Verdasys, Inc.

Verdasys Secure Cryptographic Module

Software Version: 1.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.2

Prepared for:

VERDASYS

Verdasys, Inc.

404 Wyman Street, Suite 320
Waltham, MA 22030

Phone: (781) 788-8180
Email: info@verdasys.com
http://www.verdasys.com

Prepared by:

Corsec

Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com

Table of 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 Verdasys, 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 Verdasys website (http://www.verdasys.com) contains information on the full line of products from Verdasys.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2010.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 Verdasys. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Verdasys and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Verdasys.

2 VSEC Module

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

2.1 Overview

Verdasys 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. Verdasys' Digital Guardian provides the foundation necessary for implementing an EIP platform. Through its unique architecture, Digital Guardian 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. Digital Guardian 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*, Digital Guardian 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.

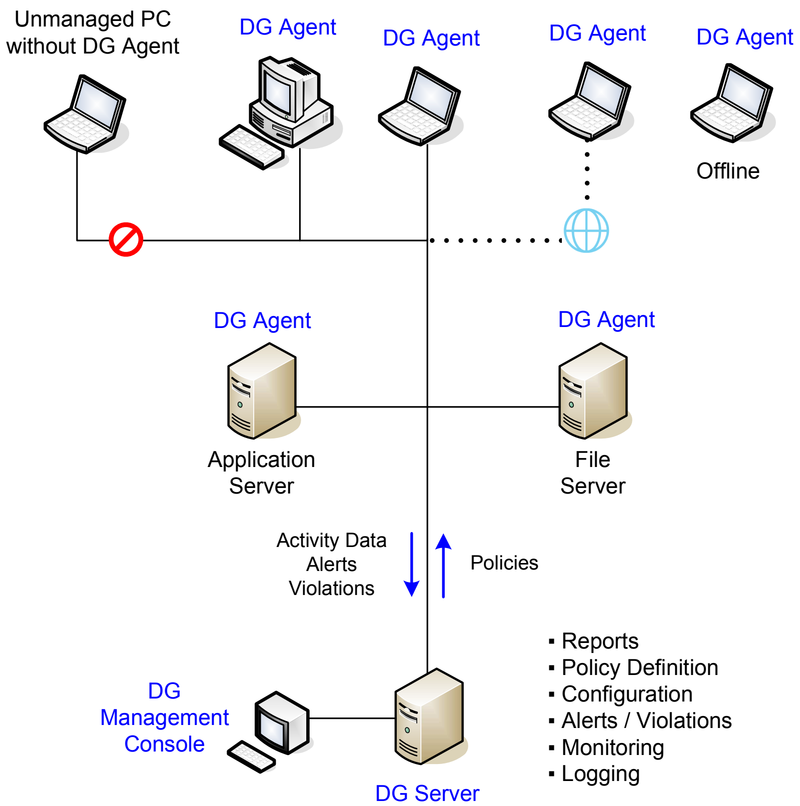


Figure 1 – Digital Guardian Architecture

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 Verdasys add-on components. Within the Digital Guardian architecture, it resides in both *DG Agent* and *DG Server*. It is custom designed and written by Verdasys in the 'C' programming language and is identical, at the source code level, for the following supported operating system (OS) platforms:

- Windows XP, 32-bit and 64-bit
- Windows 7, 32-bit and 64-bit
- Windows Vista, 32-bit and 64-bit
- Windows Server 2003, 32-bit and 64-bit
- Windows Server 2008, 64-bit

The 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 800-90 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:

