

“

Der Verbreitungsgrad von USB Authentisierungs-Tokens wird bis zum Jahr 2008 mit dem der herkömmlichen Tokens gleichgezogen haben.

IDC, 2004

”

eToken™
YOUR KEY TO eSECURITY



*Die ultimative
Authentisierungs-Technologie*

 Aladdin®
SECURING THE GLOBAL VILLAGE

⊕ Das Paradigma der Authentisierungspasswörter

In der heutigen Geschäftswelt sind die Sicherheit im Allgemeinen – und die Benutzerauthentisierung im Besonderen – zentrale Voraussetzungen für die Geschäftstätigkeit und den Schutz vertraulicher Firmendaten. Mit der Implementierung leistungsstarker Lösungen für die Benutzerauthentisierung verbessern Sie die Produktivität Ihrer Kunden, Partner und Mitarbeiter, die Ihre Geschäftsanwendungen standortunabhängig nutzen können – im Büro, zu Hause und unterwegs.

In einer Geschäftswelt, die von den Unternehmen die Einhaltung wichtiger branchenüblicher Normen abverlangt, wie etwa HIPAA, FDA, Sarbanes Oxley und Basel II, bildet die leistungsfähige Benutzerauthentisierung eine zentrale Voraussetzung für den Schutz von Daten und Privatsphäre.

Passwörter, bisher das wichtigste Werkzeug zur Authentisierung 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 sicher gestellt 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.

“Passwörter bleiben eine grundlegende Schwachstelle in der Sicherheit, auch wenn die Richtlinien für die Passwortverwendung äußerst streng sind.”

“Passwörter und PINs sollten zusammen mit einer anderen Authentisierungsmethode verwendet werden, wie etwa ein Hardware-Token.”

Gartner-Studie
"Assess Authentication Methods for Strong System Security",
August 2004

AUTHENTISIERUNG

⊕ eToken - der Organizer für die digitale Identität

Mit dem eToken von Aladdin lassen sich starke Authentisierung und ein einfaches Passwort Management realisieren. Die Besonderheit dieser Lösungen ist:

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

Der eToken von Aladdin ist ein portables, kostengünstiges USB-Device zur Authentisierung 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 Authentisierungsprozesse dar, da er Passwörter, PKI-Schlüssel und digitale Zertifikate sicher speichert. Mit dem eToken sind die Passwörter des Anwenders nie der risikoreichen Umgebung des PCs ausgesetzt.

Der eToken bietet eine starke 2-Faktor-Authentisierung



**Etwas, was Sie besitzen –
der eToken**

**Etwas, was Sie wissen –
das eToken Passwort**

⊕ eToken Lösungen

LÖSUNGEN

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.



Sicherer Netzwerkzugang

Netzwerk-Anmeldung

eToken ist ein leistungsfähiges System für die Authentisierung von Benutzern, die sich in geschützten Bereichen des Netzwerks anmelden. Er ermöglicht das Logon mithilfe von Smartcards und unterstützt sowohl die zertifikatbasierte Anmeldung, als auch den GINA-Mechanismus von Microsoft durch die Speicherung der Passwörter und Zugangsdaten der Benutzer.

VPN Security (Sicherer Remote Access)

Der eToken ermöglicht Unternehmen eine effektive Authentisierung ihrer Anwender, wenn diese von außerhalb auf das Firmennetzwerk zugreifen und bietet dabei nahtlose Integration in die gängigen VPN-Systeme. Unterstützt werden mehrere VPN-Authentisierungsarten einschließlich Einmal-Passwort (OTP) und digitale Zertifikate.

Web Access

eToken ermöglicht eine starke Benutzer-Authentisierung für den Zugriff auf geschützte Web-Ressourcen sowie für digitale Signaturen sensibler Daten. Der eToken unterstützt verschiedenartige Authentisierungsarten einschließlich Einmal-Passwörter (OTP) und digitale Zertifikate.

Datensicherheit

PC-Boot-Schutz, Datei- & Datenverschlüsselung

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

Sichere eMail

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

Digitale Signaturen (Non-repudiation)

Mit einer PKI-Technologie können Sie mit dem eToken Dokumente digital signieren und so die Echtheit der übertragenen Daten garantieren.

