

Securing the
Global
Village



eToken™

YOUR KEY TO eSECURITY

**Die ultimative
Authentifizierungs-
Technologie**



Aladdin®
SECURING THE GLOBAL VILLAGE
Aladdin.de



Das Paradigma der digitalen Identität

Die Sicherheit des firmeneigenen Netzwerks und die ständige Verfügbarkeit von Datenbeständen sind zwei extrem wichtige Faktoren für erfolgsorientierte Unternehmen. eCommerce, strategische Partnerschaften und mobile "Einzelkämpfer" führen durch den wachsenden Bedarf am Fernzugriff auf Unternehmensressourcen zur Auflösung der klassischen Unternehmensgrenzen. Bislang ungeahnte Möglichkeiten eröffnen sich, gleichzeitig jedoch steigt die Gefahr unautorisierter Datenzugriffe. Die Kontrolle der digitalen Identität von Anwendern, die auf unternehmenskritische Ressourcen zugreifen, ist folglich von höchster Priorität. Passwörter, bisher das wichtigste Werkzeug zur Authentifizierung von Anwendern, können allzu einfach verloren gehen oder gestohlen, gemeinsam genutzt oder sogar geknackt werden. Zahlreiche Unternehmen, in denen viele Anwender und Kennwörter verwaltet werden und gleichzeitig die Effektivität der verwendeten Passwörter sichergestellt werden muss, sind dazu übergegangen, extrem strikte Regeln und Richtlinien für die Passwortverwendung und -verwaltung einzuführen. Diese Entwicklung führte zu immer komplexeren Passwörtern, die im Regelfall äußerst schwer zu merken sind. Um sich an ihre zahlreichen Passwörter zu erinnern, schreiben die Anwender sie nieder und setzen so die Sicherheit aufs Spiel, der diese Passwörter eigentlich dienen sollten.

eToken - der Organizer für die digitale Identität

Der eToken von Aladdin ist ein portables, kostengünstiges USB-Gerät zur Authentifizierung von Benutzern sowie für die digitale Signatur von vertraulichen Transaktionen. Er stellt sowohl für die Anwender als auch für IT- bzw. Sicherheitsadministratoren eine wirksame Methode zur Verwaltung der Authentifizierungsprozesse dar, da er Passwörter und digitale Zertifikate generiert, sicher speichert und darüber hinaus sämtliche Anmeldungsdaten verschlüsselt - sowohl mit Public Keys als auch mit Private Keys. Auf diese Weise stellt der eToken sicher, dass die Passwörter des Anwenders nie der risikoreichen Umgebung des PCs ausgesetzt werden.

eToken - die wichtigsten Vorteile

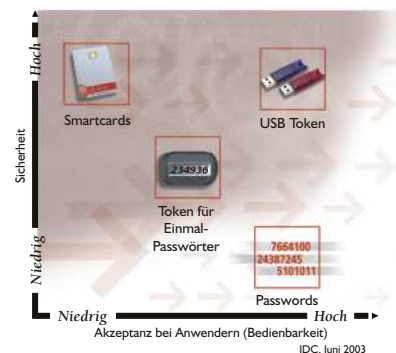
- Erhöhte Sicherheit, geschützter Datenzugriff
- Mobilität für Keys und digitale Zugriffsdaten/Zertifikate
- Besseres Passwort- und ID-Management

> Der Schutz von sensiblen Daten erfordert mehr Sicherheit als nur die Passwortüberprüfung... Die Anwender untergraben die Sicherheitsvorkehrungen nicht nur durch das Aufschreiben ihrer Passwörter, 67% aller Anwender ändern nie oder selten ihre Passwörter.
NTA Monitor, 2002

> 80% der Help-Desk-Anrufe betreffen Probleme mit Passwörtern.
www.silicon.com, 2003

> Die Kosten für das Zurücksetzen von Passwörtern bewegen sich Schätzungen zufolge zwischen \$ 40 und \$ 140 pro Anruf.
Gartner, 2003

