



Single Sign On: Just What the Doctor Ordered for the Health Care Industry

Versatile solutions for employee IDs make everybody's lives easier

Today, all experts agree on one thing: sophisticated information technology is the key to the future of the health care industry. Swift access to data and secure IT systems play an increasingly important role, second only to the provision of the very best medical services to patients.

In order to limit access to certain areas to authorized personnel, many hospitals already use contactless cards, which, held in front of a card reading device, give access to the authorized individuals. Oftentimes, the same cards are used to pay for food and beverages in the hospital's cafeteria.

Many people would like to see these existing cards used for additional functions, especially access to IT systems ("logi-

cal access"). Single Sign On (SSO) is on top of everybody's wish list, since it would make a dream come true: it would make the almost unmanageable amount of passwords a thing of the past.

Single Sign On: farewell to passwords

With Single Sign On, users will only have to remember one single PIN – all personal passwords are stored centrally and are completely secure. Until now, users often had to remember numerous passwords, which led them to choose very obvious words such as their children's names or the name of their pet. For security reasons, many hospitals now require users to select more complex passwords. However, users tend to write

these passwords down, thus creating a security risk. Other people forget them and ask the helpdesk to reset the password, which results in substantial costs. The so-called "strong authentication" requires users to both have the card and to know the PIN, thereby ensuring a high degree of data security.

The good news for all those favoring this solution: thanks to standard products, SSO solutions can be seamlessly integrated into the existing infrastructure within just a few days while keeping the costs low. In addition, this solution is scalable and can be adapted to new requirements at any given time. A large variety of options is available: the gamut runs from basic options with user ID and PINs and existing IDs to biometric solutions and highly secure, contactless or contact cryptographic cards or USB tokens. IDpendant offers Single Sign On solutions by manufacturers who meet hospitals' special requirements for strong authentication, especially since the Federal Data Protec-

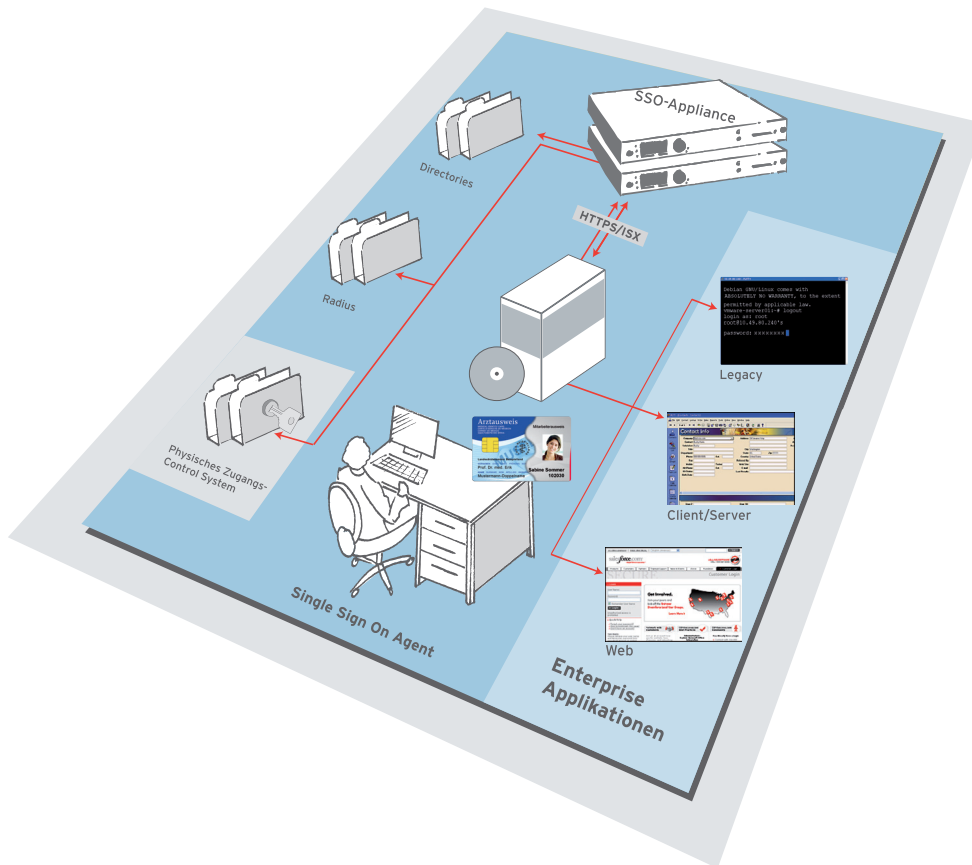
tion Act has been amended to mandate even higher data security. Hospital-specific requirements include the need to log on to systems in sterile environments, mostly operating rooms, to which access is highly restricted. For such cases, SSO can be configured to require the user to place the card on the reader without having to enter the PIN.

