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) the document, any part of the program, or any information contained in the *Enova Secure Product family* package without the written authorization of Enova Technology.

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 than the circuit receiver is connected**
- **Consult the dealer or an experienced radio/TV technician for help**
- **Move the computer away from the receiver**

Copyright Notice

Enova Technology Corporation
Building 53, #195-57, Sec. 4, Chung Hsing Road, Chutung District
Hsin-Chu County, Taiwan 310
Republic of China
Tel.: +886 3 591 0197 Fax: +886 3 591 0204
http://www.enovatech.net
info@enovatech.net

Enovatech, Inc. (dba Enova Technology)
1072 Yosemite Drive
Milpitas, California 95035, USA
Tel: 408 956 8100 Fax: 408 956 8102
http://www.enovatech.com
info@enovatech.com

Trademarks

Enova, 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 CONTENT

LIMITED WARRANTY AND DISCLAIMER

Limited Warranty. Enova Technology (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 by any third party hardware and/or software not owned by Enova; or (d) subjected to extreme power surge or electromagnetic field.

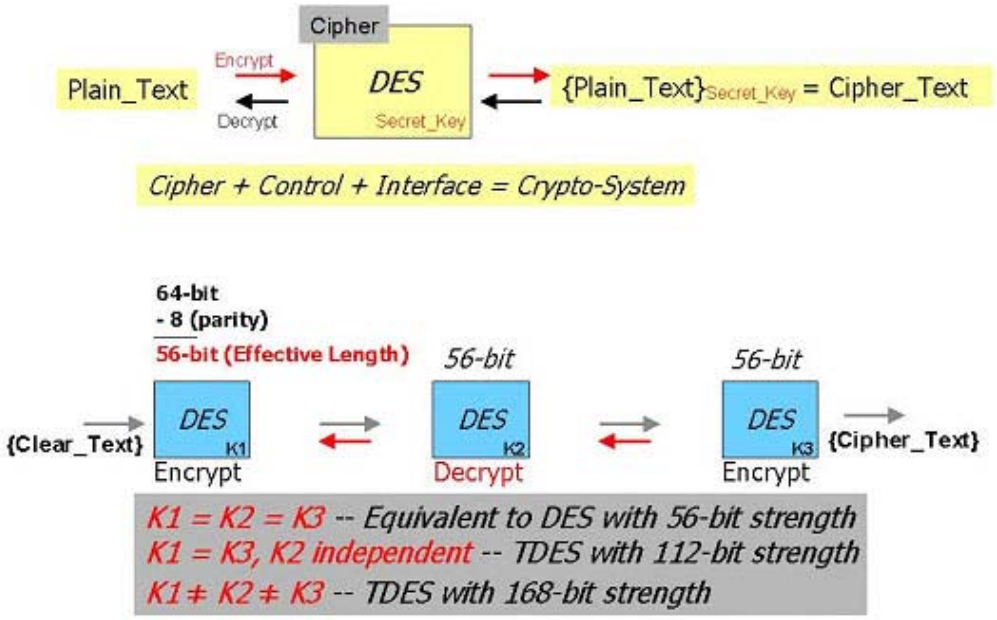
Disclaimer. THE LIMITED WARRANTY IS THE ONLY WARRANTY MADE BY ENOVA. THE WARRANTIES AND LIMITATIONS SET FORTH IN THIS ARTICLE CONSTITUTE THE ONLY WARRANTIES MADE BY ENOVA WITH RESPECT TO THE LICENSED PRODUCT, AND ENOVA SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, WRITTEN OR ORAL, STATUTORY, EXPRESS OR 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 length[1] 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 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 LX is a cutting-edge technology product that offers near military grade protection. All ***Enova X-Wall Secure products*** contain the *X-Wall®LX* family[2] 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 LX* is totally transparent to users; there are no commands or graphical user's interface to contend with. *X-WALL LX* is extremely fast, capable of processing 1.6 Giga bit per second throughput without taking extra CPU time and system resources. Furthermore, *X-Wall LX* works with ALL operating systems and does not require any device drivers.

X-Wall LX 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; at full strength it is nearly impossible to access the encrypted 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 LX 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 and native mode IDE 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 LX* microchips and their associated key length and specifications:

X-Wall	**Encryption Strength**	**NIST[4] & CSE[5] Certified 100% hardware Cipher Engine**	**Maximum Throughput**	**Ultra ATA hard disk support**	**Ultra ATA hard disk compliance**	**Protocol & Transfer mode support up to**	**Package**
LX-40	40-bit	**DES**	1.6 Gbit/sec	> 137GB	66, 100, 133	ATA 6, Mode 6 transfer	128-pin LQFP
LX-64	64-bit	**DES**	1.6 Gbit/sec	> 137GB	66, 100, 133	ATA 6, Mode 6 transfer	128-pin LQFP

[2] Four (4) different strength of encryption/decryption are provided within *X-Wall LX* family 40-bit, 64-bit, 128-bit and 192-bit. The X-*Wall LX-40* stands for 40-bit strength and vice versa.
[3] Also called IDE. The throughput of the latest Ultra ATA mode 5 standard is specified at 100Mbytes/sec. The 133Mbytes/sec specification is proposed in ATA 6.
[4] NIST – The National Institute of Standards and Technology of the United States of America
[5] CSE – The Communications Security Establishment of the Government of Canada

LX-128	128-bit	**TDES**	1.6 Gbit/sec	> 137GB	66, 100, 133	ATA 6, Mode 6 transfer	128-pin LQFP
LX-192	192-bit	**TDES**	1.6 Gbit/sec	> 137GB	66, 100, 133	ATA 6, Mode 6 transfer	128-pin LQFP

1.1 Key Features

- Totally transparent to all users
- Portable ***X-Wall Secure Key*** for authentication and access control
- Works with all operating systems
- Does NOT require any device drivers
- Works with all motherboards with standard IDE Interface
- Real-time DES 40/64-bit or TDES 128/192-bit encryption/decryption with throughput of 1.6 Giga bit per second or higher
- IDE pin to pin compatible
- Supports 48-bit LBA mode
- Low power consumption
- 128-pin LQFP small form factor package

1.2 System Requirements

- All operating systems
- Ultra ATA (Ultra DMA) 66/100/133 compliant disk drive for high throughput configuration
- PIO or native IDE 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 MOTHERBOARD COMES WITH TWO STANDARD IDE CHANNELS: PRIMARY AND SECONDARY. EACH CHANNEL ALLOWS YOU TO CONNECT UP TO TWO IDE/ATAPI DEVICES. NORMALLY A LARGE VOLUME HARD DISK DRIVE[6] RESIDING ON THE PRIMARY CHANNEL IS ASSIGNED AS THE BOOT DRIVE, WHILE OPTICAL DRIVES SUCH AS CD-ROM/CD-R/CD-RW/DVD-ROM RESIDE ON THE SECONDARY CHANNEL. SOME MAY PREFER CONNECTING TWO DISK DRIVES (ONE MASTER & ONE SLAVE) ON THE PRIMARY CHANNEL AND LEAVE THE SECONDARY CHANNEL FOR CD-ROMS ETC. THE *X-WALL LX* 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 LX*, OR YOU WILL EXPERIENCE TECHNICAL DIFFICULTIES, INCLUDING POTENTIAL DATA LOSS AND THE PRODUCT WARRANTY WILL BE REVOKED.

