

**AES 256-BIT HARDWARE  
VERSCHLÜSSELUNG**

**KEINE SOFTWAREINSTALLATION  
ERFORDERLICH**

**PLATTFORMUNABHÄNGIG**



### DAS EINZIGE FIPS 140-2 LEVEL 3 FLASHLAUFWERK DER WELT

IronKey Basic S200 wurde speziell für die Anforderungen entwickelt, die Militär, Regierung und Unternehmen an sensible Daten stellen. Es ist das einzige USB-Flashlaufwerk, das die strengen Auflagen an Security Level 3 nach dem FIPS 140-2 Standard erfüllt. Darüber hinaus schützt IronKey Daten mit einer starken Hardwareverschlüsselung. Hierzu wird der Algorithmus verwendet, der vom US-Verteidigungsministerium für die Speicherung von Top-Secret-Daten freigegeben ist. Die Technologie des IronKey Basic S200 umfasst die Kern-Plattform der IronKey S200-Produktfamilie, zu der sichere Storage- und Authentifizierungsprodukte gehören. Der extrem sichere Hochleistungsspeicher macht IronKey auch zur idealen Plattform für den Einsatz virtueller Desktops.

### Permanente Datenverschlüsselung

Alle Benutzerdaten werden per AES 256-Bit Hardwareverschlüsselung geschützt, die den offiziellen Anforderungen nach FIPS 140-2 Level 3 entspricht. Im Gegensatz zur Softwareverschlüsselung lässt sich diese permanente Verschlüsselung nicht deaktivieren. Zusätzlich erzeugt und speichert der IronKey Cryptochip starke, zufällig generierte Schlüssel – so laufen die Verschlüsselungsroutinen schneller und sicherer ab als bei jedem softwarebasierten Verschlüsselungssystem.

### Validiert nach FIPS 140-2 Level 3

IronKey Basic S200 ist das einzige USB-Flashlaufwerk, das den Sicherheitsanforderungen nach FIPS 140-2 Level 3 entspricht.

### Physisch gehärtet und manipulationsicher

Das IronKey Basic S200-Laufwerk ist eine Investition für viele Jahre. Das robuste Metallgehäuse schützt vor mechanischer Beschädigung, die Komponenten im Inneren sind zum Schutz vor Manipulation versiegelt. Durch diese Schutzmaßnahmen - in Verbindung mit dem aus einem Stück gefertigten, robusten Gehäuse aus Aluminium, einem fest eingebauten Selbstzerstörungsmechanismus, der die Schlüssel, sowie sämtliche gespeicherte Daten unbrauchbar macht - und weiteren Maßnahmen, erfüllt der IronKey Basic S200 alle Anforderungen nach FIPS 140-2 Level 3. Darüber hinaus übertrifft das Laufwerk die Anforderungen des Militärs an Wasserdichtheit bei weitem.

### Sicherheit und Selbstschutz

Die Dateien auf einem IronKey sind für niemanden zugänglich, außer es erfolgt eine Authentifizierung mit dem korrekten Passwort. Die gesamte Verschlüsselung und Passwortüberprüfung erfolgt hardwareseitig und lässt sich weder durch Malware noch durch sorglose User deaktivieren. Der IronKey mit Selbstschutz bietet auch hardwareseitigen Schutz gegen Würmer, Crimeware und sonstige Schadsoftware.

### Einfache Benutzung und Wartung

Für den IronKey ist keine Installation von Treibern oder Software erforderlich. Das Laufwerk funktioniert auch auf Windows XP und Vista ohne Administratorrechte. IronKey bietet Verschlüsselung per Drag-and-Drop sowie ein intuitives, verschlüsseltes Backup, und ist einfach per Plug-and-Play einsatzbereit. All diese Vorteile minimieren die Gesamtbetriebskosten.

### Plattformunabhängig

Der IronKey Basic S200 funktioniert mit Windows 2000, Windows XP und Vista ohne Administratorrechte und ohne Installation von Software oder Treibern. IronKey Basic S200 funktioniert auch auf Linux und Macintosh-Betriebssystemen.

„Wir sind einer der ersten Kunden von IronKey, und für uns ist dies das einzige Laufwerk, das wir bedenkenlos für den Einsatz im Ministerium freigeben.“

*Kenneth D. Rogers, Chief Information Officer,  
Science and Technology Directorate of the  
Department of Homeland Security*

#### WELCHER IRONKEY IST DER RICHTIGE FÜR SIE?

	ENTERPRISE	PERSONAL	BASIC
Remote Termine bei Verlust oder Diebstahl	✓		
Zugriffskontrolle und-widerruf	✓		
Tracking von Nutzeraktivität und Events	✓		
Wiederherstellung und Wiederinbetriebnahme	✓		
Remote-Steuerung per Internet	✓		
Umsetzung von Sicherheitsrichtlinien	✓		
Automatischer Virenschutz	✓		
RSA SecurID®, CRYPTOCard, Einmalpasswort	✓		
Web Privacy und Identitätsschutz*	✓	✓	
Eingebauter Schutz vor Malware	✓	✓	✓
Automatische Hardware-Verschlüsselung	✓	✓	✓
Zweikanal-Hochleistungsarchitektur	✓	✓	✓
Robust, manipulationsicher & wasserdicht	✓	✓	✓

