



Kingston IronKey D500S แฟลชไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์

รับรองมาตรฐาน FIPS 140-3 Level 3 (รอกการรับรอง) เข้ารหัสเชิงฮาร์ดแวร์แบบ XTS-AES 256 บิต เคสสังกะสีเน้นความทนทาน

แฟลชไดรฟ์ Kingston IronKey™ D500S/SM มอบประสิทธิภาพการทำงานเหนือกว่าเมื่อเทียบกับผลิตภัณฑ์ในกลุ่มเดียวกัน อีกทั้งยังมีระบบรักษาความปลอดภัยระดับเดียวกับการใช้งานทางทหาร IronKey จึงเป็นแบรนด์ที่ได้รับความนิยมเชื่อถือมากที่สุดด้านการปกป้องข้อมูลลับสุดยอด รับรองมาตรฐาน FIPS 140-3 Level 3 (รอกการรับรอง) พร้อมฟังก์ชันการทำงานใหม่ ๆ จาก NIST ที่กำหนดให้มีการอัปเดตไมโครโปรเซสเซอร์แบบปลอดภัยเพื่อให้ปลอดภัยมากยิ่งขึ้นและป้องกันการโจมตีได้ดีกว่าทั้งสำหรับภาครัฐและการใช้งานด้านการทหาร ข้อมูลจะถูกเข้ารหัสและถอดรหัสใน D500S โดยไม่หลงเหลือร่องรอยอยู่ในเครื่องโฮสต์ นอกเหนือจากระบบเข้ารหัสเชิงฮาร์ดแวร์ XTS-AES 256 บิต ไดรฟ์ยังเลือกใช้เคสสังกะสีที่แข็งแรงทนทาน สามารถกันน้ำ¹ กันฝุ่น¹ แรงกระแทก และแรงสั่นสะเทือนเทียบเท่ามาตรฐานการใช้งานทางทหาร² ทนต่อแรงอัด และอัดอีพอกซีแบบพิเศษเพื่อป้องกันส่วนประกอบภายในจากการเจาะทำลาย

IronKey D500S คืออุปกรณ์ที่จำเป็นอย่างยิ่งในการปฏิบัติตามแนวทาง Data Loss Protection (DLP) ซึ่งช่วยรักษาความปลอดภัยในระดับสูงสุดเกรดเดียวกับการใช้งานทางทหาร ตามกฎหมายและข้อบังคับเกี่ยวกับการเข้ารหัสข้อมูล เช่น CMMC, SOC2, NIS2, FISMA, GDPR, PIPEDA, HIPAA, HITECH, GLBA, SOX และ CCPA รวมถึง TAA D500S มีคุณสมบัติการทำงานมากกว่าไดรฟ์อื่น ๆ ในคลาสเดียวกัน จึงเป็นระบบรักษาความปลอดภัยชั้นนำของอุตสาหกรรมสำหรับการปกป้องข้อมูลความลับที่มีความสำคัญระดับสูง

ระบบทดสอบตัวเองของ D500S เมื่อบูตและตรวจพบอุณหภูมิเกินหรือแรงดันไฟเกิน หรือเมื่อเกิดความไม่ปลอดภัย จะสั่งปิดการทำงานของไดรฟ์ และเพื่อให้อุ่นใจมากยิ่งขึ้น D500S ยังใช้เฟิร์มแวร์ที่ลงนามแบบดิจิทัล ทำให้ไม่เสี่ยงจาก BadUSB ระบบป้องกันการเดารหัสผ่าน Brute Force จะทำงานตลอดเวลาเพื่อป้องกันการเดารหัสผ่านและจะมีการลบข้อมูลในไดรฟ์แบบใช้รหัสลับหากมีการกรอกรหัสผ่านไม่ถูกต้องเกินจำนวนครั้งที่กำหนด