1.3 Read This before Installation

You are urged to carefully read through the following sections prior to your installation.

[6] Drives today have more than 20GB. 40GB or more is an IDE drive standard.

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***[7] 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 impossible[8] for you to recover your data**. There is no "backdoor" in *X-Wall* technology. Enova does not retain records of the random *Secret Key* contained in *X-Wall Secure Keys*. It is the Enova's **policy** to destroy the random database[9] 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. Please note, however that you must send in your backup Key along with your order for duplication. Otherwise we cannot create additional keys.

POSSIBLE FAILURE OF X-WALL LX SECURE CHIPS

Every *X-Wall LX* family microchip we ship is 100% tested and proven and complies with International quality assurance standards[10]. However, there may be occasions that chip malfunctions after some period of time. This problem can be resolved by simply replacing the defective *X-Wall LX* 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*.

---

[7] Which stores the "Secret Key" value required for the functional 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.

[8] Depends on the product you chose, a DES 40-bit encryption is a bit easier to decrypt (thought it is extremely hard for a non-engineering major individual). Please refer to FAQ for more explanations. A DES 64-bit encryption is extremely hard to decrypt and the process will consume lots of time and money. The decryption process of TDES 128-bit without the right Secret Key is physically impossible.

[9] It is used to write the Secret Key value to every *X-Wall Secure Key*.

[10] 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.

2. INSTALLATION – Secure Mobile Rack

The Secure Mobile Rack will require a single 5.25-inch drive bay for each 3.5-inch Ultra ATA 33/66/100 hard disk drive connection. It provides a simple and easy way to remove and store the hard drive to a vault or a secure storage location for added security. The unit is designed with a powerful airflow system for superior cooling and shock absorbers for drive stability and shock resistance.

2.1 Before Installation

You will be required to **FDISK** and **FORMAT** the disk after installing the hard drive onto the X-Wall device. 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 will need to backup the data on the disk. **WE ARE NOT RESPONSIBLE FOR ANY LOST DATA**.

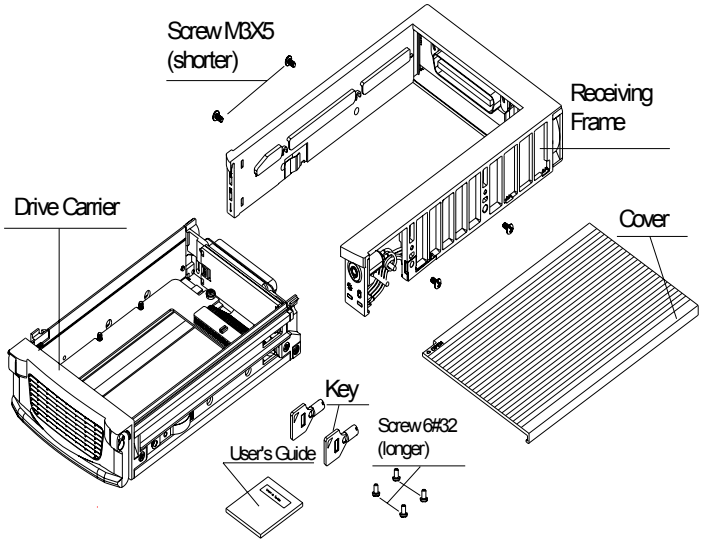
2.2 Unpack the Secure Mobile Rack

Please check if your package has everything listed below. If you discover any damaged or missing items, please contact your distributor/retailer. Some items are stored in the drive carrier.

* Receiving frame:	1
* Drive carrier	1
* Drive carrier cover	1
* Drive carrier lock key (round)	2
* Screw for frame	8
* Screw for hard drive	4
* User's guide	1
* Registration and Warranty Card	1
* External & portable *X-Wall Secure Key* (pair)	2
* Standard 80-conductor 3 IDE connectors cable	1
* Custom-made 80-conductor IDE cable (built-in)	1


Secure Key


Standard 80-conductor IDE cable



2.3 Configure Your Hard Disk Drive

Power off the computer and remove the computer cover. Determine if the hard disk will be used as a "Master" or a "Slave" drive; then set the proper jumpers on the unit. Most computers come with

two IDE channels on the motherboard. They are designated as Primary IDE and Secondary IDE. Each IDE channel can support 2 IDE devices: one must be set as master and the other as slave. A master drive is usually the boot drive where the operating system is installed. A slave drive is usually an additional drive you're adding to your system. Please refer to the hard disk user's manual for instruction on how to set the jumpers on the disk drive.

The following table shows four possible configuration options for your hard drive. You can **ONLY** choose from one of the four possible options.

X-Wall SE Controller	Primary IDE Channel	Secondary IDE Channel
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}**

Option 1: Primary Master – if the intended disk drive is to be used as a secure boot drive. Everything including the boot sector and the operating system will be encrypted real-time. You must configure the disk as MASTER by setting the proper jumpers on the drive.

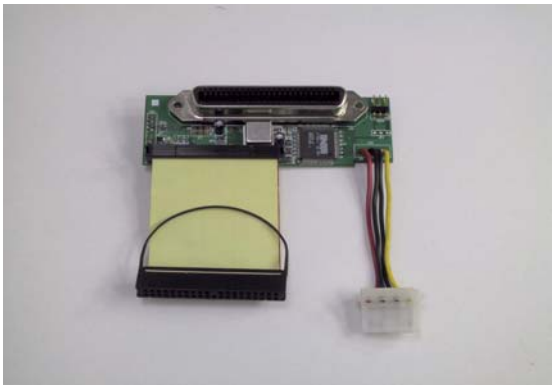
Option 2: Primary Slave – if the intended disk drive is to be used as a secure data storage drive. You must configure the drive as SLAVE by setting the proper jumpers on the drive.

