FIPS 140-2 Non-Proprietary Security Policy

Guidance Software EnCase Cryptographic Engine Version 1.0

Document Version 0.3

July 29, 2014

Prepared For:

Guidance Software, Inc.

215 North Marengo Avenue, Suite 250

Pasadena, CA 91101

www.guidancesoftware.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides a non-proprietary FIPS 140-2 Security Policy for the EnCase Cryptographic Engine Version 1.0.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment of Canada (CSEC) Cryptographic Module Validation Program (CMVP) run the FIPS 140 program. The NVLAP accredits independent testing labs to perform FIPS 140 testing; the CMVP also validates test reports for products meeting FIPS 140 validation. *Validated* is the term given to a module that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the EnCase Cryptographic Engine Version 1.0 from Guidance Software provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document contains details on the module's cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

The Guidance Software EnCase Cryptographic Engine Version 1.0 may also be referred to as the "module" in this document.

1.3 External Resources

The Guidance Software website (http://www.guidancesoftware.com) contains information on Guidance Software products. The Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2014.htm) contains links to the FIPS 140-2 certificate and Guidance Software contact information.

1.4 Notices

This document may be freely reproduced and distributed in its entirety without modification.

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
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
DVD	Digital Video Disk
DVI	Digital Video Interface
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GPC	General Purpose Computer
GSI	Guidance Software Inc
GUI	Graphical User Interface
HDMI	High Definition Multimedia Interface
HMAC	(Keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
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
RSA	Rivest, Shamir, and Adleman
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SP	Special Publication
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
VGA	Video Graphics Adaptor

Table 1 – Acronyms and Terms

2 Guidance Software EnCase Cryptographic Engine Version 1.0

2.1 Product Overview

EnCase® Enterprise has changed the landscape of enterprise and computer investigations by providing comprehensive forensic-level visibility. The solution can securely investigate/analyze multiple machines simultaneously over the LAN/WAN at the disk and memory level. EnCase® Enterprise is a scalable platform that integrates seamlessly with your existing systems to create an enterprise investigative infrastructure. This cutting-edge solution can be tailored and extended to meet your unique needs, including the automation of time-consuming investigative processes, incident response and eDiscovery.

2.2 Cryptographic Module Specification

The module is the Guidance Software EnCase Cryptographic Engine Version 1.0, which is a software shared library that provides cryptographic services required by Guidance Software host applications. The module is a software-only module installed on a multi-chip standalone device, such as a General Purpose Computer running a General Purpose Operating System.

All operations of the module occur via calls from the Guidance Software applications and their respective internal daemons/processes. As such there are no untrusted services calling the services of the module, as APIs are not exposed.

2.2.1 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
Electromagnetic Interference / Electromagnetic Compatibility	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 2 – Validation Level by FIPS 140-2 Section

2.2.2 Approved Cryptographic Algorithms

The module's cryptographic algorithm implementations have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

Algorithm	CAVP Certificate
AES ECB, CBC [128, 192, 256 bit key sizes]	32-bit: 2682 64-bit: 2683
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512	32-bit: 1669 64-bit: 1670
RSA X9.31, PKCS #1 V.1.5, PKCS#1 V.2.1 (SHA256 - PSS)	32-bit: 1382 64-bit: 1383
SHA-1, SHA-256, SHA-512	32-bit: 2253 64-bit: 2254

Table 3 – FIPS-Approved Algorithm Certificates

The bound RSAENH module provides random numbers to the Guidance Software EnCase Cryptographic Engine, and the cryptographic algorithms are implemented by the Guidance Software EnCase Cryptographic Engine module.

2.2.3 Non-Approved Cryptographic Algorithms

The module does not implement any non-approved algorithms in FIPS mode.