\* Sicherer Browser, Integrierter Identitätsmanager und VeriSign® Identity

# The World's Most Secure Flash Drive

# BASIC S200

## TECHNISCHE DATEN

Kapazität	1GB, 2GB, 4GB, 8GB oder 16GB
Geschwindigkeit*	Lesen bis zu 27MB/s Schreiben bis zu 24MB/s
Abmessungen	75mm X 19mm X 9mm
Gewicht	25 Gramm
Wasserdicht	MIL-STD-810F
Temperatur	Betrieb: 0 °C, +70 °C Lagerung: -40 °C, +85 °C
Stoßfestigkeit	16G RMS
Hardware	USB 2.0 Highspeed
Verschlüsselung kompatibel mit Betriebssystemen	Windows 2000 SP4, Windows XP SP2+, Vista, Macintosh OS X 10.4+, Linux 2.6+
Hardware Verschlüsselung	Daten: AES Cipher-Block Chained -Modus Schlüssel: 256-Bit Hardware PKI: 2048-Bit RSA Hashing: 256-Bit SHA FIPS Standard: 140-2 Level 3
Section 508 Compliant	

## VORTEILE DES IronKey Basic S200

- Höchste Datensicherheit aller USB-Sticks am Markt
- Kein Risiko mehr durch Verlust oder Diebstahl
- Umsetzung von Unternehmensrichtlinien
- Keine Windows-Administratorenrechte erforderlich
- No software or drivers to install
- Einfacher Einsatz und Nutzung

## Sicher, zuverlässig, einfach

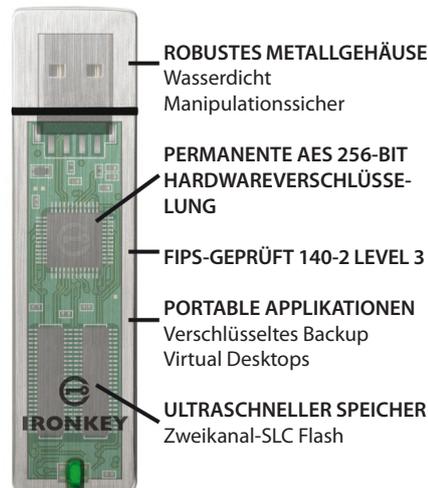
IronKey hat mit zahlreichen Unternehmen und führenden Technologie- und Security-Partnern zusammengearbeitet, um eine extrem sichere Lösung zu entwickeln, die zuverlässig und benutzerfreundlich ist und die nicht zu Mehrarbeit für das Helpdesk führt.

## Zuverlässige Premiumqualität

Mit seinem soliden, manipulations sicheren und wasserdichten Gehäuse ist der IronKey für jahrelangen harten Einsatz wie gemacht. Im IronKey kommen nur Komponenten höchster Qualität zum Einsatz. Dadurch beträgt die Lebensdauer das 10-20-fache eines herkömmlichen Flash-Laufwerks.

## Hardwareseitiges Key-Management und Schutzmaßnahmen

Wird ein IronKey an einen PC oder Laptop angeschlossen, muss sich der User mit einem Passwort identifizieren, ehe die Verschlüsselungs-Keys aktiviert werden und auf die Daten oder Applikationen zugegriffen werden kann. Anders als bei der softwarebasierten Verschlüsselung exportiert der IronKey Cryptochip keine AES Verschlüsselungs-Keys an den Hostrechner und schützt ihn so vor Cold-Boot und Malware-Angriffen. IronKey Basic S200 schützt vor Brute-Force-Passwortangriffen durch den Einsatz von nicht-flüchtigen Zählern für erfolglose Zugriffsversuche, die sich auf dem Cryptochip selbst befinden. Versucht ein Dieb mehr als 10-Mal nacheinander, mit dem falschen Passwort auf den IronKey zuzugreifen, so löscht der Cryptochip zuverlässig alle verschlüsselten Daten mit der patentierten Flash Trash-Technologie. So wird sichergestellt, dass keinerlei Daten mehr von diesem Gerät wiederhergestellt werden können.



## Endpoint Security Aware

IronKey Basic S200 wurde dafür entwickelt, nahtlos mit den führenden Endpoint-Security-Softwareprodukten zusammenzuarbeiten. Jedes Gerät besitzt eine eigene Seriennummer, so dass Nutzungsrichtlinien einfach gemanagt und angewendet werden können.



Designed and  
Assembled  
in the USA



## Sicheres Konzept

Das IronKey-Team aus renommierten Experten für Verschlüsselung, Authentifizierung und Internetsicherheit hat die IronKey USB-Sticks und Onlinedienste entwickelt, um hoch entwickelten Angriffen - einschließlich Brute Force (systematische Zeichenrekombination), USB-Sniffing, Hardware-Demontage, Differential Power Analysis und Chip-Inspektion - standzuhalten.

©Copyright 2009 IronKey, Inc. Alle Rechte vorbehalten. Kopien, ganz oder teilweise, nur mit schriftlicher Erlaubnis von IronKey. IronKey und das IronKey-Logo sind eingetragene Marken der IronKey, Inc. Windows und alle anderen Warenzeichen sind Eigentum der jeweiligen Inhaber. Technische Änderungen vorbehalten. \*Lese- und Schreibgeschwindigkeiten wurden unter Laborbedingungen getestet. Die tatsächliche Geschwindigkeit kann abweichen. Die angegebene Kapazität ist ein Näherungswert, der nicht vollständig als Speicherplatz verfügbar ist.