SECUDE AG

FinallySecure Enterprise Cryptographic Module

(SW Version: 1.0)

FIPS 140-2 Security Policy

Document Version 2.4

04/22/2010

TABLE OF CONTENTS

1. Document Information

Change History

Version	Author	Date	Description
1.0	Zhe Wang Min Xie	24.11.2008	Initial draft
1.1	Zhe Wang	25.11.2008	Add more contents.
1.2	Zhe Wang Min Xie	09.12.2008	Modify according to IG comments.
1.3	Zhe Wang	16.12.2008	Add reference table, modify according to IG comments.
2.0	Zhe Wang	19.10.2009	Revision to cope with major software version upgrade and crypto-module resize.
2.1	Zhe Wang	19.01.2009	Change title and remove FIPS unrelated authentication and CSPs, minor change to block diagram.
2.2	Zhe Wang	22.03.2010	Block diagram modified.
2.3	Zhe Wang	07.04.2010	Modify according to IG comments after Op test.
2.4	Zhe Wang	22.04.2010	Modify according to IG comments after Op test.

2. Introduction

This non-proprietary cryptographic module security policy describes how the FinallySecure Enterprise Cryptographic Module meets the security requirements of FIPS 140-2, and how to run the cryptographic module in accordance with the requirements of FIPS 140-2. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the FinallySecure Enterprise Cryptographic Module.

3. Module Overview

The FinallySecure Enterprise Cryptographic Module (Software Version: 1.0) is a software only, multi-chip standalone cryptographic module that runs on a general purpose computer (GPC). The primary purpose for this module is to provide cryptographic services for SECUDE's Full Disk Encryption software, FinallySecure Enterprise 9.4.0.

Cryptographic Boundary

The physical boundary of the module is the case of the GPC. The logical boundary of the module contains the dynamic link libraries libeay32.DLL and FIPSAlg.dll and disk filter drivers AES.sys and FDENC.sys. The FSE software consists of several logical components that form up or surround the cryptographic boundary, as depicted in Figure 1:

