

■ Neu zur CeBIT 2006: eToken NG-Flash

USB-Smartcard mit Flash-Memory-Speicher

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.

■ eToken NG-Flash: Eine neue Komponente für das All-In-One Hybrid-Device

Der neue eToken NG-Flash verbindet starke User-Authentisierung mit der Benutzerfreundlichkeit eines Flash-Memory-Speichers. Der eToken NG-Flash wird ab April in drei Varianten mit verfügbaren Speichergößen 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.

■ eToken NG-OTP 2.0: Das Hybrid-Device im neuen Gehäuse

Der Aladdin eToken NG-OTP2 basiert auf dem 2005 eingeführten Vorgängermodell und wird ab April 2006 mit einem neuen Gehäuse ausgeliefert. Das Kombi-Device für die eToken-Smartcard- und die One-Time-Password-Funktionalitäten bedient sich der Bauform des neuen eToken NG-Flash, verfügt aber im Unterschied zu diesem über ein Display und einen Knopf am hinteren Ende zur Generierung von Einmal-Passwörtern.

Der deutlich robustere eToken NG-OTP2 bietet eine wesentlich verlängerte Batterie-Lebensdauer

und reduziert dadurch die Kosten für auszutauschende Tokens. Durch die stärkere Batterie beträgt die Einsatzzeit des Tokens ungefähr sieben Jahre oder 14.000 Klicks, außerdem beinhaltet der NG-OTP2 einen Low-Batterie Indikator, der rechtzeitig vor dem Batterietod warnt.

Darüber hinaus besteht die Möglichkeit eines Batterieersatzes, was Zeit spart und die Kosten für Token-Neuanschaffungen deutlich minimiert. Hierfür bietet Aladdin einen Austauschservice für verbrauchte Batterien sowie ein Service-Kit, um die Auswechslung ausgedienter Batterien selbst vorzunehmen.

■ PKI für Linux- und Mac-Anwender: neue eToken-Middleware

Die eToken USB-Smartcard-Technologie wurde um die neue Middleware für Linux und Mac OS jeweils in den Versionen 3.60 ergänzt. Das neue Release ist ab sofort weltweit verfügbar und gewährleistet ein reibungsloses Zusammenspiel zwischen Rechnern unter diesen Betriebssystemen und Aladdin eToken als portable Hardware für die Speicherung und Übermittlung von Berechtigungsnachweisen und digitalen Zertifikaten.

Durch den Einsatz der neuen Middleware kommen Kunden in den Genuss einer vollständigen Unterstützung von Authentisierungs- und PKI-Lösungen auf Token-Basis und können die folgenden Funktionen ab sofort auch auf Mac- und Linux-Systemen nutzen:

- Import digitaler Zertifikate auf dem eToken
- Signatur und Verschlüsselung von E-Mails
- sichere Web-Authentisierung auf Grundlage von SSL-v3-Zertifikaten
- zertifikatbasierte Authentisierung für den Zugriff auf Virtual Private Networks (VPNs)
- Thin-Client-Authentisierung

■ Wolfram Dorfner



■ Von eToken und Pinguinen

eTokenOnLinux

Aladdin bietet mit dem eToken Pro und dem eToken NG-OTP eine handliche Möglichkeit, Sicherheit im Unternehmensumfeld erheblich zu erhöhen.

Die praktische SmartCard im Schlüsselanhänger wird mit durchdachter Windows-Software – wie dem Token Management System oder dem SimpleSignOn und WebSignOn – abgerundet und erfüllt die Bedürfnisse eines modernen Unternehmens. Doch schon seit Jahren sind die IT-Strukturen auf Betriebssystemebene heterogener geworden und der Bedarf an Lösungen, die quer über gemischte Windows- und Linux-Landschaften funktionieren, wird stetig größer. Gerade bei einem so heiklen Thema wie der IT-Security und sicherer Authentisierung soll ein einheitliches, sicheres Konzept für die ganze IT-Landschaft gelten und nicht vor manchen Komponenten halt machen.

