

User's Guide 1.5

Information contained in this manual is subject to change without notice and does not represent a commitment on the part of Enova Technology. The software and hardware described in this document as part of the Enova's *Secure Product family* is provided under a license agreement or nondisclosure agreement. It is unlawful for any person, persons, organization or entity to copy, reproduce, or transmit (electronically, in print, or any other way) this document, any part of the program, or any information contained in the *Enova Secure Product family* package without the written authorization of Enova Technology.

X-Wall products comply with FCC radio emissions requirements. The Federal Communications Commission Radio Frequency Interference Statement includes the following warning:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment to an outlet on a circuit different from the circuit where the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help
- Move the computer away from the receiver

Copyright Notice

Copyright ©2002, Enovatech, Inc. (Enova Technology). All Rights Reserved.

This manual may not be reproduced (in part or whole) or transmitted in any form or by any means, electronic or mechanical, including photocopying, scanning and recording, for any purpose without the express written permission of:

Enovatech, Inc. (Enova Technology)
576 Valley Way
Milpitas, California 95035, USA
Tel: 408 956 8100 Fax: 408 956 8102
<http://www.enovatech.com>
info@enovatech.com

Trademarks

X-Wall, Secure Mobile Rack, Secure PCI and Secure USB2.0 are trademarks of Enova Technology. Pentium is a trademark of Intel Corporation. Windows 95/98/NT/2000/Me/XP are registered trademarks of Microsoft Corporation. All other products mentioned in this User's Guide are the respective trademarks of their registered owners and are hereby acknowledged.

TABLE OF CONTENTS

COPYRIGHT NOTICE.....	2
LIMITED WARRANTY AND DISCLAIMER.....	5
ABOUT ENCRYPTION.....	6
1. INTRODUCTION.....	7
1.1 <i>X-WALL SYSTEM</i> FEATURES AND SPECIFICATIONS.....	8
1.2 <i>X-WALL SYSTEM</i> REQUIREMENTS.....	8
1.3 READ THIS BEFORE INSTALLATION.....	9
2. INSTALLATION.....	11
2.1 KEY FEATURES AND SPECIFICATIONS.....	11
2.2 BEFORE INSTALLATION.....	11
2.3 IMPORTANT THINGS TO REMEMBER.....	11
2.4 UNPACK THE SECURE USB2.0.....	12
2.5 PREPARE THE <i>SECURE USB2.0</i>	12
2.6 CONNECT <i>SECURE USB2.0</i> TO THE COMPUTER.....	13
2.6.1 For Windows Users	13
2.6.2 For Mac users	14
2.7 FDISK & FORMAT.....	14
2.7.1 For Windows 98 users	15
2.7.2 For Window XP users	16
2.7.3 For Windows 2000 users	16
2.8 REMOVING <i>SECURE USB2.0</i>	17
2.9 <i>READING STATUS INDICATORS</i>	17
3. TECHNICAL SUPPORT.....	18
3.1 BEFORE CONTACTING TECHNICAL SUPPORT.....	18
3.2 CONTACTING TECHNICAL SUPPORT.....	18
APPENDIX A – UNDERSTANDING CRYPTOGRAPHIC TECHNOLOGY.....	19
ABSTRACT.....	19
METHODS OF ENCRYPTION.....	21
CLASSES OF ENCRYPTION.....	21
<i>Symmetric Cipher</i>	21
<i>Asymmetric Cipher</i>	22
<i>Combination Systems</i>	22
<i>Encryption with X-Wall</i>	22
APPENDIX B -- INTRODUCING <i>X-WALL</i>®, A REAL-TIME IDE CRYPTO GATEWAY.....	24
ABSTRACT.....	24
FUNDAMENTALS.....	25
DESIGN OBJECTIVES.....	25
APPENDIX C – HOW TO USE FDISK AND FORMAT.....	26
FDISK – PARTITION.....	26
FORMAT.....	26
APPENDIX D – TROUBLE SHOOTING.....	28

User's Guide 1.5

APPENDIX E – FAQ29

LIMITED WARRANTY AND DISCLAIMER

Limited Warranty. Enova Technology Corporation (hereafter Enova) warrants the Product to be free of material defects and errors that prevent normal operation. On receipt of notice of such defect or error from Customer, Enova shall, at its own expense, exercise commercially reasonable efforts to modify the Product, upgrade the Product, 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 Customer fails to give Enova reasonable prompt, written notice of any error claimed, and such delay causes further damage to Customer.

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

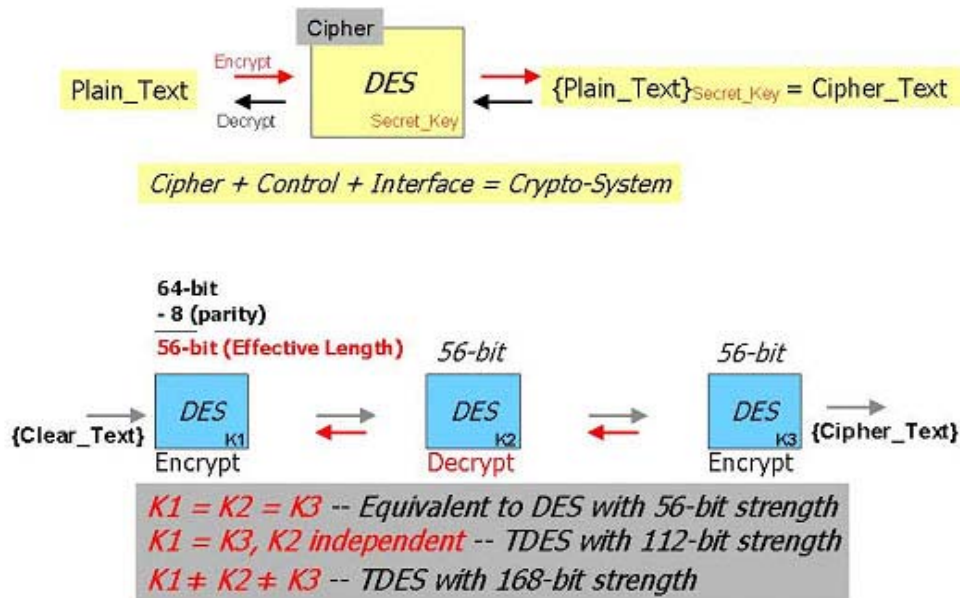
Disclaimer. THE LIMITED WARRANTY IS THE ONLY WARRANTY MADE BY ENOVA. THE WARRANTIES AND LIMITATIONS SET FORTH IN THIS ARTICLE CONSTITUTE THE ONLY WARRANTIES MADE BY ENOVA WITH RESPECT TO THE LICENSED PRODUCT, AND ENOVA SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, WRITTEN OR ORAL, STATUTORY, EXPRESS OR 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.

