

Stand der Technik



Enterprise Single Sign-On

Dieses White Paper enthält
eine Übersicht über die wichtigsten
Funktionen von Enterprise
Single Sign-On.

Es stellt auch die Evidian Enterprise
SSO Lösung insgesamt vor.

PERSPEKTIVEN

EVIDIAN
A Bull Group Company

Was versteht man unter Single Sign-On?

Während eines Arbeitstages müssen Benutzer mehrfach ihre Anwendungskennwörter eingeben und sie regelmäßig ändern. Dies kann sich schnell in eine Belastung für die Produktivität und den Helpdesk verwandeln.

Mit Single Sign-On (SSO) meldet sich der Benutzer einmalig mit seiner Authentifizierungsmethode an, anschließend kann er seine Anwendungen verwenden. Für die Anmeldung können Angestellte zum Beispiel ein Kennwort, eine USB Token oder ihren Fingerabdruck benutzen.

Wie wird Single Sign-On eingesetzt?

Um Single Sign-On zu verwenden, installieren Sie normalerweise auf Ihrem PC ein unauffälliges Softwaremodul, das die Anwendungskennwörter für Sie eingibt. Wenn Sie nur Webanwendungen nutzen oder im "Thin-Client" Modus arbeiten benötigen Sie keine lokale Installation. In diesem Fall befindet sich die SSO Software auf einem Server und gibt die Passwörter von dort ein.

SSO macht das Leben für Benutzer leichter. Evidian hat Unternehmen gesehen, in denen Benutzer etwa dreißig verschiedene Kennwörter wissen mussten und diese teilweise für alle sichtbar auf einem Zettel am Arbeitsplatz aufgeschrieben haben – heute ist ein Kennwort ausreichend. SSO verstärkt die Sicherheit und reduziert die Kosten, besonders die Helpdesk-Kosten. Darum schätzte Gartner in einem kürzlich veröffentlichten Bericht¹ ein, dass sich das Wachstum der Enterprise SSO Anbieter "beschleunigt", während Evidian zu den Marktführern in diesem Segment gehört.

Individual SSO und Enterprise SSO

Viele einzelne SSO Tools existieren, z.B. die Autovervollständigungs-Funktionen von Webbrowsern. Aber Hunderten oder sogar Tausenden von Angestellten in einem Unternehmen SSO bereit zu stellen, erfordert einen ganz anderen Ansatz. Dies ist auf die Funktionen, welche die meisten großen Organisationen benötigen, zurückzuführen: Verwaltung, starke Authentifizierung, Delegation, Mobilität und Audit. Daher sollten Sie ein SSO Tool wählen, welches diese Funktionen zufriedenstellend ausführen kann. Diese ist eine Entscheidung für die Unternehmensebene.

¹ Magic Quadrant für Enterprise Single Sign-On, 2008

Evidian's *Enterprise SSO* Lösung ist das Ergebnis von über fünfzehn Jahren Erfahrung in den Bereichen Identity und Access Management. Ca. 1,5 Millionen Benutzer weltweit greifen jeden Tag auf ihre Anwendungen Mithilfe von Evidian's Lösung zu. Der größte Kunde davon verwendet SSO auf 120 000 PCs.

Evidian's *Enterprise SSO* Lösung ist das Ergebnis von über fünfzehn Jahren Erfahrung in den Bereichen Identity und Access Management. Ca. 1,5 Millionen Benutzer weltweit greifen jeden Tag auf ihre Anwendungen Mithilfe von Evidian's Lösung zu. Der größte Kunde davon verwendet SSO auf 120 000 PCs.

Auf der Grundlage dieses Wissens gibt dieses White Paper einen Überblick über den Stand der Technik der SSO Funktionen.

Was sind die Alternativen zu SSO?

Andere Lösungen reduzieren die Anzahl von Kennwörtern, die vom Benutzer eingegeben werden müssen.

- **Kennwort-Synchronisierung** erlaubt Ihnen, dasselbe Kennwort für all Ihre Anwendungen zu verwenden. Wenn das Kennwort zum Lesen Ihrer E-Mail "abcd" lautet, dann wird das Kennwort für die Finanzanwendung ebenfalls "abcd" lauten. Es gibt keine Client Software auf den PCs, aber ein Kennwortänderungsmodul muss für jede Anwendung entwickelt werden.