When using chip cards for IT system logon, two applications are especially attractive for the health care industry because they keep up with the fast-paced routine in hospitals: Session Roaming and Multidesktop.

Session Roaming: when duty calls, the session comes along

Session Roaming provides for maximum flexibility and mobility in hospitals. When a doctor is working on a PC at a specific ward, but is urgently called away to another ward, all he or she has to do is pull the card from the card reading device and insert it into the reading device at the other ward to continue the "old" session on





the PC in the new ward. The idea is the same for contactless cards, just that the cards need to be placed in front of the reading device and then removed. In both cases, merely the PIN needs to be entered. If a biometric solution has been chosen, the user needs to scan his or her fingerprint. SSO, used in conjunction with a Citrix environment, makes the so-called "traveling user" a reality, providing substantial advantages for everybody involved in the process.

Multidesktop: new user, personal desktop

In hospitals, an average of five people share a PC. Since doctors are authorized to use different applications than the nursing staff, everybody has his or her own user profile associated with the corresponding access rights. Due to the fast-paced environment, changing from one user to the next must be done swiftly. However, until now, this process had been tedious and time-consuming, because one user had to log out and the next had to log on. With Multidesktop solu-

tions, this process takes just a few seconds: for instance, whenever a doctor working at the PC, prescribing drugs or reviewing patient files, has to leave her workstation, all she has to do is remove her card from the card reading device. Her session will stay active in the background, while the PC will remain locked until the next person logs on to the system using his or her own card and PIN. Now, if a nurse uses the same PC, she will see her own desktop and she will be able to use all the applications she has access rights for. If the doctor returns, all

she has to do is insert her own card (or hold a contactless one in front of the reading device), after which she will see her own desktop with her access rights, which will allow her to continue working where she had stopped earlier.

In a nutshell: Multidesktop dramatically increases efficiency in hectic working environments and simplifies processes.

Employee IDs with cryptochip: a panacea for all needs

The introduction of cards with cryptographic chips allows for a large range

of additional functions, adapted to meet the users' need of mobility and high data protection: these applications include secure access to BlackBerry and other mobile devices through secure VPN access, encrypted laptops, encrypted directories, encrypted e-mails, digital signatures, etc. To use these functions, digital certificates on the cryptographic cards are required. These cards can be managed with a highly

sophisticated card management system, which adapts with pinpoint accuracy to existing processes and procedures in the hospital. This Card Management System is easy to use and integrates quickly into the existing IT infrastructure. Using the corresponding interface and workflows, the card management system can be connected to the access management system, with the substantial benefit that all card

functions can be centrally managed. This is an easy way to upgrade existing employee IDs to multifunctional IDs.

Whichever solution you choose, one thing is for certain: a high level of security will be in place.

Your benefits at a glance:

- SSO works with existing contact or contactless employee IDs as well as with USB tokens and cryptographic cards
- Integrates seamlessly into the existing infrastructure and is cost-efficient thanks to the use of standard products. Requires no special development, no proprietary system
- Innovative solution that meets hospital-specific needs: for instance, SSO can be implemented for accessing systems in sterile environments without the need for PINs
- Fully meets increased level of security as mandated by the amended Federal Data Protection Act
- Scalable solution, including highly secure solutions with digital certificates
- Multidesktop function: allows several people to work on one workstation; users can access applications they have access rights for in a matter of seconds
- Session Roaming: Effortless switching from one PC to another in a different ward - the session is "taken along". New: now also available with tokens
- SSO functions can be added to existing employee IDs, turning them into multifunctional cards
- Easy installation and administration
- SSO can be implemented in both PC and Citrix environments
- The wizard makes it easier and faster than ever to incorporate new applications

IDpendant GmbH
Edisonstrasse 3
D-85716 Unterschleissheim/Munich

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