

Ein Hybrid-Device für alles

Authentisierungslösungen sind derzeit für Unternehmen die wichtigsten Sicherheitsprojekte. Consultants und reisende Mitarbeiter, die aus fremden Netzwerken heraus oder im Internetcafé ohne eigene Hardware Informationen abrufen müssen, benötigen solche Identity- und Access-Systeme, damit sie sich von beliebigen Rechnern aus sicher am VPN anmelden können. Zudem besteht der Wunsch nach einer benutzerfreundlichen Anmeldung an möglichst vielen Instanzen mittels einer kostengünstigen und effizienten Simple-Sign-On Lösung. Ein solches Anforderungsprofil lässt sich am besten durch Smartcards realisieren, allerdings –weil der mobile User über kein Lesegerät verfügt- nur in Form eines USB-Kombi-eToken, optimalerweise sogar mit einem integrierten One-Time-Password Generator.



Der eToken NG-Flash ist eine hochsichere USB-Smartcard-Lösung, die starke User-Authentisierung mit der Benutzerfreundlichkeit eines Flash-Speichers verbindet. Anwender haben somit zwei Nutzungsmöglichkeiten: die Generierung und sichere Speicherung von Zugangsdaten, Passwörtern und Zertifikaten sowie das Laden von direkt auf dem eToken vorinstallierten Applikationen.

Der Token NG-Flash verbindet starke User-Authentisierung mit der Benutzerfreundlichkeit eines Flash-Memory-Speichers. Der eToken NG-Flash wird in drei Varianten mit verfügbaren Speichergrößen von 128 Mbyte, 512 Mbyte und 1 Gbyte angeboten.

Unternehmen können Anwendern somit verschiedene Benutzungsmöglichkeiten offerieren: zum Einen die traditionelle eToken-Funktionalität zur Generierung und sicheren Speicherung von Zugangsdaten, Passwörtern und Zertifikaten. Darüber hinaus bietet der eToken NG-Flash, neben der Option, Daten auf dem Flash-Memory sicher abzulegen, auch ein Autorun-Feature, welches eToken-Lösungsanbieter in die Lage versetzt, ihre Applikationen direkt auf dem eToken vorinstalliert auszuliefern.

Der eToken NG-OTP (NG = Next Generation) revolutioniert den Markt für Zwei-Faktor-Authentisierungslösungen: Er ermöglicht sowohl Authentisierung mit Einmal-Passwörtern als auch zertifikatsbasiertes Arbeiten in PKI-Umgebungen, für Digitale Signaturen, Verschlüsselung und Zugriffsschutz auf höchstem Sicherheitsniveau. So ist eine einzige Lösung in der Lage, eine Vielfalt an Netzwerk-Umgebungen, Applikationen und Kundenbedürfnissen zu bedienen – und auf allen Ebenen für die Einhaltung höchster Sicherheitslevel zu sorgen.

Warum eToken NG-OTP?

Heutige Marktanforderungen an Authentisierungslösungen verlangen geradezu nach dem eToken NG-OTP. Viele Firmen implementieren derzeit PKI-basierte Systeme. Aber nicht jede Unternehmenssoftware ist PKI-fähig - was es häufig unmöglich macht, mit nur einer einzigen Authentisierungslösung zu arbeiten. Der neue eToken NG-OTP überwindet dieses Problem, indem er gleichzeitig PKI-Applikationen, Passwortspeicherung und starke Authentisierung mit Einmal-Passwörtern unterstützt. Er vereint die portable USB-Smartcard eToken PRO mit einem LCD Display, einer Batterie und einer Taste für die Erzeugung eines Einmal-Passwortes. Vielseitig einsetzbar und einfach in der Handhabung stellt er eine sichere, praktische und kostengünstige Alternative zu gängigen One-Time-Password-Lösungen dar. Anwender haben nun die Wahlmöglichkeit der Authentisierung mittels der USB-Token-Funktionalität oder des One-Time Passwords, alles kombiniert in einem einzigen Gerät.

