The Enova *X-Wall Secure* Product

Frequently Asked Questions

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

A: The *X-Wall SE* is an ASIC (Application Specific Integrated Circuit) that encrypts and decrypts the entire hard disk bit by bit (including boot sector, temp files, swap files and the operating system) with real-time performance using the *NIST (National Institute of Standards and Technology)* certified *DES (Data Encryption Standard)* and TDES (Triple DES) algorithms.

Q: How can *X-Wall SE* encrypt the entire disk in "real-time"?

A: *X-Wall SE* is specifically engineered for high speed communications with the disk. *X-Wall SE* offers 1.1 Giga bit per second or higher real-time performance to all IDE compatible hard drives. Since X-Wall SE hardware performs all encryption and decryption tasks, there is no software to cause memory and interrupt overhead.

Q: How does *X-Wall SE* function?

A: *X-Wall SE* sits between the host IDE and the device IDE interface. It intercepts, interprets, translates, and relays IDE commands & data to and from the disk drives, encrypting the data with DES/TDES 40/64/128/192-bit key strength.

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

A: *X-Wall SE* can be operated with *Ultra ATA (Ultra DMA) 33/66/100* compliant disk drives in *real-time* with throughput of 1.1 Giga bit per second. X-Wall SE does not work with SCSI or fiber-channel drives.

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

A: The *X-Wall SE* requires no device drivers and is independent from all operating systems. The only requirement is an Ultra ATA (Ultra DMA) compliant disk drive.

Q: Do I need any training to use *X-Wall SE*?

A: No. The good news is that you don't have to learn or manage anything. After inserting the X-Wall key, everything will function as before with no loss of performance and with no manual intervention.

Q: How does *X-Wall SE* compare *w*ith Smart Card and PCMCIA encryption products?

A: *X-Wall SE* is dramatically faster than PCMCIA or Smart Card solutions, and encrypts the entire hard drive instead of just selected files. There is no possibility that any data or credentials can be left unprotected on the hard drive. Drive locking and boot sector encryption solutions do not encrypt the data, and thus it is vulnerable to attack.

Q: Can I encrypt two hard disk drives via a single *X-Wall SE*?

A: No. *X-Wall SE* is designed to protect only one disk drive.

Q: What is "DES/TDES"?

A: DES (Data Encryption Standard) was originally introduced by NSA (National Security Agency) and IBM and has since become a Federal data encryption standard as defined in FIPS 46-3 (Federal Information Processing Standard). DES works on 64-bit data segments with a 64-bit key of which 8 bits provide parity, resulting in a 56-bit effective length. A variant on DES is TDES, in which the plain text is processed three times with two or three different DES secret keys. With two encryption keys used, the result is an encryption equivalent to using a 112-bit key. With three keys, the result is an encryption equivalent to using a 168-bit key. In practice with a 128-bit TDES, the plain text is encrypted with the first key, decrypted with the second key, and then encrypted again with the first key.

Q: How secure are DES and TDES?

A: Very secure as both algorithms are completely public, and have been surprisingly resistant to new cryptographic attacks over the last quarter century. Though DES 56-bit key length is no longer proof against a massive computer attack, for most business applications DES remains adequate.

Q: How is key length related to security?

A: In general, a larger key length creates a stronger cipher, which means an eavesdropper must spend more time and resources to find the decryption key. For instance, 2^{40} (a DES 40-bit strength) represents a key space of 1,099,511,627,776 possible combinations. While this number seems impressive, it is definitely feasible for a microprocessor or a specially designed ASIC to perform the huge number of calculations necessary to derive the 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 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.

Q: Will I expect 19-step log on procedures & complex GUI (Graphical User's Interface) like other systems require?

A: No. *X-Wall SE* does NOT change user's regular computing behavior, nor does it require a complex GUI for proper operation. It does not require you to memorize frequently used and cumbersome log on procedures. It is totally transparent to all users. You need only to present your external *X-Wall Secure Key* every time you power up your system.

Q: Why do I need to use the *X-Wall Secure Key?*

A: The *X-Wall Secure Key contains the* DES/TDES "*Secret Key*" that is used by *X-Wall SE* to encrypt or decrypt data. Without the key, the protected disk drive cannot be booted and there is no access into the PC. Together the *X-Wall Secure Key* and *X-Wall SE* comprise an effective user authentication and access control system. The X-Wall Secure Key serves as user authentication while *X-Wall SE* enforces access control.

Q: What happens if my *X-Wall Secure Key* is lost or stolen?

A: **There are no "backdoors" into X-Wall Secure systems, so without the *X-Wall Secure Key* you will not be able to access the data or operating system on the protected disk**. This means you must keep the backup key in a safe place at all times.

Q: Can I order duplicate *X-Wall Secure Keys*?

A: Yes. You can order duplicate *X-Wall Secure Keys* from your *X-Wall* reseller or directly from Enova Technology. Please visit our web site ***http://www.enovatech.com*** for details. **Note: Enova Technology does not maintain a database of *X-Wall Secure Keys*. To have additional keys made, you must send your backup key with your order for duplication.**

Q: Can I remove the *X-Wall Secure Key* while my PC is on?

A: Yes, you can remove the Key for safekeeping after your operating system has fully loaded. Remember that the X-Wall Security Key MUST be used again the next time you power up your system.

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

A: No. Remember that the *X-Wall Secure Key* contains the DES/TDES secret key; the *X-Wall SE* chip is generic. Consequently, you can simply replace the defective *X-Wall SE* component and use your original *X-Wall Secure Key* to access the data on your hard drive.

Q: Can I exchange the *X-Wall SE* encrypted files using the public network?

A: No. the *X-Wall* system was specifically designed to protect data "at rest" (stored) on your PC. The DES/TDES encryption engine built inside the *X-Wall SE* is a symmetric cipher, a "*Secret Key*" system that does NOT support the Public Key Infrastructure (PKI). Therefore, you will not be able to exchange *X-Wall SE* encrypted files through public network.

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

A: No. DES/TDES is a complicated mathematical algorithm that computes the original data with 40/64/128/192-bit key length. Regardless of the size of the encryption key, the size of data file after encryption remains unchanged.

Q: I am currently using the *X-Wall SE-64* (DES 64-bit strength). Can I upgrade the same disk drive to an *X-Wall SE-128* (TDES 128-bit strength)?

A: Yes, but first you must copy the content of your disk drive to a safe location, then you can install the *X-Wall SE-128* and restore the data to the disk drive. 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 a disk drive.