

**SCHÜTZEN SIE IHRE MOBILEN  
DATEN MIT AES 256-BIT  
VERSCHLÜSSELUNG NACH  
MILITÄRISCHEM STANDARD**

**Nutzen Sie die Fernwartung  
für alle USB Flash Drives**

**Verhindern Sie Schäden  
durch USB-Malware**



### Intelligente, selbstverteidigende und sichere Datenspeicherung

Der IronKey Enterprise S200 kombiniert den AES 256-Bit hardwareverschlüsselten IronKey USB Flash Drive mit dem IronKey Enterprise Management Service. So können Sie per Fernwartung beliebig viele IronKeys verwalten und einheitliche Policies zuordnen bzw. diese im Bedarfsfall anpassen. Das integrierte Authentifizierungsverfahren ermöglicht Ihrem Unternehmen, IronKey USB Flash Drives als skalierbare Plattform für sicheren Fernzugriff und virtuelle Desktops einzusetzen.

### Der sicherste USB-Flash Drive

Alle Benutzerdaten auf einem IronKey Enterprise USB Flash Drive werden mit Hochgeschwindigkeit im CBC-Modus per AES 256-bit Hardwareverschlüsselung codiert. Diesen starken Algorithmus setzen auch das U.S.-Militär und U.S.-Regierungsbehörden zum Schutz von streng geheimen Daten ein. Sollte der IronKey in unberechtigte Hände fallen, wird nach einer in den allgemeinen Policies voreingestellten Anzahl von Zugriffsversuchen der USB-Stick gesperrt und alle Daten werden sicher und unwiederbringlich vernichtet.

### Der einzige USB Flash Drive mit FIPS 140-2 Level 3 Standard

IronKey USB Flash Drives entsprechen offiziell den von der US-Regierung vorgeschriebenen strengen Sicherheitsanforderungen nach FIPS 140-2 Level 3. Dazu gehören zahlreiche Schutzmechanismen, darunter die vollständige Versiegelung der Chips in einem speziellen Epoxidharz, eine leistungsfähige Schlüsselverwaltung und andere wirksame Vorkehrungen zum Schutz vor Manipulationen.

### Aktiver Schutz vor Malware

Böswillige Codes und Viren, die durch Wechseldatenträger verbreitet werden, infizieren jährlich Millionen von Computern. Die mehrstufigen aktiven Sicherungsfunktionen von IronKey stoppen die Verbreitung von Malware und Würmern. Proaktive Schutzmechanismen verhindern Änderungen an Auto-Run-Dateien und ermöglichen es dem Administrator, per Fernwartung zu kontrollieren, auf welchen Computern IronKey Flash Drives genutzt werden dürfen. Ein vorinstallierter Malware-Scanner schützt den USB-Stick, wenn Dateien bewegt oder geöffnet werden. Zusätzlich verhindert ein Read-Only-Modus, dass Malware von einem infizierten Host-PC auf den Flash Drive überspringt.

### Zentrale Konfiguration der Flash Drives per Fernwartung und Vergabe allgemeiner Policies Online

Der IronKey Enterprise Remote Management Service ermöglicht es Ihnen, beliebig viele IronKeys zu verwalten und spezifische Policies – zum Beispiel Passwortstärke, maximale Anzahl von Passwort-Eingabeversuchen und Zugang zu vorinstallierten Anwendungen – einzustellen und ggf. anzupassen.

### Abschaltung von verloren gegangen und gestohlenen USB Flash Drives per Fernzugriff

Eine Hauptkomponente des IronKey Enterprise Remote Management Service ist der „Silver Bullet Service“. Dieser ermöglicht es Ihnen, den Zugriff auf IronKeys Ihres Unternehmens zu verhindern, die in falsche Hände geraten sind, z. B. durch Verlust, Diebstahl und ehemalige oder nicht vertrauenswürdige Angestellte.