Der Anwendervorteil geht hier auf Kosten der Sicherheit. Sofern das Kennwort "abcd" zu einer schlecht geschützten Anwendung gestohlen wird werden dadurch alle weiteren Anwendungen gefährdet. Sie können Ihren Zugriff auf die Finanzanwendung nicht verleihen, ohne gleichzeitig den Inhalt Ihrer Emails preis zu geben.

- Durch **Access-Token** (wie Kerberos oder SAML) delegierte Anwendungen werden auf einem externen Modul authentifiziert. Aber in den meisten Fällen muss die Anwendung modifiziert werden. Es ist nicht möglich, Zugriffe unter Kollegen zu übertragen. Reauthentifizierungsfunktionen zum Zugriff auf sensitive Anwendungen sind häufig ebenfalls nicht vorhanden.

Warum investieren Unternehmen in SSO?

Laut Evidian gibt es drei Hauptfaktoren, die Unternehmen in ihrem Entschluss motivieren, eine SSO-Lösung zu erwerben. Die Art und Weise, auf die ein SSO-Tool bereitgestellt wird, variiert mit nachfolgenden Faktoren, wobei es sich nur um ein Tool handelt. Natürlich werden einige Unternehmen auch mehrere der Anforderungen haben!

- 1> **Sicherheit erhöhen** und gesetzliche Bestimmungen erfüllen. Durch Erzeugen eines verpflichtenden Verbindungspunktes zwischen einem Benutzer und seinen Anwendungen kann eine Organisation die Zugriffe wirksam kontrollieren. Außerdem wird ein Protokoll dieser Zugriffe und Verwaltungsoperationen zentral gespeichert, wodurch die Betriebsprüfung erleichtert wird. Dies erleichtert die Einhaltung der Vertraulichkeits-, Integritäts- und Verfügbarkeitsanforderungen.
- 2> **Betriebskosten reduzieren**. Häufige Eingabe von Kennwörtern reduziert oftmals die Produktivität der Benutzer. Zu diesen "verdeckten Kosten" kommen noch Sichtbare: bis zu 30% der Helpdesk-Kosten werden durch vergessene Kennwörter verursacht. Diese Kosten können Sie mit einer SSO-Lösung signifikant senken.
- 3> **Sicheren Zugang gewähren**. Immer häufiger wird die Forderung ohne Risiko Informationssysteme der Außenwelt zur Verfügung stellen zu können. Zugang zum Netz ist leicht geworden, doch oft ist es noch schwierig für Angestellte auf Intranetanwendungen von außen zuzugreifen. Z.B. Ärzte, die ein Krankenprotokoll nachschlagen müssen, Ingenieure auf einer Baustelle oder Vertreter in ihrem Hotel: SSO ermöglicht sicheren und einfachen Zugriff auf Webanwendungen, auch von außen.

Je nach der Art des Bedarfs, sind einige Abteilungen eines Unternehmens anspruchsvoller als andere. Daher will die allgemeine Verwaltung die Einhaltung der Gesetze und Vorschriften, wie z.B. Sarbanes Oxley in den USA oder der UK Companies Act 2006. Die IT-Abteilung versucht ihre Betriebskosten zu reduzieren. Die Betriebsabteilung verlangt für ihren Teil, dass ihre mobilen Angestellten auch außerhalb des Unternehmens produktiv arbeiten können.

Sicherheit, Kostensenkung, Skalierbarkeit: Evidian *Enterprise SSO* deckt diesen Bedarf dank einer modularen Architektur. Die funktionellen Module können schrittweise implementiert werden und liefern nützliche und sichtbare Funktionen in jeder Phase. Außerdem ist es möglich zuerst eine Abteilung mit SSO auszurüsten und anschließend auf den Rest des Unternehmens zu erweitern.

