



# **SCB Access™**

## **Single Sign-On**

## **PC Secure Logon**

- *Manage all your passwords*
- *One smart card to access all your applications past & future*
- *Multi-factor authentication*



- *Dramatically increase your security*
- *Save \$150 per year per user*
- *Improve employees' productivity*
- *Enforce regulatory requirements*



# SCB Access™

## What it is. How it works. And why it is necessary for your organization.

SCB Access™ provides a secure token to store all your credentials safely



Strong authentication for computers and networks

Today, there are simply too many passwords for users to remember. Users either try to use the same password for all applications or they write them down, often on “stickies” in plain view. Users get lost and call the help desk repeatedly to gain access. This not only increases security risks and help desk costs, but substantially reduces overall productivity.

A recent study by the SANS Institute and the FBI confirms weak passwords as one of the top ten threats for computer systems. The study found that a third of users’ passwords could be broken in less than five minutes. Password crackers are much more effective today while people are still choosing passwords in the same fashion. Passwords are the weakest link in digital security.

Even though enterprises are implementing password policies that require longer passwords, our human bias for picking easy-to-remember words will continue to make passwords the Achilles heel.

SCB Access™ is a turn-key solution with PC Secure Logon and Single Sign-On applications. A user can access a PC or an application by inserting a smart card and a PIN code. With SCB Access™, user names and passwords are securely encrypted and stored on a smart card. User names and passwords are then submitted automatically to the appropriate applications. SCB Access™ eliminates the burden on users of having to remember, enter, and periodically change many individual passwords, often with different character requirements. Users need to remember only one password to unlock their smart card. All the others can be forgotten; no more need for unsafe “stickies” to remember their passwords. As a result, instead of being distracted from their jobs, users connect to applications easier, faster and more securely, freeing up the time to generate revenue, help customers or drive new business.

By storing all those hard to remember user names and passwords on a smart card or USB key, SCB Access™ allows users to seamlessly access application resources with a single PIN code.

Securing computers and network access with strong authentication has become more than a necessity. Use of antivirus and firewall solutions is no longer an efficient protection against confidential information inner attack or laptop theft.

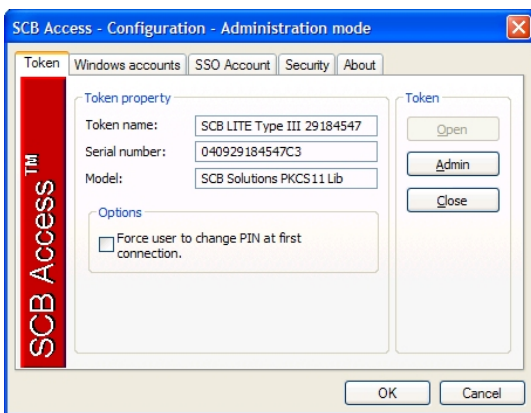
# SCB Access™

## SCB Access™, Corporate Edition

Logon credentials  
stored on security  
tokens



Rapid implementation  
and deployment



SCB Access™, Corporate Edition is designed to provide secure and convenient access for both internal and external applications. SCB Access™ can interface Windows applications, web-based applications or “green screen” applications. SCB Access™ also manages remote authentication through a Citrix session. SCB Access™ does not require enterprise applications to be modified.

### Main features:

- Automated logon and authentication to all
- Automated change of password
- Manage multiple accounts per application
- Manage multiple logon windows per application
- No need for client agents on servers
- Easy to use & supervise (locally or centralized)
- Logon credentials stored on security tokens
- Rapid implementation and deployment
- Easy to use: users sign-on once and all subsequent access is automatic
- Reduces administrative overhead and help desk costs
- Increases user productivity
- Increases PC and network security because of two or three factor requirement
- Designed for Windows 2000, Windows XP & Vista (July 2007)

SCB Access™ offers four different ways to communicate the users' credentials to the targeted applications:

1. Interface with HTML controls through Internet Explorer
2. Interface with the Windows controls in local standard Windows applications
3. Macro and keyboard simulation for applications that don't use standard controls
4. ActiveX for applications that have their own development tools or scripting processes



# SCB Access™

## Benefits

### User friendly



SCB Access™ does not require complex backend integration or custom server agents to function with Windows, web, and mainframe based network resources.

