DIGITAL GUARDIAN®

# VERDASYS SECURE CRYPTOGRAPHIC MODULE SOFTWARE VERSION 1.0

## FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level 1
Document Version 0.4
Author: Digital Guardian, Inc.

# CONTENTS

# TABLE OF FIGURES

# LIST OF TABLES

# 1. INTRODUCTION

## 1.1 PURPOSE

This is a non-proprietary Cryptographic Module Security Policy for the Verdasys Secure Cryptographic Module from Digital Guardian, Inc.. This Security Policy describes how the Verdasys Secure Cryptographic Module meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website, which is maintained by the National Institute of Standards and Technology (NIST) and the Communication Security Establishment Canada (CSEC): http://csrc.nist.gov/groups/STM/index.html.

The Verdasys Secure Cryptographic Module is referred to in this document as VSEC, the cryptographic module, or the module.

## 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 module from the following sources:

- The Digital Guardian website (http://www.digitalguardian.com) contains information on the full line of products from Digital Guardian.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

## 1.3 DOCUMENT ORGANIZATION

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Digital Guardian. With the exception of this Non-Proprietary Security Policy, the FIPS 140- 2 Submission Package is proprietary to Digital Guardian and is releasable only under appropriate non-disclosure agreements.  For access to these documents, please contact Digital Guardian.

# 2. VSEC Module

This section describes the Verdasys Secure Cryptographic Module from Digital Guardian, Inc.

## 2.1 Overview

Digital Guardian is a pioneer in Enterprise Information Protection (EIP), a data-centric and risk-based approach to security that focuses on information flow and human interaction across an organization. Digital Guardian's Digital Guardian product provides the foundation necessary for implementing an EIP platform. Through its unique architecture, the Digital Guardian product reduces the risk of data loss or misuse by its realtime enforcement of corporate security policies, automated encryption of files and emails, and automatic discovery and classification of sensitive data. The Digital Guardian product protects information at rest, in use, and in motion, mitigating both internal and external risks. Its sophisticated tracking and reporting capabilities provide visibility into how information is used and where it is located. This activity data can then be correlated into actionable intelligence. It can also provide powerful forensic support during investigations into fraud, theft, and malicious activity.

Through the enterprise-wide installation of a kernel and user mode component called *DG Agent*, the Digital Guardian product provides data protection at the point of use, where it is most vulnerable. Once installed, *DG Agent* operates invisibly on desktops, laptops, and servers. The integrated framework also consists of a centralized *DG Server* and *DG Management Console*, comprising a Web-based command center for the Digital Guardian platform. Figure 1 below gives an overview of the Digital Guardian architecture.

