Enova® X-Wall® DX

Frequently Asked Questions – FAQ Ver. 1.0

Q: What is "*X-Wall DX*"?

A: *X-Wall DX*, a USB-to-USB real-time crypto module capable of performing USB2.0 wire speed encryption to all connected USB MSC (Mass Storage Class), including USB flash drive, thumb drive, USB/SATA interfaced disk drive, SSD and Card Reader, is the ***ninth*** generation of the *X-Wall* real-time **full disk encryption** crypto module. It encrypts entire USB drives, including MBR, temporarily files and operating system with NIST/CSE certified hardware AES ECB/CBC strength up to 256-bit. The *X-Wall DX* can be mounted directly to either the USB 3.0/2.0 host or device (drive) interface, offering USB2.0 wire speed cryptographic performance.

Q: What is *Full Disk Encryption (FDE)*?

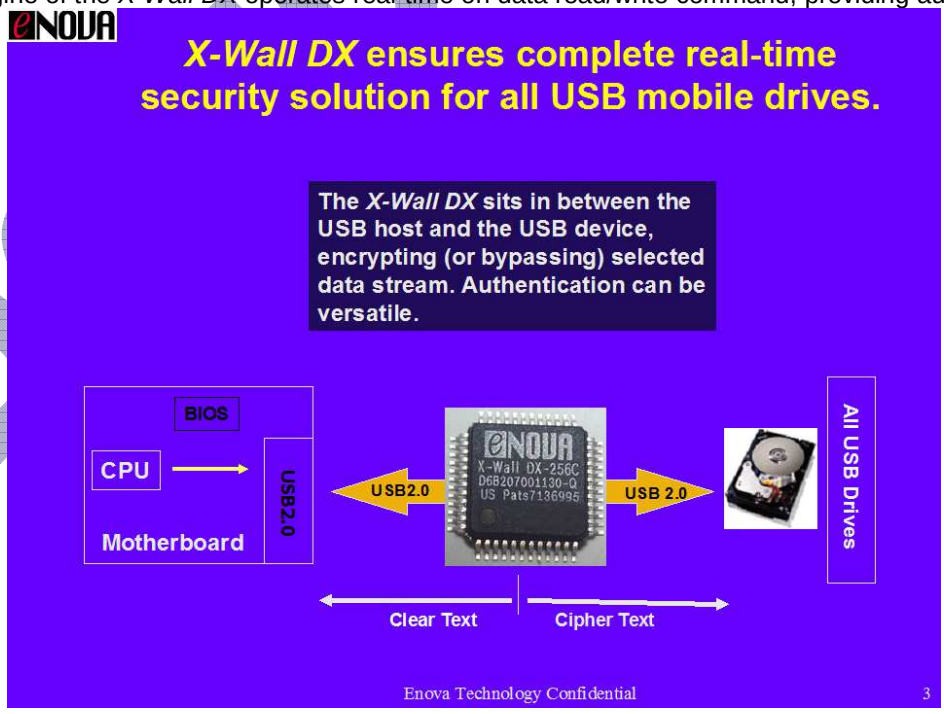
A: Full Disk Encryption is a real-time hardware based encryption technology that encrypts entire disk drive on command. Enova Technology (www.enovatech.com) invented this technology back in year 2000 and has been granted multiple patents including three issued patents in the U.S.A. Enova Technology pioneers the technology by introducing at least 9 generations of various *X-Wall* real-time encryption crypto processors and solutions for the past 10 years.

Q: What is *Self Encrypting Drive (SED)?*

A: The SED is FDE only with different name.

Q: How does *X-Wall DX* function?

A: Just like the *X-Wall* predecessors, the *X-Wall DX* sits between the USB host and USB drive, offering wire speed cryptographic performance. It intercepts, audits, translates and relays USB commands/controls & data to and from the disk drive. Data is automatically encrypted using the supplied AES Secret Keys, which can be delivered via either a secured serial interface or a secured built-in Application Programming Interface (API) on USB interface. The Cryptographic engine of the *X-Wall DX* operates real-time on data read/write command, providing automatic and



Copyright 2012, Enova Technology Corporation. All rights reserved.

transparent cryptographic operations to your disk drives.

In one application when data is read from the encrypted USB drive, *DX* decrypts before sending the data to the host. In yet another application, the data read can be cipher text which can then be sent over the public network. The encryption and decryption operations are totally transparent to all users, making *DX* invisible and independent to any operating system.

Q: What is the "Key Management" of *X-Wall DX*?

A: The *X-Wall DX* requires unique Secret Key to operate and function. At power up, the "Secret Key" is made available ***securely*** to the *DX* register interface using hardware or software protocol (authentication method). If the Secret Key was incorrect or missing, the *X-Wall DX* disallows access to the encrypted data on the USB drive. The *X-Wall DX* encrypted drive is a brick without the right secret key. This is true even if the *X-Wall DX* encrypted drive has been moved to a different platform in an attempt to by-pass the authentication. Attempts to surface scan the entire drive sectors/platters in order to access the encrypted data will be futile.