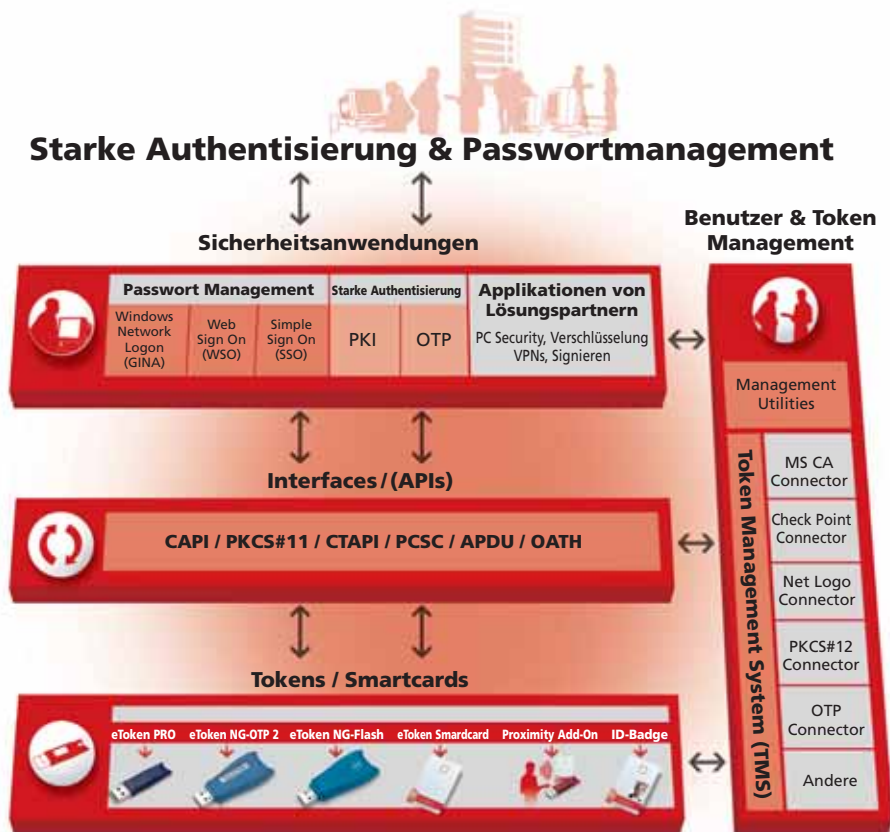


Passwort Management

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 Anmeldefenster der Online-Accounts.

⊕ eToken-Produktpalette

Der 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-Sicherheitsanwendungen

Zuverlässige Authentisierung

Die zuverlässigen eToken-Anwendungen für die Benutzerauthentisierung gewährleisten Leistungsstärke und Flexibilität für den sicheren Zugriff auf die digitalen Ressourcen Ihres Unternehmens. eToken bietet zuverlässige Benutzerauthentisierung durch die Kombination Ihres eigenen eToken (den Sie haben) und Ihres eToken-Passworts (das Sie kennen).

Public Key Infrastructure (PKI)

Mit der PKI-Funktionalität von eToken können Sie sich authentisieren sowie digitale Daten verschlüsseln und mit einer Signatur versehen. Sie können damit sicher auf das Unternehmensnetzwerk zugreifen, persönliche Dateien schützen, E-Commerce-Transaktionen ausführen, E-Mails mit einer digitalen Signatur versehen und weitere Funktionen nutzen - ohne auf Mobilität und zuverlässigen Schutz verzichten zu müssen.



Mit eToken können Sie PKI-basierte, leistungsstarke Lösungen für die Benutzerauthentisierung und Verschlüsselung problemlos und flexibel implementieren, indem Sie Private Schlüssel generieren und sie mit den digitalen Zertifikaten auf dem Token speichern.

