

iKey™ 3000 Series

Erweiterte Sicherheit



Erweiterte Sicherheit und Portabilität für Ihre Digitale Identität

Verbesserung der Sicherheit von Public Key Infrastruktur Sicherheit durch Benutzer Authentisierung

Internetbasierende Technologien ermöglichen die elektronische Automatisierung von Transaktionen und Geschäftsprozessen. Leider sind viele dieser Infrastrukturen angreifbar, wenn sie sich nur auf traditionelle Benutzernamen und Passwörter zur Authentisierung/Logon verlassen. Neben der vergleichsweise schwachen Sicherheit sind Passwörter auch noch teuer in der Haltung und erlauben keine verlässliche Auditing Informationen, wie sie z.Bsp. für elektronische Transaktionen benötigt werden.

PKIs bringen neue Herausforderungen; wo können private Schlüssel und digitale Zertifikate sicher erzeugt und gespeichert werden und wie können diese Informationen portabel gemacht werden.

Um diese Anforderungen zu erfüllen, hat Rainbow Technologies den iKey 3000 entwickelt. Als sicherer, portabler, Zwei-Faktoren-Authentisierungs USB-Token hilft der iKey3000 dabei die Identität eines Benutzers auf Basis von etwas was der Benutzer besitzt (einen iKey) und etwas was der Benutzer kennt (PIN) zu bestätigen.

Verbesserung der Sicherheit einer PKI

Der iKey 3000 funktioniert mit allen grösseren Anbietern von PKI Systemen und ergänzt diese um einen Zwei-Faktoren-Authentisierung-Token zur Speicherung von Digitalen Identitäten. Der iKey 3000 erhöht die Sicherheit von Public Key Infrastruktur Systemen (PKIs) und Anwendungen durch Bereitstellung von on-board Schlüsselerzeugung und sichere Speicherung von X.509 Zertifikaten.

Einfache Anwendung

- Der iKey 3000 passt in einen vorhandenen USB Port
- Es wird kein separater SmartCard Leser benötigt
- Stecken Sie einfach den iKey ein und geben Sie Ihre PIN zur Anmeldung ein
- Benutzer brauchen sich keine komplexen Passwörter zu merken
- Fehlversuchszähler sichert den Token gegen Angriffe
- Über PUK für den Administrator kann der Fehlversuchszähler zurückgesetzt werden

Der iKey 3000 ist ein sicherer, leistungsfähiger und portabler Zwei-Faktoren Authentisierungs USB-Token der die Sicherheit von Public Key Infrastrukturen (PKI) und anderen hochsicheren Anwendungen erhöht. Der iKey 3000 unterstützt im Besonderen die Bedürfnisse von PKIs und digitaler Signaturen durch sichere Ablage von X.509-Zertifikaten und Durchführung aller Operationen zur digitalen Authentisierung und Signatur auf dem Token.

Verbessert die Sicherheit von Windows Authentisierungen

Der iKey 3000 integriert direkt mit den Windows 2000/2003 Zertifikatsdiensten (PKI) und der Windows Smart-Card-Anmeldung. Er ermöglicht starke Zwei-Faktoren-Authentisierung die für Windows 2000 Dienste und Anwendungen verwendet werden kann:

- Sichere Benutzer-Authentisierung an die Windows 2000/2003 Domäne
- Sichere Benutzer Authentisierung für Windows 2000 oder XP Clients bei Anmeldung vom Firmennetzwerk
- Sicherer VPN Client Logon für den Remote Zugriff auf das Firmennetzwerk
- Sichere Mail Signatur und Verschlüsselung mit MS Outlook
- Mail Verschlüsselung mit Microsoft Outlook

Verbesserte Sicherheit bei Digitalen Signaturen

Der iKey 3000 kann drei oder mehr Schlüsselpaare sicher speichern und unterstützt in Kombination mit der StarCERT Anwendung mehrfache PINs um die Anforderungen der Europäischen Signaturrechtlinie und des Deutschen Signaturgesetzes zu erfüllen. Mit dem iKey 3000 können alle Operationen zur digitalen Authentisierung und Signatur on-board ausgeführt werden.

