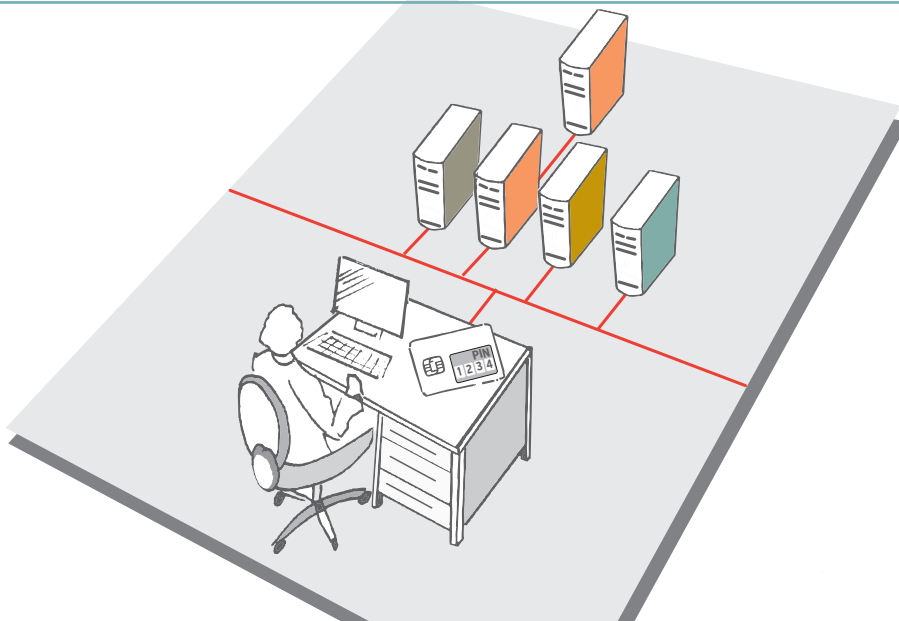


## Single Sign On



### Vorteile

- Hohe Benutzerakzeptanz und -produktivität
- Return on Investment (ROI) binnen kürzester Zeit
- Einfache Installation und Administration
- Einfache Integration in bestehende Infrastruktur durch skalierbare und verteilte Architektur
- Keine Veränderung der Verzeichnisse nötig, wie z.B. des Active Directory
- Einbinden neuer Applikationen intuitiv und schnell
- Viele Applikationsprofile werden mitgeliefert
- Unterstützung sowohl herkömmlicher als auch hochsicherer zertifizierter Authentisierungsverfahren
- Breite Unterstützung von Chipkarten und USB Tokens
- Fast User Switching mit Shared Desktop
- Automatische Aktivierung des Screen Savers nach dem Ziehen der Karte/des Tokens verhindert unberechtigten Zugang
- Hochverfügbarkeit/Ausfallsicherheit/Skalierbarkeit out-of-the-box

### Sichere Passwortverwaltung und Single Sign On (SSO)

Komplizierte, mehrstufige Anmeldeprozesse mit unterschiedlichen Benutzernamen-/Passwort-Kombinationen machen Mitarbeitern das Leben unnötig schwer und ein Unternehmen nicht sicherer. Die Erfahrung zeigt, dass Benutzer aus Bequemlichkeit fast immer naheliegende Passwörter – wie beispielsweise den Namen des Ehepartners, der Kinder oder des Haustiers – verwenden. Solche Passwörter sind leicht angreifbar und stellen ein enormes Sicherheitsrisiko dar. Aber auch unternehmensweit eingeführte Passwort-Restriktionen vermögen diese Sicherheitslücke nicht zu schließen. Der Faktor „Passwort“ bleibt dabei stets ein hohes Risiko für die Sicherheit des Unternehmens. Aus diesem Grund verlangen viele Unternehmen in ihren

