Enova® X-Wall® MX

Frequently Asked Questions – FAQs Ver. 4

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

A: *X-Wall MX* is the seventh generation of the *X-Wall* real-time full disk encryption technology. *X-Wall MX* equips with both host and device side standard Serial ATA (SATA) interfaces and provides sustained 150MB/sec cryptographic AES (up to 256-bit strength in both ECB and CBC mode of operation) throughput to entire SATA disk drive, including boot sector, temp files, swap files, **and** the operating system. *X-Wall MX* is a hardware-based cryptographic processor that can be mounted directly to either the SATA host or device (drive) interface, offering wire speed NIST and CSE certified AES cryptographic strength up to 256-bit key length. The *X-Wall MX* 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 MX* function?

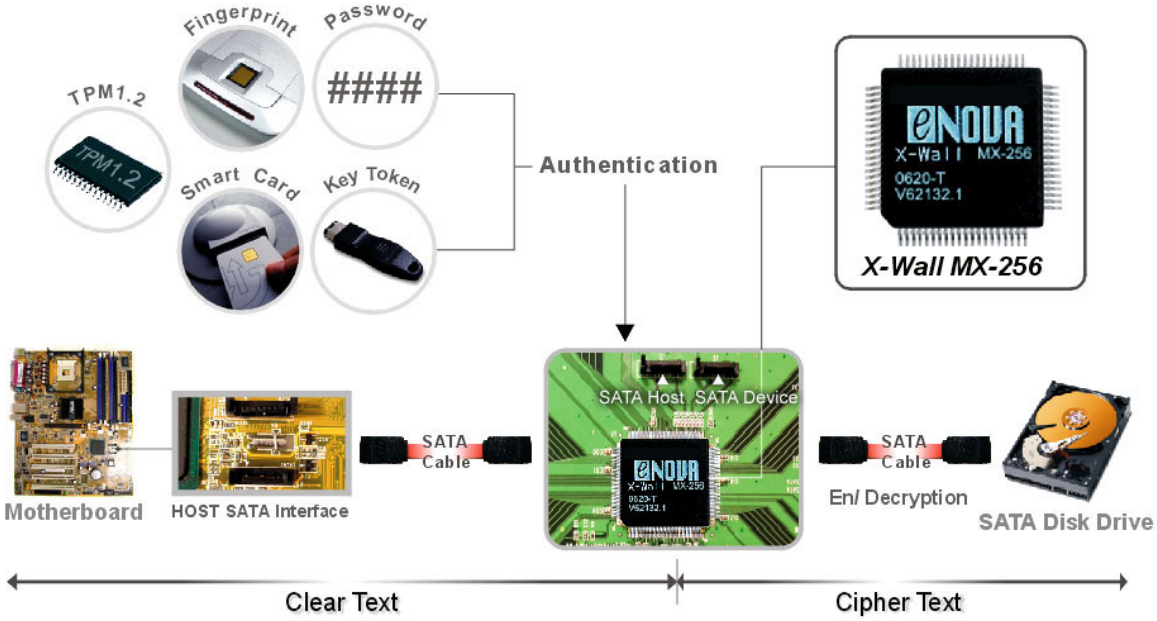
A: Enova's *X-Wall MX* sits before your SATA disk drive on the SATA interface, offering wire speed performance for the entire cryptographic operations. It intercepts, measures, audits, interprets, translates, and relays SATA commands/controls & data to and from the disk drive. Data is automatically encrypted using the supplied AES Secret Keys, which can be delivered via either a serial interface or a built-in Application Programming Interface (API) on SATA interface. The Cryptographic engine of the *X-Wall MX* 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, *MX* decrypts before sending the data to the host. The encryption and decryption operations are totally transparent to the user, making *MX* invisible and independent to any system platforms (Operating Systems).

The *X-Wall MX* requires unique Secret Keys to operate and function. At power up, the "Secret Key" is externally delivered to the *MX* internal register sets, using a proprietary hardware and/or software protocol (authentication method). If the Secret Key was incorrect or missing, *MX* 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 (including CAC and PIV cards), TPM (Trusted Platform Module) or any combination. One popular form to authenticate the *MX* secured disk drive is to use the simple but effective Key Token, which contains the "Secret Key" used by the *MX* cryptographic engine, or as simple as using a user's password entry. Without the precise authentication, attempts to access the encrypted data will be unsuccessful, even when the disk drive is moved to a different PC platform.

