Enova® Enigma 2
Hardware Crypto Module Securing Cloud Storages

Frequently Asked Questions – FAQ Ver. 2.0

Q1: *What is Enova "Enigma 2" hardware crypto module (HCM)?*

A1: "*Enigma 2* " (www.enovatech.net\products\enigma_2.htm) is a hardware crypto module (*HCM*) that encrypts existing data in place and safeguards data confidentiality over Data-In-Transit (DIT) or Data-In-Motion (DIM).

Enigma II HCM is capable of encrypting selective files and folders of any computer detectable storage devices including boot drive, external drive such as USB or 1394, network attached drive and virtual drives such as Windows SkyDrive and Google's GoogleDrive. With the *Enigma II HCM*, file/folder can be encrypted and decrypted. Without it, the encrypted file/folder remains encrypted.

Enigma II HCM further allows the sharing of an encrypted file/folder for as long as the parties possess the same Login password of an *Enigma II HCM*.

Unlike its predecessor the *Enigma* that performs full disk encryption to ANY number of the attached USB Mass Storage Class (MSC) drive, the new *Enigma II HCM* is the best alternative to your software encryption, encrypting existing data in place and sending the encrypted files/folders through public network with confidentiality. Only the recipient who has possessed the same login password can successfully decrypt those received encrypted files and folders.

Q2: *What SKU (Stock Keeping Units) are available in Enigma offering?*

A2: Below SKU are currently available:

Product	**Specification**
Enigma 2	1. *Enigma II HCM* is a physical module interfacing with standard USB protocols; 2. Supports 2-factor authentication[1] 3. Works with Windows and Macintosh operating systems; 4. Capable of encrypting existing data in place; 5. Capable of encrypting selective files/folders of any OS detectable storage drives, including boot drive, external drive such as USB or 1394, network attached storage and virtual drives such as SkyDrive and GoogleDrive; 6. Secures data-in-transit (DIT) and/or Data-In-Motion (DIM); encrypted file can be sent through public network securely; 7. Allows sharing of encrypted file/folder; 8. Simple yet very effective key management; 9. Simple to use GUI of Windows and Macintosh; requires no software and/or driver download and installation; 10. Compliance to any USB 1.0/1.1/2.0/3.0 MSC protocols;

Ordering code

Ordering Code (SKU)	AES mode of Operation	Encryption Strength	OS
EMA-DX256N-3W	ECB	256-bit	Windows
EMA-DX256C-3W	CBC	256-bit	Windows
EMA-DX256N-3M	ECB	256-bit	Windows & Mac
EMA-DX256C-3M	CBC	256-bit	Windows & Mac

Q3: What is File/Folder Encryption (FFE) ?

A3: The file/folder encryption is a file based encryption mechanism that is capable of encrypting selective files or folders of any host computer detectable storage devices including boot drive, external hard drive, flash drive, flash media, network attached drive and cloud storage such as Dropbox, Windows SkyDrive and Google's GoogleDrive etc. User can select what file to encrypt no matter where it is stored. The encrypted file cannot be decrypted without the presence of Enigma 2 HCM.

The *Enigma 2* is a hardware crypto module (HCM) with NIST(National Institute and Standard Technology) and CSE(Communication Security Establishment) certified encrypted engine. The data encryption key of *Enigma 2* is stored in the module encrypted

[1] *Enigma II HCM* is something you have possessed whereas your login password presents as the 2nd factor – something you know.

therefore is far more secure than software based encryption in which data encryption key may be exposed over system memory.

Q4: How does Enova Enigma 2 differ from the software encryption solution?

A4: The *Enigma 2* HCM is a hardware crypto module (HCM) and its hardware crypto engine is certified by NIST and CSE. You get to use the GUI to select any files/folders to encrypt. The Enigma 2 HCM is far more secure and faster than software encryption solution for its data encryption key is never exposed outside of the HCM and the performance is done through a real-time hardware crypto chip, the X-Wall DX.

Contradictory to using software encryption, system resources such as CPU time and memory are not required for the Enigma 2 to perform cryptographic operations. Security strength and performance of software encryption may be affected by other applications and dedicated drivers running on the host computer.

Q5: What is 2-factor authentication?