รองรับการเข้ารหัสผ่านหลายชุด (Multi-Password) สำหรับการสืบค้นข้อมูล ใช้ได้กับรหัสผ่านสูงสุดสามชุด ได้แก่ Admin, User และ One-Time Recovery ผู้ดูแลระบบสามารถรีเซ็ตรหัสผ่านผู้ใช้และเปิดใช้รหัสผ่านแบบใช้ครั้งเดียวเพื่อกู้คืนการใช้งานหากลืมรหัสผ่านผู้ใช้

D500S รองรับรหัสผ่านที่เดาได้ยากแบบดั้งเดิม หรือโหมดรหัสผ่านแบบชุดค่า³ รหัสผ่านแบบชุดค่ารองรับความยาว 10-128 ตัวอักษร FBI แนะนำ

ให้ใช้รหัสผ่านแบบชุดค่าความยาว 15 อักขระขึ้นไปเพื่อให้เดาได้ยากขึ้น แต่จดจำได้ง่ายกว่าเมื่อเทียบกับการใช้รหัสผ่านแบบเดาได้ยาก⁴

D500S รองรับตัวเลือก Dual Hidden Partition ซึ่งเป็นคุณสมบัติการทำงานใหม่ของกลุ่มอุตสาหกรรม โดยผู้ดูแลระบบสามารถจัดทำพาร์ติชันนिरภัยกำหนดเองสองส่วนสำหรับผู้ดูแลระบบและผู้ใช้ เพื่อให้สามารถใช้ Hidden File Store เพื่อจัดสรรไฟล์ข้อมูลไปยังพาร์ติชันของผู้ใช้ตามความต้องการขณะใช้เครื่องที่ไม่น่าเชื่อถือหรือเซิร์ฟเวอร์อยู่ Hidden File Stores จะดูแลข้อมูลให้ปลอดภัยและไม่ถูกเปิดเผยแก่ผู้ที่ไม่มิลิทธิใช้งานอย่างถูกต้อง

ลำดับคีย์แบบพิเศษทำให้ผู้ดูแลระบบสามารถรอกอร์หัสผ่าน Crypto-Erase ที่จะลบข้อมูลแบบเข้ารหัสลับกับตัวไดรฟ์เพื่อทำลายข้อมูลอย่างถาวรและรีเซ็ตการทำงานเพื่อไม่ให้มีการสืบค้นโดยไม่ได้รับอนุญาตในกรณีข้อมูลที่ตกอยู่ในความเสี่ยง

เพื่อช่วยเหลือผู้ใช้เกี่ยวกับประเด็นของแป้นพิมพ์ หน้าจอการรอกอร์หัสผ่านทั้งหมดจะมีสัญลักษณ์รูปดวงตาที่จะแสดงรหัสผ่านที่กรอกให้เพื่อลดปัญหาการป้อนข้อมูลผิดพลาด ไม่เพียงเท่านั้น ยังมีแป้นพิมพ์เสมือนจริงให้ใช้งานเป็นภาษาอังกฤษด้วย⁵ เพื่อป้องกันไม่ให้ระบบบันทึกการกรอกอร์หัสหรือการบันทึกหน้าจอบันทึกข้อมูลการกรอกอร์หัสผ่าน

นอกจากนี้ D500S ยังรองรับโหมดอ่านอย่างเดียว (ป้องกันการเขียน) สองระดับ ทั้ง Admin และ User สามารถกำหนดค่าโหมดอ่านอย่างเดียวเฉพาะสำหรับการทำรายการ (session) ได้เพื่อป้องกันไดรฟ์จากมัลแวร์ในระบบที่ไม่น่าเชื่อถือ นอกจากนี้ Admin ยังสามารถตั้งค่าโหมด Global Read-Only เพื่อให้ไดรฟ์เข้าสู่โหมดอ่านอย่างเดียวจนกว่าจะมีการรีเซ็ตไดรฟ์