Option 3: Secondary Master – if the intended disk drive is to be used as a secure data storage drive. Again, you must configure the disk as MASTER by setting the proper jumpers on the drive.

Option 4: Secondary Slave – if the intended disk drive is to be used as a secure data storage drive. You must configure the drive as SLAVE by setting the proper jumpers on the drive.

2.4 Configure Your Secure Mobile Rack

Figure 1. Secure Mobile Rack



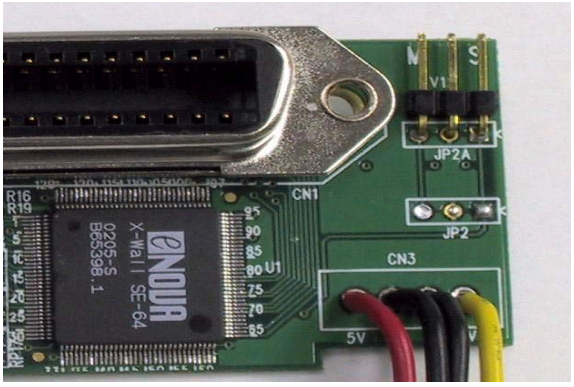


Figure 2. Main Circuit Board of the Secure Mobile Rack

Figure 3. Master/Slave Configuration of the Secure Mobile Rack

The configuration of the Master/Slave on the disk drive and the Secure Mobile Rack must match. Otherwise, the Secure Mobile Rack unit will NOT function correctly. As shown in Figure 3, the default of the Secure Mobile Rack is set as Master. If you set the disk drive as a Master drive, then you can either set the jumper on the 2 left most pins or leave the jumper unattached. If the disk drive is set as slave, you must set the jumper to the 2 right most pins.

2.5 What's So Important About Your IDE Cables (For Advanced Users)

This paragraph offers important guidelines for using your IDE cables. The Ultra ATA 66/100 transfer modes require an 80-conductor cable (as shown in **Figure 4. A standard 80-conductor IDE cable**) whereas Ultra ATA 33 and below (including PIO) only demand a 40-conductor cable (as shown in **Figure 5. A standard 40-conductor IDE cable**).

An 80-conductor IDE cable uses the same 40-pin connector as the 40-conductor IDE cable. The wires of the 80-conductor cable alternate: ground, signal, ground, signal, ground, signal, ground, etc. All the ground wires are tied together on the cable (and they are tied to the ground on the motherboard or circuit board through the ground pins in the 40-conductor Connector).

To determine if Ultra ATA 66/100 can be enabled, the system software will attempt to determine the cable type used in the system through **Pin 34** of the Host connector as shown **in Figure 4. A standard 80-conductor IDE cable**. If the system software detects an 80-conductor cable through Pin 34, the system may use any one of all the available transfer modes up to the highest transfer mode supported by **both** the system chipset and the IDE device. If a 40-conductor cable is detected, the system software can NOT enable transfer faster than Ultra ATA 33.

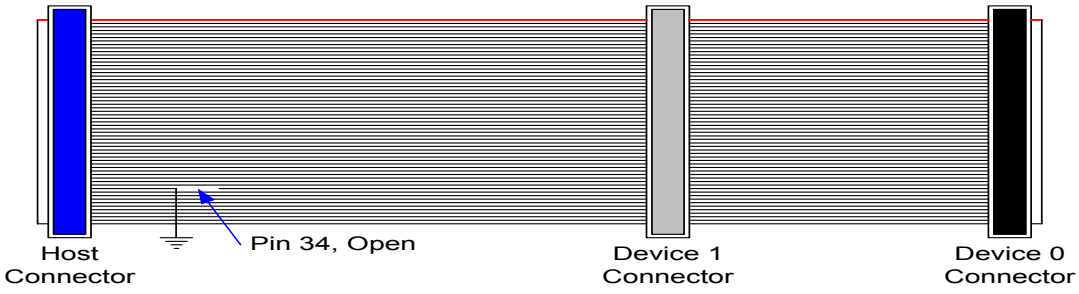


Figure 4. A standard 80-conductor IDE cable (to work with Ultra ATA 66/100 drives. The Pin 34 of the Host connector is grounded)

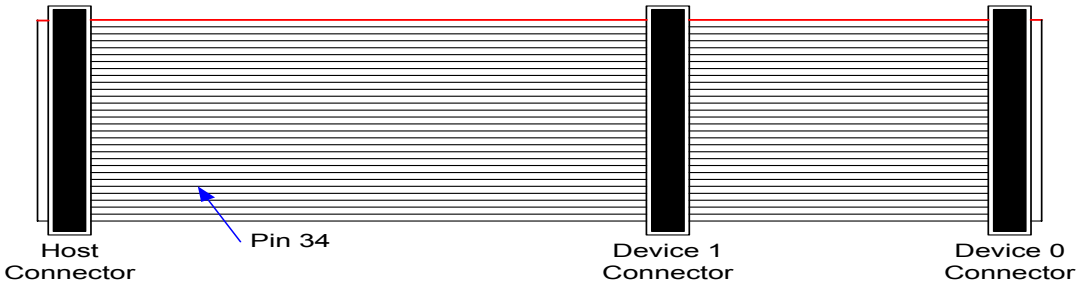


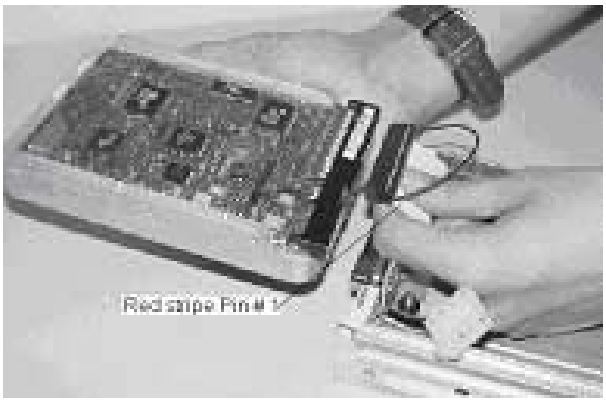
Figure 5. A standard 40-conductor IDE cable (to work with Ultra ATA 33 and below. The Pin 34 of the Host connector is NOT grounded)

