KINGSTON IRONKEY D500S

Militärische Sicherheit nach FIPS 140-3 Level 3 (ausstehend) zum Schutz mobiler Daten

Der Kingston IronKey™ D500S/SM USB-Stick bietet 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[1], staubdicht[1], 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 DSGVO, HIPAA, SOX und CCPA. Der D500S bietet mehr Funktionen als jeder andere USB-Stick seiner Klasse und ist damit eine umfassende Sicherheitslösung für den Schutz hochwertiger Daten.

Der D500S führt beim Hochfahren Selbsttests durch, und die Erkennung von Übertemperatur- oder Spannungsbedingungen führt zur Abschaltung des Sticks. Der D500S ist mit einer digital signierten Firmware ausgestattet, die ihn gegen BadUSB-Malware und Brute-Force-Angriffe 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 zuviele 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 Passphrase-Modus[3]. Mit dem herkömmlichen Komplexmodus sind Passwörter mit 8 bis 16 Zeichen unter Verwendung von 3 von 4 Zeichensätzen zulässig. Passphrasen können zwischen 10 und 128 Zeichen lang sein. Sie können aus einem Satz mit Leerzeichen, einer Liste von Wörtern oder sogar Liedtexten bestehen, um sich das Merken von aussagekräftigen und dennoch sehr sicheren Passwörtern zu erleichtern. Das FBI empfiehlt Passphrasen mit mehreren Wörtern und 15 oder mehr Zeichen, die stärker und leichter zu merken sind als komplexe Passwörter.[5]

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 krypto-gelöscht wird, wodurch die Daten für immer vernichtet werden und der Stick zurückgesetzt wird, um unbefugten Zugriff 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[4] 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 Schnelligkeit, 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) USB-Sticks erfordern SafeConsole[2]. Dies ermöglicht größeren Unternehmen oder Behörden die zentrale Verwaltung des Zugriffs auf USB-Sticks und der Nutzung einer ganzen Flotte von USB-Sticks. Eine optional-managed Version wird ebenfalls als Personalisierung angeboten.

- 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
- Kryptolöschung für Notfälle
- Robustes Zinkgehäuse zum Schutz vor Manipulationen
- Benutzerfreundliche Schnittstelle
- Vollständig personalisierbare Funktionen und Attribute
- Als Managed-Modell erhältlich, das SafeConsole[2] erfordert

Mehr ››

EIGENSCHAFTEN/VORTEILE

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. Neuer Selbsttest des USB-Sticks beim Hochfahren und Erkennung von Übertemperatur- oder Spannungsbedingungen, die zur Abschaltung des USB-Sticks führen.

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, mehrere Wörter oder sogar Liedtexte sein, an die nur Sie sich erinnern – zwischen 10 und 128 Zeichen lang. Ein Augensymbol für alle eingegebenen Passwörter hilft, Tippfehler zu vermeiden.

Branchenweit erste Option mit zwei 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.

Kryptolöschung für Notfälle — Die Kryptolöschung ist für Notfälle gedacht, in denen eine Datenschutzverletzung zu erwarten ist. Es löscht den Verschlüsselungsschlüssel und löscht alle Daten für immer indem es den USB-Stick zurücksetzt.

Robustes Gehäuse nach den strengsten IronKey Standards — Wasserdichtes[1], staubdichtes[1], bruchsicheres Zinkgehäuse mit Epoxidharzfüllung für physischen Schutz vor Manipulationen.

Vollständig personalisierbar — Aktivieren, Deaktivieren, Ändern von Laufwerksfunktionen und Profilen. Firmenlogo.

Globale und sitzungsbezogene Nur-Lesen-Modi (Schreibschutz) — Sowohl der Administrator als auch der Benutzer können einen sitzungsbasierten Nur-Lesen-Modus einstellen, um den USB-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.

TECHNISCHE DATEN

Wichtige Zertifizierungen
FIPS 140-3 Level 3 (ausstehend)
TAA/CMMC-konform, montiert in den USA

Schnittstelle
USB 3.2 Gen 1

Kapazität[6]
8GB, 16GB, 32GB, 64GB, 128GB, 256GB, 512GB

Stecker
Type-A

Geschwindigkeit[7]
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

Wasserdicht[8]
bis zu 1,2 m; IEC 60529 IPX8

Betriebstemperatur
0°C bis 50°C

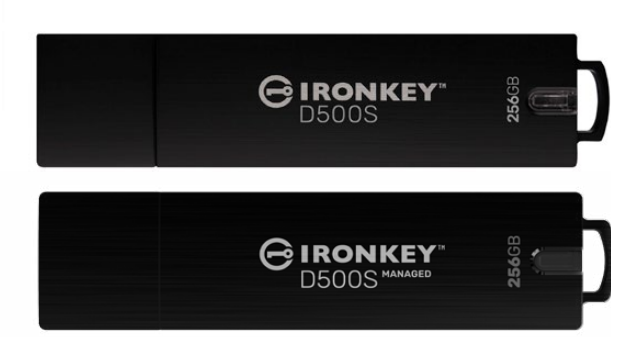
Lagertemperatur
-20°C bis 85°C

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. Optional-Managed-Version.

Garantie & Support
D500S: 5 Jahre Garantie und kostenloser technischer Support
D500SM: 2 Jahre Garantie und kostenloser technischer Support

Kompatibel mit
Windows® 11, 10, macOS® 10.15.x – 13.x, Linux[9] Kernel 4.4+



ARTIKELNUMMERN

IronKey D500S	IronKey D500SM
IKD500S/8GB	IKD500SM/8GB
IKD500S/16GB	IKD500SM/16GB
IKD500S/32GB	IKD500SM/32GB
IKD500S/64GB	IKD500SM/64GB
IKD500S/128GB	IKD500SM/128GB
IKD500S/256GB	IKD500SM/256GB
IKD500S/512GB	IKD500SM/512GB

1. Bitte die Spezifikation des Datenblatts beachten. Das Produkt darf nur sauber und trocken verwendet werden.
2. SafeConsole Managementservice, separat zu erwerben.
3. Der Passphrase-Modus wird unter Linux nicht unterstützt.
4. Virtuelle Tastatur: Nur US-Englisch unter Microsoft Windows wird unterstützt.
5. Von fbi.gov: Oregon FBI Tech Tuesday: Aufbau einer digitalen Verteidigung mit Passwörtern, 18. Februar 2020 (Link fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-with-passwords)
6. Ein Teil der auf Flashspeichern angegebenen Kapazität wird zur Formatierung oder für andere Funktionen benötigt und steht daher nicht zur Datenspeicherung zur Verfügung. Die tatsächlich zur Datenspeicherung verfügbare Speicherkapazität ist daher geringer als die auf den Produkten angegebene. Weitere Informationen entnehmen Sie dem „Flash Memory Guide" von Kingston.
7. Die Geschwindigkeit kann abhängig von Hardware, Software oder Nutzung variieren.
8. IEC 60529 IPX8-zertifiziert für Wasserdichtigkeit mit aufgesetzter Kappe. Das Produkt darf nur sauber und trocken verwendet werden.
9. 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.