LEVEL 3 SECURITY POLICY FOR

ProtectServer Internal Express (PSI-e)

DOCUMENT NUMBER:	CR-3222
AUTHOR:	B. Franklin / I. Holness / C. Brych
DEPARTMENT:	Engineering
LOCATION OF ISSUE:	Australia / Ottawa
DATE ORIGINATED:	April 21, 2010
REVISION LEVEL:	19
REVISION DATE:	October 3, 2012
SUPERSESSION DATA:	CR-3222, Revision 18
SECURITY LEVEL:	Non-proprietary

TABLE OF CONTENTS

Section **Title** **Page**

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

1. INTRODUCTION

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the ProtectServer Internal Express (PSI-e). This security policy describes how the PSI-e meets the security requirements of FIPS 140-2 and how to operate the PSI-e in a secure FIPS 140-2 mode. This policy was prepared as a part of the Level 3 FIPS 140-2 validation of the PSI-e.

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 web site at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 References

This document deals only with operations and capabilities of the PSI-e in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the PSI-e 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/data-protection/hardware-security-modules/protectserver-hsms/ .
- 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 Canada, Inc.	20 Colonnade Road Suite 200 Ottawa, Ontario K2E 7M6 **Telephone:** +1 613 723 5077 **Fax:** +1 613 723 5079
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 the SafeNet ProtectServer Internal Express card is referred to as the PSI-e, the adapter, or the module.

1.4 Document Organization

This document provides an overview of the PSI-e and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the PSI-e. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

2. THE PSI-E CARD

2.1 Cryptographic Module Specification

The SafeNet PSI-e is a high-end intelligent PCI adapter card that provides a wide range of cryptographic functions using firmware and dedicated hardware processors. This document refers specifically to PSI-e hardware versions VBD-04-0302 and VBD-04-0303 running firmware versions 3.20.00 and 3.20.01.

Both hardware versions are the same except for their length. VBD-04-0302 was slightly larger than the PCI-e hardware specification, thus VBD-04-0303 is 0.066" shorter.