Die drei Architekturen von Single Sign-On

Die SSO-Software auf dem PC eines Benutzers gibt Logins und Kennwörter für den Benutzer ein. Aber wo findet die Software diese Information? Die Antwort ist ein bedeutender Unterschied zwischen SSO und Enterprise SSO. Im letzteren Fall befinden sich die Daten an einem sicheren Ort außerhalb des Benutzer PCs. Dies dient der Kontrolle (es sollte möglich sein, einen Remotezugang zu gewähren oder zu entziehen) und um die Mobilität des Benutzers zu gewährleisten.

Auf dem Markt kann man drei grundlegende Architekturen finden, die für die Bereitstellung von SSO-Informationen wie Benutzernamen, Passwörter und Zugriffsrechten, dienen.

- **SSO-Server:** Die Information ist auf einem Server, zum Beispiel einem Windows oder Unix Server gespeichert, der diesen Aufgaben im Allgemeinen gewidmet ist. Der Client auf dem PC fragt den Server bei Bedarf. Dieser Server wird oft für hohe Verfügbarkeit ausgerüstet, obwohl der Cachemechanismus auf dem PC temporäre Ausfallzeiten kompensieren kann. Deshalb müssen Anlaufkosten in Betracht gezogen werden: Server (Sie können einen vorhandenen Server verwenden) und Softwareinstallation. In einer verteilten Architektur kann es sein, dass die Anzahl dieser Server hoch ist.
- **SSO-Appliance:** Es ist nur eine Abwandlung der SSO-Serverlösung: Software und Hardware werden zusammen verbaut. Die Kosten der Softwareverteilung werden auf diese Art und Weise reduziert. Andererseits ist es nicht möglich, die Software auf einem vorhandenen Server zu installieren, was die Verteilungskosten erhöhen kann. Im Gegensatz zu einem Server, ist es oft nicht möglich Speicher oder Festplattenplatz einer Appliance zu erweitern.
- **Enterprise-Directory:** SSO-Daten werden in verschlüsselter Form in einem Verzeichnis gespeichert, das bereits im Unternehmen vorhanden ist. Zum Beispiel das Active Directory über das die Benutzer auf Windows zugreifen. Deshalb müssen keinen zusätzlichen Server oder Appliances installiert werden. Ihre PCs sind bereits konfiguriert, da sie bereits auf das Verzeichnis zugreifen. Verteilungskosten werden bedeutend reduziert.

In solch einer Architektur ist das Verzeichnis normalerweise mit Verwaltungsstationen und einer Datenbank vervollständigt, in denen Aktivitäten (für Audits) gespeichert werden. Aber diese Module sind keine notwendigen und kritischen Punkte für das Gesamtsystem, im Gegensatz zu Server und Appliance-Architekturen.

Evidian *Enterprise SSO* verwendet eine Enterprise Directory basierte Architektur. Die Erfahrung hat gezeigt, dass diese einfache Lösung schneller zu implementieren ist und gleichzeitig die höchste Sicherheitsstufe beibehalten.

Mehrere Unternehmens-Verzeichnisse

Alle Unternehmen haben ein Benutzerverzeichnis angelegt, aber es können auch mehrere existieren. Sei es aus historischen Gründen, (ein vor kurzem erworbenes Unternehmen, eine unabhängige Tochtergesellschaft) oder funktionell (Partner sind in einer separaten Datenbank verwaltet). Dies kann ein Problem darstellen, falls Benutzer von einer Domäne zur anderen wechseln.

In diesem Fall schlägt Evidian eine Verzeichnissynchronisationslösung vor: die zuverlässigste Information ist an der richtigen Stelle enthalten und es ist somit möglich, ein zentrales Verzeichnis zu erstellen. Auf diese Weise wird ein in den Personaldatenbanken erklärter Benutzer im schnell im ganzen Unternehmen einsatzbereit sein.

Eine Architektur, die auf dem vorhandenen Enterprise-Verzeichnis basiert, ist einfach und leicht zu verwalten und schnell einsetzbar.

