ProStor Systems, Inc.

InfiniVault Server

FIPS 140-2
Non-Proprietary Security Policy

Level 2 Validation

Document Version 1.0

Trademark Notice

ProStor, RDX and InfiniVault are registered trademarks of ProStor Systems, Inc.

Revision History

Version	Modification Date	Modified By	Description of Changes
1.0	6/17/2010	DWalkes	Initial version for public release

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Security Policy for the InfiniVault Server with firmware version 2.4.0 from Secured User, Inc. It provides detailed information relating to each of the FIPS 140-2 security requirements relevant to the InfiniVault Security Policy Server along with instructions on how to run the InfiniVault Server in a secure FIPS 140-2 mode. The user may not modify the InfiniVault Server. Any modifications to the InfiniVault Server by the user will invalidate the module FIPS 140-2 validation.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy.

[1] NIST Security Requirements For Cryptographic Modules, FIPS PUB 140-2, December 3, 2002.

[2] NIST Security Requirements For Cryptographic Modules, Annex A: Approved Security Functions for FIPS PUB 140-2, July 21, 2009.

[3] NIST Security Requirements For Cryptographic Modules, Annex B: Approved Protection Profiles for FIPS PUB 140-2, June 4, 2007.

[4] NIST Security Requirements For Cryptographic Modules, Annex C: Approved Random Number Generators for FIPS PUB 140-2,July 21, 2009.

[5] NIST Security Requirements For Cryptographic Modules, Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2, July 16, 2008.

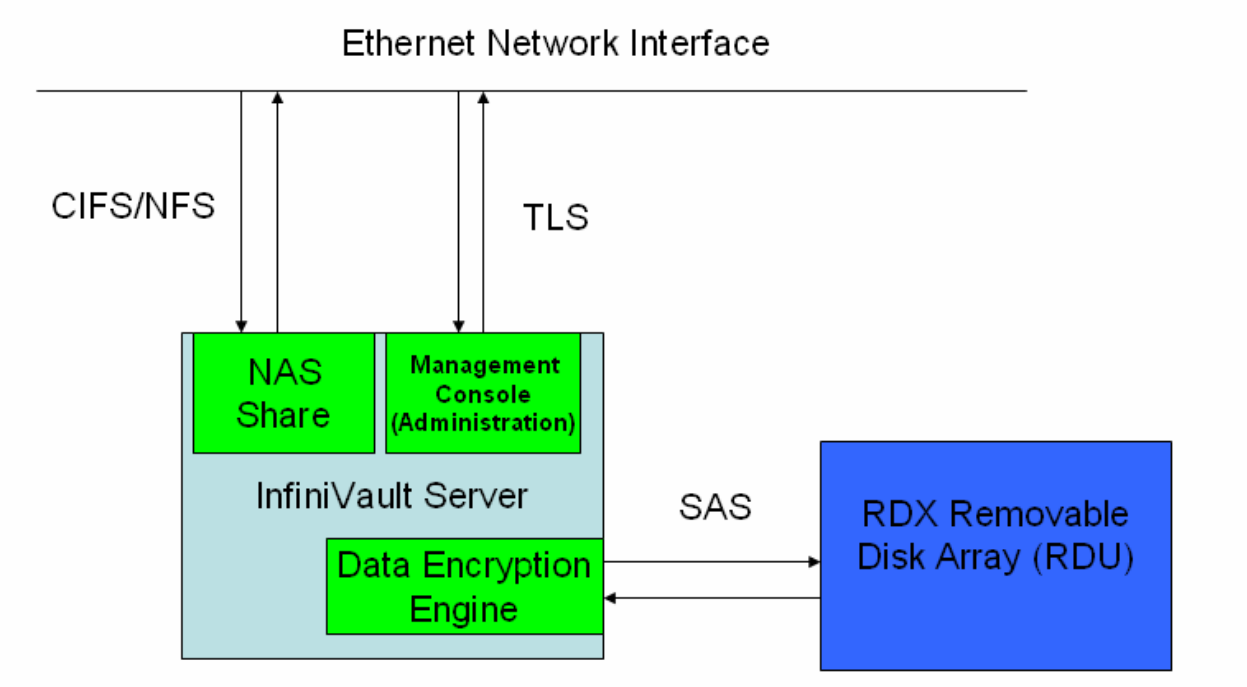
[6] NIST Derived Test Requirements for FIPS 140-2, Draft, March 24, 2004.