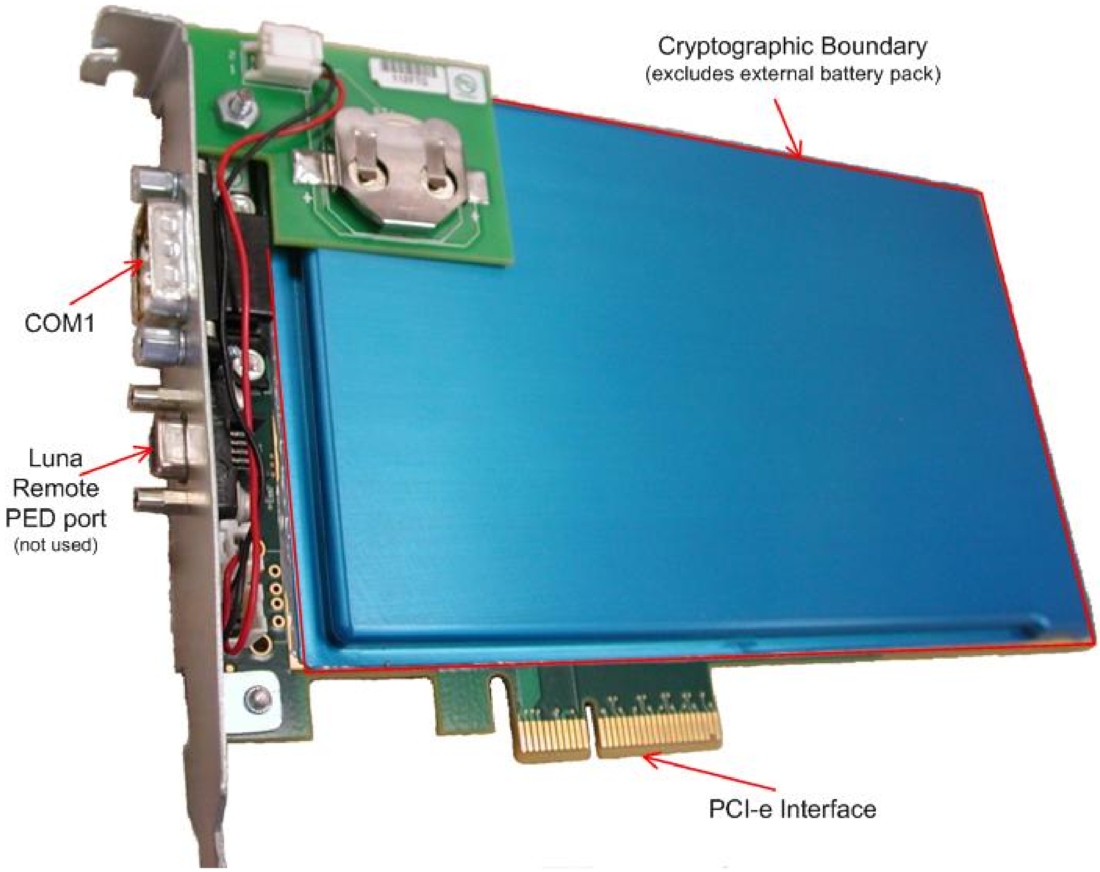

Figure 2-1 ProtectServer Internal Express Card

The module, running SafeNet's Cprov firmware, implements the Cryptoki cryptographic API as defined by RSA Data Security. While certain Cryptoki features are not supported, the module does provide a comprehensive compliance to the PKCS#11 standard as well as vendor-specific extensions.

The cryptographic boundary for this module includes the metal cover enclosure that is outlined in red above that is filled with hard epoxy. This boundary encapsulates the Data Ciphering Processor (DCP), embedded processor, SDRAM memory chips, and the Real Time Clock (RTC). The battery, battery isolation link, and external alarm input link are excluded from the FIPS 140-2 security requirements.

The module provides key management (e.g., generation, storage, deletion, and backup), an extensive suite of cryptographic mechanisms, and process management including separation between operators. The PSI-e also features non-volatile tamper protected memory for key storage, a hardware random number generator, and an RTC.

The PSI-e is classified as a multi-chip embedded processor for FIPS 140-2 purposes. The FIPS 140-2 cryptographic boundary is defined by the perimeter of the protection covers.

The PSI-e meets all level 3 requirements for FIPS 140-2 as summarized in Table 2-1.

Section	Section title	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services, and Authentication	3
4	Finite State Machine	3
5	Physical Security	3
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	EMI/EMC	3
9	Self Tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

Table 2-1 FIPS 140-2 Security Levels

2.2 Cryptographic Module Ports and Interfaces

The PSI-e has the following physical interfaces:

- A standard PCI Express bus interfacing to the motherboard of the host machine
- One asynchronous RS232 serial connector
- One Luna Remote PED connector (not used)
- An external battery isolation connector
- An external alarm input connector

The PSI-e provides a tightly secured cryptographic element. All requests for services sent to the adapter over the PCI bus or the serial ports are captured by the adapter's processor, which controls the level of access to the on-board cryptographic services and the keys. The adapter's processor also responds to PKCS #11 commands, ensuring that during FIPS operation only authenticated users receive cryptographic services.

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

FIPS 140-2 Logical Interfaces	Adapter Physical Interfaces
Data Input Interface	PCI Bus, Serial port
Data Output Interface	PCI Bus, Serial port
Control Input Interface	PCI Bus, External tamper input
Status Output Interface	PCI Bus
Power Interface	PCI Bus, External battery link

Table 2-2 FIPS 140-2 Logical Interfaces

2.3 Roles, Services, and Authentication

The PSI-e supports identity-based authentication of its operator. Operators are identified by a token name and PIN. The different roles and required authentication are shown in Table 2-3.

