Security Policy

Pointsec Cryptographic Module version 1.2

FIPS 140-2

Level 1 Validation

Document Version 1.8

March 6, 2007

Table of Contents

1. INTRODUCTION 3

1.1 PURPOSE 3
1.2 REFERENCES 3
1.3 ACRONYM LIST 3

2. POINTSEC CRYPTO MODULE VERSION 1.2 4

2.1 OVERVIEW 4
2.2 CRYPTOGRAPHIC MODULE 5
2.3 MODULE PORTS AND INTERFACES 5
2.4 ROLES, SERVICES AND AUTHENTICATION 6
2.5 PHYSICAL SECURITY 6
2.6 OPERATIONAL ENVIRONMENT 6
2.7 CRYPTOGRAPHIC KEY MANAGEMENT 7
2.8 SELF-TESTS 8
2.9 DESIGN ASSURANCE 8
2.10 MITIGATION OF OTHER ATTACKS 9

3. OPERATION OF THE POINTSEC CRYPTO MODULE VERSION 1.2 9

1. Introduction

1.1 Purpose

This non-proprietary Cryptographic Module Security Policy for the Pointsec Crypto Module Version 1.2, describes how the Pointsec Crypto Module Version 1.2 meets the Level 1 security requirements of FIPS 140-2. While validation testing was performed on Microsoft Windows 2000 Professional, Microsoft Windows XP Professional, Windows Mobile 5 and Symbian OS 9, it is also capable of running on Microsoft Windows versions 98SE/Me/NT4/Vista. This policy document is part of FIPS 140-2 validation of the Pointsec Crypto Module Version 1.2.

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 Pointsec Crypto Module Version 1.2 in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the Pointsec Crypto Module Version 1.2 application from the following source:

Refer to: http://www.pointsec.com for information on Pointsec products and services as well as answers to technical or sales related questions.

1.3 Acronym list

Acronym	Definition
TDES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
MD5	Message Digest Algorithm 5
RSA	Rivest, Shamir, Adleman Private/Public key algorithm
SHA	Secure Hashing Algorithm
PRNG	Pseudo Random Number Generator

2. Pointsec Crypto Module Version 1.2

2.1 Overview

The Pointsec Crypto Module Version 1.2 (hereinafter referenced as the crypto module) provides cryptographic support for the Pointsec line of products. The crypto module is used to perform cryptographic operations as well as create, manage and delete cryptographic keys.

The cryptographic services provided by the crypto module includes symmetric and asymmetric key based encryption algorithms, message digest, message authentication code, RSA encryption, signature generation and verification, and pseudo random number generation functions.

The crypto module can be used to provide multiple security functions in Pointsec applications. A structured set of APIs can be called to perform these functions. The API set makes the module very flexible, and enables adding crypto functions to new applications without changing the module itself.

Utilizing the crypto module, Pointsec applications can create encryption keys, which can then be used to encrypt data. The APIs provide the ability to encrypt both static data (such as hard disk blocks) as well as data streams (such as browser traffic). The crypto module also provides the ability to perform cryptographic MAC operations and Message Digest operations.