1.3 Product Overview

The ProStor InfiniVault System is comprised of two dedicated hardware components, the InfiniVault Server and the RDX Removable Disk Array (RDU.) The InfiniVault Server is a dedicated hardware Network Attached Storage (NAS) device providing secure file encryption/decryption. The RDU performs no cryptographic functionality, its purpose is to store data encrypted by the InfiniVault Server. In addition to file encryption capabilities, the InfiniVault system provides the ability to track file access chain of custody and implement retention policies to meet data preservation requirements.

Figure 1 shows a high level functional view of the InfiniVault system. The Administrator (crypto officer) interfaces with the InfiniVault system via a browser over HTTPS. This browser connection allows access to the InfiniVault Management Console firmware application running on the InfiniVault Server. The crypto officer uses the Management Console interface to configure one or more "Vaults" for operator data access via CIFS/NFS share mechanisms. When the crypto officer creates a "Vault" InfiniVault firmware creates corresponding Common Internet File System (CIFS) or Network File System (NFS) accessible NAS shares on the server. The InfiniVault firmware automatically encrypts (when in FIPS approved mode) and copies the encrypted data to an array of RDX removable disk cartridges (RDU) attached via a Serial Attached SCSI (SAS) interface.

Figure 1 – InfiniVault System Functional Block Diagram



1.4 Cryptographic Module Specification

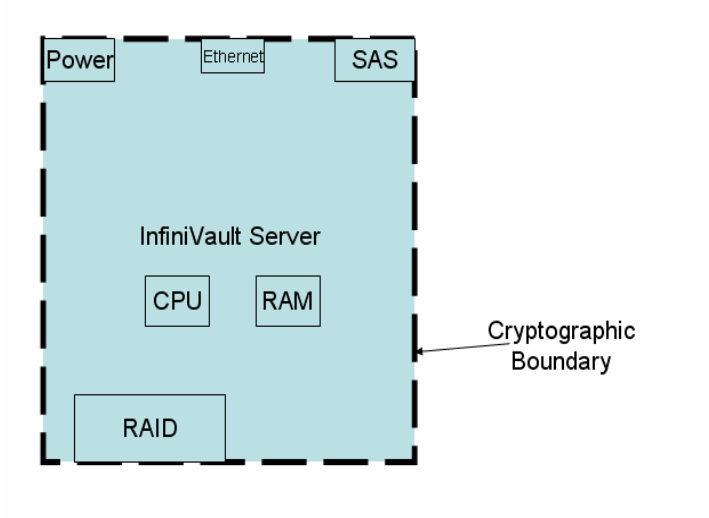
The InfiniVault Server component is the only part of the solution which deals with the encryption of operator data and therefore the only component included in the InfiniVault cryptographic module for the purposes of FIPS-140 validation. The InfiniVault Server boundary contains the entire InfiniVault server component, all associated

hardware, and InfiniVault firmware version 2.4.0. The cryptographic boundary does not include the InfiniVault RDU or the RDX removable disks contained within the RDU.

An InfiniVault User writes files to the NAS share of the InfiniVault Server. When the module is in FIPS mode, these files are encrypted and written to RDX cartridges located in the RDU through an approved security function running in InfiniVault Server firmware. After an encrypted version of the file has been written to cartridge it may be removed from the NAS share through actions of the crypto officer for the purposes of disk space reclamation or file retention considerations. At some later time, a crytpo officer may request a file restore action for a particular file. The InfiniVault Server firmware locates the encrypted file on the RDU, decrypts the file with the approved security function, and places back in its original location on the NAS share.

The InfiniVault Server is a multi-chip standalone cryptographic module consisting of production grade components contained within a production-grade steel enclosure. All removable covers and components are protected from removal by tamper evident security seals (see Section 1.7) in accordance with FIPS 140-2 Level 2. The cryptographic boundary is defined as the metal enclosure for the ProStor InfiniVault Server. All of the module services implemented by module firmware are executed by a general purpose processor on the InfiniVault Server, and the memory devices that contain the external code and data.

Figure 2 – InfiniVault Server Block Diagram



The cryptographic boundary includes an embedded validated module RSAENH (certificate #1012) running on the Windows Storage Server 2003R2 x64 SP2 OS. The cryptographic boundary also includes the Kerberos related functionality of the OS used for operator authentication.

