ProtectV StartGuard

FIPS 140-2 Level 1
Non-Proprietary Security Policy

DOCUMENT NUMBER:	002-010841-001
AUTHOR:	SafeNet Certification Team
DEPARTMENT:	R & D Program Managaement
LOCATION OF ISSUE:	Redwood City and Belcamp
DATE ORIGINATED:	June 14, 2013
REVISION LEVEL:	D
REVISION DATE:	April 14, 2014
SUPERSESSION DATA:	C
SECURITY LEVEL:	Level 1

© Copyright 2014 SafeNet, Inc.
All rights reserved
This document may be freely reproduced and distributed whole and intact including this copyright notice.

SafeNet, Inc. reserves the right to make changes in the product or its specifications mentioned in this publication without notice. Accordingly, the reader is cautioned to verify that information in this publication is current before placing orders. The information furnished by SafeNet, Inc. in this document is believed to be accurate and reliable. However, no responsibility is assumed by SafeNet, Inc. for its use, or for any infringements of patents or other rights of third parties resulting from its use. No part of this publication may be copied or reproduced in any form or by any means, or transferred to any third party without prior written consent of SafeNet, Inc.

TABLE OF CONTENTS

Section Title Page

LIST OF FIGURES

1. INTRODUCTION

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the SafeNet ProtectV StartGuard version 1.0 as implemented in the SafeNet ProtectV application version 1.0.

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 1 FIPS 140-2 validation of the Application.

FIPS 140-2 is a joint program between the National Institute of Standards and Technology (NIST) and Communication Security Establishment Canada (CSEC) for cryptographic modules. FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) details the security 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	1 (410) 931-7500
SafeNet Technical Support:	
U.S.	(800) 545-6608
International	1 (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” when discussing SafeNet ProtectV StartGuard.

2. PROTECT V

2.1 Functional Overview

ProtectV is a high assurance software solution for securing both virtual infrastructure and data, giving organizations the freedom to migrate to virtual and cloud environments while maintaining full ownership, compliance, and control of data. ProtectV security features include:

✓ **Complete Virtual Machine and Storage Encryption**

- Enables encryption of entire virtual machines and storage volumes associated with them;
- No data is written to system partition or storage volume disk without first being encrypted;
- Even data stored in the OS partition is protected;
- Encryption keys are stored on premise, in a high assurance hardware based key manager.

✓ **Pre-Launch Authentication**

- Access to data stored or processed by a protected VM requires explicit user authentication and authorization by ProtectV.

✓ **Separation of Duties**

- Role-based encryption polices, together with segregated key management ensure separation of duties between cloud service provider system administrators and the organization's IT administrators, or between different units in the organization's own virtual environment.

✓ **Security Management Across Cloud Environments**

- A unified management platform serves as a central audit point providing an at-a-glance dashboard view of all encrypted and unencrypted virtual machines and storage volumes belonging to the organization.

✓ **Enterprise Key Lifecycle Management with Government Grade Assurance**

The only solution that provides an on-premise key management system with the high assurance key store[1]. Cloud based key management can also be performed with ProtectV Manager.

Additional information on the ProtectV solution can be found here: http://www.safenet-inc.com/cloud-security/protectv-data-protection-for-the-cloud/

2.2 Cryptographic Module

The SafeNet ProtectV StartGuard is comprised of the following components in a FIPS 140-2 Level 1 configuration:

✓ VxBIOS

✓ CRYPdll

[1] As part of the ProtectV architecture, keys can be stored in SafeNet Hardware Security Modules (HSM's) but the HSM was not tested as part of this validation.