MEINE KRITERIEN	Erfordert die SSO Lösung, dass ich neue Server oder Appliances in meinem Unternehmen bereitstelle? Ist es ein Problem, wenn meine Benutzer in mehreren Datenbanken, Dateien und Verzeichnissen aufgeführt werden?
------------------------	--

SSO macht Sicherheit selbstverständlich

In einer gut gestalteten Enterprise SSO-Lösung ist Ihre Sicherheitsrichtlinie keine Belastung mehr für Ihre Benutzer. Sie führen die Anwendungen aus, zu denen sie berechtigt sind, ohne sich ständig an ihre Kennwörter erinnern zu müssen oder diese zu verwalten. Ihre Mitarbeiter richten sich automatisch nach Ihren Sicherheitsrichtlinien.

Die SSO-Lösung führt alle kennwortgebundenen Operationen durch. Sie kann diese sogar ohne den Eingriff des Benutzers ändern. Sie können ebenfalls verhindern, dass Benutzer selber das Kennwort für eine vertrauliche Anwendung kennen: der Benutzer kann dieses Passwort somit nicht offenbaren oder betrügerisch außerhalb des Unternehmens verwenden.

In einer zentralen Management-Konsole können Sie entscheiden, wer Zugriff auf welche Anwendung hat. Natürlich steht es außer Frage, bei Tausenden von Mitarbeitern und Hunderten von Anwendungen, Zugriffe einzeln zu verteilen!

Der Administrator entscheidet, welche Anwendergruppe Zugriff auf welche Applikationsgruppe hat und bei Bedarf, auf welchen PCs. Zum Beispiel:

- "Backoffice-Anwendungen können nicht auf einem Handels-PC verwendet werden."
- "Auf R&D PCs muss immer durch die Eingabe biometrischer Daten autorisiert werden."
- "Die Hauptbuchhaltungssoftware kann nur von der Finanzabteilung verwendet werden."

MEINE KRITERIEN	Kann der Zugriff auf eine Anwendung, entsprechend der Tätigkeit oder dem Einsatzort eines Benutzers, eingeschränkt werden?
------------------------	--

Kennwörter leicht verwalten

Mit Evidian *Enterprise SSO* können Sie strikte Passwortrichtlinien (z. B. mindestens zwei Zahlen zu Beginn, mehr als zehn Zeichen, etc.) festlegen, unabhängig von der Anwendung. Dies ist möglich, da diese bei allen Kennwortoperationen beachtet wird.

Aber, was passiert während der Urlaubsvertretung eines Mitarbeiters? Früher gab besagter Benutzer seinen Account weiter, mit all den Risiken in bezug auf Sicherheit und Kontrolle.

Evidian *Enterprise SSO* kann einem Arbeitnehmer vorübergehenden Zugang zu dem Account eines Kollegen übertragen ohne das Passwort offen zu legen. Natürlich nur unter Beachtung der Sicherheitsrichtlinien. Außerdem werden Zugriffe protokolliert, so dass Sie wissen, welche Operationen von welchem Benutzer durchgeführt wurden.

MEINE KRITERIEN	Erlaubt die SSO-Lösung einem Mitarbeiter, seinen Zugang für eine Anwendung zu übertragen, zum Beispiel vor dem Urlaub?
------------------------	--

Sicherheit verstärken: starke Authentifizierung

Benutzername/Passwort ist die häufigste Zugriffsmethode. Jedoch ist dieses universelle "Sesam öffne dich" oft nicht ausreichend, um wichtige Ressourcen zu schützen. Wer sagt das der Benutzer auch der rechtmäßige Kennwortbesitzer ist?

Deshalb wünschen manche Kunden SSO mit starker Authentifizierung zu erweitern. Obwohl diese Methodik selten auf allen Arbeitsplatzrechnern eingesetzt wird, ist es eine gängige Praxis, um kritische Anwendungen zu schützen: z.B. Top-Management und Händler PCs, Zugriff auf Patientenakten bei Ärzten, sensitive Laptops usw.