The module has a limited operational environment and does not have a bypass mode or a maintenance mode.

The InfiniVault Security Policy is validated at the following FIPS 140-2 Section levels:

Table 1 - Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2

Section	Section Title	Level
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

1.5 Module Ports and Interfaces

The InifiniVault Server has numerous physical ports and four logical FIPS 140-2 interfaces.

Table 2 lists the physical ports available on the InfiniVault server and associated description of each port.

Table 2 – InfiniVault Server Physical Ports

Physical Port	Description
System Power LED	Indicates green when the InfiniVault server is on.
System Status LED	Indicates InfiniVault server hardware status conditions. • Off – Server is off. • Green - Server is ready. • Amber – Server hardware error condition.
Power Button	Used to turn on or off the InfiniVault server hardware. This button does not directly interact with the cryptographic module.
Network Port 1	Network interface port used for dedicated management or redundancy of network traffic.
Network Port 2	Network interface port used for dedicated management or redundancy of network traffic.
SAS Expander Downstream Ports	Used to connect to InfiniVault RDU(s) containing RDX removable disks.
Power Input 1	This is not a FIPS 140-2 logical interface. Power (110/220 VAC) enters the InfiniVault server via the power input connectors.
Power Input 1 LED	Indicates status of power at power input 1.
Power Input 2	This is not a FIPS 140-2 logical interface. Power (110/220 VAC) enters the InfiniVault server via the power input connectors.
Power Input 2 LED	Indicates status of power at power input 2.

The logical interfaces can be categorized into following logical interfaces defined by FIPS 140-2:

- Data Input Interface

- Data Out Interface
- Control Interface
- Status Output Interface

Data input and output interfaces are used in a bi-directional configuration to convert plaintext to ciphertext and vise-versa. When the operator writes a file to the InfiniVault Server for archival, the InfiniVault Server encrypts the plaintext file and stores on an RDX cartridge contained within the InfiniVault RDU. When the operator requests a file restore action through access of an offline (stub) file on the InfiniVault Server, the module retrieves the ciphertext file from the RDU, decrypts the data file, and places the plaintext data file on the InfiniVault Server.

All logical interfaces to the InfiniVault Server are described in Table 3.

Table 3 - FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	InfiniVault Cryptographic Module Port/Interface	Physical Port/Interface
Data Input	The operator writes plaintext data to the NAS share of the InfiniVault Server through CIFS or NFS network protocols.	The original operator plaintext data was written by the operator through Network interface 1,2 or both depending on port configuration.
	InfiniVault Server firmware reads encrypted (ciphertext) data from the InfiniVault RDU.	The InfiniVault Server firmware uses a SAS connection to access RDX removable disk cartridges.
Data Output	Plaintext data output from the cryptographic module includes plaintext operator data written to its original location on the NAS share after a file “stub” restore.	The operator may access plaintext data files through the exposed CIFS or NFS NAS share.
	Ciphertext data output from the InfiniVault Server includes encrypted operator data written to cartridge.	The InfiniVault Server firmware uses a SAS connection to access RDX removable disk cartridges.
Control Input	InfiniVault Server firmware responds to HTTPS requests through the Management Console for InfiniVault device configuration.	HTTPS configuration access is available to the crypto officer through InfiniVault Server Network port 1, 2 or both depending on network configuration.
	The InfiniVault Server initially powers on when the power button is pressed.	The power button is located on the front panel of the InfiniVault Server in the top right corner.

Status Output	Status pages viewed on the HTTPS Management Console display the status of the InfiniVault Server.	HTTPS configuration access is available to the crypto officer through InfiniVault Server Network port 1, 2 or both depending on network configuration. Module LED's also display status of power or network activity into the module.

1.6 Roles, Services and Authentication

Two FIPS 140-2 approved roles are supported by the module that operators may assume: a Crypto officer (CO) role and a User role. The operator of the module must explicitly assume one of these roles based on their operation. Both of the roles and their responsibilities are described below.

1.6.1 Crypto Officer Role

The crypto officer (CO) role is used to manage the InfiniVault Server. The crypto officer is responsible for creating and configuring operator accounts and NAS accessible storage vaults.

