



## Kingston IronKey D500S Hardwareverschlüsselter USB-Stick

FIPS 140-3 Level 3 (ausstehend) zertifizierte AES 256-Bit-Hardwareverschlüsselung, robustes Zink-Gehäuse

---

Der Kingston IronKey™ D500S/SM USB-Stick bietet als Bester seiner Klasse erstklassige militärische Sicherheit, die IronKey zur vertrauenswürdigsten Marke für den Schutz geheimer Informationen macht. Er ist FIPS 140-3 Level 3 (ausstehend) zertifiziert mit neuen Verbesserungen von NIST, unter dem sichere Mikroprozessor-Upgrades für mehr Sicherheit und Angriffsschutz für Regierungs- und Militäranwendungen erforderlich sind. Die Daten werden auf dem D500S ver- und entschlüsselt, ohne dass auf dem Hostsystem Spuren verbleiben. Neben der hardwarebasierten XTS-AES 256-Bit-Verschlüsselung verfügt er über ein robustes Zinkgehäuse, das wasserdicht<sup>1</sup>, staubdicht<sup>1</sup>, stoß- und vibrationsfest nach Militärstandard<sup>2</sup>, bruchsicher und mit speziellem Epoxidharz gefüllt ist, um die internen Komponenten vor Eindringversuchen zu schützen.

Der IronKey D500S ist eine wesentliche Säule zur Erfüllung der Best Practices zum Schutz vor Datenverlust (DLP) und bietet höchste militärische Sicherheit zur Einhaltung von Gesetzen und Vorschriften zur Datenverschlüsselung wie CMMC, SOC2, NIS2, FISMA, GDPR (DSGVO), PIPEDA, HIPAA, HITECH, GLBA, SOX und CCPA zusammen mit TAA. Der D500S bietet mehr Funktionen als jeder andere USB-Stick seiner Klasse und ist damit eine branchenführende Sicherheitslösung für den Schutz hochwertiger, vertraulicher Daten.

Der D500S führt beim Hochfahren Selbsttests durch, und Übertemperatur- oder Spannungsbedingungen führt zur Abschaltung des Sticks. Der D500S ist mit einer digital signierten Firmware ausgestattet, die ihn gegen BadUSB-Malware immunisiert, was für zusätzliche Sicherheit sorgt. Der Schutz vor Brute-Force-Passwortangriffen ist immer aktiviert, um das Erraten von Passwörtern zu verhindern, und löscht den Stick, wenn zu viele ungültige Passwortversuche unternommen werden.

Er bietet eine Multi-Passwort-Option für den Zugriff auf Daten, die bis zu drei Passwörter unterstützt: Admin, Benutzer und einmalige Wiederherstellung. Der Administrator kann ein Benutzerpasswort zurücksetzen und auch ein Einmal-Wiederherstellungspasswort aktivieren, um den Zugang wiederherzustellen, wenn das Benutzerpasswort vergessen wurde.

Der D500S unterstützt das traditionelle komplexe Passwort oder den Passphrasen-Modus<sup>3</sup>. Passphrasen können zwischen 10 und 128 Zeichen lang sein. Das FBI empfiehlt Passphrasen mit mehreren Wörtern und 15 oder mehr Zeichen, die stärker und leichter zu merken sind als komplexe Passwörter.<sup>4</sup>

Der D500S bietet als erster in der Branche die Option von zwei versteckten Partitionen, mit der der Administrator zwei sichere Partitionen in benutzerdefinierter Größe für den Administrator und den Benutzer erstellen kann. Bei der Verwendung von nicht vertrauenswürdigen Systemen oder der gemeinsamen Nutzung des Sticks halten die verborgenen Dateispeicher ihre Daten sicher und unsichtbar, solange nicht ordnungsgemäß darauf zugegriffen wird.

Mit einer speziellen Schlüsselsequenz kann der Administrator die Kryptolöschung einsetzen, mithilfe dessen der Stick kryptogelöscht wird, wodurch die Daten für immer vernichtet werden und der Stick zurückgesetzt wird, um unbefugten Zugriff in kompromittierenden Situationen zu verhindern.

Als Unterstützung bei Problemen mit der Tastatur enthalten alle Bildschirme zur Passworteingabe ein Augensymbol, über das das eingegebene Passwort angezeigt wird, um Tippfehler zu vermeiden. Eine virtuelle Tastatur ist auch in Englisch<sup>5</sup> verfügbar, um die Passworteingabe vor Keyloggern und Screenloggern zu schützen.

Der D500S unterstützt außerdem zwei Stufen von Schreibschutzmodi (Nur Lesen). Sowohl der Administrator als auch der Benutzer können einen sitzungsbasierten Nur-Lesen-Modus einstellen, um den Stick vor Malware auf nicht vertrauenswürdigen Systemen zu schützen. Der Administrator kann auch einen globalen Schreibschutz-Modus einstellen, der den USB-Stick bis zum Zurücksetzen in den Nur-Lesen-Modus versetzt.