The Enova *MX* is a generic cryptographic processor 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 MX* differ from previous *versions?***

A: ***MX improvements over previous models include:***

Generic host and device side SATA Interface – MX is equipped with standard SATA interfaces that can be operated on standard SATA 1.0a and SATA 2.0 disk drives at a sustained 150MB/sec cryptographic real-time throughput.

Power On Self-Test (POST) – *MX 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 can reveal a functional *MX* ASIC.

Low Power Consumption – the *MX* is engineered with advanced 0.18 micron technology (0.18u) that offers lower power consumption for power sensitive applications. The *MX* can sustain throughput at 150MB/sec.

Multiple Key Loads – the *MX* 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 *MX* 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 *MX* thus can not be read out from any external interface. Beside, *MX* 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 MX*?

A: *X-Wall MX-128* – RoHS & Lead-free compliant AES 128-bit encryption strength under ECB mode.
X-Wall MX-256 – RoHS & Lead-free compliant AES 256-bit encryption strength under ECB mode.
X-Wall MX-128C – RoHS & Lead-free compliant AES 128-bit encryption strength under CBC mode.
X-Wall MX-256C – RoHS & Lead-free compliant AES 256-bit encryption strength under CBC mode.

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

A: *X-Wall MX* is specifically engineered for high speed communications with the disk drive through built-in SATA interface. It offers a sustained 150MB/sec throughput to enable real-time communications with all Serial ATA 1.0a and SATA 2.0 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 *MX;* thus memory and interrupt overheads are completely eliminated.

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

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

Q: Can *MX* encrypt logical drive?

A: Yes, as long as the designer has total control over using file system. *X-Wall MX* 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 MX* 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 *MX* secure external drive as data leaving the *MX* interface is automatically decrypted. Thus writing to an external drive without *MX* built-in presents only clear text. If the external backup drive has an Enova *X-Wall MX* 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 MX* work with all types of disk drives?

A: The Enova *MX* products are compatible with all SATA interfaced disk drives. *X-Wall MX* can be operated with SATA 1.0a/2.0 compliant disk drives with sustained throughput of 150MB/sec. *X-Wall MX* is not compatible with SCSI or FC (fiber-channel) interfaces. Future plans are to increase the transfer throughput to 300MBsec ore more using the same SATA or enhanced serial interfaces.

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

A: Yes -- the *X-Wall MX* is independent from 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 MX*?

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 *MX* 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 MX* compare *w*ith Smart Card and PCMCIA encryption products?

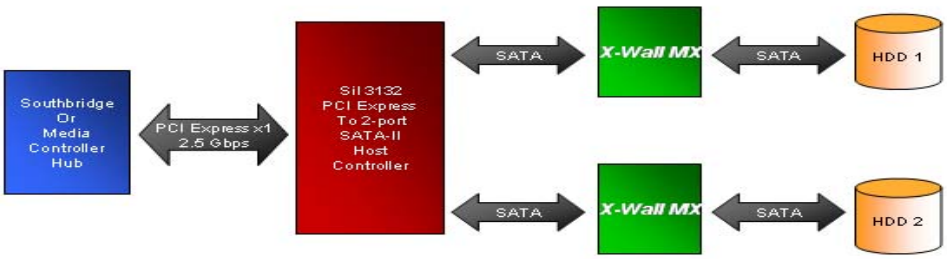
A: **Speed and Simplicity.** *X-Wall MX* operates at drive interface speeds, and is much faster than PCMCIA or Smart Card solutions. In addition, *MX* does not tax the Motherboard CPU, putting power back into the User's hands. *MX* encrypts all data on the disk drive, as opposed to selected files or 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 *X-Wall MX* support a SATA RAID Controller?

A: Yes. Enova's *MX* can work with any SATA RAID controller. Illustration shown below is an example of how to design a real-time encrypted mini storage tower using both *X-Wall MX* and Silicon Image's Sil 3132 RAID controller. The typical connection of using an Sil3132 RAID controller is to connect one SATA drive on its respective SATA channel, making a simple two drives RAID 0 or 1 operation. See below Figure 1 for a normal RAID connection without MX features.

A generic PCI Express to SATA RAID Controller that connects two SATA disk drives on respective channels.

Adding a real-time *X-Wall MX* real-time full disk encryption technology is simple. As illustrated in Figure 2, simply add one *X-Wall MX* right on the respective SATA channels in front of a SATA drive, enabling full disk encryption to the connected SATA drives.



A generic PCI Express to SATA RAID Controller that has *X-Wall MX ASIC controls* SATA disk drive on respective channels.

The two *X-Wall MX* chips get to use the same or different secret key, depending on how the key management scheme will be structured. As simple and effective as an Enova Key Fob and be deployed on the chassis of a mini storage tower. Sophisticated key management scheme can also be devised and the solution may vary from some unique applications.

