SafeNet ProtectDrive Cryptographic Engine

FIPS 140-2 Level 2 Non-Proprietary Security Policy

DOCUMENT NUMBER:	002-010784-001
AUTHOR:	Chris Brych
DEPARTMENT:	Enterprise Engineering
LOCATION OF ISSUE:	Ottawa and Belcamp
DATE ORIGINATED:	May 24, 2012
REVISION LEVEL:	E
REVISION DATE:	September 5, 2013
SUPERSESSION DATA:	D
SECURITY LEVEL:	Non-Proprietary

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the SafeNet ProtectDrive Cryptographic Engine 1.0.1 as implemented in the SafeNet ProtectDrive application version 9.4.2.

This security policy describes how the module meets the security requirements of FIPS 140-2 and how to operate the Application in a secure FIPS 140-2 mode. This policy was prepared as a part of the Level 2 FIPS 140-2 validation of the Application.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval.

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. More information is available on the Application and other SafeNet products from the following sources:

- The SafeNet Internet site contains information on the full line of security products at http://www.safenet-inc.com/products.
- For answers to technical or sales-related questions please refer to the contacts listed on the SafeNet Internet site at http://www.safenet-inc.com/company/contact.asp.

SafeNet Contact Information:	
SafeNet, Inc. (Corporate Headquarters)	4690 Millennium Drive Belcamp, MD 21017 **Telephone:** 410-931-7500 **TTY Users:** 800-735-2258 **Fax:** 410-931-7524
SafeNet Sales:	
U.S.	(800) 533-3958
International	(410) 931-7500
SafeNet Technical Support:	
U.S.	(800) 545-6608
International	(410) 931-7520
SafeNet Customer Service:	
U.S.	(866) 251-4269
EMEA	+44 (0) 1276 60 80 00
APAC	852 3157 7111

1.3 Terminology

In this document, reference will be made to the “module” or “SPCE” when discussing SafeNet ProtectDrive Cryptographic Engine.

2. THE APPLICATION

2.1 Functional Overview

ProtectDrive is a full-disk encryption software product that secures entire hard drives in laptops, workstations, servers and removable media.

- **Strong security**

  ProtectDrive encrypts and decrypts data “on the fly” using FIPS Approved strong encryption algorithms. Security is further enhanced with password based pre-boot authentication or for more security sensitive organizations, by using multi-factor authentication products such as tokens and smart cards as part of the pre-boot authentication process[1].

- **Removable media protection**

  ProtectDrive protects a wide range of removable media, including USB memory sticks and portable hard drives. Once a medium is protected, only authorized users within an organization can access the sensitive data stored on it.

- **Port management and control**

  ProtectDrive lets administrators define port management and control policies for optical media plus serial connections.

- **Local management**

  ProtectDrive permits local administration of policies and keys.

ProtectDrive security features include:

- Unauthorized sign-on protection activation after a configurable number of failed pre-boot sign-on attempts;
- Controlled access to device classes such as storage devices, printers, modems, digital cameras and scanners etc.

ProtectDrive may be deployed to multiple clients using a Windows Installer (MSI) package over a network or individual clients by personal installation.

2.2 Cryptographic Engines

The SafeNet ProtectDrive Cryptographic Engine (SPCE) is comprised of 5 components:

- VxBIOS
- NetBSD INIT
- CRYPdll
- SafeCGX.sys system driver for 32-bit Windows environments
- CryptoAPI_NT.dll

[1] Note: Cryptographic tokens and smart cards were not tested as part of the pre-boot authentication process.

