Product Introduction: Enigma®

USB Real-time Full Disk Encryption Module - Frequently Asked Questions

Table of Contents

 .

Who is Enova Technology?

A: Enova Technology (www.enovatech.net) pioneered the hardware-based full disk encryption technology. Since 2000, Enova has introduced 9 generations of cryptographic modules (Hardware Real-time Encryption Engines), and is committed to providing usable and simple to use solutions for today's challenging data security requirements.

Why haven't I ever heard of Enova?

A: In the past, we have focused our sales efforts to the Original Equipment Manufacturers.

In an effort to bring high quality, high performance security products to the Consumer and Enterprise customers, Enova has made a commitment to sell our best-in-class security products thru our Retail, Channel and Distributor partners on a global scale. We are very excited about this, and promise to deliver world class best in security class products.

I am a Distributor/Channel/Retail reseller, and would like to speak to someone about picking up the product line—who should I speak to?

A: Great; we are looking forward to the opportunity to tell you more about our products; please send an e-mail to **info@enovatech.com**, or call Bob Fleming (**bob.fleming@enovatech.com**) at +1 303-915-4164 (US)

What is Enova's guiding principle?

A: Our message to the market is "Protect Your Data; Safeguard Your Privacy®". And, we are pleased to introduce you to our best in class line of data security products.

What is Enova '*Enigma*'?

A: *Enigma* is a USB hardware encryption solution designed to provide real time, in-line encryption of ANY USB enabled mass storage device, regardless of size, including Blu-Ray and DVD/DVD/CD-R USB devices. *Enigma* can and will encrypt data from a camera, smart phone, tablet, USB backup drives, 'thumb' drives, and much more.

Figures 1-3, from left clockwise: Photo of *Enigma* module; the *Enigma connected to a USB3.0/SATA hard drive; t*he *Enigma* connected to a USB2.0 Thumb drive.

Enigma + USB MSC = Connected Pair

 .

Enigma incorporates Enova's Patented *X-WALL DX-256* and *X-Wall DX-256C* real-time USB-to-USB crypto module, which performs full disk encryption with AES ECB/CBC 256-bit strength to all connected USB MSC (Mass Storage Class) storage drives. VERY heavy duty protection indeed!

What is disk encryption?

A: Disk encryption is a technology which protects data by converting it into an unreadable format called cipher text. Without the correct deciphering key, the data will remain encrypted.

What is *Full Disk Encryption (FDE)*?

A: The term *"full disk encryption*" is often used to signify that all of the data on a disk is encrypted.

What is *Self Encrypting Drive (SED)?*

A: A self encrypting drive is the same as an FDE (full disk encrypting drive); the meaning is the same, only with a different name.

What are the Features and Benefits of *Enigma*?

A: Glad you asked! There are many great features of Enigma:

Feature	Benefit
Enigma is totally transparent	No training required!
USB1.1/2.0/3.0 compliant	Easy to use for years to come
Encrypts all USB MSC devices[1] including card readers	
Simple yet very effective key management	A "Recovery Password" that performs two-factor authentication
Encrypts Blu-Ray DVD, DVD RW, CD-R;	
Compatible with just about any OS	Windows[2], MAC and Linux operating systems
NO software or complicated drivers to install	Simple to initialize and use
Full disk encryption protects all of your data	Both 512 bytes or 4K bytes sectors are protected
NIST/CSE certified hardware AES ECB 256 bits strength	Virtually impenetrable
Slim, compact and ultra light weight form factor	60.7mm (H) x 19.6mm (W) x 10.1mm (H) with 11g (0.39 oz) weight

Why choose the *Enigma* over FDE or SED?

A: Enigma was designed to be convenient, portable, transparent and simple to use - all the while securing your valuable data. Its purpose is to encrypt data on the fly. If you travel, take Enigma with you to protect your mobile data. If you don't travel, use Enigma to protect your home and office data.

---

1 Some composite device such as Western Digital's My Book Studio Edition 4TB is equipped with more than one interface. The WD 4TB drive comes with an extra HID/SES interface in addition to the USB MSC interface. The Enigma supports current WD 4TB drive under Windows 7 32/64-bit platform. However, we have not exhausted our testing of other brands and cannot guarantee full compatibility with other 4TB drives. If an incompatibility issue occurs, please inform us and send us your configuration data as we will be pleased to try to resolve the technical difficulties for you.

