



Believe in  
a higher level  
of  
IT Security

SECUDE  
Business  
White Paper

How to Improve  
Business Results  
through Secure  
Single Sign-on to  
SAP

## Executive Summary

CIOs and IT managers face tremendous demands today to reduce IT costs, improve user productivity and create an IT environment that complies with best practices for IT risk management and regulations. Efficient and secure user access to SAP is a specific challenge in today's powerful but also complex and heterogeneous SAP environments.

Furthermore, unencrypted communication between users' workstations and the backend SAP servers is a significant vulnerability to your SAP environment. This can put the availability of your SAP environment, the confidential data inside your SAP systems, and your entire business activity at risk. It can have a negative impact on your customers. And it also exposes your company and its management to potential compliance issues with regulations and data privacy laws.

But the two challenges can be solved with a secure single sign-on solution to SAP, which has been proven to save significant costs. SAP offers an optional feature to implement secure single sign-on between SAP client software and SAP servers, called Secure Network Communications (SNC). With this feature activated, users don't have to enter user name and password multiple times, when they connect to the multiple SAP servers within the distributed SAP landscape. Nor do they have to change passwords frequently, and they also don't need to call the help desk to reset passwords. Yet, the security of the SAP environment is not compromised. In fact, with this feature in use, the security of the SAP environment is significantly improved – confidentiality, integrity, and proof of origin of any communication within the distributed SAP landscape are ensured. But it's important to select the right solution that enables the efficient use of SNC in your environment.

This whitepaper shows how to improve your company's business results by improving user and IT productivity, and by avoiding this specific IT security risk within your SAP environment. You will get insights into the security situation around communication in distributed SAP environments, you'll get an overview of Secure Network Communications (SNC), and you will find selection criteria for 3rd-party solutions that enable the use of SNC. Last but not least, you will learn how strong protection can be implemented efficiently and with the flexibility you need to adjust to your company's specific situation.

## The Business Case for Single Sign-On for SAP

Single Sign-On (SSO) improves usability and productivity of SAP users by providing or leveraging a single authentication service (for example the Windows authentication) that allows users to logon once and then to transparently access all SAP applications on different servers. No further logon is being required until after the user logs out. Alternatively, customers can define policies that define after what time interval a user has to re-authenticate.

Cost savings of single sign-on come from four different aspects:

- Improved SAP user productivity  
Once users are authenticated, they no longer need to enter user name or password, when they log into SAP. This saves time and also improves the user experience. Both have an impact on user productivity.
- Reduced password administration effort  
Best practices for password management require users to change passwords on a regular basis – typically every 90 days. And many companies introduce strict rules about how passwords need to be formed. If you have multiple SAP systems, your SAP users may have to do this multiple times, leading to a significant effort. Users don't have to worry about these administrative changes anymore, if single sign-on is used.
- Reduced effort for recovering passwords  
Studies have shown that in average users try for 7 minutes to search or remember passwords that they have forgotten. Some users have a fix set of password and they try different variations. Others have documented the password somewhere and they try to find it. If they are unsuccessful, then they call the IT help desk.

- Reduced number of calls to IT help desk due to forgotten passwords  
If users forget their SAP password, they have to make IT help desk calls for password resets. Studies have shown that password reset requests can make up to 70% of a company's help desk calls. Single sign-on solutions avoid these types of help desk calls completely.

## ROI of Single Sign-on

Single Sign-on investments typically have a very quick return on investment.

For an environment with 1000 users, the cost savings can easily add up to multiple 100'000 \$ per year. Most cost savings come from the improvement in user productivity. With a reduction from an average of 6 logins per day to 1 login, the rate of incorrect logins and subsequent efforts to recover the password or to contact the help desk to reset the password is reduced significantly. Estimations point to more than 100 \$ savings per month through improved user productivity.

The cost savings for the IT help desk are also significant. With an estimated 35% of help desk calls being related to password reset, the IT help desk can expect about 700 calls per month for a 1000 user environment. Cost savings for avoiding these kinds of calls can easily amount to multiple 10'000 \$ per year. Plus, the IT team no longer needs to maintain and coordinate password policies across different SAP systems and versions.

## The Business Case for IT Security Risk Management for your ERP Software

### Risk Management - An Essential Business Activity

Risk management is essential for any serious business activity, whether implicitly or formalized through processes and risk management frameworks. For many companies, formalized risk management is mandatory, because of laws and regulations. But even without these legal drivers, it is essential to the success of every business to understand and manage its risks – whether originating in IT or any other area – in order to minimize the potential negative impact to the business.