Remedies. The entire liability of Enova and the sole and exclusive remedy for licensee under the limited warranty set forth in this article shall be (a) for Enova to replace defective product as provided in this agreement and (b) for licensee to terminate this Agreement without further liability to Enova.

By installing the Product you specifically agree to be bounded by this article. If you disagree with above stated limited warranty and disclaimer, promptly return your purchase to your reseller or dealer for a refund.

ABOUT ENCRYPTION

DES (Data Encryption Standard) & TDES (Triple DES)



As illustrated above, a DES algorithm with a default 64-bit length¹ Secret Key is called a Cipher. A Cipher with proper control and interface implementation is called a Crypto-System. DES mathematically computes the original data (Clear Text) with its 64-bit length Secret Key. The result after DES computation (encryption) is called Cipher Text, an illegible form of text. A reverse DES computation is called a decryption. However, to derive the original data (Clear Text) from the decryption process, one MUST use a correct (bit by bit match) Secret Key. If the wrong key is used to decrypt, the result will be Cipher Text.

Triple DES (TDES) is three (3) DES operations cascaded together in sequence. On the first pass, DES encrypts the data with a Secret Key1. On the next pass, DES decrypts the Cipher Text with Secret Key2. On the third pass, that result is re-encrypted with Secret Key3. The length of each of the three Secret Keys can be selected to obtain an overall equivalent key strength ranging from 64-bit to 192-bit.

¹ 8 bits are taken out for parity calculation by standard, leaving 56-bit as the Effective Length. Therefore, a DES 64-bit is also called DES 56-bit, indicating a key space of 2^{56} . A TDES with 112-bit (56x2) key strength can have a key space of **5,192,296,858,534,827,628,530,496,329,220,096**. Please refer to the Appendix E - FAQ for more details.

1. INTRODUCTION

Congratulations on your purchase of **Enova's X-Wall Secure product family**. **You now have a high performance access control and encryption system that will safeguard the privacy of your stored data.**

X-Wall SE is a cutting-edge technology product that offers near military grade protection. All **Enova X-Wall Secure** products contain the *X-Wall[®]SE* family² encryption microchips. The X-Wall ASICs (Application Specific Integrated Circuit) are physical-layer, silicon-based, **real-time** processors that encrypt the entire disk content bit-by-bit - including the boot sector, temp files, swap files and operating system - without performance degradation. X-Wall SE is totally automatic and transparent to users; there are no commands to learn or user interfaces to monitor. X-WALL SE is extremely fast and capable of processing 1.1 Giga bit per second throughput without taking extra CPU time or system resources. Furthermore, X-Wall SE works with ALL operating systems and does not require any device drivers.

X-Wall SE utilizes the NIST (National Institute of Standards and Technology certified DES 64-bit <http://csrc.nist.gov/cryptval/des/desval.html> & TDES 128/192-bit <http://csrc.nist.gov/cryptval/des/tripledesval.html> hardware real-time encryption & decryption engine. These algorithms are certified to provide reliable security. With 128 or 192 bit encryption keys it is nearly impossible to access the protected data by guessing or deriving the right DES/TDES Key. Because everything on the disk is encrypted, your data is safe even if attackers try to boot from their own disk, or to move your disk to an unprotected machine.

X-Wall SE is engineered to be 100% compatible with all the latest motherboards and Ultra ATA (Ultra DMA)³ devices. It is also backward compatible with PIO, DMA and Fast ATA drives. This user's guide describes the product functionality and the correct ways of physical installation.

For those who wish to learn more about encryption and decryption technology, please read "Understanding Cryptographic Technologies" provided in Appendix A.

The following table shows available X-Wall SE microchips with their associated key length and specifications:

² Four (4) different strengths of encryption/decryption are provided within X-Wall SE family: 40-bit, 64-bit, 128-bit and 192-bit. The X-Wall SE-64 stands for 64-bit strength.

³ Also called IDE, the throughput of the latest Ultra ATA mode 5 standard is specified at 100Mbytes/sec. The 133Mbytes/sec specification proposed by Maxtor is NOT in the standard.

X-Wall	Key Strength	NIST Certified 100% hardware Cipher Engine	Maximum Throughput	Protocol & Interface support up to	Package
SE-40NB	40-bit	DES	712Mbit/sec	Ultra ATA 33/66	128-pin LQFP
SE-64NB	64-bit	DES	712Mbit/sec	Ultra ATA 33/66	128-pin LQFP
SE-40A	40-bit	DES	1.1Gbit/sec	Ultra ATA 33/66/100	128-pin LQFP
SE-64A	64-bit	DES	1.1Gbit/sec	Ultra ATA 33/66/100	128-pin LQFP
SE-128A	128-bit	TDES	1.1Gbit/sec	Ultra ATA 33/66/100	128-pin LQFP
SE-192A	192-bit	TDES	1.1Gbit/sec	Ultra ATA 33/66/100	128-pin LQFP