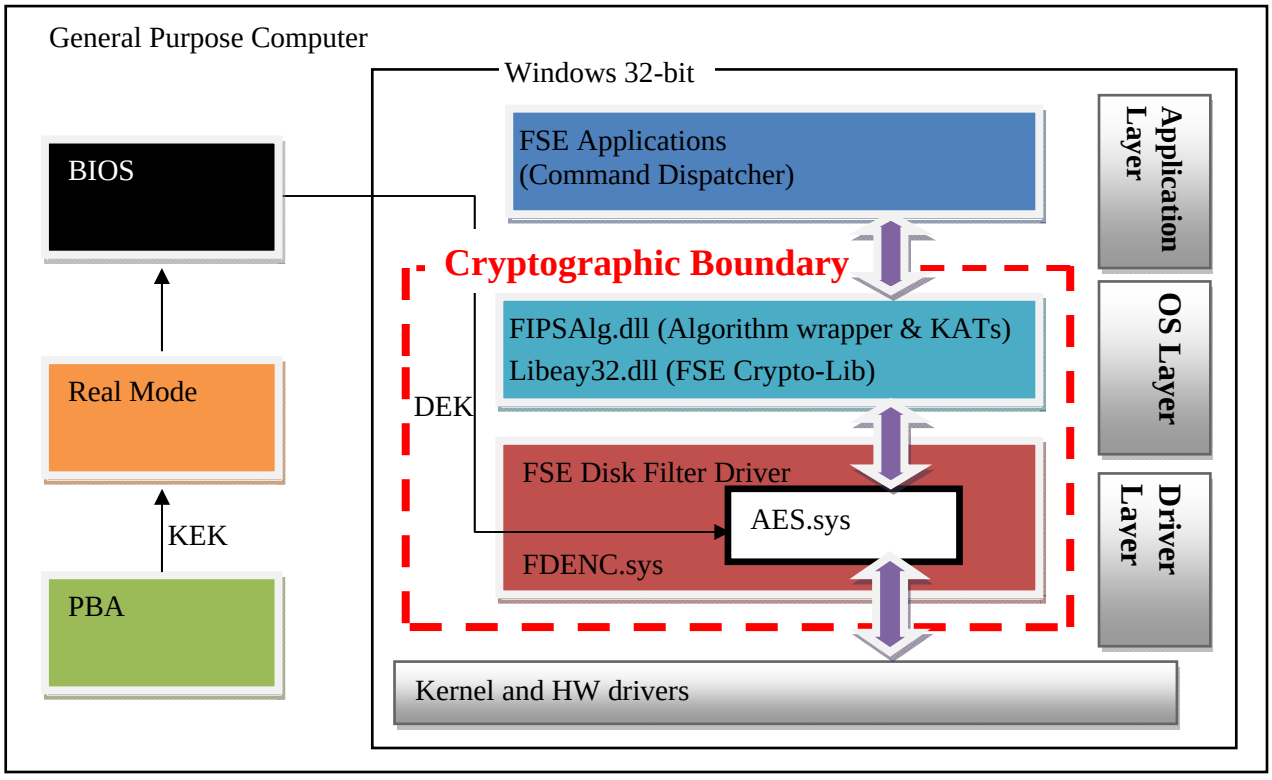

Figure 1 - Cryptographic Module Diagram

Operating Platforms

The cryptographic module runs and was operationally tested on the following platforms:

- Windows 7 (single-user mode)
- Windows Vista (single-user mode)
- Windows XP (single-user mode)

4. Security Level

The cryptographic module meets the overall requirements of FIPS 140-2 Security Level 1.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
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
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

5. Modes of Operation

Approved Mode of Operation

The cryptographic module only supports FIPS Approved algorithms as follows:

- AES - CBC mode; Encrypt/Decrypt; 128, 192, 256-bit (Certificate number 958)
- SHA-1 (Certificate number 930)
- HMAC-SHA-1 (Certificate number 534)
- RNG (Certificate number 541) - The module relies on the implemented random number generator (RNG) that is compliant with ANSI X9.31 Appendix A.2.4.

Invocation of Approved Mode of Operation

The cryptographic module only supports an Approved mode of operation. The FinallySecure Enterprise Cryptographic Module is installed as part of SECUDE's FinallySecure Enterprise full disk encryption software. Once installed, the module is considered to be running in the FIPS Approved mode of operation.

6. Ports and Interfaces

The physical ports of the FinallySecure Enterprise Cryptographic Module are consistent with those of the General Purpose Computers on which the software is installed. Although data input, data output, control input and status output share physical ports, the information flows for input, output, control and status are kept logically separate through the cryptographic module API.

External input/output devices are not applicable to the FinallySecure Enterprise Cryptographic Module.

The cryptographic module defines the following logical interfaces:

- The API function calls of the Disk Filter Driver.

Table 2 - FinallySecure Enterprise APIs and Logical Interfaces

Logical Interface	Mapping to Module API	Physical Ports
Control Input Interface	API function calls to control and initialized the module	• Keyboard • Mouse • HIDs • Data storage devices • External ports (network, USB, etc.)
Data Input Interface	API function calls containing parameters with input data or pointers to input data buffers	• Keyboard • Mouse • HIDs • Data storage devices • External ports (network, USB, etc.)
Data Output Interface	API function calls with output data or pointers to output data buffers.	• Data storage devices • Display
Status Output Interface	API function calls with output data or pointers to output data buffers.	• Data storage devices • Display
Power Interface	N/A. No power interface is applicable since the module is a software only module running on a General Purpose Computer.	• PC power interface

7. Identification and Authentication Policy

Assumption of Roles

The FinallySecure Enterprise Cryptographic Module only supports a single operator, who assumes both the User and Cryptographic Officer (CO) roles. A Maintenance role is not implemented in FinallySecure Enterprise Cryptographic Module software.

Concurrent operations are not supported by the FinallySecure Enterprise Cryptographic Module. All the concurrent operations attempted will be automatically queued for sequential execution.

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Cryptographic Officer/User	N/A	N/A

8. Access Control Policy

Roles and Services

Table 4 - Services Authorized for Roles

Role	Authorized Services
Cryptographic Officer/User:	• Encrypt Partition: This allows the administrator to encrypt partition/partitions. • Decrypt Partition: This allows the administrator to decrypt partition/partitions.

The FinallySecure Enterprise Cryptographic Module supports the following services which may be performed without assuming an authorized role:

- Self-tests: This service executes the suite of self-tests required by FIPS 140-2. This service is invoked upon system power-up or at run time.
- Status query: This returns the encryption/decryption information of all partitions and the status of the cryptographic module.
- Zeroize: This service zeroizes all plaintext CSPs stored on the GPC hard drive. This service is invoked by uninstalling the module.