Descriptions of the services available to the crypto officer role are provided in the table below. The Show Status and Create/Modify Operators services are available both prior to the module being set in a FIPS Approved mode and once the model is in FIPS Approved mode. The "Configure Vault" service is a service performed to set the module into FIPS approved mode. All other services are available once the module is initialized for FIPS approved mode of operation.

Table 4 – Mapping of Crypto Officer Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Show Status	Display the current status of the InfiniVault Server	HTTPS InfiniVault Management Console login and browse to system hardware tab.	Current Status	Crypto officer password authentication (Read)
Create/Modify Operators	Create and modify operator (user and crypto-officer) accounts.	Operator account information.	Confirmation of operator account information settings.	Operator Passwords (Write)
Configure Vaults	Configures vault access permissions and settings. Sets module in FIPS mode by configuring all vaults to "enable" encryption.	Vault access details, Encryption set to "Enabled"	Vaults configured and Encryption enabled.	Crypto officer password authentication (Read)
Key Zeroization	Zeroizes all plaintext keys within the crypto boundary	See crypto-officer guidance Section 2.1.2.	Confirmation of Zeroize status.	All (Write)
Self Test	The crypto officer may initiate self-tests by restarting the InfiniVault through the InfiniVault HTTPS Management Console	HTTPS InfiniVault Management Console reboot request	HTTPS Management Console confirmation of InfiniVault successful boot (login screen.)	Crypto officer password authentication (Read)
File Restore Request	The crypto officer may initiate a Restore job using the HTTPS InfiniVault Management console	Name and location of file to be restored selected through HTTPS InfiniVault Management Console "Files" tab.	A decrypted file in the original location on the NAS share.	Crypto officer password authentication (Read)

1.6.2 User Role

The User role accesses the module's cryptographic services that include encryption and decryption of files. Each service is described in detail in the following sections. User services are available once the module is initialized for FIPS approved mode of operation.

The following table lists the services available to the User role.

Table 5 – Mapping of User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
User File Input	The user role creates files on the InfiniVault Server for encryption.	Plaintext files on NAS	Encrypted files on RDX cartridges.	User password authentication (Read)
User File Restore Requests	The user role may request restore of files which have been stubbed on InfiniVault Server.	The name and location of a file to restore on the NAS share	A decrypted file in the original location on the NAS share.	User password authentication (Read)

1.6.3 Authentication

The InfiniVault supports identity based operator authentication for both user and crypto officer operator roles. Authentication data displayed to the operator is obscured with "*" characters during entry.

The InfiniVault is shipped with a default Administrator account with default password. The password should be changed after the first login (see Section 2.1.1.) The Administrator (crypto officer) may create other operator accounts with specified initial passwords. New operator accounts may be specified as Administrator (crypto officer) or standard user accounts.

Selection of a crypto officer role is achieved by requiring identity based authentication for a operator account designated as an Administrator.

A crypto officer can change roles for other operator accounts through the "Edit" feature of the user configuration screen accessed through the Management Console.

The results of all previous operator authentications are cleared when the module is powered off.

1.6.4 Strength of Authentication

Each operator password must contain a minimum of 8 to a maximum of 256 characters in the set of lowercase, uppercase and numeric a-z,A-Z,0-9. This yields a minimum of 218 E+12, over 218 trillion possible combinations; thus, the possibility of correctly guessing a password is less than 1 in 1,000,000 in a single attempt.

The system allows no more than 10,000 login attemps per minute. Given a 218 trillion possibility of guessing a password in a single attempt the possibility of guessing a password in one minute is greater than 20 billion. This means the possibility of randomly guessing a password in 60 seconds is less than 1 in 100,000.

1.7 Physical Security

The cryptographic module is entirely contained within a metal product-grade enclosure (the InfiniVault server enclosure) which includes a removable cover. The enclosure is opaque within the visible spectrum and the cover of

the enclosure is protected with sixteen tamper-evident seals applied by ProStor. All tamper evident seals are opaque within the visible spectrum.

All entry points to the module are protected with tamper evident seals. The operator should periodically inspect tamper evident seals to ensure physical security is maintained. **Figure 3**-6 show the location of the tamper evident seals are on the InfiniVault server.