Passwort Policies die Vergabe von schwierigen Passwörtern, d.h. Passwörter mit bis zu acht Stellen. Je nach Unternehmensvorgabe müssen diese sowohl Buchstaben, Ziffern als auch Sonderzeichen beinhalten. Solche Passwörter sind schwierig zu merken. Kontrollen belegen, dass diese Passwörter aller Warnungen zum Trotz zumeist schriftlich festgehalten werden. Kaum ein Arbeitsplatz, an dem sich nicht nach kurzer Suche Passwortlisten mit zehn oder mehr Passwörtern finden – zumeist ganz klassisch unter der Schreibtischablage, in der obersten Schublade oder im Terminkalender notiert. Bei einem gezielten Angriff besteht die Gefahr, dass Unbefugte nicht nur an die Daten des jeweiligen Arbeitsplatzrechners gelangen, sondern auch in das Firmennetzwerk eindringen können, da die meisten PCs heute ver-

netzt sind. Die Lösung für dieses Sicherheitsrisiko heißt Single Sign On, welches das herkömmliche Identifikationsverfahren mittels Benutzername und Passwort und darüber hinaus die zertifizierbare Anmeldung gleichzeitig unterstützt. Die Verbindung mit einer Chipkarte oder einem USB-Token ermöglicht die problemlose und skalierbare Migration von einer schwachen zu einer starken Authentisierung im Unternehmen.

### Sicherheit durch Portabilität

Beim auf Chipkarten basierenden Single Sign On werden die Schlüssel auf der Chipkarte dazu verwendet, die persönlichen Geheimnisse abzusichern. Dadurch ist ein Höchstmaß an Sicherheit gewährleistet. Jedes Benutzerprofil wird zentral auf einem Server verwaltet und kann



jederzeit an jeder beliebigen Arbeitsstation aufgerufen werden. Damit wird die völlig freie Wahl des PC-Arbeitsplatzes (Free Seating) Realität. Zudem wird ein schneller Benutzerwechsel (Fast User Switching) ermöglicht. Meldet sich ein Benutzer an einer Arbeitsstation durch Entfernen der Chipkarte ab, kann sich ein neuer Benutzer an der gleichen Arbeitsstation mit Hilfe seiner Chipkarte anmelden. Falls gewünscht, werden neue Passwörter ohne Interaktion mit dem Benutzer generiert und gewechselt, was bei allen gewählten Anwendungen bedeutet: „Sicherheitsstufe hoch“.

### **Sicherheit mit Kosteneffizienz**

Single Sign On wird von den Benutzern sehr gerne angenommen und sorgt zudem für erhöhte Produktivität und Effizienz im Unternehmen. Die Suche nach verlorenen Passwörtern gehört der Vergangenheit an und spart somit kostbare Arbeitszeit und letztlich Geld. Gleichzeitig wird der User Help-Desk, der erfahrungsgemäß überdurchschnittlich oft mit passwortbezogenen Anfragen befasst ist, stark entlastet. Durch innovative Lösungen zur Kartenverwaltung sind Karten schneller und einfacher verfügbar. Etwaige Probleme werden von Help-Desk-Assistenten online oder offline rasch und unkompliziert direkt am Arbeitsplatz des jeweiligen Anwenders behoben. Der Return on Investment (ROI) ist dank den damit erzielten Kosteneinsparungen binnen kürzester Zeit erreicht.

### **Hohe Interoperabilität durch Standards**

Durch die Unterstützung diverser Chipkarten, USB-Tokens und Chipkartenleser von PC/SC, PKCS#11 und Microsoft CSP lassen sich Single Sign On-Lösungen mühelos in die gewählte PKI-Umgebung integrieren.

### **Single Sign On im Überblick**

IDpendant bietet mit der SSO-Lösung ein umfangreiches Package inklusive Support, das die komfortable Authentisierung mit Karte/Token und PIN an Zielsystemen jeglicher Art ermöglicht. Dabei authentisiert sich der Nutzer nur einmal gegenüber dem Sicherheitssystem und wird dann automatisch bei allen weiteren Applikationen wie z. B. SAP, Lotus Notes etc. sowie Netzwerken angemeldet.

### **Professionelle Installation und Training**

Die auf Standards basierende Lösung besteht aus einer Client-Software, Kartenlesern und Chipkarten der neuesten Generation für die hochsichere Authentisierung. Dabei gibt es keine versteckten Zusatzkosten: vielmehr sind sowohl die Installation vor Ort inklusive aller Reisekosten und Spesen sowie die Einschulung in das Sicherheitssystem im Festpreis enthalten. Damit sind die kostengünstigen Single Sign On-Lösungen von IDpendant der optimale Einstieg ins Identity & Access Management für jedes Unternehmen.