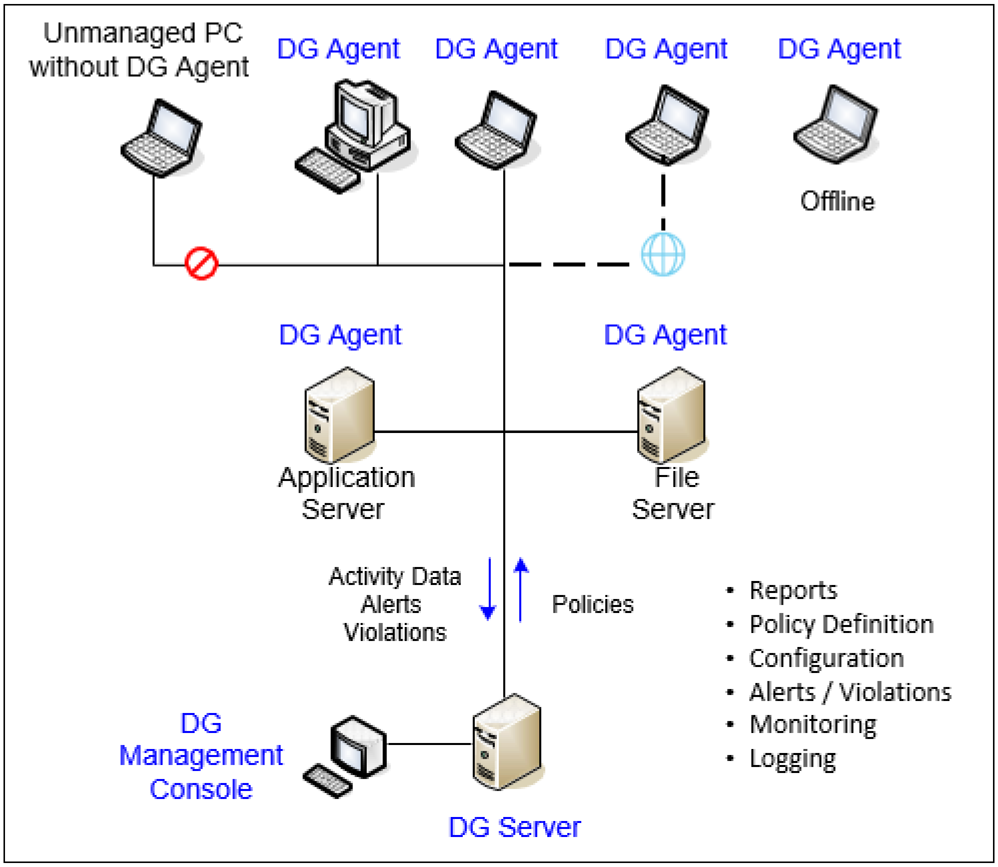

**Figure 1: Digital Guardian Architecture**

Digital Guardian's primary use of cryptography is in the following two components: the Adaptive Mail Encryption module (AME) and the Adaptive File Encryption module (AFE). Based on content and security policy rules, AME and AFE encrypt and decrypt files, emails, and attachments selectively and automatically, in most cases without end-user knowledge or action.

The Verdasys Secure Cryptographic Module, VSEC, is a software module that provides cryptographic functionality for Digital Guardian's AME and AFE modules, and other Digital Guardian add-on components. Within the Digital Guardian architecture, it resides in *DG Agent*. It is custom designed and written by Digital Guardian in the 'C' programming language and is identical, at the source code level, for the supported operating system (OS) platforms as shown.

Verdasys Secure Cryptographic Module has been validated on the following platforms and no claims can be made as to correct operation of the Verdasys Secure Cryptographic Module or the security strengths of the generated keys when operating on a platform that is not listed on the validation certificate:

- Windows XP 32-bit
- Windows XP 64-bit (single-user mode)

In addition to the validation, the Verdasys Secure Cryptographic Module has been tested by Digital Guardian, Inc. on the following platforms:

- Windows 7, 32-bit and 64-bit
- Windows Server 2008 R2, 64-bit
- Windows 10. 32-bit and 64-bit
- Windows Server 2012 R2, 64-bit

This module includes implementations of the following FIPS-Approved algorithms:

- Advanced Encryption Standard (AES)
- Secure Hash Algorithm (SHA)
- Keyed-Hash Message Authentication Code (HMAC)
- RSA[1] signature generation and verification
- SP 800-90A Deterministic Random Bit Generator (DRBG)

The Verdasys Secure Cryptographic Module always operates in a FIPS-Approved mode of operation and is validated at the following FIPS 140-2 Section levels:

[1] RSA: Rivest, Shamir, Adleman

| 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 Model | 1 |
| 5 | Physical Security | N/A |
| 6 | Operational Environment | 1 |
| 7 | Cryptographic Key Management | 1 |
| 8 | EMI/EMC[2] | 1 |
| 9 | Self-tests | 1 |
| 10 | Design Assurance | 1 |
| 11 | Mitigation of Other Attacks | N/A |

**Table 1: Security Level Per FIPS 140-2 Section**

## 2.2 MODULE SPECIFICATION

The Verdasys Secure Cryptographic Module is a software module with a multi-chip standalone embodiment. The overall security level of the module is 1. The following sections will define the physical and logical boundary of the VSEC module.

### 2.2.1. Physical Cryptographic Boundary

As a software cryptographic module, there are no physical protection mechanisms implemented. The module must rely on the physical characteristics of the host system. The physical boundary of the cryptographic module is defined by the hard enclosure around the host system on which it runs. The module supports the physical interfaces of a General Purpose Computer (GPC). See Figure 2 below for a standard GPC block diagram.

