Aegis Secure Key 3.0

HARDWARE ENCRYPTED USB FLASH DRIVE

WORKS WITH:

symbian OS

- ON-THE-FLY 256-BIT AES-XTS HARDWARE ENCRYPTION
- SOFTWARE-FREE INSTALLATION & OPERATION; COMPLETELY CROSS-PLATFORM COMPATIBLE
- HIGH-QUALITY RUGGED ALUMINIUM HOUSING Water and Dust Resistant
- EMBEDDED 7-16 DIGIT PIN AUTHENTICATION No Security Parameters Shared with Hosts
- ADMIN MODE FOR SECURE DEPLOYMENT
- INDEPENDENT USER AND ADMIN PINS
- FORCED ENROLLMENT AT FIRST USE
- TOUGH EPOXY INTERNAL FILLING FOR PHYSICAL-ATTACK PROTECTION
- BRUTE-FORCE PROTECTION
- SELF-DESTRUCT PIN FEATURE
- COMPATIBLE WITH ANY OS Windows®, Mac®, Linux

SUPER-FAST USB 3.0

- 10X Faster than USB 2.0
- VARIABLE TIMING CIRCUIT
- LOCK-OVERRIDE MODE
- DRIVE-RESET FEATURE
- AUTO-LOCK FEATURE
- READ-ONLY MODE

Inside This Tiny Key is a World Of Advanced Data Protection.

Software-free operation, cross-platform compatibility, USB 3.0 speed, increased capacities of up to 240GB, plus a host of high-level security features that you'd never expect to find in a flashkey.

Military Grade 256-bit AES XTS Hardware Encryption: All data on the Aegis Secure Key is encrypted on-the-fly with built-in 256-bit AES XTS.

Software-Free Design: The Aegis Secure Key is ready to use right out of the box–no software, no drivers, no updates involved. It can even be utilized where no keyboard is present (e.g., cockpits, medical equipment, AV gear.) Completely cross-platform compatible, the Aegis Secure Key excels just about anywhere–PCs, MACs, Linux, or any OS with a powered USB port and a storage file system.

Embedded Keypad: All PIN entries and controls are performed on the keypad of the Aegis Secure Key. Since there is no host involvement in the key's authentication or operation, the risk of software hacking and key-logging is completely circumvented.

Independent User and Admin PINs: The Aegis Secure Key can be configured with independent User and Admin PINs, making it an ideal device for corporate and government deployment. Should the User forget his or her PIN, the drive can still be unlocked with the Admin PIN and a new User PIN can be created.

Auto-Lock Feature: Locks automatically whenever it's unplugged from its powered USB port, and is further programmable to lock after a predetermined period of inactivity.

Drive Reset Feature: Effectively clears both the User and Admin PINs, performs a crypto-erase on the drive, creates a new randomly generated encryption key, and allows the drive to be redeployed. Capable of generating an infinite number of randomly generated encryption keys, The Aegis Secure Key permits the admin to reset the drive as many times as desired.

Super Tough, Inside and Out: IP-58 certified as tough enough to go anywhere, the Aegis Secure Key's resilient design makes it perfect for travel. Its rugged, extruded aluminium casing is resistant to dust and water, and the keypad is wear-resistant. Inside, another layer of protection is added with the injection of a tough epoxy compound to prevent physical access to the key's encryption circuitry.

Brute-Force Protection: After a predetermined number (programmable; up to 20) of incorrect PIN entry attempts, the Aegis Secure Key will conclude that it is under *Brute Force Attack* and will respond by performing a crypto-erase – deleting the encryption key which will render all of the key's data useless.

VTC Technology: Apricorn's Variable Time Circuit (VTC) technology is designed to thwart *Timing Attacks* aimed at accessing the drive by studying usage patterns and infiltrating the Secure Key's electronics.

Lock-Override Mode Feature: Designated for specific cases in which the key needs to remain unlocked, e.g., during reboot, passing the key through a virtual machine, or other similar situations that would normally prompt the key to automatically lock. When enabled, Lock-Override Mode allows the key to remain unlocked through USB port re-enumeration and will not re-lock until USB power is interrupted.