Operator	Role	Type of authentication	Authentication Data
Admin SO	Crypto-Officer	Identity Based	Operator Unique PIN
Administrator	User	Identity Based	Operator Unique PIN
Token SO	Crypto-Officer	Identity Based	Operator Unique PIN
Token User	User	Identity Based	Operator Unique PIN

Table 2-3 Roles and Required Identification and Authentication

The PSI-e supports three types of Tokens: one Administration Token, multiple Cprov Tokens and one or more Smart Card Tokens. All Tokens have two operators: a Security Officer (SO) and a User. For the Administration Token, the Admin SO is the Security Officer and the Administrator is the User. For all other Tokens, the Security Officer is the Token SO and the Token User is the User.

The operator explicitly selects a role when logging in by selecting a PKCS#11 Token and nominating either User or SO Role. The adapter provides restricted services to an operator based on the role to which the operator authenticated. There is only one operator assigned to each role. The Admin SO, Admin and Token SO perform FIPS 140-2 Crypto Officer roles while the Token User performs a FIPS 140-2 User role.

The PSI-e enforces a minimum PIN length of 4 characters and a maximum PIN length of 32 characters. The module allows the PIN character to be any value but the software typically used with the module restricts the dictionary to the ANSI C character set. This character set provides for 92 visible characters which, with a 4 character PIN, provides a probability of less than one in 1,000,000 that a random PIN attempt (e.g., guess) will succeed (actual probability is approximately 1/71,600,000). The module is protected from brute force PIN attacks by imposing an increasing delay for every failed PIN attempt after the first three failed attempts. The initial delay is 5 seconds and increases by an additional 5 seconds for each subsequent failed attempt, e.g., 3 fails causes a 5 second delay; 4 fails causes a 10 second delay; 5 fails causes a 15 second delay; etc.

2.3.1 Services for Authorized Roles

Table 2-4 lists the services related to each authorized role within the adapter:

Role	Services
Admin SO	Initialize Administrator Token User PIN
Admin	Manage Adapter and Admin Token
Token SO	Manage Token
Token User	Use Token and manage token keys
Unauthenticated operator	Unauthenticated services

Table 2-4 Types of Available Services

2.3.2 Administrator Security Officer

The primary role of the Administrator Security Officer (ASO) is to introduce the Administrator to the system. The ASO is able to set the initial Administrator PIN value but is not able to change the administration PIN after it is initialized. The ASO can perform the following services:

- Set the initial Administrator PIN value (may not change it later).
- Set the CKA_TRUSTED attribute on a Public object in the Admin Token.
- Set the CKA_EXPORT attribute on a Public object in the Admin Token.
- Manage Host Interface Master Keys
- Exercise cryptographic services with Public objects
- Create, destroy, import, export, generate, and derive[1] Public objects
- May change his/her own PIN
- Read the Hardware Event Log
- May modify Monotonic Counter object

2.3.3 Administrator

The Administrator is responsible for the overall security management of the adapter. Token Security Officers and Slots are controlled by the Administrator. The following services are available to the Administrator:

- Set or Change RTC value
- Read the Hardware Event Log
- Purge a full Hardware Event Log
- Configure the Transport Mode feature
- Specify the Security Policy of the adapter
- Create new Cprov Slots/Tokens and specify their Labels, SO PINs, and minimum PIN Length
- Initialize smart cards and specify their Labels and SO PINs
- Destroy individual Cprov Slots/Tokens
- Zeroize all adapter Secure Memory including all PINs and User Keys
- Perform Firmware Upgrade Operation
- Manage Host Interface Master Keys
- Exercise cryptographic services with Public objects on Admin Token
- Exercise cryptographic services with Private objects on Admin Token
- Create, destroy, import, export, generate, and derive Public objects on Admin Token
- Create, destroy, import, export, generate, and derive Private objects on Admin Token
- May change his/her own PIN
- May revoke Authentication

2.3.4 Token SO

[1] Key Derive operations are listed in Table 2-10.