Hier sind übliche Arten starker Authentifizierungsmethoden:

TYP	Beispiel von Benutzern	Beispiel von Lösungen
Chipkarte oder USB-Token mit Zertifikaten	Krankenhäuser, Industrie, Banken	Health professional cards - CPS (Frankreich) NHS Connecting for Health - CfH (UK) eID Card (Belgien)
Biometrie	Industrie, Banken	Fingerabdruckleser
Karte oder USB Token mit Benutzernamen und Passwörtern	Verwaltungen	Firmenausweis
Einmal Kennwort	Banken	TAN Liste
'Defense' Chipkarte	Verteidigungsbereich	Multifunktionsgesicherte Karte
Funkausweis	Krankenhäuser, Groß- und Einzelhandel	RFID-Technik

Evidian *Enterprise SSO* ist kompatibel mit einer Vielzahl von starken Authentifizierungsmethoden. Als reiner Softwarehersteller stellt Evidian keine Authentifizierungshardware her. Aber *Enterprise SSO* kann diese Geräte für ganze Unternehmen verwalten: Zuweisung von Chipkarten und USB Token, Verleihoperationen, Blacklisting etc. Zugriffssicherheit verstärkt ohne die Administration zu belasten.

Was soll gemacht werden, wenn ein Benutzer seine Authentifizierungshardware verliert oder wenn diese defekt ist?

Ein Notzugriff ist notwendig, um übermäßige Helpdeskarbeitsbelastung zu verhindern.

MEINE KRITERIEN	<p>Ist die SSO-Lösung kompatibel mit der gewählten starken Authentifizierungsmethode?</p> <p>Kann ich eine Anwendung auf einem PC verbieten, der nicht durch eine starke Authentifizierung geschützt ist?</p> <p>Ist es möglich, zur gleichen Zeit mehrere Authentifizierungsmethoden, basierend auf Benutzer oder PC-Profilen zu unterstützen?</p> <p>Liefert die SSO-Lösung die Kontinuität des Benutzerzugriffs, wenn die starke Authentifizierung fehlschlägt?</p>
------------------------	--

Reduzierung Ihrer Betriebskosten dank Servicekontinuität

Ein gut gestaltetes SSO-Tool reduziert die Betriebskosten. Mancher dieser Kosten sind schwer auszuwerten, da sie die Produktivität der Benutzer betreffen. Andere jedoch leicht zu messen: die Helpdesk Arbeitsbelastung.

Evidian *Enterprise SSO* verwaltet alle Anwendungskennwörter, damit brauchen Sie sich keine Sorgen mehr um vergessene Passwörter oder gesperrte Konten zu machen. Helpdesk-Anfragen sinken bis zu 30%, da Benutzer Anwendungskennwörtern nicht mehr vergessen können.

Allerdings müssen Sie bei vergessenen Primärkennwörtern oder verlorenen Zugriffskarten handeln. Zum Beispiel, wenn ein Vertreter in einem Hotel bemerkt, dass seine Smartcard nicht mehr funktioniert. Evidian *Enterprise SSO* wird Ihren Zugriff Offline entsperren, mit oder ohne Helpdesk Interaktion. Es ist nicht notwendig mit dem Netzwerk verbunden zu sein.

Wenn Sie diese Funktion aktivieren, wird der Benutzer beim ersten Starten von SSO aufgefordert mehrere Fragen und Antworten zu geben. Wenn der Benutzer sein Zugriffskennwort vergisst oder seine Zugriffskarte verliert, beantwortet er die vordefinierten Fragen und setzt so sein Kennwort zurück. Auf diese Weise wird der Benutzer nicht durch einen verlorenen Zugriff gesperrt.

MEINE KRITERIEN

Werden meine Benutzer in der Lage sein, ihr Kennwort zurückzusetzen, ohne den Helpdesk zu kontaktieren?

Ist es möglich ein Passwort Offline zurückzusetzen?

Wie Sie eine Ihrer Anwendungen in die SSO-Lösung integrieren können.

SSO ersetzt den Benutzer, in der Hinsicht, dass es an seiner Stelle die Anmeldung an Anwendungen vornimmt. Dafür muss SSO das Anmelde- Kennwort- und Kennwortänderungsfenster der Programme erkennen. Dies wird einmalig für jede Anwendung im Unternehmen durchgeführt und anschließend an die PCs der Mitarbeiter über das Unternehmensweite Directory verteilt.