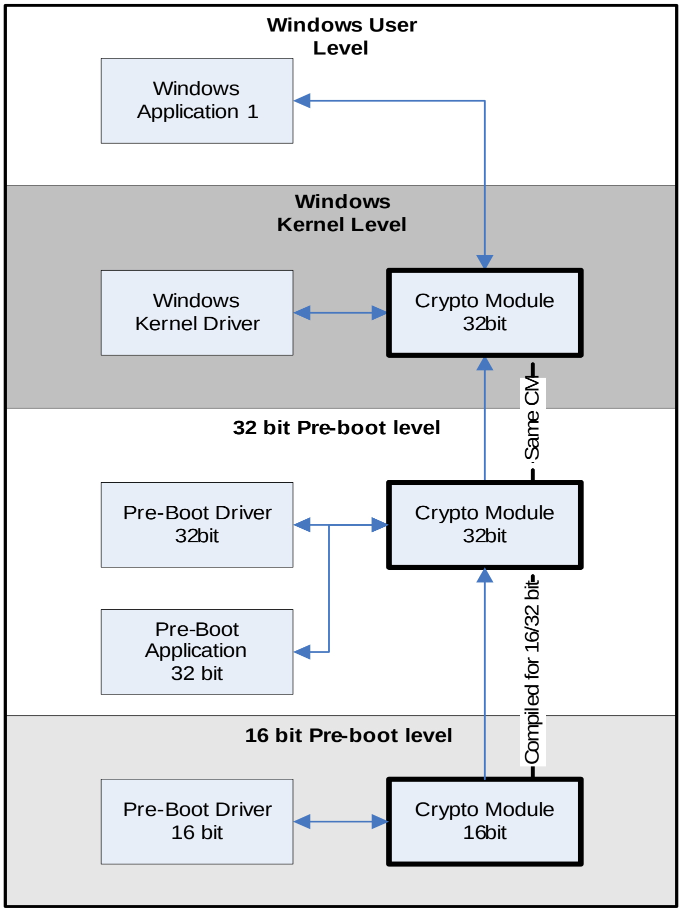

Figure 1 Interaction of Crypto module in different operating system modes on Microsoft Windows (PC) platforms

2.2 Cryptographic Module

The Pointsec Crypto Module Version 1.2 is classified as a multi-chip standalone module for FIPS 140-2 purposes. The module was tested for FIPS compliance on a GPC running Windows 2000 Professional, Windows XP Professional, Windows Mobile 5 and Symbian OS 9 configured in the single user mode. The module is also capable on running on any commercially available IBM compatible PC under Windows 98/98SE/Me/NT4/2000/XP/Vista Operating Systems (OS).

The Windows Cryptographic Module is packaged in the form of one 32-bit module, used by all 32-bit components in the system and one 16-bit module that operates alongside the 32-bit module in the Pre-Boot environment. In the Windows environment the 32-bit module will be used both in kernel mode and in user mode. For Windows Mobile 5 and Symbian OS 9 the module is packaged as a 32-bit dynamic link library (dll) specific to the respective platform.

For the Microsoft Windows (PC) module the relationship between the 16-bit and 32-bit modes is shown in Figure 1 (above). The 16-bit mode provides cryptographic functions during 16 bit pre-boot operation while the 32 bit mode provides crypto functions thereafter. In Microsoft Windows Mobile 5 and Symbian OS 9 the module only operates in 32-bit mode.

2.3 Module Ports and Interfaces

The Pointsec Crypto Module Version 1.2 is classified as a multi-chip standalone module for FIPS 140-2 purposes. As such, the module's cryptographic boundary includes the following:

- Microsoft Windows (PC) binaries: ccore16.bin and ccore32.bin.
- Microsoft Windows Mobile 5 binary: cryptocore.dll
- Symbian OS 9 binary: cryptocore.dll

A PC or mobile device running an operating system and interfacing with the computer, keyboard, mouse screen, floppy drive, CD-ROM drive, speaker, serial ports, parallel ports, and power plug.

The Pointsec Crypto Module Version 1.2 provides a logical interface via an Application Programming Interface (API). The API provided by the module is mapped to the FIPS 140-2 logical interfaces: data input, data output, control input, and status output. All of these physical interfaces are separated into the logical interfaces from FIPS as described in the following table:

FIPS 140-2 Logical Interface	Module Mapping
Data Input Interface	**Parameters passed to the module via the API call**
Data Output Interface	**Data returned by the module via the API call**
Control Input Interface	**Control input through the API function calls**
Status Output Interface	**Information returned via exceptions and calls**
Power Interface	**Does not provide a separate power or maintenance access interface beyond the power interface provided by the computer itself**

Table 1 – FIPS 140-2 Logical Interfaces

2.4 Roles, Services and Authentication

The cryptographic module provides Crypto Officer and User roles. All the services exported by the module are common to both the roles except key zeroization. Only the Crypto-officer is allowed to perform key zeroization. Since the module is validated at security level 1, it does not provide an authentication mechanism.

