

UseNet Software – Identity & Access Management



Der Einsatz von SSO mit Smartcards am Stations-PC Schneller Benutzerwechsel im klinischen Alltag.

Von
Alexander Görig
Senior Consultant
UseNet Software GmbH
goerig@use-net.at



USENET
T R U S T

UseNet Software – Identity & Access Management

Die Situation heute

Als Patientenakten noch in Papierform geführt wurden, war die Dokumentation zwar nicht besonders flexibel, hatte aber auch klare Vorteile: Alle Eintragungen, etwa bei der Visite, wurden handschriftlich vorgenommen und vom Arzt per Unterschrift bestätigt. Ob in einer elektronisch geführten Akte ebenso eindeutig und schnell nachvollzogen werden kann, welcher Arzt bei einem Patienten beispielsweise eine bestimmte Medikation angeordnet hat, hängt dagegen entscheidend davon ab, wie diese eingesetzt wird. In der Anfangszeit des Krankenhaus-Informationssysteme waren ausschließlich die jeweils diensthabenden Krankenschwestern berechtigt, die entsprechenden Eintragungen auf Anweisung der Ärzte vorzunehmen.

Im Laufe der letzten Jahre vergrößerte sich die Anzahl der Anwendungen sowie der Benutzer, da alle Mitarbeiter eigenen Zugriff zu den Systemen erhielten. Infolgedessen müssen sich Mitarbeiter, die im Laufe eines Tages an mehreren Arbeitsplätzen und mit verschiedenen Applikationen arbeiteten, zahlreiche Passwörter merken. „Der Zeitaufwand, der mit den einzelnen Log-In-Vorgängen verbunden ist, passte nicht zum straffen Arbeitsalltag in einem Krankenhaus.“ „Das ist Zeit, die für die Arbeit mit den Patienten dringend notwendig ist.“, so Stimmen von Kunden der UseNet Software GmbH. Zudem führen die vielen verschiedenen Kombinationen von Benutzername und Passwort für die unterschiedlichen Anwendungen oft zu Zugangsproblemen, die durch den Help Desk beseitigt werden müssen. In der Praxis des Krankenhausbetriebs verzichten viele Mitarbeiter deshalb bei einem Nutzer- oder Arbeitsplatzwechsel darauf, sich ab- und wieder anzumelden. Dies führt dazu, dass Eingaben diverser Nutzer unter einem

einigen Account verbucht werden, wodurch die Nachvollziehbarkeit der Abläufe nur noch eingeschränkt möglich ist.

Durch stetige Änderung der Anforderungen an die Dokumentation im medizinischen Bereich und der Nachvollziehbarkeit der Abläufe im Krankenhaus (z.B. Joint Commission International), ist ein Fortschritt auf diesem Gebiet dringend notwendig. Medizinische Dokumentation ist nicht nur ein Arbeits- und Kommunikationsmittel, sondern muss im Bedarfsfall auch als Beweismittel verwendbar sein. Daher ist es erforderlich, Zugriffsrechte auf klinische Software-Anwendungen je nach Mitarbeiter genauer zu differenzieren und die Erstellung, Bearbeitung und Einsicht von Patientendaten einfacher und besser nachvollziehbar zu machen. Gleichzeitig muss aber der Komfort für die Mitarbeiter der Dreh- und Angelpunkt des Konzepts sein, um keine Einbußen bei der Qualität der Versorgung der Patienten hinzunehmen.

Die Lösung

Aus Sicht des klinischen Personals soll der Einsatz einer neuen Softwarekomponente, die für eine An- und Abmeldung am PC und den Anwendungen zuständig ist, so wenig wie möglich in den gewohnten Arbeitsablauf eingreifen. Die Art der eindeutigen Identifikation eines Mitarbeiters spielt hierbei eine zentrale Rolle. Es gibt mehrere Möglichkeiten, Mitarbeiter bei der PC Anmeldung zu identifizieren:

- > die Eingabe von Benutzername und Passwort
- > der Einsatz eines One Time Passworts (OTP)
- > die Authentifizierung über Biometrie
- > der Einsatz von Smartcards

UseNet Software – Identity & Access Management

Ein One Time Passwort ist, wie der Name schon sagt, nur einmalig einsetzbar und muss daher bei jedem Vorgang erneut angefordert werden, wodurch dieses Szenario im Krankenhaus nicht verwendbar ist. Sowohl Benutzername /Passwort als auch die Verwendung einer biometrischen Lösung mittels Fingerabdruck bringen den Nachteil mit sich, dass sie beim Verlassen des PCs eine Aktion des Personals voraussetzen, um sich von allen Anwendungen abzumelden. Eine Smartcard eliminiert diese Unzulänglichkeiten.

