NetBackup Media Server Encryption Option (MSEO) Driver Security Policy Version 6.1.0

FIPS 140-2 Level 1 Validation

November 4, 2008
Document Version 1.05

---

1 Introduction **3**
1.1 Document History 4
1.2 Acronyms and Abbreviations 4

2 MSEO Driver **5**
2.1 Functional Overview 5
Module Description 5
2.2 Module Ports and Interfaces 7

3 Security Functions **8**

4 FIPS Approved Mode of Operation **8**

5 Identification and Authentication **9**

6 Cryptographic Keys and CSPs **9**

7 Roles and Services **10**

8 Access Control **11**

9 Self Tests **11**

10 Physical Security **12**

11 Mitigation of Attacks **12**

12 References **12**

1 Introduction

This document is the Security Policy for the NetBackup Media Server Encryption Option (MSEO) Driver, Version 6.1.0 cryptographic module. This Security Policy specifies the security rules under which the module shall operate to meet the requirements of FIPS 140-2 Level 1. It describes how the module functions to meet the FIPS requirements, and the actions that operators must take to maintain the security of the module.

This Security Policy describes the features and design of the MSEO driver cryptographic module using the terminology contained in the FIPS 140-2 specification. *FIPS 140-2, Security Requirements for Cryptographic Modules* specifies the security requirements that must be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2 standards. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

The FIPS 140-2 standard, and information on the CMVP program, can be found at csrc.nist.gov/groups/STM/cmvp/index.html. More information describing the MSEO driver can be found at www.Vormetric.com.

In this document, the MSEO driver X.x is also referred to as the “MSEO driver”, “the driver”, the cryptographic module, or “the module”.

This Security Policy contains only non-proprietary information. All other documentation submitted for FIPS 140-2 conformance testing and validation is “Vormetric’ - Proprietary” and is releasable only under appropriate non-disclosure agreements.

The MSEO driver cryptographic module meets the overall requirements applicable to Level 1 security for FIPS140-2.

Table 1. Cryptographic Module Security Requirements

Security Requirements Section	*Level*
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles and Services and Authentication	1
Finite State Machine Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	2
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	1

1.1 Document History

Table 2. Document Version

Version	Date	Comments	Name
1.00	4/20/07	Initial Draft	Ward Rosenberry
1.01	4/28/07	Initial Draft Update	Ward Rosenberry
1.02	7/20/07	Submission Draft	Ward Rosenberry
1.03	6/25/08	Submission Update	Ward Rosenberry
1.04	10/17/08	Final Version	Ward Rosenberry
1.05	11/4/08	Final Version with CMVP comments addressed	Ward Rosenberry

1.2 Acronyms and Abbreviations

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Data Encryption Standard
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FEK	File Encryption Key
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
MIB	Management Information Block
NIST	National Institute of Standards and Technology
PRNG	Pseudo Random Number Generator
PUB	Publication
RAM	Random Access Memory
RFC	Request for Comment
RSA	Rivest Shamir and Adleman Public Key Algorithm
SHA-1	Secure Hash Algorithm
SRDI	Security Related Data Item
X.509	Digital Certificate Standard RFC 2459

2 MSEO Driver

2.1 Functional Overview

The MSEO driver cryptographic module consists of a driver that AES encrypts data being written to a tape drive unit and decrypts AES encrypted data being read from a tape drive unit. The driver is a subsystem contained within a larger controlling system that is outside the evaluation scope of this module.