The following algorithms are deprecated for digital signature generation and will be disallowed according to timelines specified in NIST SP 800-131A:

- RSA (1024-bit)
- SHA-1
- HMAC-SHA1

2.3 Module Interfaces

The figure below shows the module's physical and logical block diagram:

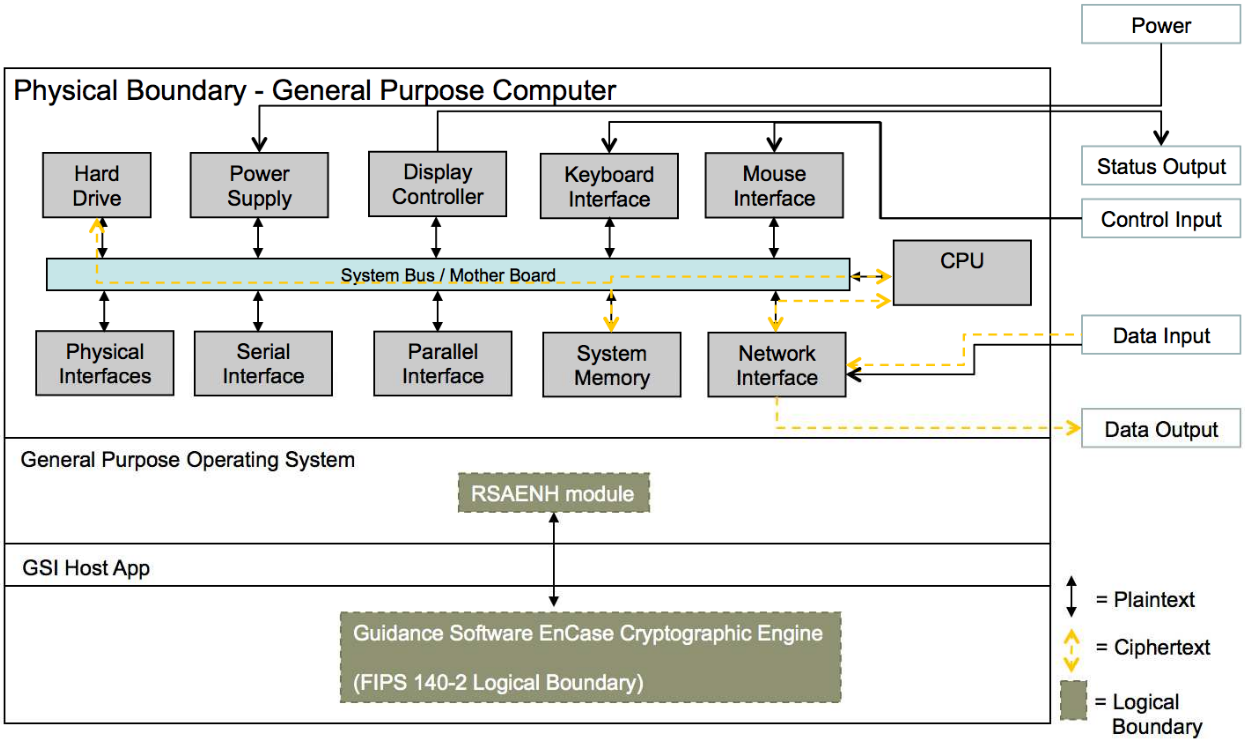

Figure 1 – Module Boundary and Interfaces Diagram

The interfaces (ports) for the physical boundary include the computer keyboard port, CDROM drive, floppy disk, mouse, network port, parallel port, USB ports, monitor port and power plug. When operational, the module does not transmit any information across these physical ports because it is a software cryptographic module. Therefore, the module's interfaces are purely logical and are provided through the Application Programming Interface (API) that a calling daemon can operate. The logical interfaces expose services that applications directly call, and the API provides functions that may be called by a referencing application (see Section 2.4 – Roles, Services, and Authentication for the list of available functions). The module distinguishes between logical interfaces by logically separating the information according to the defined API.