- Blockieren – verhindert den Zugriff auf Daten auf dem USB-Stick, bis sein Status geklärt werden kann
- Abschalten – verweigert dem Benutzer den Zugriff, wenn das Gerät das nächste Mal angeschlossen wird
- Zerstören – gibt dem IronKey den Befehl zur Einleitung der Selbstzerstörungssequenz

### Starke Authentifizierung

IronKey Enterprise USB-Sticks verfügen über eine umfassende „Public-Key“-Verschlüsselungsfunktionalität. Damit ist eine sichere Verwaltung – auch im Rahmen der Fernwartung – gewährleistet. IronKey Enterprise unterstützt auch „One-Time-Password“-Technologie wie z. B. RSA SecurID®. So können IronKeys zur Zwei-Faktor-Authentifizierung eingesetzt werden und Ihre Mitarbeiter müssen nicht mehrere Geräte mitführen. Optionale Identity-Management-Software schützt Nutzerdaten vor Keystroke-Logging, Spyware und anderen Online-Gefahren.

„IronKey Enterprise ist eine leistungsfähige und effektive Möglichkeit, mobile Datenträger zu verwalten und zu kontrollieren.“

Information Security Magazine,  
Februar 2009

Welcher IronKey ist der richtige für Sie?	ENTERPRISE	PERSONAL	BASIC
Ferngesteuerte Abschaltung für verloren gegangene oder gestohlene USB Flash Drives	●		
Zugriffskontrolle und -entzug*	●		
Verlaufsprotokoll für Benutzeraktivitäten und Ereignisse	●		
Wiederbeschaffung und Neuausgabe von Geräten	●		
Fernwartung per Internet	●		
Vergabe von Sicherheitspolicies	●		
Automatischer Virensan	●		
RSA SecurID®, CRYPTOCARD, One-Time-Password	●		
Internetsicherheit und Identitätsschutz*	●	●	
Integrierter Malware-Schutz	●	●	●
Automatische Hardwareverschlüsselung aller Daten	●	●	●
Leistungsfähiger Dual Channel Chip	●	●	●
Robust, manipulationssicher und wasserfest	●	●	●

\*Sicherer Browser, eingebauter Identity-Manager und VeriSign® Identity Protection (VIP)

## Technische Daten

### Speicherkapazität

1 GB, 2 GB, 4 GB, 8 GB oder 16 GB

### Geschwindigkeit\*

Lesegeschwindigkeit bis zu 27 MB pro Sekunde, Schreibgeschwindigkeit bis zu 24 MB pro Sekunde

### Maße

75 mm x 19 mm x 9 mm

### Gewicht

25 Gramm

### Wasserdicht

MIL-STD-810F

### Umgebungstemperatur

Betriebstemperatur: 0 °C bis +70 °C  
Lagertemperatur: -40 °C bis +85 °C

### Stoßfestigkeit im Betrieb

16 G rms

### Hardware

USB 2.0 Highspeed

### Kompatibilität mit folgenden Betriebssystemen

Windows 2000 SP4, Windows XP SP2+, Vista, Windows 7, Macintosh OS X 10.4+, Linux 2.6+

### Hardwareverschlüsselung

Daten: AES Cipher-Block chained mode  
Verschlüsselungscodes: 256-bit Hardware  
PKI: 2048-bit RSA  
Hashing: 256-bit SHA  
Entspricht FIPS 140-2 Level 3

### Barrierefreiheit gemäß Section 508 des US-Rehabilitation Act gewährleistet

## Die Vorteile des IronKey Enterprise S200

- Alle gespeicherten Daten werden permanent verschlüsselt
- Sicheres Passwort Management
- Sicher surfen in geschützter Privatsphäre
- Keine Windows-Administratorrechte nötig
- Eine sichere Plattform für mobile Anwendungen
- Keine Installation von Software oder Treibern nötig
- Unkomplizierter Einsatz und Anwendung

## Verwalten Sie sicher alle IronKey Enterprise USB Flash Drives Ihrer Firma per Fernwartung übers Internet



### Integration von Endpoint- und Firmenanwendungen

Bei der Entwicklung von IronKey Enterprise wurde darauf geachtet, dass die USB-Sticks mit den gängigen, am Markt befindlichen „Endpoint Security“-Produkten problemlos zusammenarbeiten. IronKey Enterprise S200 Flash Drives verfügen über ein vorinstalliertes digitales PKCS #11 Zertifikat und Interface, das eine schnelle, starke Authentifizierung für Online-Firmenanwendungen ermöglicht.

