ProtectServer Gold

Non-Proprietary Security Policy

FIPS140-2 Level 3

Document number: CR-2970

Revision: 1

THIS PAGE INTENTIONALLY LEFT BLANK

Preface

Copyright

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

Publication Improvements

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be dispatched to the following address:

SafeNet Canada, Inc.
20 Colonnade Road, Suite 200
Ottawa, Ontario
CANADA K2E 7M6

Voice:	1 613 221 5000
Fax:	1 613 723 5079
Website:	www-safenet-inc.com

Supersession Information

This document supersedes document CR-2505, revision 14.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

1 Introduction

1.1 Purpose

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

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 PSG in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the PSG and other SafeNet products from the following sources:

- The SafeNet internet site contains information on the full line of security products at www.safenet-inc.com
- For answers to technical or sales related questions please refer to the contacts listed on the SafeNet internet site at www.safenet-inc.com.

1.3 Terminology

In this document the SafeNet ProtectServer Gold card is referred to as the PSG, the adapter, or the module.

1.4 Document Organization

The Security Policy document is part of the complete FIPS 140-2 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Module Software Listing
- Other supporting documentation as additional references

This document provides an overview of the PSG 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 PSG. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

This Security Policy and other Certification Submission Documentation were produced by SafeNet. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Certification Submission Documentation is Proprietary to SafeNet and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact SafeNet.

2 The PSG Card

2.1 Cryptographic Module Specification

The SafeNet PSG 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 PSG hardware revisions B2, B3, and B4 running firmware version 2.03.00.

Please note that the difference between hardware revision B2 and hardware revision B3 is that hardware revision B2 contains components that are not RoHS[1] compliant while hardware revision B3 contains RoHS-compliant components. Hardware revision B4 differs from hardware revision B3 in that a filter circuit has been replaced with a jumper. Functionally, all hardware revisions are identical.

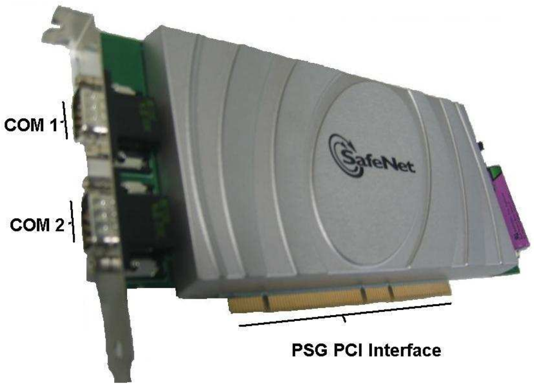

Figure 1 - The PSG

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 encapsulates the majority of the adapter card. An opaque, metal cover surrounds the card to provide tamper-protection and to establish the cryptographic boundary. This boundary encapsulates the Data Ciphering Processor (DCP), embedded processor, SDRAM memory chips, and the Real Time Clock (RTC).

[1] RoHS – Restriction on Hazardous Substances came into effect July 2006 in member states of the EU. RoHS restricts the usage of lead, mercury, cadmium, hexavalent chromium, and the bromines PBB and PBDE in products sold in the EU.

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 *PSG* also features non-volatile tamper protected memory for key storage, a hardware random number generator, a Real Time Clock.

The *PSG* is classified as a multi-chip embedded processor for FIPS140-2 purposes. The FIPS140-2 cryptographic boundary is defined by the perimeter of the protection covers. The Battery, battery isolation link, external alarm input link are excluded from the FIPS140-2 security requirements.

The *PSG* meets all level 3 requirements for FIPS140-2 as summarized in Table 1 - FIPS 140-2 Security Levels.

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	3

Table 1 - FIPS 140-2 Security Levels

2.2 Cryptographic Module Ports and Interfaces

The *PSG* has the following physical interfaces:

- A standard PCI bus interfacing to the motherboard of the host machine
- Two asynchronous RS232 serial connectors
- A battery isolation connector
- An external alarm input connector.

The *PSG* 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 – FIPS 140-2 Logical Interfaces:

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

Table 2 – FIPS 140-2 Logical Interfaces

2.3 Roles, Services and Authentication

The *PSG* 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 3 - Roles and Required Identification and Authentication below.

Role	Type of authentication	Authentication Data
Admin SO	Identity Based	PIN
Administrator	Identity Based	PIN
Token SO	Identity Based	PIN
Token User	Identity Based	PIN

Table 3 - Roles and Required Identification and Authentication

The *PSG* 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. 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 FIPS140-2 Crypto officer roles while the Token User performs a FIPS140-2 User role.

The PSG enforces an absolute minimum PIN length of 4 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 sec delay; 4 fails 10 sec; 5 fails 15 sec; etc.

