# Single Sign On

# im Bereich Web-To-Host

## Was ist Single Sign On?

Betritt man als Benutzer ein Firmengelände oder Behörde, so gibt es meist auch nur beim Pförtner oder Wachschutz eine Authentifizierung über die Prüfung des Personalausweises. Für die Mitarbeiter im Hause reicht diese Kontrolle aus und man verlässt sich auf diese Prüfung. Nur beim Zutritt zu einem Bereich mit einer erhöhten Sicherheit kommt eventuell eine erneute, eventuell sogar verstärke, Prüfung hinzu.

Genau auf diese Art lässt sich in der EDV ein Single Sign On, abgekürzt SSO, realisieren. Die Benutzeranmeldung am System entspricht dem Pförtner und die erweiterte Prüfung lässt sich z.B. durch ein „4 Augen Prinzip mit zwei Smartcards oder zwei Kennwörtern“ realisieren.

Unter Single Sign On wird ein Verfahren verstanden, wo der Benutzer sich nur einmal an einem EDV System, z.B. an seinem PC, anmeldet und danach einen freien Zugang zu weiteren EDV Systemen hat. Hierzu wird ein SSO System installiert, was diese Erstanmeldung überwacht und danach automatisch eine Anmeldung dieses Benutzers an die weiteren EDV Systeme durchführt.

## Warum Single Sign On?

Das SSO wird in der gemischten EDV Landschaft verstärkt von den Administratoren und Anwendern gefordert. Dies hat unterschiedliche Gründe.

Zum einen ist es die Bequemlichkeit, dass man sich nicht mehr per Hand anmelden muss. Dieser Anmeldevorgang wird Tag für Tag, und teilweise auch mehrmals am Tag, für jedes Zielsystem, wiederholt. Wird dies automatisiert, so erspart sich der Anwender diese Prozedur. Im Laufe der Wochen und Monate summieren sich diese Minuten der Ersparnis auf. Da der Anwender keine falschen Kennwörter mehr eingibt, erspart dies dem Administrator auch das Freischalten von gesperrten Kennwörtern auf Grund von mehrfacher Fehleingabe.

Zum anderen kann das SSO auch eine Verstärkung der Sicherheit bedeuten. In unserer Projektpraxis hatten wir einen extremen Fall, bei dem auf Grund von gewachsener EDV Landschaft und mehrfachen Fusionen von Firmen die Endanwender 13 verschiedene EDV Systeme zu bedienen hatten. Dies führte dazu, dass entweder auf allen Systemen das gleiche Kennwort verwendet wurde, die Kennwörter trivial waren oder der Endanwender diese Kennwörter auf einem Zettel notierte. Alle drei Folgen sind für die Sicherheit nicht tragbar, da sie zu einem schwächeren Zugangsschutz führen.

Geht man von einem strengen Zugangsschutz zum PC aus, abgesichert durch entsprechende Maßnahmen wie z.B. einer erweiterten PC Anmeldung über Smartcard (oder ähnliches), so können die Benutzer maschinell an den dahinter liegenden EDV Systemen angemeldet werden. Die vom SSO System gespeicherten Zugangsdaten müssen natürlich auch entsprechend einem erweiterten Schutz unterliegen und z.B. verschlüsselt in einem geschützten Netzwerk oder auf einer Smartcard liegen.

Ist dies alles gegeben, so kann sogar zu den EDV Systemen mit automatisch generierten und dem Endanwender unbekannten Kennwörtern gearbeitet werden. D.h. der Endanwender kennt nur die Zugangsdaten zu seinem geschützten PC und kann z.B. auch nur von dort mit dem Host arbeiten. Über andere PCs, z.B. von zu Hause, kommt er nicht in das System, da er das Kennwort für den Hostzugang nicht kennt. Dies funktioniert natürlich nur für stationär arbeitende Anwender.

Das SSO System überwacht dabei ebenfalls automatisch die notwendigen Wechsel der Kennwörter über eine Zeitsteuerung oder gesteuert durch die Host Anwendung.

## Für welche Systeme gibt es SSO?

Alte Anwendungen arbeiteten meist für sich allein und sahen Möglichkeiten für ein SSO nicht vor. Die Benutzeranmeldung erfolgt über eine Dialogbox.

Neuere Anwendungen sehen es vor, dass eine automatische Anmeldung erfolgt. Diese automatische Anmeldung kann beim Aufruf über Parameter erfolgen (Anwendung /user:hugo /password:meier), es kann aber auch z.B. über standardisierte Verfahren wie Kerberos erfolgen.

Sieht die Anwendung beides nicht vor, kann man versuchen, trotzdem ein SSO zu realisieren. So können z.B. mit SSO Tools von Drittanbietern die Dialogboxen automatisiert versorgt werden, Eingabefelder in HTML Seiten gefüllt werden oder Hostanmeldungen maschinell durchgeführt werden.

Für die Hostanwendungen gibt es bei den Emulationen meist Schnittstellen, die ein SSO ermöglichen. So kann z.B. eine Hostanwendung gesteuert werden, in dem zu der Emulation eine Verbindung über eine „HLLAPI“ (standardisierte Schnittstelle von IBM definiert), über DDE (standardisierte Schnittstelle von Microsoft definiert) und OLE (standardisierte Schnittstelle von Microsoft definiert), oder über Java Bean Schnittstelle aufgebaut wird. Über diese Schnittstellen können die Bildschirme ausgelesen und mit Benutzereingaben versorgt werden.