The authentication method can be versatile including PIN/Password, Numeric Keypad, Biometrics, Smartcard (including CAC and PIV cards), SSO or any combination. Please consult Enova Engineering (info@enovatech.com) for details.

Q: What SKU (Stock Keeping Units) are available in *X-Wall DX*?

A: We are currently maintaining four different SKU in the *DX* family crypto modules, namely:

SKU	**Package Type**	**Product Description**
X-Wall DX-128	48-pin QFP, RoHS & Lead Free	DX-128 USB crypto module w/ AES ECB 128-bit
X-Wall DX-128C	48-pin QFP, RoHS & Lead Free	DX-128C USB crypto module w/ AES CBC 128-bit
X-Wall DX-256	48-pin QFP, RoHS & Lead Free	DX-256 USB crypto module w/ AES ECB 256-bit
X-Wall DX-256C	48-pin QFP, RoHS & Lead Free	DX-256C USB crypto module w/ AES CBC 256-bit

Q: What is the AES cryptographic performance of an *X-Wall DX*?

A: *X-Wall DX* performs AES 256-bit cryptographic operation at USB 2.0 wire speed at 480Mbits/sec. Typical throughput of a connected USB2.0/SATA (and/or USB3.0/SATA) based disk drive will be somewhere between 25Mbytes/sec to 30Mbytes/sec. The throughput varies noticeably from different USB flash drive, thumb drive and card reader media however, which depends mostly on the type of USB flash controller and flash chips being deployed. Typical write performance of flash media ranges from 2Mbytes/sec to 15Mbytes/sec, which may be the reason that one needs to carefully choose the USB flash controller and flash media for the specific task. The operations of encryption and decryption are accomplished using high-speed hardware circuitry to ensure no measurable loss of performance. Software device drivers are not used to enable the *X-Wall DX;* thus memory and interrupt overheads are completely eliminated.

Q: Can *X-Wall DX* encrypt Blue Ray DVD, DVD RW and/or CD-R media?

A: Yes. The *X-Wall DX* can encrypt/decrypt generic USB interfaced or bridged interfaced (such as USB2.0/SATA or USB3.0/SATA) Blue Ray DVD, DVD RW and CD-R media real-time.

Q: What happens when an *X-Wall DX* encrypted Blue Ray DVD, DVD RW and/or CD-R media is lost or stolen?

A: The encrypted media will be seen as a brick (brand new media without being previously formatted) without the presence of the *X-Wall DX*.

Q: What happens when an *X-Wall DX* encrypted USB drive is lost or stolen?

A: The encrypted USB storage will be seen as a brick (brand new storage without being previously formatted) without the presence of the *X-Wall DX*.

DO NOT COPY

Copyright © 2012, Enova Technology Corporation. All Rights Reserved.

Q: Does *X-Wall DX* support 4KB/sector drives?

A: Yes. *X-Wall DX* encrypts standard 512 bytes per sector drive as well as 4K bytes per sector drive, irregardless any geometry. If you have a 3TB hard drive, the entire 3TB will be encrypted with AES strength.

Q: Does *X-Wall DX* support drive capacity over 2TB (2 Terabytes)?

A: Yes. *X-Wall DX* supports drive over 2TB per drive with an exception over a Multi-LUN Composite Device such as Western Digital "My Book Studio Edition 4TB" which by itself is an HID/SES and Mass Storage composite device.

Q: Does X-Wall DX support various file systems?

A: Yes. *X-Wall DX* supports all file systems including FAT, FAT32, NTFS, Linux and MAC OS. Note that file system in MAC OS may not be compatible with other file systems as usually seen in a PC Windows environment.

Q: Why choose the *X-Wall DX* over FDE or SED?

A: Convenience, simplicity and security. Unlike limited selection over FDE and SED drives which usually involves with using costly key management software, *X-Wall DX* works reliably with every drive with any geometry and you get to control your own secret key.

Q: Do I need to establish a separate "encrypted folder" under file directory as required by some software solutions?

A: No. All data written to the disk drive via the *X-Wall DX* is automatically encrypted. There is no exception that clear text is left unprotected.

Q: If I back my data up to an external drive, is that backed up data encrypted?

A: Yes as long as you backup your data using another *X-Wall DX* crypto module. Or choose the ***X-Wall FX*** (USB-to-SATA) crypto module enabled external enclosure for data backup.

Q: Is *X-Wall DX* compatible with various operating systems?

A: Yes – the *X-Wall DX* is independent from all operating systems, and does not require device drivers. It supports popular MAC OS (10.6 and 10.7), Windows (7, Vista, XP 32/64-bit), Linux and Android.

Q: Do I need any training to use *X-Wall DX*?

A: The good news is that you don't have to learn or manage anything. You use the *X-Wall DX* enabled key dongle just like using your regular USB drive. At first insertion of both DX key dongle and the USB drive, the OS detects the storage then asks if you want to format the drive. Click YES and every operation from there is automatic and transparent.

Q: How is key length related to security?