Für Windowsapplikationen ist dies eine einfache drag and drop Konfiguration, da SSO entsprechend der Microsoft Empfehlungen entwickelt wurde. Aber auch seltenere Anwendungen müssen in Betracht gezogen werden:

- Interne Anwendungen, die vor vielen Jahren entwickelt wurden
- Mainframe-Anwendungen im Terminal Emulationsmodus
- Pakete mit speziellen Schnittstellen wie SAP R/3 und Lotus Notes
- Java Anwendungen oder Applets
- Webseiten und Portale durch Internet Explorer oder Firefox

Wie kann man sicherstellen, dass die SSO Software meine Anwendungen integrieren kann, selbst die 'exotischsten'? Oft ist es besser, den Lieferanten zu bitten, die Lösung bei Ihnen zu testen und die kritischsten Anwendungen zu integrieren.

Evidian *Enterprise SSO* erlaubt Ihnen, die meisten Anwendungen mit wenigen Klicks zu integrieren. Starten Sie die Anwendung und bewegen Sie die Maus auf "Login" oder "Passwort" Felder. Die Anwendung wird automatisch erkannt und kann im gesamten Unternehmen verwendet werden. Anwendungen, wie z.B. Lotus Notes, SAP R/3 oder Browser werden von Haus aus unterstützt. Ein grafisches Skripttool behandelt die seltenen, widerspenstigen Anwendungen.

MEINE KRITERIEN

Wird die SSO-Lösung mir erlauben meine Anwendungen einfach zu integrieren oder erfordert sie eine Programmierung?

Tägliche Verwaltung von SSO

Die SSO Lösung ermöglicht es, erhebliche Einsparungen zu erzielen. Allerdings sollten Sie nicht im Gegenzug hohe Verwaltungskosten erzeugen! Wenn Sie Dutzende von Benutzern haben, wäre es sehr umständlich, die Zugriffsrechte individuell zu verteilen. Stattdessen muss die Rechteverwaltung bei Eintritt oder Verlassen eines Benutzers im Unternehmen extrem einfach und schnell sein.

Hinzu kommt, sofern einige Anwendungen während der Implementierung in einem Unternehmen 'entdeckt' werden, müssen diese auch schnell integrierbar sein. Da der Benutzer die Kennwörter für seine kritischen Anwendungen nun nicht mehr kennt, wie übertragen Sie seine Accounts während seines Urlaubs, ohne die Arbeitsbelastung des Helpdesk zu steigern?

Es empfiehlt sich eine Vorort-Evaluierung durchzuführen, um die tägliche Verwaltungsauslastung eines SSO Tools zu schätzen. So können sie für einige Tage die verschiedenen Verwaltungsszenarien testen. Sie werden feststellen, ob die Profile der SSO Administratoren hinreichend sind und Sie können ihre Arbeitsbelastung einschätzen.

Evidian hat viele Verwaltungsfunktionen in *Enterprise SSO* integriert. In mehr als fünfzehn Jahren Erfahrung, wurden Ergonomie und Funktionen verfeinert, um Administratoren produktiver zu machen. Zum Beispiel:

- Wenn ein Benutzer nicht anwesend ist, kann er seine Accounts delegieren ohne dabei seine Kennwörter zu verraten.

- Lokale Administratoren integrieren ihre eigenen Applikationen und verwalten die Zugriffsrechte ihres Teams.
- Spezifische Administrationsrollen umfassen Anwendungen, Smartcards, Passwörter, Audit, etc.
- Wenn ein Administrator sein Aufgabengebiet ändert, können seine Rechte schnell weitergeleitet oder delegiert werden.

MEINE KRITERIEN Was wird die von der SSO-Lösung generierte tägliche Verwaltungsbelastung sein?

Ihr Informationssystem wird ohne Risiko zur Außenwelt geöffnet

Wenn Ihre Mitarbeiter sich außerhalb Ihrer Firma aufhalten, müssen sie einen speziell konfigurierten PC benutzen, um die Intranetanwendungen zu nutzen? Die bessere Wahl ist die Verwendung von SSO-Funktionen, die es Ihnen ermöglichen, dass sie sicher auf interne Webanwendungen über jeden Browser (zum Beispiel im Internetcafe oder vom Kunden aus) zugreifen können.