1.1 X-Wall System Features and Specifications

- Portable **X-Wall Secure Key** for user authentication and encryption
- Automatic encryption is totally transparent to users
- Compatible with all operating systems
- Does NOT require any device drivers
- Compatible with all motherboards with standard IDE Interface
- IDE “pin to pin” compatible
- 128-pin LQFP small form factor package

1.2 X-Wall System Requirements

- Ultra ATA (Ultra DMA) 33/66/100 compliant disk drive for high throughput configuration
- DMA, PIO or Fast ATA mode disk drive for slower speed (up to 16Mbytes/sec) configuration
- Motherboards with standard IDE Interface
- Selectable disk drive configuration from **ONLY ONE** of the four configurations below:

X-Wall SE	Primary	Secondary
Master	Yes, secure boot drive {Default, Do NOT set any jumper on the controller}	Yes, secure data drive {Default, Do NOT set any jumper on the controller}
Slave	Yes, secure data drive {MUST jumper-on Slave on the controller}	Yes, secure data drive {MUST jumper-on Slave on the controller}

Warning:

CONNECT ONLY ONE DISK DRIVE TO AN *X-Wall Secure product*. THE X-WALL SE IS DESIGNED TO PROTECT A SINGLE HARD DISK DRIVE ONLY, WHETHER IT IS CONFIGURED AS A MASTER OR A SLAVE DRIVE. DO NOT APPLY TWO DISK DRIVES TO THE X-WALL SE, OR YOU WILL EXPERIENCE TECHNICAL DIFFICULTIES, INCLUDING POTENTIAL DATA LOSS, AND THE PRODUCT WARRANTY WILL BE REVOKED.

1.3 Read This Before Installation

Please carefully read through the following sections prior to your installation.

Like any other modification related to your hard drive, you are urged to completely backup the hard drive before taking any further steps. A full backup is your best insurance against losing your data to errors or unforeseen problems.

X-Wall chips *are* engineered to be 100% compatible with all Ultra ATA disk drives. However, there may be system configurations that cause difficulties during installation. Please refer to Appendix E -- Q&A for troubleshooting.

Your X-Wall Secure product comes with a pair of **external X-Wall Secure Keys**⁵ to authenticate you as the authorized user and to enable encryption/decryption. Without the enclosed ***X-Wall Secure Key***, your computer will NOT be able to boot (if you choose the intended disk drive as the Primary Master); or the data on the disk drive will NOT be seen (if you choose the intended disk drive as the Slave).

ALWAYS STORE THE DUPLICATE X-WALL SECURE KEY IN A SAFE REPOSITORY!!!

The Secret Key of the DES/TDES real-time cipher engine is stored inside the *X-Wall Secure Key*. Consequently, you cannot decrypt without the correct, unique *X-Wall Secure Key*. Therefore it is extremely important that you always store the duplicate key in a safe repository. **Loss of both X-Wall Secure Keys will make it virtually impossible⁶ for you to recover your data.** There is no "backdoor" in X-Wall technology. Enova does not retain records of the random Secret Key

⁴ Drives today have more than 20GB. 40GB or more is an IDE drive standard.

⁵ X-Wall Secure Keys store the "Secret Key" value required for the DES & TDES hardware cipher engine. The "Secret Key" is a random combination of digitized bit of "0" and "1" in a specified length such as 40-bit, 64-bit, 128-bit or 192-bit.

⁶ The degree of security depends upon the version of X-Wall product you purchased. For example, a DES 40-bit encryption is vulnerable to people with advanced skills and appropriate tools. In contrast, a DES 64-bit encryption is extremely hard to decrypt and the process will consume substantial time and money. At present, decrypting data protected with a TDES 128-bit key without the right Secret Key is virtually impossible.

User's Guide 1.5

contained in *X-Wall Secure Keys*. It is Enova's policy to destroy the random database⁷ after it is used to program *X-Wall Secure Keys*.

Enova provides a key duplication service that allows you to make as many additional keys as desired for a small additional fee per duplicate key. Please note, however, that you must send in your backup Key along with your order for duplication. Otherwise we cannot create additional keys.

IN CASE X-WALL SE SECURE CHIPS FAIL

Every *X-Wall SE* family microchip we ship is 100% tested and complies with International quality assurance standards⁸. However, it is possible for the X-Wall chip to malfunction after some period of time. This problem can be resolved by simply replacing the product containing the defective X-Wall SE microchip. The contents of the disk drive will NOT be lost as long as you retain the original *X-Wall Secure Key* intact. Nevertheless, disk failures can occur, so it is good practice to always keep a backup of your important data. In case of system failure, please double-check with your disk drive prior to reporting any malfunction of the X-Wall.

DO NOT ATTEMPT TO CONNECT 1394 OR OTHER DEVICES TO THE KEY INSERT OR DAMAGE MAY OCCUR AND YOUR WARRANTY MAY BE REVOKED!

⁷ The database is used to write a unique Secret Key value to each X-Wall Secure Key.

⁸ Our quality assurance program includes reliability tests performed in accordance with MIL-STD-883E as the primary 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.

2. INSTALLATION

The **X-Wall Secure USB2.0** provides very secure external storage for your sensitive credentials and data. It requires the installation of a single 2.5-inch (9.5mm in height) Ultra ATA 33/66/100 hard disk drive connected to the PC with a standard USB2.0 or USB1.1 interface. The unit is designed with an ultra light-weight but extremely durable Aluminum-Magnesium case that makes it ideal for portable computing.