Unsupported Services

The FinallySecure Enterprise Cryptographic Module does not implement bypass capability within the module.

Service Inputs & Outputs

Table 5 - Specification of Service Inputs & Outputs

Service	Control Input	Data Input	Data Output	Status Output
Encrypt Partition	Program API	Plaintext data and DEK	Ciphered data	Success/fail
Decrypt Partition	Program API	Ciphered data and DEK	Plaintext data	Success/fail
Status Query	Program API	None	None	Status information
Self-Tests	Program API	Known answer	None	Success/BSOD
Zeroize	Program API	None	None	Success/fail

Definition of Critical Security Parameters (CSPs)

The following are CSPs and secret keys that are protected within and around the cryptographic boundary:

- Data Encryption Keys (DEKs): AES 256-bit keys used to encrypt partitions on the HD. Each partition is encrypted with a unique DEK.
- Seed Key: Used to initialize RNG.
- Seed: Used to initialize RNG.

Definition of Public Keys

The module does not contain any public keys.

Definition of CSPs Modes of Access

Table 6 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

Table 6 - CSP Access Rights within Services

Service	Cryptographic Keys and CSPs Access Operation
Encrypt Partition	Read/Write DEK.
Decrypt Partition	Read DEK
Status Query	N/A
Self-Tests	N/A
Zeroize	Zeroize Seed, Seed Key, DEKs

Definition of CSPs Storage and Zeroization

The FinallySecure Enterprise Cryptographic Module stores the DEK hashed and obfuscated.

All the CSPs will be erased (zeroized) during the FinallySecure Enterprise software uninstallation process by the operator who assumes the Cryptographic Officer/User role.

9. Operational Environment

As per FIPS 140-2 Implementation Guidance the FinallySecure Enterprise Cryptographic Module is compliant with the requirements of FIPS 140-2 when operating on the following operating systems on top of 32-bit General Purpose Computer in single user mode:

- Windows 7
- Windows Vista
- Windows XP

10. Security Rules

The FinallySecure Enterprise Cryptographic Module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of the FIPS 140-2 Level 1 module.

1. The cryptographic module shall provide one distinct operator role: the Cryptographic Officer/User.
2. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
3. The cryptographic module shall encrypt and decrypt data using the Approved AES algorithm.
4. The cryptographic module shall perform the following self-tests without operator intervention:

   A. Power up Self-Tests:

      1. Cryptographic algorithm tests:
         a. AES Known Answer Test
         b. RNG Known Answer Test
         c. SHA-1 Known Answer Test
         d. HMAC Known Answer Test (performed during Software Integrity Test)
      2. Software Integrity Test (HMAC-SHA-1)
      3. Critical Functions Tests (None)

   B. Conditional Tests:

      1. Continuous RNG Test
5. Prior to each invocation, the internal RNG shall be tested using the conditional test specified in ANSI X9.31 Appendix A.2.4.
6. Any failure of the Power-up Self-tests or Software Integrity Test shall enter the software into the error state and block the Windows OS from common use.
7. Data output shall be strictly inhibited during key generation and self-tests.

8. Only status output shall be allowed during the error state.
9. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. The module shall not support multiple concurrent operators.

11. Physical Security Policy

The FinallySecure Enterprise Cryptographic Module is a software only module and therefore does not support any physical security mechanisms. The cryptographic module's physical boundary is the General Purpose Computer (GPC) that the module is installed on.

12. Mitigation of Other Attacks Policy

The Mitigation of Other attacks security section of FIPS 140-2 is not applicable to the FinallySecure Enterprise Cryptographic Module.

13. References

Table 7 - References

ID	Reference
1	FIPS PUB140-2 Security Requirements For Cryptographic Modules
2	FIPS PUB140-2 Derived Test Requirements
3	Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program
4	FIPS PUB 197 Advanced Encryption Standard
5	FIPS PUB 198 The Keyed-Hash Message Authentication Code
6	Approved Random Number Generators for FIPS PUB 140-2

14. Definitions and Acronyms

Table 8 - Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
BSOD	Blue Screen of Death
CO	Cryptographic Officer
CSP	Critical Security Parameter
DEK	Data Encryption Key
DES	Data Encryption Standard
ERI	Emergency Recovery Information
FDE	Full Disk Encryption
FIPS	Federal Information Processing Standard
FSE	FinallySecure Enterprise
GPC	General Purpose Computer
HID	Human Interface Device
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
RNG	Random Number Generator
SHA	Secure Hash Algorithm