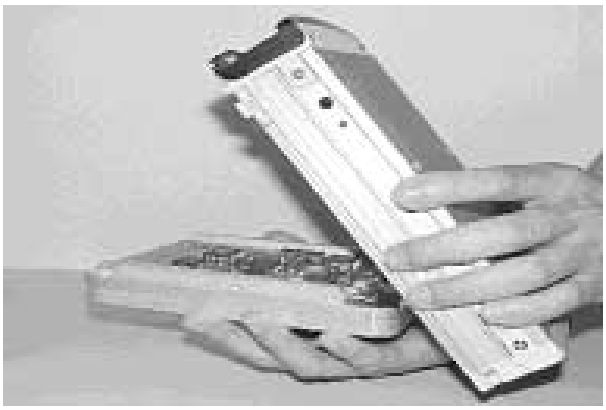
The Host connector should be directly connected to the motherboard. Device 0 is the connector for Master device where as Device 1 is the connector for Slave device. It is highly recommended that for a single device configuration the device must be placed at the opposite end of the cable from the host. If a ***single device configuration*** is chosen and the single device is not connected at the opposite end of the cable from the host, signal degradation may occur which may in terms deteriorate the Ultra ATA transfer.

2.6 Installing the Hard Drive into the Drive Carrier

Locate a place to work on a soft surface to prevent excessive shock to the drive. You will need a #2 Phillips screw driver to perform this procedure.

1. Pull on the drive carrier handle to slide the carrier out of the receiving frame.
2. Remove the top cover of the carrier by pushing the button on the front corner and sliding the cover back.
3. Gently connect the flat cable on the drive carrier to the hard drive's IDE connector. You must align the red stripe on the carrier's cable with "pin 1" on the hard drive connector.
4. Connect the 4-pin power cable in the drive carrier to the hard drive.
5. Holding the drive and carrier upside down, gently and slowly move the drive carrier over the hard drive. Check to be sure none of the cables is pinched.
6. Use the 4 provided screws to fasten the drive into the carrier.
7. Slide the top cover onto the drive carrier from the back and snap it into place. The drive carrier is ready for use.

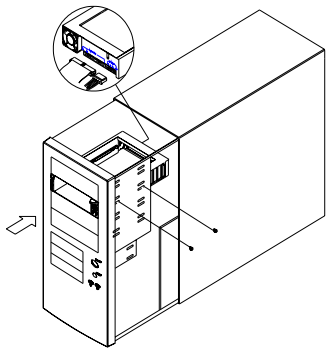




2.7 Installing the Receiving Frame into the Computer

Figure 6. Standard 80-conductor 3 IDE connectors cable

The unit comes with one standard 80-conductor IDE cable as shown in Figure 6. The included cable has three (3) standard IDE connectors. It is recommended to use the provided cable to connect one end to either the Primary or Secondary IDE Channel on the Motherboard and the one of the other two IDE connectors to the back of the receiving frame. Hard drives other than Ultra DMA/ATA 66/100 can be used with your regular 40-conductor IDE cable. In this scenario, your system software will therefore determine the best possible transfer rate.



1. Remove the computer cover and an available bay cover plate. Save all the mounting screws and clips.
2. Slide the receiving frame into the drive bay. Make sure the provided IDE cable and the 4-pin power cable you intend to use will reach the back of the receiving frame.
3. Connect the provided IDE cable to the 40-pin connector and an available 4-pin power cable to the receiving frame.
4. Use the screws provided to secure the receiving frame into the drive bay. Make sure the front of the receiving frame aligns evenly with the devices in the other drive bays. If not, adjust the positions as necessary and tighten the screws.
5. Replace the computer cover and reconnect the power cord.
6. Pull on the carrier handle and slide the carrier into the receiving frame until you feel a slight resistance as the drive carrier connector pushes against the receiving carrier connector.
7. Lower the handle to seat the carrier into the receiving frame.
8. Insert the lock key (round) into lock carrier of the receiving frame turn it clockwise. This will provide power to the unit.
9. Properly insert the X-Wall Secure Key (long) into the key insert on the front panel.
10. You must now perform FDISK and FORMAT operations on the disk. These operations will prepare the disk to be used and encrypt both the boot sector and the file allocation table (FAT). Please refer to Appendix C – How to use FDISK and FORMAT. With each X-Wall product, the FDISK and FORMAT operations must be performed on the disk regardless if the drive is brand new or old.

    Note: The FDISK and FORMAT operations will erase everything on a disk. Please backup the data before starting these operations. **We are not responsible for any lost data.**

Please do NOT attempt to turn the lock key or remove the drive while the system is running, doing so may result in data loss or damage to the entire unit and your warranty will be revoked.

2.8 What Would You See On A Functional Secure Mobile Rack?

As shown in Figure 1, there are a total of three (3) LED lights on the Secure Mobile Rack. The receiving frame has two LED lights (Green and Yellow) that display the current status of the unit. A blinking Yellow LED light indicates disk activities and a solid Green LED light indicates proper power is connected to the unit. The Red LED light on the drive carrier gives you the status of the *X-Wall Secure Key*. An emitting Red light indicates an **ERROR** in reading the Secret Key from the *X-Wall Secure Key*. Your disk drive will NOT be bootable or recognizes by the system until the correct *X-Wall Secure Key* is inserted.

It is extremely important that you properly insert the correct *X-Wall Secure Key* prior to powering up your computer. Do **NOT** attempt to connect any 1394 devices to the KEY insert on the drive carrier. It is designed to read the *X-Wall Secure Key* only.

After a successful boot up, you may remove the *X-Wall Secure Key* or wait until the computer is properly shut down. Removing the *X-Wall Secure Key* after the system is booted up will not affect the operation of the computer.

3. INSTALLATION – Secure PCI Adapter

Your Secure PCI Adapter allows you to encrypt/decrypt data on a single 3.5-inch hard disk drive. It comes with two 80-conductor IDE cables to be used on your hardware installation. One has 2 IDE connectors for connecting the hard disk to the Secure PCI adapter and the other has 3 IDE connectors for connecting the Secure PCI adapter to the motherboard. ***It is recommended you use these custom-made cables for the installation.*** Details follow.

3.1 Preparation and Backing up your Data

The *Enova Secure Product* is susceptible to static electricity. Keep the product in its anti-static bag to avoid electrical damage until proper grounding is performed. To ground, simply put your bare hands on the computer chassis for a couple seconds, then you can remove the product from the anti-static bag.

3.2 Unpack the Secure PCI Adapter

Please check if your package has everything listed below. If you discover damaged or missing items, please contact your distributor/retailer for a replacement.