The Token SO is responsible for granting and revoking ownership of the token. If the Token does not have a User PIN, the Token SO should initialize it by assigning the Label and User PIN. The token SO may also revoke the Token User's privileges (and possibly reassign the token to another operator) but only by destroying all the key material of the original operator first. The following services are available to the Token SO:

- Set the initial User PIN value (may not change it later)
- Reset (re-initialize) the Token (destroys all keys and User PIN on the Token) and set a new Label
- Set the CKA_TRUSTED attribute on a Public object in his or her Token
- Set the CKA_EXPORT attribute on a Public object in his or her Token
- Exercise cryptographic services with Public objects in his or her Token
- Create, destroy, import, export, generate, and derive Public objects in his or her Token
- May change his/her own PIN
- May modify Monotonic Counter object

2.3.5 Token User

Token users may manage and use private and public keys on their own tokens. The following services are available to the Token User:

- Exercise cryptographic services with Public objects in his or her Token
- Exercise cryptographic services with Private objects in his or her Token
- Create, destroy, import, export, generate, derive Public objects in his or her Token
- Create, destroy, import, export, generate, and derive Private objects in his or her Token
- May change his/her own PIN

2.3.6 Unauthenticated Operators

Certain services are available to operators who have not (yet) authenticated to the adapter:

- Exercise status querying services
- Authenticate to a Token
- Force session terminate, restart adapter by setting the doorbell register on the hardware. The doorbell register is a memory map to the PCI bus. The host application can force a restart by writing a certain value to the register through the PSI-e device driver. The transparent PCI chip will then generate a bus cycle restart which in turn will restart the adapter.

All of the services available to the Unauthenticated Operators are also available to all authenticated operators.

2.4 Physical Security

The adapter provides tamper evidence and tamper response mechanisms. The non-removable metal casing and epoxy covered PCB board provides a strong tamper evident enclosure. The Administrator should perform routine visual inspection of the module for evidence of tamper such as scratches.

The module is actively protected through a combination of an external tamper jumper switch, a light sensor, and a voltage monitor. The PSI-e protection can also be activated by removal of the adapter from the host machine or via an external alarm input capability. In the event of a tamper the PSI-e enters a Tamper state in which all processing is halted and the secure memory is zeroized.

2.5 Operational Environment

This section does not apply. The PSI-e does not provide a modifiable operational environment.

2.6 Cryptographic Key Management

The PSI-e is a general-purpose cryptographic management device and thus securely administers both cryptographic keys and other critical security parameters (CSPs) such as passwords.

2.6.1 Key Generation

The PSI-e Module supports the generation of DSA, RSA, ECDSA (also known as ECC), and DH public and private keys. The module also supports the generation of three-key Triple-DES keys as well as AES 128-bit, 192-bit, and 256-bit keys. The module implements the FIPS approved RNG specified in FIPS 186-2 x-Original using SHA-1 that is used for generating random values required for key generation. The RNG is seeded from the HRNG from the crypto chip.

2.6.2 Key Access / Storage

All keys except module specific keys are stored as plaintext token objects in secure memory (battery-backed RAM), and the module prevents physical access to this RAM through the physical security mechanisms discussed in section 2.4. Logical access to keys and other CSPs is restricted to authenticated operators with valid permissions. Any key input to the module is done so over a Triple-DES encrypted trusted channel or by components through a dedicated port and the module only allows keys to be output if they are wrapped using a FIPS Approved algorithm.

Table 2-5 outlines all the keys stored by the module.