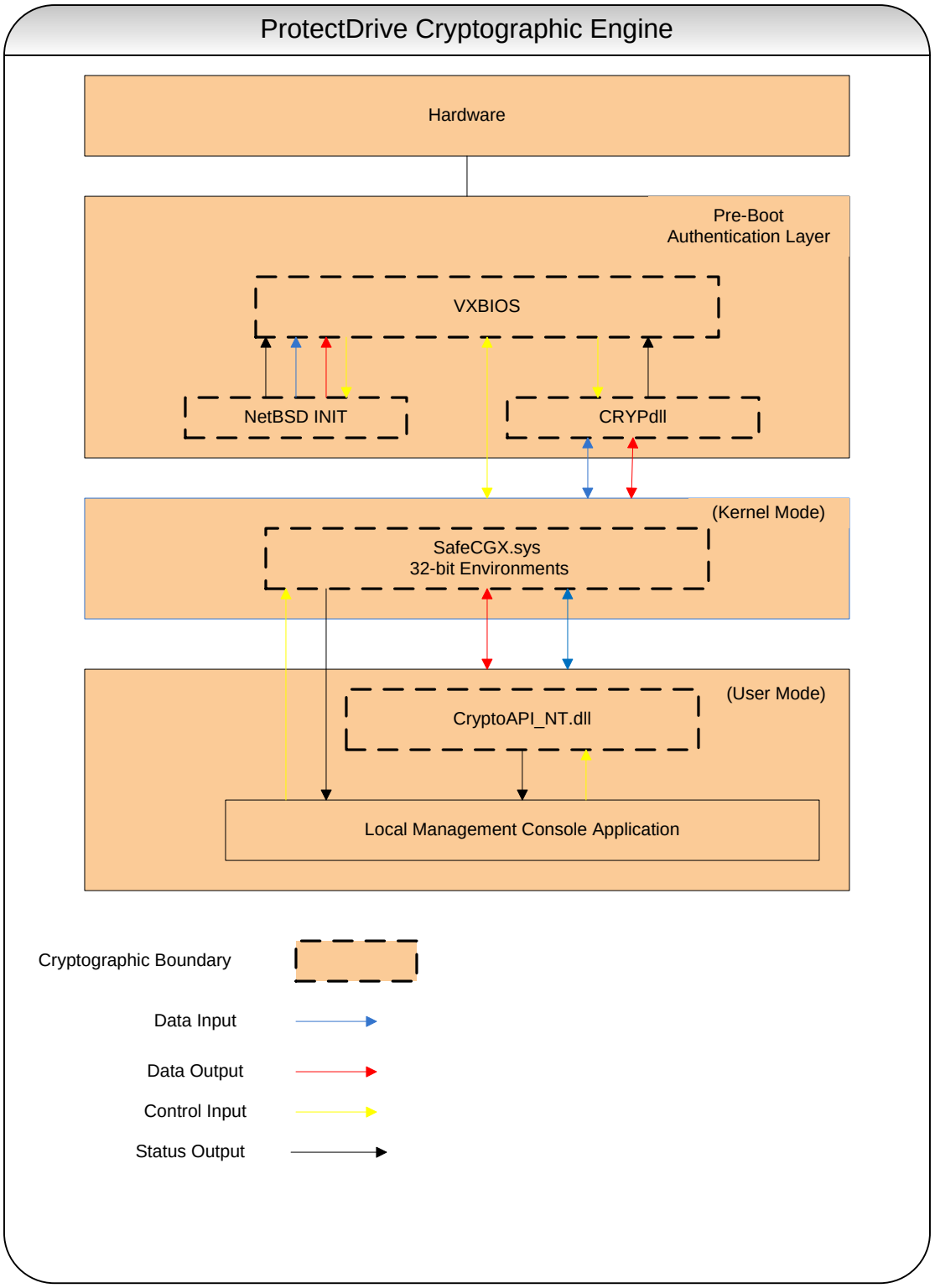

Figure 1. – Boot Environments and Cryptographic Engines

As seen in Figure 1, the NetBSD INIT components handle operator authentication at system

startup. CRYPdll.sys handles initial decryption of the operating system kernel once successful authentication of an operator has taken place. Transfer of decryption operations then occurs when SafeCGX is decrypted and initialized. SafeCGX takes over and decrypts the remainder of the kernel, operating system, and hard disk. The role of CryptoAPI_NT.dll is only to generate keys in FIPS Approved mode of operation.

3. CRYPTOGRAPHIC MODULE SPECIFICATION

From the point of view of FIPS 140-2, the SafeNet ProtectDrive Cryptographic Engine (SPCE) 1.0.1 is a multi-chip standalone cryptographic module whose cryptographic boundary is composed of a logical and a physical boundary. The logical boundary comprises the cryptographic implementation files and the physical boundary includes the hardware platform the module resides on.

This document refers specifically to the SafeNet ProtectDrive Cryptographic Engine version 1.0.1.

3.1 FIPS 140-2 Security Levels

The Module meets all Level 2 requirements for FIPS 140-2 as summarized in Table 1. No components are excluded from the requirements of FIPS 140-2.

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 Machine	2
5	Physical Security	N/A
6	Operational Environment	2
7	Cryptographic Key Management	2
8	EMI / EMC	3
9	Self Tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

Table 1 – FIPS 140-2 Security Levels

4. CRYPTOGRAPHIC MODULE PORTS AND INTERFACES

The cryptographic module provides several interfaces for data input, data output, status output, and command input.

4.1 Interfaces

All requests for services are sent to the ProtectDrive Cryptographic Engine via an API.