Figure 3 - Tamper Evident Seal Placement: Front View

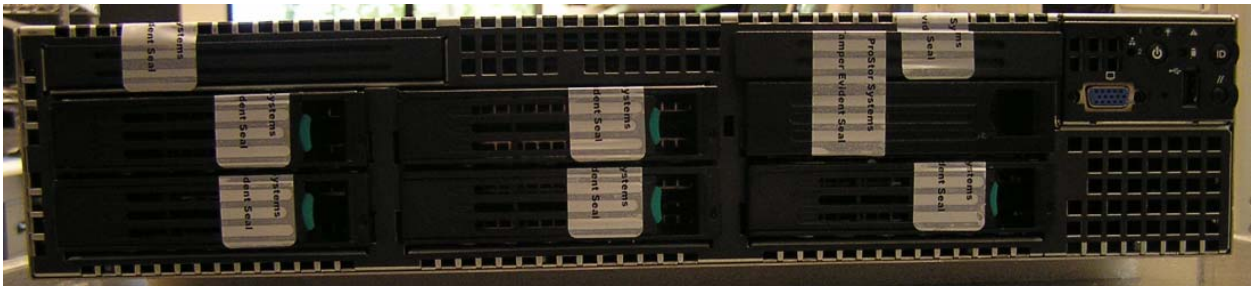


Figure 4 - Tamper Evident Seal Placement: Side View

Figure 5 - Tamper Evident Seal Placement: Back View

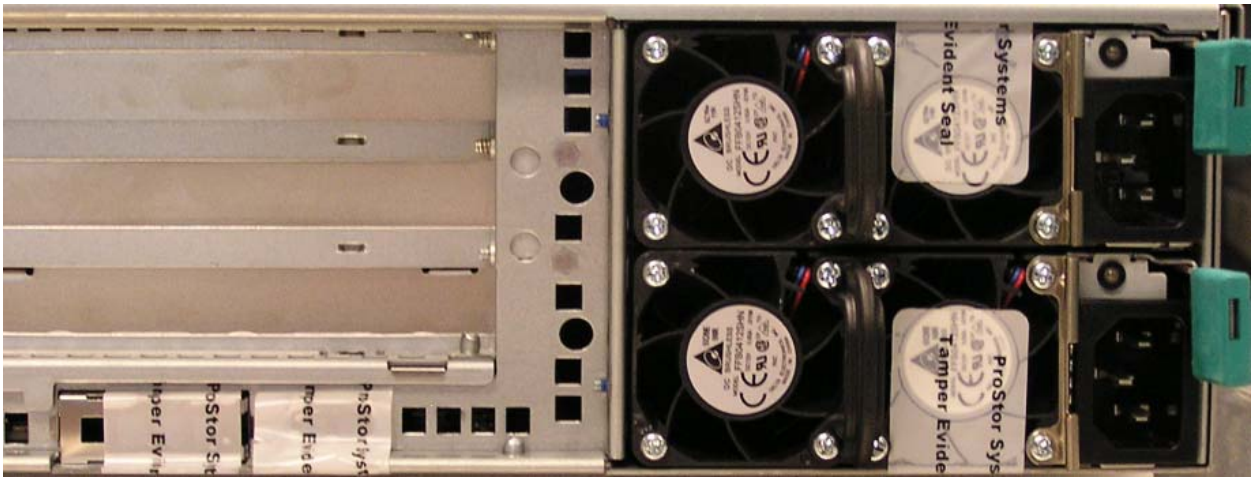
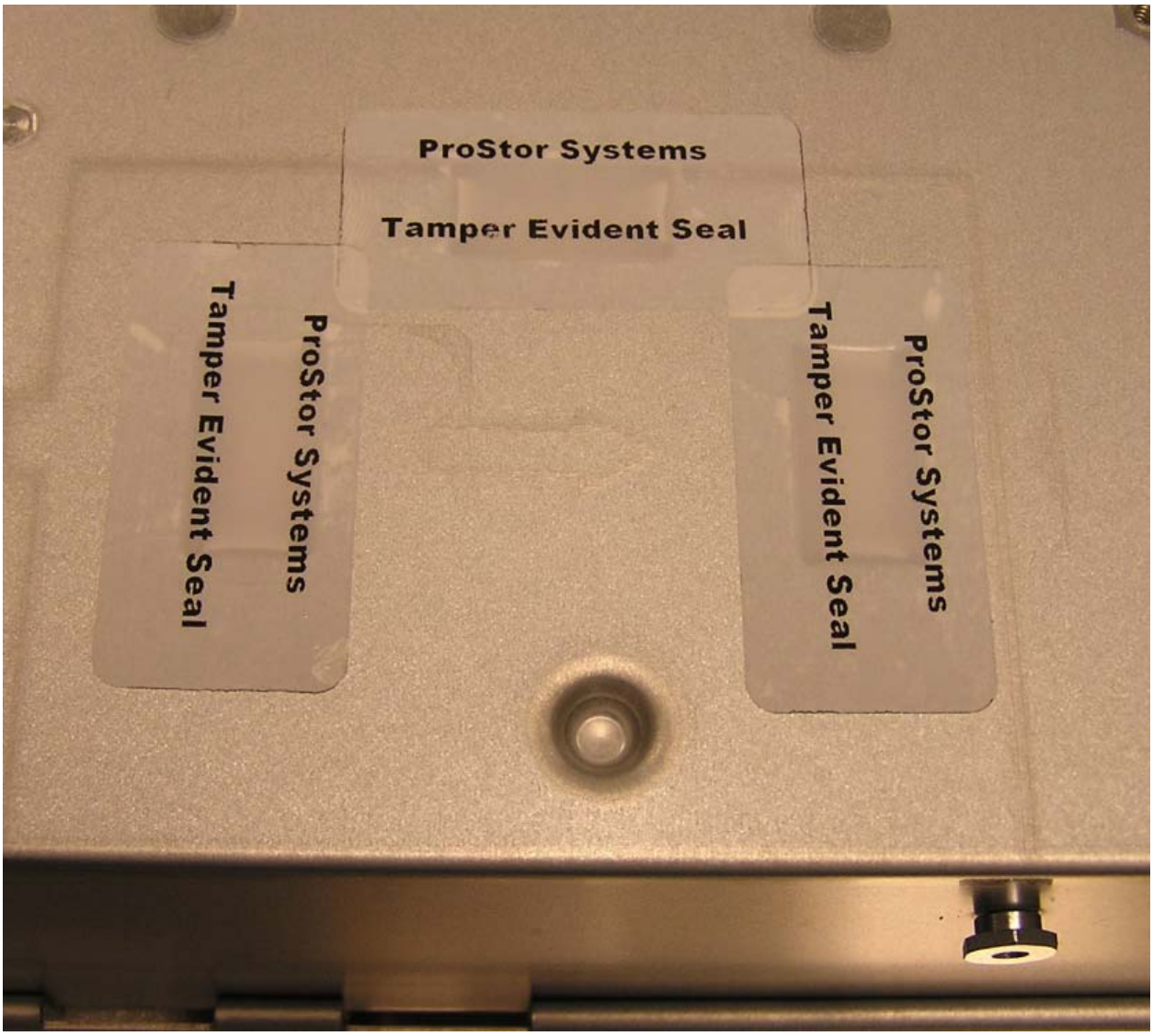