2.1 Key Features and Specifications

- External X-Wall Secure Key (pair) for authentication and encryption
- Supports USB 2.0 for high speed 480 Mega bit per second transfer
- Backward compatible with USB1.1 for lower speed transfer rate of 12 mega bit per second
- Supports all standard 2.5-inch (9.5mm height) Ultra ATA hard drives
- LED status indicator
- Supports real-time TDES 128-bit or 192-bit key length encryption
- Supported operating systems: Windows 98/98SE/2000/Me/XP, Mac OS, Linux 2.4 and above. (**Although X-Wall itself requires no device drivers and is independent from all operating systems, USB communication requires appropriate device drivers in each operating system.**)
- Power requirement: +5V (power from the USB host, or from power adapter).
- USB2.0 transfer in most cases will NOT require an external power supply

2.2 Before Installation

You will be required to FDISK and FORMAT the hard disk after installing it inside of the **Secure USB2.0**. Performing these operations will erase all the data on the disk. If you are adding a brand new disk, then no backup will be required. Otherwise, you are advised to back up the disk. **WE ARE NOT RESPONSIBLE FOR ANY LOST DATA.** The main circuit board of the **Secure USB2.0** is susceptible to static electricity. Proper grounding is required to avoid electrical damage. To ground yourself, simply put your bare hands on the computer chassis for a couple seconds before removing the product from its anti-static bag.

2.3 Important Things to Remember

1. The operation system will NOT detect the *Secure USB2.0* until you install a disk drive to it.
2. Always place the *Secure USB2.0* on a smooth surface. Avoid any dramatic movement, vibration or percussion.
3. Do NOT allow water to enter the *Secure USB2.0* unit.

User's Guide 1.5

4. Avoid placing the *Secure USB2.0* unit close to magnetic device (such as a mobile phone), high-electricity device (such as a hair dryer), or high temperature place (such as the glass wind shield of automobiles).
5. Always perform FDISK/FORMAT with the *X-Wall Secure Key* plugged in. Otherwise, the encryption function can not be enabled.
6. Plug in the *X-Wall Secure Key* every time you connect the *Secure USB2.0* to the USB host. You may remove the *X-Wall Secure Key* after the *Secure USB 2.0* unit has been detected..
7. If your computer supports a true USB2.0 transfer, you will probably NOT need an external power supply. However, a USB1.1 connection WILL require an external power supply. In that case, connect the power supply prior to connecting the USB2.0 cable.

2.4 Unpack the Secure USB2.0

Please check to make sure your package has everything listed below. If you discover damaged or missing items, please contact your distributor/retailer.

▪ Main Circuit Board with Aluminum-Magnesium case	1
▪ USB2.0 cable	1
▪ Power adapter	1
▪ Screws	4
▪ CD-ROM containing drivers	1
▪ This User's Guide	1
▪ Registration and Warranty card	1
▪ External <i>X-Wall Secure Key</i> (pair)	2

2.5 Prepare the Secure USB2.0

1. Prepare a 2.5-inch (9.5mm height) disk drive.
2. Follow the arrow symbol on the back of the case and push to remove the top cover.



3. Carefully connect the disk drive to the IDE connector of the main circuit board. Proper grounding is required to avoid electrical damage to your unit.



4. Fasten the disk drive to the main circuit board with the screws (come with your purchase of the disk drive). Place it back to the top cover.



5. Align the signs on the side of both covers, and then push the top cover back to its original location.
6. Fasten the *Secure USB2.0* with the provided screws.



2.6 Connect *Secure USB2.0* to the Computer

Make sure you have inserted the *X-Wall Secure Key* into the *Secure USB2.0* and then follow the instructions below:

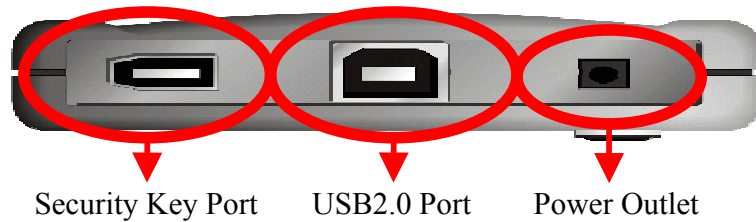
2.6.1 For Windows Users

1. Most computers come with several standard USB1.1 ports that support a transfer rate of 12 Mega bit per second. If you want to take advantage of the higher USB2.0 transfer rate (480 Mega bit per second), determine whether your computer is equipped with a USB2.0 port. If not, you may purchase

User's Guide 1.5

internal or external USB 2.0 adapters from third-party vendor and then continue with the installation. The *Secure USB2.0* product you have purchased can also work with the USB1.1 with slower speed.

2. Install the driver from the supplied CD-ROM. (If you use Windows 2000/ME/XP, you may skip this step).
3. Insert the *X-Wall Secure Key* in the *Secure USB2.0*.



4. Connect the *Secure USB2.0* to a USB port on your computer using the supplied USB2.0 cable.
5. Your computer will detect the *Secure USB2.0* automatically. The Green LED of the *Secure USB2.0* should light up, indicating the high-speed USB 2.0 connection is activated. However, the Green LED remains off if only USB1.1 connection is detected and enabled.
6. The host finds the new device but connection fails, an icon with exclamation mark will appear on the lower-right icon tray, indicating that the new device is not yet formatted. Proceed to Paragraph 2.7. FDISK & FORMAT.