SCB Access™ adds a level of security to existing applications by adding an authentication layer and not by replacing it with a central authentication, avoiding the security problem coming with server-based single sign-on: the “key to the kingdom” problem. If somehow a user is able to breach the security to one application, that won’t give him or her access to other applications.

SCB Access™’s small footprint enables you to deploy it throughout your organization in days, not months.

SCB Access™’s storage of logon credentials on a smart card provides maximum protection against password theft. Since the smart card is protected by a secret code of 4 to 24 digits, it is impossible to gain access within three (3) tries. After three (3) incorrect tries the microprocessor chip locks and can only be accessed through an administrative process.

### Easy for the administrators



SCB Access™ manages the cards or the tokens through PKI/PKCS #11. This standard interface brings multiple benefits:

- The organization is not committed to a given token/card technology
- The same cards/tokens can be used to sign and encrypt emails
- The cards can be used by other PKI-aware applications

SCB Access™ allows you to enforce complex and secure passwords without compromising ease of use. While your network resources will see highly secure text-based passwords, network users will only have to insert their smart cards and enter their PIN codes to authenticate themselves to the card.

### Maximum security

# SCB Access™

## SCB Access™, Advanced Edition Active Directory, Citrix

### Card management with Active Directory



### Active Directory & Terminal Server Edition

With the LDAP/Active Directory option SCB Access™ provides a central database that contains an encrypted mirror copy of every card.

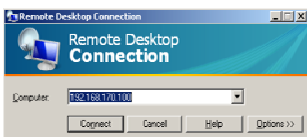
The administrator can re-issue a lost card using the mirror copy.

The administrator can change the card credentials without having the card in hand. The card's credentials are then resynchronized with the LDAP mirror copy after the next logon.

The administrator can also put the card on a hot-list prohibiting any future use of the card.

With the LDAP/Active Directory option, SCB Access™ is a turn key solution which contains all the required components to manage the users and the secure smart cards. No expensive third party card management system is required.

### Multi factor authentication with virtualized applications



### Citrix & Terminal Server Edition

SCB Access™ is the first security product that brings together the convenience of single sign-on on a Virtualized environment with the strong security of 2-factor or 3-factor authentication.

SCB Access runs from a thin client or a regular PC.



## Biometric Authentication

### Maximum security with a 3-factor authentication



### Fastest Bio-Engine on the market

SCB Access™ also manages biometric authentication. Depending of the context, the application can use the biometric authentication alone or, to reach maximum security, the biometric authentication can complete the smart card authentication. In that case, SCB Access™ provides 3-factor authentication:

1. Something you know : PIN
2. Something you have: smart card
3. Something you are: fingerprint

SCB Access™ uses the fingerprint reader Certis “Gull” integrated with the ID3 Bio-Engine.

The Certis reader has a high definition, 500dpi, Pyro-Electric fingerprint sensor. It measures the temperature differential between the sensor pixels that are in contact with the ridges and those not in contact.

Main features of the Certis reader:

- Certis works in every environmental condition: light, climate, humidity.
- It allows enrolling and matching the most difficult fingers: dirty, moist, thin, small, dry, and shivering.
- It has a strong immunity to electrostatic discharges.
- It does not work with severed fingers.
- It is almost impossible to deceive with artificial fingertips.
- It does not leave a residual fingerprint.
- It is maintenance free.
- Its performance does not deteriorate with time.

Performance of the bio-engine:

Biometric performances are measured by the three following rates:

- False Acceptance Rate (FAR),
- False Rejection Rate (FRR) and
- Failure to Enroll (FTE)

With a high security threshold: FAR <0.01% and FRR <0.0027%

With a medium threshold: FAR <0.05% and FRR <0.0008%

With a low threshold: FAR <0.1% and FRR <0.0003%.

The FTE is virtually 0% in any circumstances.

The ID3 bio-engine matches 1 fingerprint in over 2500 users in less than 1 second.

SCB Access™ pays for  
itself in less than  
**1 year**



Passwords are expensive to support. A Meta Group study reveals that, on average, companies with annual revenue of more than \$500 million have more than 75 applications, databases and systems that require authentication. With so many passwords, it is not only a security challenge but also a management problem. Gartner estimates that an average enterprise spends \$150-400 per user per year on password management. A major US bank with more than 100,000 employees estimates that they spend US\$8 million a year managing passwords.

Most security products are only seen as a necessary cost to avoid the consequences of a possible security breach in the future. By facilitating password management, SCB Access™ generates significant savings by dramatically reducing the cost of password management.