Table 1 – Security Level Per FIPS 140-2 Section

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

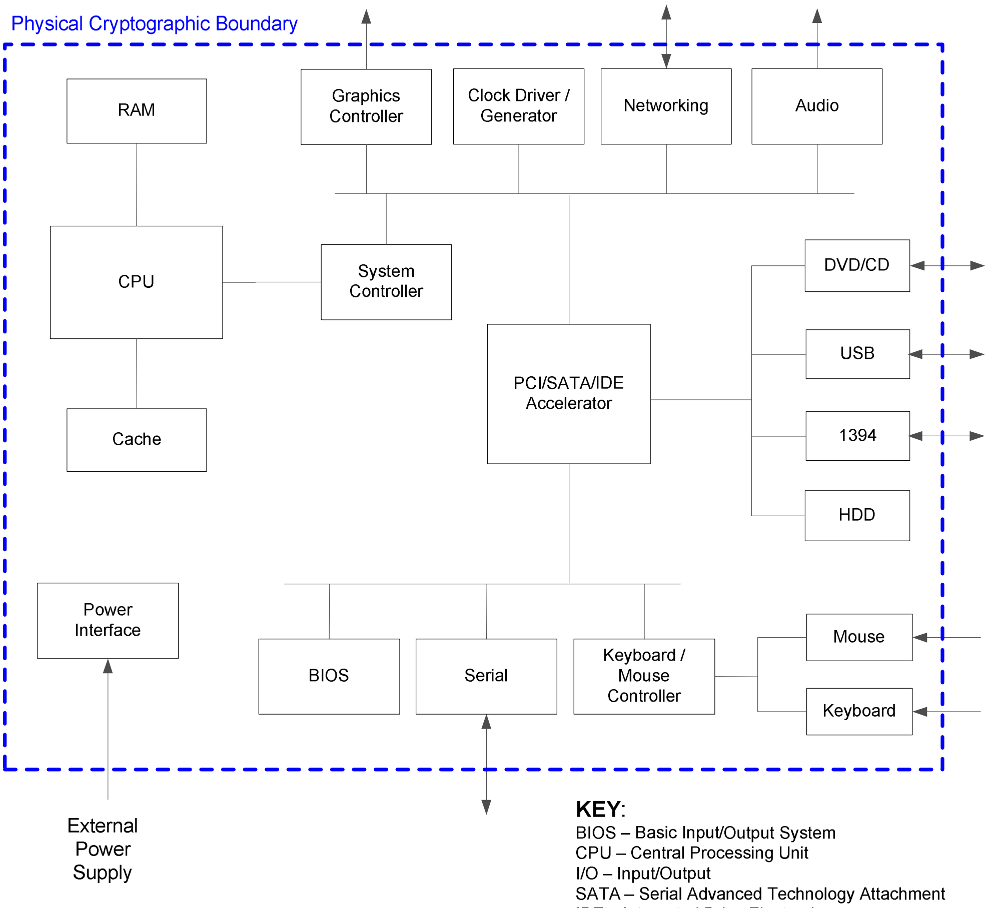
[1] RSA – Rivest, Shamir, Adleman
[2] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

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.



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 Verdasys kernel mode drivers, with which it has active sessions. For clarity, the diagram only depicts one active session with the module.

