



Believe in  
a higher level  
of IT Security.

**SECUDE**  
White Paper

Simple, Secure Enterprise  
Single Sign-On—  
Advantages for Your  
Company



Quote:

*"Release your users from passwords so they can focus on more important issues."  
Norbert Steinhauser*



*Norbert Steinhauser, Vice President Business Management, SECUDE IT Security*



## Table of Contents

<b>Table of Contents</b>	<b>3</b>
<b>1 Introduction</b>	<b>4</b>
<b>2 The Challenges of User Authentication</b>	<b>5</b>
2.1 Already working or still authenticating?	5
2.2 The Password Dilemma	6
<b>3 SECUDE signon</b>	<b>8</b>
3.1 Powerful and Reliable User Authentication	8
3.2 Ease of Use Instead of Endless Authenticating	9
3.3 SECUDE signon Reduces Costs and Increases Productivity	10
3.4 Scalable Security for Individual Security Requirements	11
3.5 Easy Administration and Comprehensive Support	13
<b>4 Conclusion</b>	<b>14</b>
<b>5 Glossary</b>	<b>15</b>
<b>6 About SECUDE</b>	<b>18</b>



## 1 Introduction

**“Passwords cost time, money and are a pain in the neck.”  
Dr. Sachar Paulus, CSO, SAP AG**

User authentication with user name and passwords can simply be reduced to this provocative and simple denominator. And if you add the factor security, passwords are no longer an appropriate solution to secure the access to sensitive company data and IT systems.

And still, this kind of user authentication remains one of the most common. Companies are reluctant to introduce more efficient and powerful authentication methods because they are afraid of complex integration efforts with extraordinary expense. This Whitepaper will show that this is absolutely wrong. It is also meant to be an orientation guide because it describes how the requirements for a reliable and powerful user authentication can be realized efficiently, conveniently, and at a low cost.

The Whitepaper outlines in Chapter 2 the challenges of user authentication. Chapter 3 describes how SECUDE signon simplifies and optimizes the process of user authentication:

- Simple, convenient user access to IT systems with Single Sign-On.
- Increased user productivity through Single Sign-On.
- Password-related help desk requests reduced by up to 95 percent.
- Minimization of costs per password reset.
- Reduced administration efforts.
- Streamlined password management.
- Easy implementation of security policy and guidelines.
- Increased access control.



## 2 The Challenges of User Authentication

### 2.1 Already working or still authenticating?

During a routine day of work, computer users will need to enter a long list of passwords to gain access to their company's various IT resources. For example, the Windows system, the SAP system, the email server, and many other applications each provide their own authentication dialog. Typically, each application requires users to enter a combination of user name and password to identify themselves. Users also need to re-authenticate themselves frequently, for example, when switching between systems or after the system has gone into standby mode.

Unfortunately, this authentication approach is very time-consuming and can significantly reduce actual working time. In addition, there can be annoying delays when a user forgets a password. This happens most commonly after weekends, holidays or sick leave—especially where the company's security policy requires regular password changes, minimum password lengths, and passwords made up of complex combinations of numerical and alphanumeric characters and even combined with different duration of validity as well.

In most companies, forgotten passwords are encountered on a daily basis. Instead of taking it directly to the administrator, however, employees will typically try to access the system using all kinds of probable and improbable combinations so they can actually start to work. If this fails, they will still need to call the help desk for support. More valuable working time is wasted before one of the administrators will have time to look into the problem and then reset the password(s) so that the employee can access relevant data or information.

Gartner assumes that a user will call the company help desk up to 19 times per year, frequently as a result of password issues.<sup>1</sup> If there are several hundred employees, the amount of time and money spent on password resetting adds up very quickly.

---

<sup>1</sup> GARTNER: What Is the Right IT Service Desk Staff Size and Structure?



Moreover forgotten passwords are a burden for the user and the helpdesk at the same time. Inconvenience and a great deal of time are often justified with pretended higher level of security, but unfortunately this is an illusion. User name/password authentication no longer is the adequate protecting of vital company data when it comes to internal or external unauthorized access attempts.

## **2.2 The Password Dilemma**

Combining a user name with a password (single-factor authentication) is still the most common method of user authentication for businesses. Although it is no longer suitable to withstand the more and more sophisticated attacks from external hackers nor to fulfill the growing security requirements for sensitive company data — many businesses are reluctant to give up this seemingly simple authentication method in favor of a more powerful and efficient one.