* Secure PCI card as shown in Figure 7	1
* Extension cord for key insert as shown in Figure 7.1	1
* User's guide	1
* Registration and Warranty Card	1
* External *X-Wall Secure Key*	2
* Standard 80-conductor with three IDE connectors cable	1
* Custom-made 80-conductor with two IDE connectors cable	1

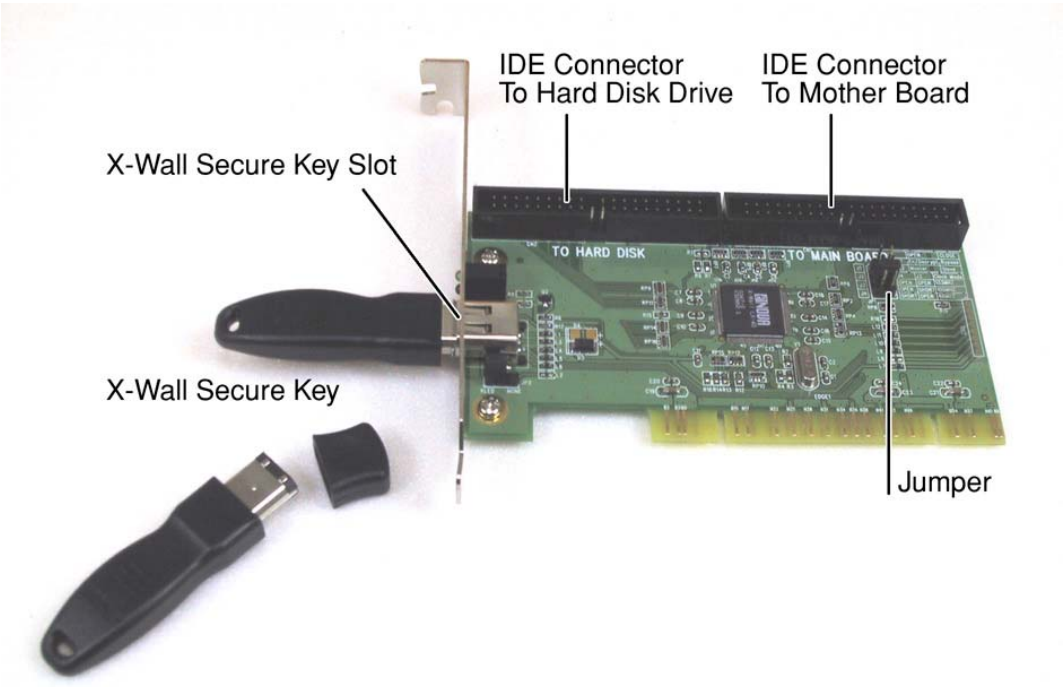


Figure 7. Secure PCI Adapter

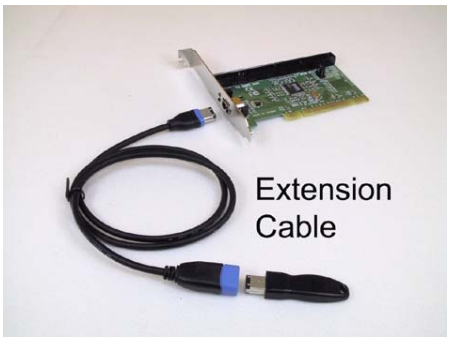


Figure 7.1 Extension Cord for key insert

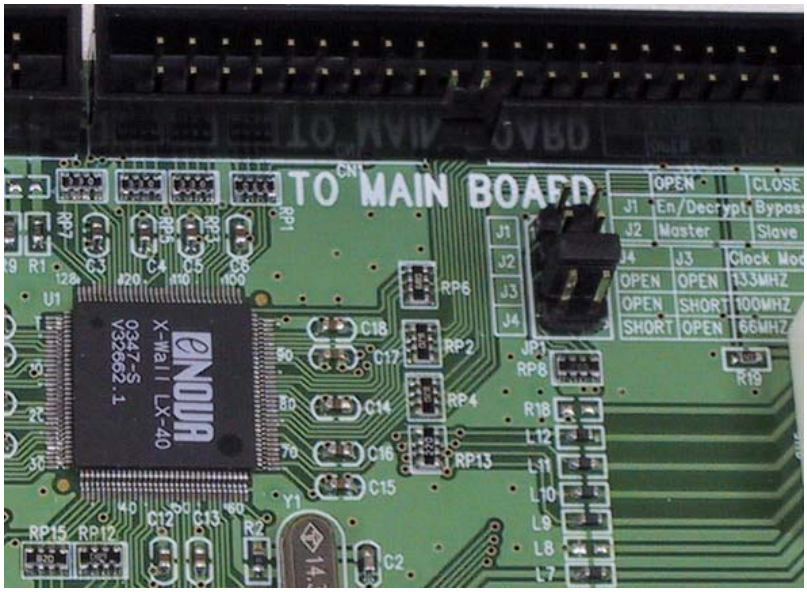


Figure 7.2 Jumper Selections of Master/Slave and various operating frequencies

3.3 Configure Your Secure PCI Adapter

The configuration on the disk drive MUST match with the configuration on the Secure PCI Adapter. The Secure PCI Adapter will NOT function correctly if there is a mismatch on the Master/Slave configuration. As shown in Figure 7.2, the default configuration for the Secure PCI Adapter is set as Master. If you set the disk drive as a Master drive, you don't have to do anything. Otherwise you must set the jumper to Slave on the Secure PCI Adapter and verify the jumper on the disk drive is set to Slave as well. To set the jumper to Slave on the Secure PCI Adapter, place the jumper on J2.

The Secure PCI Adapter is default at operating at 100MHz (Ultra ATA 100MB/sec) on J3. This is the performance setting for all computers. However, just in case you do want to operate your hard disk (need to verify with your disk drive makers 133MB/sec burst mode support) at Ultra ATA 133MB/sec, you may do so via removing jumpers on J3 and J4 for 133MHz extra high speed operation. Please note, however, the 133MHz setting will allow operations on both Ultra ATA 100MB/sec and Ultra ATA 133MB/sec. It does not allow operations on the Ultra ATA 66MB/sec. To operate an old Ultra ATA 66MB/sec drive, you must set the jumpers of J3 & J4 to enable either 100MHz or 66MHz settings. This version of Secure PCI Adapter (with X-Wall LX chips) does not support Ultra ATA 33MB/sec burst mode. To enable an Ultra ATA 33MB/sec hard drive, one must use the X-Wall SE version Secure PCI Adapter. You may contact us for a dealer nearby.