นอกจากนี้ยังทำงานแบบสองช่องทางได้อย่างรวดเร็วโดยไม่กระทบต่อมาตรฐานการรักษาความปลอดภัย ไดรฟ์แต่ละอันมีซีเรียลนัมเบอร์ 8 หลักไม่ซ้ำกัน ซึ่งบันทึกไว้ในระบบอิเล็กทรอนิกส์และสล็อตยูเอสบีซี พร้อมบาร์โค้ดแบบสแกนได้สำหรับการติดตั้งใช้งานและตรวจสอบไดรฟ์

D500S มีตัวเลือกในการปรับแต่งมากมายและได้มาตรฐาน TAA/CMMC และประกอบในสหรัฐฯ

รุ่น Managed

ไดรฟ์ Kingston IronKey D500SM (M = Managed⁶) ช่วยให้จัดการการสืบค้นและการใช้งานไดรฟ์ได้จากส่วนกลางสำหรับการบริหารจัดการไดรฟ์เป็นจำนวนมากภายในองค์กรขนาดใหญ่หรือหน่วยงานรัฐ

- รับรองมาตรฐาน FIPS 140-3 Level 3 (รอกอร์รับรอง) ว่ามีมาตรฐานการรักษาความปลอดภัยระดับเดียวกับการใช้งานด้านการทหาร
- ตัวเลือกรหัสผ่านหลายชุดพร้อมโหมดรหัสผ่านแบบ Complex/Passphrase
- ระบบทำงานเสริม Dual Hidden Partition ครั้งแรกของกลุ่มอุตสาหกรรม
- รหัสผ่าน Crypto-Erase สำหรับใช้ในกรณีข้อมูลที่ตกอยู่ในความเสี่ยง
- เคลสสังกะสีแข็งแรงทนทานช่วยป้องกันการเจาะทำลาย อีกทั้งยังทนต่อแรงกระแทกและแรงสั่นสะเทือนตามมาตรฐานการใช้งานทางทหาร และกันน้ำ/ฝุ่นตามมาตรฐาน IP67⁷
- อินเทอร์เฟซที่ใช้งานได้ง่าย
- พีเจอร์ปรับแต่งได้อย่างเต็มรูปแบบ
- มีจำหน่ายในรุ่น Managed

คุณสมบัติเด่น

- USB เข้ารหัสเชิงฮาร์ดแวร์เกรดใช้งานด้านการทหาร

รับรองมาตรฐาน FIPS 140-3 Level 3 (รอกการรับรอง) และการเข้ารหัส XTS-AES 256 บิต พร้อมชุดอัลกอริทึมไมโครโปรเซสเซอร์แบบปลอดภัยเพื่อให้มั่นใจได้มากยิ่งขึ้น ระบบป้องกันในตัว BadUSB และ Brute Force ระบบทดสอบตัวเองของไดรฟ์ใหม่เมื่อบูตและเมื่อตรวจพบความร้อนและแรงดันผิดปกติ จะปิดทำงานโดยอัตโนมัติเมื่อค่าถึงเกณฑ์ที่กำหนด

- ตัวเลือกในการกำหนดรหัสผ่านหลายชุดสำหรับการกู้ข้อมูล

เปิดใช้งานรหัสผ่านสำหรับ Admin, User และ One-Time Recovery ได้ตามความต้องการ ผู้ดูแลระบบสามารถรีเซ็ตรหัสผ่านผู้ใช้และเปิดใช้รหัสผ่านแบบใช้ครั้งเดียวเพื่อให้ผู้ใช้สามารถสืบค้นข้อมูลได้อีกครั้งหากลืมรหัสผ่านผู้ใช้

- โหมด Complex หรือ Passphrase

เลือกระหว่างโหมด Complex และ Passphrase รหัสผ่านแบบชุดคำอาจเป็นประโยคที่สมบูรณ์หรือชุดคำที่คุณเท่านั้นที่จดจำได้ มีความยาวตั้งแต่ 10 ถึง 128 อักขระ สัญลักษณ์รูปดวงดาวสำหรับการกรอกรหัสผ่านทั้งหมดจะช่วยลดข้อผิดพลาดในการพิมพ์ได้