Außerdem bietet er schnelle Dual-Channel-Leistung, ohne die Sicherheit zu beeinträchtigen. Der USB-Stick umfasst eine eindeutige 8-stellige elektronische Seriennummer, die mit der auf dem Gehäuse eingravierten Nummer übereinstimmt, sowie einen einscannbaren Barcode für die Bereitstellung des USB-Sticks oder zu Audit-Zwecken.

Der D500S bietet viele Personalisierungsmöglichkeiten, ist TAA/CMMC-konform und wird in den USA montiert.

## Managed Modell

Kingston IronKey D500SM (M = Managed (Verwaltet)<sup>6</sup>) USB-Sticks ermöglichen größeren Unternehmen oder Behörden die zentrale Verwaltung des Zugriffs auf USB-Sticks und der Nutzung einer ganzen Flotte von USB-Sticks.

- 
- FIPS 140-3 Level 3 (ausstehend), zertifiziert für erstklassige Sicherheit auf militärischem Niveau
  - Multi-Passwort-Option mit Komplex-/Passphrasen-Modi
  - Die branchenweit erste Option mit zwei versteckten Partitionen
  - Crypto-Lösch-Passwort für kompromittierende Situationen
  - Robustes Zinkgehäuse zum Schutz vor Penetrationsangriffen, Stoß- und Vibrationsfestigkeit nach Militärstandard, wasser- und staubdicht nach IP67<sup>7</sup>

- Benutzerfreundliche Schnittstelle
- Vollständig anpassbare Funktionen
- Verfügbar in einem Managed-Modell

## Wichtige Merkmale

- **Hardwareverschlüsselter USB-Stick in Militärqualität**

FIPS 140-3 Level 3 (ausstehend) zertifizierte XTS-AES 256-Bit-Verschlüsselung mit sicheren Mikroprozessor-Upgrades für noch mehr Schutz. Integrierter Schutz gegen BadUSB und Brute-Force-Angriffe. Neue Selbsttests beim Hochfahren sowie Thermo- und Spannungsschutz, der bei Erreichen bestimmter Schwellenwerte die USB-Sticks automatisch abschaltet.
- **Multi-Passwort-Option für die Datenwiederherstellung**

Aktivieren Sie Administrator-, Benutzer- und einmalige Wiederherstellungspasswörter. Der Administrator kann ein Benutzerpasswort zurücksetzen und ein einmaliges Wiederherstellungspasswort erstellen, um dem Benutzer wieder den Zugriff auf die Daten zu ermöglichen, wenn das Benutzer-Passwort vergessen wurde.
- **Komplex- oder Passphrase-Modus**

Wählen Sie zwischen dem Passwortmodus Komplex oder Passphrase. Passphrasen können ganze Sätze oder mehrere Wörter sein, an die nur Sie sich erinnern – zwischen 10 bis 128 Zeichen lang. Ein Augensymbol für alle eingegebenen Passwörter hilft, Tippfehler zu vermeiden.
- **Die branchenweit 1. Option mit 2 versteckten Partitionen**

Der Administrator kann zwei benutzerdefinierte versteckte Doppelpartitionen für den Administrator und den Benutzer für einen verborgenen Dateispeicher erstellen, um Daten sicher und unsichtbar zu halten, wenn nicht ordnungsgemäß darauf zugegriffen wird. Zwei versteckte Partitionen können zusätzliche Sicherheit auf nicht vertrauenswürdigen Systemen bieten oder wenn eine gemeinsame Nutzung erforderlich ist.
- **Crypto-Lösch-Passwort für kompromittierende Situationen**

Das Crypto-Lösch-Passwort löscht den Verschlüsselungsschlüssel und löscht alle Daten für immer, indem es den USB-Stick zurücksetzt.
- **Globale und sitzungsbezogene Nur-Lesen-Modi (Schreibschutz)**

Sowohl der Administrator als auch der Benutzer können einen sitzungsbasierten Nur-Lesen-Modus einstellen, um den Stick vor Malware auf nicht vertrauenswürdigen Systemen zu schützen. Der Administrator kann auch einen globalen Schreibschutz-Modus einstellen, der den Stick bis zum Zurücksetzen in den Nur-Lesen-Modus versetzt.
- **Robustes Gehäuse nach den strengsten IronKey Standards**

Bruchsicheres Zinkgehäuse mit Epoxidharzfüllung für physischen Schutz vor Manipulationen. MIL-STD-810F-zertifiziert mit mechanischen Schock-, Vibrations- und Falltests. IP67-zertifiziert für Wasser-<sup>1</sup> und Staubdichtigkeit<sup>1</sup>.
- **Eindeutige 8-stellige Seriennummer und scannbarer Barcode**

Zeitsparendes Ablesen oder Scannen des Barcodes sowohl bei der Bereitstellung als auch der Rückgabe eines Sticks sowie bei allen mechanischen Hardwareprüfungen.
- **Vollständig personalisierbar**

Aktivieren, Deaktivieren, Ändern von Laufwerksfunktionen und Profilen. Firmenlogo.

