Product name/code	DataPort 25 Secure USB
Interface Types & Speeds	• SATA Passthrough: up to 1.5 GB/s • USB: up to 480 Mbps
Compatibility	2.5" SATA Hard Drives
Data Connectors	• One (1) SATA connector (for use with DataPort 25 frames) • One (1) USB B connector • One (1) mini-USB Security Key connector
Encryption	128-bit AES (Advanced Encryption Standard) or 256-bit AES **128-bit and 256-bit encryption are not cross-compatible**
Connector Insertion Rating	25,000+ Carrier-to-frame
Operating System Requirements	• Windows 7, Vista, or XP • Mac OS X • Linux distributions that support ATA133, SATA, and/or USB
Compliance	EMI Standard: FCC Part 15 Class B, CE EMC Standard: EN55022, EN55024 FIPS: FIPS 140-2, FIPS PUB 197
Shipping Weight	2.00 Pounds (includes accessories)
Product Dimensions	Complete Assembly: 4.02" x 6.10" x 1.02" (102mm x 155mm x 26mm) Removable Carrier: 3.11" x 5.24" x 1.02" (79mm x 133mm x 26mm)
Warranty	We don't expect anything to go wrong with your CRU product. But if it does, Tech Support is standing by and ready to help. Contact us at http://www.cru-dataport.com/support. We also offer phone support at (800) 260-9800.

Product Warranty
CRU-DataPort (CRU) warrants this product to be free of significant defects in material and workmanship for a period of five years from the original date of purchase. CRU's warranty is nontransferable and is limited to the original purchaser.

Limitation of Liability
The warranties set forth in this agreement replace all other warranties. CRU expressly disclaims all other warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose and non-infringement of third-party rights with respect to the documentation and hardware. No CRU dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty. In no event will CRU or its suppliers be liable for any costs of procurement of substitute products or services, lost profits, loss of information or data, computer malfunction, or any other special, indirect, consequential, or incidental damages arising in any way out of the sale of, use of, or inability to use any CRU product or service, even if CRU has been advised of the possibility of such damages. In no case shall CRU's liability exceed the actual money paid for the products at issue. CRU reserves the right to make modifications and additions to this product without notice or taking on additional liability.

FCC Compliance Statement: "This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation."

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 when the equipment is operated in a home or commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

In the event that you experience Radio Frequency Interference, you should take the following steps to resolve the problem:

1) Ensure that the case of your attached drive is grounded.
2) Use a data cable with RFI reducing ferrites on each end.
3) Use a power supply with an RFI reducing ferrite approximately 5 inches from the DC plug.
4) Reorient or relocate the receiving antenna.

FC Tested to comply with FCC standards
FOR HOME OR OFFICE USE

DataPort®25 Secure USB Version Quick Start Guide

Visit http://www.cru-dataport.com/technical-support/product-manuals.php to download a copy of the complete User Manual. Additional product information can be found at http://www.cru-dataport.com.

Models Covered:
DataPort 25 Secure USB with AES 128
DataPort 25 Secure USB with AES 256

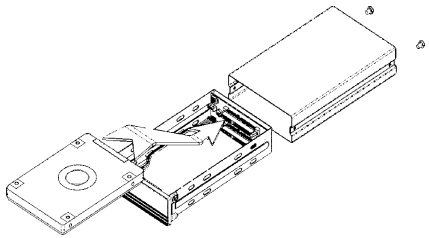
1. Installation Steps

1.1 Receiving Frame Installation

a. Slide the receiving frame into an open 3.5" Floppy Drive bay.
b. Secure the receiving frame to the chassis with the mounting screws provided.
c. Attach a SATA data cable to the JP4 connector on the rear of the frame and attach the other end of the data cable to the appropriate SATA port on the computer's motherboard.
d. Attach a 4-pin Floppy power connector to the rear of the receiving frame.

1.2 Hard Drive Installation

a. If the carrier is bundled with a frame, press the Eject button once to release the button, and again to eject the carrier from the frame.
b. Slide the cover of the carrier back and off.
c. Remove the screw kit from the carrier.
d. Insert a 2.5" SATA hard drive with the top label facing down into the unified power and data connector inside the carrier.
e. Secure the hard drive to the carrier by using the mounting screws provided.
f. Replace the cover and secure it by inserting two screws from the screw kit into the rear of the carrier.



1.3 Operating the DataPort 25 Secure USB Version

1.3.1 Using USB

Insert the Security Key into the mini-USB Security Key port on the front of the carrier.

Bus Power

Take the USB cable out of the box and insert the USB B plug into the front of the carrier and the two USB A plugs into two free USB ports on the computer to bus-power the unit.

AC Adapter

Insert the USB B plug into the front of the carrier and the black USB A plug into a free USB port on the computer. Then plug the AC Adapter into the AC adapter port on the front of the carrier and plug the other end into a power outlet.

Bus-powering the unit or plugging it into a power outlet will cause the unit to power on. When both green LEDs are lit, showing that the drive is ready and encrypted, the Security Key may be removed and stored in a safe location.

1.3.2 Using a DataPort 25 Frame

a. Slide the DataPort 25 Secure USB Version carrier into an open DataPort 25 frame (may be sold separately) installed in the computer.
b. Insert the Security Key into the Mini-USB port on the face of the carrier.
c. Power on the DataPort 25 frame with a DataPort Key by inserting it into the keylock and turning it 90 degrees clockwise.
d. When both green LEDs are lit, showing that the drive is ready and encrypted, the Security Key may be removed and stored in a safe location.

When any hard drive is first used with the DataPort 25 Secure it will show up as a blank, unallocated drive and you'll need to format the drive in the DataPort 25 Secure before you can use it in the enclosure. **Note that formatting a drive will erase <u>all</u> data on the drive, so be sure to back up your data before beginning this operation.** See the "Usage with Mac and Windows Operating Systems" section of the complete User Manual for formatting instructions.

1.4 Safe Carrier Removal from DataPort 25 Frames

a. Turn off the computer or properly dismount the drive from the system. See the "Usage with Mac and Windows Operating Systems" section of the complete User Manual for instructions on how to properly dismount the drive from your computer.
b. Use a DataPort Key to turn the keylock 90 degrees counter-clockwise to unlock and power off the unit.
c. Push the eject button below the keylock once to release the button, and again to eject the carrier.

2. Encryption

- The DataPort 25 Secure USB Version uses full disk hardware encryption to encrypt the entire contents of the drive - including the boot sector, operating system and all files - without performance degradation.

- The encryption key must be installed prior to powering on the DataPort 25 Secure for the data to be decrypted on the drive. If the key is externally connected to the Mini-USB Security

- Key Port and is not internally installed, then once it has been accepted, it may be removed and stored apart from the data so that in the event that the drive is lost or stolen, the data is protected.

- When a drive is formatted using an encryption key, the same or a duplicate key must be used in order to access the data. There is no "back door" to access the data; lost keys make data recovery virtually impossible.