2.6.2 For Mac users

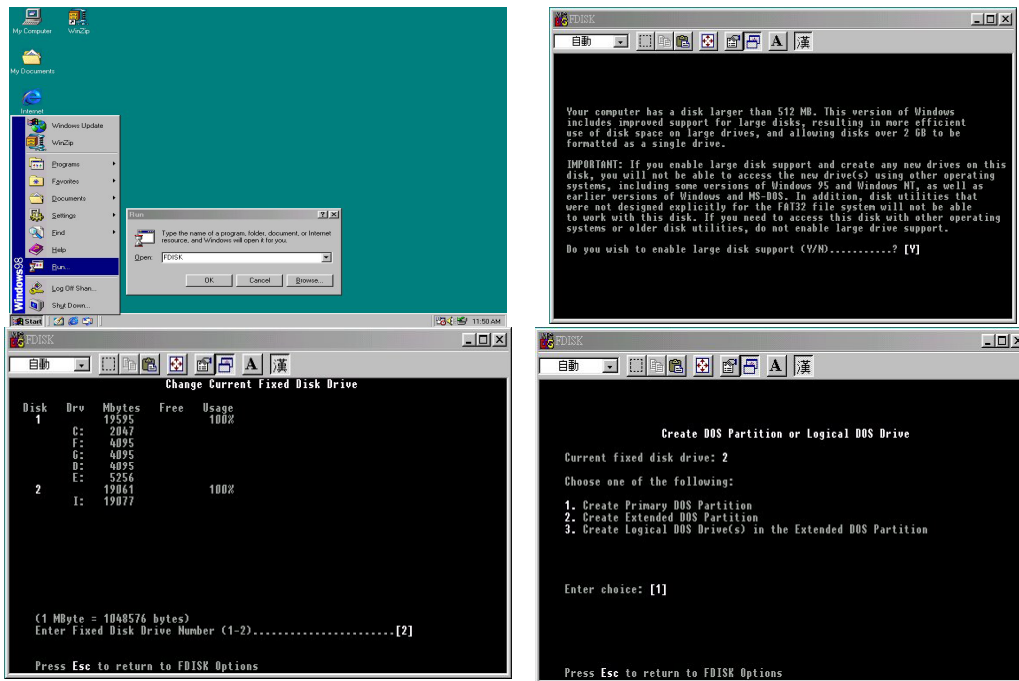
1. Please determine if your Mac computer is equipped with a USB port.
2. Connect *Secure USB2.0* to your Mac using the supplied USB2.0 cable.
3. Install the driver from the supplied CD-ROM. The CD-ROM folder will appear on the screen.
4. Drag the driver and drop it to the desktop. If you have:
 - a. Mac OS X 10.1 (driver version 1.0.1)
DB250/Mac/CYMSC_MACOSX_1_01.hqx – Mac OS X Storage Driver
 - b. Mac OS 9.x: (driver version 3.1)
DB250/Mac/MSC-DrvrInstaller.hqx – Mass Storage Class Driver
5. Run the driver and the system will add a driver installer folder automatically.
6. Open the driver installer folder, and then run the "Install Cypress Driver".
7. The system will start installing the driver. After installation, a message indicating that the installation was successful will appear on the screen.
8. Restart your computer.

2.7 FDISK & FORMAT

Remember - always plug in the *X-Wall Secure Key* while you perform the FDISK and FORMAT! After the completion of the FORMAT, you can safely remove the *X-Wall Secure Key* for normal operation.

2.7.1 For Windows 98 users

1. Click [Start] then [Run]. Type in "FDISK." The computer will enter the DOS mode.
2. Select the new disk to create a partition. Then remove the Secure USB2.0 from the host USB port and re-attach it (this is necessary as Windows plug & play will detect a new device). Remember the *X-Wall Secure Key* should always be plugged in while you perform these procedures.



3. After reattaching to the host USB port, a new device icon will appear in the icon tray.



4. You can find a new disk in the Windows Explorer. Click the new disk. A warning message pops up, indicating that the new disk is not functioning.



5. Right-click the disk and format it. Remove the *X-Wall Secure Key* after formatting. You can now use the *Secure USB2.0*.

2.7.2 For Window XP users

You must be logged on as an administrator.

Create a Partition

1. Open the **Disk Manager** tool, click **Start**, point to **Settings**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Computer Management**.
2. In the console tree under storage, click **Disk Management**.
3. Select the disk you want to partition, then right click on the mouse, and select **New Partition**. Then click "next" on the partition wizard.
4. Select **Primary or Extended** partition and click next.
5. Enter the amount of disk to use and click next.
6. Select a drive letter and click next.
7. Select the **File System Type**, **Allocation Unit Size**, enter a Volume label, click "next" when ready, and click "finish" to proceed with creating the partition.

Format a Drive

1. Open the **Disk Manager** tool, click **Start**, point to **Settings**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Computer Management**.
2. In the console tree under storage, click **Disk Management**.
3. Right click on the drive you want to format and select **Format**.
4. Enter the Volume label, File System type, the Allocation size, and click OK.

2.7.3 For Windows 2000 users

You must be logged on as an administrator.

Create a Partition

1. Open the **Disk Manager** tool, click **Start**, point to **Settings**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Computer Management**.
2. In the console tree under storage, click **Disk Management**.
3. Select the disk you want to create the partition on, right click on the mouse, select create partition and click next.
4. Select **Primary or Extended** partition and click next.
5. Enter the amount of disk to use and click next.
6. Select a drive letter and click next.
7. Select the File System Type, Allocation Unit Size, and enter a Volume label, click next when ready, and click finish to proceed with creating the partition.

Format a Disk

1. Open the **Disk Manager** tool, click **Start**, point to **Settings**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Computer Management**.
2. In the console tree under storage, click **Disk Management**.
3. Right click on the drive you want to format and select **Format**.
4. Enter the Volume label, File System type, the Allocation size, and click OK.

2.8 Removing Secure USB2.0

1. Make sure that all read/write tasks are completed. (The activities of the Yellow LED stop completely).
2. Click the "new device" icon on the tray. Choose "Safely Remove". A message will appear to indicate that you can safely remove the *Secure USB2.0* from the computer.
3. Unplug the USB cable.

Warning:

Removing the Secure USB2.0 before the disk activities have come to a complete stop may cause damage to your disk drive or the loss of data. We recommend that you always follow the "Safely Remove" command provided in Windows.



2.9 Reading Status Indicators

On the front cover of the *Secure USB2.0 unit*, there are total of three (3) LED lights (facing you from right to left: Green, Yellow and Red) that display the real-time status. The Green LED indicates that the high speed USB2.0 connection is enabled. It remains off if the host computer supports only USB1.1 transfer rates. The Yellow LED blinks off and on during normal disk activity. The Red LED reports an **ERROR** in reading the required Secret Key value from the *X-Wall Secure Key*. (Your disk drive will NOT be seen by the system until the correct *X-Wall Secure Key* is found inserted properly. Therefore, it is extremely important that you insert the correct *X-Wall Secure Key* properly prior to connecting the *Secure USB2.0*.)