Die LSE Leading Security Experts GmbH [1] stellt Ihnen anhand eines kurzen Beispiels vor, wie Sie dieses Maß an Sicherheit auf Linux-Systeme in einer heterogenen Landschaft homogen erweitern.

■ Windows und Linux

In eine bestehende Windows-2003-Domäne sollen Linux-Server und Linux-Workstations eingebunden werden. Auch an diesen Linux-Maschinen sollen sich alle Benutzer mit ihrer unter Windows ausgerollten Smartcard anmelden können. Alle Benutzer werden im Active Directory verwaltet. Unter Linux wird die Authentisierung mittels PAM (Pluggable Authentication Modules) gesteuert. Dadurch erreicht man eine hohe Flexibilität, die im Folgenden genutzt werden soll.

- Auf dem Domänen-Controller werden die Microsoft Windows Services for Unix 3.5 [2] installiert. Diese führen eine notwendige Schemaerweiterung durch.
- Auf dem Linux-System wird der eToken Treiber von Aladdin installiert. Damit Linux seine Benutzer-Accounts aus dem Active Directory bezieht, wird das Active Directory auf der Linux-Maschine als LDAP-Server angegeben und in der entsprechenden PAM-Konfigurationsdatei der Account mit Hilfe des pam_ldap-Modul geprüft.
- Damit sich der Benutzer mit dem Zertifikat auf seinem eToken authentisieren kann, wird das pam_pkcs11-Modul benutzt, das inzwischen konsequenterweise in das openssl-Projekt [3] integriert wurde.



Bild: photocase

- Das PAM-Modul pam_mkhomeidir kann dazu genutzt werden, um das Heimatverzeichnis eines Benutzers auf der Maschine neu anzulegen. In der Regel wird man die Heimatverzeichnisse aber über das Netzwerk gemountet haben.
- Die unter Windows ausgerollten Smartcards werden nun mit dem LSE Certificate Converter umgeschrieben, so dass Sie PKCS11-konform auf dem eToken vorliegen. Nun kann der Benutzer sich mit seinem eToken sowohl an den Windows- als auch an den Linux-Maschinen anmelden.

■ PKCS11 und openssl

Weitere Einsatzbereiche sind openssl, openssh oder openvpn. Mit der PKCS11-Engine [3] lässt sich die Aladdin PKCS11 Bibliothek auch in openssl einbinden, so dass eTokens nun auch mit Hilfe von openssl ausgerollt werden können. Dabei erfolgen die kryptographischen Funktionen wie bspw. das Erzeugen des Schlüsselpaars auf dem eToken. Bei openssh werden die Schlüssel des Zertifikates als SSH-Keys genutzt und bei openvpn wird mit Hilfe des Zertifikats vom eToken der VPN-Tunnel aufgebaut. Außerdem kann der eTokenNG OTP ebenfalls zur Authentisierung mit einem Einmalpasswort an Linux-Maschinen oder auf Webseiten gegenüber Apache genutzt werden. Der Phantasie sind dabei faktisch keine Grenzen gesetzt.

Noch offene Lücken schließt die LSE mit eigenen Entwicklungen aus dem Authentisierungs- und Smartcard-Umfeld. So entwickelte sie beispielsweise den o.a. LSE Certificate Converter oder den Anmeldedialog RadiusGina, der die Authentisierung an einem Terminalserver mittels Einmalpasswort mit dem eTokenNG ermöglicht. Um Windows und Linux weiter zusammenwachsen zu lassen, entsteht bei der LSE derzeit ein Anmeldedialog, der es ermöglichen soll, sich per Zertifikat an Windows-Clients mit einem reinem Linux-Backend anzumelden.

Für weitere Informationen sei Ihnen [4] oder ein Besuch auf dem Messestand ans Herz gelegt.