[2] EMI/EMC: Electromagnetic Interference / Electromagnetic Capability

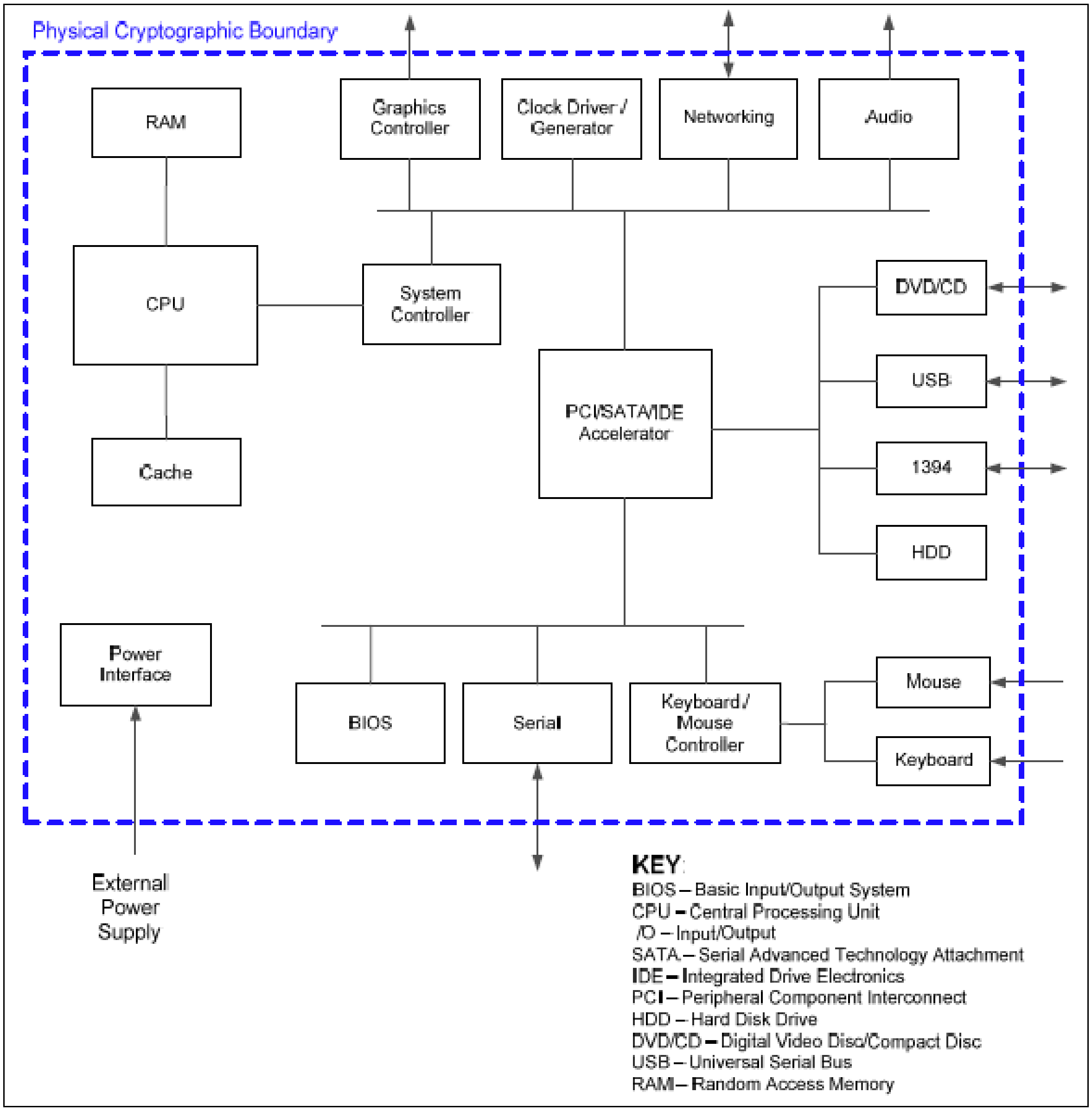
Physical Cryptographic Boundary
RAM
Graphics Controller
Clock Driver / Generator
Networking
Audio
CPU
System Controller
DVD/CD
USB
PCI/SATA/IDE Accelerator
1394
Cache
HDD
Power Interface
Mouse
BIOS
Serial
Keyboard / Mouse Controller
Keyboard
External Power Supply
KEY:
BIOS – Basic Input/Output System
CPU – Central Processing Unit
I/O – Input/Output
SATA – Serial Advanced Technology Attachment
IDE – Integrated Drive Electronics
PCI – Peripheral Component Interconnect
HDD – Hard Disk Drive
DVD/CD – Digital Video Disc/Compact Disc
USB – Universal Serial Bus
RAM – Random Access Memory