2 Windows and Macintosh are registered marks of Microsoft and Apple Computers respectively.

Convenience, simplicity and security. Unlike the limited selection of FDE and SED drives, which usually involves with using costly key management software, *Enigma* works reliably with any drive with any geometry; and best of all, you get to control your own ciphering key.

How does *Enigma* work?

A: Follow these three simple steps:

1. Insert the USB drive to the female connector of the *Enigma* device.
2. Insert the *Enigma* to any host USB port. At first usage, you must properly initialize *Enigma* by executing a code utility called "enigma(fde).exe." The code utility will guide you through the simple initialization procedure.
3. After initialization, you can start using *Enigma*.

The initialization procedure is:

1. Download the code utility and unpack it
2. Insert the USB drive to the *Enigma* then insert the *Enigma* to any host USB port
3. Execute "enigma(fde).exe" from the code utility then follow the two steps as guided
4. ***Un-plug*** then ***re-plug*** the *Enigma* along with the USB drive to allow Enigma to save the settings
5. The OS detects the attached USB drive, and asks if you want to format the drive. Click YES and every cryptographic operation is now automatic and transparent.

What will happen if *Enigma* isn't properly initialized?

A: The Enigma is not fully functional other than detects your connected USB drive. Attempt to format the USB drive through the un-initialized Enigma will produce an error message prompted by Windows as "The disk is write protected." See below Windows error message.

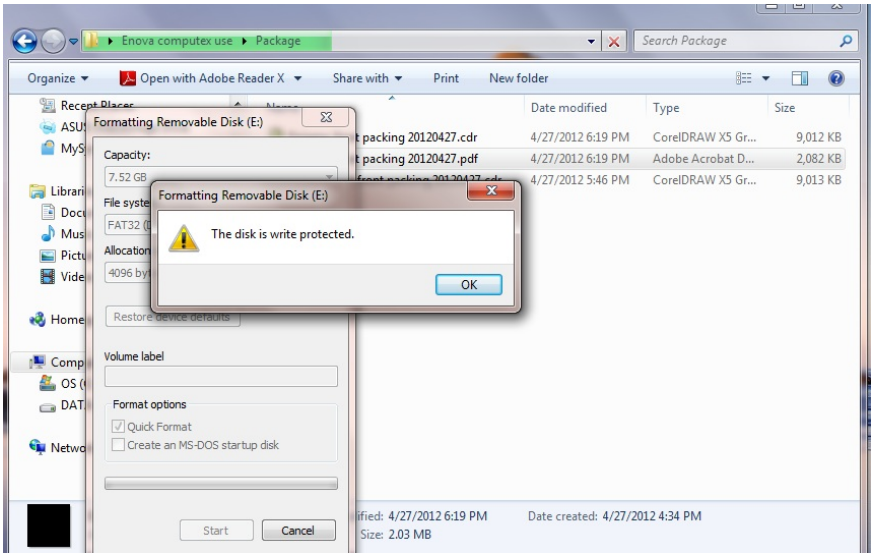

FIG. 4 – A "Write-Protected" message displays by the OS if Enigma wasn't properly initialized.

Do I need any training to use *Enigma*?

A: NO! You don't have to learn or manage anything. After the initialization procedure is completed, simply insert the *Enigma* along with USB drive into any host USB port. The OS detects the

attached USB storage drive and asks if you want to format the drive. Click YES and every cryptographic operation is automatic and transparent.

What is the "Key Management" of *Enigma*?

A: Every *Enigma* comes with a code utility (enigma.exe) that allows user to initialize their Enigma. The *Enigma* may not be used without being initialized through the establishment and confirmation of the "Recovery Password."

The "Recovery Password" generates the Data Encryption Key (DEK) needed to authenticate the *Enigma*. This "Recovery Password" generates the same DEK programmed to the *Enigma*.

If the DEK was incorrect or missing, the *Enigma* will not allow access to the encrypted data on the USB drive. Without the correct recovery password, the resulting encrypted drive appears to be an unformatted drive. This is true even if the encrypted drive has been moved to a different platform. Attempts to surface scan the entire drive sectors/platters in order to access the encrypted data will be futile.