In today's world of IT, however, it is relatively easy to find out passwords, even for attackers with limited hacking experience. If there is physical access to office workstations, it can be as simple as collecting the post-it notes from the computer monitors. Practice has shown that the more passwords a user has to remember, the more likely he will write them down somewhere.

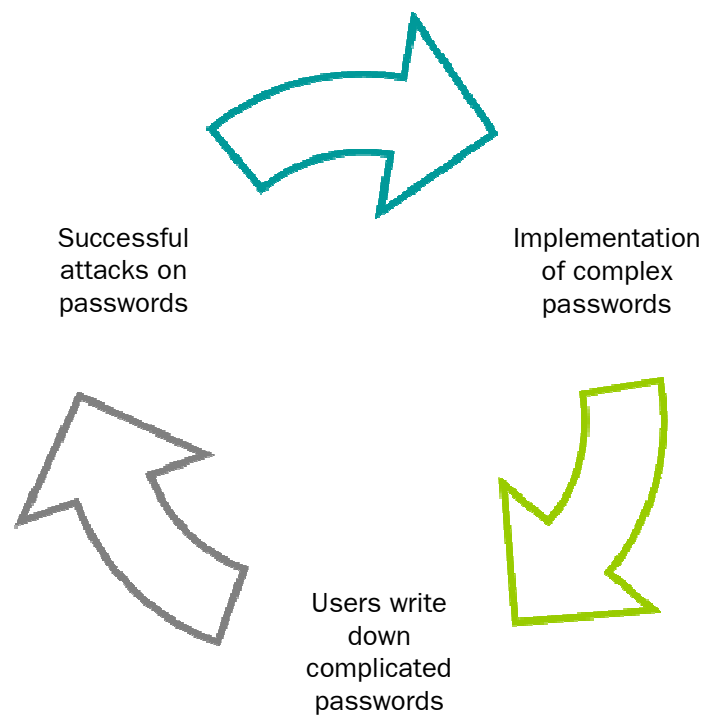
Another successful approach is to simply analyze the user's personal traits. The so-called "social engineering methods" are based on the fact that a user - confronted with a large number of passwords - usually tends to choose simple passwords that he will never or very rarely change. If there are several authentication procedures to be performed, he will often use the same user name/password combination which he can easily remember.

This makes it relatively easy for attackers to guess the passwords; typically, a password is a reference to the user's personal life, such as the partner's or child's name or even birthday. Innocent small talk in the staff lounge or on the telephone is often enough to reveal an employee's vital personal details.

The internet is a popular source of information to find out more about people and to guess potential passwords. In addition, the internet also offers numerous tools and manuals on how to bypass and crack passwords. In the wrong hands, even commercial password recovery tools can easily be used to obtain passwords. That is why



passwords are not really security obstacles anymore in today's sophisticated world of information sharing.



The current problems with password-based user authentication can only be addressed by implementing a more user-friendly and powerful method of authentication.

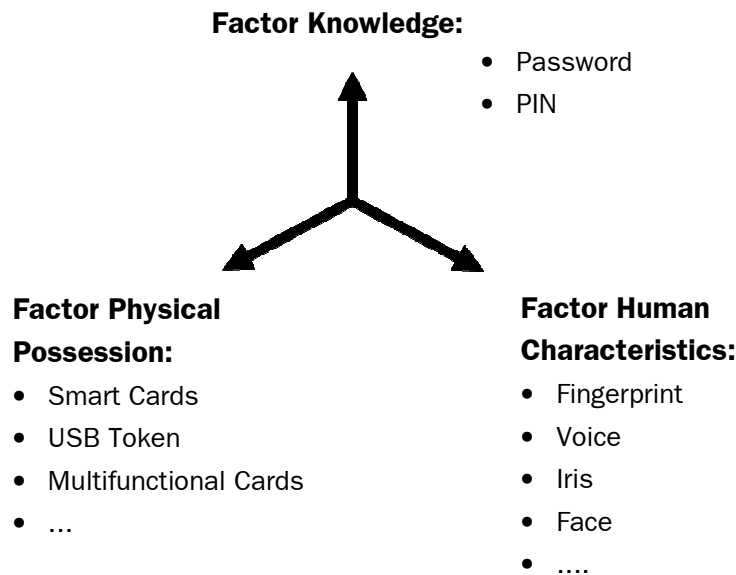


### 3 SECUDE signon

To prevent hacker attacks, user authentication must be secure and absolutely reliable. At the same time, it should be user-friendly so that the users will easily accept it. SECUDE signon liberates both the users and the administrators from having to deal with password problems. With SECUDE signon, businesses will be able to easily move to a more powerful and reliable method of user authentication.