3.4 Installing the Secure PCI Adapter

You MUST configure the hard disk to act as either a Master or a Slave drive. See Section 2.3 for 4 possible options. The Master/Slave configuration on the Hard Disk and the Secure PCI Adapter must match. Otherwise, the Secure PCI Adapter will not function correctly.

1. Back up any critical data prior to the hardware installation.
2. Power down your system and unplug the power cord.
3. Remove your computer cover and an available PCI slot cover plate.
4. Carefully align the Secure PCI adapter to the PCI slot and gently push down the adapter until it is well seated.
5. Secure the adapter with a proper screw.
6. Using the enclosed 80-conductor with three IDE connectors cable, connect the host connector end (see figure 4) to either the Primary IDE or the Secondary IDE channel on the motherboard, connect the device connector end (see figure 4) to the Secure PCI Adapter (Device 0 connector is for a Master drive. Device 1 connector is for a Slave drive.).
7. Connect the disk drive to the "To Hard Disk" IDE Connector on the Secure PCI Adapter using the supplied custom-made 80-conductor two IDE connectors cable as shown in Figure 8. Align the red stripe on the cable to pin one on the connector closest to the power. To reduce potential technical difficulties, avoid using regular 3 IDE connectors cable to connect the disk drive to the Secure PCI Adapter.
8. Place the computer cover and attach the power cord.
9. Insert your *Enova Secure Key* into the Secure Key insert and power up the PC.
10. You must now perform FDISK and Format operations on the disk. These operations will prepare the disk to be used and encrypt both the boot sector and the file allocation table (FAT). Please refer to Appendix C – How to use FDISK and FORMAT. With each *Enova Secure Product*, the FDISK and FORMAT operations must be performed on the disk regardless if the drive is brand new or old.
    Note: The FDISK and FORMAT operations will erase everything on the disk. Please backup the data before starting these operations. **We are not responsible for any lost Data.**

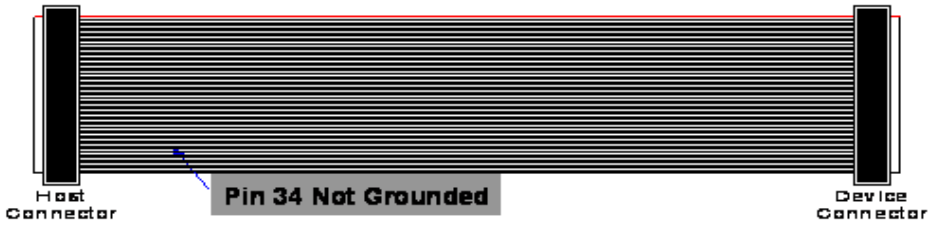


Figure 8. Custom-made 80-conductor two IDE connectors cable (to work with Ultra ATA 66/100. The Pin 34 of the Host connector is NOT grounded)

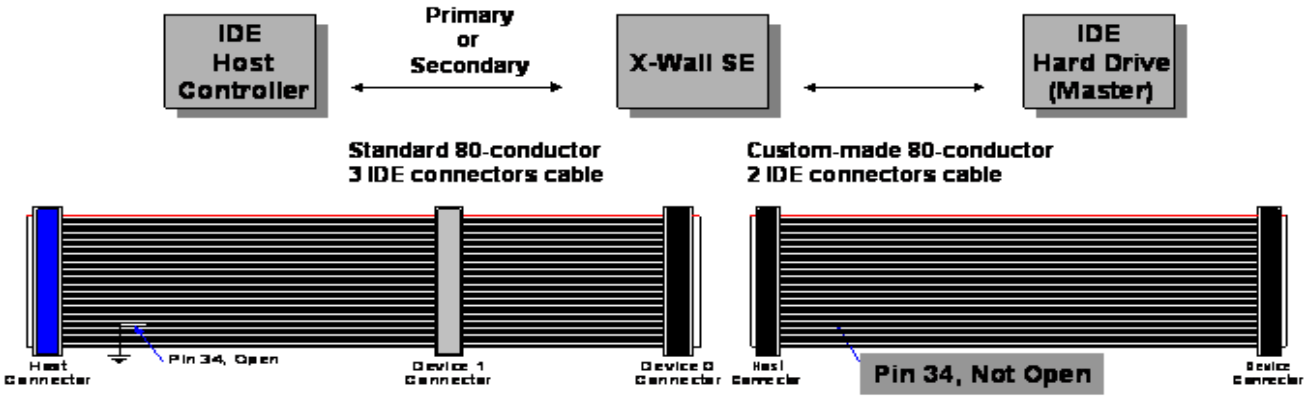
3.5 What Would You See On A Functional Secure PCI Adapter?

There are two (2) LED lights, green & red in the front of the Secure PCI adapter. It displays the current status of unit. The Green LED light indicates proper power is connected to the adapter and should stay lit until the power is turn off. A solid Red LED light reports an **ERROR** in reading the required Secret Key value from the *X-Wall Secure Key*. The disk drive will NOT boot or recognize by the system until the correct *X-Wall Secure Key* is inserted. **Therefore, It is extremely important that you properly insert the correct *X-Wall Secure Key* prior to powering up your computer.** Do **NOT** attempt to connect any 1394 devices to the KEY insert on the drive carrier. It is designed to read the *X-Wall Secure Key* only.

After a successful boot up, you may remove the *X-Wall Secure Key* or wait until the computer is properly shut down. Removing the *X-Wall Secure Key* after the system is booted up will not affect the operation of the computer.