3. TECHNICAL SUPPORT

3.1 Before Contacting Technical Support

1. Make sure you have properly inserted the 2.5-inch (9.5mm in height) disk drive to the main circuit board.
2. Make sure that you have correctly connected the *Secure USB2.0* to the host computer using the supplied USB2.0 cable.
3. Make sure that you have performed FDISK and FORMAT.
4. Make sure that you have correctly inserted the *X-Wall Secure Key* to the key insert of the *Secure USB2.0*.

If, after checking the above items, your *Secure USB2.0* still doesn't work properly, please read Appendix D – Trouble Shooting for additional information.

3.2 Contacting Technical Support

Enova's Technical Support Department is open Monday through Friday 9:00am - 5:00pm, Pacific Standard Time. Please call 408.956.8100, visit our web site <http://www.enovatech.com>, or email Technical Support support@enovatech.com.

APENDIX A – Understanding Cryptographic Technology

Abstract

Cryptography is a fundamental security technology that preserves the privacy and confidentiality of data that is stored or transmitted. This short guide will help you understand the basic principles of cryptography and why X-Wall is the strongest available product of its type.

Since the invention of electronic communication, encryption has been used extensively for both military and commercial purposes. Consequently, most people think about data “in motion” when they consider security risks. This makes sense because, in the IT world, stored data generally resided on carefully monitored mainframes and minicomputers. Now, however, the proliferation of mobile computing devices such as notebook PCs, PDAs, and smart phones has irreversibly changed the risk pattern. Large amounts of sensitive data and important personal credentials can be stored on portable devices that are easily lost or stolen.

The hard drives of notebook PCs are especially at risk because they are used in non-secure environments. These drives typically contain key strategic data, engineering projects, patent applications, private health care information, payroll data and other sensitive data. Users frequently store passwords and access codes to the corporate network on notebook PCs. If these credentials are stolen, interlopers can penetrate network security at will and perpetrate serious crimes.

However, the problem is not confined to mobile devices. Statistics compiled annually by the FBI continue to show that the majority of computer security breaches are perpetrated by employees or contractors who have access to sensitive data on the internal network. Since unattended PCs are the easiest entry point into the network, it becomes important to implement access controls that prevent unauthorized usage. There are also hidden risks, such as when a failed hard-drive is sent to a third-party for repair, or when PCs are retired or donated.

Encryption is a useful tool in responding to all these concerns. Nevertheless, not all encryption systems are equally practical or adequate for every job. There are seven (7) factors that you should consider:

- Application
- Environment
- Algorithm
- Implementation
- Length of encrypting key
- System Performance
- Human Factors

Application

The type of applications used determines the value of the data. The patent application for a new drug is obviously more valuable than an inventory report. Some applications in the finance and health sectors are subject to US Federal regulations that require the protection of private information pertaining to customers.

Environment

Data stored on a stationary machine in a well monitored facility would appear to be less at risk than the same data stored on the notebook PC of an executive that travels extensively abroad. However, the risk of unauthorized access by other employees is still present.

Algorithm

Since it is extremely difficult to determine the actual quality of encryption algorithms, it is essential to use algorithms that have been tested and certified to meet high standards of integrity. Federally approved algorithms are listed at the NIST website.

Implementation

Even a system that uses strong encryption is at risk if the algorithm is poorly implemented. Once again, it requires expert skills and substantial testing to determine whether a system is well conceived. Consequently, the US government, in partnership with Canada, has approved a number of testing laboratories that certify products as complying with the FIPS (Federal Information Processing Standards) and international Common Criteria standards.

Length of encrypting key

Since standard algorithms must be published to be worthwhile, the secret is in the keys that drive the algorithms. The longer the key used in encryption, the more combinations that must be tried to break the encryption. The length of key required to maintain a given level of security is constantly growing because of continued improvements in the technology used to hunt for keys. Currently 40bit keys are at the lower end of acceptability and 128 bit keys are very secure.

System Performance

No security system is acceptable if it is so cumbersome that overall system performance is noticeably impaired. The speed at which encryption proceeds depends on a variety of factors – the algorithm, the length of keys used, and whether software or hardware is used to perform the encryption. Properly implemented, hardware can encrypt at a much higher rate than software.

Human Factors

No security system will succeed if the users refuse to participate. Poorly conceived encryption systems require significant advance user training and frequent manual intervention. Other problems include forcing people to work in a different manner or placing them under undue pressure to remember constantly changing

User's Guide 1.5

passwords. Successful security implementations begin with the philosophy that management should provide users with security tools that help them support the company security policy and don't impede their ability to perform their jobs.

Methods of Encryption

Encryption is accomplished by using mathematical computations that make it extremely difficult and time consuming for anyone other than authorized recipients to recover the plain text. Proper encryption guarantees that information will be safe even if it falls into hostile hands. Either software or hardware, or the combination can perform the functionality of encryption and decryption. Common approaches include writing the algorithm on a disk for execution by a central processing unit; placing it in ROM or EPROM for execution by a microprocessor; and isolating storage and execution in computer accessory device such as smart card or PCMCIA.

The degree of protection obtained depends on several factors. These include: the quality of the crypto system; the way it is implemented in software or hardware (especially its reliability and the manner in which the keys are generated); and the total number of possible keys that can be used to encrypt the information. A cryptographic algorithm is considered strong if:

There is no shortcut that allows the opponent to recover the plain text without using brute force to test keys until the correct one is yielded; and the number of possible keys is sufficiently large to make such an attack infeasible.

The principle here is similar to that of a combination lock on a safe. If the lock is well designed, a burglar cannot hear or feel its inner workings. Consequently a person who does not know the combination can open it only by dialing one set of numbers after another until it yields. Thus a crucial determinant of the strength of a cryptographic system design is the length of the key. The size of an encryption key is measured in bits and the difficulty of trying all possible keys grows exponentially with the number of bits used. Adding one bit to the key doubles the number of possible keys; adding ten increases it by a factor of more than a thousand.

