Aegis Secure Key 3NXC

Patent Pending

HARDWARE ENCRYPTED USB 3.2 C-TYPE

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

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

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

AEGIS CONFIGURATOR™ COMPATIBLE

FIPS 140-2 LEVEL 3 VALIDATION (PENDING 4Q 2020)

HIGH-QUALITY RUGGED ALUMINUM HOUSING
IP68 as 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

PIN GUARD™ ACCIDENTAL KEY PRESS RECOGNITION

REMOVABLE MEDIA OR FIXED DISK SETUP OPTION (PATENTED)

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

2 READ-ONLY MODES

CONFIGURABLE

WORKS WITH:
symbian OS

The First 256 Bit AES XTS Hardware-Encrypted Flash Key with USB 3.2 C Connector for Next Generation Device Compatibility

The Latest Addition to the Aegis Secure Key Line Brings All of the Features and Performance of the 3NX, Plus the Ability to Plug into Any C-Type Device without an Adapter.

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 3NXC 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 IP67 rated as resistant to dust and water. 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.

Removable Media / Fixed Disk Toggle: Configure at time of setup to be recognized by any OS or machine with a USB port as one or the other. (U.S. Patent No. 10,338,840)

Auto-Lock: Locks automatically whenever the device is 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 as many times as needed. Capable of generating an infinite number of randomly generated encryption keys.

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 3NXC 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.

APRICORN

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	With no default factory preset PINs, the Admin is required to create a unique PIN upon first use; forced enrollment feature can also be extended to first 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
Fixed Disk / Removable Media Toggle	Configure Secure Key to be recognizable by any OS or machine with a USB port
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
PIN Guard	Firmware Recognizes incidental / accidental keypad contact and powers down the drive to prevent battery rundown.
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 Rubberized Cap and Quick Start Guide

Specifications	
Data Transfer Rates	Up to 77MB/s (Read) / 72MB/s (Write)
Interface	USB 3.2 gen. 1 Type C connector
7 Flash Drive Capacities	4GB, 8GB, 16GB, 32GB, 64GB, 128GB
Dimensions & weight	81mm x 18.4mm x 9.5mm(w/o CAP)	22g
Warranty	3-year limited
Approvals	FIPS 140-2 Level 3 pending, IP-68
System Requirements	OS independent: Windows, Mac® OS, Linux, Android, Symbian

*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 3NXC** and other innovative Apricorn products **www.apricorn.com** or call 1-800-458-5448

APRICORN