If risks are not managed, a company's valuation will likely be affected at some point in time. IT security risks are one example: according to analyst studies, companies with publicized IT security breaches experienced an above-average loss in valuation. This is not only caused by direct cost for managing the security breach (estimations point to at least 25-50\$ per customer record), but also by the negative impact on the company's reputation.

### Attack Patterns are Changing - Moving to ERP Systems

Change is inherent to the nature of IT security risk management. Once a vulnerability of an IT solution has been detected and tools have been developed to remove the vulnerability or to prevent any use of it, potential attackers are likely to move on to a new approach for their attacks, looking for vulnerabilities which are less protected. Consequently, IT security measures need to adapt too.

With network security, e-mail security, and basic user & role management being covered more thoroughly by many companies, attacks shift to other levels of the IT infrastructure. For example to the business application level, with targets like the SAP environment. The fact that SAP servers are typically in the company-internal network, inside the firewall, are no remedy here. There are many different statistics about the relative importance of external versus internal attacks, but nearly all of the studies agree that internal attacks are a serious problem for every large company. So, there is a concrete risk that your SAP systems will be a target for attack.

Many successful companies rely on SAP business software to automate their business processes, making the SAP system the central IT solution to store company-critical information and automate business processes. For many businesses, a problem with the SAP environment or a leak of company-confidential data would result in a significant loss of revenue and profit. Insufficient protection for SAP

applications can also cause compliance problems with data privacy regulations and overall risk management regulations.

## IT Security Features Available within SAP

SAP supports their customers in the challenge to secure their business-critical applications by providing a wealth of security features in the SAP software. SAP solutions are built from the ground up to ensure the highest levels of security in the most sensitive environments. SAP follows rigorous security standards in the design and development of all its solutions, and SAP application developers receive extensive security training. Often there are even multiple options, giving customers the choice to implement the approach that fits best their specific risk situation.

Some examples of security features within SAP include:

- Various authentication mechanisms, including standard X.509 digital certificates, smart cards, ticketing, and username and password authentication.
- Powerful authorization via user roles and authorization objects, allowing for both coarse and fine-grain authorization management
- Options to digitally sign documents created within SAP
- Security audit logs that record events such as log-on attempts and transaction starts

However, many companies do not fully utilize these powerful security features, either because they are not aware of specific vulnerabilities, or because the effort to initially configure and maintain a proper configuration is too high to justify the investment. That leaves many companies with default configurations, which are of course well known to attackers.

## The Underestimated Risk to your Business: Unencrypted Remote Access to SAP

One of the areas, where your company-critical information assets and business processes in SAP are potentially at risk, is the area of remote user access.

SAP is a distributed application, where client software (e.g. SAPGUI for Windows, or MS Internet Explorer) installed on a user's workstation is used to access the central SAP server remotely over the company's network. Users need to authenticate themselves when accessing SAP. By default this is done via SAP user name and password, which is a relatively weak authentication mechanism. Communication between SAP client software and SAP server should be secure. By default, however, SAP uses unencrypted communication, which allows potential company-internal attackers to get access to usernames and passwords by listening on the network. This can expose the complete SAP system, if a person is able to get access to this information for a user with extended authorizations in the SAP system.

Information about this vulnerability is publicly accessible on the Internet.

SAP offers an option to strongly protect communication between clients and servers, called Secure Network Communications (SNC). With this feature activated, confidentiality, integrity, and proof of origin are ensured. But still too many companies are not leveraging this feature to protect their SAP system, even though it can be implemented quickly and efficiently, and it is being successfully used by many companies.

## Secure Network Communications

SNC is a software layer in the SAP system architecture that enables the use of stronger authentication, encryption and single sign-on mechanism. For secure server-to-server communication, SAP delivers this capability for free. For secure client access and single sign-on, companies need to purchase an additional software module from external partners.

By default, SAP systems include basic security measures, which include the SAP authorization concept and user authentication based on passwords. With SNC, SAP customers can extend SAP system security beyond these basic measures to include the additional protection offered by stronger authentication methods, by encryption and by single sign-on.

Advantages of using SNC, according to SAP, include:

- SNC provides application-level, end-to-end security.
- SNC secures all communications between two SNC-protected components (for example, between SAPGUI and an SAP application server).
- Companies can implement additional security features that the SAP system does not directly provide (e.g. single sign-on or the use of strong authentication measures, like 2-factor authentication).
- Companies can determine their specific single sign-on and security requirements and then choose a vendor of choice for their specific needs.