Verstärken Sie Ihre PKI basierte Lösung



eToken PKI-Funktionen garantieren eine robuste Verwaltung auf Unternehmensebene

Das Aladdin Token Management System (TMS) ermöglicht eine umfassende Implementierung und die Lebensdauer umspannende Verwaltung von Benutzer-Token und den damit verbundenen PKI-Lösungen.

One-Time-Password (OTP)-Authentisierung

Die eToken One-Time Password (OTP)-Authentisierung ermöglicht einen sicheren Logon im Netzwerk durch die Verwendung von Einmal-Passwörtern. So können Sie sich von jedem beliebigen Standort aus sicher im Netzwerk anmelden, ohne auf eine Client-Software oder eine USB-Verbindung zurückgreifen zu müssen.

eToken NG-OTP 2 bietet umfassende, leistungsfähige Funktionen für die Authentisierung und Passwortverwaltung sowohl am USB-Port angeschlossen, als auch ohne direkte Verbindung zum Computer auf One-Time Password Basis.

Die eToken OTP-Architektur beinhaltet den eToken RADIUS-Server für die Back-End OTP-Authentisierung. Dies ermöglicht eine Integration mit allen RADIUS Gateways/Applikationen. Dazu gehören die gängigen VPN-Lösungen, Webzugriff-Lösungen und mehr. Der eToken RADIUS-Server benutzt die Active Directory-Infrastruktur (mittels Aladdin TMS) für Benutzerinformationen.



Die eToken OTP-Authentisierung garantiert eine robuste Verwaltung auf Unternehmensebene

Das Aladdin Token Management System (TMS) ermöglicht eine umfassende Implementierung und die Lebensdauer umspannende Verwaltung von Benutzer-Token und den damit verbundenen OTP-Authentisierungslösungen.

Passwortverwaltung

eToken bietet eine umfassende Palette benutzerfreundlicher Anwendungen für die Passwortverwaltung. Diese eToken-Anwendungen verwenden die Reduced Sign-On (RSO) Technologie, dank der alle vertraulichen Anmeldedaten sicher auf einem einzigen eToken gespeichert und verwaltet werden können. Es ist nicht mehr erforderlich, die Fülle an Passwörtern für diverse Anwendungen und Konten präsent zu haben, Sie benötigen nur noch ein einziges eToken-Passwort.

SSO (Simple Sign On)

Die SSO-Funktionalität von eToken vereinfacht den Anmeldeprozess zu Windows-basierten Anwendungen durch die sichere Speicherung der persönlichen Zugangsdaten auf der eToken Smartcard und das automatische Einfüllen dieser Daten bei der Anmeldung. Sie müssen nur den eToken am Rechner anschließen und Ihr eToken Passwort eingeben. Dann haben Sie Zugriff auf alle Ihre Anwendungen.

Die eToken-SSO-Funktionalität ermöglicht das sichere Speichern der Zugriffsdaten für alle standardgemäßen Anmelde-masken unter Windows, wie z.B. Notes, MS Outlook, 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 SSO garantiert eine robuste Verwaltung auf Unternehmensebene

eToken SSO ist nicht nur ein zuverlässiges Werkzeug für sichere und benutzerfreundliche Authentisierung, sondern bietet darüber hinaus auch intuitive, einfach anzuwendende Tools, mit denen dank einer zentralen Benutzerverwaltung stets höchste Sicherheit beim Zugriff auf Ihre Unternehmenssysteme gewährleistet ist.

eToken SSO ist vollständig in das Aladdin Token Management System (TMS) integriert, welches Administratoren ein Komplettpaket von Dienstprogrammen für die Token-Verwaltung zur Verfügung stellt. Hierzu zählen die Einrichtung und Deaktivierung des eToken, Self-Service-Funktionen für das Zurücksetzen von eToken Benutzerpasswörtern sowie Backup und Wiederherstellung von Benutzerdaten (Credentials) bei verlorenen oder beschädigten Token.

WSO (Web Simple Sign On)

Mit eToken WSO lassen sich einfach, praktisch und sicher alle Passwörter des Anwenders für Web Logon und Access direkt von Web-Seiten speichern. Ein Anwender kann ein beliebiges Passwort eingeben, egal wie lange und komplex, und muss sich keine Gedanken darüber machen, sich daran zu erinnern. Die Passwörter können nicht ausgelesen werden, die Informationen sind geschützt und das Netzwerk ist sicher, denn nur autorisierte Benutzer haben Zugang.