CSP	CSP Type	Generation	Input/Output	Storage	Destruction Mechanism	Use
Firmware upgrade Certificate	2048 bit RSA	FIPS 186-2 RNG	Not input/output	Plaintext in Flash	None	To verify the signature attached to a new firmware image.
Default Administrative Token SO PIN	PIN	N/A	Not input/output	Plaintext in Flash	Replaced as part of the initialization process	For initial authentication to the module. Replaced after the module is initialized.
D-H Key Agreement Keys	1024-4096 bit Modulus Size	Private Component Generated Via FIPS 186-2 RNG; Public Value Computed via Diffie-Hellman	Public key exported as part of key agreement	Working memory	Power cycle, tamper, or C_DestroyObject() API	To establish an encrypted channel between an operator and the module.
DH Shared Secret Key	Triple-DES	Established via DH	Not input/output	Working memory	Power cycle, tamper, or C_DestroyObject() API	Protects data between an operator and the module. Triple-DES is used to protect the secure channel established using DH.
EC-DH Key Agreement Keys	ECDH (P192-P521)	Private Component Generated Via FIPS 186-2 RNG; Public Value Computed via Diffie-Hellman	Public key exported as part of key agreement	Working memory	Power cycle, tamper, or C_DestroyObject() API	To establish an encrypted channel between an operator and the module.
ECDH Shared Secret Key	Triple-DES	Established via ECDH	Not input/output	Working memory	Power cycle, tamper, or C_DestroyObject() API	Protects data between an operator and the module. Triple-DES is used to protect the secure channel established using ECDH.
Message Authentication Key	HMAC-SHA-1	Established via DH/ECDH	Not Input/Output	Working memory	Power cycle, tamper, or C_DestroyObject() API	Provide data authentication of encrypted data between an operator and the module.

CSP	CSP Type	Generation	Input/Output	Storage	Destruction Mechanism	Use
RSA Public/Private Keys	1024 – 4096 bit RSA	ANSI X9.31	Public key exported as part of key agreement	Working memory	Power cycle, tamper, or C_DestroyObject() API	Key wrapping as part of a TLS key establishment protocol.
Operating PINs	PIN	N/A	Input encrypted[2]	Encrypted with MMK	Tamper or C_DestroyObject() API	All users' PINs – Admin Token SO, Admin Token User, Token SOs, and Token users used to authenticate to the module.
Token Keys	AES or Triple-DES	FIPS 186-2 RNG	Encrypted[3] or split knowledge	Secure memory encrypted with MMK	Tamper or C_DestroyObject() API	User-created keys for use by user applications
Application Keys	AES or Triple-DES	FIPS 186-2 RNG	Output encrypted	Secure memory encrypted with MMK	Tamper or C_DestroyObject() API	Used to wrap Token Keys output from the module.
RNG Seed Key	Seed Key	H/W RNG	Not input/output	Not permanently stored	Power cycle or tamper	Used as part of the RNG process.
Module Master Key	3-key Triple-DES	FIPS 186-2 RNG	Not input/output	Tamper responsive memory in NVRAM of RTC	Tamper or Zeroize command (ctconf –x)	Used to encrypt contents of secure memory

Table 2-5 List of Keys Stored in Module

Table 2-5 outlines the access that "Authorized Services" (see Table 2-4) have to the keys listed in Table 2-5. Here 'R' stands for "Read", 'W' stands for "Write", X stands for "Execute" and "Z" stands for "Zeroize".

[2] PINs encrypted using Triple-DES
[3] Token Keys encrypted using AES or Triple-DES Application Keys

	FW Upgrade Cert	Default Admin Token SO PIN	DH / ECDH Ephemeral Keys	Key Agreement Keys	Message Authentication Key	Operating PINs	Token Keys (Public)	Token Keys (Private)	RNG Seed Key	Module Master Key
Initialization	-	-	-	X	-	WX	-	-	-	W
Administrator SO	WX	WX	-	WXZ	-	WXZ	RWXZ	RWXZ	-	RWXZ
Administrator	-	-	WZ	X	WZ	WXZ	-	-	-	RWXZ
Token SO	-	-	RXZ	X	RXZ	X	-	-	-	-
Token User	-	-	RXZ	X	RXZ	X	XZ	XZ	XW	-
Unauthenticated Operators	-	-	-	-	-	X	-	-	-	-

Table 2-6 Access to Keys for Authorized Services

Please note that the FW Upgrade Cert is never zeroized because it is a public key. The Default Admin Token SO PIN is never zeroized because it's a pre-initialization value. The RNG Seed Key is zeroized when a tamper event is detected or overwritten when the module is restarted. All other CSPs/Keys identified in Table 2-5 are zeroized by a call to C_DestroyObject() API by the respective role or through a tamper event.

