Aegis Secure Key 3NX™

AES 256 Bit XTS Hardware-Encrypted
FIPS 140-2 Level 3 Validated
USB 3.2 type-A Flash Key

The NeXt Generation of Aegis Secure Key.

Tiny footprint, giant security. The Aegis Secure Key 3NX is our 4th generation of secure keys and incorporates all of the functions and features you've come to expect from Apricorn, all at lower operating temperatures and lower costs. Bootable, OS agnostic, and completely cross-platform compatible, the Aegis Secure Key 3NX comes in 7 capacities from 4GB to 256GB.

The Practical Choice.

From small businesses to large corporations, the Aegis Secure Key 3NX delivers the most data security for your buck. With capacities starting as low as 4GB and as high as 256GB, the size and cost of the device can be closely alligned to match the amount of data that an associate normally needs to carry. Its low cost and Aegis Configurator™ compatibility make it the smart choice for company deployments both large and small.

Portable Versatility.

Roughly the size of a five stick pack of gum, the Aegis Secure Key 3NX easily fits in any pocket, purse, or computer carry case. Its type-A connector is universally backward compatible to all type A ports, and can further be adapted to work with Type C ports with our A to C adapter (sold separately.) And since it's OS agnostic, the 3NX can go from a Windows machine to a Mac with ease.

Tough on the Outside.

IP 67 rated against water immersion and blowing dust. Rugged terrain, sand, wet locations and extreme temperatures are no match for the 3NX. The crush-resistant aluminum alloy outer enclosure and durable sleeve are ready for anywhere. And the abrasion resistant keypad with polymer coating prevents keypad wear to conceal those commonly pressed keys. Inside, a hardened epoxy potting serves to prevent internal tampering.

No Software. Period.

Apricorn's unique hardware based approach delivers the highest levels of data security and workflow compatibility. Like all Aegis secure drives, the Secure Key 3NX is software-free, hardware-encrypted, and completely cross-compatible. And since it's software-free, 100% of its authentication and encryption processes take place within the device itself, never involving the host computer in any of its security processes.

CITRIX

APRICORN

Aegis Secure Key 3NX™

Super portable secure flash key with AES 256-Bit XTS Hardware encryption and USB 3.2 Type-A Connector
And Rugged Aluminum Alloy enclosure and durable protective sleeve.
Software-Free / Locked-Down Firmware to Prevent Introduction of Malware Such as BadUSB

aegisware

Our patented firmware delivering the industry's most advanced feature set– the heart and soul of every Apricorn device.

Separate Admin and User Modes / PINs
Admin (Device Configuration) Mode and User Access Mode. The Admin mode controls the universal programmable settings of the device and can only be accessed with the Admin PIN. The User mode is for general external drive usage like read /write, unlock / lock, and certain other functions. The User mode is accessible via a User PIN or the Admin PIN. Up to four User PINs may be enrolled.

Admin Forced Enrollment
Eliminates factory default PIN vulnerability by forcing the enrollment of an Admin PIN prior to use. As with all Apricorn Aegis secure devices, there are no default passwords, and no back-doors. In order to use any Apricorn secure drive, the Admin must first establish a complex PIN.

User Forced Enrollment
Beyond the admin PIN, one additional PIN can be generated to access the device's data. This User PIN can be set up by the admin at initial setup, or the device can be deployed in a state of User Forced Enrollment, allowing the user to establish his or her own PIN prior to use.

Data Recovery PINs
Programmed by the admin at time of setup to permit regaining access to the drive by creating a state of User Forced Enrollment in which a new User PIN can be created without affecting the drive's existing data or the Admin PIN.

Two Read-Only Modes
Universal Read Only: set by the admin from within the admin mode and can't be modified or disabled by anyone but the admin. The second (User) mode can be set and disabled by a user but can also be enabled or disabled by the admin.

Programmable PIN Length
Admin designates minimum and maximum PIN lengths (between 7 and 16 Characters). The longer the PIN, the more secure the data on the device becomes. For example, the odds of brute force success go from 1/10,000,000 with a 7-digit PIN to 1/100,000,000 with an 8 digit PIN. In cases where the User sets up his or her own PIN from User Forced Enrollment, the Admin can still affect User password length requirements

Unattended Auto Lock
Programmable length of time of inactivity permitted before drive locks itself. All Aegis Secure Drives will automatically lock once disconnected from a computer's USB port or the power to that USB port is interrupted, or after a pre-programmed period of inactivity.

Lock Override
Allows drive to remain unlocked during USB Port re-enumeration (Virtual Machine, Remote Boot). Designated for specific cases in which the drive needs to remain unlocked through USB port re-enumeration such as during reboot, or passing through a virtual machine.

Self-Destruct PIN
When programmed and activated, performs a crypto-erase and becomes new access PIN. The last line of defense for data security when the device's physical security is at risk. The Self-Destruct PIN defends against these physically compromising situations by erasing the drive's contents, leaving it in normal working order appearing yet to be deployed.

Brute Force Defense
Programmable number of consecutive invalid PIN attempts permitted (4-20) before crypto-erase. If the device comes under a physical brute force attack, once the programmed number (between 4 and 20) of consecutive incorrect password entries has been attempted, the device will delete its own encryption key and destroy the ability to decrypt its stored data.

Provision Lock
Patented setting where the admin can designate whether the device will permit itself to be reset by a User or after a brute force attempt. If Provision Lock is enabled, any attempt at complete reset will "brick" the device for good.

Fixed Disk or Removable Media
Can be Configured as Fixed Disk or Removable Media in device setup. Easily adapts to embedded equipment and OSs that will only recognize one or the other for removable storage. Some applications or embedded systems may allow one type but not the other. U.S. Patent No. 10,338,840

TECHNICAL SPECIFICATIONS

CAPACITIES
Flash: 4GB, 8GB, 16GB, 32GB, 64GB, 128GB, 256GB

TRANSFER RATE
FLASH: up to 171MB/s (r) / 160MB/s (w)*

INTERFACE
USB 5Gbps TYPE-A

DIMENSIONS and WEIGHT
81mm x 18.4mm x 9.5mm | 22g
3.25" x .75" x .375" | .78oz

POWER SUPPLY
USB port / Internal battery (for PIN entry only)

OPERATING TEMPERATURE RANGES
32° to 158°F (0°C to 70°C)

OPERATING HUMIDITY RANGES
95% @ temps under 131°F (55°C)

CRUSH RESISTANT
up to 6500 LBS

SHOCK FLASH
OPERATING / NON-OPERATING: 1500G .5ms

OPERATING VIBRATION
OPERATING: 5.0 gRMS, 10-2000Hz

WARRANTY
3-Year Limited

SYSTEM COMPATIBILITY
WINDOWS, MAC OS, LINUX, ANDROID, CITRIX
any that supports a USB mass storage device

SKU NUMBERS
FLASH: ASK3-NX-4GB, ASK3-NX-8GB, ASK3-NX-16GB, ASK3-NX-32GB, ASK3-NX-64GB, ASK3-NX-128GB, ASK3-NX-256GB

ECCN / HTS / CAGE CODE
5A992.c / 8523.51.0000 / 3VYK8

STANDARDS / CERTIFICATIONS
FIPS 140-2 level 3
IP-67
TAA COMPLIANT

PACKAGE CONTENTS
Aegis NX, Protective Sleeve,
Multi-Language Quick-Start Guide

* To achieve these speeds, your computer's internal hard drive must be an SSD; all transfer rates will be limited by computer's internal drive
One gigabyte (GB) = one billion bytes; accessible capacity will be less and actual capacity depends on the operating environment and formatting.