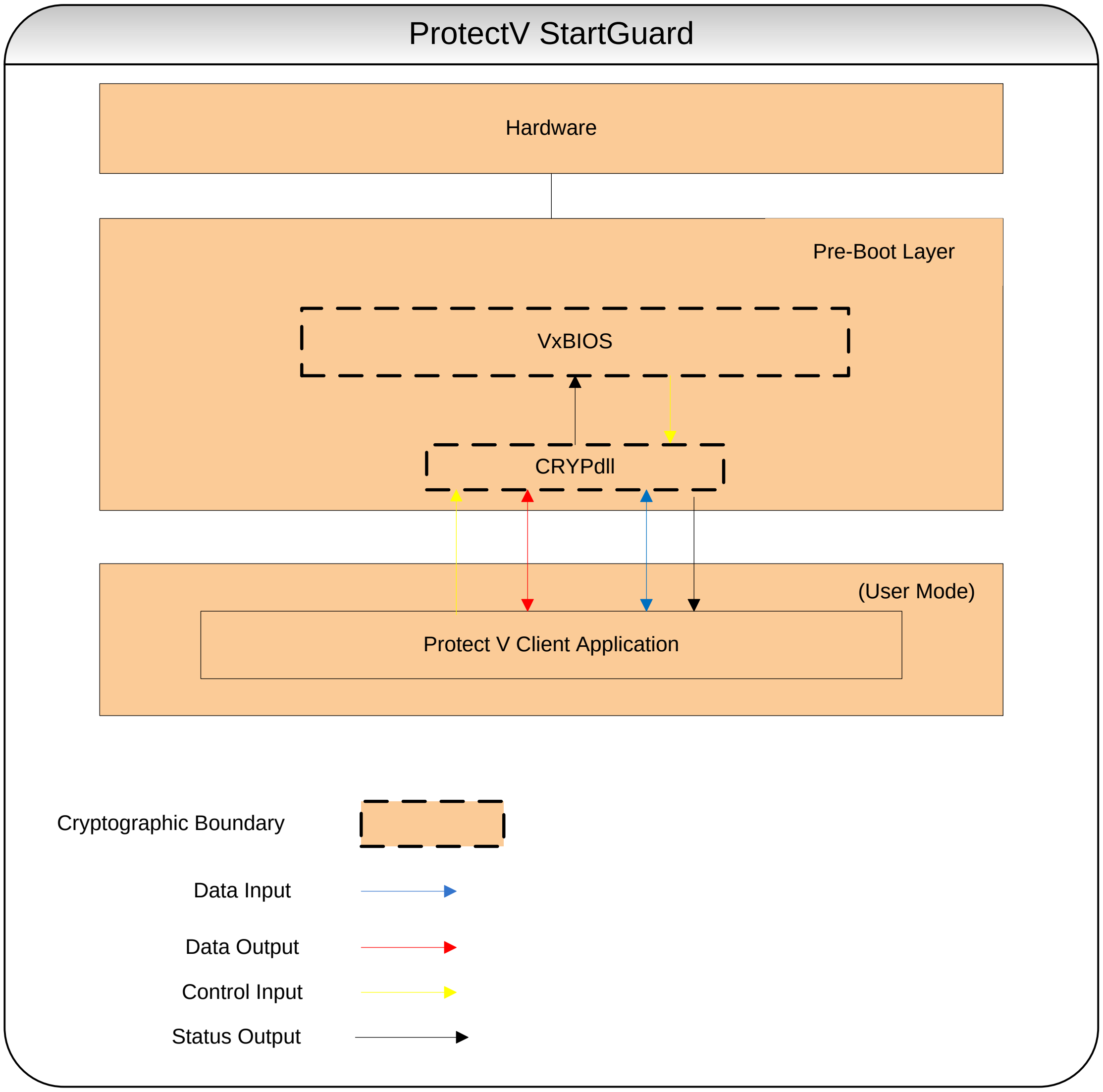

Figure 1. – Cryptographic Module Boundary

The function of CRYPdll system driver is to support INT13-based sector encrypted sector I/O performed by the boot loader after pre-boot chains to the native master boot record. The boot loader thus performs the function of loading all boot-start device drivers.

ProtectV StartGuard is always running in FIPS mode as it only provides FIPS Approved services.

3. CRYPTOGRAPHIC MODULE SPECIFICATION

From the point of view of FIPS 140-2, the SafeNet ProtectV StartGuard version 1.0 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 ProtectV StartGuard version 1.0.