Technischer Hintergrund

Mit integriertem RSA 1024 Bit (optional 2048-Bit)-Schlüssel für allgemeine PKI-Operationen und einem symmetrischen 160 Bit-Verschlüsselungsalgorithmus für OTP unterstützt der neue eToken NG-OTP sowohl Standardschnittstellen wie CAPI/PKCS11 als auch RADIUS. Im OTP-Modus benötigt die Lösung keine spezielle Client-Software auf dem Anwender-PC oder -Laptop. Der eToken NG-OTP unterstützt -wie auch schon der klassische eToken- alle gängigen Sicherheitsapplikationen wie VPN- und Web Access, Network Logon, Single-Sign-On sowie eMail- und Daten-Verschlüsselung und gewährleistet damit Mobilität und Sicherheit auf höchstem Niveau.

Komplette Verwaltungsarchitektur aus einer Hand: Das neue Token Management System TMS

Um die Verwaltung und das Handhabung verschiedener Token innerhalb eines Unternehmensnetzwerkes zu vereinfachen, hat Aladdin das Token Management System (TMS) auf

Basis des bewährten Microsoft Active Directory Framework entwickelt. Da TMS auch im Stand Alone Modus eingesetzt werden kann, ist es Unternehmen möglich, ein beliebiges User Management System anzubinden.

eToken TMS von Aladdin bildet die komplette Verwaltungsarchitektur für sämtliche Aspekte der Zuweisung, Implementierung und Personalisierung von Token, Smartcards und Mitarbeiterausweisen innerhalb eines Unternehmens. Das Token Management System unterstützt eine Vielzahl von Sicherheitsanwendungen wie Network Logon, VPN, Web Access, Secure eMail, Data Encryption und vieles mehr. Zusätzlich bietet TMS durch die Verbindung von PKI- und nicht PKI-Systemen eine lückenlose und zuverlässige Verwaltung für Security Services in Unternehmen.

Durch die direkte Verknüpfung mit den vorhandenen Nutzer-Verwaltungssystemen des Unternehmens stellt das TMS eine leistungsfähige und gleichzeitig flexible Verbindung zwischen Anwender, Sicherheitsapplikation, dem verwendeten Authentifizierungsgerät und nicht zuletzt den Regeln und Richtlinien des Unternehmens dar.

Aladdins Token Management System verbindet somit auf einzigartige Weise alle genannten Komponenten zu einem automatisierten und vollständig konfigurierbaren Registrierungs- und Verwaltungsprozess, während Schwierigkeiten bezüglich Implementierung dieser Sicherheitsservices – insbesondere solche, die auf PKI-Technologie basieren – ausgeräumt werden.

Schnelles und einfaches Anwender-Management

Mit TMS müssen Administratoren nur einen Anwender oder eine Gruppe von Anwendern in der Benutzer und Computer Ansicht des Active Directory markieren, um einen einfachen Enrollmentprozess zu initialisieren. TMS überprüft automatisch, welche Applikationen (Konnektoren) dieser Gruppe zugewiesen wurden und generiert entweder vertrauliche Daten (z.B. Schlüssel, Zertifikate und Passwort-Profile) oder fordert sie vom entsprechenden Service im Namen des Anwenders an. Die Daten werden dann automatisch auf den Token geladen.

Flexibler Support und Implementation

Aufgrund der offenen Architektur von TMS ist es möglich, externe Systeme, die über Standards mit einem Token oder einer Smartcard mittels APIs kommunizieren, flexibel über Konnektoren anzubinden. IT-Manager benötigen bei der Arbeit mit dem Token Management System kein fundiertes Wissen über die jeweiligen Applikationen.

Vorteile TMS:
▪ Einfache und zuverlässige Verwaltung von Tokens innerhalb des Unternehmens.
▪ Leichte Integration in bestehende Security-, PKI- bzw. Smartcardstrukturen in Unternehmen.
▪ Reduzierung der Kosten für Identitäts- und Passwort-Management durch eine verbesserte Verwaltung der Anwender-Keys und Zugangsprofile.
▪ Vereinfachung der Implementierung zahlreicher, insbesondere auf PKI-Technologie basierender, Security Services.
▪ Unterstützung unterschiedlicher Applikationen und Tokens dank der offenen Architektur.