Read-Only Mode Feature: Perfect for accessing data on the key in a public setting to protect against USB viruses or Trojan attachments. Particularly important in forensics, Read-Only Mode is ideal for applications that require data to be preserved in its original, unaltered state and can't be overwritten or modified.

Self-Destruct Feature: The last line of defense for data security where all of the drive's contents must be wiped to avert breach. The Secure Key's Self-Destruct PIN defends against physically compromising situations by erasing the key's contents, leaving it in normal working order and to appear as if it has yet to be deployed.

APRICORN

Visit our web site at www.apricorn.com or call 1-800-458-5448

STEP 1

Enter your PIN

STEP 2

Plug & Play

STEP 3

Press Lock or Unplug to Lock

Security	Benefits
Easy to Use Onboard Keypad	Unlock the drive with unique 7 to 16-digit pin; Wear-resistant keys to obscure use
On-the-Fly 256-bit AES XTS Hardware Encryption	100% of your data is hardware-encrypted on-the-fly with military-grade, full-disk AES XTS encryption
Software-Free / Cross-Platform Compatible	No software involved to setup or operate *EVER* – completely cross-platform compatible and perfect for corporate deployments
Forced-Enrollment	For added security, Secure Key requires that you create your unique PIN upon first use
Administrator Mode	Allows enrollment of one independent user and one administrator for setting parameters for PIN management, Read-Only, Auto-Lock, Self-Destruct, Lock-Override, and Brute Force
Drive-Reset Feature	Infinite number of resets; performs a crypto-erase with new encryption key regeneration
Auto-Lock Feature	The Aegis Secure Key automatically locks after a predetermined period of inactivity or whenever it's unplugged from its powered USB port or if power to the USB port is turned off
Internally Sealed by Tough Epoxy Compound Filling	Internal drive components are sealed by a super-tough epoxy compound barrier which prevents would-be hackers from physically accessing the encryption circuitry
OS and Platform Independent	Compatible with Windows, Mac, Linux and embedded systems Works with any USB / USB On-the-Go devices
Features	**Benefits**
Advanced Options / Modes	Read-Only Mode, Lock-Override Mode, Self-Destruct PIN, Variable Time Circuit
Thermal Management	Prevents excessive external temperatures by throttling back r/w speeds to lower its internal temperature
USB 3.0 Interface	Compatible with any computer USB port or any USB / USB On-the-Go devices
Aluminum Enclosure	Dust and water resistant durable aluminium housing
Flash Drive Capacities	30GB, 60GB, 120GB, 240GB
Plug-n-Play and Compatible on any system	Works with Windows®, Mac®, Linux, Android and Symbian systems, or any powered USB OS with a storage file system
Secure storage	Excellent for government, health care, insurance companies, financial institutions, HR departments and executives with sensitive data
Box Contents	Aegis Secure Key, Protective Aluminum Cap and Quick Start Guide
Specifications	
Data Transfer Rates	Up to 190MB/s (Read) / 160MB/s (Write) | Small File (4K): 14k read; 40k write
Interface	USB 3.0
Dimensions & weight	95.5mm x 24.5mm x 12.6mm | 93mm x 24.5mm x 12.6mm (w/o sleeve) | 46 g
Warranty	3-year limited
Approvals	FIPS 140-2 Level 3 ***Pending,*** IP-58, FCC & CE
System Requirements	OS independent: Windows, Mac® OS, Linux, Android, Symbian
Ordering Information	**Apricorn Part Number: ASK-256-30GB ASK-256-60GB ASK-256-120GB ASK-256-240GB**

*One gigabyte (GB) = one billion bytes; accessible capacity will be less and actual capacity depends on the operating environment and formatting.

For more information on **Aegis Secure Key** and other innovative Apricorn products visit our web site at www.apricorn.com or call 1-800-458-5448

APRICORN