The module's physical interfaces are separated into the logical interfaces, defined by FIPS 140-2, and described below:

FIPS 140-2 Interface	Logical Interface	Physical Interface
Data Input Interface	Data input parameters of API function calls	keyboard port, mouse port, USB port, serial port
Data Output Interface	Data output parameters of API function calls	VGA port, USB port, serial port
Control Input Interface	Control input parameters of API function calls that command the module	keyboard port, mouse port
Status Output Interface	Status output parameters of API function calls that show the status of the module	VGA port
Power Interface		Power connector

Table 2. – FIPS 140-2 Logical Interfaces

5. ROLES, SERVICES AND AUTHENTICATION

5.1 Identification and Authentication

SPCE supports identity-based authentication of one operator at a time. Operators are identified by a username, password, and domain name.

The different roles and required authentication are shown in Table 3.3:

Role	Type of Authentication	Authentication Data
User	Identity-based	Username, Password, and Domain Name
Cryptographic Officer	Identity-based	Username, password, and Domain Name

Table 3. – Roles and Required Identification and Authentication

The module supports two distinct operator roles: User and Cryptographic Officer/Administrator. The ProtectDrive Cryptographic Engine enforces the separation of roles using identity-based operator authentication. To log in, an operator must enter a username, domain name, and password. The username is an alphanumeric string of one or more characters. The password is a string of one or more characters (eight or more are recommended) chosen by the operator from the 95 printable and human-readable characters. Upon successful authentication, the role is assumed based on the identity of the operator as a Windows Domain credential.

5.2 Strength of Authentication

Authentication Mechanism	Strength of Mechanism
Operator password	The characters used in the password must be from the 95 printable and human-readable ASCII characters. - With an 8 character password, this yields a minimum of 95^8 (or 6,634,204,312,890,625) possible combinations; thus the possibility of correctly guessing a password is greater than 1 in 1,000,000. - By default, the module locks the login interface for 3 minutes after 3 consecutive failed login attempts, giving a possibility well under less than 1 to 100,000 to guess the password within 1 minute.

Table 4. – Strength of Authentication Mechanism

5.3 Roles

5.3.1 Administrator / Cryptographic Officer

This role is associated with Administrators / Cryptographic Officers (COs) who can administer the module and ProtectDrive locally using the Local Management Console (LMC) application.

This role provides all services that are necessary for the secure management of the module.

5.3.2 User

This role is associated with the User who logs into a system protected by ProtectDrive, with minimal access to module services as set by a Crypto-Officer. This role can access the LMC to view its settings, but cannot make changes.

5.4 Services for Authorized Roles and Access Control

Table 5 shows the 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.

X - The item is **executed** by the service. (The item is used as part of a cryptographic function.)

Crypto-Officer: CO

User: U

Services	Role	Key/CSP	Access Control
Pre-Boot			
Authenticate	CO, U	Password	W, X
Self-Test	CO, U	None	X
Decrypt	CO, U	UK, DK, VK	X

Services	Role	Key/CSP	Access Control
Post-Boot			
Self-Test	CO, U	None	X
Generate Key	CO	DK, VK	X
Show Status	CO, U	None	R
Change Password	CO, U	Authentication Data	W, X
Change LMC Settings	CO	Authentication Data	R, W, X
Encrypt	CO, U	DK, VK	X
Zeroize	CO, U	All Keys and CSP's	W, X
Set FIPS Mode	CO	None	W, X

Table 5. – SPCE Services and Authorized Roles

None of the above services can be accessed until an operator successfully authenticates into one of the specified roles.

6. PHYSICAL ENVIRONMENT

The SafeNet ProtectDrive Cryptographic Engine is implemented as a software component and thus the FIPS 140-2 physical security requirements are not applicable.

7. OPERATIONAL ENVIRONMENT

For the purpose of FIPS 140-2 Level 2 validation, the SafeNet ProtectDrive Cryptographic Engine is classified as a multi-chip standalone module as defined by FIPS PUB 140-2. The module has been tested on a Dell Optiplex GX620 3.0 GHz Intel Pentium D Processor 830 (1 CPU), running 32-bit Windows XP version 5.1 SP2 and a specified list of security updates as specified in the CC EAL4+ Validation Report for the named OS at http://www.niap-ccevs.org/st/st_vid10151-vr.pdf

8. CRYPTOGRAPHIC KEY MANAGEMENT

8.1 Key Generation

The module supports the generation of AES 128-bit, 192-bit and 256-bit keys. The module employs a ANSI X9.31 Appendix 2.4 specified PRNG for generating keys used in FIPS Approved mode of operation.

