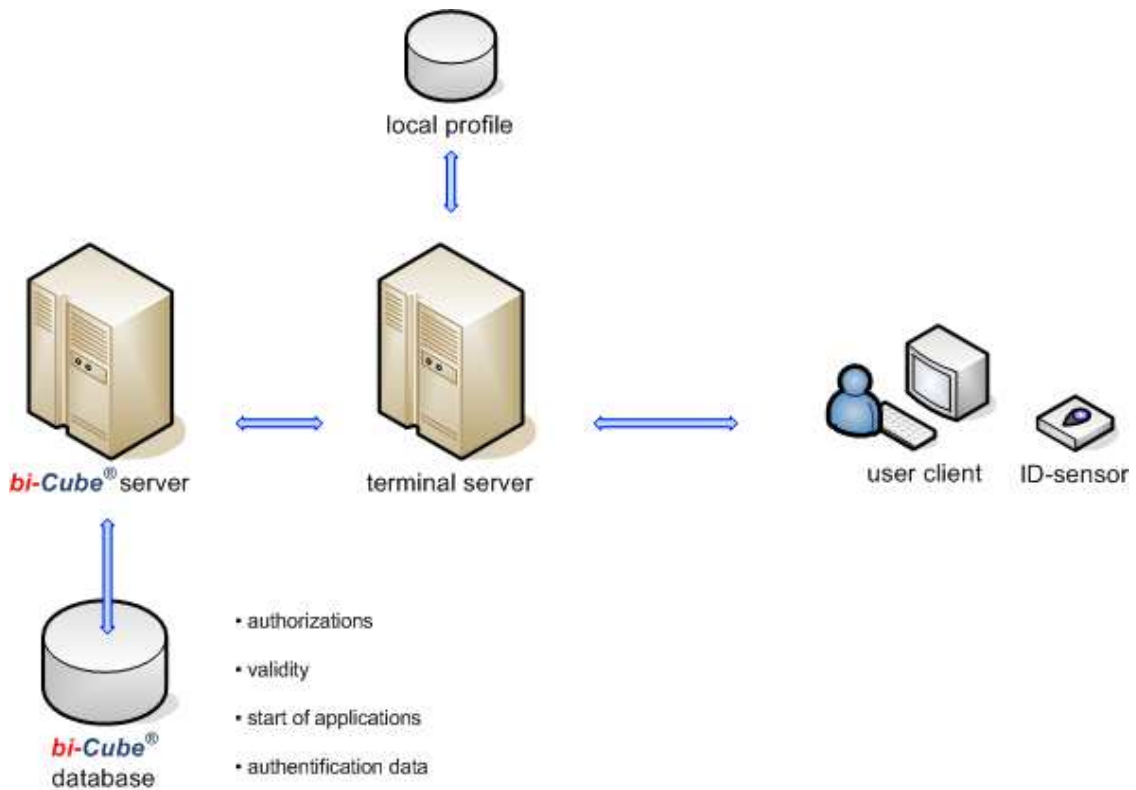
The architecture is based on the basic **bi-Cube<sup>®</sup>** architecture; but only required components are used.

Templates of the user and their logon data, to access the different target systems, are provided via the **bi-Cube<sup>®</sup>** SSO Client and are stored in the central **bi-Cube<sup>®</sup>** database. All data is encrypted with the 3DES method.