Vergleich von Authentifizierungsmethoden nach Sicherheit und Anwenderakzeptanz





Lösungen und Applikationen

In den heutigen IT-Umgebungen gilt es mit weniger Aufwand mehr Leistung zu erzielen. eToken bietet Ihnen eine breite Plattform an Lösungen, die bei geringeren Implementierungs- und Verwaltungskosten eine umfassendere Standardisierung ermöglichen. Ein einziger eToken bietet unter anderem folgende Lösungen:



[VPN-Sicherheit (sicherer Remote-Zugriff)]

eToken ermöglicht Unternehmen eine effektive Authentifizierung ihrer Anwender, wenn diese von außerhalb auf das Firmennetzwerk zugreifen und bietet dabei nahtlose Integration mit den gängigen VPN-Systemen von Anbietern wie z.B. Cisco, Check Point, Microsoft, SSH u.v.a.

[Internet-Zugriff]

eToken ermöglicht eine starke Benutzer-Authentifizierung für den Zugriff auf geschützte Web-Ressourcen sowie digitale Signaturen für die Übertragung von sensiblen Daten. Mithilfe von Standard-Browsertechnologien und digitalen Zertifikaten können auch die Anwender feststellen, ob die Websites, auf die sie zugreifen, wirklich authentisch sind.

[Netzwerk-Anmeldung]

Mit dem eToken verfügen Unternehmen zudem über ein leistungsfähiges System für die Authentifizierung von Benutzern, die sich in geschützten Bereichen des Netzwerks anmelden. Er ermöglicht das Logon mithilfe von SmartCards und unterstützt sowohl PKI als auch den GINA-Mechanismus von Microsoft durch die Speicherung der Passwörter und Zugangsdaten der Benutzer.

[Zugangskontrolle in Gebäuden (Türen/Ausweise)]

eToken ermöglicht die Integration zahlreicher Proximity-Technologien zur Gebäudezugangskontrolle in Kombination mit dem Netzwerkzugriff sowohl für traditionelle Smartcards und auch USB-Tokens. Als ideale Lösung für Unternehmen, die Wert auf einen visuellen Identitätsnachweis legen, bietet es sich an, neben den Identifikationsdaten ein Foto des Benutzers auf die Smartcard zu drucken.

[Verschlüsselung von Dateien und Daten]

eToken bietet herausragende Konnektivität mit zahlreichen Datenschutzsystemen, von der Festplattenverschlüsselung über Boot-Schutz bis zur Verschlüsselung und Signatur einzelner Dateien.

[Sicheres E-Mail]

eToken bietet nahtlose Interoperabilität mit allen wichtigen E-Mail-Clients, die die gängigen Sicherheitstechnologien verwenden.

[Erweitertes Passwort-Management]

Mit eToken muss sich der Benutzer nicht mehr die zahlreichen Kennwörter für seine verschiedenen Accounts merken - ein einziges Passwort für den eToken reicht aus und er kann von der gesamten Funktionalität des eToken profitieren. Der eToken verwaltet sämtliche vertraulichen Benutzerdaten und überträgt sie automatisch an die verschiedenen Logon-Applikationen.

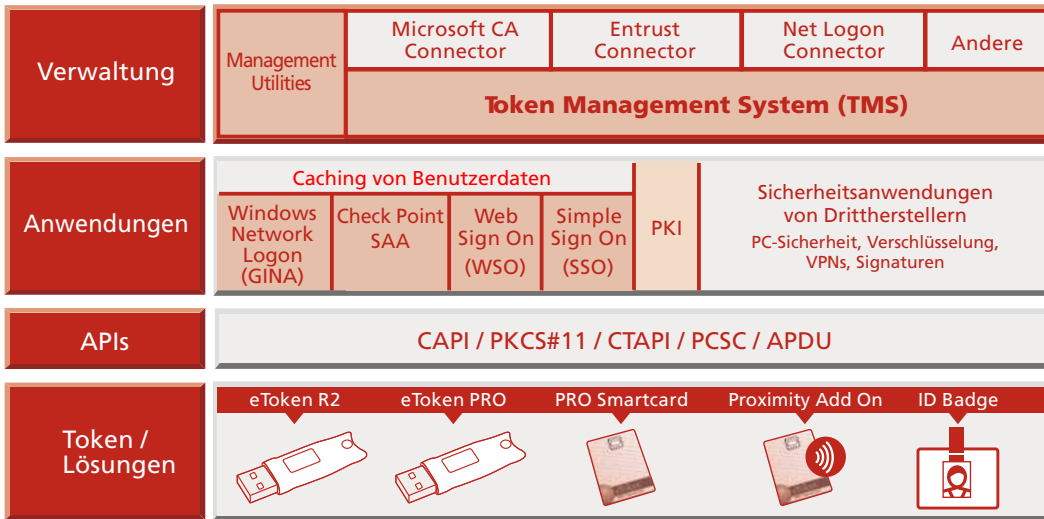
[Signieren von Transaktionen und Dokumenten (Non-Repudiation - Nachvollziehbarkeit von Transaktionen)]