### Bereitstellung und Implementierung von Nutzer-Policies

Mittels einer intuitiven und sicheren Online-Benutzeroberfläche können die IronKey-Administratoren von zentraler Stelle aus unternehmensweit die Nutzer-Policies für die IronKey Enterprise S200 USB Flash Drives einstellen. Der Benutzer kann den Stick selbst aktivieren, oder der Administrator aktiviert das Gerät und gibt es an den Endbenutzer aus.

### Passwortwiederherstellung in Eigenregie

IronKey bietet Ihnen optional einen online-basierten Service zur Passwortwiederherstellung. Dieser ermöglicht es Ihnen durch eine sichere wechselseitige Authentifizierungsmethode, den Nutzer eines betreffenden IronKey zweifelsfrei zu identifizieren.

### Entsperrungs- und Reset-Funktion für Administratoren

Mit der Public-Key-Authentifizierung von IronKey Enterprise können autorisierte Administratoren auch ohne „Back Door“-Passwort auf Daten der USB-Sticks Ihrer Angestellten zugreifen. Darüber hinaus können Sie mit IronKey Enterprise einzelnen Mitarbeitern Administratorenrechte vergeben oder entziehen.

### Sicherungssoftware zum Mitnehmen

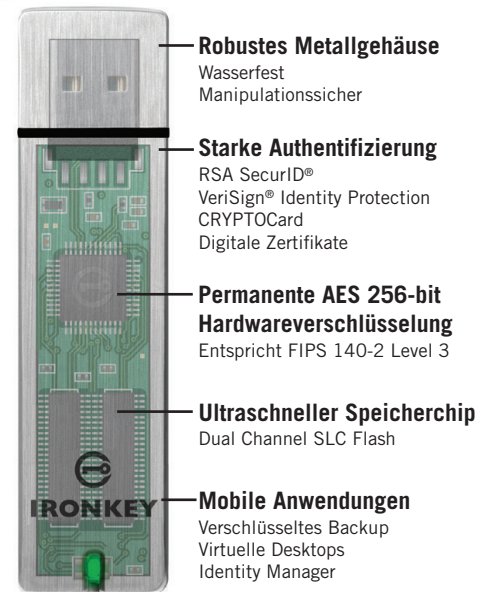
Optional ist der IronKey Enterprise mit einem Anwendungspaket erhältlich, das u. a. eine mobile Version von Mozilla Firefox, den IronKey Passwortmanager und den IronKey Secure Sessions Service, zum Aufbau verschlüsselter Internetverbindungen beinhaltet. Diese Anwendungen können von den Systemadministratoren nach Bedarf aktiviert oder deaktiviert werden.

### Sichere Plattform zur Virtualisierung

Hardware-Ebene und eine große Speicherkapazität (bis zu 16 GB) machen den IronKey zur idealen Plattform für sichere virtuelle Desktops und mobile Anwendungen.

### Von Haus aus sicher

Das IronKey-Team aus renommierten Experten für Verschlüsselung, Authentifizierung und Internetsicherheit hat die IronKey-Geräte und -Onlinedienste speziell dafür entwickelt, auch den komplexesten Angriffen standzuhalten, einschließlich Demontage, Passwortentschlüsselungsprogrammen, USB-Sniffing, DPA-Angriffen und Chip-Inspektion.



kainoa

ELITE SOLUTION PROVIDER  
www.kainoa.de



© Copyright 2009 IronKey, Inc. Alle Rechte vorbehalten. Nachdruck (auch teilweiser Nachdruck) ohne schriftliche Genehmigung von IronKey ist untersagt. IronKey und das IronKey-Logo sind geschützte Marken von IronKey, Inc. Windows und alle anderen Markennamen sind Eigentum der jeweiligen Inhaber. Änderungen der Leistungsmerkmale und technischen Daten bleiben vorbehalten.  
\*Die Lese-/Schreibgeschwindigkeit wurde unter Laborbedingungen getestet. Die tatsächlich erreichte Geschwindigkeit kann abweichen. Die Speicherkapazitäten sind Zirkel-Angaben. Nicht die gesamte Speicherkapazität steht zur Datenspeicherung zur Verfügung.