2.3.1 Services for Authorized roles

Table 4 - Services for Authorized Roles below listed the services related to each authorized role within the adapter:

Role	Authorized 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 4 - Services for Authorized Roles

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 actions:

- Set the initial Administrator PIN value (may not change it later)
- Set the CKA_TRUSTED attribute on a Public object
- Set the CKA_EXPORT attribute on a Public object
- Manage Host Interface Master Keys
- Exercise cryptographic services with Public objects
- Create, destroy, import, export, generate, derive Public objects
- May change his/her own PIN

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 actions 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
- Erase 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
- Exercise cryptographic services with Private objects
- Create, destroy, import, export, generate, derive Public objects
- Create, destroy, import, export, generate, derive Private objects
- May change his/her own PIN
- May revoke Authentication

2.3.4 Token SO

The Token SO is responsible for granting and revoking ownership of its 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.

- 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
- Set the CKA_EXPORT attribute on a Public object
- Exercise cryptographic services with Public objects
- Create, destroy, import, export, generate, derive Public objects
- May change his/her own PIN

2.3.5 Token User

Token users may manage and use private and public keys on their own tokens.

- Exercise cryptographic services with Public objects
- Exercise cryptographic services with Private objects
- Create, destroy, import, export, generate, derive Public objects
- Create, destroy, import, export, generate, derive Private objects
- 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. Doorbell register is a memory map to the PCI bus. The host application can forced restarted by writing a certain value to the register through the PSG device driver, the transparent PCI chip will then generate a bus cycle restart which in term restart the adapter.

2.4 Physical Security

The adapter provides tamper evidence and tamper response mechanisms. The non-removable metal casing provides a strong tamper evident enclosure.

The module is actively protected through a combination of tamper switches, light sensor and voltage monitor. The *PSG* 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 *PSG* enters a Tamper state in which all processing is halted and the secure memory is erased.

2.5 Operational Environment

This section does not apply. The *PSG* does not provide a modifiable operational environment.

2.6 Cryptographic Key Management

The *PSG* 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 *PSG* Module supports generation of DSA, RSA, ECDSA, and DH public and private keys. The module also supports generation of double and triple DES keys as well as AES 128 bit and 256 bit keys. The module employs a FIPS 186-2 PRNG for generating keys used in FIPS approved algorithms. The PRNG is seeded from the HRNG from the Pijnenburg 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 TDES encrypted trusted channel, and the module only allows wrapped (TDES encrypted) keys to be output.

The following table outlines the keys stored by the module.

Security Relevant Data Item	SRDI Description
Firmware Upgrade Certificate	An X.509 certificate containing a 2048-bit RSA public key embedded within the module’s firmware image (in Flash memory). This key is used to verify the signature attached to a new firmware image.
Default Administrative Token SO PIN	Default SO PIN used for the Administrative Token. This PIN is generally modified as the first step in initialising the module. This default PIN is stored in the module’s

Security Relevant Data Item	SRDI Description
	firmware image.
Host Interface Master Key	192-bit 3DES key. It is not used when the modules is put into FIPS mode but will still exist on the module. This key is stored in the module's secure memory.
Diffie-Hellman parameters	Used to establish an encrypted channel between an operator and the module. These parameters are stored in the module's secure memory.
Operating PINs	All users' PINs – Admin Token SO, Admin Token User, Token SOs and Token users. All PINs stored in the module's secure memory.
Token Keys	All user created keys for use by user applications. These keys are stored in the module's secure memory.

Table 5 - List of Keys Stored in Module

The following table outlines the access that approved services have to the keys listed in Table 5.

	Fw Upgrade Cert t	Default Admin Token SO PIN	HIMK	DH Parameters	Operating PINs	Token Keys (Public)	Token Keys (Private)
Init Token Admin PIN	-	-	-	X	WX	-	-
Manage Adapter & Admin Token	WX	WX	-	WXZ	WXZ	RWXZ	WRXZ
Manage Token	-	-	-	X	X	-	-
Use Token & Manage Token Keys	-	-	-	X	X	XZ	XZ
Unauthenticated Services	-	-	-	-	X	-	-

Table 6 - Access to Keys for Authorized Services

2.6.3 Security Functions

The *PSG* 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 7 - Approved Security Functions below lists the *PSG* approved security functions, along with their validation certificate number. In the FIPS mode of operation only these Approved security functions are available.

Approved Security Function	Validation Certificate
AES	*382*
DSA	*166*
ECDSA	*26*
RSA	*134*
SHA-1, SHA-256, SHA-384, SHA-512	*457*
HMAC: SHA-1, SHA-256, SHA-384, SHA-512	*171*
TDES	*426*
TDES MAC	*426*
RNG	*184*

Table 7 - Approved Security Functions

Table 8 - Non-Approved FIPS Allowed Security Functions below lists the *PSG* Non-Approved security functions, but FIPS allowed. In the FIPS mode of operation these Non-Approved security functions are available.