Features of the software include:

- Strong (AES, 256-bit) data encryption and compression
- FIPS 140-2 power-on self test

Module Description

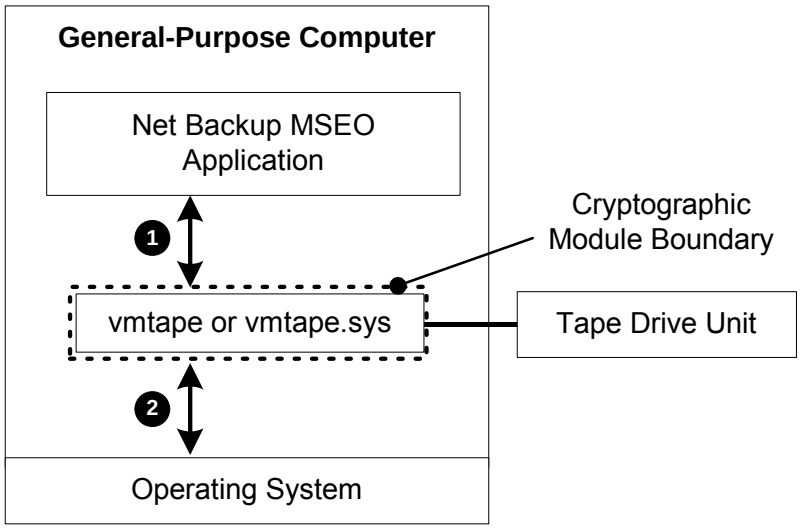
The MSEO driver cryptographic module is a multi-chip standalone cryptographic module consisting of cryptographic driver within application software that executes on a general-purpose computing platform that is configured in single-user mode. Only a single user may access the driver at any point in time. Multiple concurrent operators are not allowed.

The module relies on the computing platform declaration of conformance that it meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements as defined in Subpart B of FCC Part 15, for Class A devices.

The driver has been tested on Windows, Solaris, and Linux systems:

- Red Hat Linux Enterprise 4 with Update 4 on a 64-bit AMD, 1.6 GHz Opteron Processor;
- Solaris 8 with a 64-bit, UltraSparc II, 502MHz Processor;
- Solaris 9 with a 64-bit, UltraSparc II, 550MHz Processor;
- Solaris 10 with a 64-bit, UltraSparc II, 502MHz Processor;
- Windows 2000 Advanced Server SP4, with an Intel Xeon, 2.8GHz Processor;
- Windows 2003 Server Enterprise SP2, 32-bit with an Intel Xeon, 2.8GHz Processor;
- Windows 2003 Server Enterprise SP2, 64-bit with an Itanium 2, 1.4GHz Processor;
- Windows 2003 Server Enterprise SP2, X64 Edition with an Intel Xeon, 2.0GHz Processor.

The module provides data encryption and decryption services, and software integrity services assuring operators of a valid firmware state within the module. The module does not have a bypass or maintenance mode. The following diagram illustrates the module relationship to the MSEO application and the operating system.



1. The module interacts with the MSEO application to startup and receive cryptographic keys.
2. The module interacts with the operating system to use the system services such as reading and writing data to and from the tape device.

2.2 Module Ports and Interfaces

The cryptographic module has four physical interfaces and four FIPS 140-2 logical interfaces. The physical ports have the functions described in Table 3. Where distinct logical interfaces share the same physical port, the system timing, software and hardware protocols, software APIs, and other controls logically separate and isolate these distinct categories of data from one another. The internal system bus acts as the physical path for clocking data into and out of the module. System synchronization and timing controls, and the protocol of the data ensure that logically distinct categories of data do not occupy the data path at the same time.

Table 3. Physical Interfaces and Logical 140-2 Interfaces

Physical Interface	*FIPS 140-2 Logical Interface*
Data input buffers on the I/O Control channel	Data input interface, control input interface
Data output buffers on the I/O Control channel	Data output interface
Control input buffers on the I/O Control channel	Control input interface
Status output buffers on the I/O Control channel	Status output interface
API to load and unload the driver	Power interface

The physical interfaces map to logical interfaces as described in Table 4.