A5: 2-factor authentication is a method for authentication which requires the presence of two factors: something you have possessed and something you know. The Enigma2 HCM is something you have (first factor) and the login password is something you know (the 2nd factor).

Q6: Can the Enigma 2 HCM be used to encrypt existing data on a hard drive?

A6: Yes. You can selectively encrypt any files/folders stored on a hard drive using Enigma 2 HCM. The encrypted files/folders can only be decrypted through the presence of correct Enigma 2 HCM and login password.

Q7: Can the Enigma 2 HCM be used to encrypt data in a network attached storage (NAS) ?

A7: Yes. You can selectively encrypt any files/folders stored on a NAS storage using Enigma 2 HCM. The encrypted files/folders can only be decrypted through the presence of correct Enigma 2 HCM and login password.

Q8: Can the Enigma 2 HCM be used to encrypt data on cloud storages such as GoogleDrive, SkyDrive and Dropbox etc.?

A8: Yes. You can selectively encrypt any files/folders stored on any cloud storage using Enigma 2 HCM. The encrypted files/folders can only be decrypted through the presence of correct Enigma 2 HCM and login password.

Dropbox Google Drive SkyDrive

On standard installation, those cloud drives locations can be found as below:
For Microsoft SkyDrive: “Computer\OS (C:)\Users\your account name\SkyDrive”

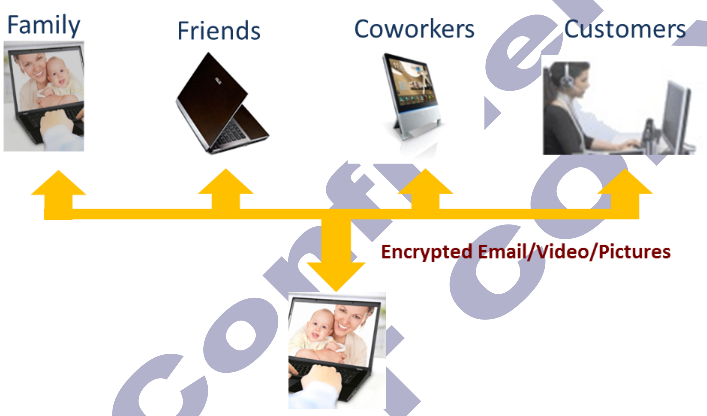
For Goggle's GoogleDrive: "Computer\OS (C:)\Users\your account name\Google Drive"
For Dropbox: "Computer\OS (C:)\Users\Your account name\Dropbox"

Q9: Can I send Enigma 2 HCM encrypted files/folders by email attachment?

A9: Yes you can. In real world, your email attachment may be exposed through public network. You can protect your confidentiality and privacy using the Enigma 2 HCM.

You can send those Enigma 2 HCM encrypted files/folders through email attachment to your associates and friends through public network while preserving all confidentiality. Try to decrypt? No problem. Your associates and friends just need to have the same Enigma 2 HCM coded with the same login password to decrypt the files.

The people who owns the same solution(DX) as yours can decrypt the files you send to them by setting up the same password



Q10: Can the Enigma 2 HCM with ECB crypto engine access a CBC encrypted file with the same password?

A10: No. ECB and CBC use different encryption algorithm and they are not interchangeable.

Q11: What operation system does Enigma 2 HCM support?

A11: The Enigma 2 module comes with utility that supports Windows only or Windows and MAC platforms. Identify which operating system you'd like to work with Enigma 2 HCM.

See below ordering information for details:

Ordering Code (SKU)	AES mode of Operation	Encryption Strength	OS
EMA-DX256N-3W	ECB	256-bit	Windows
EMA-DX256C-3W	CBC	256-bit	Windows
EMA-DX256N-3M	ECB	256-bit	Windows & Mac
EMA-DX256C-3M	CBC	256-bit	Windows & Mac

Q12: What happens when an Enigma 2 HCM encrypted file is stolen?

A12: No worries. The Encrypted file remains secure.

Q13: If the Enigma 2 HCM malfunctions, will I lose my encrypted data?

A13: No, as long as you remember the login password you had performed at initialization stage. Just go out and purchase a new one then setup the same login password to regain access to your encrypted data.

Q14: How is key length related to security?