Der eToken dient als sicherer Container für Passwörter, PIN-Nummern, Kontonummern und -details, Kreditkartendetails, URLs und Ablaufdaten. Mit eToken WSO haben Anwender sofortigen Zugang zu all ihren Internet Web Accounts. Die gespeicherten Seiten werden erkannt und die benötigten Informationen direkt aus dem eToken ausgelesen und automatisch in die entsprechenden Webformulare übertragen.



Network Logon (Microsoft GINA API)

eToken Network-Logon bietet eine kosteneffektive und sichere Methode für die Implementierung einer Token-basierten starken Authentisierung am Netzwerk. Der eToken speichert Benutzername, Passwort und Domainname für den Netzwerkzugriff und kommuniziert mit dem Microsoft Network-Logon (GINA-Mechanismus). Anwender müssen nur den eToken anschließen und das dazugehörige Passwort eingeben, um auf das Netzwerk zugreifen zu können.



eToken Network Logon garantiert eine robuste Verwaltung auf Unternehmensebene

eToken Network Logon ist vollständig in das Aladdin Token Management System (TMS) integriert und ermöglicht eine umfassende Implementierung und die Lebensdauer umspannende Verwaltung von Benutzer-Token und den damit verbundenen eToken-Lösungen für die Netzwerkanmeldung.

Identitäts- und Token-Management

Token Management System (TMS)

Das Token Management System (TMS) von Aladdin ist ein leistungsstarkes Verwaltungssystem für die Implementierung, Zuweisung und Verwaltung von Token, Smartcards und Mitarbeiterausweisen in einem Unternehmen. Das Token Management System unterstützt eine Vielzahl von Sicherheitsanwendungen wie Netzwerkanmeldung, VPN, Internetzugriff, OTP-Authentisierung, sicheres E-Mail, Datenverschlüsselung und vieles mehr.

Eine wesentliche Herausforderung für die Sicherheitssysteme eines Unternehmens ist es, Benutzer, deren Sicherheitsgeräte, die Richtlinien des Unternehmens und die damit verbundenen Sicherheitsanwendungen gleichermaßen zu berücksichtigen. Aladdin TMS ist eine einzigartige Lösung, die all diese Elemente in einem einzigen automatischen und vollständig konfigurierbaren System zusammen bringt.

TMS hält leistungsstarke Tools bereit, mit denen alle Aspekte der Token-Verwaltung während ihrer gesamten Lebensdauer kostengünstig und pragmatisch angegangen werden können. Die TMS-Möglichkeiten umfassen das Einrichten und Deaktivieren von Tokens, ein Web-Interface für die persönliche Token-Verwaltung und Passwort-Reset, automatische Backups, das Wiederherstellen von vertraulichen Benutzerinformationen, die Handhabung verlorener oder beschädigter Tokens und mehr.

TMS setzt auf einer offenen Standardarchitektur auf, die auf konfigurierbaren Konnektoren basiert, mit der sich eine Vielzahl unterschiedlicher Sicherheitsanwendungen einbinden lassen. Durch die nahtlose Integration von TMS in das Active Directory (oder im Betrieb als Stand-Alone-Anwendung, z.B. Shadow-Domain-Modus) können Sie Token im ganzen Unternehmen einfach verwalten und die Token-Verwaltung transparent an den Regelungen des Unternehmens ausrichten.

TMS enthält ein robustes SDK für die Integration und Verwaltung der Sicherheitsanwendungen von Drittherstellern.

Unternehmensrichtlinien

- Zentralisierte Personalisierung
- User Repository
- Gruppenrichtlinien
- Token Bestandsaufnahme
- Backup & Wiederherstellen von Profilen



Active Directory

Token Management System

WEB/ LAN

MS CA

OTP-Authentisierung

Network Logon

Weitere

Sicherheitsanwendungen

Anwender & Devices



Weitere Informationen über die eToken-Sicherheitsanwendungen finden Sie unter:
<http://www.Aladdin.com/eToken>

⊕ eToken-fähige Anwendungen von Lösungspartnern


















































eToken SDK

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 standardmäßigen APIs sowie umfassende Dokumentationen und ermöglicht so eine reibungslose Integration in Anwendungen von Lösungspartnern.

