

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

**ECHTES PLUG & PLAY**

**PLATTFORMÜBERGREIFEND**



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

Der IronKey Basic S200 wurde entwickelt, um speziell den Anforderungen an hoch sensible IT-Netzwerke gerecht zu werden. Er findet seinen Einsatz im Bereich des Militärs, der Regierungsorganisationen und diverser Firmennetzwerke. Weiter ist er der einzige USB-Stick, der offiziell den strengen Bedingungen für den FIPS 140-2 Level 3 entspricht. Zusätzlich schützt er die Daten mit einer leistungsstarken Hardwareverschlüsselung. Der IronKey Basic S200 bildet das Herzstück der IronKey-S200-Produktfamilie zur sicheren Datenspeicherung und Authentifizierung. Die leistungsfähige, speicherstarke Datensicherung macht den IronKey Basic S200 zudem zu einer idealen Plattform zum Einsatz von virtuellen Desktops.

### Permanente Datenverschlüsselung

Beim Speichern der Benutzerdaten auf dem USB-Stick werden diese mit einer AES 256-bit Hardwareverschlüsselung codiert. Diese Verschlüsselung entspricht den Qualitäts- und Sicherheitsanforderungen der US-Regierungsstellen nach FIPS 140-2 Level 3. Im Gegensatz zu einer softwarebasierten Verschlüsselung kann die hardwarebasierte Verschlüsselung des IronKey nicht abgeschaltet oder umgangen werden. Der im IronKey verbauter Cryptochip generiert und speichert die sicheren und zufälligen Schlüssel selbst. Dadurch laufen die Verschlüsselungsprozesse schneller und sicherer als in einem softwarebasierten System.

### Robust und manipulationssicher

Der IronKey Basic S200 ist eine Investition, die sich auf Jahre auszahlt. Sein widerstandsfähiges Metallgehäuse schützt ihn gegen Schäden von außen. Die innen liegenden Bestandteile sind in einen harten Kunststoff eingegossen und so gegen Manipulationen geschützt. Dieser Schutz und ein in der Hardware verankerter aktiver Selbstzerstörungsmechanismus, der die Verschlüsselungscodes zerstört und alle gespeicherten Daten löscht, sowie viele andere Sicherheitsvorkehrungen sorgen dafür, dass der wasserdichte IronKey Basic S200 die Anforderungen von FIPS 140-2 Level 3 erfüllt oder sogar noch übertrifft.

### Sicher und selbstverteidigend

Der Zugriff auf die Daten des IronKey ist nur nach Eingabe des korrekten Passwortes möglich. Sowohl die Verschlüsselung der zu speichernden Daten als auch die Überprüfung des Passwortes finden direkt in der Hardware des IronKey statt und können nicht durch Malware oder fahrlässige Handhabung außer Kraft gesetzt werden. Der sich selbst verteidigende IronKey USB Flash Drive bietet zudem auf Hardware-Ebene aktiven Schutz gegen die Verbreitung von Würmern, Crimeware und anderen bössartigen Codes.

### Unkomplizierte Anwendung

Für den Einsatz des IronKey ist keine Installation von Software oder Treibern nötig. Er läuft selbst auf Windows 2000, Windows XP und Vista ohne Administratorrechte oder Installation von Software und zusätzlichen Treibern. Einmal initialisiert, läuft der IronKey auch auf Linux-Systemen oder Macintosh. Eine Drag & Drop-Verschlüsselung, unkompliziertes „Plug & Play“ und ein intuitives verschlüsseltes Backup machen den IronKey benutzerfreundlich und insgesamt kostengünstig.

„Als einer der ersten IronKey-Kunden können wir sagen, dass dieser USB-Stick der einzige ist, dem wir genug vertrauen, um ihn für den Gebrauch in unserer Behörde zuzulassen.“

Kenneth D. Rogers, Chefinformatiker im Dezernat für Wissenschaft und Technologie der US-Heimatschutzbehörde.