A14: 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 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 3.4028236692093846346337460743177e+38. An AES 256-bit key length will have a key combination of 1.1579208923731619542357098500869e+77.

Q15: How secure is Enigma 2 hardware crypto module?

A15: A hardware-based real-time cryptographic solution significantly reduces a hacker's successful entry into the encrypted disk drive. Every incorrect login password to the Enigma 2 HCM requires a fresh hardware power-on-reset cycle. Your computer hardware would fail way before the one million attempts. As such, Enigma 2 hardware crypto module will be strong enough to withstand physical attack as well as sophisticated computer attacks.

Q16: What is the "Key management" of Enigma 2 HCM?

A16: Key management of Enigma 2 HCM is simple yet effective. User just need to setup their login password at initialization phase and that's it. Sophisticated key management including Administrator password and/or network manageability as usually required by Enterprises and Government can be provided at extra cost. Please contact **info@enovatech.com** for details.

Limitation of Liability & Warranty Disclaimer

a. Limited Warranty. Enova warrants the Enigma Products to be free of material defects and errors that prevent normal operation. On receipt of notice of such defect or error from reseller, Enova shall, at its own expense, exercise commercially reasonable efforts to modify the Products, upgrade the Products, or suggest an alternate procedure or routine which eliminates the adverse effect of the defect or error. Notwithstanding the foregoing, Enova shall be relieved from any such obligation if reseller fails to give Enova reasonable prompt, written notice of any error claimed, and such delay causes further damage to reseller.

b. Qualifications. Notwithstanding the warranty provisions set forth in the Limited Warranty, Enova's obligation with respect to such warranties shall be contingent on reseller and reseller's customers' use of the Products in accordance with instructions as provided in the Quick Guide, FAQ and Design Guide. Enova shall have no warranty obligations with respect to any portion of the Products which has been: (i) operated by the reseller in a manner inconsistent with requirements set forth in the Quick Guide, FAQ and Design Guide or that has been modified by any party other than Enova; (ii) damaged in any manner and by any cause other than any act or omission of Enova; (iii) operated by any third party hardware and/or software not owned by Enova; or (iv) subjected to extreme power surge or electromagnetic field.

c. DISCALIMER. THE LIMITED WARRANTY IS THE ONLY WARRANTY MADE BY ENOVA WITH RESPECT TO THE PRODUCTS, AND ENOVA SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, WRITTEN OR ORAL, STATUTORY, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF DESIGN, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, OR WARRANTIES ARISING FROM A COURSE OF DEALING, TRADE USAGE OR TRADE PRACTICE.

d. Remedies. The entire liability of Enova and the sole and exclusive remedy for reseller under the limited warranty set forth in this article shall be (i) for Enova to replace defective Products as provided in this agreement. Reseller may ask for valid RMA (Return Material Authorization) number for warranty issues within 12 months from the date the said warranted Products are shipped; and (ii) for reseller to terminate without further liability to Enova.

e. RMA. Only defective Products maybe returned to ENOVA for analysis of the cause of defect and possible replacement. No Products maybe returned without a valid RMA (Return Material Authorization) number issued by ENOVA for which reseller must request directly from ENOVA.

f. IN NO EVENT SHALL ENOVA OR RESELLER BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN ANY WAY CONNECTED WITH THIS AGREEMENT, THE SERVICES PERFORMED, OR ANY OTHER MATTER RELATED HERETO, INCLUDING WITHOUT LIMITATION, LOST BUSINESS OR LOST PROFITS WHETHER FORESEEABLE OR NOT, EVEN IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Contact Us
www.enovatech.net
Phone: +886 3 5772627
Fax: +886 3 5772770
Email: webmaster@enovatech.com

About Enova Technology (Enova)

Enova builds and provides comprehensive enterprise based security products for Data at Risk (DAR) management and compliance solutions on a global basis. Enova offers the tools to automate and protect data distributed to virtually any USB enabled storage device, and manages these efforts using simple to understand processes.

Using Enova data security products, security teams will become more proactive, while compliance teams can more effectively manage, collaborate and enforce secure accountability.

Enova's growing customer base includes leading Governments, Global 2000 organizations in the financial services, healthcare, retail, energy and utility, transportation and manufacturing. For more information, pleas