Dank der integrierten PKI-Technologie des eToken können Transaktionen und Dokumente zur Gewährleistung der Authentizität mit digitalen Signaturen versehen werden.



eToken-Produktpalette

eToken bietet eine robuste Architektur für die Integration mit Anwendungen zahlreicher führender Hersteller sowie eine breitgefächerte Palette von Applikationen, die allen unternehmensspezifischen Anforderungen gerecht werden.



eToken - Sicherheitslösungen für Unternehmen

PKI-Lösungen

eToken bietet eine starke zweifache Challenge/Response-Authentifizierung, die auf dem Einsatz von PKI-Schlüsseln und -Zertifikaten beruht. eToken ist mit jeder PKI-fähigen Standardanwendung unter Einsatz von PKCS#11 oder Microsoft CAPI kompatibel. Für zahlreiche Anwendungen, u.a. die im Folgenden aufgeführten, ist volle Unterstützung gewährleistet: Netzwerk-Logon mit Microsoft Smartcard Logon, Novell NMAS oder Entrust Entelligence; Secure Web Access über die Sicherheitsfunktionen von Standard-Webbrowsern mit erweitertem Secure Sockets Layer V3; Remote-Zugriff über VPN-Authentifizierung mit den Systemen von Cisco, Check Point, Microsoft und SSH sowie zahlreicher weiterer führender Hersteller; signierte und verschlüsselte E-Mails gängiger E-Mail-Systeme wie Outlook, Netscape oder Eudora; digitale Signaturen von Dokumenten mit Adobe Acrobat und anderen Systemen.

WSO (Web Simple Sign On)

Die WSO-Applikation von eToken ermöglicht eine sichere Speicherung und Verwaltung der vertraulichen Anmeldedaten, Kennungen und Passwörter. Nach der Eingabe des eToken-Passworts werden alle Anmeldeinformationen automatisch eingetragen. An der Internet-Anwendung müssen keinerlei Änderungen vorgenommen werden und nur berechtigte Anwender erhalten Zugang zu sensiblen Bereichen im Netz.

SSO (Simple Sign On) Lösungen für sicheres Credential Caching

Die SSO-Funktionalität von eToken vereinfacht den Anmeldeprozess für zugangsbeschränkte Anwendungen durch die sichere Speicherung und – wenn erfordert – Angabe der digitalen Identitätsdaten des Benutzers. Darüber hinaus lassen sich deutliche Zeiteinsparungen bei der Verwaltung von Passwörtern und insgesamt Produktivitätssteigerungen der Benutzer erzielen. Die eToken-SSO-Funktionalität ermöglicht das Cachen der Zugriffsdaten für alle standardgemäßen Anmeldemasken unter Windows, wie z.B. Notes, RAS-Dialer, VPN-Clients etc. Der Benutzer muss lediglich ein einziges Passwort für den eToken kennen, um über alle seine vertraulichen Login-Daten verfügen zu können.

eToken für Network Logon

Die eToken-Lösung für die Netzwerk Anmeldung. Diese Lösung bietet eine kosteneffiziente Methode für die Implementierung einer Hardware-basierten Netzwerk-Authentifizierung. Sie unterstützt Domainnamen-Kombinationen, Benutzernamen und Authentifizierungspasswörter sowie PKI-Schlüssel und -Zertifikate. Durch die Zufallsgenerierung von Passwörtern zur Benutzer-Authentifizierung müssen die Benutzer sich diese nicht mehr merken (Unterstützung für Microsoft GINA und Novell Netware).