Figure 6 - Tamper Evident Seal Placement: Bottom View



1.8 Cryptographic Key Management

The InfiniVault Security Policy implements the following FIPS-approved algorithms:

- AES 256 (certificate #1214)
- FIPS 186-2 Random Number Generator (Microsoft RSAENH) (certificate #470.) This RNG is used within the included validated module RSAENH (certificate #1012.)

AES 256 is used in CBC mode for encryption and decryption of operator data files. The FIPS 186-2 random number generator is used for file encryption key generation.

In addition, the InfiniVault Security Policy implements the following non-FIPS approved algorithms:

- Blowfish

- Triple DES, (SunJCE)
- SHA-1
- MD5

The Blowfish and Triple DES algorithms are used for purposes not related to FIPS approved security functions. All data encrypted with these algorithms are considered plaintext for the purpose of the FIPS-140 standard. The MD5 algorithm is used for a file hashing function not related to the FIPS approved security function. SHA-1 is used to validate cryptographic module components on startup.

Table 6 lists the cryptographic keys, cryptographic key components and CSP's used by the InfiniVault Server. Each key is listed along with the type of key and additional details describing:

- How the key/CSP is generated or input into the cryptographic module.
- How/whether the key/CSP is output from the cryptographic module.
- Where the key/CSP is stored within the cryptographic module
- How the key/CSP is zeroized.
- How the key/CSP is used.

