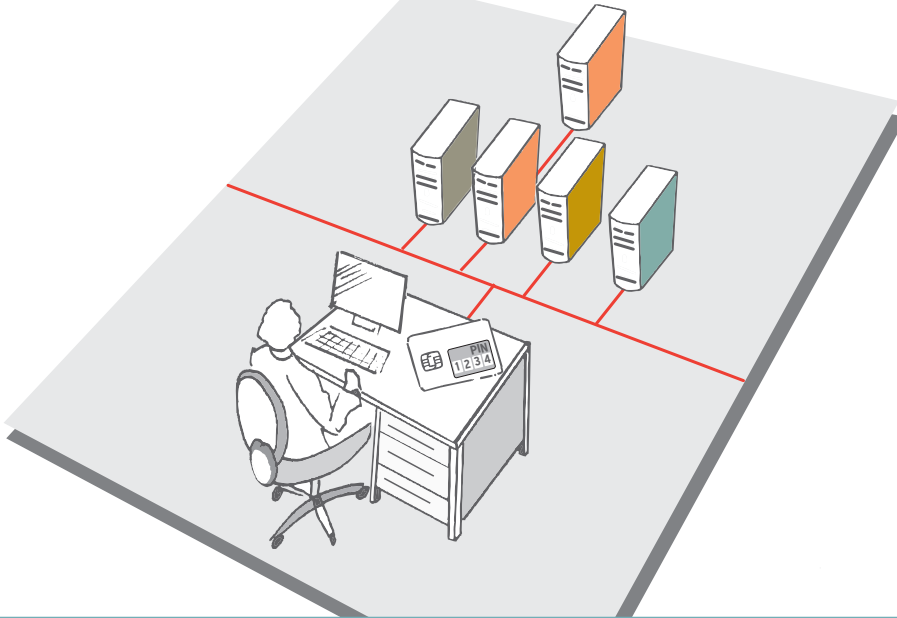


## Single Sign On



### Secure password administration and Single Sign On (SSO)

Complex, multi-step login processes with different user names and password combinations give employees an unnecessarily hard time and do not make companies any safer. Experience has shown that users, out of sheer convenience, mostly use rather obvious passwords, such as the name of their spouse, their children, or pet. Passwords like these are very easy to attack and present a major security risk. However, even the introduction of company-wide password restrictions cannot close this security gap. Therefore, passwords remain an important risk factor for corporate security. This is why many companies, in their password policies, require employees to use difficult passwords, i.e., passwords with up to 8 charac-

ters including numbers and symbols. Passwords like these are hard to remember. Monitoring has shown that despite all warnings, difficult passwords are mostly written down. There are hardly any workstations that do not have hidden password lists containing up to 10 or even more passwords – which are usually very easy to find. The hiding places of choice are underneath the desk pad, in the top drawer, or written down on the calendar. In the case of a targeted attack, unauthorized persons could not only access the data on the respective workstation, but could also get into the corporate network because most PCs are interconnected these days. The solution to this security risk is a Single Sign On system, which both supports conventional (user name and password) and credentials-based identification processes. Combining it with chip cards or

USB tokens facilitates the hassle-free and scalable migration from weak to strong corporate authentication processes in any corporate environment.

### Portability to ensure security

Single Sign On is based on chip cards and personal passwords that are stored locally on the chip card, thus ensuring maximum security. All user profiles are managed centrally on a server and can be accessed anytime at any given workstation. Choosing workstations without any constraints or limitations (Free Seating) has thus become a reality. In addition, it is quick and easy to change users (Fast User Switching). As soon as a user signs off from a workstation by removing his or her chip card, a new user can work on the same workstation by using his or her own card. If desired, passwords may be generated and changed auto-

- High user acceptance and user productivity
- Full Return on Investment (ROI) within a short period of time
- Easy installation and administration
- Easy integration into existing infrastructure thanks to its scalable and distributed architecture
- No need to change directories such as the Active Directory
- Integrating new applications is intuitive and quick
- Comes with various application profiles
- Supports both conventional and highly secure credential-based authentication processes
- Supports most chip cards and USB tokens
- Fast User Switching with Shared Desktop
- Screen saver is activated automatically after the card/token has been removed to prevent unauthorized access
- High availability / system stability / out-of-the box scalability



matically without any user interaction. The bottom line for all chosen application is "maximum security."

### **Security with cost-effectiveness**

Single Sign On is very well received by users. An additional benefit is that it increases productivity and efficiency in any corporate environment. SSO means no more searching for lost passwords, which helps save valuable time and, ultimately, money. Help desk requests will decrease significantly because helpdesk employees predominantly assist users with password problems. Thanks to innovative card administration solutions, cards are available more quickly and easier than before. The help desk assistant is available for quick and straightforward solutions to any problem, either offline or online, right at the user's workstation. In view of all these savings, full Return on Investment (ROI) is reached within a very short period of time.

### **Standards for high interoperability**

Since our Single Sign On solution supports various chip cards, USB tokens, and chip card readers for PC/SC, PKCS#11, and Microsoft CSP, it effortlessly integrates into the chosen PKI environment.

### **Single Sign On at a glance**

IDpendant's SSO package is a comprehensive kit that includes support services and allows for easy-to-use authentication processes with cards/

tokens and PINs on any given system. The major benefit for users is that they only need to authenticate themselves on the security system once and will then automatically be logged on to all other applications such as SAP, Lotus Notes, etc. as well as all networks.

### **Professional installation and training**

This standards-based solution consists of client software, latest-generation card readers and chip cards to ensure highly secure authentication. There are no hidden extra costs. Quite the contrary is true: on-site installation including all travel expenses and incidental expenses as well as training on the new security system are all part of the package. This makes IDpendant's Single Sign On solution the perfect first step towards corporate Identity & Access Management.

IDpendant GmbH  
Edisonstrasse 3  
D-85716 Unterschleissheim/Munich

Phone +49 89 3700 110-0  
Fax +49 89 3700 110-10  
info@idpendant.com

[www.idpendant.com](http://www.idpendant.com)