2.6.3 Security Functions

The PSI-e supports a wide variety of security functions. FIPS 140-2 requires that only FIPS Approved algorithms be used whenever there is an applicable FIPS standard.

Table 2-7 lists the PSI-e FIPS Approved security functions. In the FIPS mode of operation these Approved security functions are available.

FIPS Approved Security Function	FW 3.20.00 / 3.20.01	HW
AES	*Cert. 1859*	*Cert. 1860*
DSA	*Cert. 579*	
ECDSA– Only NIST Recommended Curves	*Cert. 259*	
RSA	*Cert. 940*	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	*Cert. 1636*	
HMAC: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	*Cert. 1106*	
Triple-DES	*Cert.1206*	*Cert. 1207*
Triple-DES MAC (Vendor Affirmed)	*Cert. 1206*	
RNG	*Cert. 975*	

Table 2-7 FIPS Approved Security Functions

Table 2-8 lists the PSI-e Non-Approved but FIPS allowed security functions. In the FIPS mode of operation these Non-Approved security functions are available.

Non-Approved FIPS but Allowed Security Functions
AES[4] *Key Wrapping/Unwrapping*
Triple-DES[5] *Key Wrapping/Unwrapping*
DH[6]
RSA Key Wrapping/Unwrapping[7]
ECDH[8] *- Only NIST Recommended Curves*

Table 2-8 Non-Approved FIPS Allowed Security Functions

[4] AES (Certs. #1859 and #1860, key wrapping; key establishment methodology provides 128, 192 or 256 bits of encryption strength);
[5] Triple-DES (Certs. #1206 and #1207, key wrapping; key establishment methodology provides 80 or 112 bits of encryption strength);
[6] Diffie-Hellman key agreement; key establishment methodology provides between 80 and 150 bits of encryption strength; non-compliant less than 80-bits of encryption strength;
[7] RSA key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength;
[8] EC Diffie-Hellman key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength.

Table 2-9 lists the PSI-e Non-FIPS Approved security functions. When the PSI-e is in the FIPS mode of operation these security functions are not available.

Non-FIPS Approved Security Functions
DES (ECB, CBC, OFB64)
DES MAC
AES MAC
CAST 128 (ECB, CBC)
CAST MAC
IDEA (ECB, CBC)
IDEA MAC
RC2 (ECB, CBC)
RC2 MAC
SEED (ECB,CBC)
SEED MAC
MD2
MD5
MD5 HMAC
RC4 (ECB)
RIPEMD-128
RIPEMD-160
RMD128 HMAC
RMD160 HMAC
ECIES
ARIA

Table 2-9 Non-FIPS Approved Security Functions

Table 2-10 lists the PSI-e key derivation mechanisms.

MECHANISMS FOR SPLIT KNOWLEDGE ENTRY/OUTPUT OF KEY (Allowed in FIPS Mode)	DISABLED/NON-ALLOWED DERIVATION METHODS (Not Allowed in FIPS Mode)
CKM_CONCATENATE_BASE_AND_KEY	CKM_DES3_DERIVE_CBC _DERIVE
CKM_XOR_BASE_AND_DATA	CKM_DES3_DERIVE_ECB
CKM_XOR_BASE_AND_KEY	CKM _SHAxxx_KEY_DERIVATION
CKM_EXTRACT_KEY_FROM_KEY	CKM_SSL3_KEY_AND_MAC_DERIVE
CKM_SECRET_SHARE_WITH_ATTRIBUTES	CKM_SSL3_MASTER_KEY

Table 2-10 Summary of Key Derivation Mechanisms

2.7 Self-Tests

The PSI-e Module performs a number of power-up and conditional self-tests to ensure proper operation.