Dies kann äußerst nützlich sein. Einige Evidian Kunden verwenden diese Funktion, um ihren mobilen Angestellten Unabhängigkeit zu sichern: Verkäufer auf Reisen, Polizeibeamte bei einem Auftrag, Ingenieure auf einer Baustelle im Ausland usw.

Einige andere SSO-Lösungen betrachten Webzugriffe als schwach integriertes Add-On: deshalb erfolgt der Austausch von "Web" und "Intranet" Teilen nicht ordnungsgemäß. Im Gegensatz zu diesen Lösungen benutzt Evidian *Enterprise SSO* dieselbe geschützte Information, unabhängig von dem Zugriffsmodus.

MEINE KRITERIEN Wird der User noch Zugriff von außen auf Anwendungen haben, wenn SSO das Kennwort, ohne Kenntnis des Users geändert hat?

Skalierbarkeit - SSO auf den Rest des Unternehmens erweitern

Sie möchten nur Ihre Abteilung oder einen Standort Ihres Unternehmens mit einer SSO-Lösung ausrüsten. Beachten Sie dabei die Möglichkeit diese in Zukunft auf den Rest des Unternehmens auszuweiten. Dementsprechend brauchen Sie eine skalierbare Lösung oder sie riskieren, das Konzept ändern zu müssen mit den dazu gehörenden Schwierigkeiten einer Kennwortmigration.

Skalierbarkeit ist ein ernstes Problem für bestimmte SSO-Produkte, die für ein paar hundert Anwender ausgerichtet sind. Wie können Sie Daten freigeben, damit Benutzer in mehreren Ländern mobil werden können? Müssen Sie Administratoren pro Website oder pro Abteilung schulen? Ändern sich die grundlegenden Technologien mit der Mitarbeiterzahl? Werden mehrere Domänenverzeichnisse unterstützt? Müssen Sie dedizierte Hardware an vielen Stellen installieren?

Evidian *Enterprise SSO* wird bei Unternehmen mit über 100.000 Benutzern eingesetzt. Die Lösung ist leicht zu erweitern: dieselbe einfache Technik, auf der Grundlage des Unternehmensverzeichnis, wird für Kunden mit Hunderten sowohl als auch mit Zehntausenden von Benutzern verwendet.

MEINE KRITERIEN

Hat die SSO-Lösung bewiesen, dass sie für Tausende von Benutzern eingesetzt werden kann?

Integration mit Identity und Access Management

Evidian weiß, dass SSO sehr oft den Auftakt zu einem ehrgeizigen Identitäts- und Zugriffsverwaltungsprojekt darstellt. In einer zweiten Stufe können strikte Zugriffsrichtlinien definiert werden, welche entsprechend einem strengen und regelmäßigen Prozess überwacht werden. Mitarbeiter werden natürlich über den vorhandenen SSO Mechanismus nachkommen.

Aber das ist nicht alles: da SSO Informationen über die Verwendung von Anwendungen bereitstellt, ist es möglich, die Einhaltung der Sicherheitsrichtlinien kontinuierlich zu überwachen. Schließlich können Konten automatisch erstellt, aktualisiert und aus den Anwendungen selbst entfernt werden; der Benutzer ist somit sofort einsatzbereit.

Evidian *Enterprise SSO* ist ein Teil der Evidian IAM Suite Identity and Access-Management-Lösung. Sie kann mit Evidian *User Provisioning* kombiniert werden, um das Passwortmanagement zu automatisieren oder die tatsächlichen Zugriffsdaten an den Evidian *Policy Manager* zu senden und um die Sicherheitsrichtlinien zu verfeinern.

Schließlich brauchen Sie die Verteilung von Kennwörtern an Benutzern nicht mehr: In Abstimmung mit ihren Identity Management Prozessen synchronisiert ein Provisioning-Modul oder Workflow die Anwendungskonten mit SSO.

MEINE KRITERIEN

Kann die SSO-Lösung, durch die Integration von Role Based Access Management und Provisioning zu einem späteren Zeitpunkt erweitert werden?

Evidian Enterprise SSO: Übersicht der Merkmale

Evidian *Enterprise SSO* ermöglicht es Ihnen, schnell eine wirkungsvolle Single-Sign-On-Lösung einzusetzen. So können Benutzer auf ihre Anwendungen leicht und sicherer zugreifen. Je nach gewünschten SSO-Funktionen, können Sie Module hinzufügen, welche starke Authentifizierungen und zusätzliche Verwaltungsfunktionen bereitstellen.