- [1] www.lsexperts.de
- [2] www.microsoft.com
- [3] www.opensc-project.org
- [4] www.ETOKENONLINUX.ORG

■ Cornelius Kölbl

LSE Leading Security Experts GmbH

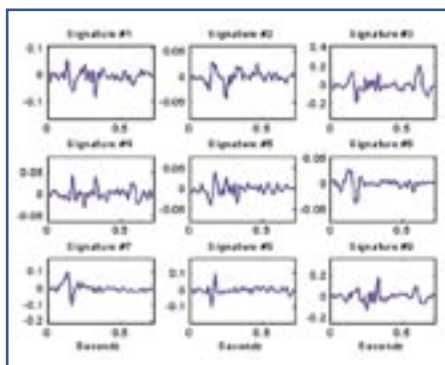
■ IDesia & Aladdin

Der BioDynamic Reader

Aladdin investiert in innovative Technologien und verstärkt die Forschungsaufwendungen auch im Bereich Biometrie.

Zusammen mit IDesia Ltd. entwickelt Aladdin derzeit den BioDynamic Reader zur Authentisierung individueller biodynamischer Signaturen (BDS™). In diesem Artikel möchten wir Ihnen die Funktionsweise dieser Zukunftstechnologie darstellen und Sie einladen, auf unserem CeBIT-Stand einen ersten Prototyp selbst zu begutachten.

Der Aladdin BioDynamic Reader ist ein neuartiges Authentisierungstool. Der BioDynamic Reader authentisiert Anwender aufgrund ihrer individuellen biodynamischen Signatur (BDS™), die auf bioelektrischen Signalen basiert, welche vom Körper erzeugt werden. Diese Signale werden während dem Auflegen von zwei Fingern auf einen kleinen metallischen Sensor eingefangen.



Der Aladdin BioDynamic Reader ist die erste Lösung ihrer Art, die biologische Signale des menschlichen Körpers und Herzens mittels einem kompakten und benutzerfreundlichen Tool erfassen kann. Der Reader eröffnet eine neue Ära biometrischer Technologie und bietet Performance und Einsetzbarkeit auf höchstem Niveau. Es ist eine einfache aber dennoch hochsichere Lösung für Daten- und Zugriffsschutz.

■ Wie funktioniert der BioDynamic Reader?

Im Gegensatz zu vielen anderen biometrischen Technologien, die statische biometrische Daten zur Authentisierung eines Anwenders benutzen, basiert die BioDynamic Reader-Technologie auf dynamischen elektrophysiologischen Charakteristika des Körpers, inklusive dem Herzschlag.

Während sich das Herz eines jeden Menschen prinzipiell gleich verhält, führen sowohl der genetische Aufbau als auch Umwelteinflüsse in früher Jugend zu geringfügigen Unterschieden in

den Elektrosignalen des Körpers und Herzens. Diese winzigen Unterschiede sind einzigartig und gleichbleibend bei jedem Menschen und können – wenn sie gemessen werden – zur Authentisierung einer Person verwendet werden.

Genau das ist mit dem BioDynamic Reader von Aladdin möglich. Durch das Auflegen von zwei Fingern auf den Sensoren, sammelt der Reader die individuellen Körpersignale eines Anwenders, verstärkt sie und stellt damit die individuelle BioDynamic Signatur (BDS™) eines Anwenders fest. Während der Enrollment-Phase wird eine biometrische Vorlage für jeden einzelnen Benutzer erstellt, welche die BDS enthält. Das mittels des Readers erfasste Signal kann dann mit der gespeicherten biometrischen Vorlage eines Anwenders verglichen und zur Authentisierung verwendet werden.

In absehbarer Zukunft ist geplant, den BioDynamic Reader Technologieanbietern als SDK anzubieten, damit diese ihn in ihre Lösungen einbinden können. Damit können Partner ihr Produktportfolio mit einer exakten, benutzerfreundlichen und haltbaren Authentisierungslösung abrunden.

Hinweis: Die beschriebene Technologie befindet sich gegenwärtig in der Entwicklungsphase und kann gewissen Änderungen unterliegen. Aladdin unternimmt derzeit keine Aussagen bzgl. Fertigstellung, Lieferzeitpunkt oder Preisstrukturen. Bei Interesse wenden Sie sich bitte an einen Mitarbeiter aus unserem eToken-Team.



■ Georg Knon