Do I have the option of selecting a method of authentication myself?

A: Sure. You may select one of several authentication methods, including PIN/Password, Numeric Keypad, Biometrics, Smartcard (including CAC and PIV cards), SSO or any combination. The Enigma provides simple yet effective 2-factor authentication, i.e. something you have (the Enigma module) and something you know (recovery password). Please consult Enova Engineering (**info@enovatech.com**) for more details.

For Enterprise and Government applications, please contact Enova at **info@enovatech.com** for details and pricing.

Can *Enigma* encrypt Blue-Ray DVD, DVD RW and/or CD-R media?

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

What happens when an Enigma 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 *Enigma*. The only way to gain access to the media will be to connect it to *Enigma*, and load in the correct recovery password.

What happens when an Enigma is lost or stolen?

A: If the *Enigma* is ever damaged, lost or stolen, simply purchase another *Enigma*. Install the *Enigma* in the same fashion and use the same "Recovery Password" to generate the same DEK to allow operation over the encrypted media that was previously encrypted with the lost or damaged *Enigma*.

Does Enigma support 4KB/sector drives?

A: Yes, *Enigma supports both* standard 512 bytes per sector drive and 4K bytes per sector drives without regard to capacity of the drive.

Does Enigma support drive capacity over 2TB (2 Terabytes)?

A: Yes. *Enigma* supports drives greater than 2TB per drive. See additional comments in 'What is the likelihood of an Enigma malfunction' answer on the next page.

Does *Enigma* support various file systems?

A: Sure. *Enigma* supports all file systems including FAT, FAT32, NTFS, Linux and MAC OS. Note that certain file systems in MAC OS may not be compatible with other file systems as seen in a PC Windows environment.

Does *Enigma* feature Anti-Malware?

A: Yes. Enigma features "Write-Protect Entire Storage" and "Safeguard Boot Sector" that prevent malicious virus, worms and spyware from Implanting to your USB drive.

Is *Enigma* compatible with various operating systems?

A: Yes – the *Enigma* 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. This represents over 98% of the operating systems available today.

Has the Enova *Enigma* product line been US Government certified?

A: Yes, many times over. Enova Technology has been working with the US Government and CSE since year 2001.

The AES ECB/CBC crypto engines of *Enigma* 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 correct 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.

Is *Enigma* a certified FIPS 140-2 solution?

A: The FIPS 140-2 level 2 certification of the ***X-Wall DX*** crypto module is in progress. Contact us (info@enovatech.com) for more information.

If the *Enigma* malfunctions, will I lose my data?

A: No, as long as you maintain your own Recovery Password as mentioned above. Go out and purchase a new *Enigma* device and initialize it as you did previously. You should have no problems recovering your encrypted data.

What's the likelihood of an *Enigma* malfunction?

A: Extremely unlikely. Each Enova *X-Wall* family microchip is tested using a zero tolerance manufacturing policy and complies with international quality assurance standards[3] prior to being shipped. 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 *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 DEK is intact).

[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.

Can I exchange the *Enigma* encrypted files over the public Internet?

A: Great question! Not using this current product release. If this type of support is required, please contact us at info@enovatech.com.

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 *Enigma* is automatically encrypted without exception.

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 *Enigma*. If your backup drive is USB enabled, protect that data with the *Enigma*.

Or, choose the ***X-Wall FX*** (USB-to-SATA) crypto module enabled external enclosure for data backup.

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

A: **No, not at all.** *Enigma* has been carefully designed not to change the user's regular computing behavior, nor does it require learning a complex GUI. The user is not required to memorize frequently used and cumbersome log on procedures.

Enova's prime objectives include building a secure product that will make the user's life a little more enjoyable. You need only to present your *Enigma* every time you attempt to access your encrypted disk. Period.

What is "*X-Wall DX*"?

A: *X-Wall DX*, a patents protected 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 drives, thumb drives, USB/SATA interfaced disk drives, SSD's and Card Readers, 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.

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.

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, 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 transparent cryptographic operations to your disk drives.

FIG. 5 – The product image of the X-Wall DX real-time crypto module.