#### 3.1 Powerful and Reliable User Authentication

Efficient user authentication is achieved through a combination of multiple authentication factors.



SECUDE signon extends single-factor password authentication (“Factor Knowledge”) with a second factor (“Physical Possession”) to produce a so called Two Factor method of authentication. This increases the authentication’s reliability dramatically.



The user passwords are now stored on a smart card or a USB token. These security devices are able to perform complex encryption algorithms and secure the passwords against third-party access, even when the smart card or token is lost or stolen.

Another advantage of two-factor authentication is that users notice very quickly that their smart card or token is lost or stolen—in contrast to compromised or hacked passwords. The smart cards or tokens employed for authentication can further be used to safely store private keys and certificates, for example, for secure email or digital signatures and other security relevant information of users.

Smart cards and tokens are small, easy to use, and greatly simplify access to terminals, networks, and applications. For authentication the user only needs a smart card or a USB token (the “Physical Possession” factor) and the PIN that unlocks the card or token (the “Knowledge” factor). Successful authentication is only possible when both factors are given.

## **3.2 Ease of Use Instead of Endless Authenticating**

Instead of having to memorize numerous passwords, users now only need to remember one single PIN for the SECUDE signon smart card or USB token. The employees are relieved and can focus on their properly workload instead. Help desk staff and IT administrators are also relieved, as the number of password-related queries and issues is significantly reduced.

SECUDE signon optionally also provides Single Sign-On (SSO). Single Sign On means that a user only has to sign on only once to the system to access all data, applications and services he is authorized for—without requiring to repeat authentications over and over again. Whenever an application or system environment requires a new user authentication, SSO automatically signs on the user in the background without requiring any further (manual) input.

Authentication via smart cards or tokens is not limited to specific workstations and accommodates “free seating” in the workplace. Smart card users can sign on at all computers equipped with a card reader. If USB tokens are used for authentication, card readers are not required at all, as a USB token incorporates the functions of a smart card with those of a card reader. Tokens can be used for any computer with a USB port.



Giving users the option of having the same security device to authenticate themselves on different computers is a definite advantage in workplaces where users need to shift between locations during their workday.

Furthermore this kind of authentication enables organization to define passwords as long and as complex as necessary and to update them as often as required without ever involving the users. With SECUDE signon absolutely no user interaction is required for the generation and changing of passwords.

With such a range of functions, SECUDE signon offers a maximum of convenience. This is very important in terms of user acceptance; many employees and in particular the management are not willing to engage in complex technologies, even if this technology improves the company's IT security level. SECUDE signon, however, never meets with any user resistance, as it offers users a much simpler alternative to passwords and greatly speeds up the authentication process. In fact, user resonance to this solution has been positive throughout thanks to its simple, easy-to-use conception. Users don't even need to be trained in how to work with SECUDE signon—acceptance and satisfaction are guaranteed.

### **3.3 SECUDE signon Reduces Costs and Increases Productivity**

With username/password authentication, password issues occur on a daily basis. According to Gartner, a user contacts the help desk up to 19 times per year. In the average 3.8 times of these contacts are related to password issues.<sup>2</sup> According to Forrester, a password reset costs about \$38, which means that the password-related costs add up very quickly. Even with a more conservative estimate of a password reset cost of €10–€15, the total sum is still staggering.

#### Sample calculation:

3.8 help desk calls x 200 employees = 760 calls to be processed

760 calls at €15 ea. = **€11,400** per year just for the resetting of passwords

---

<sup>2</sup> GARTNER: What Is the Right IT Service Desk Staff Size and Structure?

With a larger company consisting of 3,000 employees, the costs associated with password resetting shoot up to **€171,000** per year. Reason enough to adopt a more cost-efficient and reliable authentication method!

SECUDE signon takes the administrative burden off users by introducing Single Sign-On, and at the same time helps businesses to cut down on their costs. According to IDC, Single Sign-On reduces the amount of password-related help desk queries by 95 percent.

With such a significant reduction in password problems, employees and IT administrators alike can focus on more important tasks than password resetting. This is not just a matter of workload efficiency and company expenditures—seeing that IT departments are very often chronically understaffed and hacker attacks are always on the rise, it means there is more time for analyzing data from intrusion detection or intrusion prevention systems, implementing counteractive strategies, and improving the overall security of the company's IT environment.