Keys stored in the internal database are obfuscated with non-FIPS compliant encryption algorithms. These keys are considered to be stored plaintext for the purpose of this standard. The database file is stored in an unencrypted format on an unencrypted logical hard disk drive partition. The logical partition is made up of several physical hard disk drives in a RAID configuration. The Crypto Officer and User accounts do not have access to the plaintext keys due to the limited operational environment configuration of the InfiniVault Server.

Table 6 - List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use/Access
Cipher Keys (1 per file stored)	AES 256	FIPS 186-2 RNG (certificate #470)	No	Obfuscated on Unencrypted Internal Logical Hard Disk Partition	HTTPS Management Console "Zeroize" request.	Encrypts/Decrypts an individual operator file stored on the NAS. No access.
Crypto officer Authentication Data	Password	Operator input through the Ethernet port using HTTPS	No	Obfuscated on Unencrypted Internal Logical Hard Disk Partition	HTTPS Management Console "Zeroize" request.	Crypto officer login to the InfiniVault Management Console. The crypto officer has write access.
RSAENH RNG Seed	FIPS 186 RNG seed	Generated within RSAENH (certification # 470)	No	None (generated as needed in volatile memory.)	Zeroized when InfiniVault is powered off.	Input to the RNG when AES file encryption key is generated. No access.
User Authentication Data	Password	Operator input through the Ethernet port using CIFS NAS share login (Kerberos)	No	Kerberos authentication storage through Windows Storage Server 2003 OS.	Zeroized by overwriting passwords with new values. See crypto-officer guidance Section 2.1.2.	Identity based authentication to NAS datastore (file area.) The crypto officer has write access.

1.8.1 Electromagnetic Interference

The InfiniVault server is tested to conform to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A.

1.9 Self-Tests

The InfiniVault Server performs the following self-tests. This group of self-tests test all critical functions utilized by the module.

- Power-Up Self-Tests:
  - Known Answer Tests (KATs)
    - The AES 256 encryption algorithm is verified through a known-answer test when the module is first powered up.
  - Software/firmware integrity test
    - An EDC is calculated and compared with the known value(s), using a 160-bit error detection code (EDC), SHA hash, to confirm the integrity of the module.
  - Random Number Generator Startup Tests
    - The FIPS 186-2 random number generator provided by RSAENH is tested at power-up (see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1012.pdf)

- Continuous Random Number Generator Test
  - The FIPS 186-2 random number generator provided by RSAENH (certificate #470) completes a continuous random number generator test each time a random number is generated

All power-up tests are initiated on system startup without any input or actions by the operator. Upon successful completion of power-up self tests the login screen of the HTTPS InfiniVault Management Console is displayed. The presence of the login screen provides a means for the crypto officer to verify power-up self tests completed with success. The crypto officer can initiate self-tests by restarting the module through the Management Console.

A failure of self test (either startup or continuous) causes the InfiniVault to enter a “safe mode” whereby no further file processing takes place. In “safe mode” an attempt to access the system through the HTTPS Management Console displays an error message indicating the system was unable to start. The system may be rebooted through the Management Console in this state but no further configuration can take place and no cryptographic operations are performed. When the module is in a safe mode error state the crypto officer may reboot the module to re-attempt self test. If after rebooting the module again goes to a safe mode error state the crypto officer should contact ProStor systems support.

2 Secure Operation

When properly configured the InfiniVault Security Policymeets Level 2 requirements for FIPS 140-2. The sections below describe how to configure and maintain the module in a FIPS-approved mode of operation. Operating the module without following this guidance will cause the module to be in a non FIPS-approved mode of operation.

The FIPS-approved mode of operation for the InfiniVault exists when all vaults are created with encryption enabled and the Management Console is configured for HTTPS operation.

2.1 Crypto officer Guidance

2.1.1 Initial Setup

Connect power to the InfiniVault and RDU. Press the power button on the front of the InfiniVault to power-on the InfiniVault server. Connect a crossover network cable between the InfiniVault server and a client machine. Wait for an HTTP login screen to be displayed on the client machine at IP address http://192.168.117.254.

On the first login, the crypto officer must use the default username and password “Administrator” to connect to the InfiniVault.

During initial configuration, the crypto officer must select HTTPS as the configured mode of operation for the InfiniVault Management Console.

Enabling HTTPS:

1. Click **System**.
2. Click the **Configuration** tab.
3. Click the **HTTPS** tab.
4. Select the Enable Secure HTTP (HTTPS) option.

