

Biometrically user authentication in a Citrix-environment

The situation

The authentication of users at the Windows-Logon represents the first stage of warranty of enterprise security on the desktop-level. By these it is guaranteed, that only entitled persons get entrance to the computer and data. Thus it is ensured that the users get only the data and programs made available, which they are permitted for.

However, the weak point of the system lies exactly here. If an unauthorized person knows the login-data of an employee, he can use unnoticed its entrance and thus its data. If this user in addition uses a SSO, the intruder has extensive possibilities.

By a reasonable password management, that means, definition of the quality, the length, the age of the passwords (password guidelines) as well as the definition of a cyclic change, a high measure at security can be achieved. Simultaneous the danger rises, that users note their passwords to "secret" places or rather the inquiries accumulate at the User-Help-Desk because of the forgotten passwords. A password misusage is also not excluded with a reasonable password management.

The solution

The employment of biometric characteristics, independently of logon-names and passwords, for this reason applies already multiple in the desktop sector.

In a terminal environment e.g. with use of Citrix terminal servers this strategy however is pushed to its borders.

Work in terminal environments

Essentially a terminal environment consists of 3 components:

- Terminalserver
- Terminalclient and
- Communication protocol

At this, the terminal client serves only as in- and output-station. All used programs are central implemented on the terminal server.

Within this terminal meeting also resources of the terminal client can be used.

For example if a user attached a printer at his local computer, programs, which are executed on the terminal server, can use these like a local printer.

In this way also drives, serial connections, Smartcards and audio resources of the clients can be used.

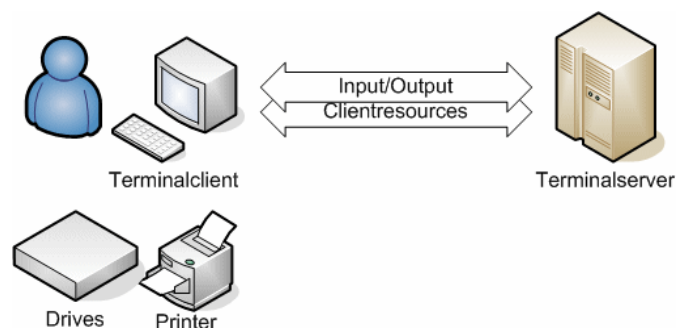


Figure 1 Citrix – Client resources

The problem

Which resources are available and on which way they can be used is regulated by the assigned Communication Protocol.

In the most frequently assigned terminal protocols "rdp" and/or "ica" however there exist no possibility of connecting and using attached biometric devices on client site during a terminal meeting.

The **bi-Cube**® Bio-Transfer-Service

With the solution created by "Institut für System-Management", these problems belong to the past. The **bi-Cube**® Bio ID-Transfers Service permits the use of biometric devices (e.g. the ID –Mouse Professional) and at the same time takes over the transmission of the biometric data from client to the terminal server.

How does it work?

On the terminal server (Citrix) the iSM developed "iSM Windows Logon" is installed.

From this moment on during the "Windows-Logon" the well known "iSM-Gina" is at the user's disposal and can be used to logon at the operating system with fingerprint.

If a user would like to announce to the operating system, the following happens.