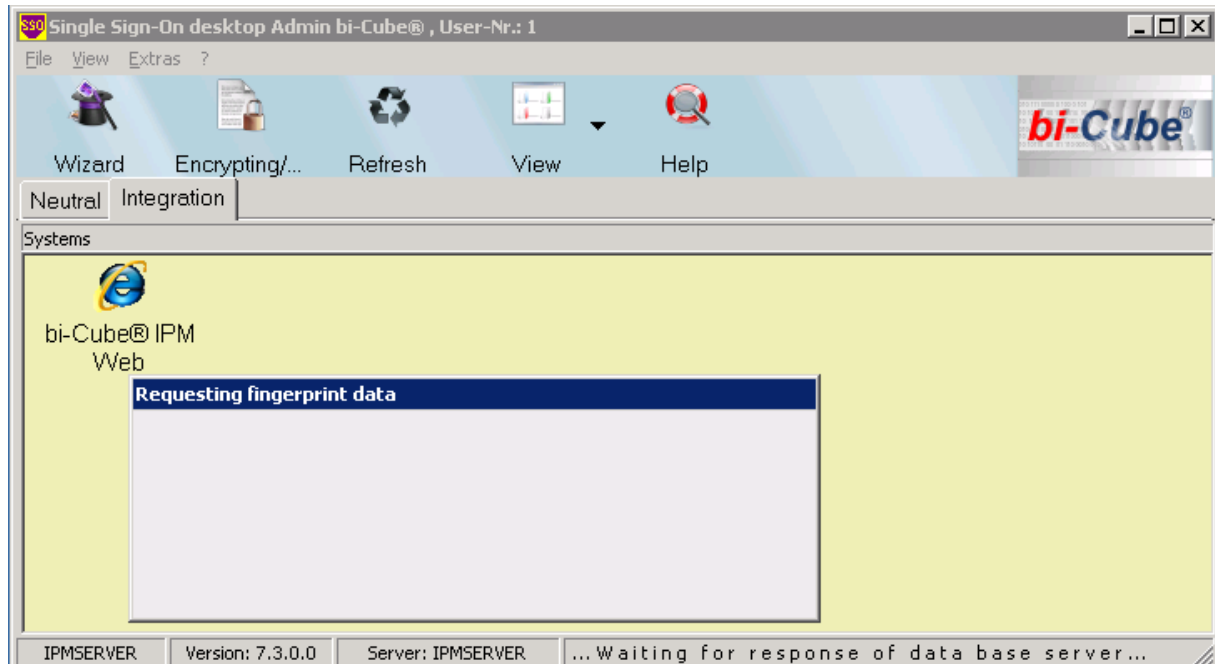
Picture 2: **bi-Cube<sup>®</sup>** User Manager, tab Extras

When requested, the **bi-Cube<sup>®</sup>** server provides all required logon data of all logged on users to the terminal server, or the logon of requesting users.



Picture 3: **bi-Cube<sup>®</sup>** SSO in the Terminal

The so called SAD file (secure access data) is created and encrypted at the **bi-Cube®** server and saved to the terminal server. This file is automatically requested (if so configured) when the user logs on or the system starts. It is also updated when the logon data is changed or authorization changes have been executed. Also, if so configured, an automatic adjustment of the profile can be organized also during a running operation.



**Picture 4:** **bi-Cube®** SSO Client updating the profile and fingerprint data

The correct assignment to the user is executed by a special **bi-Cube®** service at the terminal server. The right SAD file is assigned to the specific user via an IP address of the client.

## 4.1 Biometric Logon to the Terminal Server

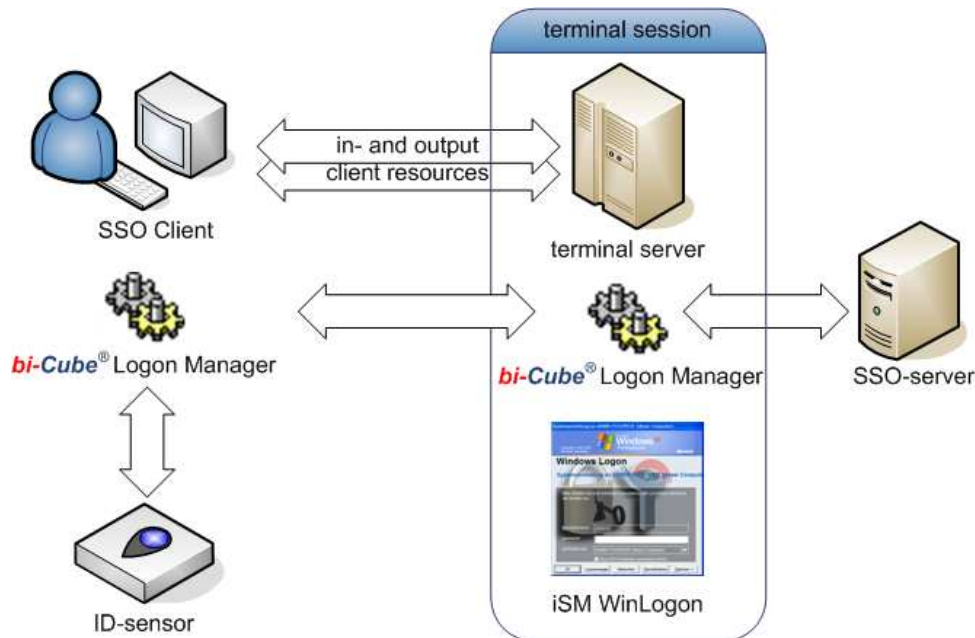
With a special procedure it is possible to logon on to the terminal server via fingerprint. For this, the iSM GINA must be imported before the MS GINA.