Das eToken SDK arbeitet mit Standardschnittstellen und bietet volle Unterstützung für Windows 98 / NT 4.0 / ME / XP und 2000 Betriebssysteme und unterstützt folgende Standards: PC/SC, PKCS#11, X509 v3 Zertifikate, Microsoft Crypto API, RAS/Radius/PAP/CHAP, IPSec/IKE, SSLv3. Daneben sind auch SDKs für Linux und Mac OS X erhältlich.

eToken Lösungspartner

eToken kann in eine Vielzahl von Applikationen integriert werden, wie zum Beispiel Anwendungen für sichere Benutzer-Identifizierung und Authentisierung, für Digitale Signaturen, für Ver- und Entschlüsseln von vertraulichen Informationen. Das eToken SDK enthält standardmäßige APIs. Die "eToken enabled" Zertifizierung für Anwendungen unserer Partner gewährleistet ein Höchstmaß an Interoperabilität zwischen der Partnerlösung und der eToken-Produktfamilie.

Partner*	Boot Protection & Disk Encryption	E-Mail Protection	CA/PKI	Single Sign On	VPN Remote Access	Web & Remote	Network/ Workstation Logon	Weitere
 Check Point								
 Cisco								
 CITRIX								
 CA								
 SafeBoot								
 DocuWare								elektr. Signatur
 Entrust								
 fis								Proximity/RFID
 IBM								
 Microsoft								
 Novell								
 PGP								
 pointsec								
 RSA								
 SAP								
 utimaco								
 VeriSign								

Weitere Informationen finden Sie unter <http://www.Aladdin.com/partners>

*Ein Auszug

+ 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 kosten-effiziente System bietet starke Zwei-Faktor-Authentisierung und ist einfach zu implementieren. Der eToken PRO kann nahtlos in jede Sicherheits- oder PKI-Infrastruktur integriert werden.



eToken NG-OTP 2 (One Time Password)

Der eToken NG-OTP 2 bietet mit einer Hardware die Technologie einer Smartcard UND eines One-Time Password (OTP). Er kann einfach rechnerunabhängig, stand-alone (OTP) eingesetzt oder direkt am USB-Port angeschlossen genutzt werden.

Weitere Features siehe eToken PRO.



eToken NG-Flash

Der eToken NG-Flash bietet die gleiche Funktionalität wie der eToken Pro, verfügt aber zusätzlich über einen Flash-Speicher, der den mobilen Austausch von Daten und das direkte Laden von vorinstallierten Applikationen (Autorun) ermöglicht.



eToken PRO (Smartcard)

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



Transponder Chip-Technologie (RFID)

Die eToken Smartcard ist ideal als ID-Badge mit visueller Identifizierung und bietet höchste Sicherheit sowohl für den Gebäudezugang, als auch den Netzwerkzugriff. Die Transponder Chip-Technologie (RFID) kann in alle eToken Bauformen integriert werden.



+ eToken-Produktzertifizierungen

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



Novell

Entrust Ready



SAP Certified Integration



IBM



RSA Keon



Cisco Compatible

⊕ Technische Spezifikationen

eToken PRO USB

• Betriebssysteme	Windows 95(OSR2)/98/98SE/Me/2000/XP sowie Windows NT4.0 SP4 und höher, Linux, Mac OS X
• 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)	32 KB, 64 KB
• On-Board-Sicherheitsalgorithmen	RSA 1024/2048-Bit, 3DES (Triple DES), SHA1, (optional MD5)
• Sicherheitsstufe	ITSEC LE4 Hoch***, CC EAL 5+*, CC EAL 4+**, FIPS 140-1 Level 2 & 3
• ISO-Unterstützung	Unterstützung für ISO-Spezifikationen 7816-1 bis 4
• 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 NG-OTP 2

