



## Single Sign On – Die beste Medizin fürs Gesundheitswesen

## Vielfältige Lösungen mit Mitarbeiterausweisen entlasten alle Beteiligten

Alle Expertinnen und Experten sind sich einig: Modernste IT-Technologie ist der Schlüssel für die Zukunft im Gesundheitswesen. Abgesehen von der optimalen Versorgung der Patientinnen und Patienten werden in Krankenhäusern der rasche Zugriff auf Daten und sichere IT-Systeme immer wichtiger.

Um jeweils nur den berechtigten Personen Zutritt zu den entsprechenden Bereichen zu gewährleisten, verwenden bereits viele Krankenhäuser Kontaktloskarten, die vor ein Lesegerät gehalten werden und somit dem berechtigten Personal die richtige Tür öffnen. Die gleichen Karten werden oft auch für die Bezahlung in der Kantine eingesetzt.

Vielfach wird der Wunsch geäußert, diese bereits

im Einsatz befindlichen Karten auch für weitere Funktionen zu verwenden, insbesondere den Zugriff auf IT-Systeme („logical access“). Ganz oben auf der Wunschliste steht hier Single Sign On (SSO), wodurch ein oft langgehegter Wunsch Realität wird: Die beinahe unüberschaubare Flut an Passwörtern gehört mit SSO der Vergangenheit an.

### Single Sign On: nie wieder Passwörter

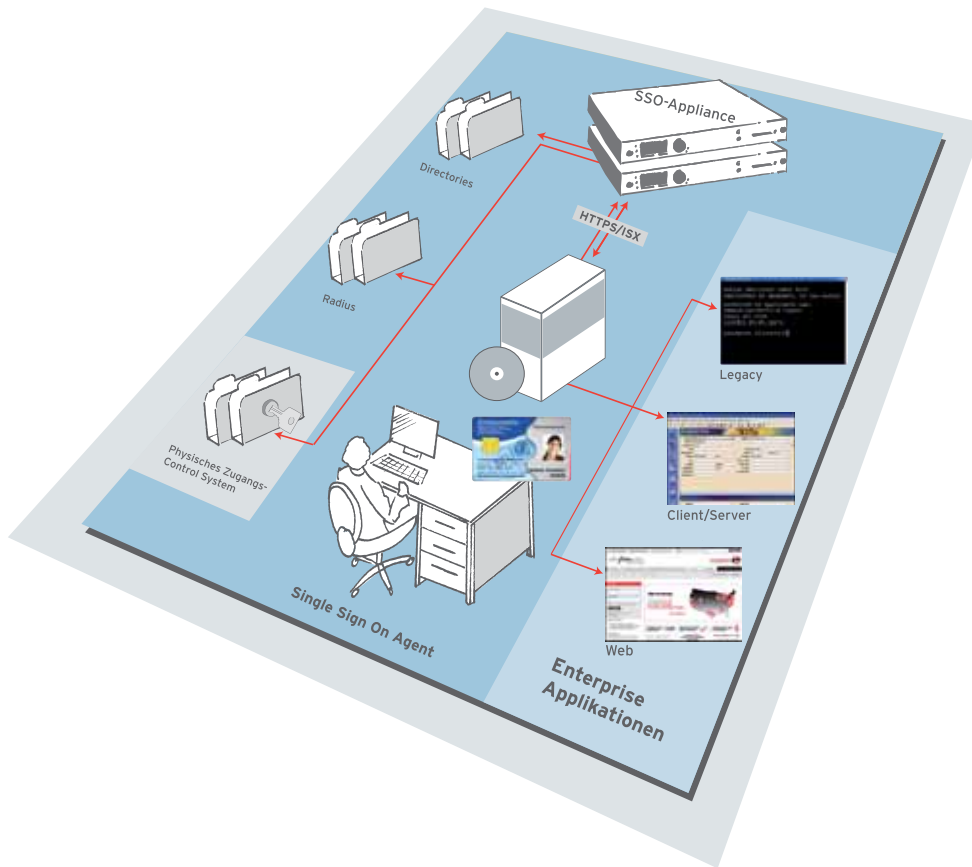
Bei Single Sign On müssen sich die Anwenderinnen und Anwender nur noch eine einzige PIN merken – alle persönlichen Geheimelemente werden dezentral und absolut sicher gespeichert. Bisher mussten sich Benutzerinnen und Benutzer oft zahlreiche Passwörter merken und