2.7.1 Power-Up Self-Tests

When the module is initially powered-on, it executes a battery of power-up self-tests. If any of the power-up self-tests fail, the module will enter an error state and prohibit an operator from exercising the module's cryptographic functionality. Table 2-11 lists the power-up self-tests:

Test	Function	FIPS 140-2 Required
SDRAM	Tests the module's volatile working memory by performing a connectivity test	No
SRAM	Tests the module's static RAM by performing a connectivity test	No
Secure Memory File System Integrity	Initializes and checks the module's secure memory file system	No
Flash Boot Block	Verifies a checksum over the module's personalization data in ROM	No
RTC Connectivity	Verifies that the CPU can connect to the UART device	No
RNG KAT	Performs a known answer test for the FIPS 186-2 RNG.	Yes
Symmetric Cipher KATs	Performs known answer tests for AES, Triple-DES, CAST, IDEA, RC2, DES, and RC4.	AES and Triple-DES
MAC and HMAC KATs	Performs known answer tests for CAST MAC, IDEA MAC, RC2 MAC, DES MAC and Triple-DES MAC. Performs known answer tests for MD5 HMAC, HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, RMD128 HMAC and RMD160 HMAC.	Triple-DES MAC HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512
Asymmetric Cipher KATs	Performs known answer tests for RSA operations.	Yes
Asymmetric Key Derive KATs	Performs known answer tests for ECDH1 Derive	No
Asymmetric Pairwise Consistency Test	Performs a pairwise consistency test on a DH key pair	No
Sign/Verify	Known Answer signature/verification tests for RSA, DSA and ECDSA.	Yes
Message Digest KATs	Verifies known message/hash pairs for MD2, MD5, RMD128, RMD 160, SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512.	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
Software/Firmware Integrity	Ensures that the software/firmware on the module has not been modified / damaged by calculating a SHA-1 hash over all software/firmware components and comparing the digest to a known good result.	Yes
Statistical RNG	Performs a Statistical Chi Square test of 2500 bytes of random data	(Legacy)

Table 2-11 Power-up Self-Tests

2.7.2 Conditional Self-Tests

The module performs conditional self-tests as outlined in Table 2-12.

Test	Function	FIPS 140-2 Required
Pairwise Consistency	Runs a pairwise consistency check each time the module generates a DSA, RSA, ECDSA, or DH public/private key pair.	DSA, RSA, ECDSA
Continuous HW RNG	Performs the FIPS 140-2 required continuous RNG check each time the module's Hardware RNG is used to produce random data.	Yes
Continuous RNG	Performs the FIPS 140-2 required continuous RNG check each time the module's RNG is used to produce random data.	Yes
Firmware Load	Checks that the firmware to be loaded is verified with a digital signature. If the signature cannot be verified, the module will report an error and the firmware will not be loaded. **Note:** Following a successful verification, all keys and CSPs will first be zeroized and then the firmware will be updated . After the firmware is updated, the PSI-e will automatically transition to a non-FIPS mode and will require reconfiguration to return to FIPS mode.	Yes

Table 2-12 Conditional Self-Tests

2.8 Mitigation of Other Attacks

The PSI-e does not employ any technology specifically intended to mitigate against other attacks.

3. FIPS APPROVED MODE OF OPERATION

3.1 Description

The PSI-e allows its administrators the choice of employing a wide range of security technologies. To comply with FIPS mode of operation the PSI-e must be configured in a secure manner. This includes:

- Operation with FIPS Approved algorithms as listed in Table 2-7 and Non-Approved but FIPS allowed algorithms as listed in Table 2-8;
- Not permitting the export of clear keys;
- Locking the security mode to prevent circumvention of the mode setting;
- Not permitting PINs to be used in clear;
- Not permitting changes to the PSI-e firmware without first clearing all protected keys and CSPs; and
- Providing authentication and session management security.

