

Enova® X-Wall® DX

Frequently Asked Questions – FAQs

More questions? info@enovatech.com

Q: What is “X-Wall DX”?

A: *X-Wall DX* is the seventh generation of the *X-Wall* real-time full disk encryption technology. *X-Wall DX* equips with standard Serial ATA (SATA) interfaces and provides 1.5Gbit/sec cryptographic throughput to entire SATA disk drive, including boot sector, temp files, swap files, **and** the operating system. *X-Wall DX* is a hardware-based cryptographic ASIC (Application Specific Integrated Circuit) that can be mounted directly to either the SATA host or device (drive) interface, offering wire speed with NIST and CSE certified TDES cryptographic strength up to 192-bit key length. The *X-Wall DX* can also be engineered to work on the USB interfaced portable SATA storage by connecting behind a USB to SATA bridge chip and before the SATA disk drive.

Q: How does X-Wall DX function?

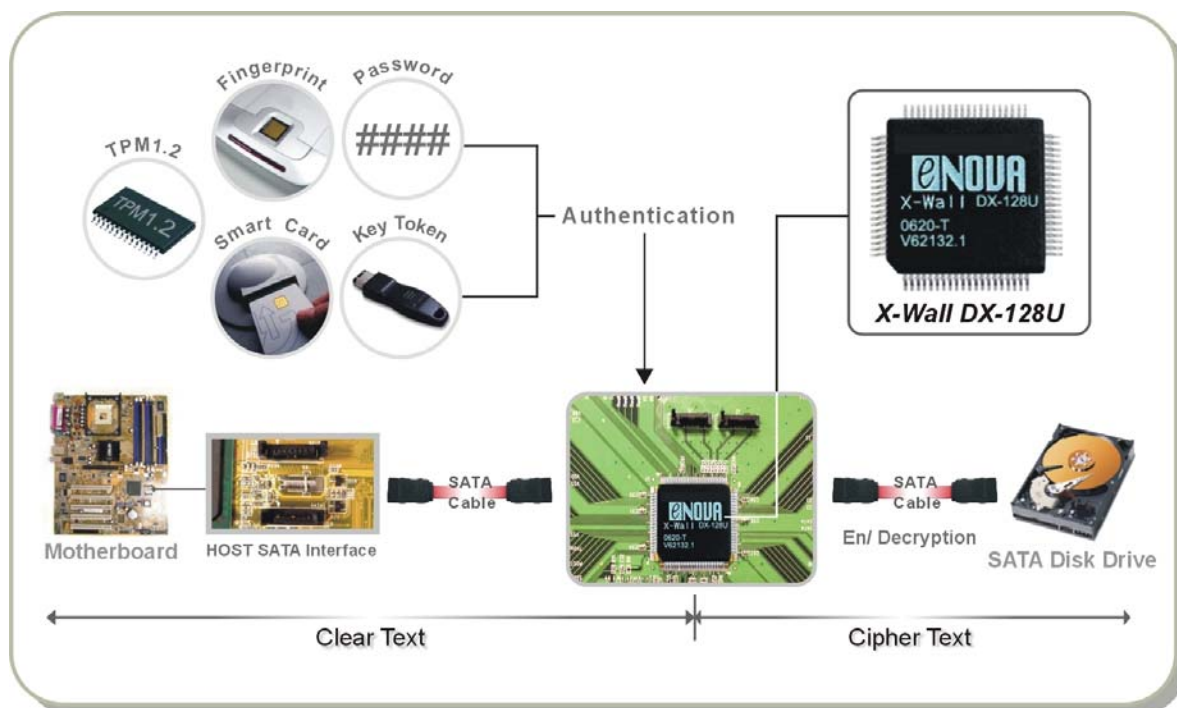
A: Enova's *X-Wall DX* sits before your SATA disk drive on the SATA interface, offering wire speed performance for the entire cryptographic operations. It intercepts, measures, audits, interprets, translates, and relays SATA commands/controls & data to and from the disk drive. Data is automatically encrypted using the externally provided Secret Keys. The Cryptographic engine of the *X-Wall DX* operates real-time on data read/write command, providing automatic and transparent cryptographic operations to your SATA disk drive.

