FIPS 140-2 Non-Proprietary Security Policy

for the

Guidance Software EnCase Enterprise Cryptographic Module Version 1.0

Level 1 Validation

Document Version: Version 1.6

April 7, 2008

Prepared For:

Guidance Software, Inc.
215 North Marengo Avenue, Suite 250
Pasadena, CA 91101
www.guidancesoftware.com

Prepared By:

Apex Assurance Group, LLC
5448 Apex Peakway Drive, Ste. 101
Apex, NC 27502
www.apexassurance.com

REVISION HISTORY

The table below provides revision history of this document.

Version	Date	Author(s)	Comments
1.0	July 18, 2007	Apex Assurance Group	Initial draft for customer review
1.1	July 31, 2007	Apex Assurance Group	Update with GSI comments, additional details
1.2	September 13, 2007	Apex Assurance Group	Address initial comments from DOMUS
1.3	November 12, 2007	Apex Assurance Group	Address additional comments from DOMUS
1.4	December 7, 2007	Apex Assurance Group	Final comments from functional testing
1.5	February 13, 2008	Apex Assurance Group	Update with NIST CMVP comments
1.6	April 7, 2008	Apex Assurance Group	Update with additional NIST CMVP comment

Table 1 – Security Policy Revision History

TABLE OF CONTENTS

INTRODUCTION

Background

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic products to be deployed in a Sensitive but Unclassified environment. 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/index.html.

This non-proprietary Cryptographic Module Security Policy for the EnCase Enterprise Cryptographic Module 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 modules in a FIPS 140-2 mode of operation.

External Resources

The Guidance Software website (http://www.guidancesoftware.com) contains information on the full line of products from Guidance Software, including a detailed overview of the EnCase Enterprise Cryptographic Module solution. The NIST Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains Guidance Software contact information for answers to technical or sales-related questions.

Notices

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

Relationship to the EnCase Enterprise Product

The module is designed for use within the full range of Guidnace Software's products, including the EnCase Enterprise suite. As such the module implements the security relevant functions of Guidance Software's products. The typical "users" of the module are therefore EnCase Enterprise software processes referred to as "calling daemons" in the following text.

GUIDANCE SOFTWARE ENCASE ENTERPRISE CRYPTOGRAPHIC MODULE

Product Overview

EnCase® Enterprise has changed the landscape of enterprise and computer investigations by providing complete network visibility, immediate response and comprehensive, forensic-level analysis of servers and workstations anywhere on a network. 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 to meet your unique needs, including the automation of time-consuming investigative processes, incident response and eDiscovery.

- Securely investigate/analyze many machines simultaneously over the LAN/WAN at the disk and memory level.
- Acquire data in a forensically sound manner, using software that has an unparalleled record in courts worldwide.
- Limit incident impact and eliminate system downtime with immediate response capabilities.
- Investigate and analyze multiple platforms — Windows, Linux, AIX, OS X, Solaris and more — using a single tool.
- Efficiently collect only potentially relevant data upon eDiscovery requests.
- Proactively audit large groups of machines for sensitive or classified information, as well as unauthorized processes and network connections.
- Identify fraud, security events and employee integrity issues wherever they are taking place — then investigate/remediate with immediacy and without alerting targets.
- Identify and remediate zero-day events, injected dlls, rootkits and hidden/rogue processes..

Cryptographic Module Specification

The module is the Guidance Software EnCase Enterprise Cryptographic Module version 1.0. The module is an object module that is distributed as part of the Encase Enterprise application and is therefore classified as a multi-chip standalone cryptographic module.