Table 4. FIPS 140-2 Logical Interfaces

Logical Interface	*Description*
Data input	The data input is: • All plaintext data entering the driver for the purpose of being encrypted or passed as plaintext and stored on an external tape drive. • All plaintext or ciphertext data entering the driver from the external tape drive for the purpose of being passed as plaintext or decrypted and output. The internal I/O control channel provides these interfaces.
Data output	The data output is: • All plaintext data exiting the MSEO driver for storage or retrieval. • All ciphertext data exiting the MSEO driver for storage. The internal I/O control channel provides these interfaces.
Control input	The driver accepts control input from the following sources: • Commands embedded within the input data stream originating from the NetBackup server. • The PEM (policy enforcement module) that is external to the driver provides encryption and decryption keys retrieved from the security server. • Tape header data that contains encrypted decryption keys. The internal I/O control channel provides these interfaces.
Status output	The status output consists of all messages either logged by or returned from the module. To view the logged error messages, use the log viewer that is outside the scope of the module. The internal I/O control channel provides this interface.

3 Security Functions

The MSEO driver cryptographic module implements the security functions described in Table 5:

Table 5. Module Security Functions.

Approved Security Function	*Certificate*
Symmetric Key Encryption/Decryption	
AES (FIPS PUB 197) CBC (e/d; 128,192,256)	809
Hashing	
SHS byte-oriented hashing used with HMAC. FIPS PUB 180-2	806
Keyed Hash Message Authentication Code (HMAC)	
HMAC (FIPS Pub 198)	448

The module provides the following cryptographic functions:

- AES symmetric key encryption / decryption of data.
- SHA-1 hashing for use with HMAC for the software integrity test
- HMAC/SHA-1 for the power-on self test software integrity test

4 FIPS Approved Mode of Operation

The module's approved mode of operation is restricted to performing only FIPS-approved cryptographic algorithms and security functions. The module has only a FIPS approved mode of operation that becomes active after the module has powered up and passed the power-on self-test. The approved mode lets the user read and write data from and to a tape drive.

The module must run on one of the platforms described in section 2.1. The system is configured in single-user mode by configuring the OS to provide only a Root (Solaris or Linux) or Administrator (Windows) account. Disable any other administrative, guest, and user accounts during setup of the server.

Keys entered from outside of the cryptographic boundary or output from the cryptographic boundary must do so in encrypted form using FIPS Approved Cryptography.

When the module is installed, confirm the MSEO driver has the correct version number.

On Windows, Solaris, and Linux, enter the command C:\>**cgconfig version**. It will return:

MSEO Agent
Version: 6.1.0

5 Identification and Authentication

The module supports a crypto officer role and a user role. The crypto officer and user may be different people or they may be the same person performing role-specific module operations.

The crypto officer role is implicitly assumed by the operator configuring the module for use. Crypto officer operations consist of running the installation program to install the driver and MSEO application software, running the cgconfig utility to enable or disable the driver (these operations insert or remove the driver in the driver chain), or uninstall the driver.

The user role is implicitly assumed by the operator after the module is installed and is enabled. The user is the NetBackup service providing data to, or receiving data from tape via the module for the purpose of encryption or decryption. Approved mode operations available to the user consist of data encryption and decryption services.

Multiple concurrent operators are not allowed. only a single user may access it at any given point in time. Operators cannot change roles while using the module. Access to the authorized roles is maintained by the operational rules of the module restricted as explained in Table 6.

Table 6. Roles and Required Identification and Authentication.

Role	*Type of Authentication*	*Authentication Data*
Crypto Officer	None	Authentication occurs outside of the module. The module considers all access to module configuration services to be authenticated.
User	None	Authentication occurs outside of the module. The module considers all access to module user services to be authenticated.

The strength of the operator authentication, per the above roles, does not apply to this cryptographic module as it it occurs outside of the module. For the same reason, the need to remove results of previous authentications over a power down cycle do not apply to this module. The module does not require any physical maintenance.

6 Cryptographic Keys and CSPs

The following table identifies the single cryptographic key employed within the module.

Table 7. Cryptographic Keys and CSPs.

Data Item	*Description*
File Encryption Key (FEK)	The FEK is a 256-bit AES key that is automatically generated outside the module and passed into the module in response to a request from the module. The FEK is used for encrypting and decrypting data written to or restored from an external storage device.
HMAC Integrity Key	This key is used for the software integrity test. The HMAC key is hard-coded within the driver.