Non-Approved FIPS allowed Security Function
DH
RSA ENCRYPT / DECRYPT [2]

Table 8 - Non-Approved FIPS Allowed Security Functions

[2] NOTE – RSA Encrypt/Decrypt should be used only for Key Transport in FIPS mode of operation.

Table 9 - Non-Approved Security Functions below lists the *PSG* Non-Approved security functions. When the *PSG* is in the FIPS mode of operation these functions are not available.

Non-Approved Security Function
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

Table 9 - Non-Approved Security Functions

2.7 Self-Tests

The *PSG* 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 10 - Power-up Self-Tests 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	Yes
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
PRNG FIPS G	Verifies the PSG implementation of the FIPS G SHA-1 function	No
Symmetric Cipher KATs	Performs known answer tests for AES, TDES, CAST, IDEA, RC2, DES, and RC4.	AES and TDES
MAC and HMAC KATs	Performs known answer tests for CAST, IDEA, RC2, DES and TDES MAC. Performs known answer test for MD5, SHA-1, SHA-256, SHA-384, SHA-512, RMD128 and RMD160 HMAC.	TDES MAC SHA-1, SHA,256, SHA-384, SHA-512
Asymmetric Cipher KATs	Performs a known answer test for RSA operations.	Yes
Sign/Verify	Tests signature verification tests for RSA, DSA and ECDSA.	RSA, DSA, ECDSA
Message Digest KATs	Verifies known message/hash pairs for MD2, MD5, RMD128, RMD 160, SHA-1, SHA-256, SHA-384 and SHA-512.	SHA-1, SHA-256, SHA-384, SHA-512

Test	Function	FIPS 140-2 Required
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 10 - Power-up Self-Tests

2.7.2 Conditional Self-Tests

The module performs conditional self-tests outlined in Table 11 - Conditional Self-Tests:

Test	Function	FIPS 140-2 Required
Pairwise Consistency	Runs a pairwise consistency check each time the module generates a DSA, RSA, ECC, or DH public/private key pair.	DSA, RSA, ECC
Continuous RNG	Performs the FIPS 140-2 required continuous RNG check each time the module's PRNG is used to produce random data.	Yes
Software Load	Checks that software is digitally signed before it can be loaded. Note: following a successful verification all keys and CSPS will be zeroized. After the zeroization, the PSG will automatically transition to a Non-FIPS mode and will require reconfiguration to return to FIPS mode. .	Yes

Table 11 - Conditional Self-Tests

2.8 Mitigation of Other Attacks

The *PSG* does not employ any technology specifically intended to mitigate against other attacks.

THIS PAGE INTENTIONALLY LEFT BLANK

3 FIPS Approved Mode of Operation

3.1 Description

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

- operation with only FIPS approved algorithms as listed in Table 9 - Non-Approved Security Functions,
- 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 PSG firmware without first clearing all protected Keys and CSPs; and
- providing authentication and session management security.

This Security Policy describes a particular PSG Firmware and Hardware. The PSG 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 PSG are validated configurations.

The PSG 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 PSG 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 PSG in “FIPS mode” by simply running the administrative `CTCONF -fF` command from the remote management facility. Once this command is executed the PSG will reject all requests for non-FIPS algorithms or configurations.

3.3 Mode of operation indicator

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

3.4 Invoking mode of operation indicator

An operator may easily view the current PSG mode of operation by simply running the administrative `CTCONF –v` command from the remote management facility. Once this command is executed the PSG 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.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A – Glossary

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
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
DSA	Digital Signature Algorithm
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
MAC	Message Authentication Code
MD2	Message Digest Algorithm 2
MD5	Message Digest Algorithm 5
MD5 HMAC	MD5 Hashed Message Authentication Code
NIST	National Institute of Standards and Technology
NO	Normal Operator
PSG	ProtectServer Gold MkII
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RC2	Rivest’s Code 2
RC4	Rivest’s Code 4
RNG	Random Number Generator

Acronym	Definition
RoHS	Restriction on Hazardous Substances
ROM	Read Only Memory
RSA	Rivest, Shamir and Adleman
RWXZ	Read, Write, Execute, Zero
SDRAM	Synchronous Dynamic Random Access Memory
SHA1	Secure Hash Algorithm
SO	Security Operator
SRAM	Static Random Access Memory
TDES	Triple Data Encryption Standard
USB	Universal Serial Bus
USO	User Security Operator
VGA	Video Graphics Array