This Security Policy describes a particular PSI-e firmware and hardware. The PSI-e firmware can be replaced (with a firmware upgrade operation) or extended (by loading Functionality Modules [FMs]). The operator should ensure that the firmware and hardware of the PSI-e are validated configurations.

The PSI-e checks that new firmware is digitally signed before it can be loaded. Following a successful verification all keys and CSPs will be zeroized. After the zeroization, the PSI-e will automatically transition to a non-FIPS mode and will require reconfiguration to return to FIPS mode.

3.2 Invoking Approved Mode of Operation

An operator may easily place the PSI-e in "FIPS mode" by simply running the administrative `CTCONF -fF` command from the remote management facility. Once this command is executed the PSI-e will reject all requests for non-FIPS algorithms or configurations. Please note that the operator has to be logged in as an Administrator to invoke the FIPS mode of operation.

3.3 Mode of Operation Indicator

Running the display status command from a remote management facility will return a status displaying the current PSI-e operating mode.

```
Security Mode: FIPS 140-2 Mode: <list of flags indicating attributes set for FIPS>
```

When the module is not running in FIPS mode, this status displays as:

```
Security Mode:
```

3.4 Invoking Mode of Operation Indicator

An operator may easily view the current PSI-e mode of operation by simply running the administrative `CTCONF –v` command from the remote management facility. Once this command is executed the PSI-e will respond with full details of the adapter configuration. The configuration details include details of the firmware loaded and a listing of the adapter security mode flags one of which indicates that the module is in the FIPS mode of operation.

4. DESIGN ASSURANCE

4.1 Distribution and Delivery of Module

The module is shipped in an anti-static shipping envelope that is sealed with a SafeNet security sticker and placed inside a SafeNet shipping box. The user should inspect the product shipping boxes to make sure they have not been tampered with or damaged upon receiving the modules, which could indicate a security compromise.

APPENDIX A. ACRONYMS AND ABBREVIATIONS

Acronym	Definition
AES	Advanced Encryption Standard
AK	Application Key
ANSI	American National Standards Institute
API	Application Programming Interface
ARIA	Korean Government Standard Encryption Algorithm
ATSO	Administrative Token Security Operator
ATU	Administrative Token User
CA	Certificate Authority
CPU	Central Processing Unit
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie-Hellman
DHEK	Diffie-Hellman Ephemeral Key
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDHEK	Elliptic Curve Diffie-Hellman Ephemeral Key
FIPS	Federal Information Processing Standard
HRNG	Hardware Random Number Generator
IDEA	International Data Encryption Algorithm
KAT	Known Answer Test
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MAK	Message Authentication Key
MD2	Message Digest Algorithm 2
MD5	Message Digest Algorithm 5
MD5 HMAC	MD5 Hashed Message Authentication Code
MMK	Module Master Key
NIST	National Institute of Standards and Technology
NO	Normal Operator
PSI-e	ProtectServer Internal-Express
PIN	Personal Identification Number
PKI	Public Key Infrastructure

Acronym	Definition
RAM	Random Access Memory
RC2	Rivest’s Code 2
RC4	Rivest’s Code 4
RNG	Random Number Generator
RoHS	Restriction on Hazardous Substances
ROM	Read Only Memory
RSA	Rivest, Shamir and Adleman
RWXZ	Read, Write, Execute, Zeroize
SDRAM	Synchronous Dynamic Random Access Memory
SHA	Secure Hash Algorithm
SO	Security Operator
SRAM	Static Random Access Memory
Triple-DES	Triple Data Encryption Standard
USB	Universal Serial Bus
USO	User Security Operator
VGA	Video Graphics Array