## Technische Daten

Wichtige Zertifizierungen	FIPS 140-3 Level 3 (ausstehend) MIL-STD-810F TAA/CMMC-konform, montiert in den USA
Schnittstelle	USB 3.2 Gen 1
Kapazität*	8GB, 16GB, 32GB, 64GB, 128GB, 256GB, 512GB
Stecker	Typ-A
Geschwindigkeit <sup>8</sup>	USB 3.2 Gen 1 8GB – 128GB: 260MB/s beim Lesen, 190MB/s beim Schreiben 256GB: 240MB/s beim Lesen, 170MB/s beim Schreiben 512GB: 310MB/s beim Lesen, 250MB/s beim Schreiben  USB 2,0 8GB – 512GB: 30MB/s beim Lesen, 20MB/s beim Schreiben
Abmessungen	77,9mm x 21,9mm x 12,0mm
Étanche à l'eau/à la poussière <sup>9</sup>	Certification IP67
Betriebstemperatur	0°C bis 50°C
Lagertemperatur	-20°C bis 85°C
Kompatibilität	USB 3.0/USB 3.1/USB 3.2 Gen 1
Kundenspezifische Optionen	D500S: Aktivieren, Deaktivieren, Ändern von Laufwerksfunktionen und Profilen. Firmenlogo. D500SM: Ändern des Laufwerksprofils. Firmenlogo.

Garantie & Support	D500S: 5 Jahre Garantie und kostenloser technischer Support D500SM: 2 Jahre Garantie und kostenloser technischer Support
Kompatibel mit	Windows® 11, 10, macOS® 11.x – 14.x, Linux <sup>10</sup> Kernel 4.4+

## Teilenummern

### Serialisierte USB-Sticks

IKD500S/8GB
IKD500S/16GB
IKD500S/32GB
IKD500S/64GB
IKD500S/128GB
IKD500S/256GB
IKD500S/512GB

### Serialized Managed-Sticks

IKD500SM/8GB
IKD500SM/16GB

IKD500SM/32GB

IKD500SM/64GB

IKD500SM/128GB

IKD500SM/256GB

IKD500SM/512GB

## Produktbild



\* Ein Teil der hier genannten Kapazität des Flash-Speichers wird zur Formatierung oder für andere Funktionen genutzt und steht daher nicht zum Speichern von Daten zur Verfügung. Die tatsächlich zur Datenspeicherung verfügbare Kapazität ist daher geringer als die auf den Produkten gelistete. Weitere Informationen finden Sie im Kingston's [Flash Memory Guide](#).

1. Bitte die Spezifikation des Datenblatts beachten. Das Produkt darf nur sauber und trocken verwendet werden.
2. MIL-STD-810F-zertifiziert mit mechanischen Schock-, Vibrations- und Falltests.
3. Der Passphrase-Modus wird unter Linux nicht unterstützt.
4. Von fbi.gov: [Aufbau einer digitalen Verteidigung mit Passwörtern](#), 18. Februar 2020
5. Віртуальна клавіатура: Підтримує лише англійську мову (США) на Microsoft Windows та macOS.
6. SafeConsole Managementservice, separat zu erwerben.
7. Produkt darf nur sauber und trocken verwendet werden.
8. Die Geschwindigkeit kann abhängig von Hardware, Software oder Nutzung variieren.
9. IEC 60529 IPX8-zertifiziert für Wasserdichtigkeit mit aufgesetzter Kappe. Das Produkt darf nur sauber und trocken verwendet werden.
10. Die Unterstützung von Funktionen unter Linux ist begrenzt. Weitere Einzelheiten sind im Benutzerhandbuch zu finden. Bestimmte Distributionen von Linux benötigen Superuser-(root)-Berechtigungen, um IronKey-Befehle im Fenster der Terminal-Anwendung richtig ausführen zu können.

DIESES DOKUMENT KANN OHNE VORANKÜNDIGUNG GEÄNDERT WERDEN.

©2023 Kingston Technology Europe Co LLP und Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, England. Tel: +44 (0) 1932 738888, Fax: +44 (0) 1932 785469. Alle Rechte vorbehalten. Alle Marken und eingetragenen Marken sind Eigentum ihrer jeweiligen Besitzer. MKD-11272023

