

Aegis Secure Key 3z

Patent Pending

HARDWARE ENCRYPTED USB 3.1 FLASH DRIVE

ON-THE-FLY 256-BIT AES-XTS HARDWARE ENCRYPTION

SOFTWARE-FREE AUTHENTICATION & OPERATION;
COMPLETELY CROSS-PLATFORM COMPATIBLE

COMPATIBLE WITH ANY OS:
Windows®, Mac®, Linux, etc.

AEGIS CONFIGURATOR™ COMPATIBLE

FIPS 140-2 LEVEL 3 VALIDATION

HIGH-QUALITY RUGGED ALUMINUM HOUSING
IP57 (PENDING) Water and Dust Resistant

EMBEDDED 7-16 DIGIT PIN AUTHENTICATION
No Security Parameters Shared with Hosts

PROGRAMMABLE MINIMUM PIN LENGTH

ADMIN MODE FOR SECURE DEPLOYMENT

INDEPENDENT USER AND ADMIN PINS

RECOVERY PINS IN CASE OF
FORGOTTEN OR LOST PIN

ADMIN FORCED-ENROLLMENT AT
FIRST USE

USER FORCED-ENROLLMENT

TOUGH EPOXY INTERNAL
FILLING FOR PHYSICAL-
ATTACK PROTECTION

BRUTE-FORCE PROTECTION

SELF-DESTRUCT PIN

LOCK-OVERRIDE MODE

DRIVE-RESET FEATURE

AUTO-LOCK FEATURE



WORKS
WITH:



FIPS
140-2
Level 3
Validated

The Next Big Thing in Advanced Data Protection.

Software-free, cross-platform compatible, Aegis Configurator Compatible, plus a host of high-level security features packed into a USB 3.1 (3.0) flashkey.

Military Grade 256-bit AES XTS Hardware Encryption:

All data 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. It can even be utilized where no keyboard is present. Completely cross-platform compatible, the Aegis Secure Key excels virtually anywhere—PCs, MACs, Linux, or any OS with a powered USB port and a storage file system.

Configurable: Create custom profiles and mass configure multiple Secure Keys at once with Apricorn's new Configurator / Powered Hub bundle.

Embedded Keypad: All PIN entries and controls are performed on the keypad of the Aegis Secure Key. No critical security parameters are ever shared with the host computer. Since there is no host involvement in the key's authentication or operation, the risks of software hacking and key-logging are completely circumvented.

Super Tough, Inside and Out: The Aegis Secure Key's rugged, extruded aluminum casing and polymer-coated keypad is resistant to dust and water (IP57 certification pending.) Inside, another layer of protection is added by encasing the inner componentry with a hardened epoxy compound to prevent physical access to the encryption circuitry.

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 after which, a new User PIN can then be created.

One-Time Recovery PINs: In the event that a User PIN is forgotten, up to 4 one-time use recovery PINs can be programmed to permit access to the drive's data.

Auto-Lock: 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: Allows the drive to be cleared and redeployed. Capable of generating an infinite number of randomly generated encryption keys, The Aegis Secure Key 3z can be reset as many times as desired.

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.



Lock-Override Mode: 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.

Two Read-Only Modes: Perfect for accessing data on the key in a public setting to protect against USB viruses. 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. The Secure Key 3z has two read-only modes. One is set by the admin in the admin mode and can't be modified or disabled by anyone other than the admin. The second read-only mode can be set and disabled by a user but can also be overridden by the admin as well.

Self-Destruct PIN: 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.





| Security | Benefits |
|---|---|
| Easy to Use Onboard Keypad | Unlock the drive with unique 7 to 16-digit pin; Wear-resistant keys to obscure use |
| Programmable Minimum PIN length | For added PIN length and enhanced security, minimum PIN length requirement can be increased from 7 characters up to 16 maximum |
| 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 | Requires no software to set up or operate – completely cross-platform compatible and perfect for corporate deployments |
| Forced-Enrollment / User Forced Enrollment | For added security, the Secure Key 3z has done away with default factory preset PINs, requiring the Admin to create a unique PIN upon first use; additionally allows forced enrollment feature to be extended to User PIN at setup |
| 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 |
| Aegis Configurator Compatible | Configures multiple Configurator compatible devices at the same time in a matter of seconds with pre-set device profiles. |
| Advanced Options / Modes | 2 Read-Only Modes, Lock-Override Mode, Self-Destruct PIN |
| LED Flicker Button Confirm | Indicates positive button entry with visual LED confirmation |
| Recovery PINs | 4 one-time use PINs to recover Data in cases of forgotten User / Admin PINs |
| 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 aluminum housing |
| 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, healthcare, 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) / 80MB/s (Write) Small File (4K): 16MB/s read; 33MB/s write |
| Interface | USB 3.0 |
| 5 Flash Drive Capacities | 8GB, 16GB, 32GB, 64GB |
| Dimensions & weight | 81mm x 18.4mm x 9.5mm(w/o CAP) 22g |
| Warranty | 3-year limited |
| Approvals |  RoHS FC CE  FIPS 140-2 Level 3 (CERT #2824), IP-57 |
| System Requirements | OS independent: Windows, Mac® OS, Linux, Android, Symbian |
| Ordering Information | Part Numbers: ASK3Z-8GB ASK3Z-16GB ASK3Z-32GB ASK3Z-64GB |

*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

©2016 Apricorn, Inc. Corporate Offices: 12191 Kirkham Rd., Poway, CA. 92064