Module Block Diagram

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

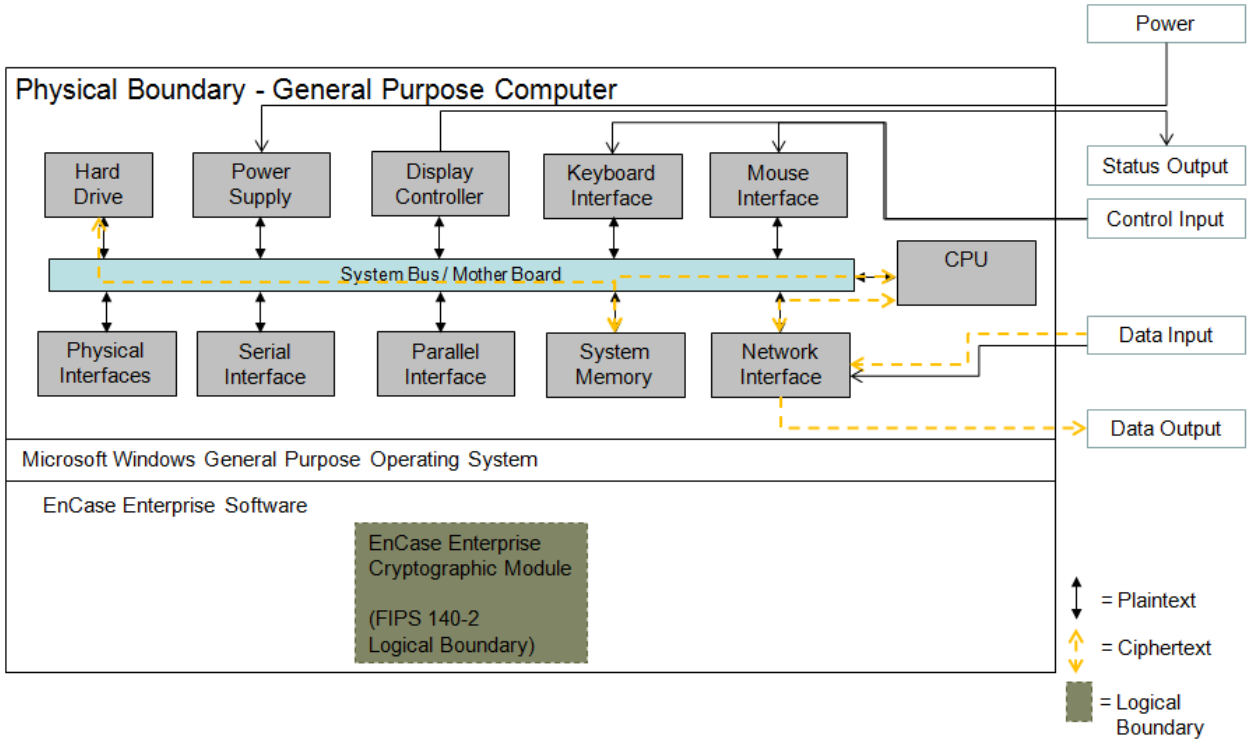

Figure 1 – Physical/Logical Boundary Diagram

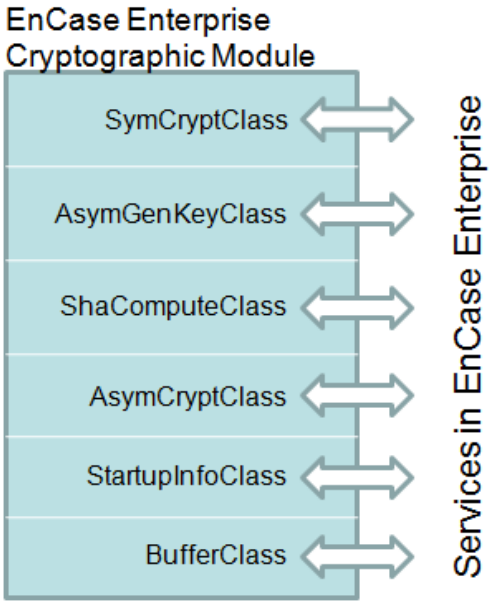

Figure 2 – Module Block Diagram

Validation Level and Algorithm Implementation Certificates

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

FIPS 140-2 Section Title	Module 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	1
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	1

Table 2 – Validation Level by DTR Section

The "Mitigation of Other Attacks" section is also not relevant as the module does not implement any countermeasures towards special attacks.