• Betriebssysteme	Windows 95(OSR2)/98/98SE/Me/2000/XP, Windows NT4.0 SP6 und höher, Linux, Mac OS X
• 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)	32 KB, 64KB
• On-Board-Sicherheitsalgorithmen	RSA 1024/2048-Bit, 3DES (Triple DES), SHA1, (optional MD5), HMAC-SHA1
• OTP Sicherheitsalgorithmus	VeriSign OATH compliance basierend auf HMAC/SHA1
• Sicherheitsstufe	ITSEC LE4 Hoch***, CC EAL 5+*, CC EAL 4+**
• ISO-Unterstützung	Unterstützung für ISO-Spezifikationen 7816-1 bis 4
• Verbindung	USB Typ A (Universal Serial Bus)
• Gehäuse	Hartschalenplastik, manipulationssicher
• Lebensdauer der Batterie	Erzeugung von mindestens 14000 One-Time-Passwörtern / 7 Jahre, auswechselbar
• Datensicherung	Mindestens 10 Jahre
• Speicherzellen-Rewrites	Mindestens 100.000

eToken NG-Flash

• Betriebssysteme	Windows /2000/XP
• 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
• Speicherkapazität	64KB
• Flash Speicher	128 MB, 512 MB, 1 GB
• On-Board-Sicherheitsalgorithmen	RSA 1024/2048-Bit, 3DES (Triple DES), SHA1, (optional MD5)
• Sicherheitsstufe	ITSEC LE4 Hoch***, CC EAL 5+*, CC EAL 4+**
• ISO-Unterstützung	Unterstützung für ISO-Spezifikationen 7816-1 bis 4
• Verbindung	USB Typ A (Universal Serial Bus)
• Gehäuse	Hartschalenplastik, manipulationssicher
• Datensicherung	Mindestens 10 Jahre
• Speicherzellen-Rewrites	Mindestens 100.000

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)	32 KB, 64 KB
• On-Board-Sicherheitsalgorithmen	RSA 1024/2048-Bit, 3DES (Triple DES), SHA1, (optional MD5)
• Sicherheitsstufe	ITSEC LE4 Hoch***, CC EAL 5+*, CC EAL 4+** Smartcard Security Certification
• ISO-Unterstützung	Unterstützung für ISO-Spezifikationen 7816 1 bis 4
• Datensicherung	Mindestens 10 Jahre
• Speicherzellen-Rewrites	Mindestens 500.000

*Infineon Smartcard Chip **Siemens CardOS

+ Über Aladdin

Aladdin Knowledge Systems (NASDAQ: ALDN) ist weltweit einer der führenden Anbieter im Bereich IT-Security und entwickelt und vertreibt auf Hard- und Software basierende Produkte und Komplettlösungen für die Bereiche Software- und Internet-Sicherheit. Das Unternehmen ist eine 100%ige Tochter der Aladdin Knowledge Systems Ltd. in Tel Aviv/ Israel. Aladdin Knowledge Systems Ltd. unterhält zehn internationale Niederlassungen und ein Vertriebsnetz mit mehr als 50 Distributoren.

Jetzt kostenlos testen! Weitere Informationen
und Bestellformular finden sie unter:
www.aladdin.de/etokentest/



Weitere Informationen erhalten Sie unter www.Aladdin.de

Deutschland	T: +49-89-894 221-11	F: +49-89-894 221-40
North America	T: 1-800-562-2543, 1-847-818-3800	F: 1-847-818-3810
International	T: +972-3-636-2222	F: +972-3-537-5796
UK	T: +44-1753-622-266	F: +44-1753-622-262
Benelux	T: +31-30-688-0800	F: +31-30-688-0700
France	T: +33-1-41-37-70-30	F: +33-1-41-37-70-39
Spain	T: +34-91-375-99-00	F: +34-91-754-26-71
Israel	T: +972-3-636-2222	F: +972-3-537-5796
Asia Pacific	T: +852-2166-8605	F: +852-2166-8999
Japan	T: +81-426-607-191	F: +81-426-607-194