eToken Management-Lösungen

> TMS (Token Management System)

Das Token Management System von Aladdin bildet die komplette Verwaltungsarchitektur für sämtliche Aspekte der Zuweisung, Implementierung und Personalisierung von Token innerhalb einer Organisation. Auf der Grundlage von offenen Standards und Active Directory konzipiert, ermöglicht das TMS die Verwaltung der Authentifizierungs-Token mithilfe einfacher Plug-Ins, die zentrale Implementierung von Software-Updates sowie das Einspeisen und Löschen von vertraulichen Benutzerdaten. Durch die direkte Verknüpfung mit den vorhandenen Nutzer-Verwaltungssystemen des Unternehmens stellt das TMS eine robuste und gleichzeitig flexible Verbindung zwischen Anwender, Sicherheitsapplikation, dem verwendeten Authentifizierungsgerät und nicht zuletzt den Regeln und Richtlinien des Unternehmens dar.

> eToken-Utilities

Mit den eToken-Utilities steht Netzwerkadministratoren ein Basisset für die Definition und Verwaltung der unternehmensspezifischen Token-Sicherheitsvorgaben zur Verfügung. Zu den Hilfsprogrammen zählen: ein Eigenschaften-Tool, mit dem der Benutzer grundlegende Funktionen der Token-Verwaltung ausführen kann, wie beispielsweise Passwortänderungen, die Anzeige von Daten, etc.; ein Application-Viewer-Tool, mit dem Benutzer und Administratoren alle Profile und Zertifikate auf dem eToken anzeigen können; ein Formatierungs-Tool, mit dessen Hilfe Administratoren den eToken gemäß den speziellen Anforderungen oder Sicherheitsrichtlinien des Unternehmens formatieren können; ein Certificate-Converter-Tool, das für Benutzer und Administratoren gleichermaßen eine einfache Transfermöglichkeit für digitale Zertifikate und Keys zwischen PC und eToken darstellt; ein Password-Quality-Tool zur Änderung der Parameter, anhand derer sich die Qualitätseinstufung eines Passworts von eToken errechnet; und nicht zuletzt ein Vendor-ID-Tool, für das Signieren des eToken mit Unternehmenssignaturen.

eToken Entwicklungs-Tools

Das SDK (Software Developer's Kit) von eToken ermöglicht Softwareentwicklern die Integration der Sicherheitsfunktionalität von eToken in eigene Anwendungen. Das benutzerfreundliche SDK enthält ein Set von standardgemäßen APIs sowie umfassende Dokumentationen und ermöglicht so eine reibungslose Integration mit Fremdanwendungen. Das eToken SDK arbeitet mit Standard-Sicherheitschnittstellen für Windows, Linux, MS CAPI und PKCS#11. Dank spezieller 16-Bit-Bibliotheken wird die Integration mit Sicherheitslösungen für den Boot-Schutz möglich, die vor dem Laden des Betriebssystems eine Anmeldung erfordern.

eToken-fähige Anwendungen von Drittherstellern

eToken kann in eine Vielzahl von Applikationen der führenden Anbieter von Sicherheitstechnologien integriert werden. Mit dem Logo "eToken Enabled" für die Anwendungen unserer Partner wird zum Ausdruck gebracht, dass diese durch die Integration mit dem eToken eine umfassende Sicherheitslösung darstellen.

Partner	Boot-Schutz	Festplatten-verschlüsselung	Datei-/Ordner-Verschlüsselung	E-Mail-Verschlüsselung	PKI-Infrastruktur	Single Sign On	VPN-Client	Internetzugang & Remote Access	Netzwerk/Workstation-Anmeldung
Check Point									
Cisco									
CA									
IBM									
Microsoft									
Novell									
PGP									
Pointsec									
RSA									
SafeBoot									
SAP									
Utimaco									
VeriSign									
Entrust									