wählten dabei oft sehr naheliegende Geheimwörter wie den Namen der Kinder oder des Haustiers. Aus Sicherheitsgründen verlangen viele Krankenhäuser mittlerweile die Verwendung komplizierterer Passwörter. Diese werden aber häufig notiert – was zu einem Sicherheitsrisiko führt –, aber auch oft vergessen, wodurch erhebliche Kosten beim Helpdesk für die Rücksetzung entstehen. Die so genannte „starke Authentisierung“ verlangt, dass die Benutzerin oder der Benutzer sowohl über die Karte verfügt als auch die PIN weiß, womit hohe Datensicherheit garantiert ist. Die gute Nachricht für alle, die sich diese Lösung wünschen: SSO-Lösungen sind binnen weniger Tage und dank Standardprodukten zu überschaubaren Kosten umsetzbar und fügen sich nahtlos in die bestehende Infrastruktur ein. Dazu ist die Lösung skalierbar und kann jederzeit an neue Anforderungen angepasst werden. Die Palette ist breit: Von einer Minimalvariante mit User-ID und PIN über be-

stehende Ausweise bis hin zu Biometrie-Lösungen oder hochsicheren, kontaktlosen oder kontaktbehafteten Kryptokarten oder USB Token ist alles möglich. IDpendant bietet Single-Sign-On-Produkte von Herstellern an, die ganz besonders die speziellen Anforderungen von Krankenhäusern erfüllen, insbesondere nach hoher Sicherheit beim Datenschutz, wie seit der Verschärfung des Bundesdatenschutzgesetzes gefordert. Zu den besonderen Anforderungen in Krankenhäusern gehört auch die Anmeldung an Systeme in sterilen Umgebungen, also vor allem OPs, deren Zutritt stark eingeschränkt ist. Die SSO-Lösung kann dort so konfiguriert werden, dass keine PIN eingegeben, sondern lediglich die Karte aufgelegt werden muss.

Beim Einsatz von Chipkarten zur Anmeldung an IT-Systemen sind im Gesundheitswesen zwei Anwendungen besonders interessant, weil sie dem schnelllebigen Alltag im Krankenhaus gerecht werden: Session Roaming und Multidesktop.





**Session Roaming: Die Arbeit ruft, die Session kommt mit**

Session Roaming sorgt für maximale Flexibilität und Mobilität im Krankenhaus. Arbeitet eine Ärztin oder ein Arzt am PC, wird aber dringend an eine andere Station gerufen, muss sie bzw. er einfach die Karte aus dem Kartenleser ziehen und sie in der anderen Station in das dortige Lesegerät einstecken – und schon ist die „alte“ Session am PC der neuen Station verfügbar. Analog funktioniert es natürlich auch mit Kontaktloskarten, die vors Lesegerät

gelegt bzw. entfernt werden. Da wie dort muss lediglich die PIN eingegeben oder, bei biometrischen Lösungen, der Fingerprint abgegeben werden. Durch SSO in Verbindung mit einer Citrix-Umgebung wird der so genannte „Traveling User“ zur Realität – mit entscheidenden Vorteilen für alle Beteiligten.

**Multidesktop: neuer User, persönlicher Desktop**

In Krankenhäusern ist es üblich, dass sich im Schnitt fünf Personen einen PC teilen. Da Ärztinnen und Ärzte für an-

dere Anwendungen berechtigt sind als das Pflegepersonal, verwendet jeder einen eigenen Rechteprofil. Das hohe Arbeitstempo erfordert aber den raschen Wechsel von einem Benutzer zum nächsten. Hier musste bisher mühsam und zeitraubend der eine User ausgeloggt und der nächste eingeloggt werden. Mit der Multidesktop-Lösung geht dieser Wechsel in Sekundenbruchteilen: Arbeitet beispielsweise eine Ärztin am PC, verschreibt Medikamente oder studiert eine Krankenakte und muss den Arbeitsplatz