Exported Services	Supported in 16-bit Mode	Supported in 32-bit Mode	Exported to
PT_RV cryptInitSystem	X	X	User/CO
PT_RV cryptCipherInit		X	User/CO
PT_RV cryptCipherDestroy		X	CO
PT_RV cryptCipherSetParams	X	X	User/CO
PT_RV cryptCipherSetKey	X	X	User/CO
PT_RV cryptCipherSetIV	X	X	User/CO
PT_RV cryptCipherGetIV	X	X	User/CO
PT_RV cryptEncrypt	X	X	User/CO
PT_RV cryptDecrypt	X	X	User/CO
PT_RV cryptDigestInit		X	User/CO
PT_RV cryptDigestDestroy		X	CO
PT_RV cryptDigestCopy		X	User/CO
PT_RV cryptDigestUpdate		X	User/CO
PT_RV cryptDigestFinal		X	User/CO
PT_RV cryptHmacInit		X	User/CO
PT_RV cryptHmacDestroy		X	CO
PT_RV cryptHmacCopy		X	User/CO
PT_RV cryptHmacUpdate		X	User/CO
PT_RV cryptHmacFinal		X	User/CO
PT_RV cryptPrngInit		X	User/CO
PT_RV cryptPrngDestroy		X	CO
PT_RV cryptPrngAddEntropy		X	User/CO
PT_RV cryptPrngReadBytes		X	User/CO
PT_RV cryptPkInit		X	User/CO
PT_RV cryptPkDestroy		X	CO
PT_RV cryptPkSetKey		X	User/CO
PT_RV cryptPkGetKey		X	User/CO
PT_RV cryptPkGenKey		X	User/CO
PT_RV cryptPkSign		X	User/CO
PT_RV cryptPkVerify		X	User/CO
PT_RV cryptPkEncrypt		X	User/CO
PT_RV cryptPkDecrypt		X	User/CO
PT_RV cryptGetFunctionList	X	X	User/CO

Table 2 – Exported Functions

2.5 Physical Security

Since the Pointsec Crypto Module is implemented solely in software, the physical security section of FIPS 140-2 is not applicable.

2.6 Operational Environment

The Cryptographic module's software components are designed to be installed on the targets listed below as indicated in section 2.2 above.

2.6.1 Microsoft Windows

The Cryptographic module's software components are designed to be installed on an IBM-compatible PC running Microsoft Windows Operating Systems Win2000/XP and Vista.

2.6.2 Microsoft Windows Mobile

The Cryptographic module's software components are designed to be installed on a mobile device running Microsoft Windows Mobile 5.

2.6.3 Symbian OS

The Cryptographic module's software components are designed to be installed on a mobile device running Symbian OS 9.

Each software components of the module will implement an approved message authentication code, used to verify the integrity of software component during the power-up self-test (see section on self-test below). While loaded in the memory, the respective target OS will protect all unauthorized access to the Cryptographic module's address memory and process space.

2.7 Cryptographic Key Management

The Pointsec Crypto Module Version 1.2 implements the following algorithms.

The FIPS approved column specifies whether the algorithm is available in the FIPS-mode (non-approved algorithms are not to be used, see section 3 for more information).