Q: Can *X-Wall MX* support a Port Multiplier?

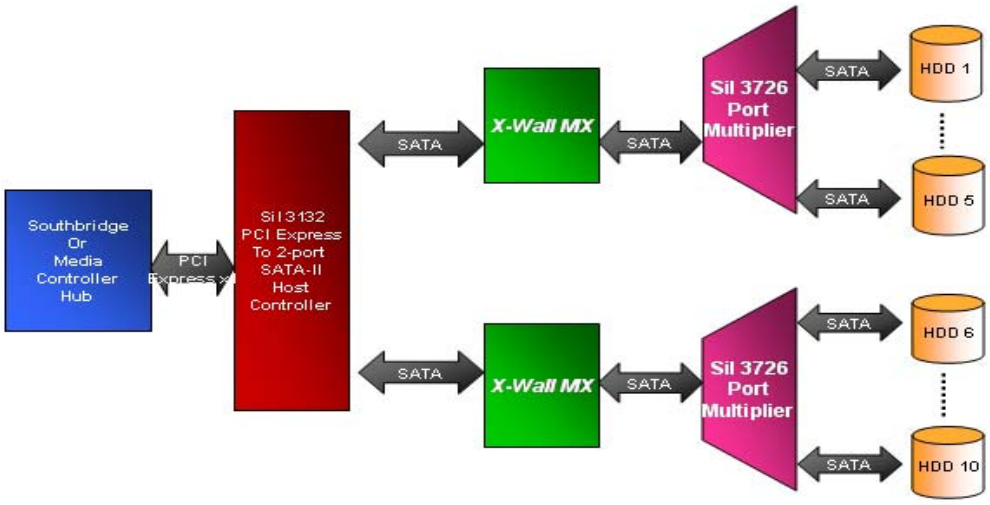
A: Yes. Enova's *MX* can work with a Port Multiplier to enable multiple connected SATA drives with the same cryptographic AES strength. A Port Multiplier such as the one from Silicon Image Sil3726 can be used to connect to any available SATA host port while allows to operate up to 5 (five) SATA drives. This simple connection, without *MX* features, is illustrated below:

SATA Host Port → Sil 3726 Port Multiplier → Connected up to 5 (five) SATA drives

Adding an *X-Wall MX* right before the Port Multiplier but after the SATA Host Port allows full disk encryption capability to all 5 (five) connected SATA drives. The best part of this configuration is that one *X-Wall MX* encrypts all Port Multiplier connected SATA drives. The MX features enabled structure is illustrated below:

SATA Host Port → ***X-Wall MX*** → Sil 3726 Port Multiplier → Connected up to 5 (five) SATA drives

Figure shown below illustrates how an *X-Wall MX* enables a Port Multiplier that in turn controls the RAID stacked SATA disk drives.



A generic PCI Express to SATA RAID Controller that has *X-Wall MX* ASIC controls a Port Multiplier that in turn controls multiple SATA disk drive to form a RAID configuration on respective channels.

Q: Can *X-Wall MX* work with a {SATA RAID+Port Multiplier} configuration?

A: Yes. Please reference to above illustration in Q&A.

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 MX-128* (AES 128-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 MX-128* 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 128-bit encryption strength will be strong enough to withstand physical attack as well as sophisticated computer attacks.

Q: Has the Enova *X-Wall MX* product line been certified by government agencies?

A: Several times over. Enova's *MX* 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: Should I expect a lengthy login procedure and complex GUI that other systems require?

A: **No, not at all.** *MX* 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 MX* 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 MX* 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 MX* encrypts and decrypts all data at rest on the disk drive. See below illustration of Enova Key Fob.

Enova Key Fob

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

A: **Yes.** The *X-Wall MX* 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 *MX* at proper timing. The *MX* 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 MX* 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 MX* malfunctions, will I lose my data?

A: **No, as long as your original Secret Key is intact.** The *MX* is a generic cryptographic engine and the *Key* token (or any authentication method) contains the AES cryptographic key. Consequently, you can simply replace the defective *X-Wall MX* 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 MX* 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, or at some unique unpredictable circumstances. This problem can be resolved by simply replacing the defective *MX* with the same microchip. A malfunctioning *MX* 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 MX* encrypted files over the public Internet?

A: **Yes, as long as the designer can have full control of the file system.** The *MX* 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 Technology for design details.

Q: Does *X-Wall MX* 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.

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

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

[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.

1. You can order the *X-Wall MX-256 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 MX-256* 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.