**Figure 2: Standard GPC Block Diagram**

### 2.2.2. Logical Cryptographic Boundary

Figure 3 shows a logical block diagram of the module executing in memory and its interactions with surrounding components, as well as the module's logical cryptographic boundary. The module's services (or exported functions) are designed to be called by other Digital Guardian kernel mode drivers, with which it has active sessions. For clarity, the diagram only depicts one active session with the module.

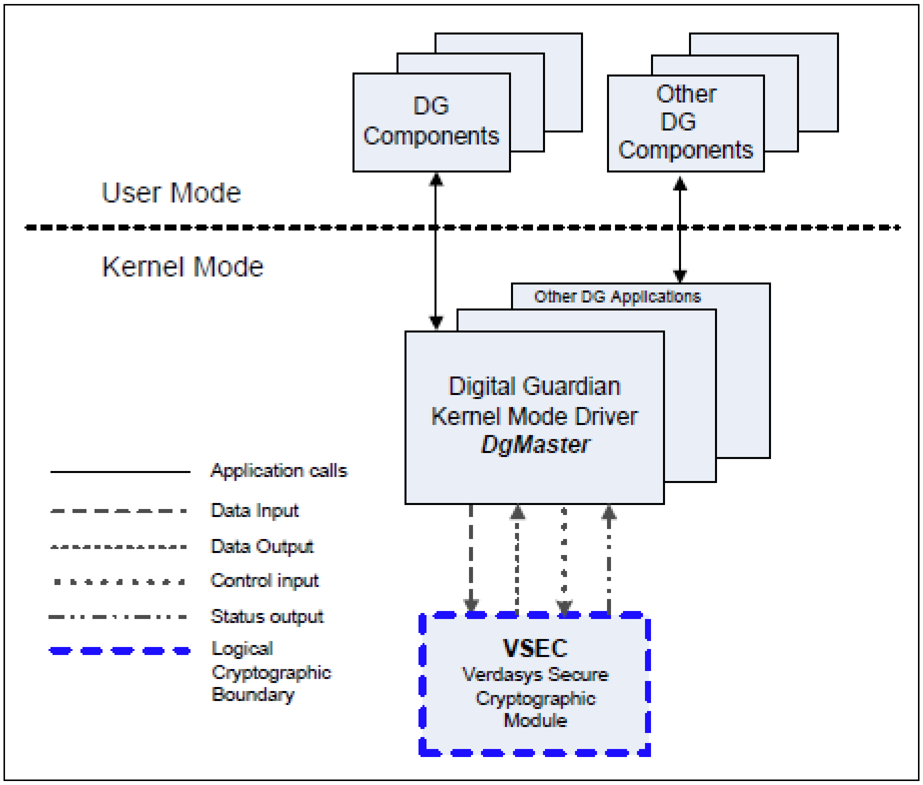

**Figure 3: Logical Block Diagram and Cryptographic Boundary**

## 2.3 MODULE INTERFACES

The module's logical interfaces exist in the software as an Application Programming Interface (API). Physically, ports and interfaces are considered to be those of the GPC. Both the API and physical interfaces can be categorized into following interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface
- Power Interface

A mapping of the FIPS 140-2 logical interfaces, the physical interfaces, and the module interfaces can be found in the following table:

| FIPS 140-2<br>Interface | Physical Interface | Module Interface (API) |
|---|---|---|
| Data Input | Keyboard, mouse, serial/USB/network ports, DVD/CD drive | Function calls that accept, as their arguments, data or pointers to data to be processed by the module |
| Data Output | Monitor, DVD/CD drive, serial/USB/network/audio ports | Arguments for a function that specify where the result of the function is stored |
| Control Input | Keyboard, mouse, network port, power switch | Function calls and arguments that initiate and control the operation of the module. |
| Status Output | Serial/USB/network ports, monitor | Return values from function calls and error messages |
| Power Input | Power Interface | N/A |

**Table 2: FIPS Interface Mappings**

## 2.4 ROLES AND SERVICES

The module supports the following roles: Crypto-Officer (CO) and User. Both roles are implicitly assumed when services are executed. All services offered by the module are available to both the CO and User and are itemized below in Table 3.