## How to Select a Solution for Secure Single Sign-on to SAP

When selecting a solution for secure single sign-on to SAP, companies should consider multiple factors. The most important ones include:

### End-to-End Coverage

SAP business software solutions have become more and more powerful. Compared to a few years ago, SAP now offers more applications, for example Customer Relationship Management (CRM), Supply Chain Management (SCM). SAP has introduced new technology components with SAP NetWeaver, including a full J2EE-compliant application server. SAP now also enables the assembly of new business solutions based on the concepts of Service Oriented Architecture (SOA). With all these additional capabilities, the SAP landscape turns more complex.

Any solution for secure single sign-on to SAP should enable companies to protect their entire SAP landscape end-to-end. This means the solution should support:

- all versions of all SAP applications
- all user access methods to these SAP applications (i.e. all user interface technologies like SAP GUI, web browser, ...)
- all OS platforms

This avoids unnecessary costs for implementing and maintaining multiple solutions. It will also increase user acceptance, because they only have to interact with one solution.

Ideally, the solution should even be extensible to other non-SAP enterprise applications. Business processes in any company typically involve not only SAP applications but also depend on data or processes from non-SAP enterprise applications, and it is desirable to have just one single sign-on solution for all involved applications.

End-to-end coverage also implies that the entire communication flow – from the user's desktop to the backend SAP server – is encrypted, and not just parts of the communication flow.

## Enterprise Operations

SAP business software solutions touch almost every business activity of companies today. When we talk about secure single sign-on to SAP, this typically applies to thousands or ten thousands of users in large corporations. A solution needs to be able to address environments of this size, and also needs to support other operational requirements that enterprises typically have for their solutions:

- The solution needs to be highly available
- The solution needs to provide interfaces for backup, 24x7 monitoring and operations, etc.
- The solution needs to be able to scale up to many thousands of users accessing SAP. The configuration of such an environment needs to be done efficiently.
- The solution should be able to support the company-internal standards defined for efficient operations and integration without problems (e.g. directory server standards, authentication standards, etc.)
- The solution should be able to easily integrate in related IT solutions, for example existing identity management solutions, security event management solutions, application management solutions, or desktop software distribution solutions.

## Flexibility

The solution needs to be flexible enough to allow companies to implement their specific authentication policies. Many companies want to choose different levels of authentication, based on:

- The type of SAP application (e.g. specific SAP servers with HR data may need to be stronger protected than other SAP servers)
- The user type (some companies want to use a stronger authentication mechanism (2-factor authentication) for specific SAP user roles, e.g. SAP administrators)

## SAP Certification

Any solution that integrates and thus interacts with the business-critical SAP environment should have certifications by SAP that ensure the solution is using the SAP interfaces properly and thus is not a risk to ongoing operations of the SAP environment.

## Total Cost of Ownership (TCO)

IT budgets are not increasing. Thus, CIOs and CISOs need to find efficient solutions to their IT challenges. Therefore, they look for solutions that have not only low purchase costs but more importantly, that are low in maintenance costs. Besides providing efficient administration tools, the solution should also integrate into a company's existing processes around software distribution, configuration, etc.

## Investment Protection

Investment protection for the solution is another important factor in the evaluation of solutions. For some customers, requirements may change over the course of time, and the solution should be able to grow with the company's security and authentication roadmap. For example, a customer that has started out with a fast implementation of a solution based on Windows authentication may later on want to move to 2-factor authentication via one-time password token (e.g. from RSA or Secure Computing) and PIN to increase security.

The solution needs to be able to adjust to these changes, and help protect previous investments by customers.