There is no definitive way to look at a cipher and determine whether a shortcut exists. Nevertheless, several encryption algorithms -- most notably the US Data Encryption Standard (DES) -- have been extensively studied in the public literature and are widely believed to be of very high quality.

Classes of Encryption

Symmetric Cipher

A symmetric cipher uses the same key to encrypt and decrypt the data. Also described as a "secret-key" or "shared key" system, the symmetric key must be

User's Guide 1.5

known to both the sending and receiving parties and kept secret from others. Symmetric algorithms such as DES and TDES are very efficient, and thus useful for encrypting large blocks of data for transit. The drawback is that symmetric keys require a secure mechanism to transmit the secret key from the sender to the receiver. In times past, such a key could be sent by arranged courier service, by exchange of floppy disk, transferred over a secure modem link, or simply transcribed over a telephone. However, in the networked world, no secure channel exists between the sender and the users on the Internet. Also as the number of parties that increases, the number of shared secret keys grows geometrically making secure key management a difficult problem.

Asymmetric Cipher

Asymmetric key systems are critical to the future of e-commerce. The asymmetric key system, also described as a "public-key" system, makes use of the difficulty of solving certain kinds of mathematical problems. In the asymmetric system, one key encrypts the data while another related but different key decrypts it. Related keys are called "key pairs"; one is the "private key", which is never divulged, and the other is the "public key" which can be openly published or transmitted. If A wishes to send a secure message to B, A will encrypt the message using party B's public key. The resulting message can only be decrypted using B's private key. Since B is responsible to keep this key secure, it is assumed that only B can read it. Clearly, an asymmetric system solves the problem of key exchange. A server can now set up a secure channel with a previously unknown client by setting up a channel using an asymmetric channel. One challenge is that the key pair generation algorithms are compute-intensive; this is not a problem for the clients, but key pair generation can cripple a big transaction server. Dedicated hardware key pair generation units appear to alleviate such a bottleneck. Another limitation of asymmetric systems is that they are very inefficient. Consequently asymmetric systems are generally used to transmit small amounts of data.

In summary, asymmetric systems use uniquely matched key pairs that are the encryption/decryption inverses of each other but cannot be derived from an encrypted message, its plain text, and the other key. Secrets can be exchanged in a public environment but at the cost of greater computational resources.

Combination Systems

An ideal system would combine the public key exchange properties of the asymmetric cipher with the bandwidth handling capability of the symmetric cipher. By combining features in symmetric and asymmetric cipher, a private communication channel can be established while conducting high bandwidth data transfer. Such systems are in common use today.

Encryption with X-Wall

User's Guide 1.5

The X-Wall uses the symmetric DES or TDES algorithms to enable high speed encryption of everything written to the hard disk. The X- Wall provides a choice of key lengths ranging from 40 bits to 192 bits to suite the needs of a wide variety of applications. The secret key is NOT stored in the *X-Wall* microchip or anywhere on the hard disk. Instead, it is stored in the *X-Wall Secure Key* supplied with your product. The secret key is transmitted into the *X-Wall* microchip at boot up and is retained in protected volatile memory inside the chip until the power is turned off. This means the secret key cannot be extracted from the chip, and is never stored anywhere else on the machine. This combination of US approved algorithms, coupled with very strong key management and the ability to select the appropriate key length, makes X-Wall the most secure product of its type available.

APPENDIX B -- Introducing *X-Wall*[®], A Real-time IDE Crypto Gateway

Abstract

DES was introduced as a US encryption standard in 1971 after exhaustive testing and has since been publicly proven as a solid and quality algorithm. TDES (Triple DES) was then introduced to reinforce the original 56-bit DES bit length because advances in microprocessor and integrated circuit manufacturing increased the possibility that a “brute force” attack might succeed. Over time, many security products have utilized the DES standard to protect transmitted data.

In contrast, comparatively few products have been developed to protect data at rest, and most of these are software applications that perform file-level encryption. File encryption can be done using application software or hardware devices such as PCMCIA cards or external ASIC-based devices. On the surface, encrypting only selected files seems to make sense since not everything is confidential and this procedure reduces the amount of material that must be encrypted, and thus diminishes the overall performance loss associated with software encryption.

These advantages are largely illusory however. File encryption is inherently slow because the entire file must be decrypted before any portion of it can be presented to the user. Also, file encryption ignores the temp and swap files that are automatically created and stored in clear text. Worse still, file encryption requires manual intervention by users who easily become confused and frustrated. From the organizational standpoint, because file encryption is not automatic, it is difficult to enforce security policy. The level of security attainable with file encryption is also questionable, since file encryption programs run under the control of the operating system. If you can subvert the operating system you can often subvert the file encryption program and access encrypted data. Encrypting PCMCIA cards and external ASIC devices have been created to provide greater key security and to improve performance, but have had only marginal success and suffer from a variety of compatibility issues. With all these deficiencies, it is increasingly clear that file encryption is not suitable for organizations that require security, convenience and performance.

Full disk encryption coupled with machine level access control is a much more powerful solution. Everything on the hard drive -including data files, swap files, temp files and the operating system - is automatically and transparently encrypted without user intervention. User authentication and access control occurs at the bios level, thus preventing illicit users from access to the operating system where they can use a variety of well-known and easily obtainable tools to subvert the entire system. Both the organization and the users win – the organization can maintain a very effective security policy without requiring any training or involvement from the users.

User's Guide 1.5

Full disk encryption can be done with advanced software or hardware. In either case, everything sent to the drive is encrypted. But a “real-time” physical layer ASIC-based hard disk crypto-system hardware offers three substantial advantages over software solutions. First, the secret encryption key is more secure in hardware. Second, specially designed ASICs can encrypt in real time without the overhead and interrupts required by software encryption programs. Third, a physical layer ASIC does not require device drivers and is independent from, and thus compatible with, all operating systems.