verlassen, muss sie nur ihre Karte aus dem Lesegerät entfernen. Ihre Session bleibt im Hintergrund offen, während der PC gesperrt bleibt, bis sich die nächste Person mit ihrer eigenen Karte und PIN am System anmeldet. Wenn also nun eine Krankenschwester denselben PC verwendet, erscheint ihr eigener Desktop und ermöglicht ihr den Zugriff auf alle Anwendungen, für sie berechtigt ist. Kehrt die Ärztin wieder zurück, steckt sie wiederum ihre Karte ein (oder hält eine kontaktlose vors Lesegerät), erhält ihren Desktop mit

ihren Berechtigungen und arbeitet exakt dort weiter, wo sie aufgehört hat. Sie sehen: Multidesktop sorgt für deutlich gesteigerte Effizienz im hektischen Alltag und vereinfacht die Abläufe.

**Mitarbeiterausweise mit Kryptochip: das Nonplusultra für alle Bedürfnisse**

Durch die Einführung von Kryptochipkarten kann eine enorme Bandbreite von Zusatzfunktionen ge-

nutzt werden, wodurch dem Bedürfnis nach Mobilität und hohem Datenschutz Rechnung getragen wird: Zu diesen Anwendungsmöglichkeiten gehören der sichere VPN-Zugriff über Blackberrys und andere mobile Geräte, verschlüsselte Notebooks, verschlüsselte Verzeichnisse, verschlüsselte E-Mails, digitale Signaturen etc. Für all diese Funktionen sind digitale Zertifikate auf den Kryptokarten notwendig. Für die Verwaltung dieser Kar-

ten steht ein hochintelligentes Card Management System zur Verfügung, das sich punktgenau an bestehende Prozesse und Abläufe in Krankenhäusern anpassen lässt. Das Card Management System ist einfach zu bedienen und rasch in die bestehende IT-Infrastruktur zu integrieren. Dank entsprechender Schnittstellen und Workflows kann eine Anbindung an das Zutrittsmanagement erfolgen, wodurch alle Funktionen der Karte zen-

tral verwaltet werden können. So werden bestehende Mitarbeiterausweise zu multifunktionalen Ausweisen aufgewertet. Damit gilt im Krankenhaus in jedem Fall: Sicherheitsstufe sehr hoch.

**Die Vorteile auf einen Blick:**

- SSO funktioniert mit bestehenden kontaktlosen oder kontaktbehafteten Mitarbeiterausweisen genauso wie mit USB Token oder Kryptokarten
- Nahtlose Integration in bestehende Infrastruktur, kostengünstige Lösung dank Verwendung von Standardprodukten. Keine Sonderentwicklung notwendig, kein proprietäres System
- Erfüllt erstmals die besonderen Anforderungen von Krankenhäusern: z.B. Lösungen für sterile Arbeitsräume, wo keine PIN eingegeben werden kann, sind problemlos möglich
- Trägt gestiegenen Datenschutz-Anforderungen gemäß novelliertem Bundesdatenschutzgesetz voll und ganz Rechnung
- Skalierbare Lösung bis hin zu hochsicheren Lösungen mit digitalen Zertifikaten
- Multidesktop-Funktion: Macht eine Arbeitsstation für mehrere Personen nutzbar; jeder User greift mit dem eigenen Rechteprofil in Sekundenschnelle auf die entsprechenden Applikationen zu
- Session Roaming: Wechsel zwischen PCs in unterschiedlichen Stationen problemlos möglich – Session wird „mitgenommen“. Erstmals auch mit Tokens verwendbar
- Bestehende Mitarbeiterausweise können um die SSO-Funktionen erweitert werden und werden so zu Multifunktionskarten
- Einfache Installation und Administration
- SSO ist sowohl in PC- als auch in Citrix-Umgebungen implementierbar
- Der Wizard macht die Einbindung neuer Applikationen unübertroffen einfach und schnell

IDpendant GmbH  
Edisonstraße 3  
D-85716 Unterschleißheim/München

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