Verlässt der Mitarbeiter den Arbeitsplatz, so wird die Smartcard mitgenommen. Je nach Arbeitsplatz wird die Sitzung geparkt, oder es findet eine Abmeldung von laufenden Anwendungen statt. Beim erneuten Stecken der Smartcard am selben oder an einem anderen PC, wird entweder die Sitzung wiederhergestellt oder es erfolgt eine erneute Anmeldung an den laufenden Applikationen. Eine Eingabe von Passwörtern für die Sitzung oder die Anmeldung an Anwendungen wird durch die einmalige Eingabe einer PIN für die Smartcard beim Stecken abgelöst. Selbst die in regelmäßigen Zeitabständen vorgeschriebenen Passwortwechsel werden automatisch durchgeführt. Sollte die Smartcard einmal vergessen werden, so kann sich der Benutzer durch die Beantwortung von wenigen Sicherheitsfragen an jedem PC schnell und problemlos anmelden. Alternativ kann auch eine temporäre Ersatzkarte durch die Administration oder die Personalabteilung ausgestellt werden. Mit der eindeutigen Identifikation der Mitarbeiter kann dann auch die Funktion des Enterprise Single Sign On (E-SSO) unter Berücksichtigung der Sicherheitsanforderungen umgesetzt werden: Anmeldung einmal für alle Applikationen.

Aus Sicht der IT-Administration ist der Einsatz von Enterprise SSO eine große Erleichterung:

Die Anzahl der eingehenden Anrufe wegen Passwortproblemen sinkt drastisch. Aufgrund der Einfachheit der Lösung beschränken sich auch die für die Endanwender notwendigen Schulungsmaßnahmen zur Verwendung auf ein Minimum.

Die Technik hinter der Lösung

Eine der Hauptanforderungen an die E-SSO Lösung für die BenutzerInnen stellt die Mitnahme von geöffneten Sitzungen und Anwendungen zu einem anderen PC dar. Weiters muss die Anmeldung an einer Sitzung extrem schnell erfolgen, da die Lösung aufgrund häufiger Arbeitsplatzwechsel im Alltag ansonsten von den Anwendern nicht akzeptiert werden würde.

Der Einsatz von Terminal- und Citrix Servern ist bereits heute in vielen Krankenhäusern nicht mehr wegzudenken. Häufig erfolgt die Anmeldung an den Servern automatisch mit den Anmeldedaten des Windows Benutzers oder einer Eingabe des Benutzernamen und des Passworts von Hand. Das Beenden einer solchen Sitzung muss zwangsweise ebenfalls durch die Anwender manuell ausgelöst werden. Da dies unter Zeitdruck im Alltag oft nicht durchgeführt wird, ergeben sich die im ersten Kapitel beschriebenen Schwierigkeiten der Nachvollziehbarkeit und Überprüfbarkeit.

Eine Lösung für diese Probleme stellt Evidian, der europäische Marktführer für das Enterprise Single Sign On, bereit. Neben anderen funktionalen und technischen Vorteilen war dies ein entscheidender Faktor dafür, dass sich die UseNet Software bei ihren Lösungen für den Einsatz von Evidian SSO entschieden hat.

UseNet Software – Identity & Access Management

Für die technische Lösung wird auf einem Windows Thin Client oder einem Standard Windows PC ein Teil der Evidian SSO Lösung für den schnellen Benutzerwechsel (Fast User Switching = FUS) installiert. Durch das Stecken einer Smartcard wird der zugehörige Benutzer ermittelt und mit diesem Benutzer eine Terminal Server- (TS) oder Citrix-Sitzung gestartet. Innerhalb dieser Sitzung läuft eine weitere SSO Komponente, die die automatische Anmeldung an allen Anwendungen durchführt. Beim Ziehen der Smartcard wird die laufende TS- oder Citrix-Session automatisch geparkt. Der PC steht dem nächsten Benutzer zur Verfügung. Beim erneuten Stecken derselben Smartcard wird die geparkte TS- oder Citrix-Session wiederverbunden. Alle zu Beginn gestarteten Anwendungen sind genau an derselben Stelle, an der sie verlassen wurden, wieder verfügbar und ein unmittelbares Weiterarbeiten ist gewährleistet.

In vielen Häusern gibt es sehr ressourcenhungrige Anwendungen, die nicht innerhalb einer TS oder Citrix Umgebung laufen können, da sie die Server schnell überlasten würden. Auch für diesen Typ von Anwendungen bietet Evidian die perfekte Lösung: Die nun lokal am Client PC installierte Anwendung wird ebenfalls von SSO durch das Stecken und Ziehen der Smartcard so bedient, dass immer nur Mitarbeiter mit gerade gesteckter Smartcard an der Anwendung angemeldet werden. Beim Ziehen der Karte erfolgt ein sauberes Abmelden des Benutzers von der Anwendung. Ist dies nicht möglich, so wird diese beendet.