• The Change HTTP Security window displays confirming that you want to enable secure HTTP.

5. Click **Yes**.

• The system restarts.

Note

After the InfiniVault Restart window displays, wait about ten minutes for the restart to complete.

After configuring HTTPS, the crypto officer must login to the system from the client machine using https://192.168.117.254. The crypto officer must next change the password of the default Administrator (crypto officer) account.

Modifying Operator Password:

1. Click **System**.
2. Click the **Users** tab.
3. Select the operator to modify. The default crypto officer account is “Administrator”
4. Click **Edit**.
5. Do not modify the operator type, click **Next**.
6. If needed, modify the user name to enter a new user name.

   • ProStor recommends using up to 15 characters. Use only printable ASCII characters (letters, numbers, and punctuation), but no spaces.

7. Enter a new password in both password fields.

   • ProStor recommends using up to 15 characters. Use only letters and numbers, but no spaces.8. Click **Modify User**.

The crypto officer may now create vaults for storage purposes. When each vault is created, the crypto officer has the option to enable or disable "Data Encryption"on the vault. Setting the data encryption to disabled is considered a FIPS140-2 non-compliant mode of operation. It is not possible to disable encryption on vaults which were created with encryption turned on. To create a vault with encryption enabled, please follow the instructions below after connecting to the InfiniVault through https://192.168.117.254 and entering the crypto officer username and password.

Creating Encrypted Vaults:

1. Click **Vaults**.
   • The Manage Vaults page displays with a list of the existing vaults and vault folders on the left side.
2. Click **New Vault**.
   • The Vault Name window displays.
3. Enter a name for the vault and click **Next** until the "Data Encryption" setting is displayed.
4. Select "On" for the vault Data Encryption setting.
   • Selecting "Off" for encryption setting is considered a FIPS-140-2 non-compliant mode of operation.
5. Complete the vault configuration menu with appropriate settings for your installation.
6. Review vault settings at the final screen and Select **Finish** to create the vault.

The crypto officer may optionally create additional user accounts following the sequence below.

Creating User Accounts:

1. Click **System**.
2. Click the **Users** tab.
   • The Users tab displays with a list of the existing users.
3. Click **Add**.
   • The Create New User window displays.
4. Select **InfiniVault User** and click **Next**.
   • The Create New User window displays.
5. In the User Name field, enter a user name for the person you want to add.
   • ProStor recommends using up to 15 characters. Use only printable ASCII characters (letters, numbers, and punctuation), but no spaces.
6. Enter a password in both password fields.
   • ProStor recommends using at least eight characters. You can use any character. Passwords are case sensitive.
7. Click **Create User**.

Finally, the crypto officer should use the Configuration page for Network properties to set appropriate IP parameters for the system. The network ports should be connected to appropriate network switches on the corporate network.

The crypto officer may disable user accounts when user accounts are no longer needed or as a step in the zerization procedure.

Disabling User Accounts:

1. Click **System**.
2. Click the **Users** tab.
3. Select the operator to modify.
4. Click **Edit**.
5. Do not modify the user type, click **Next**.
6. Un-check the "Enable" box to disable the user.
7. Click **Modify User**.

2.1.2 Zeroization

To Zeroize the system, first follow instructions in section “Modifying Operator Password” to change the passwords for all operator accounts to new values. Follow instructions in section “Disabling User Accounts” to disable all user accounts.

Next, use the HTTPS Management Console “Zerioze” operation to Zeroize cipher keys and crypto officer authentication data.

3 Acronyms

Table 7 - Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CIFS	Common Internet File System
CPU	Central Processing Unit
DES	Data Encryption Standard
DLL	Dynamic Linked Library
EMC	ElectroMagnetic Compatibility
EMI	ElectroMagnetic Interference
FIPS	Federal Information Processing Standards
HTTPS	Hypertext Transfer Protocol Secure
KAT	Known Answer Test
LED	Light Emitting Diode
NAS	Network Attached Storage
NFS	Network File System
RAID	Redundant Array of Inexpensive Disks
RAM	Random Access Memory
RDU	Removable Disk Unit
RDX	A ProStor removable disk cartridge format specification
RNG	Random Number Generator
RSAENH	Microsoft's RSA Enhanced cryptographic provider.
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SunJCE	Sun Java Cryptography Extension