8.2 Key Input / Output

Keys are not input or output from the cryptographic boundary.

8.3 Key Zeroization

Keys are zeroized by uninstalling the ProtectDrive application and performing a low level format of the hard disk drive.

8.4 Algorithms

Tables 6 to 10 list the modules approved algorithms. In the FIPS mode of operation only these Approved algorithms are available.

The module implements the following FIPS Approved or Allowed algorithms for VxBIOS:

Approved or Allowed Security Functions	*Certificate*
Secure Hash Standard (SHS)	
SHA-256 (Byte Only)	1754
Data Authentication Code	
HMAC-SHA-256 (Key Size KS = BS)	1210
Password Based Key Derivation Function	
NIST SP 800-132 Section 5.4(2.a) (Vendor Affirmed[2])	

Table 6. - VxBIOS FIPS Approved or Allowed Algorithms

The module implements the following FIPS Approved or Allowed algorithms for NetBSD INIT:

Approved or Allowed Security Functions	*Certificate*
Symmetric Encryption/Decryption	
AES: (CBC, Mode; Encrypt/Decrypt; Key Size = 256)	1999
Secure Hash Standard (SHS)	
SHA-1 (Byte Only)	1752

Table 7. - NetBSD INIT FIPS Approved or Allowed Algorithms

The module implements the following FIPS Approved or Allowed algorithms for CRYPdll:

Approved or Allowed Security Functions	*Certificate*
Symmetric Encryption/Decryption	
AES: (CBC Modes; Encrypt/Decrypt; Key Sizes = 128; 192; 256)	1998

Table 8. - CRYPdll FIPS Approved or Allowed Algorithms

The module implements the following FIPS Approved or Allowed algorithms for SafeCGX:

Approved or Allowed Security Functions	*Certificate*
Symmetric Encryption/Decryption	
AES: (CBC Mode; Encrypt/Decrypt; Key Sizes = 128, 192, 256)	2000
Secure Hash Standard (SHS)	
SHA-1 (Byte Only)	1753
Data Authentication Code	

[2] Passwords sent to the PBKDF2 function shall be at minimum 8 characters. The probability of guessing the password at random is shown in Table 4.

Approved or Allowed Security Functions	*Certificate*
HMAC-SHA-1 (Key Size KS < BS)	1209
Non Approved Security Functions	
RSA (Non-Compliant)	

Table 9. - CGX FIPS Approved or Allowed Algorithms

The module implements the following FIPS Approved or Allowed algorithms for CryptoAPI_NT.dll:

Approved or Allowed Security Functions	*Certificate*
Secure Hash Standard	
SHA-256	1751
Data Authentication Code	
HMAC-SHA-256 (Key Size KS = BS)	1208
Random Number Generation	
ANSI X9.31 Appendix A, para 2.4 [AES-256]	1048
Non-Approved Security Functions	
DES	
Triple-DES (2-Key)	
IDEA	

Table 10. – CryptoAPI_NT.dll FIPS Approved or Allowed Algorithms

8.5 Security Functions, Cryptographic Keys and CSPs

Table 11 lists the security functions by indicating each CSP, the type of key it is, and how it is used.

CSP	CSP Type	Generation	Input/Output	Storage	Destruction Mechanism	Use
Volume Key (VK)	AES key 128/192/256-bit	ANSI X9.31 RNG	Not Input/Output	Plaintext in Embedded File System	Format HDD	Encryption/Decryption of Data Volume
Authentication Data	Data String	Derived	Not Input/Output	Plaintext in Volatile Memory for duration of login and Plaintext in Non-Volatile Memory in Embedded File System	Power Cycle and Format of HDD	Authentication
User Key (UK)	AES key 256-bit	NIST SP 800-132 (PBKDF2)[3]	Not Input/Output	Volatile Memory	Power Cycling	Wrap Disk Key stored in Embedded File System
Disk Key (DK)	AES key 256-bit	ANSI X9.31 RNG	Not Input/Output	Encrypted by User Key (UK) in Embedded File System	Format HDD	Encryption/Decryption operations on system partitions.
Seed	Seed Input	Generated from entropy source	Not Input/Output	Volatile Memory	Power Cycling	Input into generating random numbers
RNG Seed Key	AES key 256-bit	Generated from entropy source	Not Input/Output	Volatile Memory	Power Cycling	Used in generating random numbers

Table 11. – Approved Security Functions, Cryptographic Keys and CSPs

[3] Keys derived from passwords, as shown in SP 800-132, shall only be used in storage applications.

9. SELF-TESTS

The ProtectDrive Cryptographic Engine performs a number of power-up and conditional self-test to ensure proper operation.

