Check Point®
SOFTWARE TECHNOLOGIES INC.

Security Policy

Check Point Crypto Core version 1.3

FIPS 140-2

Level 1 Validation

Document Version 2.1

March 5, 2009

Table of Contents

1. Introduction

1.1 Purpose

This non-proprietary Cryptographic Module Security Policy for the Check Point Crypto Core Version 1.3, describes how the Check Point Crypto Core Version 1.3 meets the Level 1 security requirements of FIPS 140-2. Validation testing for the module was completed on Windows Mobile 6.0..

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/groups/STM/cmvp/.

1.2 References

This document deals only with operations and capabilities of the Check Point Crypto Core Version 1.3 in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the Check Point Crypto Core Version 1.3 application from the following source:

Refer to: http://www.checkpoint.com for information on Check Point 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. Check Point Crypto Core Version 1.3

2.1 Overview

The Check Point Crypto Core Version 1.3 (hereinafter referenced as the crypto module) provides cryptographic support for the Check Point 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 Check Point 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, Check Point 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.

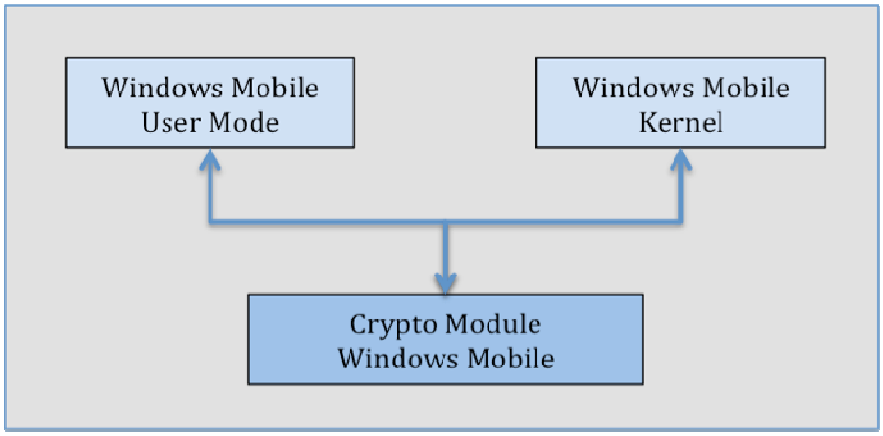

Figure 1 Interaction of Crypto module in different operating system modes on Microsoft Windows Mobile

2.2 Cryptographic Module

The Check Point Crypto Core Version 1.3 is classified as a multi-chip standalone module for FIPS 140-2 purposes. Version 1.3 was tested on Windows Mobile 6.

For Windows Mobile 6 the module is packaged as a 32-bit dynamic link library (dll) specific to the respective platform.

2.3 Module Ports and Interfaces

The Check Point Crypto Core Version 1.3 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 Mobile 6 binary: cryptocore.dll

A mobile device running an operating system and possibly interfacing with external devices connected through any connection method supported by the operating system.

The Check Point Crypto Core Version 1.3 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	Exported to
PT_RV cryptInitSystem	User/CO
PT_RV cryptCipherInit	User/CO
PT_RV cryptCipherDestroy	CO
PT_RV cryptCipherSetParams	User/CO
PT_RV cryptCipherSetKey	User/CO
PT_RV cryptCipherSetIV	User/CO
PT_RV cryptCipherGetIV	User/CO
PT_RV cryptEncrypt	User/CO
PT_RV cryptDecrypt	User/CO
PT_RV cryptDigestInit	User/CO
PT_RV cryptDigestDestroy	CO
PT_RV cryptDigestCopy	User/CO
PT_RV cryptDigestUpdate	User/CO
PT_RV cryptDigestFinal	User/CO
PT_RV cryptHmacInit	User/CO
PT_RV cryptHmacDestroy	CO
PT_RV cryptHmacCopy	User/CO
PT_RV cryptHmacUpdate	User/CO
PT_RV cryptHmacFinal	User/CO
PT_RV cryptPrngInit	User/CO
PT_RV cryptPrngDestroy	CO
PT_RV cryptPrngAddEntropy	User/CO
PT_RV cryptPrngReadBytes	User/CO
PT_RV cryptPkInit	User/CO
PT_RV cryptPkDestroy	CO
PT_RV cryptPkSetKey	User/CO
PT_RV cryptPkGetKey	User/CO
PT_RV cryptPkGenKey	User/CO
PT_RV cryptPkSign	User/CO
PT_RV cryptPkVerify	User/CO
PT_RV cryptPkEncrypt	User/CO
PT_RV cryptPkDecrypt	User/CO
PT_RV cryptGetFunctionList	User/CO

Table 2 – Exported Functions

2.5 Physical Security

Since the Check Point Crypto Core 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, as indicated in section 2.2 above, are designed to be installed on the targets listed below.

2.6.1 Microsoft Windows Mobile

The Cryptographic module's software components are designed to be installed on a mobile device running Microsoft Windows Mobile 6.

Each software component of the module implements 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 Check Point Crypto Core Version 1.3 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	FIPS Approved
Symmetric Key	AES - ECB, CBC – 128, 192, 256	Yes
	DES - ECB, CBC – 64	No
	TDES – ECB, CBC – 168	Yes
	Blowfish ECB, CBC - 56 – 448	No
	CAST-128, 256	No
Message Digest	MD5 (128)	No
	SHS (160, 256, 384, and 512)	Yes
	SHS (224)	No
HMAC	SHS (160, 256, 384, and 512)	Yes
Asymmetric Key	RSA (all mod sizes) encrypt/decrypt	No
	RSA (512) PKCS#1 sign/verify	No
	RSA (1024, 2048, 4096) PKCS#1 sign/verify	Yes
PRNG	X9.31 PRNG	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 Check Point Crypto Core Version 1.3 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

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

2.10 Mitigation of Other Attacks

The Check Point Crypto Core Version 1.3 does not employ security mechanisms to mitigate specific attacks.

3. Operation of the Check Point Crypto Core Version 1.3

The Check Point Crypto Core Version 1.3 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 key pair with a minimum modulus size of 1024-bits to comply with CMVP requirements.

The Check Point Crypto Core Version 1.3 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.