When data is read from the disk drive, *DX* decrypts before sending the data to the host. The encryption and decryption operations are totally transparent to the user, making *DX* invisible and independent to any system platforms (Operating Systems).

The *X-Wall DX* requires unique Secret Keys to operate and function. At power up, the “Secret Key” is externally delivered to the *DX* internal register sets, using a proprietary hardware and/or software protocol (authentication method). If the Secret Key was incorrect or missing, *DX* will not allow access to the encrypted data on the disk drive. The X-Walled hard drive will be seen as a new drive as the entire encrypted content remains protected and secure. This is true even if the X-Walled hard drive has been moved to a different platform in an attempt to by-pass the authentication. Attempts to surface scan the entire disk drive platters in order to access protected data will be futile.

The authentication method can be versatile including PIN/Password, Fingerprint, any other Biometrics, Smartcard, TPM (Trusted Platform Module) or any combination. One popular form to authenticate the *DX* secured disk drive is to use the simple but effective Key Token, which contains the “Secret Key” used by the *DX* cryptographic engine. Without this unique key token, attempts to access the encrypted data will be unsuccessful, even when the disk drive is moved to a different PC platform.

The Enova *DX* is a generic engine and it relies on the “Secret Key” to enable all functionalities. The following illustration best describes how the *X-Wall* functions.



Q: How does X-Wall DX differ from previous versions?

A: DX improvements over previous models include:

Generic SATA Interface – DX is equipped with standard SATA interfaces that can be operated on standard SATA disk drives at 1.5Gbit/sec cryptographic real-time throughput.

Power On Self-Test (POST) – DX is equipped with POST, which facilitates manufacturing and testing procedures. Upon power up, the POST executes standard cryptographic “known answers test” to verify the functionalities of the crypto engine. A software poll reveals a functional DX ASIC.

Low Power Consumption – the DX is engineered with advanced 0.18 micron technology (0.18u) that offers lower power consumption for power sensitive applications. The DX can burst a SATA disk drive at 150MB/sec, which is the maximum bandwidth a modern SATA 1.0a compliance disk drive allows.

Multiple Key Loads – the DX features multiple key loads during the same power cycle. This feature allows changing to a different key without additional power on reset cycle. It is particularly useful during drive re-purposing or disposing stage as the old key information will be replaced by the new key, rendering the old content (that are encrypted with the old key) completely illegible.

Keys Rotation – the DX allows the drive that was encrypted with the first Key to be decrypted via the first Key then re-encrypted with the 2nd Key without taking the physical drive off line. These controls can be done through internal register settings and some software works. For instance, a firmware code can decrypt the encrypted hard drive (with Key 1) then re-encrypt it with the new Key 2 without additional power on reset cycle. This feature is useful in term of frequently swapping the secret key value to safeguard the sensitive information.

The **secret key value** is secret to the internal registers of DX thus can not be read out from any external interface. Beside, DX does not contain non-volatile memory thus prying effort using semiconductor extraction over the non-volatile memory is futile.

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

A: X-Wall DX-128U – RoHS & Lead-free compliant TDES 128-bit encryption strength
X-Wall DX-192U – RoHS & Lead-free compliant TDES 192-bit encryption strength

Q: How can X-Wall DX encrypt the entire disk without sacrificing drive performance?

A: X-Wall DX is specifically engineered for high speed communications with the disk drive through built-in SATA 1.0a interface. It offers 1.5 Gbit/sec throughput to enable real-time communications with all Serial ATA 1.0a compliant disk drives. The operations of encryption and decryption are accomplished using high-speed hardware circuitry to ensure no measured loss of performance. Software device drivers are not used to enable the DX; thus memory and interrupt overheads are completely eliminated.

Q: Is there a capacity limitation as are other products?