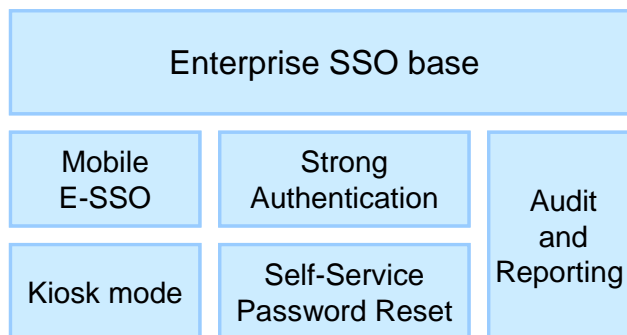


Abbildung 1 - Eine vollständige Single Sign-On Lösung

Evidian Enterprise SSO besteht aus mehreren komplementären Modulen:

- Schnellzugriff auf Single Sign-On: **Enterprise SSO Base** bietet einzelne Single Sign-On-Funktionen, wie Zugriff und Kennwortregelverwaltung, Delegation, Authentifizierung und Audit an.
- SSO Zugriff über das Internet: **Mobile E-SSO** ermöglicht es Benutzern, sich sicher Mithilfe von SSO auf ihre Anwendungen, von jedem Webbrowser aus, zu zugreifen.
- Passwort-Management: Durch **Self Service Password Reset**, können Benutzer ihr persönliches Kennwort selbstständig zurücksetzen.
- Der **Kiosk Mode** ermöglicht Mitarbeitern die gemeinsame Nutzung eines PCs, ohne die Windowssitzung neu zu starten. Deshalb findet der Benutzerwechsel innerhalb von wenigen Sekunden statt.

- **Starke Authentifizierung** ermöglicht es, Authentifizierungsmethoden wie z. B. kryptografische Karten, USB Token, Zertifikate, aktive RFID und Biometrie zu verwenden.
- **Audit und Reporting** erstellt Berichte über Verwaltungs- und Authentifizierungsereignisse und über Zugriffe auf Zielanwendungen. Der Anwendungszugriff kann auf bestimmte Access Points beschränkt werden.

Unterstützte Umgebungen

- Der SSO-Client ist verfügbar für Windows 2000, 2003, XP, Vista, Citrix und Terminal Server.
- Die meisten Windows-, HTML- oder Java-Anwendungen sind durch einfaches "Drag and Drop" konfigurierbar. Die Funktionalität spezifischer Anwendungen wird in Standardkonfigurationen (SAP, Lotus Notes und Mainframe-Emulatoren) oder durch graphische Konfiguration unterstützt.
- Das Verzeichnis, das die User und die Sicherheitsrichtlinien enthält, kann Active Directory oder ADAM, Sun Java System Directory Server, Fedora Directory Server, Novell eDirectory, IBM Directory Server oder OpenLDAP sein.
- Auditereignisse werden im Microsoft SQL Server, MySQL, IBM DB2 oder Oracle gespeichert.

Für weitere Informationen, besuchen Sie bitte www.evidian.com

Email: info@evidian.com

© 2008-2009 Evidian

Die in diesem Dokument enthaltenen Informationen stellen die Ansicht von Evidian in bezug auf die Fragen, die zum Zeitpunkt der Veröffentlichung erörtert wurden, dar. Da Evidian auf die sich ändernden Marktbedingungen reagieren muss, steht dieses Whitepaper nicht unveränderlich für die Haltung von Evidian. Evidian kann die Richtigkeit der hier dargelegten Informationen nach dem Datum der Veröffentlichung nicht garantieren.

Dieses Schreiben ist nur für informative Zwecke gedacht. EVIDIAN ÜBERNIMMT KEINE GARANTIE FÜR ANGEDEUTETE ODER AUSDRÜCKLICHE HINWEISE IN DIESEM DOKUMENT.

Wir erkennen die Rechte der Marken-Eigentümer an, die in diesem Buch erwähnt werden.