Algorithm Type	Algorithm, Modes and Key length	Supported in 16-bit Mode	Supported in 32-bit Mode	FIPS Approved
Symmetric Key	AES - ECB, CBC – 128, 192, 256	X	X	Yes
	DES - ECB, CBC – 64		X	No
	TDES – ECB, CBC – 168	X	X	Yes
	Blowfish ECB, CBC - 56 – 448		X	No
	CAST-128, 256		X	No
Message Digest	MD5 (128)		X	No
	SHS (160, 256, 384, and 512)		X	Yes
	SHS (224)		X	No
HMAC	SHS (160, 256, 384, and 512)		X	Yes
Asymmetric Key	RSA (all mod sizes) encrypt/decrypt		X	No
	RSA (512) PKCS#1 sign/verify		X	No
	RSA (1024, 2048, 4096) PKCS#1 sign/verify		X	Yes
PRNG	X9.31 PRNG		X	Yes

Table 3 – Algorithms list

The following table provides a list of keys and key sizes that can be generated and/or used with the module. Keys are generated or inserted as specified in the API listing.

Key Name	Created	Size(s) in bits	Purpose
AES_key	Inserted	128, 192, 256,	Encryption, Decryption
TDES_key	Inserted	128 (112),192 (168)	Encryption, Decryption
RSA_Private_key	Inserted/Generated	1024, 2048, 4096 mod size	Key transport Decryption and Signing
RSA_Public_key	Inserted/Generated	1024, 2048, 4096 mod size	Key transport Encryption and Verification,
HMAC_SHA1_key	Inserted	160	HMAC creation
HMAC_SHA256_key	Inserted	256	HMAC creation
HMAC_SHA384_key	Inserted	384	HMAC creation
HMAC_SHA512_key	Inserted	512	HMAC creation
TDES_MAC_MIT_key	Hard-coded	192 (168)	Module Integrity Testing
PRNG_key1 (AES Key)	Inserted	256	PRNG Generation

Table 4 – List of Keys

When keys are set for deletion, the key is zeroized by overwriting the keys to ensure it cannot be retrieved.

2.8 Self-Tests

The Pointsec Crypto Module Version 1.2 performs several power-up self-tests including known answer tests for the FIPS Approved algorithms listed in the table below.

The crypto module also performs a self-test integrity check using TDES-MAC with a fixed key to verify the integrity of the module.

Algorithm	Power-up self-test	Conditional self test
AES KAT	Yes	N/A
TDES KAT	Yes	N/A
SHA-1 KAT	Yes	N/A
SHA-256 KAT	Yes	N/A
SHA-384 KAT	Yes	N/A
SHA-512 KAT	Yes	N/A
HMAC-SHA-1 KAT	Yes	N/A
HMAC-SHA-256 KAT	Yes	N/A
HMAC-SHA-384 KAT	Yes	N/A
HMAC-SHA-512 KAT	Yes	N/A
RSA	Yes	Yes
PRNG	Yes	Yes

Table 5 – List of Self tests

The crypto module performs two conditional tests: continuous tests on the PRNG each time it is used to generate random data, and a pair-wise consistency test each time the module generates RSA key pairs.

2.9 Design Assurance

Pointsec maintains versioning for all source code and associated documentation through CVS versioning handling system.

2.10 Mitigation of Other Attacks

The Pointsec Crypto Module Version 1.2 does not employ security mechanisms to mitigate specific attacks.

3. Operation of the Pointsec Crypto Module Version 1.2

The Pointsec Crypto Module Version 1.2 contains both FIPS-approved and non-FIPS-approved algorithms. In FIPS mode only Approved algorithms must be used.

To exemplify what we mean by FIPS mode vs. non-FIPS mode we provide the following example:
If TDES is being used to encrypt plaintext data, then the module is operating in FIPS-mode, but if the Blowfish algorithm was being used, it would not be in FIPS-mode.

While RSA encryption and decryption is not an approved FIPS algorithm it may be used in a FIPS approved mode as part of a key transport mechanism; however, when transporting keys, the operator must use an RSA keypair with a minimum modulus size of 1024-bitsto comply with CMVP requirements.

The Pointsec Crypto Module Version 1.2 is designed for installation and use on a computer configured in single user mode, and is not designed for use on systems where multiple, concurrent users are active.

In order to maximize the entropy provided to the approved PRNG the operator must ensure that the seed and the seed key have different values.