A: In the case of Symmetric Cipher (DES, TDES, and AES), a larger Cryptographic Key length creates a stronger cipher, which means an intruder must spend more time and resources to find the Cryptographic Key. For instance, a DES 64-bit strength represents a key space of 72,057,594,037,927,936 (2^{56}, 2's power 56) possible combinations. While this number may seem impressive, it is definitely feasible for a microprocessor or a specially designed ASIC to perform the huge number of calculations necessary to derive the Cryptographic Key. Surprisingly an investment of only about US$10,000 investment in FPGA (Field Programmable Gate Arrays) will be able to recover a 64-bit key in several days. Further, a US$10,000,000 investment in ASIC will be able to recover a 64-bit key in a few seconds. A government agency that can afford investing US$100,000,000 or more will be able to recover a 64-bit key in a fraction of a second! Thus a 64-bit length symmetric cipher offers a bare minimum protection for your confidentiality

DO NOT COPY

Copyright © 2012, Enova Technology Corporation. All Rights Reserved.

and privacy. Fortunately, the "work factor" increases exponentially as we increase the key length. For example, an increase of one bit in length doubles the key space, so 2^{57} represents key space of 144,115,188,075,855,872 possible combinations. A TDES 128-bit cipher offers extremely strong security (5,192,296,858,534,827,628,530,496,329,220,096 possible key combinations) that should resist known attacks for many years to come, considering the advance of semiconductor design and manufacturing. The new AES key length does not come with any parity bit. Therefore, unlike the TDES counterpart, an AES 128-bit has a real key length of 128-bit, meaning a key combination of 3.40282366920938463463374607431768e+38. An AES 256-bit key length will have a key combination of 1.15792089237316195423570985008687e+77.

Q: How secure is *X-Wall DX-128* (AES 128-bit strength)?

A: *X-Wall's* hardware-based real-time cryptographic solution significantly reduces a hacker's successful entry into the encrypted disk drive. Every incorrect entry to the Cryptographic Key requires a hardware power cycle. To hack an *X-Wall DX-128* encrypted disk drive, one must process at least hundred of thousand trillion times (50% of the available key space) reboots. The hardware would fail way before the one million attempts. As such, an *X-Wall* product using 128-bit encryption strength will be strong enough to withstand physical attack as well as sophisticated computer attacks.

Q: Has the Enova *X-Wall DX* product line been US Government certified?

A: Several times over. Enova's *DX* hardware AES cryptographic engines have been certified by ***NIST*** *(National Institute of Standards and Technology) and* ***CSE*** *(The Communications Security Establishment).* These certificates are available on NIST web links: (http://csrc.nist.gov/cryptval/des/desval.html and http://csrc.nist.gov/cryptval/des/tripledesval.html). These hardware algorithms are certified to provide reliable security. At full strength, it is virtually impossible to access the encrypted data by guessing or deriving the right AES Key. All data at rest on the disk drive is encrypted, which means that the data on that drive is safe even if attackers try to boot from their own disk, or to move your disk to an unprotected machine.

Q: Other than algorithm being certified, is FIPS 140-2 certification available?

A: The FIPS 140-2 level 2 certification of the X-Wall DX crypto module is in progressing. Contact us for more information.

Q: Should I expect a lengthy login procedure and complex GUI that other systems require?

A: **No, not at all.** *DX* has been carefully designed not to change the user's regular computing behavior, nor does it require learning a complex GUI. Enova's objectives include building a secure product that will make the user's life a little more enjoyable. The user is not required to memorize frequently used and cumbersome log on procedures. You need only to present your DX *Key* Dongle every time you attempt to access your encrypted disk. Period.

Q: If the *X-Wall DX* malfunctions, will I lose my data?

A: **No, as long as you maintain your own Secret Key.** The same *X-Wall DX* crypto module can be replaced to allow data retrieval.

Q: What's the likelihood of an *X-Wall DX* malfunction?

A: Extremely unlikely. Every *X-Wall* family microchip is tested and complies with International quality assurance standards[1] prior to being shipped. Enova employs a zero tolerance policy for such errors. However, there may be occasions that a chip might malfunction after some period of time,

[1] Our quality assurance program including reliability tests are performed in accordance with MIL-STD-883E as the prime standard and with JEDEC-STD, where applicable. The JEDEC (Joint Electronic Device Engineering Council) Solid State Technology Association is the semiconductor engineering standardization body of the Electronic Industries Alliance (EIA), a trade association that represents all areas of the electronics industry.

DO NOT COPY

Copyright © 2012, Enova Technology Corporation. All Rights Reserved.

or at some unique unpredictable circumstances. This problem can be resolved by simply replacing the defective *X-Wall DX* with the same crypto module**.** A malfunctioning *X-Wall DX* unit can easily be replaced, and the encrypted contents of the disk drive will be intact and accessible (as long as the original "Secret Key" is intact).

Q: Can I exchange the *X-Wall DX* encrypted files over the public Internet?

A: **Yes or No, depends on the solutions you had obtained. See additional FAQ over the solution page**.

Q: Does *X-Wall DX* increase the original file size after encryption?

A: No. AES is an encryption algorithm that computes the original data with 128/192/256-bit cryptographic key length. Regardless of the size of the key, the size of data file after encryption remains unchanged.

DO NOT COPY

Copyright © 2012, Enova Technology Corporation. All Rights Reserved.