Weitere Partner finden Sie unter: <http://www.ealaddin.com/partners>



Der passende eToken

Die verschiedenen Features und Ausführungen des eToken bedeuten für Unternehmen ein Höchstmaß an Flexibilität zur Erfüllung ihrer individuellen Anforderungen. Von USB-Token für PCs und Remote-Umgebungen über Smartcards für die Zugriffssteuerung bis zu Ausweiskarten (ID-Badges), der einfach zu handhabende eToken funktioniert effizient und hat in jeder Tasche Platz. Diese Vorzüge machen ihn zur intelligenten Wahl für alle Unternehmen, die sich in der heutigen, im steten Wandel begriffenen digitalen Welt behaupten wollen. Alle Geräte bieten Unterstützung für die gleichen Sicherheits-Schnittstellen und Interoperabilität sowohl mit den Enterprise- als auch den SDK-Sicherheitslösungen.

eToken Pro (USB)

eToken PRO ist eine USB-Smartcard, die kein Lesegerät erfordert. Das äußerst kosteneffiziente System bietet starke Zweifach-Authentifizierung und ist einfach zu implementieren. Die integrierte Unterstützung für RSA 1024-Bit-Schlüssel ermöglicht die nahtlose Integration des eToken PRO in jede Sicherheits- oder PKI-Infrastruktur.



eToken Pro (Smartcard)

Die eToken Pro Smartcard bietet die gleiche Funktionalität wie die USB-Smartcard, allerdings in der klassischen Form einer Kreditkarte. Die eToken Smartcard kann mit jedem Standard-Lesegerät für Smartcards gelesen werden.



eToken R2

eToken R2 ist als USB-Gerät ideal geeignet für die sichere Speicherung von Private Keys und Zugangsdaten. Durch die integrierte 120-Bit DESX-Verschlüsselungsfunktionalität stellt der R2 die perfekte Kombination aus einfacher Bedienbarkeit und hoher Sicherheit dar.



Proximity Access (Zugangskontrolle für Gebäude)

Die eToken Smartcard ist ideal als ID-Badge mit visueller Identifizierung und bietet höchste Sicherheit sowohl für den Gebäudezugang als auch den Netzwerkzugriff. Die Proximity-Technologie kann sowohl in Token als auch Smartcards integriert werden.



eToken-Zertifizierungen

Der eToken von Aladdin erfüllt die höchsten Anforderungen von Industriestandards und Zertifizierungen.

Produktzertifizierungen:





Technische Spezifikationen

eToken PRO USB

Betriebssysteme	Windows 95(OSR2)/98/98SE/Me/2000/XP sowie Windows NT4.0 SP4 und höher
API- & Standards-Support	PKCS#11 v2.01, CAPI (Microsoft Crypto API), Siemens/Infineon APDU Commands, PC/SC, X.509 v3 Zertifikate, SSL v3, IPSec/IKE
Modelle (nach Speicherkapazität)	16K, 32K
On-Board-Sicherheitsalgorithmen	RSA 1024-Bit, DES, 3DES (Triple DES), SHA1, (MD5 - optional)
Sicherheitsstufe	ITSEC LE4 (Infineon und Siemens), FIPS 140-1 Level 2 & 3
Geschwindigkeit	RSA 1024-Bit-Signatur ca. 1 Sekunde RSA 1024-Bit-Schlüsselgenerierung ca. 11 Sekunden
Maße	47 x 16 x 8 mm (1,85 x 0,63 x 0,31 Zoll)
ISO-Unterstützung	Unterstützung für ISO-Spezifikationen 7816-1 bis 4
Gewicht	5g
Verlustleistung	120mW
Betriebstemperatur	0°C bis 70°C (32°F bis 158°F)
Lagertemperatur	-40°C bis 85°C (-40°F bis 185°F)
Feuchtigkeit	0-100% ohne Kondensation
Wasserdichtigkeit	nach IP X8 IEC 529
Anschluss	USB Typ A (Universal Serial Bus)
Gehäuse	Hartschalenplastik, manipulationssicher
Datensicherung	Mindestens 10 Jahre
Speicherzellen-Rewrites	Mindestens 500.000