This procedure is called GINA Chaining. A special service (*bi-Cube<sup>®</sup>* Logon Manager) must be installed to the Fat-Client or Thin-Client and the terminal server, to enable a biometric logon.

From the *bi-Cube<sup>®</sup>* Server the necessary data for the user's logon to the terminal server is requested by the installed *bi-Cube<sup>®</sup>* Logon Manager (client wise). Verification is executed by the user ID and the fingerprint template.

This process is suggested for all available iSM authentication methods.

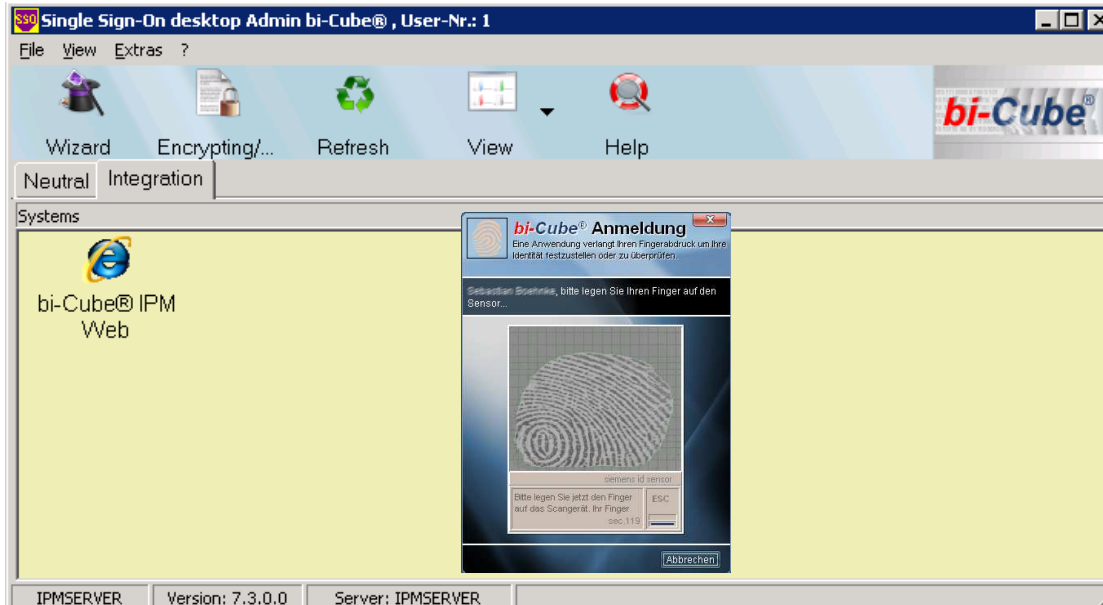
Also, the identification of a user is possible. The number of users is relevant. The size of biometric teams should not be too large since this could cause performance problems. Usually a maximum of 100 users per team is feasible.



Picture 5: *bi-Cube<sup>®</sup>* Logon Manager in the Terminal

#### 4.1.1 Additional Biometric Authentication

For special critical applications an additional authentication is demanded by the SSO-Client prior to the start. To use this special method of additional authentication, it must be so configured at the Object Manager (Objects->System).



**Pictures 6:** *bi-Cube®* SSO Client including the additional biometric authentication

## 5 Advantages

Technologically no change to the terminal protocol, in use, is executed.

Virtually any application can be secured with an additional authentication method, like:

- biometrics (fingerprint)
- memory -/RFID card
- Windows password
- token