**Note 1:** The following definitions are used in the "CSP[3] and Type of Access" column in Table 3.

***R – Read:*** *The plaintext CSP is read by the service.*

***W – Write:*** *The CSP is established, generated, modified**,** or zeroized by the service.*

***X – Execute:*** *The CSP is used within an Approved (or allowed) security function*

**Note 2:** Input parameters of an API call that are not specifically plaintext, ciphertext, or a key are NOT itemized in the "Input" column, since it is assumed that most API calls will have such parameters.

**Note 3:** The "Input" and "Output" columns are with respect to the module's logical boundary.

[3] CSP: Critical Security Parameter

| Service | Input | Output | CSP and Type of Access |
|---|---|---|---|
| Load and initialize module | None | Status | None |
| Run self-tests on demand | API call parameters | Status | None |
| Create session with application | API call parameters | Status | None |
| Close session with application | API call parameters | Status | None |
| Generate random number | API call parameters | Status, random bits | None |
| Generate Hash (SHA-1, SHA- 224, SHA-256, SHA-384, SHA-<br>512) | API call parameters, plaintext | Status, hash | None |
| Generate Keyed Hash (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) | API call parameters, key, plaintext | Status, hash | HMAC key - RX |
| Generate key | API call parameters | Status, key | AES, HMAC key – W |
| Zeroize key | API call parameters | Status | AES, HMAC, RSA private key – W |
| Delete key | API call parameters | Status | AES, HMAC, RSA private key - W |
| Import key | API call parameters, key | Status | AES, HMAC, RSA private key – W |
| Export key | API call parameters | Status, key | AES, HMAC, RSA private key – R |
| Create crypto contexts | API call parameters | Status | None |
| Delete crypto contexts | API call parameters | Status | None |
| Symmetric encryption | API call parameters, plaintext | Status, ciphertext | AES key – RX |
| Symmetric decryption | API call parameters, ciphertext | Status, plaintext | AES key – RX |
| Check RSA key | API call parameters | Status | RSA private key – R |
| RSA encryption | API call parameters, plaintext | Status, ciphertext | RSA private key – RX |
| RSA decryption | API call parameters, ciphertext | Status, plaintext | RSA private key – RX |

| Service | Input | Output | CSP and Type of Access |
|---|---|---|---|
| Signature Generation | API call parameters, key, plaintext | Status, signed data | RSA private key – RX |
| Signature Verification | API call parameters, signed data | Status, result | RSA public key – RX |

**Table 3: Mapping Services to Inputs, Outputs, CSPs, and Type of Access**

## 2.5 PHYSICAL SECURITY

The Verdasys Secure Cryptographic Module is a software module only and does not include physical security mechanisms. Thus, the FIPS 140-2 requirements for physical security are not applicable.

## 2.6 OPERATIONAL ENVIRONMENT

The module, intended for use on a GPC, was tested and found to be compliant with FIPS 140-2 requirements on commercially available GPCs with Intel Core 2 Quad processors running Windows XP 32- bit and Windows XP 64-bit operating systems. For FIPS 140-2 compliance, these are considered to be single user operating systems when configured as such by the CO.