3.1 FIPS 140-2 Security Levels

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

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Machine	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI / EMC	3
9	Self Tests	1
10	Design Assurance	1
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 ProtectV StartGuard via an API.

The module’s interfaces are separated into the logical and physical 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, USB 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 Interfaces

5. ROLES, SERVICES AND AUTHENTICATION

5.1 Identification and Authentication

The ProtectV StartGuard does not support authentication mechanisms.

5.2 Roles

The Cryptographic-Officer and User roles are both implicitly assumed by the operator as both roles can execute all services.

5.3 Services for Authorized Roles and Access Control

Table 3 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
Self-Test	CO, U	None	X
Decrypt	CO, U	Volume Key (VK)	R, X
Encrypt	CO, U	Volume Key (VK)	R, X
Show Status	CO, U	None	R
Zeroize	CO, U	Volume Key (VK)	X

Table 3. – ProtectV StartGuard Services and Authorized Roles

6. PHYSICAL ENVIRONMENT

ProtectV StartGuard was tested on a Dell PowerEdge R610 server with an Intel Xeon E5620 CPU that meets FCC Class B requirements at FIPS 140-2 Level 3. The SafeNet ProtectV StartGuard is implemented as software only components and thus the FIPS 140-2 physical security requirements are not applicable.

7. OPERATIONAL ENVIRONMENT

For the purpose of FIPS 140-2 Level 1 validation, the SafeNet ProtectV StartGuard is classified as a multi-chip standalone module as defined by FIPS PUB 140-2. The module has been tested on a Windows 2012 Server 64-bit running VMware's ESXi 5.0.

8. CRYPTOGRAPHIC KEY MANAGEMENT

8.1 Key Generation

The module does not generate keys.

8.2 Key Input / Output

ProtectV StartGuard has no logic to manage keys but keys can be input in encrypted form but keys are never output.

8.3 Key Zeroization

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

8.4 Algorithms

Tables 4 and 5 list the module 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)	2151
Message Authentication Code	
HMAC-SHA-256 (KeySize = Block Size)	1571

Table 4. - VxBIOS 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 Mode; Encrypt/Decrypt; Key Size = 256)	2550

Table 5. - Crypdll FIPS Approved or Allowed Algorithms

8.5 Security Functions, Cryptographic Keys and CSPs

Table 6 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 256-bit	Not Generated	Input - Encrypted	Not stored, resides in volatile memory	Format HDD	Decryption of System Volume

Table 6. – Approved Security Functions, Cryptographic Keys and CSPs

9. SELF-TESTS

The ProtectV StartGuard performs a number of power-up self-tests to ensure proper operation.

9.1 Power-On Self-Tests (POST)

When the SafeNet ProtectV StartGuard is initially powered-on, it executes power-on self-tests automatically as the module is the first thing that loads. 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. The operator can try clearing the error by rebooting the system. If the module cannot pass the power-on self-test it will remain in the error state. Table 7 lists the power-on self-tests:

Test	Function	FIPS 140-2 Required
Symmetric Cipher AES KAT	Performs known answer test for AES encrypt/decrypt for CRYPdll	Yes
Software Integrity Tests	HMAC-SHA-256 for VxBIOS and CRYPdll	Yes

Table 7. – Power-On Self-Tests

10. 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.

11. FIPS APPROVED MODE OF OPERATION

11.1 Description

The ProtectV StartGuard only contains FIPS Approved algorithms such that when the module is installed, it is automatically in FIPS mode.

11.2 Invoking Approved Mode of Operation

The ProtectV StartGuard is installed in FIPS Approved mode as its only function is to perform symmetric decryption.

11.3 Mode of Operation Indicator

The module is in FIPS mode when the module boots successfully. If the module fails a power-on self-test, the module and operating system will not boot.

12. GLOSSARY OF ACRONYMS, TERMS AND ABBREVIATIONS

Term	Definition
AES	Advanced Encryption Standard
CO	Cryptographic Officer
EFS	Embedded File System
LMC	Local Management Console
POST	Power On Self Test
VK	Volume Key