- ระบบทำงานเสริม Dual Hidden Partition ครั้งแรกของวงการ

ผู้ดูแลระบบสามารถจัดทำ Dual Hidden Partitions สองชุดสำหรับผู้ดูแลระบบและผู้ใช้เพื่อจัดเก็บ Hidden File Store ในการดูแลข้อมูลให้ปลอดภัยโดยที่ไม่มีใครเห็นยกเว้นหากมีการสืบค้นอย่างถูกต้อง Dual Hidden Partitions ช่วยเสริมการรักษาความปลอดภัยสำหรับเครื่องที่ไม่น่าเชื่อถือหรือในกรณีที่ต้องมีการแฮ็คไดรฟ์

- รหัสผ่าน Crypto-Erase สำหรับกรณีที่ข้อมูลตกอยู่ในความเสี่ยง

รหัสผ่าน Crypto-Erase จะล้างคีย์สำหรับเข้ารหัสและลบข้อมูลทั้งหมดอย่างถาวร พร้อมกับรีเซ็ตไดรฟ์

- โหมด Read-Only (Write-Protect) แบบ Global และ Session

ทั้ง Admin และ User สามารถกำหนดค่าโหมดอ่านอย่างเดียวเฉพาะสำหรับการทำรายการ (session) ได้เพื่อป้องกันไดรฟ์จากมัลแวร์ในระบบที่ไม่น่าเชื่อถือ ยังไม่หมดเพียงเท่านั้น Admin ยังตั้งค่าโหมด Global Read-Only เพื่อให้ไดรฟ์เข้าสู่โหมดอ่านอย่างเดียวจนกว่าจะมีการรีเซ็ตไดรฟ์ได้ด้วย

- เคสที่ทนทานตามมาตรฐาน IronKey ที่เน้นความแข็งแรงระดับสูงสุด

เคสสังกะสีทนต่อการบีบอัด และอัดด้วยอีพอกซีเพื่อกันกระแทกและเพิ่มการรักษาความปลอดภัยทางกายภาพขึ้นไปอีกชั้น รับรองมาตรฐาน MIL-STD-810F สำหรับการทดสอบแรงกระแทก การสั่นสะเทือน และการตก รับรองมาตรฐาน IP67 สำหรับคุณสมบัติกันน้ำ¹ และกันฝุ่น¹

- ซีเรียลนัมเบอร์ 8 หลักไม่ซ้ำกัน พร้อมบาร์โค้ดสำหรับสแกน

ประหยัดเวลาเพียงแค่อ่านหรือสแกนบาร์โค้ดเมื่อต้องการใช้งานหรือเมื่อต้องส่งคืน หรือระหว่างที่มีการตรวจสอบฮาร์ดแวร์ใด ๆ

- ปรับแต่งได้อย่างเต็มที่

เปิดใช้งาน ปิดใช้งาน ปรับแต่งคุณสมบัติและโปรไฟล์การทำงานของไดรฟ์ Co-logo

รายละเอียดทางเทคนิค

การรับรองมาตรฐานที่สำคัญ	FIPS 140-3 Level 3 (รอกการรับรอง) MIL-STD-810F ผ่านเกณฑ์ TAA/CMMC ประกอบในสหรัฐฯ
อินเทอร์เฟซ	USB 3.2 Gen 1
ความจุ*	8GB, 16GB, 32GB, 64GB, 128GB, 256GB, 512GB
หัวต่อ	Type-A
ความเร็ว ⁸	USB 3.2 Gen 1 8GB – 128GB: อ่าน 260MB/s เขียน 190MB/s 256GB: อ่าน 240MB/s เขียน 170MB/s 512GB: อ่าน 310MB/s เขียน 250MB/s USB 2.0 8GB – 512GB: อ่าน 30MB/s เขียน 20MB/s
ขนาด	77.9 x 21.9 x 12.0 มม.
กันน้ำ/กันฝุ่น ⁹	รับรองมาตรฐาน IP67
อุณหภูมิการทำงาน	0°C ถึง 50°C
อุณหภูมิการจัดเก็บ	-20°C ถึง 85°C
การรองรับการทำงาน	USB 3.0/USB 3.1/USB 3.2 Gen 1
ตัวเลือกในการปรับแต่ง	D500S: เปิดใช้งาน ปิดใช้งาน ปรับแต่งคุณสมบัติและโพรไฟล์การทำงานของไดรฟ์ Co- logo D500SM: ปรับแต่งโพรไฟล์การทำงานของไดรฟ์ Co- logo