### **3.4 Scalable Security for Individual Security Requirements**

SECUDE signon offers Single Sign-On and powerful authentication for practically every application. It supports conventional authentication with Windows Credentials (username/password) as well as certificate-based authentication with digital certificates. The USB token or smart card is used to store passwords as well as other personal user data, such as certificates and private keys for the encryption of documents, digital signatures and secure email communications. All stored data is protected against unauthorized third-party access.

Thanks to PC/SC, PKCS#11 and Microsoft CSP support, you can smoothly integrate SECUDE signon into virtually any PKI environment. A wide range of smart cards and USB tokens from different manufacturers are supported. The PKCS#11 interface works with smart cards from manufacturers such as Siemens, Giesecke & Devrient, and Aladdin, as well as JavaCards compliant with the GlobalPlatform Specifications such as GemPlus, IBM, Axalto/Schlumberger, and Oberthur. A great variety of the USB tokens supplied by these manufacturers are also compatible. Additionally, SECUDE signon supports a wide range of PC/SC-based card readers.



Smart cards satisfy today's sophisticated security requirements and meet virtually all the security needs of companies and businesses of any scale. This includes security devices that comply with standard security requirements, as well as highly secure smart cards that are certified according to ITSEC E4 and offer protection against even the most sophisticated illegal decryption attempts. SECUDE signon also works with smart cards that have RSA keys up to a length of 2048-bit. A key length of 2048 bits offers a high level of long-term security; even with processor capabilities evolving rapidly, these keys will remain completely unbreakable in the foreseeable future. 2048-bit keys are therefore especially recommended for companies that need to protect their data against unauthorized third-party access over long periods of time (for example, in pharmaceutical R&D). This makes SECUDE signon a suitable option for medium and large-scale companies with top-level security requirements.

Biometric authentication solutions are becoming increasingly popular. On the one hand, the procurement costs for biometric solutions have decreased. On the other hand the error rate of, e.g., fingerprint recognition has improved significantly. With SECUDE signon, businesses can select their security devices according to their own requirements, and even retain their existing cards and tokens – the protection of their investments is assured. Even future generations of PKCS#11-based security devices can easily be integrated without further efforts. This is why the solution is fully future-proof.

And finally, the use of multifunctional cards lets you extend your security devices' functional range well beyond the scope of secure authentication and data encryption/decryption. For example, you can not only store personal data such as passwords and private keys on multifunctional cards and multifunctional USB- but also parameters for access control to buildings or particular departments. If issued with the user's photo and name, a smart card can also double as an employee ID card. By providing miscellaneous other functions such as logging the working time or even the user's cafeteria account balance, multifunctional cards can greatly streamline, simplify, and speed up daily processes for employees and administration alike. That is why the use of multifunctional cards and tokens does not only make sense from the security point-of-view but in particular from the cost effective point-of-view.

As more and more businesses are adopting application server computing (ASC), SECUDE signon fully supports Citrix environments. In ASC systems, user-accessed business applications are stored on centralized Citrix Presentation Servers. The advantage of such a system structure is that the user terminals do not have any

software applications installed that need to be maintained. Authentication processes are directly transferred to the client terminal and the user's smart card. This means that applications installed on the Presentation Server do not need to be modified at all for authentication with SECUDE signon. Instead, a smooth transition to two-factor authentication can easily be realized.

### **3.5 Easy Administration and Comprehensive Support**

SECUDE signon can simply be integrated into an existing IT infrastructure and features an easy and timesaving administration throughout its entire lifecycle. When business security requirements are revised, the administrative effort involved in updating authentications is minor and requires only very little manual input.

According to the company's security policy SECUDE signon allows the passwords to be as long and as complex as required. Passwords can also be changed whenever necessary without requiring user input because passwords are centrally generated and allocated without any user interference. This way, even the most demanding security requirements are facilitated in a very user-friendly manner.

Comprehensive support functions ensure that in cases where users forgot their smart card or token or lost their security device or PIN can quickly resume productive work without lots of administrative efforts.

SECUDE signon also supports businesses in their compliance efforts. Organizations are committed by national and international data protection laws and industry regulations and guidelines to dealing accurately with personnel and customer data and to providing a reliable protection of such data against unauthorized third-party access. It ensures e.g. SOX compliance by providing safe access to systems. This is a functionality that every auditor will definitely check.