The API provided by the module is mapped onto the FIPS 140- 2 logical interfaces: data input, data output, control input, and status output. Each of the FIPS 140- 2 logical interfaces relates to the module's callable interface, as follows:

FIPS 140-2 Interface	Logical Interface	Module Physical Interface
Data Input	Input parameters of API function calls	USB ports, network ports, serial ports, SCSI/SATA ports, DVD, audio Ports
Data Output	Output parameters of API function calls	Display (e.g. VGA, HDMI, DVI, etc.), USB ports, network ports, serial ports, SCSI/SATA ports, audio ports, DVD

FIPS 140-2 Interface	Logical Interface	Module Physical Interface
Control Input	API function calls	USB ports, network ports, serial ports, power switch
Status Output	Function calls returning status information and return codes provided by API function calls.	Display, serial ports, network ports
Power	None	Power supply/connector

Table 4 – Logical Interface / Physical Interface Mapping

As shown in Figure 1 – Module Boundary and Interfaces Diagram and Table 5 – Module Services and Descriptions, the output data path is provided by the data interfaces and is logically disconnected from processes performing key generation or zeroization. No key information will be output through the data output interface when the module zeroizes keys. No key information is output during key generation.

2.4 Roles, Services, and Authentication

The module supports a Crypto Officer and a User role. The module does not support a Maintenance role. The User and Crypto-Officer roles are implicitly assumed by the entity accessing services implemented by the Module.

2.4.1 Operator Services and Descriptions

The module supports services that are available to users in the various roles. All of the services are described in detail in the module's user documentation. The following table shows the services available to the various roles and the access to cryptographic keys and CSPs resulting from services:

Service	Roles	Cryptographic Keys and CSPs	Type of Access
Symmetric encryption/decryption	User, Crypto Officer	AES Key	User and CO: execute
Digital signature	User, Crypto Officer	RSA Private Key, RSA Public Key,	User and CO: execute
Symmetric key generation	User, Crypto Officer	AES Key	User and CO: execute
Asymmetric key generation	User, Crypto Officer	RSA Private Key	User and CO: execute
Keyed Hash (HMAC)	User, Crypto Officer	HMAC Key HMAC SHA-1, HMAC SHA-256, HMAC SHA-512	User and CO: execute
Message digest (SHS)	User, Crypto Officer	SHA-1, SHA-256, SHA-512	User and CO: execute
Show status	User, Crypto Officer	None	User and CO: execute

Service	Roles	Cryptographic Keys and CSPs	Type of Access
Self test	User, Crypto Officer	AES Key, RSA Public Key, RSA Private Key, HMAC Key, Integrity Key	User and CO: execute
On-Demand Self Test	User, Crypto Officer	AES Key, RSA Public Key, RSA Private Key, HMAC Key, Integrity Key	User and CO: execute
Zeroize	User, Crypto Officer	All CSPs	User and CO: execute
Initialize	Crypto Officer	none	CO: execute

Table 5 – Module Services and Descriptions

Please note that the module makes use of the Windows Server 2008 R2 Enhanced Cryptographic Provider (RSAENH) validated to FIPS 140-2 under Cert. #1337 in the Symmetric Key Generation and Asymmetric Key Generation services.

2.4.2 Operator Authentication

As required by FIPS 140-2, there are two roles (a Crypto Officer role and User role) in the module that operators may assume. As allowed by Level 1, the module does not support authentication to access services.

2.5 Physical Security

This section of requirements does not apply to this module. The module is a software-only module and does not implement any physical security mechanisms.

2.6 Operational Environment

The module operates on a general purpose computer (GPC) running on a modern version of Microsoft Windows as a general purpose operating system (GPOS). For FIPS purposes, the module is running on Microsoft Windows in single user mode and does not require any additional configuration to meet the FIPS requirements.

The module was tested on the following platforms:

- Windows Server 2008 R2 running on a Dell OptiPlex 755

The GPC(s) used during testing met Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B. FIPS 140-2 validation compliance is maintained when the module is operated on other versions of the Microsoft Windows GPOS running in single user mode, assuming that the requirements outlined in NIST IG G.5 are met.

