Enova® X-Wall® MX+

Frequently Asked Questions – FAQs Ver 1.0

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

A: *X-Wall MX+* is the tenth generation of the *X-Wall* real-time full disk encryption technology family. *X-Wall MX+* equips with both host and device side Serial ATA (SATA) interfaces and protocol stacks and can provide a maximum of 6Gbps (six gigabit per second) AES ECB/CBC/XTS 256-bit strength throughput to the connected SATA disk drive (SSD included), 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 onto either the SATA host or device (drive) interface. The operation of which is independent from to all operating systems. More, the *X-Wall MX+* can also be engineered to work with the latest USB3.0/USB3.1 to SATA bridge, making a secure portable storage.

The *X-Wall MX+* is currently a candidate for FIPS 140-2 Level 2 or 3 single chip crypto module certification.

Q: How does *X-Wall MX+* function?

A: Enova's *X-Wall MX+* ***sits in-line*** before your SATA disk drive on the SATA interface, offering wire speed cryptographic performance. 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 built-in 2-wire serial interface or an 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 the connected 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 transparent to both the host computer and the disk drive, making *MX+* invisible and independent to any operating system.

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. Your disk drive without a valid secret key will be seen as an un-initialized unformatted drive while the entire content remains encrypted. This is true even if the disk drive has been moved to a different platform to by-pass the authentication. Attempts to surface scan the entire disk drive platters or sectors to access encrypted data will be futile.

The X-Wall MX+ came equipped with various FIPS 140-2 approved authentication mechanisms including RSA 2048 DS (Digital Signature), HMAC (Key-Hashed Message Authentication Code), CMAC (Cryptographic Message Authentication Code), SHA256, DRBG_RNG, AES ECB/XTS/CBC engines and TRNG 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. Thanks to the enhanced *MX+* HMAC capability, the Key Token can now be secured as the communications on the 2-wire serial bus, where the Key Token resides, can now be encrypted. Without the precise authentication, attempts to access the encrypted data will be unsuccessful, even when the disk drive is moved to a different platform.

Q: How does *X-Wall MX+* differ from previous *versions?*
A: *MX+ improvements over previous models include:*

SATA Interface Speed at Generation 2 and 3 – *MX+* can support SATA generation 2 at 3Gbps (three gigabit per second) and generation 3 at 6Gbps cryptographic 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 nanometer technology that offers lower power consumption for power sensitive applications.

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. This feature is useful in term of frequently swapping the secret key value to safeguard the sensitive information.

Volatile Key Registers - The **secret key along with other critical security parameters** are secret to the internal volatile registers of *MX+* and cannot be read out from any external interface.

Q: What SKU (Stock Keeping Units) are available?
A:

X-Wall MX+ xF[1]	**MX+ SATA crypto module, FIPS 140-2 certified**
X-Wall MX+ xN[2] (or X-Wall MX+ D)	**MX+ SATA crypto module, None FIPS 140-2**
--------- MX+e	*X-Wall MX+* ECB 256-bit FDE
--------- MX+c	*X-Wall MX+* CBC 256-bit FDE
--------- MX+s	*X-Wall MX+* XTS 256-bit FDE
--------- MX+eO	*X-Wall MX+* ECB 256-bit SED, OPAL2.0/IEEE1667

For example, to order an *MX+* ECB FDE with none FIPS, the correct SKU would be *X-Wall MX+eN.* Likewise, to order an *MX+* XTS FDE with none FIPS, the correct SKU would be *X-Wall MX+sN*. Yet another example, to order an *MX+* CBC FDE with FIPS certification, the correct SKU would be *X-Wall MX+cF.*

[1] Where "x" denotes selection over e, c, or s.
[2] Where "x" denotes selection over e, c, s or eO. The xN part is equivalent to the D part for both electrical and functional aspects.

Q: Can *X-Wall MX*+ support TCG OPAL 2.0 specification?
A: Yes, the *X-Wall MX*+ supports TCG OPAL2.0 specification. It automatically converts **ANY** standard SATA drive into a TCG OPAL2.0 drive regardless of any capacity

Q: Can *X-Wall MX*+ support Mac OS X?
A: Yes, the *X-Wall MX*+ supports Mac OS X as it is operating system independent.

Q: Can *X-Wall MX*+ support Linux or Unix?
A: Yes, the *X-Wall MX*+ supports Linux or Unix as it is operating system independent.

Q: Can *X-Wall MX*+ support eDrive specification?
A: Yes, the *X-Wall MX*+ supports eDrive, especially Microsoft EHDD (Encrypted Hard Disk Drive) specification. In fact, the *X-Wall MX*+ is certified by Microsoft EHDD with certified logo shown below:

Q: Can *X-Wall MX*+ work with all types of disk drives?
A: Yes as long as they are SATA specification compliance.