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

Algorithm Type	Algorithm	Standard	FIPS Validation Certificate	Use
Asymmetric Key	DSA	FIPS 186-2	248	Sign / verify operations Key generation
Hashing	SHA-1	FIPS 180-2	698	Message digest
Keyed Hash	HMAC-SHA1	FIPS 198	350	Module integrity
Symmetric Key	AES CBC mode with 128-bit keys	FIPS 197	666	Data encryption

Table 3 – Algorithm Certificates

Please note that for RNG functionality, the module relies on the FIPS 186-2 based Microsoft Enhanced Cryptographic Provider (Cryptographic Application Programming Interface CAPI), which earned certificate number 238.

Module Interfaces

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 library. 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 *Roles and Services* for the list of available functions).

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	Ethernet/Network port
Data Output	Output parameters of API function calls	Ethernet/Network port
Control Input	API function calls	Keyboard and mouse
Status Output	Function calls returning status information and return codes provided by API function calls	Monitor
Power	None	Power supply/connector

Table 4 – Logical Interface / Physical Interface Mapping

Roles and Services

The module supports a *Crypto Officer* and a *User* role. The Crypto Officer can access all services in the module and perform initialization while the User role can only access the services of the module. The module supports no *Maintenance* role.

The Module does not implement authentication of the two roles. Roles are implicitly selected via the services being called and the situation in which they are called as described below. There are also no internal audit trails tracking any of the events or data generated or used by the module during FIPS approved mode of operation.

Crypto Officer Role

The Crypto Officer role is responsible only for the initialization of the module. The Crypto Officer role has no special access to keys or data *inside* the module except for generating the shared secret at initialization time. The Crypto Officer role is implicitly selected or assumed when initializing module.

User Role

The User role includes all the calling daemons (other software modules outside the EnCase Enterprise Cryptographic Module) using the module as part of their normal operation.

The User role is implicitly selected or assumed when calling any services on the module API when using the module during normal operations.

Available Services

The services available to the User and Crypto Officer roles in the Module consist of the following:

SERVICE	DESCRIPTION	ROLES	CLASS NAME
Encrypt Block Symmetric	Encrypts a block of data Using AES	Both	SymCryptClass
Decrypt Block Symmetric	Decrypts a block of data Using AES	Both	SymCryptClass
Key Generation	Generates DSA keys using the Microsoft CAPI PRNG	Crypto Officer	AsymGenKeyClass
Hash Block	Hashes a block using SHA-1 and the standard IV	Both	ShaComputeClass
Sign Block	Signs a block with DSS	Both	AsymCryptClass
Verify Block	Verifies the Signature of a DSS-signed block	Both	AsymCryptClass
Encrypt Block Asymmetric	Encrypts a block of data using DH	Both	AsymCryptClass
Decrypt Block Asymmetric	Decrypts a block of data using DH	Both	AsymCryptClass
Load Asymmetric key	Loads an asymmetric key into the module	Both	AsymCryptClass
Show Status	Shows status of the module	Both	StartupInfoClass
Zeroize CSPs	Clears CSPs from memory	Both	BufferClass
Run Self-Tests	Performs power-on self-tests	Crypto Officer	Subsystem
Installation and Initialization	Installs the module and initializes the module for FIPS mode of operation	Crypto Officer	Compiled in; no load needed

Table 5 – Operator Services and Descriptions

Physical Security

No physical security is claimed as the Cryptographic Module is software-only.

Operating Environment

The module operates on a general purpose computer running on a modern version of the Microsoft Windows general purpose operating system (GPOS), including Microsoft Windows Vista, Windows XP and Windows 2003 Server. 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 a GPOS with the following specifications:

- Operating System: Microsoft Windows XP Professional SP2
- Processor: Intel Pentium 4 at 3.2 Ghz
- RAM: 2GB
- Hard Drive: 30GB
- Network Controller: Intel Pro/1000 Dual Port Server
- Video Controller: Nvidia GeForce 6200

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.