A: No. X-Wall DX encrypts all disk volume, irregardless any geometry. If you have a 1TB hard drive, the entire 1 TB will be encrypted with TDES strength.

Q: Can DX encrypt logical drive?

A: Yes, as long as the designer has total control over using file system. X-Wall DX allows switching **crypto** vs. **by-pass** modes of operation, enabling flexibility in reading and/or writing to specific sector under respective mode of operation.

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, if switching mode of operation is not being chosen.

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

A: No if you do not have a DX secure external drive as data leaving the DX interface is automatically decrypted. Thus writing to an external drive without DX built-in presents only clear text. If the external backup drive has an Enova X-Wall DX chip installed, all data backed up will be encrypted. Enova recommends that your backup device be capable of encrypting its contents and that you back your data up on a regular basis. To enable your secure back up, Enova recommends using Enova Secure USB2.0 to IDE (or USB2.0 to SATA) external storage device. See below web link for product description and other available Enova products: http://www.enovatech.net/products/reference/usb2.0_ide.htm.

Q: Can X-Wall DX work with all types of disk drives?

A: The Enova DX products are compatible with all SATA interfaced disk drives. X-Wall DX can be operated with SATA 1.0a/2.0 compliant disk drives with throughput of 1.5 Giga bit per second. X-Wall DX is not compatible with SCSI or FC (fiber-channel) interfaces. Future plans are to increase the transfer throughput to 3Gbit/sec ore more using the same SATA or enhanced serial interfaces.

Q: Can X-Wall DX work with all types of operating systems?

A: Yes -- the X-Wall DX is compatible with all operating systems, and does not require device drivers. The only requirement is a SATA compliant disk drive.

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. After successful authentication, or inserting the Key Token as an example, everything will function as before. Before you can use a DX enabled system/disk drive, you must use the “Secret Key” that comes

with the authentication method to partition (FDISK) and format (FORMAT) the drive. The figure below presents an Enova *Secure Key*. There is no bad news.

Q: How does X-Wall DX compare with Smart Card and PCMCIA encryption products?

A: Speed and Simplicity. X-Wall DX operates at drive interface speeds, and is much faster than



PCMCIA or Smart Card solutions. In addition, DX does not tax the Motherboard CPU, putting power back into the User's hands. DX encrypts all data on the disk drive, as opposed to selected files or directories. There is **no** possibility that any data or credentials will be unprotected on the hard drive. Drive locking and boot sector encryption solutions do **not** encrypt the data, leaving the data vulnerable to attack.

Q: Can I encrypt two or more hard drives via a single X-Wall DX?

A: No. DX can only work with one single hard drive. Multiple drives will require corresponding number of DX chips. Consult us for more engineering details.

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 40-bit strength represents a key space of 1,099,511,627,776 (2^{40} , 2's power 40) 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 40-bit key in 12 minutes. Further, a US\$10,000,000 investment in ASIC will be able to recover a 40-bit key in 0.05 second. A government agency that can afford investing US\$100,000,000 or more will be able to recover a 40-bit key in a whopping 0.002 second! Thus a 40-bit length cipher offers a bare minimum protection for your confidentiality 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^{41} represents key space of 2,199,023,255,552 possible combinations. A 2^{112} bit (128-bit key length taken out 16 parity bits) TDES cipher offers extremely strong security (5,192,296,858,534,827,628,530,496,329,220,096 possible combinations) that should resist known attacks for the next 15 to 20 years, considering the advance of semiconductor design and manufacturing. Just a note that AES key length does not come with parity. Therefore, unlike the TDES counterpart, an AES 128-bit has a real key length of 128-bit.

Q: How secure is X-Wall DX-192U (TDES 192-bit strength)?

A: X-Wall's hardware-based real-time cryptographic solution significantly reduces a hacker's successful entry into the disk drive. Every incorrect entry to the Cryptographic Key requires a hardware power cycle. To hack an X-Wall DX-192U encrypted disk drive, one must process at least hundred of thousand trillion times (50% of the available key space) reboots. As such, an X-Wall product using 192-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 certified by government agencies?

