



Eine Plattform zur Benutzerauthentifizierung

DIESES WHITE PAPER BESCHREIBT EINE PLATTFORM FÜR DIE AUTHENTIFIZIERUNG VON BENUTZERN UND DIE VERWALTUNG VERSCHIEDENER ARTEN VON ELEKTRONISCHEN BERECHTIGUNGSNACHWEISEN (CREDENTIALS) IN EINER WEBBASIERTEN UMGEBUNG. ES ZEIGT DIE DAMIT VERBUNDENEN VORTEILE AUF UND WEIST AUF EINIGE GRUNDSÄTZLICHE ASPEKTE HIN, DIE VOR DER EINFÜHRUNG VERSCHIEDENER AUTHENTIFIZIERUNGSMECHANISMEN ÜBERLEGT WERDEN MÜSSEN.

Warum verschiedene

Authentifizierungsmethoden?

Viele Organisationen und Unternehmen bieten über ihre Websites den Zugang zu einer Reihe von Dienstleistungen an: Aktienhandel, Web-Hosting, Online-Banking, Abschluss von Versicherungsverträgen, um nur einige zu nennen. Der Benutzer wird dabei oft noch über Benutzername und Passwort authentifiziert (Ein-Faktor-Authentifizierung durch Kenntnis eines Geheimnisses) – diese Methode ist jedoch in den meisten Fällen nicht sicher genug. Ein höherer Sicherheitsstandard schützt den Anbieter vor möglichem Datendiebstahl, der mit wirtschaftlichem Schaden und Vertrauensverlust seitens der Kunden verbunden wäre. Erst ein effektives Zwei-Faktoren-System zur Benutzerauthentifizierung genügt auch gesetzlichen Anforderungen, im Hinblick auf die Bekämpfung von Geldwäsche und Betrug. Sicherheit muss als unverzichtbares Merkmal jedes Web-Dienstes betrachtet werden, der mit sensiblen Informationen oder finanziellen Transaktionen zu tun hat.

Überblick über die Lösung

Die Authentifizierungsplattform von Nexus erlaubt es Organisationen und Unternehmen, ein ganzes Spektrum an Authentifizierungsmethoden einzusetzen, unter anderen PKI-Zertifikate, OTP-Tokens und SMS-OTPs. Abhängig vom Risikoniveau kann so jede einzelne Benutzergruppe mit dem für sie geeignetsten Berechtigungsnachweis ausgestattet werden. Darüber hinaus können die Benutzer ihre Berechtigungsnachweise über ein webbasiertes Self-Service-Portal anfordern, sperren und erneuern, ohne das Helpdesk kontaktieren zu müssen. Die hier beschriebene Lösung beinhaltet auch eine Monitor-Funktion, die es den Administratoren erlaubt, die Aktionen eingeloggter User zu verfolgen.

Überlegungen

Die Einführung geeigneter Authentifizierungsmethoden sollte mit einer Risikoabschätzung hinsichtlich der Web-Dienste der Institution beginnen, und zwar unter folgenden Gesichtspunkten: Kundentyp (Einzelhandel,

Gewerbe usw.), Zweck der Transaktionen des Kunden (Einzugsverfahren, Überweisungen, Kreditvergabe usw.), Sensibilitätsniveau der verwalteten Informationen, Praktikabilität der Kommunikationsmethoden, vorgesehene Gesamtvolumen an Transaktionen, akzeptable Zusatzkosten pro Kunde. Es sollte sodann ein effektives Verfahren für die Benutzerauthentifizierung eingeführt werden. Die Authentifizierungsprozesse selbst sollten so ausgelegt sein, dass sie maximale Interoperabilität gewährleisten und sich gut in die übergeordneten Strategien der Web-Dienste des Kunden integrieren lassen.