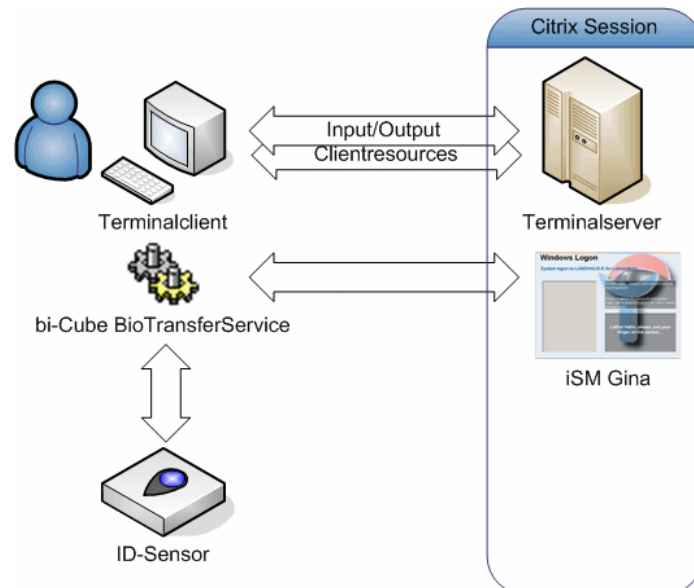


Figure 2 Citrix – iSM Windows-Logon

- The iSM-Gina recognizes the meeting as a terminal server meeting.
- At first it is examined whether or not the user has a valid fingerprint file present. If this is not the case, the iSM Gina requests the fingerprints and dates of registration of the user which are central stored in the **bi-Cube**® Professional.
- The **bi-Cube**® Bio-Transfer-Service receives the instruction from the "iSM-Gina" for scanning the finger and starts the fingerprint sensor (e.g. in the ID Mouse)
- The user put on his finger.
- The fingerprint sensor passes the scanned finger to the **bi-Cube**® Bio-Transfer-Service. This transmits the data to the iSM Gina.
- The iSM-Gina examines the identity of the user by comparison of the transferred fingerprint data with the locally stored data. If the examination is successful, it logs on the user with the data of registration which are locally saved in fingerprint-file.
- The user was successfully announced to the operating system.

The achievable comfort of a Single Sign-On solution by the automatic registration of the user at different applications is simultaneous the largest problem of such a solution.

Once started, the intruder has unhindered entrance to all resources of the employee. Also here the iSM has a solution.

By the use of **bi-Cube® Single Sign-On Professional** it is possible to additionally secure each application with fingerprint.

Thereby the technical problem in a terminal environment is the same as with the Windows-logout and is just as well solved.

How does it work?

On the terminal server, the server components for **SSO Professional** become installed. Since this moment, the SAD-Server is available. This service controls the different user meetings, which parallel runs on the terminal server and processes all inquiries from the SSO to the ZAMServer.

If a user would like to start an application, secured with fingerprint, the following happens:

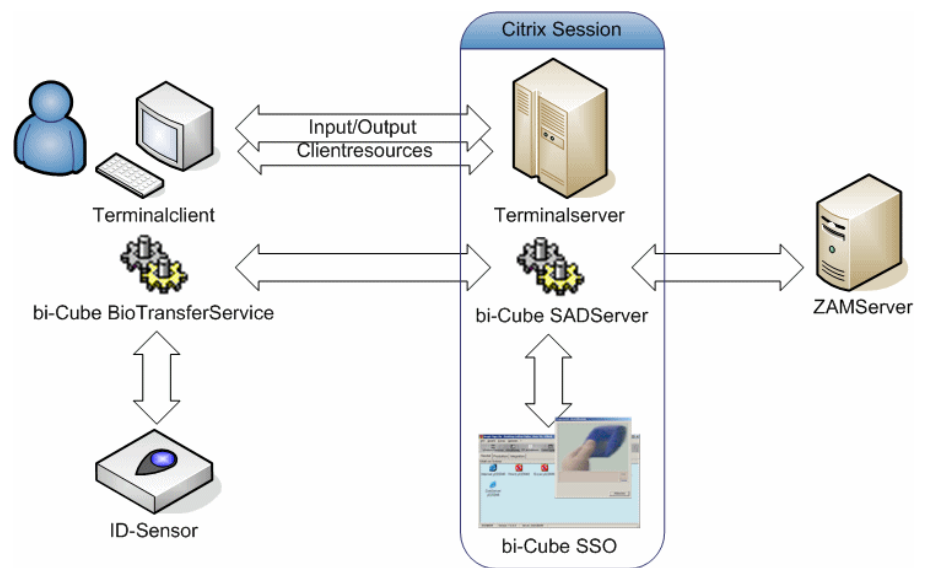


Figure 3 Citrix – **bi-Cube®** SSO

- **bi-Cube® Single Sign-On** recognizes the meeting as a Terminalserver meeting.
- **bi-Cube® SSO** sends the fingerprint requirement to the SADServer, which transfers the instructions for scanning the finger to the **bi-Cube® Bio-Transfer-Service**.
- The fingerprint sensor (e.g. in the ID Mouse) is started and the user put on his finger. The fingerprint sensor passes the scanned fingerprint to the **bi-Cube® Bio-Transfer-Service**. This transmits the data to the **bi-Cube® SADServer**.
- **bi-Cube® SSO** examines the identity of the user by comparison of the transferred fingerprint data with the locally stored data. If the examination is successful, it logs on the user with the data of registration which are saved in the **bi-Cube® SSO** profile.
- The user was successfully announced to the application.

Advantages

Independently of the used protocol happens the communication of the **bi-Cube® Bio ID-Transfer Service** on a separate, free configurable TCP-Port. Thereby, the by iSM developed biometric solutions for use in terminal environment are usable with Microsoft Terminal Server and Citrix Terminal Server. It doesn't take place a technological interference into terminal protocol. The solution for **bi-Cube® SSO** follows the same approach. Because there is no contact to applications which can be secured, practically any application with fingerprint can become secured.