eToken PRO Smartcard

Betriebssysteme	Windows 95(OSR2)/98/98SE/Me/2000/XP sowie Windows NT4.0 SP4 und höher
API- & Standards-Support	PKCS#11 v2.01, CAPI (Microsoft Crypto API), Siemens/Infineon APDU Commands, PC/SC, X.509 v3-Zertifikate, SSL v3, IPSec/IKE
Modelle (nach Speicherkapazität)	32K
On-Board-Sicherheitsalgorithmen	RSA 1024-Bit, DES, 3DES (Triple DES), SHA1, (MD5 - optional)
Sicherheitsstufe	ITSEC LE4 Smartcard Security Certification (Infineon und Siemens)
Geschwindigkeit	RSA 1024-Bit-Signatur ca. 1 Sekunde RSA 1024-Bit-Schlüsselgenerierung ca. 11 Sekunden
ISO-Unterstützung	Unterstützung für ISO-Spezifikationen 7816 1 bis 4
Datensicherung	Mindestens 10 Jahre
Speicherzellen-Rewrites	Mindestens 500.000

eToken R2 USB

Betriebssysteme	Windows 95(OSR2)/98/98SE/Me/2000/XP, Windows NT4.0 SP4 und höher
API- & Standards-Support	PKCS#11 v2.01, CAPI (Microsoft Crypto API), PC/SC, X.509 v3-Zertifikate, SSL v3, IPSec/IKE
Modelle (nach Speicherkapazität)	16K & 32K
On-Board-Sicherheitsalgorithmen	DES-X 120-Bit
Sicherheitsstufe des Smartcard Chip	Gesicherter und verschlüsselter EEPROM-Speicherchip
Maße	47 x 16 x 8 mm (1,85 x 0,63 x 0,31 Zoll)
Gewicht	5g
Verlustleistung	120mW
Betriebstemperatur	0°C bis 70°C (32°F bis 158°F)
Lagertemperatur	-40°C bis 85°C (-40°F bis 185°F)
Feuchtigkeit	0-100% ohne Kondensation
Wasserdichtigkeit	nach IP X8 IEC 529
Verbindung	USB Typ A (Universal Serial Bus)
Gehäuse	Hartschalenplastik, manipulationssicher
Datensicherung	Mindestens 10 Jahre
Speicherzellen-Rewrites	Mindestens 100.000

eToken

Der eToken repräsentiert eine portable und robuste Methode zur Speicherung und Übermittlung von Berechtigungsnachweisen und digitalen Zertifikaten gemäß einer starken Zwei-Faktor-Authentifizierung. Das USB-basierte Smartcard-System von der Größe eines Hausschlüssels gibt es in den Versionen PRO (mit einer dem Signaturgesetz konformen Sicherheitsarchitektur und einem Infineon Smartcard-Chip) und R2 (stellt dem Betriebssystem die Funktionalität einer Smartcard zur Verfügung, das Secret-File wird hier nicht im eToken erstellt, sondern sicher gespeichert). Das Lösungspaket eToken Enterprise ist ein „Out-of-the-box“ Solutionset für mobile Authentisierung, RemoteAccess und die Speicherung digitaler Zertifikate. Mit eToken Enterprise können kostengünstig typische Smartcard-Anwendungen für Netzwerk- und eBusiness Sicherheits-Lösungen realisiert werden. Durch die Unterstützung von offenen, nicht-proprietären Standards wie Microsoft CAPI & PKCS#11 verläuft die Integration in Sicherheitsapplikationen schnell und reibungslos.

Zertifizierungen



Weitere Information finden Sie unter: www.Aladdin.de

Germany	T: +49-89-89-42-21- 0	F: +49-89-89-42-21-40	info.etoken@Aladdin.de
International	T: +972-3-636-2222	F: +972-3-537-5796	info.isr@eAladdin.com
North America	T: +1-800-562-2543, 847-808-0300	F: 212-564-3377	info.us@eAladdin.com
UK	T: +44-1753-622-266	F: +44-1753-622262	info.uk@aldn.com
Benelux	T: +31-30-6880-800	F: +31-30-688-0700	info@eAladdin.nl
France	T: +33-1-41-37-70-30	F: +33-1-41-37-70-39	info@Aladdin.fr
Japan	T: +81-42-660-7191	F: +81-426-60-7194	info@eAladdin.co.jp
Spain	T: +34-91-375- 9900	F: +34-91-754-2671	info.es@ealaddin.com