2.7 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters used within the module:

Keys and CSPs	Storage Locations	Storage Method	Input Method	Output Method	Zeroization	Access
AES Key CBC, ECB 128, 192, 256	Volatile RAM	Plaintext	Plaintext	None	ReleaseCryptoObject() power cycle	CO: RWD U: RWD
RSA Public Key	Volatile RAM	Plaintext	Plaintext	Plaintext	ReleaseCryptoObject() power cycle	CO: RWD U: RWD
RSA Private Key	Volatile RAM	Plaintext	Plaintext	None	ReleaseCryptoObject() power cycle	CO: RWD U: RWD
HMAC Key SHA-1, SHA-256, SHA-512	Volatile RAM	Plaintext	Plaintext	None	ReleaseCryptoObject() power cycle	CO: RWD U: RWD
Integrity Key	Volatile RAM	Plaintext	None	None	None	CO: RWD U: RWD

R = Read W = Write D = Delete

Table 6 – Module Keys/CSPs

2.7.1 Key Entry, Output, and Protection

All keys and CSPs reside on memory internally allocated by the module and can only be output using the exposed APIs. The module does not support key entry or output from the physical boundary. The operating system protects the memory and process space from unauthorized access.

2.7.2 Key/CSP Storage and Zeroization

Public and private keys are provided to the Module by the calling process, and are destroyed when released by the appropriate API function calls. The Module does not perform persistent storage of keys.

2.8 Self-Tests

FIPS 140-2 requires that the module perform self-tests to ensure the integrity of the module and the correctness of the cryptographic functionality at start up. In addition some functions require continuous verification of function. All of these tests are listed and described in this section. In the event of a self-test error, the module will log the error and will halt. The module must be reinitialized and reloaded into memory to become functional again.

The following sections discuss the module's self-tests in more detail.

2.8.1 Power-On Self-Tests

The module implements the following power-on self-tests:

TYPE	DETAIL
Software Integrity Check	HMAC-SHA512
Known Answer Tests	• AES (encrypt/decrypt) • HMAC SHA-1 • HMAC SHA-256 • HMAC SHA-512 • RSA • SHA-1 • SHA-256 • SHA-512
Pair-wise Consistency Tests	• RSA

Table 7 – Power-On Self-Tests

Power-on self-tests are executed automatically when the module is loaded into memory.

2.8.2 Conditional Self-Tests

The module implements the following conditional self-tests:

TYPE	DETAIL
Pair-wise Consistency Tests	• RSA

Table 8 – Conditional Self-Tests

2.9 Mitigation of Other Attacks

The Module does not contain additional security mechanisms beyond the requirements for FIPS 140-2 Level 1 cryptographic modules.

3 Guidance and Secure Operation

This section describes how to configure the module for FIPS-approved mode of operation. Operating the module without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

3.1 Crypto Officer Guidance

3.1.1 Software Packaging and OS Requirements

The module must be installed on a General Purpose Operating System running in single user mode. To configure single-user mode, the following must be disabled:

- Remote registry and remote desktop services
- Remote assistance
- Guest accounts
- Server and terminal services

Contact Microsoft support for configuration details; specific configuration steps are beyond the scope of this document.

3.1.2 Enabling FIPS Mode

The module only provides FIPS mode of operation. No special instructions are required to put the module into FIPS mode.

3.1.3 Additional Rules of Operation

1. All host system components that can contain sensitive cryptographic data (main memory, system bus, disk storage) must be located in a secure environment.
2. The writable memory areas of the Module (data and stack segments) are accessible only by the calling application so that the Module is in "single user" mode, i.e. only the calling application has access to that instance of the Module.
3. The operating system is responsible for multitasking operations so that other processes cannot access the address space of the process containing the Module.
4. The end user of the operating system is also responsible for zeroizing CSPs via wipe/secure delete procedures.

3.2 User Guidance

3.2.1 General Guidance

The module is not distributed as a standalone library and is only used in conjunction with the Database Security Sensor solution. As such, there is no direct User Guidance.