Durch Verwendung des Giesecke & Devrient STARCOS Betriebssystemes wird eine Vielzahl von bestehenden Anwendungen unterstützt. Mit der Unterstützung von Nicht-Windows Plattformen wie Linux, Mac OS X und Solaris können nun auch gemischte Umgebungen PKI basierte Systeme und Anwendungen nutzen. Die Middleware ist bereits in 11 Sprachen erhältlich, weitere - auch nicht-europäische - werden zukünftig unterstützt.



Vorteile Smart Key basierenden PKIs

Verbesserungen

- Der Austausch von Passwörtern zwischen Benutzern ist nicht mehr möglich
- Der iKey 3000 kann die Schlüsselerzeugung und Anwendungssignaturen direkt auf dem Token durchführen
- Der private Schlüssel des Benutzers verlässt niemals den iKey

Geringere TCO durch minimierte Kosten für Verteilung und Betrieb

- Keine zusätzlichen Kartenleser müssen beschafft, verteilt und unterstützt werden
- Rückgang von Kosten für Administrations- und Benutzer-Passwortverwaltung

iKey 3000 Eigenschaften

Hardware-PKI

- Kryptographischer Generator für schnelle RSA-basierende Schlüsselpaarerzeugung
- Signatur auf dem Token
- 32k bytes EEPROM (bis zu 25k Bytes sind für Zertifikate und Schlüsselspeicherung verfügbar)

Lieferumfang

- iKey 3000 USB Token
- CD-ROM mit iKey 3000 Software und Dokumentation

Zertifizierungen

- ISO 7816-3 und 7816-4 kompatibel
- FCC und CE zertifiziert
- ITSEC E4 hoch zertifizierter Chip und Kartenbetriebssystem

Software

- AET SafeSign Software
- Unterstützte Schnittstellen
 - Microsoft CAPI (CSP)
 - PKCS#11 (V2.11), PKCS#12, PKCS#15
 - Microsoft PC/SC
- Mehrsprachig, 11 europäische Sprachen, weitere in Vorbereitung

Betriebssystem Unterstützung

- Microsoft Windows 2000/XP Prof./ME/98/NT (Rainbow USB Treiber auf CD-ROM)
- USB 1.1 & 2.0 kompatibel
- Windows Plug & Play Unterstützung
- Linux (Red Hat 8.0, 9.0; SuSe 8.1; Mandrake 9.1)
- Mac OS X
- Solaris

Anwendungen

Microsoft Windows

- Sichere Benutzer Authentisierung für Windows 2000/XP Arbeitsstationen an Windows 2000/2003 Domänen, Netzwerken und VPNs
- Sichere Mail mit Microsoft Outlook (Signatur und Verschlüsselung)

PKI Systeme und Anwendungen

- | | | |
|---|---|---|
| <ul style="list-style-type: none">• Baltimore (SelectAccess, UniCERT)• Cisco Systems (VPN Client)• Checkpoint (Firewall-1 NG)• Computer Associates (eTrust)• GlobalSign | <ul style="list-style-type: none">• NCP (VPN)• NetScreen• Netscape/Planet• PGP• RSA (SecurID, Keon) | <ul style="list-style-type: none">• SafeNet• Utimaco (SafeGuard)• VeriSign and affiliates (Certificates)• WISEKey (Zertifikat) |
|---|---|---|

In Zusammenarbeit mit



Giesecke & Devrient



Making Security Simple

www.de.rainbow.com or www.rainbow.com

Corporate: 50 Technology Drive, Irvine, CA 92618 USA

Tel: +1 949 450 7300 or +1 800 852 8569 eMail: sales@rainbow.com

Deutschland

Tel.: 01803 7246269 (R-A-I-N-B-O-W)

Fax: 01803 000 924

Mail: sales@de.rainbow.com