4. CONFIGURE TWO IDE DEVICES WITH THE *X-WALL SE* ON THE SAME CHANNEL (FOR ADVANCED USERS)

4.1 Standard Configuration: One *X-Wall* and One IDE Device

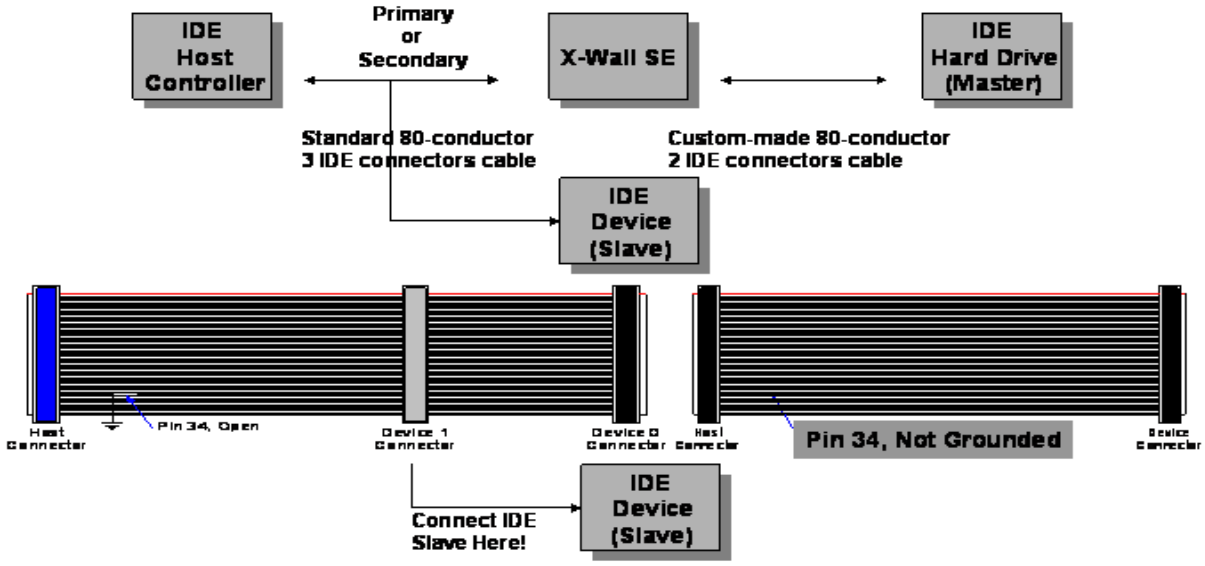


As illustrated above, the product comes with two 80-conductor IDE cables (your Secure Mobile Rack has a built-in cable. Therefore, you will only find one 80-conductor three IDE connectors cable inside the box) to facilitates your installation. Use only the custom-made 80-conductor 2 IDE connectors cable to connect the *X-Wall* to the hard disk drive. And use the standard 80-conductor 3 IDE connectors cable to connect the *X-Wall* to the motherboard.

4.2 Special Configuration: One *X-Wall* and Two IDE Devices

CAUTIONS:

ALWAYS USE THE SUPPLIED CUSTOM-MADE 80-CONDUCTOR 2 IDE CONNECTORS CABLE TO CONNECT THE *X-WALL* AND THE HARD DISK DRIVE. YOU CAN FIND TWO IDE CABLES INSIDE YOUR SECURE PCI ADAPTER PACKAGE. HOWEVER, YOUR SECURE MOBILE RACK HAS A BUILT-IN CUSTOM-MADE 80-CONDUCTOR 2 IDE CONNECTORS CABLE ALREADY. YOU CAN ONLY FIND ONE STANDARD IDE CABLE.



As illustrated above, you can connect two IDE devices to the same IDE channel (be it a Primary or a Secondary IDE) using the *X-Wall* (please note that the *X-Wall* encrypts/decrypts only one single hard disk drive. The IDE device connected before the *X-Wall* will not be encrypted), be sure to connect the other IDE device in front of the *X-Wall* using the standard 80-conductor 3 IDE connectors cable supplied within your package. Set the 2nd IDE device as "Slave" then connect it through the middle connector. This configuration applies to either the Primary or the Secondary IDE channel.

5. TECHNICAL SUPPORT

5.1 Before Contacting Technical Support

1. Make sure you have correctly set "Master" or "Slave" on your disk drive.
2. Make sure your Main Circuit Board correctly reflects the mode setting of your intended disk drive. This setting **MUST** match **EXACTLY** with your disk drive mode selection.
3. Make sure that you have correctly connected Motherboard Primary or Secondary channel using the provided 80-conductor 3 IDE connectors cable**.** The red dotted line of the cable must be aligned to pin 1 of those connectors.
4. Make sure that you have correctly connected the intended disk drive using the provided custom-made 80-conductor 2 IDE connectors cable. The red dotted line of the cable must be aligned to pin 1 or those connectors.
5. Make sure that you have connected the power cable to all the devices.
6. For Secure Mobile Rack, make sure you have turned the lock key clockwise to power the drive.
7. Make sure that you have inserted the *X-Wall Secure Key* properly.

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

5.2 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 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 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

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 – 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]

```
1.  Create DOS Partition or Logical DOS Drive
2.  Set Active Partition
3.  Delete Partition or Logical DOS Drive
4.  Display Partition Information
```