The module does not input or output keys on its own. It takes in a key as a parameter of the API command to encrypt or decrypt data. All keys may be zeroized by uninstalling the module to destroy the key.

7 Roles and Services

The module supports services that are available to crypto officers and users. All of the services are described in detail in the module's user documentation.

As authentication is handled outside of the module, the crypto officer role is established by the operational rules of the module. The crypto officer may install, uninstall, disable (remove from the driver path) or enable (place in the driver path) the module while the module is not running. The crypto officer may also view version information, run the power-up self test (by starting the MSEO application), and view status information (event logs).

The user role is also established by the operational rules of the module. The user role is available only to the NetBackup system (sending backup and restore commands) via the MSEO application when the module is running.

Table 8 shows the services available to the various roles. Encrypt and decrypt services delete the ephemeral AES key from memory when the operation completes without modifying, disclosing, or substituting the key in any manner.

Table 8. Roles and Services

Service	*Crypto Officer*	*User*
Install the module	●	
Uninstall the module (& zeroization)	●	
Disable the module	●	
Enable the module	●	
Encrypt data being written to storage		●
Decrypt data being read from storage		●
View version information	●	
Run Self-Test	●	

8 Access Control

Table 9 shows services that use or affect cryptographic keys or CSPs. For each service, the key or CSP is indicated along with the type of access.

R - The item is **read** or referenced by the service.
W - The item is **written** or updated by the service.
E - The item is **executed** by the service. (The item is used as part of a cryptographic service.)
D - The item is **deleted** by the service.

Table 9. Access Control

Authentication Data (Key or CSP)	*Role*	*Service*	*Access Control*
File Encryption Key (FEK)	User	Encrypt data being written to storage	R,E,
	User	Decrypt data being written to storage	R,E
HMAC Integrity Key	Crypto Officer	Run the self test	R,E

9 Self Tests

The module performs a power-on self test (POST) to verify the integrity and correct operational functioning of the cryptographic module. The module does not perform any conditional tests. If the system fails a self test, it reports status indicating which failure occurred and transitions to an error state. The module does not contain any user data before or during the POST so it is impossible for the module to output user data in this state or a subsequent error state that halts module operation. The module does output its status in the event of a failed power on self test.

Operators can run the POST on demand by stopping and restarting the containing application. Table 10 summarizes the system self tests.

Table 10. Self Tests.

Self Test	*Description*
Mandatory power-up tests performed at power-up and on demand:	
Cryptographic Algorithm Known Answer Tests	The AES cryptographic algorithm is tested using a “known answer” test to verify the operation of the function. The AES known answer performs both encryption and decryption. The module also performs an HMAC-SHA-1 KAT to verify its correct operation. SHA-1 is also tested as part of the HMAC-SHA-1 known answer test.
Software Integrity Test	The module verifies the integrity of the software by generating an HMAC-SHA-1 data authentication code for the MSEO driver and comparing the code against the expected values stored outside the module in the application binary. SHA-1 is tested as part of the HMAC-SHA-1 software integrity test.

10 Physical Security

As this module is purely a software module, physical security does not apply.

11 Mitigation of Attacks

The cryptographic module is not designed to mitigate specific attacks such as differential power analysis or timing attacks.

12 References

The following National Institute of Standards and Technology publications are available at URL http://www.nist.gov/groups/STM/cmvp:

FIPS PUB 140-2: Security Requirements for Cryptographic Modules.

FIPS 140-2 Annex A: Approved Security Functions.

FIPS 140-2 Annex B: Approved Protection Profiles.

FIPS 140-2 Annex C: Approved Random Number Generators.

FIPS 140-2 Annex D: Approved Key Establishment Techniques.

Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules.

Advanced Encryption Standard (AES), FIPS Publication 197.

Secure Hash Standard (SHS), FIPS Publication 180-2.

***Keyed-Hash Message Authentication Code (HMAC),* FIPS Publication 198.**