Q: How can *X-Wall MX*+ encrypt the entire disk without sacrificing drive performance?
A: *X-Wall MX*+ offers in-line SATA 6Gbps cryptographic operation. The operations of encryption and decryption are accomplished using high-speed hardware circuitry to ensure the maximum attainable performance. Software device drivers are not used to enable the *MX+;* therefore memory and interrupt overheads are eliminated.

Q: Is there a capacity limitation as are other products?
A: No. *X-Wall MX*+ encrypts all disk volume, regardless of any geometry. If you have a 6TB hard drive, the entire 6TB will be in-line encrypted with AES strength.

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 to establish a separate “encrypted folder” under file directory as required by some software solutions?
A: No. Unlike software operated “encrypted folder” over file/directory of application layer that operates with significant overheads (thereby with significant performance degradation), the *X-Wall MX*+ operates on physical SATA layers on SATA 6Gbps interface speed which is efficient and transparent to the host computer and the connected disk drive.

Q: If I back my data up to an external drive which has integrated an *MX*+, is that backed up data encrypted?
A: Yes. All data written to the *MX*+ integrated storage device is automatically encrypted.

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 an *MX+* enabled system/disk drive, you must use the "Secret Key" that comes with the authentication method to initialize and format the drive.

Q: Can *X-Wall MX+* support a SATA RAID Controller?

A: Yes. Enova's *MX+* can work with any SATA RAID controller. The connection of using an example Sil3132 RAID controller is to connect one SATA drive on its respective SATA channel, making a simple two drives RAID 0 or 1 operation.

Adding an *X-Wall MX+* real-time full disk encryption technology is simple. Simply add the *X-Wall MX+* on the respective SATA channels in-line before the SATA drive, enabling full disk encryption to the connected SATA drives.

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. The X-Wall MX+ support a PM integration. Consult Enova Engineering **info@enovatech.com** for details.

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

A: Several times over. See below all available NIST CAVP certificates. The *MX+* is currently a FIPS 140-2 Level 2 or 3 single chip crypto module candidate.

Algorithm	Description	Certificate No.
SHS	SHA-256 in byte mode is the hashing algorithm.	SHS (Cert. #3311)
RSA	Used for key-pair generation, digital signature generation/verification, and encryption/decryption (key encapsulation/de-capsulation) with key size of 2048 bits.	RSA (Cert. #2090)
RSADP	Basic RSA decryption primitive. It recovers plaintext from ciphertext using an RSA private key.	CVL (Certs. #836 and #885)
RSASP1	Basic RSA signature primitive. It produces a signature representative from a message representative under the control of a private key	CVL (Cert. #884)
AES	AES encrypts and decrypts designated data output from, input into, or within the module. It supports 256-bit key size. It supports ECB, CBC, and XTS modes of operation. It uses separated keys to encrypt/decrypt data and initial vectors (or data unit sequence numbers).	AES (Cert. #4013)
HMAC	Used for generating HMAC-SHA-256 message authentication codes.	HMAC (Cert. #2627)
800-90A DRBG	A hash-based deterministic random bit generator using SHA-256.	DRBG (Cert. #1201)

800-38B CMAC	Used for generating CMAC-AES-256 authentication code.	AES (Cert. #4025)
800-108 KDF	Key Derivation Functions using either HMAC or CMAC as pseudorandom functions.	KBKDF (Cert. #100)

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. User is not required to memorize frequently used and cumbersome log on procedures. You need only to present your *Key* every time you power up your computer -- It is transparent to all users.

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

A: **Yes.** Enova's *Key token contains a* ***Cryptographic Key***. *X-Wall MX*+ uses this key 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. Note however, the Key Token can now be encrypted using built-in HMAC capability.

Q: Does *MX*+ support other *2-factor authentication methods?*

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, for as long as the Secret_Key will be delivered to *MX*+ at proper timing. The *MX*+ design guide offers details on possible 2FA 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.

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 ask 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[3] 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, 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 if 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 offers portable design using the latest USB3.0/USB3.1 interface technology that has integrated the X-Wall MX+. Consult Enova engineering info@enovatech.com 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, only if the designer can have full control of the file system.

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

A: No. The X-Wall MX+ AES hardware engine computes the original data with 256-bit cryptographic key length. The size of data file after encryption remains unchanged.

Q: I am currently using the predecessor *X-Wall MX* product. Can I upgrade the same disk drive to an *X-Wall MX+* drive without change?

A: **Unfortunately, no.** The new *MX+* has a different key format and data structure which isn't compatible with its predecessor *X-Wall MX*. To use the *MX* encrypted disk drive, one needs to back up the data, use the new *MX+* to format the drive, then write the backup data to the drive.

[3] 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.