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 ***securely*** over the public network. The encryption and decryption operations are totally transparent to all users, making *DX* invisible and independent to any operating system.

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.

How is key length related to security?

A: In the case of Symmetric Cipher (DES, TDES, AES or other block ciphers), 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 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 a parity bit. Therefore, unlike the TDES counterpart, an AES 128-bit has a real key length of 128-bit, meaning a key combination of 3.402823669209384634633746074317e+38. An AES 256-bit key length will have a key combination of 1.157920892373161954235709850086 9e+77.

BECOMING FAMILIAR WITH THE TERMINOLOGIES

There are several terminologies that are specific to the *Enigma* and it's time to get familiarized with those so that when confusion occurs, this could be the best paragraph to reference to.

USB MSC – USB Mass Storage Class; In general, it refers to a storage device under USB protocol;

AES - Advanced Encryption Standard as published in FIPS 197;

ECB - Electronics Code Book, is a confidentiality mode that features, for a given DEK, the assignment of a fixed cipher text block to each plaintext block, analogous to the assignment of code words in a codebook. Essentially the same DEK is applied to every plaintext data block independently.

CBC - Cipher Block Chaining, is a confidentiality mode whose encryption process features the combining ("chaining") of the plaintext blocks with the previous cipher text blocks. The CBC mode requires an IV (Initialization Vector) to combine with the first plaintext block, in addition to using a given DEK. The security level of a CBC implementation is quadruple trillions times more than that of an ECB.

DEK - Data Encryption Key, a 256-bit key responsible for data encryption and decryption based on AES ECB or CBC mode of operation.

Default DEK - Default Data Encryption Key, a 256-bit key embedded during the manufacturing process. This default DEK can be changed or replaced upon entering the "Recovery Password."

Enigma_CD – an *Enigma* on-board emulated CD-ROM that contains all software code utilities including the main utility "enigma.exe," quick guide, user's guide, warranty and FAQ.

Initialization - a process required to initialize the *Enigma* dongle by asking the user to enter and confirm the "Recovery Password," which allows the user to regain access to encrypted data in the event that *Enigma* is lost, stolen, or may have malfunctioned. If the *Enigma* dongle wasn't properly initialized, the *Enigma* connected USB drive won't be able to get formatted. A system warning message of "This device is write-protected" will prompt when a user performs the action of "FORMAT" through an un-initialized *Enigma*.

Recovery Password – an essential part of the *Enigma* key management. A recovery password is responsible for generating the DEK value to regain access to the encrypted data, in the event that your *Enigma* is lost, stolen, or may have malfunctioned. The same recovery password generates the same DEK. This "Recovery Password" should be kept with confidentiality.

Start Programming - a part of the "Recovery Password" process that writes the new DEK value to the *Enigma* to replace the old DEK value. Note that a new DEK value can be equivalent to the old DEK value.

Write-Protect Entire Storage – Using *Enigma*, the **"*write-protect entire storage*"** feature disables all write operations to the connected USB drive, making the USB drive "read-only" which effectively rejects any virus, spyware or malware intrusion. While this feature is turned ON, all contents of the drive remain encrypted. There isn't any extra driver to install. See also **"*Safeguard Boot Sector.*"**

Safeguard Boot Sector [4] – Using *Enigma*, the ***"Safeguard Boot Sector"*** feature disables all write operations to the boot sector of a connected USB thumb drive and card reader storage media, making it

[4] Using *Enigma*, the "Safeguard Boot Sector" feature also protects the Master Boot Record (MBR) of a connected USB/SATA type fixed disk drive.

"read-only" which effectively rejects any virus, spyware or malware intrusion. While this feature is turned ON, write operation is only permitted to the other sectors with written data being encrypted. More, the *Enigma* blocks the "autorun.ini" type malware so that the malware won't be able to implant itself to the *Enigma* built-in CD-ROM (***Enigma_CD***) that contains all software code utilities. There isn't any extra driver to install. See also "***Write-Protect Entire Storage.***"

Firmware Update – a process that replaces your existing firmware using a newer version. This is only required whenever there is a newer version release that resolves known compatibility issue or enhances the security operation. There isn't any extra driver to install.

 .