Die Authentifizierungsmethode für eine bestimmte Anwendung sollte für diese geeignet und auch wirtschaftlich dem absehbaren Risiko dieser Anwendung angemessen sein. [1]

Die Risikoanalyse sollte:

- alle über das Internet laufenden Transaktionen und die entsprechenden Zugangsniveaus (Sicherheitsstandards) umfassen
- die Methoden zur Risikominderung einschließlich Methoden zur Benutzerauthentifizierung, die für jeden Transaktionstyp und jedes Zugangsniveau angewandt werden können, aufzeigen und bewerten
- für jeden Transaktionstyp und für jedes Zugangsniveau eine mögliche Beurteilung der Effektivität der Methoden zur Risikominderung – für bestehende und zukünftige, sich verändernde Risikofaktoren – beinhalten [2]

Nähere Beschreibung der Lösung

Kern der Lösung ist eine Plattform für die Ausgabe von Software-Tokens oder Chipkarten mit Zertifikaten. Sie umfasst außerdem ein Self-Service-Portal, über das die Benutzer selbstständig Zertifikate und andere Berechtigungsnachweise anfordern, sperren und erneuern können.

Dazu gehört auch ein Server, der auf Anfrage ein OTP (one-time password) an das Mobiltelefon eines Benutzers sendet. Mit diesem sowie Benutzername und Passwort kann sich der Benutzer in eine Anwendung oder einen Web-Dienst einloggen.

Ein Online-Validierungsserver verifiziert die Gültigkeit der Berechtigungsnachweise der Benutzer. Der Server ist vorkonfiguriert zur Verifikation vom Anbieter selbst ausgegebener Zertifikate und einer Reihe von eIDs und OTPs, die von marktgängigen OTP-Tokens generiert werden.

Jeder Benutzer bekommt einen PKI-Client, mit dem Chipkarten und Software-Tokens zum Einloggen benutzt sowie deren Zertifikate und PINs verwaltet werden können usw.

Literatur[1] „FFIEC GUIDANCE Authentication in an Internet Banking Environment“, Financial Institution Letter FIL-103-2005. [2] Ebd.

Beschreibung einzelner Funktionen

Anmeldung/Registrierung

Der Kunde füllt auf der Website ein Formular mit Name, Adresse, Telefonnummer usw. aus und sendet die Angaben an den Anbieter. Er bekommt einen Brief mit den für die erste Nutzung benötigten Informationen. Die PIN folgt in einem zweiten Brief. Nun hat er alles, um sich zum ersten Mal einzuloggen und einen PKI-Client und ein Zertifikat herunterzuladen. Dieses Zertifikat nutzt er für die Anmeldung bei allen weiteren Besuchen der Website.

Alternativ zu den Briefen könnte das System auch so ausgelegt sein, dass es Anmelde Informationen und PIN per SMS an ein vorher registriertes Mobiltelefon sendet.

Erneuerung/Sperrung

Für diese Funktionen besucht der Benutzer das entsprechende Self-Service-Portal, logt sich mithilfe des jeweiligen Berechtigungsnachweises ein und führt die gewünschte Aktion aus.

Installation/Integration

Das System wird mit gut definierten Schnittstellen geliefert, die eine schnelle, problemlose Integration in jede bestehende Umgebung ermöglichen. Lediglich eine minimale Konfiguration ist nötig. Es arbeitet sehr gut mit herkömmlichen Identity-Management-Systemen zusammen.

Administration

Das System wird über ein zentrales Administrationsmenü verwaltet. Die Administratoren können Benutzer hinzufügen oder löschen, Zertifikate herausgeben und sperren und das System allgemein überwachen.