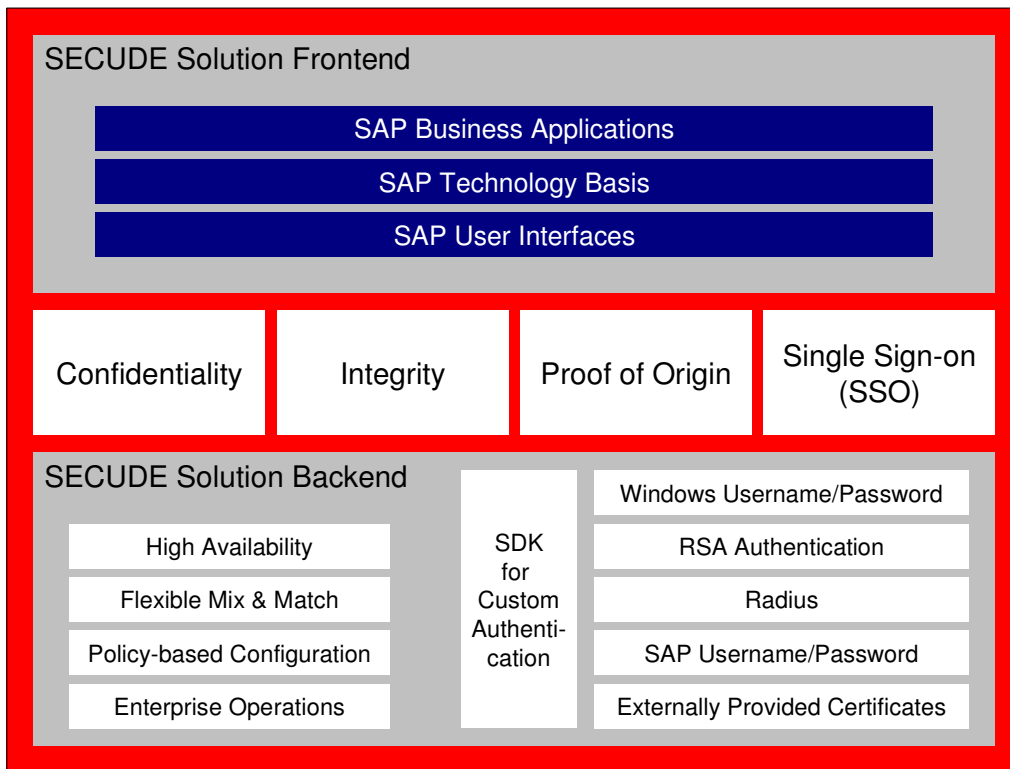
## Vendor Viability

For critical solutions like SAP, companies are looking for providers that are reliable, trustworthy, and that have focus and specific expertise on SAP technology.

## SECUDE Solution Summary

### Solutions Description

SECUDE provides an easy-to-implement and easy-to-use solution for secure single sign-on to SAP, based on SAP's Secure Network Communications (SNC) layer. With its market-leading capabilities, the solution is able to fulfill the selection criteria listed above.



*SECUDE solution for secure single sign-on to SAP*

The SECUDE solution for secure single sign-on to SAP consists of two major functional modules: the frontend portion handles the single sign-on and secure communication from the SAP User Interfaces (SAPGUI, Web Browser, etc.) to the various SAP systems. The backend portion of the solution is used for the authentication of users (selected ones can be implemented, also in a mix & match approach) and for the administration of the entire environment. The authentication service can be configured to be highly available. The specific selection of which authentication service to use for which user can be configured centrally for a large number of users via a policy-based approach. The backend portion also handles operational requirements like backup, logging, etc.

SECUDE provides complete solutions to its world-wide customers. Besides software this includes world-class consulting and support services.

### Value Proposition

First and foremost, SECUDE solutions reduce IT security risks from unencrypted user access to SAP. SECUDE helps to ensure confidentiality, integrity, and proof of origin of the communication between SAP

users and the backend SAP servers. It also helps to ensure availability of your SAP environment and performance according to your users' expectations, enabling a proper execution of business processes.

With SECUDE software, you can build a solution for your entire SAP landscape, using authentication mechanisms of your choice and need.

Companies can save significant implementation costs, because the SECUDE solution does not require a PKI, and thus the efforts for installing and maintaining a company-wide PKI solution are saved. SECUDE provides a customized, SAP-specific certificate management server – based on standard technology used in almost every company. It is extremely easy to install, highly available, and requires virtually zero maintenance effort. Certificates are securely transferred to users' workstations using a standards-based protocol. If companies have a company-wide PKI solution, it can be leveraged, and they want to move to a PKI solution at a later time, the investment is protected.

Through the single sign-on capabilities, which come with the SECUDE solution, you can significantly improve user productivity (users only have to authenticate once – no more repeated typing of user name and password, and no more password changes), and you can reduce IT costs by avoiding help desk calls about lost passwords. For one large US Company that uses the SECUDE solution for secure single sign-on, the savings add up to multiple hundred thousands of dollars.