## Authentifizierung von Benutzern

Wie oben beschrieben, sollte die erste Authentifizierung der Benutzer im System möglichst streng sein. Dies kann z.B. bei Windows Betriebssystemen über Erweiterungen geschehen, die den Login Mechanismus über eine eigene GINA (Windows Login Komponente) mit Verfahren für Smartcard, Kennworthistorie, Ausschluss von trivialen Kennwörtern, etc erweitern. Ist dieses Verfahren streng / sicher genug, so kann dies für die dahinter liegenden Systeme ausreichen.

Ist es im Projekt gewollt, so kann natürlich der Benutzer auch gegen eine weitere Instanz geprüft werden. So kann z.B. mit den Benutzerdaten eine Anmeldung am LDAP-Server, am IBM RACF oder an einem Unix-System durchgeführt werden.

## Speicherung und Transport von Kennwörtern

Das SSO benötigt für die automatisierte Anmeldung des Benutzers an Fremdsysteme meist die Benutzerdaten im Klartext. D.h. diese Zugangsdaten müssen vom SSO verwaltet und gespeichert werden. Diese Zugangsdaten werden „zweiweg“ verschlüsselt gespeichert. Sie werden also so verschlüsselt gespeichert, dass sie auch wieder entschlüsselt werden können. Dies ist leider nicht zu vermeiden, wenn die Fremdsysteme mit Kennwörtern arbeiten.

Daraus folgt aber auch, dass die Daten in einem „Tresor“ gehalten werden müssen und der Zugang zu diesem Tresor möglichst sicher sein muss. In diesem Tresor werden die Daten verschlüsselt gespeichert, z.B. mit Triple-DES oder IDEA. Der Tresor selbst muss mit Netzwerkmitteln gegen Manipulationen oder Entwendung geschützt sein.

Natürlich muss auch der Transport der Daten, so weit wie möglich, verschlüsselt erfolgen.

## Kerberos

Kerberos ist ein standardisiertes Verfahren zur Authentifizierung von Benutzern welches mit „Tokens“ (Tickets) und ohne Kennwörter arbeitet. Dies hat den großen Vorteil, dass die Kennwörter nicht mehr „zweiweg“ verschlüsselt gespeichert und im Klartext übergeben werden müssen.

Soll eine Anmeldung an ein Fremdsystem mit Kerberos Unterstützung erfolgen, so wird (über gesicherte Verfahren) ein Token an das Fremdsystem gesendet, aus dem die Authentizität des Benutzers eindeutig hervorgeht.

## SSO bei INTRA-SYS

### Windows Emulationen

Die Windows Emulationen von INTRA-SYS haben für die Fremdsteuerung programmierbare Schnittstellen implementiert. Dies sind die von IBM standardisierte HLLAPI Schnittstelle, eine DDE Schnittstelle, eine OLE Schnittstelle, die von Siemens vorgegebene Schnittstelle FHSDoors und die von SAG vorgegebene Schnittstelle „Entire Connection“. Hiermit lässt sich nahezu aus jeder Programmierumgebung eine Hostautomatisierung erreichen, z.B. aus Visual Basic oder Microsoft Office. Ein Aspekt der Automatisierung ist natürlich das SSO zum Host.

Sofern der Host Kerberos unterstützt, werden hierfür in den INTRA-SYS Emulationen auch diese Verfahren implementiert.

**Java Emulationen**

Die Java Emulationen von INTRA-SYS liegen in einem Java Bean vor und lassen sich sowohl auf dem Client als auch auf den Servern sehr komfortabel einbinden.

Beispiele in realisierte Projekte sind:

- im Browser als Applet mit Java-Script Interface
- auf den PCs eingebunden in Java Applikationen
- auf dem Server eingebunden in ein Java Servlet
- auf dem Server eingebunden in JSP Applikationen

Weitere Informationen hierzu sind im Produktblatt „HostBean SDK“ verfügbar.

Auch hier lassen sich die Abläufe auf dem Host und ein SSO an den Host realisieren.

**Server Komponenten**

Bisher arbeiten die Server Komponenten von INTRA-SYS mit einer Benutzeranmeldung durch Übergabe eines Benutzernamens und Kennwortes. Diese Daten werden entweder z.B. von der Java Emulation oder einer HTML-Seite abgefragt und dann übergeben.

An einer Kerberos Unterstützung für die Server Komponenten wird gearbeitet.

**Internet Portale**

Gerade in den Internet Portalen ist das SSO ein ganz zentrales Thema, da das Portal die zentrale Stelle für alle Applikationen sein soll. Auch hier ist das SSO für viele Bereiche und fremde Anwendungen gut zu realisieren.

Bisher realisierte SSO Lösungen im Portal:

- Anmeldung an Hostsysteme über Java Emulationen
- Anmeldung an fremde Internet Seiten über HTML- / HTTP-Tunneling
- Anmeldung an Microsoft Netzwerk (und Abmeldung beim Ende des Portals)
-
- Authentifizierung an IBM RACF
- Authentifizierung über Natural Prozeduren
- Authentifizierung an LDAP Server
- Authentifizierung an Unix Systeme
-
- Absenderidentifizierung über SmartCard
- Absenderidentifizierung über PC „NodeID“ (analog zur Windows Produktaktivierung)