9.1 Power-On Self-Tests (POST)

When the SafeNet ProtectDrive Cryptographic Engine is initially powered-on, it executes a number of power-on self-tests. If any of these tests fail, the module will enter an error state and prohibit an operator from exercising the module's cryptographic functionality. No data is output by the module while these tests are running. Table 12 lists the power-on self-tests:

Test	Function	FIPS 140-2 Required
Symmetric Cipher AES KAT	Performs encrypt/decrypt known answer tests for AES for NetBSD INIT,CRYPdll, and SafeCGX[4]	Yes
SHA-1 KAT	Performs known answer test for SHA-1 on NetBSD INIT	Yes
RNG KAT	Performs known answer test for the RNG in CryptoAPI_NT.dll	Yes
HMAC-SHA-1	Peforms separate known answer test for HMAC-SHA-1 on SafeCGX.	Yes
HMAC-SHA-256 KAT	Performs known answer tests for HMAC-SHA-256 on VxBIOS and CryptoAPI_NT.dll	Yes
Software Integrity Test	HMAC-SHA-256 for VxBIOS, NetBSD INIT, and CRYPdll HMAC-SHA-256 for CryptoAPI_NT.dll HMAC-SHA-1 for SafeCGX[5]	Yes

Table 12. – Power-On Self-Tests

9.2 Conditional Self-Tests

Test	Function	FIPS 140-2 Required
Continuous RNG	Performs the continuous RNG check each time the module's PRNG is used to produce random data to verify that the previously generated output from the RNG is not the same as the currently generated value.	Yes
Continuous Entropy Test	Performs a continuous entropy test on the seeding material for the RNG. The test checks that the previous seeding material is not the same as the current seed material	Yes

Table 13. – Conditional Self-Tests

[4] AES KATs are performed separately by CRYPdll, NetBSD INIT, and SafeCGX for their respective AES implementations.
[5] SafeCGX performs its own software integrity test separately from SPCE components.

9.3 Mitigation of Other Attacks

The FIPS 140-2 Mitigation of Other Attacks requirements are not applicable because the module is not designed to mitigate any specific attacks.

10. FIPS APPROVED MODE OF OPERATION

10.1 Description

The module can be configured to operate in a FIPS Approved mode of operation by setting the Encryption Mode to Enable FIPS. Enabling FIPS Mode will disable all Non-FIPS Approved symmetric algorithms.

10.2 Invoking Approved Mode of Operation

The FIPS Approved Mode of Operation can be invoked by performing the following steps:

1. The Crypto-Officer (Windows Administrator) must first authenticate to the workstation. The Crypto-Officer must then install the SafeNet ProtectDrive Application and set a Crypto-Officer password for ProtectDrive by changing the local System Administrator Windows account's password.
2. The workstation must then be restarted
3. The Crypto-Officer must then reauthenticate
4. The Crypto-Officer will launch the Local Management Console and select the PD Users tab to create a User account
5. The Crypto-Officer will next select the Advanced Tab\Encryption Directory\Encryption Mode
6. In the "Encryption Mode", the Crypto-Officer will then select "Enable FIPS" check box
7. The Crypto-Officer must next select the "Fixed Disk" directory and select an AES key size.
8. The Crypto-Officer must then select the Status Tab and Encrypt the Disk.
9. Upon completion of encrypting the disk, the system must be restarted
10. After the User or Administrator successfully authenticates, they can go to the Advanced Tab\Encryption Directory\Encryption Mode to see that "FIPS Mode is enabled" and verify that the disk/volume is encrypted.

10.3 Mode of Operation Indicator

The module is in FIPS mode when the 'Enable FIPS' Encryption Mode setting in the LMC under the Encryption section of the Advanced Settings tab is set and the Fixed Disk Status Tab shows an encrypted partition.

10.4 Non-FIPS mode of Operation

In non-FIPS mode, the module also provides the following non-FIPS Approved algorithms:

- DES
- 2-key Triple-DES
- IDEA
- RSA

11. GLOSSARY OF ACRONYMS, TERMS AND ABBREVIATIONS

Term	Definition
AES	Advanced Encryption Standard
CO	Cryptographic Officer
CRC	Cyclic Redundancy Check
EFS	Embedded File System
DK	Disk Key
IDEA	International Data Encryption Algorithm
LMC	Local Management Console
PBKDF2	Password Based Key Derivation Function
POST	Power On Self Test
RNG	Random Number Generator
Triple DES (EDE)	Data Encryption Standard (Encrypt Decrypt Encrypt)
UK	User Key
VK	Volume Key