A: Several times over. Enova's DX hardware TDES 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 TDES 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: 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 Key token every time you power up your computer -- It is totally transparent to all users.

Q: Does the Key token provide authentication of the user?

A: **Yes.** Enova's Key token contains a **Cryptographic Key**. This key is used by X-Wall DX to encrypt or decrypt data on the disk drive. Without this key, the disk drive **cannot** be booted or accessed. The Key token and X-Wall DX create an effective user authentication for access control, and strong encryption for data protection. The Key token serves as user authentication for access control, while the X-Wall DX encrypts and decrypts all data at rest on the disk drive.

Q: Does DX support other authentication methods such as TPM, Fingerprint, Password, and Smartcard?

A: **Yes.** The X-Wall DX is a generic cryptographic engine that needs to be enabled by external authentication methods. The authentication methods can be versatile, as long as the Secret_Key will be delivered to DX at proper timing. The DX design guide offers details on implementations. Please contact us at info@enovatech.com for details.

Q: What happens if my Key token is lost or stolen?

A: There are no "backdoors" into X-Wall DX secure systems, so without the original Key token you will not be able to access the data or operating system on the protected disk drive. This means you must keep the key token in a safe place at all times. Enova Technology has developed several key management systems that will allow the trace of lost keys. For the security conscious, you now have the ability to generate and maintain your own key distribution. For more information about how to manage the key token, please go visit: http://www.enovatech.net/key_management.htm

Q: Can I order duplicate Key Tokens?

A: Yes. You can order duplicate Key Tokens from your reseller/distributor or directly from Enova Technology. Please visit our web site http://www.enovatech.net/key_management.htm or write to us info@enovatech.com for details. Note: Enova Technology does not maintain a database of Key Token unless customers specifically require it. To have additional keys made, you must send your backup key with your order for duplication.

Q: Can I remove the Key token while my PC is on?

A: Yes. The Key token can be removed for safekeeping after your operating system has fully loaded. Remember that the Key token **must** be used the next time you power up your PC or resume after the PC has been in hibernation.

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

A: **No, as long as your original Secret Key is intact.** The DX is a generic cryptographic engine and the Key token (or any authentication method) contains the TDES cryptographic key.

Consequently, you can simply replace the defective *X-Wall DX* component, if that ever occurs, and use your original Secret Key to access the data on your hard drive.

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 standards¹ 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, or at some unique unpredictable circumstances. This problem can be resolved by simply replacing the defective *DX* with the same microchip. A malfunctioning *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).

In the case of using Enova Key Token as a mean of authentication, the contents of the disk drive will not be lost as long as you retain the original *Key token*. Nevertheless, disk drive failures can occur, so it is good practice to always keep a backup of your important data, for which we do have a good secure solution on the back up device: Enova Secure USB2.0 to IDE. Please refer to http://www.enovatech.net/products/reference/usb2.0_ide.htm for details. In case of system failure, please double-check with your disk drive prior to reporting any malfunction of the *X-Wall*.

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

A: **Yes, as long as the designer can have full control of the file system.** The *DX* allows switching over crypto vs. by-pass mode of operations. Cipher text transfer over the public network will be made possible without utilizing a traditional SSL (Secure Socket Layer) or PKI (Public Key Infrastructure). Contact Enova for design details.

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

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

Q: I am currently using the *X-Wall DX-128* (TDES 128-bit strength). Can I upgrade the same disk drive to an *X-Wall DX-192* (TDES 256-bit strength)?

A: **Yes.** Follow these two essential steps:

1. You can order the *X-Wall DX-192U circuit board* from your supplier. The package you will receive will have a new *Key token*.
2. Copy the content of your disk drive to a safe location, and then install the new *X-Wall DX-192U* board and restore the data to the disk drive using the new *Key token*. This is necessary because the disk content will be lost due to re-performing of FDISK and FORMAT commands. Only one cipher strength can be used on the same disk drive.

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.