Hauptkomponenten der Lösung

Nexus Certificate Manager ist ein verlässliches, offenes, auf Standards basierendes System zur Ausgabe und Verwaltung elektronischer Berechtigungsnachweise (Credentials). Da es Benutzern einen großen Umfang an PKI-Funktionen und hohe Sicherheit bietet, ist Certificate Manager das effektivste Tool auf dem Markt für den Einsatz in Zertifizierungsstellen. Das System passt sich jeder Größenordnung an – von der Verwaltung interner

Firmenausweise in kleinen Unternehmen bis hin zur Ausgabe von Millionen von Reisepässen oder nationalen Ausweisen. Durch seine Mandantenfähigkeit können Hunderte von Zertifikatausgebern (CAs) auf der gleichen Plattform effizient und virtuell völlig getrennt betrieben werden.

Nexus MultiID Server ist eine Plattform, die PKI-Validierungsdienste für Online-Authentifizierung und -Signaturprüfung bietet. Sie ist kompatibel mit verschiedenen PKI-Client-Typen, Zertifikatausgebern und elektronischen IDs. Sie ist modular aufgebaut und lässt sich dadurch leicht erweitern, zum Beispiel kann sie zusätzliche PKI-Clients, Protokolle, Verzeichnisdienste und Online-Dienste zur Statusüberprüfung von Zertifikaten unterstützen, wenn dies notwendig wird. MultiID Server hat sich im Einsatz im eBanking-Umfeld als außerordentlich verlässlich und skalierbar erwiesen.

Nexus Personal ist ein sehr schlanker PKI-Client, der sichere Authentifizierung und digitale Unterschriften über Chipkarten und Softtokens ermöglicht. Er unterstützt alle verbreiteten Chipkarten und ist für Windows, Mac OS und Linux erhältlich. Nexus Personal ist der führende PKI-Client in Schweden und wird von BankID, der wichtigsten schwedischen eID, genutzt, deren Installationszahl 2009 die 2-Millionen-Marke überschreiten wird.

Zusätzliche Vorteile

Eine sichere Plattform zur Benutzerauthentifizierung ist mit zusätzlichen wirtschaftlichen Vorteilen verbunden, denn sie intensiviert die Beziehung zwischen Marke und Konsument. Im Einzelnen kann die Organisation bzw. das Unternehmen über die Plattform:

- Kundenvertrauen und -loyalität aufrechterhalten,
- die Marke schützen und festigen, denn das Risiko durch Betrug wird eingeschränkt,
- registrierten Benutzern Werbemittel und Informationen zukommen lassen,
- neue Kunden gewinnen, insbesondere durch die überzeugende, weil sichere und leicht zu nutzende Lösung,
- durch die Selbstverwaltung seitens der Nutzer die Verwaltungskosten der Zugangslösung minimal halten bzw. den Akzeptanzgrad der Lösung bei den Kunden steigern.

Über Nexus

Nexus ist ein international agierendes Unternehmen für Sicherheitslösungen und E-Kommunikation. Zu unseren Kunden weltweit gehören große Unternehmen und Organisationen, die bei der Verwaltung von sensiblen Informationen und bei der Kommunikation von Daten auf IT und das Internet angewiesen sind. Nexus bietet ein umfassendes Portfolio integrierter Produkte und verfügt über 25 Jahre Erfahrung in diesem Geschäftsbereich. Nexus ist ein internationales Unternehmen mit Hauptsitz in Schweden und Niederlassungen in mehreren europäischen Ländern sowie bekannten Partnern überall auf der Welt. Weitere Informationen zu Nexus finden Sie auf unserer Homepage unter www.nexus-safe.com.

contact@nexus-safe.com

www.nexus-safe.com

Sweden

Headquarter:
Technology Nexus AB
Box 47057
100 74 Stockholm
Phone: +46 8 655 39 00

Germany

Nexus Technology GmbH
Kantstraße 13
10623 Berlin
Phone: +49 30 206 14 15 0

Sweden

Technology Nexus AB
Nämndemansgatan 3
431 33 Mölndal
Phone: +46 31 720 60 00

France

Nexus Technology SAS
112 ter, rue Cardinet
75017 Paris
Phone: +33 1 40070606



nexus

Providing safety in a digital world