Fundamentals

The *X-Wall SE*, represents the next generation of real-time, high bandwidth full drive encryption and machine access control. A cryptographic system controller ASIC, X-Wall SE utilizes a standard IDE/ATA bus to protect sensitive information stored on an IDE hard drive. The ***X-Wall SE*** encrypts and decrypts the entire hard disk bit by bit (including boot sector and operating system) in **real-time** performance using *NIST (National Institute of Standards and Technology)* certified *DES/TDES* algorithm. Other public domain algorithms such as AES (Advanced Encryption Standard) can be utilized to replace DES/TDES.

X-Wall SE sits between Host IDE and the device IDE interface as the real-time IDE crypto gateway. It intercepts, interprets, translates, and relays those commands & data to and from the disk drives, encrypting the data with DES/TDES 64/128/192-bit key strength. *X-Wall SE* can be operated with Ultra ATA (Ultra DMA) 33/66/100 compliant disk drives in **real-time** mode with a throughput of 1.1 Giga bit per second or higher.

Design Objectives

The device will function between the IDE host controller and the IDE hard drive. It incorporates both a target and a host interface for IDE Ultra DMA 33/66/100, and effectively captures and decodes commands from the host, encrypts data, and then regenerates the commands and data to the target interface. The device includes a real-time encryption pipeline engine that can be inserted into the data stream to encrypt or decrypt the data to or from the hard disk drive. This design provides the following benefits:

- TDES (or DES) real-time encryption & decryption
- Performance identical to that of a non-encrypted system
- Completely independent from all operating systems
- Completely free from device drivers
- Completely transparent from all system configurations
- Low power consumption
- Machine access control
- Ability to indicate operational states
- Detect errors and prevents sensitive data and secret keys from being compromised due to errors

APPENDIX C – How to Use FDISK and FORMAT

FDISK – Partition

Under DOS prompt, type FDISK and press <Enter>.

Do you wish to enable large disk support? (Y/N) [Y]

- | |
|--|
| <ol style="list-style-type: none">1. Create DOS Partition or Logical DOS Drive2. Set Active Partition3. Delete Partition or Logical DOS Drive4. Display Partition Information |
|--|

Select "1" to create DOS Partition or Logical DOS Drive.

- | |
|---|
| <ol style="list-style-type: none">1. Create Primary DOS Partition2. Create Extended DOS Partition3. Create Logical DOS Drive(s) in the Extended DOS Partition |
|---|

Select "1" to create Primary DOS Partition.

Do you wish to use the maximum available size for a Primary DOS Partition and make the Partition active (Y/N) [Y]

The following screen appears after you have chosen "Y."

Total disk space is xxxxx Mbytes (1 Mbytes = 1,048,576 bytes) Maximum space available for partition is xxxxx Mbytes (%) Enter partition size in Mbytes or percent of disk space (%) To create the Primary DOS partition []
--

Enter the desired size in Mbytes or as a percentage of disk space (for example: 50%).

FORMAT

An FAT16 format with LBA support can format up to 2GB per partition (512MB per partition without proper BIOS support). An updated FAT32 format from Windows 95B, Windows 98 and Windows 2000 can format up to 8GB per partition. The latest NTFS (NT file system) from Windows NT and Windows XP can format up to 8GB per partition. The Motherboard onboard BIOS extended INT13 service capability, along with FAT32 and NTFS, allows you to partition and format a drive larger than 8.4GB as one single partition. The NTFS is backward compatible with FAT32 and FAT16. A Windows NT/2000/XP Operating System supports drives formatted with FAT32 and/or FAT16. However, Windows 95, 98 and ME Operating System do NOT support drives formatted with NTFS. Therefore, it is extremely important that you choose the right diskette containing the right "FDISK" and "FORMAT" programs to partition and format your new disk.

User's Guide 1.5

To format your new drive, insert a bootable diskette containing the "FDISK" and "FORMAT" programs into the A: drive then power on the computer. Type "FORMAT <drive letter>" under DOS prompt then press <Enter>. For example, to format the C: drive, under DOS prompt, type "FORMAT C:" to start formatting. Type "FORMAT C:/S" to start formatting with the system files copied.

APPENDIX D – Trouble Shooting

The following procedures provide a general guideline to work with *your Secure USB2.0* if you experience any problems.

I do not observe any disk activities through the Yellow LED light.

Make sure your USB2.0 cable is connected correctly both to the host computer and *Secure USB2.0*.

The Green LED light isn't on

You have only the USB1.1 connection enabled. Your computer can only support up to USB1.1 transfer. The GREEN LED of the *Secure USB2.0* will be on when the host computer has a true USB2.0 hardware established.

The Red LED light is on

Your *Secure USB2.0* can NOT read the Secret KEY value from the X-Wall Secure Key. Make sure that you have properly inserted the X-Wall Secure Key onto the key insert. Without the presence of the correct and original X-Wall Secure Key, your disk drive will NOT boot or will not be seen.

What's the normal condition of those LED lights?

The Yellow LED light blinks whenever there is disk activity. The Green LED stays on when the host computer has a true USB2.0 hardware. Otherwise, the Green LED is off. The Red LED light shall remain off unless condition of X-Wall Secure Key error occurs.

APPENDIX E – FAQ

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, there is no software to cause memory and interrupt overhead.

Q: How does X-Wall SE function?

A: X-Wall SE, sits between the PCI south bridge and the device on the 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 that the disk drive is Ultra ATA (Ultra DMA) compliant.

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 with 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 of any data or credentials being left unprotected on the hard drive. Drive locking and boot sector encryption solutions do not encrypt the data, and it is thus 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

User's Guide 1.5

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 of 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 the DES 56-bit key length is no longer proof against 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 special design 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 increases 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 seen cumbersome log on procedures. It is totally transparent to all users. You only need 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 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?

User's Guide 1.5

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* 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 use on a disk drive