การรับประกัน/บริการ	D500S: รับประกัน 5 ปีพร้อมบริการทางเทคนิคฟรี D500SM: รับประกัน 2 ปีพร้อมบริการทางเทคนิคฟรี
ใช้งานได้กับ	Windows® 11, 10, macOS® 11.x – 14.x, Linux ¹⁰ Kernel 4.4+

หมายเลขชิ้นส่วน

ไดรฟ์ Serialized

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

ไดรฟ์ Serialized Managed

IKD500SM/8GB
IKD500SM/16GB

IKD500SM/32GB
IKD500SM/64GB
IKD500SM/128GB
IKD500SM/256GB
IKD500SM/512GB

รูปภาพสินค้า



* ความจุบางส่วนที่ระบุในแฟลชการ์ดใช้สำหรับการฟอร์แมตและฟังก์ชันอื่น ๆ ไม่ใช่สำหรับการจัดเก็บข้อมูล ด้วยเหตุนี้ความจุที่ใช้งานได้จริงเพื่อเก็บข้อมูลจะต่ำกว่าที่แจ้งไว้ในตัวผลิตภัณฑ์ ดูรายละเอียดเพิ่มเติมได้จากคู่มือหน่วยความจำแฟลชเมมโมรี่ของ Kingston's [Flash Memory Guide](#)

1. ดูรายละเอียดทางเทคนิคได้จากเอกสารข้อมูล จะต้องทำความสะอาดและเช็ดให้แห้งก่อนใช้งานผลิตภัณฑ์
2. รับรองมาตรฐาน MIL-STD-810F สำหรับการทดสอบแรงกระแทก การสั่นสะเทือน และการตก
3. โหมดรหัสผ่านแบบชุดค่าไม่สามารถใช้ได้กับ Linux
4. จาก fbi.gov: [Oregon FBI Tech Tuesday: Building a Digital Defence with Passwords](#), February 18, 2020
5. เป็นที่พิมพ์เสมือนจริง: รองรับเฉพาะ US English สำหรับ Microsoft Windows และ macOS
6. ระบบจัดการ SafeConsole ต้องจัดซื้อแยกต่างหาก
7. จะต้องทำความสะอาดและเช็ดให้แห้งก่อนใช้งานผลิตภัณฑ์
8. ความเร็วอาจแตกต่างกันไปเนื่องจากฮาร์ดแวร์ ซอฟต์แวร์และการใช้งาน
9. รับรองมาตรฐาน IEC 60529 IPX8 ว่ากันน้ำได้ขณะปิดฝา จะต้องทำความสะอาดและเช็ดให้แห้งก่อนใช้งานผลิตภัณฑ์
10. รองรับการทำงานกับ Linux แบบจำกัด ดูรายละเอียดเพิ่มเติมได้จากคู่มือผู้ใช้ ระบบ Linux บางส่วนต้องมีสิทธิ์ซูปเปอร์ยูสเซอร์ (ราก) เพื่อสั่งการคำสั่ง IronKey ในหน้าต่างแอปพลิเคชันใช้งาน



เอกสารนี้อาจมีการเปลี่ยนแปลงเนื้อหาโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

©2567 Kingston Technology Far East Corp. (Asia Headquarters) No. 1-5, Li-Hsin Rd. 1, Science Park, Hsin Chu, Taiwan, สงวนลิขสิทธิ์ เครื่องหมายการค้าและเครื่องหมายการค้าจดทะเบียนทั้งหมดถือเป็นกรรมสิทธิ์ของผู้เป็นเจ้าของ MKD-12192566