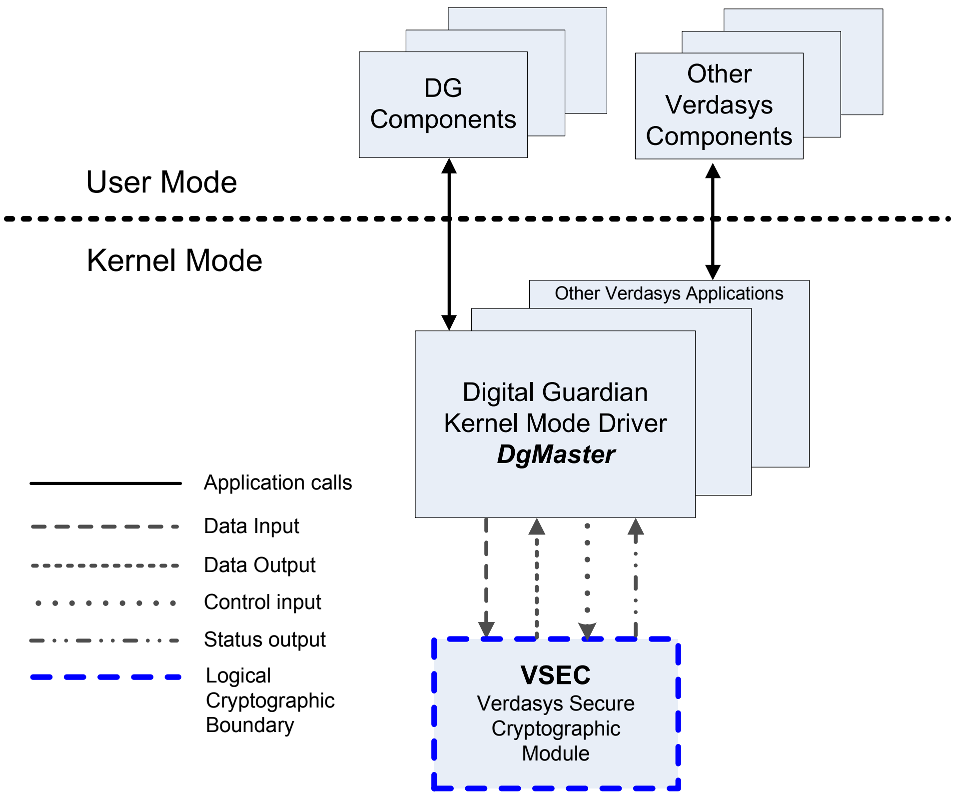


Figure 3 – Logical Block Diagram and Cryptographic Boundary

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:

Table 2 – FIPS Interface Mappings

FIPS 140-2 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

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.

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

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

[3] CSP – Critical Security Parameter

Service	Input	Output	CSP and Type of Access
Generate Hash (SHA-1, SHA-224, SHA-256, SHA-384, SHA-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
Signature Generation	API call parameters, key, plaintext	Status, signed data	RSA private key – RX
Signature Verification	API call parameters, signed data	Status, result	None

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:

Table 4 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES–CBC[4] with 128, 192, and 256 bit key sizes, AES- CTR[5], ECB[6] with 256 bit key sizes	1384
RSA (RSASSA[7]-PKCS1[8]-v1_5) Signature Generation – 2048, 3072, 4096 bit key sizes	677
RSA (RSASSA-PKCS1-v1_5) Signature Verification – 1024, 1536, 2048, 3072, 4096 bit key sizes	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	1261
HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	814
SP[9] 800-90 Hash_DRBG	50

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

- RSA PKCS#1 - 1024, 1536, 2048, 3072, 4096 bit keys (Key wrapping; key establishment methodology provides 80 to 150 bits of encryption strength)
- A non-Approved RNG[10] used for gathering entropy as input to the Approved SP 800-90 Hash_DRBG

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.

Table 5 – List of Cryptographic Keys, Key Components, and CSPs

CSP/Key	CSP/Key Type	Generation / Input	Output	Storage	Zeroization	Use
AES key	AES 128-bit AES 192-bit AES 256-bit	Generation: Internally Input: Via API call	None	Plaintext in volatile memory	By API call, power cycle	Encryption, decryption
HMAC	HMAC-SHA-1	Generation:	None	Plaintext in	By API call,	Message

[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
[9] SP – Special Publication
[10] RNG – Random Number Generator

CSP/Key	CSP/Key Type	Generation / Input	Output	Storage	Zeroization	Use
key	HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	Internally Input: Via API call		volatile memory	power cycle	Authentication
RSA private key	RSA 1024, 1536, 2048, 3072, 4096-bit	Input: Via API call	Via API call	Plaintext in volatile memory	By API call, power cycle	Signature generation, Key Establishment
RSA public key	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 input	RNG seed	Generated internally	None	Plaintext in volatile memory	By API call, power cycle	Instantiate DRBG

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 800-90 Hash-DRBG

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

- Continuous DRBG test
- Continuous RNG test

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 Verdasys 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 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 Verdasys applications such as Digital Guardian. 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

Verdasys applications, such as Digital Guardian, 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. Verdasys applications manage use of the module on behalf of the end user, who does not directly interface with the module.

4 Acronyms

Table 6 – 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

Prepared by:
Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com