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 Virenskan	●		
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 Basic S200

- Bietet die für einen USB-Stick höchstmögliche Datensicherheit
- Vergabe von Verschlüsselungspolicies
- Minimiert die Risiken, die durch verlorene oder gestohlene USB-Sticks entstehen
- Fördert Policy Compliance
- Keine Administratorrechte für Windows nötig
- Keine Installation von Software oder Treibern
- Einfacher Einsatz, einfache Handhabung

## Sicher, zuverlässig und einfach in der Handhabung

IronKey kooperiert mit zahlreichen Unternehmen, führenden Technologie- und Sicherheitspartnern, um eine extrem sichere, zuverlässige und einfach anzuwendende Lösung zu entwickeln. Anrufe bei der Servicehotline wegen Anwendungsschwierigkeiten gibt es mit dem IronKey nicht.

## Zuverlässige Premiumqualität

Geschützt durch ein robustes, manipulationssicheres und wasserdichtes Metallgehäuse ist der IronKey darauf ausgelegt, jahrelanger höchster Beanspruchung standzuhalten. IronKey verwendet nur Komponenten mit höchster Qualität. Deshalb überlebt der IronKey 10- bis 20-mal länger als ein herkömmlicher USB-Stick.

## Hardwarebasierte Verschlüsselung und Sicherheit

Wenn der IronKey an einen Laptop oder Desktop-Computer angeschlossen wird, muss der Nutzer sich mit einem Passwort anmelden, bevor die Verschlüsselungsmechanismen aktiviert werden und Daten und Anwendungen zugänglich sind. Anders als bei der softwarebasierten Verschlüsselung sendet der IronKey Cryptochip keine AES-Verschlüsselungsdaten zum Rechner. So ist er gegen „Cold Boot“-Attacken und Malware-Angriffe geschützt.

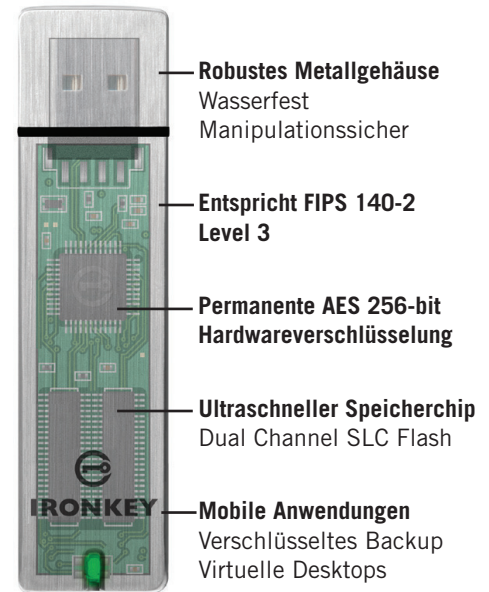
Der IronKey Basic S200 schützt vor Angriffen und speichert jeden erfolglosen Zugriffsversuch auf dem Cryptochip selbst. Wird versucht, in einen IronKey „einzubrechen“ und 10 falsche Passwörter eingegeben, löscht der Cryptochip garantiert alle verschlüsselten Daten mithilfe der zum Patent angemeldeten Flash-Trash-Technologie. So ist sichergestellt, dass kein Zugriff auf die Daten des Sticks erfolgen kann.

## Endpoint Security

Der IronKey wurde entwickelt, um nahtlos mit vielen der führenden „Endpoint Security“-Softwareprodukten zusammenzuarbeiten. Zudem hat jeder IronKey eine individuelle Seriennummer, wodurch User-Policies einfach verwaltet und angewendet werden können.

## 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, Passwort-entschlüsselungsprogrammen, 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 Zirk-Angaben. Nicht die gesamte Speicherkapazität steht zur Datenspeicherung zur Verfügung.



Designed and  
Assembled in the USA

10 10 09