SECUDE solutions can also be seamlessly integrated in existing workflows, for example in an Identity Management workflow for user provisioning.

## Why SECUDE?

For more than 10 years, SECUDE has been successfully delivering solutions for secure single sign-on to SAP. Our long history in this area and our unique relationship to SAP – the company was founded in 1996 out of a partnership between SAP AG and Fraunhofer Institute in Darmstadt, Germany – is representative of the unique expertise in the area of SAP security. SECUDE has been instrumental in the development of the SNC technology. SECUDE has also been a founding member of the SAP Global Security Alliance, and has been the first company with a SAP-certified SNC solution.

SECUDE software has been successfully implemented and is currently in use in many enterprises of any size and from various industries throughout the world. For more information about customer references, please visit [www.secude.com](http://www.secude.com).

The capabilities of our solution are unique in the industry. No other solution for secure single sign-on to SAP provides the level of security, flexibility, and manageability that SECUDE solutions offer, giving you a choice what authentication mechanism you want to use for different users and different SAP applications. SECUDE solutions also offer the broadest support of SAP versions and platforms, mostly at day 1 of general availability from SAP. All that is implemented based on a trusted infrastructure that requires almost no maintenance, once installed and configured.

SECUDE offers the only solution that can be used with SAPCryptolib, a security library that SAP provides for free to encrypt server-to-server communication. This means less effort to install new software on the SAP server, and more consistency in the SAP environment.

Last but not least, SECUDE offers complete solutions to our customers, including software, consulting and world-class support services. We can help you secure your entire SAP environment, starting from disk encryption to proper user role definition. Our consulting organization hosts some of the leading SAP Security experts in the world.

## For More Information

SECUDE's industry-leading security technology portfolio combined with SAP's industry-leading business software suite makes our alliance the single source for integrated, certified solutions that are tailored to the customers' needs.

Together, SAP and SECUDE offer an end-to-end solution for enabling enterprises of any size to securely operate their SAP environment while maintaining a consistent cost structure.

Through our collaborative approach to developing and delivering solutions, we enable customers to build businesses that are agile, yet still secure — thus effectively reducing business risk.

For further information, please contact your local SECUDE representative or visit [www.secude.com/sap](http://www.secude.com/sap).

### **SECUDE International AG**

Alpenquai 28b  
6005 Lucerne / Switzerland  
Phone: +41 (0)41 560 6100  
Fax: +41 (0) 44 404 82 01  
[info@secude.com](mailto:info@secude.com)

### **SECUDE IT Security, LLC**

380 Sundown Drive  
Dawsonville, GA 30534  
Phone: +1 (706) 216-8609  
[info@usa.secude.com](mailto:info@usa.secude.com)

You also have the option to:

Register for the SECUDE newsletter: [www.secude.com/htm/321/en/Newsletter\\_abonnieren.htm](http://www.secude.com/htm/321/en/Newsletter_abonnieren.htm)

Download SECUDE whitepapers: [www.secude.com/htm/406/en/mySECUDE\\_White\\_Papers\\_Welcome.htm](http://www.secude.com/htm/406/en/mySECUDE_White_Papers_Welcome.htm)

Learn about other SECUDE solutions: [www.secude.com/htm/575/en/Solutions.htm](http://www.secude.com/htm/575/en/Solutions.htm)

## About SECUDE

**SECUDE**, the end-to-end IT security solution company, is a market leader in user authentication and authorization technology, data integrity and encryption solutions, and digital identity management systems, with a solution focus on SAP. Our mission is to deliver a higher level of IT security to organizations around the world. Passionate about quality in all that we do, we provide advanced single sign-on and role-based access control solutions, plus enterprise-wide security for documents, applications and transactions, to an internationally respected client base.

**SECUDE** is a member of iT\_SEC SWISS AG and was founded in 1996 out of a partnership between SAP AG and Fraunhofer Institute in Darmstadt, Germany. This partnership resulted in the Secure Network Communications (SNC) module for SAP AG. Headquartered in Lucerne, Switzerland, we have a worldwide customer and partner base, and offices in the USA, Germany, the Netherlands, Spain and the United Arab Emirates.

Copyright SECUDE International AG 2007

SAP\_bw8\_en\_200709

SECUDE is a registered trademark of iT\_SEC SWISS AG.  
Microsoft is a registered trademark of the Microsoft Corporation.  
Other product and company names mentioned herein serve for clarification purposes and may be trademarks of their respective owners.