With several hundreds of thousands of users around the world, SECUDE signon offers businesses a reliable and practice-proven security solution.



## 4 Conclusion

SECUDE signon provides organizations with a reliable and powerful two-factor authentication that ensures system integrity at all times. The implementation of Single Sign-On dramatically reduces password-related issues, reducing costs while increasing employee productivity. SECUDE signon is a straightforward and convenient application that also ensures a very fast user acceptance. Due to comprehensive support of all common authentication standards, SECUDE signon can quickly be integrated into an IT infrastructure. The wide range of functionalities and supported security devices of SECUDE signon lets organizations implement tailor-made solutions for their specific IT security demands and requirements.

## 5 Glossary

### **Authentication**

A predefined procedure, such as the entry of a PIN or the matching of a fingerprint, to verify a person's identity and his/her authorization to access a computer system and/or the data stored on it.

### **Verification**

Verification is used to check whether a file or message indeed originates from the person or organization that claims to have sent it.

### **CSP**

**Cryptographic Service Provider:** A software module that provides smooth access of Microsoft CryptoAPI-based applications to cryptographic security devices such as smart cards. This is Microsoft's alternative to PKCS#11.

### **GlobalPlatform Specifications**

A standard published by an international specifications board representing a wide range of manufacturers. The aim of GlobalPlatform specifications is to provide easy communication between different devices.

### **ITSEC E4**

**Information Technique System Evaluation Criteria (ITSEC):** A European standard for the evaluation and certification of software and computer systems, specifically their functionality and reliability in terms of data integrity and computer security. In Germany, ITSEC certification is issued by BSI (Federal Office for Information Security).



### **JavaCard**

A card equipped with a microprocessor that runs a simplified version of Java as its operating system. Due to a special software updater, JavaCards can be loaded with new software at any time.

### **(Chip) Card Reader / Card Reader Units**

Card readers supply power to chip cards (smart cards) and enable the communication with the computer.

### **PC/SC**

Personal Computer / Smart Card (PC/SC): A specification designed for the integration of chip cards and card readers. It ensures that the computer and the smart card (card reader) can easily communicate.

### **PIN**

Personal Identification Number: PINs are usually employed for smart cards (as well as bank cards and credit cards). A PIN can be a combination of numerical and alphanumeric code that identifies the cardholder (with a card or a token).

### **PKCS#11**

Public Key Cryptography Standard: A platform-independent interface standard developed by RSA. It is used to provide access to cryptographic devices such as smart cards or tokens.

### **Security Device**

A smart card or USB token that stores encrypted personal user data such as passwords, private keys, and certificates to protect them from unauthorized third-party access.



### **SSO / Single Sign-On**

Single Sign-On provides an authentication process whereby the user only needs to identify himself once during startup with only one single PIN. All other sign-ons are performed automatically in the background without any further user input.

### **Smart Card**

A plastic card with a built-in microchip that may contain embedded integrated circuits, memory, or a microprocessor. The card's microprocessor can be individually programmed, which means that functional scope of a smart card is limited only by the available memory and the processor's limitations. Microprocessors are frequently used to perform cryptographic operations to protect the stored data from unauthorized third-party access.

### **Cryptography / Encryption**

A process where plaintext is converted into a secret code using an encryption algorithm. Encryption employs one or several keys to encode the data. The algorithms for encryption and decryption do not need to be the same.



## 6 About SECUDE

SECUDE IT Security GmbH is a market leader in the areas of authentication & authorization, encryption, data integrity and the management of digital identities, delivering a higher level of IT Security to organizations around the world. We offer solutions in single signon, role-based access control, and the security of documents, applications and transactions.

SECUDE IT Security GmbH is a member of [IT\\_SEC SWISS AG](#) and was formed in 1996 from a partnership between SAP AG and the Fraunhofer Institute in Darmstadt, Germany. This partnership resulted in the Secure Network Communication (SNC) module for SAP AG. SECUDE is headquartered in Zurich, Switzerland, and has offices in the USA, Germany, Netherlands, Spain and United Arab Emirates.

For further information, please consult [www.secude.com](http://www.secude.com).

SECUDE IT Security GmbH  
Rautistrasse 75  
8048 Zurich  
Switzerland

Ph.: +41 (0)44 404 82 00  
Fax: +41 (0) 44 404 82 01  
[info@secude.com](mailto:info@secude.com)