Alle für den Betrieb notwendigen Informationen werden verschlüsselt in einem zentralen Verzeichnis wie dem Active Directory gespeichert und stehen somit immer zur Verfügung. Folgende Abbildung zeigt die Architektur der SSO Lösung:

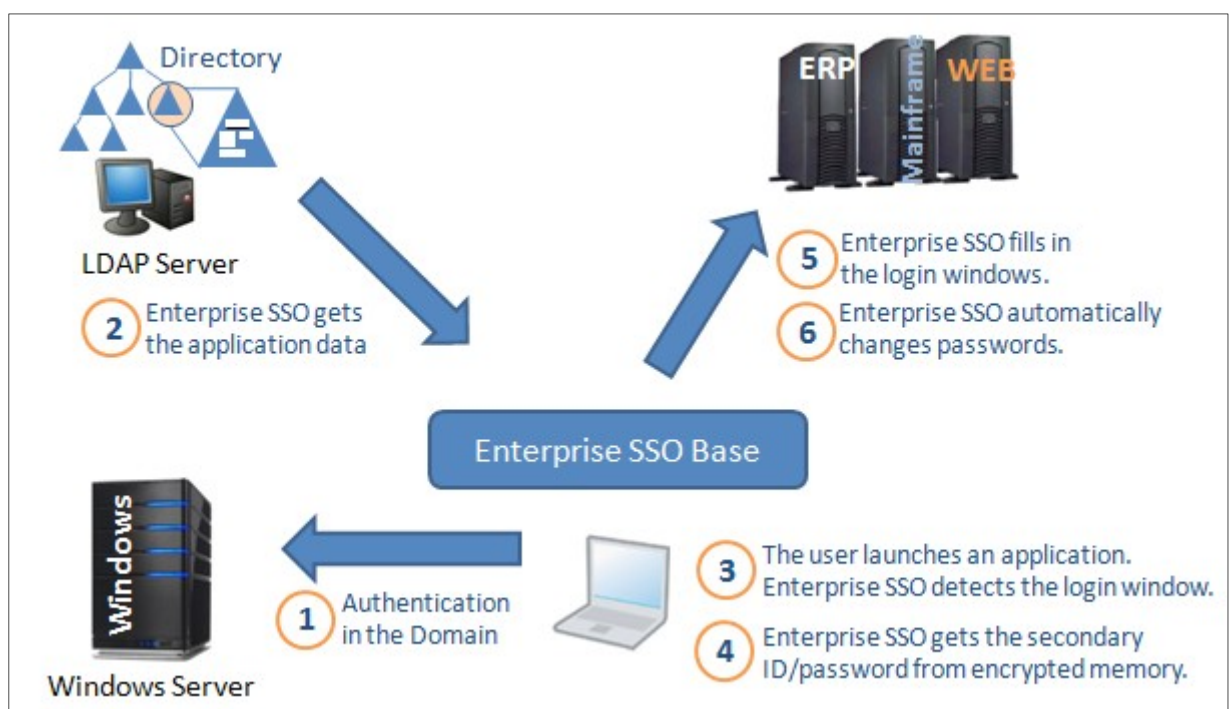


Abbildung 1: Architektur einer Enterprise SSO Lösung

UseNet Software – Identity & Access Management

Viele Unternehmen haben versucht, die Funktion des schnellen Benutzerwechsels mit Mitteln des Windows Betriebssystems umzusetzen. Der größte Nachteil dieser Variante ist die verhältnismäßig lange Zeit des eigentlichen Benutzerwechsels. Dieser dauert je nach Hardware und Auslastung des PCs zwischen 30 und 300 Sekunden. Für das Tagesgeschäft eines Krankenhauses ist diese Lösung somit nicht geeignet. Die von der UseNet Software vorgestellte Lösung des schnellen Benutzerwechsels benötigt hierzu nur 6 Sekunden.

Der Nutzen

UseNet Software hat sich als Evidian Implementierungspartner auf Enterprise Single Sign On spezialisiert. Durch diese Fokussierung kennen wir die Anforderungen an den Betrieb einer Krankenhaus IT-Infrastruktur sowie deren Anwender und Prozesse sehr genau. Unserer Erfahrung nach ist die Einführung einer Evidian SSO Lösung mit schnellem Benutzerwechsel und Smartcard-Login in sehr kurzer Zeit durchführbar. Die Reaktion der Anwender auf die neue SSO-Smartcard Lösung ist in der Regel äußerst positiv.

Der Gewinn für das Krankenhaus durch die Möglichkeit schneller, einfacher Reports für Audits und Compliance Überprüfungen (z.B. „Wann wurde der letzte Passwort Wechsel durchgeführt?“), die Entlastung der IT-Mitarbeiter und des Helpdesks und vor allem die hohe Zufriedenheit des medizinischen Personals sind die Hauptargumente für die Implementierung des schnellen Benutzerwechsels mit einer Enterprise Single Sign On Lösung und Smartcards.

In der Customer Success Story über das IAM Projekt im LKH Villach, die im Downloadbereich der Homepage der UseNet Software GmbH zu finden ist, können Sie mehr über Single Sign On und Fast User Switching in der Praxis erfahren.

Kontaktieren Sie uns, um mehr über SSO und schnellen Benutzerwechsel zu erfahren:

UseNet Software GmbH

A-8074 Grambach, Parkring 1

Tel: +43 (316) 40 23 97

E-Mail: info@use-net.at

Web: www.use-net.at