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

```
1. Create Primary DOS Partition
2. Create Extended DOS Partition
3. 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.

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 C – Trouble Shooting

The following procedures provide a general guideline to work with *your X-Wall Secure products* if you experience any problems.

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

Make sure your IDE cables and power connector are securely connected to their intended destinations.

The Green LED light isn't on

Make sure you have connected the power connector correctly. In addition, check on the power lock key to see if it has turned horizontally.

The Red LED light is on

Your X-Wall Secure Products 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 Green LED light stays on until the computer power is turned off. The Yellow LED light blinks whenever there is disk activity; and the Red LED light shall remain off unless condition of X-Wall Secure Key error occurs.

APPENDIX D – Q&A

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

A: *X-Wall LX* is the third generation of *X-Wall* security ASIC (Application Specific Integrated Circuit) that encrypts and decrypts the entire hard drive 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: What's the variety of "*X-Wall LX*"?

A: *X-Wall LX* is available now through four different microchips:
X-Wall LX-40 – DES 40-bit encryption strength
X-*Wall LX-64* – DES 64-bit encryption strength
X-Wall LX-128 – TDES 128-bit encryption strength
X-Wall LX-192 – TDES 192-bit encryption strength

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

A: *X-Wall LX* is specifically engineered for high speed communications with the disk. *X-Wall LX* offers 1.6 Giga bit per second or higher real-time performance to all IDE compatible hard drives. Since *X-Wall LX* hardware chips perform all encryption and decryption tasks, there is no software to cause memory and interrupt overhead. The operation of encryption and decryption is totally transparent to all users.

Q: Entire disk drive? Not just 10 or 20GB as seen on other products?

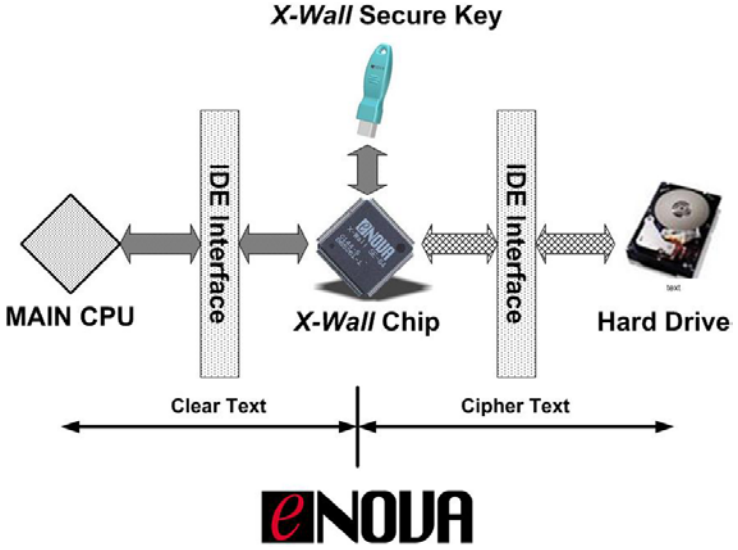
A: *X-Wall* encrypts every thing on your disk drive including operating system. It encrypts the entire volume of your disk drive such that if you have a 180GB hard drive, the entire 180GB will be encrypted.

Q: Do I need to establish a separate "encrypted folder" under file directory as required by some software solutions?

A: No. Every thing you write to the disk drive is automatically strongly encrypted. There is no need to establish a separate "encrypted folder."

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

A: *X-Wall LX* 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. The following illustration best describes how the *X-Wall* functions.



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

A: *X-Wall LX* can be operated with *Ultra ATA (Ultra DMA) 66/100/133* compliant disk drives in *real-time* with throughput of 1.6 Giga bit per second. *X-Wall LX* does not work with SCSI or fiber-channel drives.

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

A: The *X-Wall LX* 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 LX*?

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

intervention. Figure shown below is *X-Wall Secure Key*.

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

A: *X-Wall LX* 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 LX*?

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

Q: Does *X-Wall LX* support 48-bit LBA addressing?

A: Yes. *X-Wall LX* supports 48-bit addressing and can control disk volume over than 137GB per drive.

Q: Can *X-Wall LX* be utilized to protect the RAID system?

A: Yes. *X-Wall LX* can be designed to fit in a RAID 0, 1 and 0+1 system, as long as all disk drives are with standard IDE interface.

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 (128-bit) key. With three keys, the result is an encryption equivalent to using a 168-bit (192-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 software 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 (128-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: Such that *X-Wall LX-40* (DES 40-bit strength) is insecure?

A: Not true. Above explained *Secure Key* finding process is specifically relating to decrypting software-based encryption. The innovative *X-Wall* hardware based encryption solution increases the difficulties tremendously as every guess of the S*ecret Key* requires a hardware reset (power on). To break an *X-Wall LX-40* encrypted hard drive, one must process at least 500 billion times (50% of the available key space) reboot. As such, *X-Wall* even with its DES 40-bit strength will be strong enough against massive computer attacks.

Q: How would I make sure the security offered by *X-Wall LX* is solid?

A: The DES/TDES hardware engine that *X-Wall LX* utilized has been certified by the ***NIST*** *(National Institute of Standards and Technology) and* ***CSE*** *(The Canadian Security Establishment)*, for which the certificates can be reviewed on NIST web links: http://csrc.nist.gov/cryptval/des/desval.html & http://csrc.nist.gov/cryptval/des/tripledesval.html. These hardware algorithms are certified to provide reliable security; at full strength it is nearly impossible to access the encrypted 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.

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

A: No. *X-Wall LX* 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 LX* 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 LX* comprise an effective user authentication for access control and encryption for data protection. The *X-Wall Secure Key* serves as user authentication for access control while *X-Wall LX* encrypts and decrypts.

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

A: **There are no "backdoors" into *X-Wall LX* 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 reseller/distributor or directly from Enova Technology. Please visit our web site ***http://www.enovatech.com*** or write to us **info@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 *Secure Key* for safekeeping after your operating system has fully loaded. Remember that the *Secure Key* MUST be used again the next time you power up your system.

Q: Can I manage my own *X-Wall Secure Key* distribution?

A: Yes, you can do so via licensing the entire Enova Key Management Platform which consists of the following items:

1. Random Number Generator
2. Enova Hawk-II key burner
3. Software that connects Hawk-II to a PC
4. Empty Secure Keys

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

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

Q: What's the likelihood an *X-Wall LX* malfunctions?

A: Every *X-Wall LX* family microchip we ship is 100% tested and proven and complies with International quality assurance standards [11]. However, there may be occasions that chip malfunctions after some period of time. This problem can be resolved by simply replacing the defective *X-Wall LX* 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, for which we do have a good solution on the back up device: Secure USB2.0. Please refer to our website for more details. In case of system failure, please double-check with your disk drive prior to reporting any malfunction of the *X-Wall*.

Q: Can I replace the Secure Key token with Password, Biometrics or Smartcard authentication?

A: Yes, it's possible. This will require system level design effort. You can ask your supplier to work with us to deliver the specific solution you desire to own.

Q: Can I exchange the *X-Wall LX* 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 LX* 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 LX* encrypted files through public network, as every file leaving X-Wall interface is the clear text.

Q: Does *X-Wall LX* 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 LX-40* (DES 40-bit strength). Can I upgrade the same disk drive to an *X-Wall LX-128* (TDES 128-bit strength)?

A: Yes, but with two essential steps:

1. You can order the *X-Wall LX-128 (or any strength other than LX-40)* board from your supplier. The package you will receive will have different *Secure Key*;

[11] 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.

2. You must copy the content of your disk drive to a safe location, and then you can install the new *X-Wall LX-128* board and restore the data to the disk drive, using the new *Secure Keys*. 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.

Filename: User's Manual Rev 1.6.1
Directory: C:\Documents and Settings\Robert Wann\My Documents
Template: C:\Documents and Settings\Robert Wann\Application Data\Microsoft\Templates\Normal.dot
Title: X-Wall User's Guide Ver. 1.2
Subject:
Author: Robert Wann
Keywords:
Comments:
Creation Date: 4/16/2004 2:01 PM
Change Number: 3
Last Saved On: 1/26/2005 1:09 PM
Last Saved By: Robert Wann
Total Editing Time: 799 Minutes
Last Printed On: 1/26/2005 1:10 PM
As of Last Complete Printing
Number of Pages: 30
Number of Words: 9,851 (approx.)
Number of Characters: 56,153 (approx.)