Cryptographic Key Management

Table 6 provides a complete list of critical security parameters used within the module:

KEY / CSP NAME	DESCRIPTION	Crypto Officer Privileges[1]	User Privileges
GSI Key	Vendor Key pair (DH/DSS), Root of trust	R W D	None
Keymaster	Client crypto officer Key pair (DH/DSS); used for authentication to the SAFE and key distribution	R W D	None
SAFE	Server Key pair (DH/DSS)	R W D	R W D
Session key	128-bit AES session key	R W D	R W D

Table 6 – Critical Security Parameters

Please note that the module does not support key storage.

Zeroization has been implemented to ensure no traces are left in memory of any CSPs upon termination of the service using the CSP. Zeroization has been implemented by overwriting the allocated memory buffer with zeros before freeing the memory to other uses. Any service using a CSP will zeroize the CSP upon normal termination and when transitioning into error states. Zeroization is initiated by terminating the process and powering off the module.

Self-Tests

The module includes an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly. The following sections discuss the module's self-tests in more detail.

In the event of any self-test failure, the module will output an error dialog and will shutdown. No keys or CSPs will be output when the module is in an error state.

Power-On Self-Tests

Power-on self-tests are run upon every initialization of the module and if any of the tests fail, the module will not initialize. The module will enter an error state and no services can be accessed by the users. The module implements the following power-on self-tests:

[1] R = Read | W = Write | D = Delete

- Module integrity check via HMAC-SHA1
- DSA pairwise consistency key (signing and signature verification)
- AES KAT (encryption and decryption)
- SHA-1 KAT

The module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by reinitializing the module in FIPS approved Mode of Operation or by calling the corresponding service on the API.

Conditional Self-Tests

Conditional self-tests are on-demand tests and tests run continuously during operation of the module. If any of these tests fail, the module will enter and error state. The module can be re-initialized to clear the error and resume FIPS mode of operation. No services can be accessed by the operators. The module performs the following conditional self-tests:

- Pairwise consistency test for DSA
- Continuous RNG test run on output of CAPI RNG

The module does not support a bypass function.

Mitigation of Other Attacks

The module does not mitigate other attacks.

SECURE OPERATION OF THE ENCASE ENTERPRISE CRYPTOGRAPHIC MODULE

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.

Crypto Officer Guidance

Module Initialization and Configuration

Crypto Officer must configure and enforce the following initialization procedures:

1. Install module using setup program.
2. Verify that the software version is 1.0 and that FIPS mode is enabled. No other version is allowed to be used in FIPS mode of operation.
3. Verify that the GPOS is configured to a single-user mode of operation.

User Guidance

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

Approved Cryptographic Algorithms

In FIPS mode of operation, only the following FIPS approved algorithms are used:

- AES for encryption/decryption
- DSA for signing and verifying
- SHA-1 for hashing
- HMAC-SHA1 for module integrity
- CAPI for random number generation[2]

Non-FIPS Approved Algorithms

The module implements the following non-FIPS-approved cryptographic algorithms:

- Diffie-Hellman
  - DH key sizes of 1024-bits and 2048-bits
  - Key agreement; key establishment methodology provides 80 or 112 bits of encryption strength

[2] As implemented in Microsoft Enhanced Cryptographic Provider (Cryptographic Application Programming Interface CAPI), which earned certificate number 238.

ACRONYM LIST

AES	Advanced Encryption Standard
API	Application Programming Interface
CAPI	Cryptographic Application Programming Interface (CAPI)
CBC	Cipher Block Chaining
CSP	Critical Security Parameter
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DTR	Derived Test Requirements
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GPOS	General Purpose Operating System
GSI	Guidance Software, Inc.
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random Access Memory
SHA	Secure Hash Algorithm