## 2.7 CRYPTOGRAPHIC KEY MANAGEMENT

The module implements the following FIPS-Approved algorithms:

| Algorithm | Certificate Number |
|---|---|
| FIPS 197 AES–CBC[4] with 128, 192, and 256 bit key sizes,<br>FIPS 197 AES-CTR[5], ECB[6] with 256 bit key sizes | 1384 |
| FIPS 186-2 RSA (RSASSA[7]-PKCS1[8]-v1_5) Signature Generation – 2048, 3072, 4096 bit key sizes | 677 |
| FIPS 186-2 RSA (RSASSA-PKCS1-v1_5) Signature Verification – 1024, 1536, 2048, 3072, 4096 bit key sizes | |

[4] CBC: Cipher Block Chaining mode

[5] CTR: Counter mode

[6] ECB: Electronic Code Book

[7] RSASSA: RSA Signature Scheme with Appendix

[8] PKCS1: Public-Key Cryptography Standard #1

| | |
|---|---|
| FIPS 180-4 SHA-1, FIPS 180-4 SHA-224, FIPS 180-4 SHA-256, FIPS 180-4 SHA-384, FIPS 180-4 SHA-512 | 1261 |
| FIPS 198-1 HMAC-SHA-1, FIPS 198-1 HMAC-SHA-224, FIPS 198-1 HMAC-SHA-256, FIPS 198-1 HMAC-SHA-384, FIPS 198-1 HMAC-SHA-512 | 814 |
| SP[9] 800-90A Hash_DRBG | 50 |

**Table 4: FIPS-Approved Algorithm Implementations**

Additionally, the module utilizes the following allowed algorithms used in an Approved mode of operation:

- RSA PKCS#1 - 2048, 3072, 4096 bit keys (Key wrapping; key establishment methodology provides 112 to 150 bits of encryption strength)
- A non-Approved NDRNG[10] used for gathering entropy as input to the Approved SP 800-90A Hash_DRBG

Additionally, the module implements the following algorithms which cannot be used in the Approved mode of operation: RSA PKCS#1 – 1024, 1536 keys.

The CSPs supported by the module are shown in Table 5 below.

**Note:** The "Input" and "Output" columns in Table 5 are in reference to the module's physical boundary. In reference to its logical boundary, all keys can be input to and output from the module using API calls.

| CSP/Key | CSP/Key Type | Generation / Input | Output | Storage | Zeroization | Use |
|---|---|---|---|---|---|---|
| FIPS 197 AES key | FIPS 197 AES 128-bit FIPS 197 AES 192-bit FIPS 197 AES 256-bit | Generation: Internally<br>Input: Via API call | None | Plaintext in volatile memory | By API call, power cycle | Encryption, decryption |
| FIPS 198-1 HMAC key | FIPS 198-1 HMAC-SHA-1<br>FIPS 198-1 HMAC-SHA-224<br>FIPS 198-1 HMAC-SHA-256<br>FIPS 198-1 HMAC-SHA-384<br>FIPS 198-1 HMAC-SHA-512 | Generation: Internally<br>Input: Via API call | None | Plaintext in volatile memory | By API call, power cycle | Message Authentication |
| FIPS 186-2 RSA private key | FIPS 186-2 RSA 2048, 3072, 4096-bit | Input: Via API call | Via API call | Plaintext in volatile memory | By API call, power cycle | Signature generation, Key Establishment |

[9] SP: Special Publications

[10] NDRNG: Non-Deterministic Random Number Generator

| CSP/Key | CSP/Key Type | Generation / Input | Output | Storage | Zeroization | Use |
|---|---|---|---|---|---|---|
| FIPS 186-2 RSA public key | FIPS 186-2 RSA 1024, 1536,2048, 3072, 4096-bit | Input: Via API call | Via API call | Plaintext in volatile memory | By API call, power cycle | Signature verification, Key Establishment |
| DRBG entropy input | Entropy (256-bits) | Generated internally | None | Plaintext in volatile memory | By API call, power cycle | Instantiate DRBG |
| DRBG seed | Seed (440-bits) | Generated by DRBG mechanisms | None | Plaintext in volatile memory | By API call, power cycle | Instantiate DRBG |
| DRBG C Value | Internal State Value (440-bits) | Generated by DRBG mechanisms | None | Plaintext in volatile memory | By API call, power cycle | Random Number Generation |
| DRBG V Value | Internal State Value (440-bits) | Generated by DRBG mechanisms | None | Plaintext in volatile memory | By API call, power cycle | Random Number Generation |

**Table 5: List of Cryptographic Keys, Key Components, and CSPs**

## 2.8 SELF-TESTS

The Verdasys Secure Cryptographic Module performs the following self-tests and known-answer tests (KATs) at power-up:

- Software integrity check using HMAC-SHA-256
- Known Answer Tests (KATs)
  - AES-CBC 128, 192, and 256 bit key encrypt/decrypt
  - AES-CTR 256 bit key encrypt/decrypt
  - AES-ECB 256 bit key encrypt/decrypt
  - HMAC-SHA-1
  - HMAC-SHA-224
  - HMAC-SHA-256
  - HMAC-SHA-384
  - HMAC-SHA-512
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384

- SHA-512
- RSA signature generation/verification
- RSA encryption/decryption
- SP 800-90A Hash-DRBG

The Verdasys Secure Cryptographic Module performs the following conditional self-tests:

- Continuous DRBG test
- Continuous RNG test on the non-Approved NDRNG
- SP800-90A Hash-DRBG Health Tests

If a self-test fails, the module will enter an error state and be unloaded. While in an error state, the module inhibits all data output and does not provide any cryptographic functionality until the error state is cleared.

## 2.9 MITIGATION OF OTHER ATTACKS

This section is not applicable.  The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

# 3. SECURE OPERATION

The Verdasys Secure Cryptographic Module meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in the FIPS-Approved mode of operation.

## 3.1 INITIAL SETUP

The cryptographic module is included with the Digital Guardian application with which it will be used. With Digital Guardian, the VSEC module can be installed by following the installation procedures found in the *Digital Guardian Installation and Upgrade Guide*. This will install the appropriate VSEC 32- or 64-bit driver depending on the processor and OS.

After installation, the module requires no set-up, as it only executes in a FIPS-Approved mode of operation. When the module is powered up, it runs the power-on self-tests. If the power-up self-tests pass, the module is deemed to be operating in FIPS mode.

## 3.2 CRYPTO OFFICER GUIDANCE

VSEC is designed for use by Digital Guardian applications such as the Digital Guardian product. In addition to providing for the persistent storage, secure transport, and management of cryptographic keys and CSPs, these applications request cryptographic services to be performed by the module, such as data encryption. They instantiate the data types required by the cryptographic module’s API, and then pass data references to the module so that cryptographic operations can be performed and results accessed by the calling application. VSEC does not input, output, or persistently store CSPs with respect to the physical boundary. It is the responsibility of the calling application to provide persistent storage of cryptographic keys and CSPs, and to ensure that keys are transmitted in a secure manner.

The CO must ensure that the host GPC is placed into single user mode.

The CO is required to use HMAC key lengths ≥ 80 bits (through 2010) and key lengths ≥ 112 bits (beyond 2010) to ensure the security strength of the keyed hash function.

## 3.3 USER GUIDANCE

Digital Guardian applications, such as the Digital Guardian product, employ the services of VSEC to provide information protection to their customers using FIPS Approved cryptographic services. These applications are designed to use their kernel mode components to make function calls to the VSEC export driver via the module’s API. Digital Guardian applications manage use of the module on behalf of the end user, who does not directly interface with the module.

# 4. Acronyms

| Acronym | Definition |
|---|---|
| AES | Advanced Encryption Standard |
| AFE | Adaptive File Encryption |
| AME | Adaptive Mail Encryption |
| API | Application Programming Interface |
| CBC | Cipher Block Chaining |
| CMVP | Cryptographic Module Validation Program |
| CO | Crypto Officer |
| CSEC | Communications Security Establishment Canada |
| CSP | Critical Security Parameter |
| CTR | Counter |
| DG | Digital Guardian |
| DRBG | Deterministic Random Bit Generator |
| ECB | Electronic Code Book |
| EIP | Enterprise Information Protection |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| FIPS | Federal Information Processing Standard |
| GPC | General Purpose Computer |
| HMAC | (Keyed-) Hash Message Authentication Code |
| KAT | Known Answer Test |
| NIST | National Institute of Standards and Technology |
| NVLAP | National Voluntary Laboratory Accreditation Program |
| OS | Operating System |
| PKCS | Public-Key Cryptography Standards |
| PRNG | Pseudo Random Number Generator |
| RNG | Random Number Generator |
| RSA | Rivest, Shamir, and Adleman |
| SHA | Secure Hash Algorithm |
| SP | Special Publication |