BeCrypt DISK Protect and BeCrypt DISK Protect for Afaria Security Manager

Security Policy

FIPS 140-2 Level 1 Module Validation

November 2008

Document Version 1.2

1 INTRODUCTION 3

2 THE CRYPTOGRAPHIC MODULE 4

FUNCTIONAL OVERVIEW 4
MODULE DESCRIPTION 5
HIGH LEVEL BLOCK DIAGRAM 6
MODULE PORTS AND INTERFACES 8

3 SECURITY FUNCTIONS 11

4 IDENTIFICATION AND AUTHENTICATION 12

5 CRYPTOGRAPHIC KEYS AND CSPS 14

6 ROLES AND SERVICES 15

7 ACCESS CONTROL 17

8 SELF TESTS 18

9 FIPS APPROVED MODE OF OPERATION 20

FIXED DISK ENCRYPTION 20
CRYPTO OFFICERS GUIDE 20
Installation *20*
Use of Removable Media *22*
Zeroization *22*
Device Recovery *23*
Required Practice *23*
USERS GUIDE 23
Security Requirements on the Environment *24*

10 REFERENCES 25

11 GLOSSARY 26

1 Introduction

This is a non proprietary Security Policy for the BeCrypt DISK Protect and DISK Protect for Afaria Security Manager cryptographic modules. It describes how these modules meet all the requirements as specified in the FIPS 140-2 Level 1 requirements. This Policy forms a part of the submission package to the validating lab. In this document, DISK Protect and DISK Protect for Afaria Security Manager (which is a re-branded OEM version of DISK Protect) are referred to as “the module”.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2) specifies the security requirements for a cryptographic module protecting sensitive but unclassified information. For more information about the standard visit http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

More information describing the module can be found at http://www.becrypt.com.

This Security Policy describes how this module complies with the eleven sections of the Standard. The operating environment used in testing was Windows XP Professional SP2 with realmode Pre-boot environment. All testing was performed using software version 4.2.10.5 of the module.

Security Requirements Section	**Level**
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles and Services and Authentication	1
Finite State Machine 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

Table 1. Cryptographic Module Security Requirements

2 The Cryptographic Module

Functional Overview

The module is a full-disk encryption product that provides up to three layers of security: full disk encryption, strong pre-boot authentication, and optional removable media encryption.

Features of the software include:

- **Full disk encryption**: the module encrypts a computer's hard disk(s) using 128 bit AES data encryption. After successful authentication, data is automatically decrypted and re-encrypted on the fly. If anyone attempts to bypass authentication the data is encrypted and unintelligible.

- **Pre-boot authentication**: the module can be configured to authenticate the user by password, by password and USB token. Authenticating the user pre-boot allows the module to encrypt the entire hard drive, including the Operating System, which ensures that data cannot be accessed using low level tools.

- **Removable media encryption**: Optional removable media encryption secures data on USB-connected storage devices and floppy disks.

- **Multiple user support**: the module supports one or more Administrator and multiple user accounts per protected machine. Only one user is allowed to operate the PC in single user mode as per FIPS requirements. The hard disk is encrypted using a single Encryption Key (DEK) but each user has a unique password or password and token.

- **Single Sign On (SSO)**: the Single Sign On feature simplifies start up by synchronising the user’s and Windows passwords allowing users to automatically log into Windows. The module supports SSO for both password and token based authentication.

- **Secure hibernation**: hibernation allows a computer to start up rapidly by storing an image of system memory at shutdown. The module intercepts the hibernation process, encrypting the hibernation file as it is written to disk and decrypting it on start up, allowing the system to boot rapidly with no threat to security.

- **Token support**: The module supports USB tokens and smartcards to provide dual-factor authentication. Extended smart card support allows an organisation to use a card that is already part of its security systems, issuing its staff with a single card for access control and authentication. FIPS compliance testing has only been performed using the RSA 6100 token, however, the operation and use of tokens for dual-factor authentication by the module is identical for the following tokens and smartcards that are also supported: Aladdin R2e and eToken PRO USB tokens, Setec smart cards, and RSA 5100, 5200 and SID800 smart cards.

- The module has been developed in collaboration with RSA Security and is compatible with RSA Security Authentication solutions. RSA tokens can be used for pre-boot authentication and SSO into Windows. The solution is interoperable with RSA SecureID authentication, the RSA Authentication Utility and RSA Sign-On Manager.

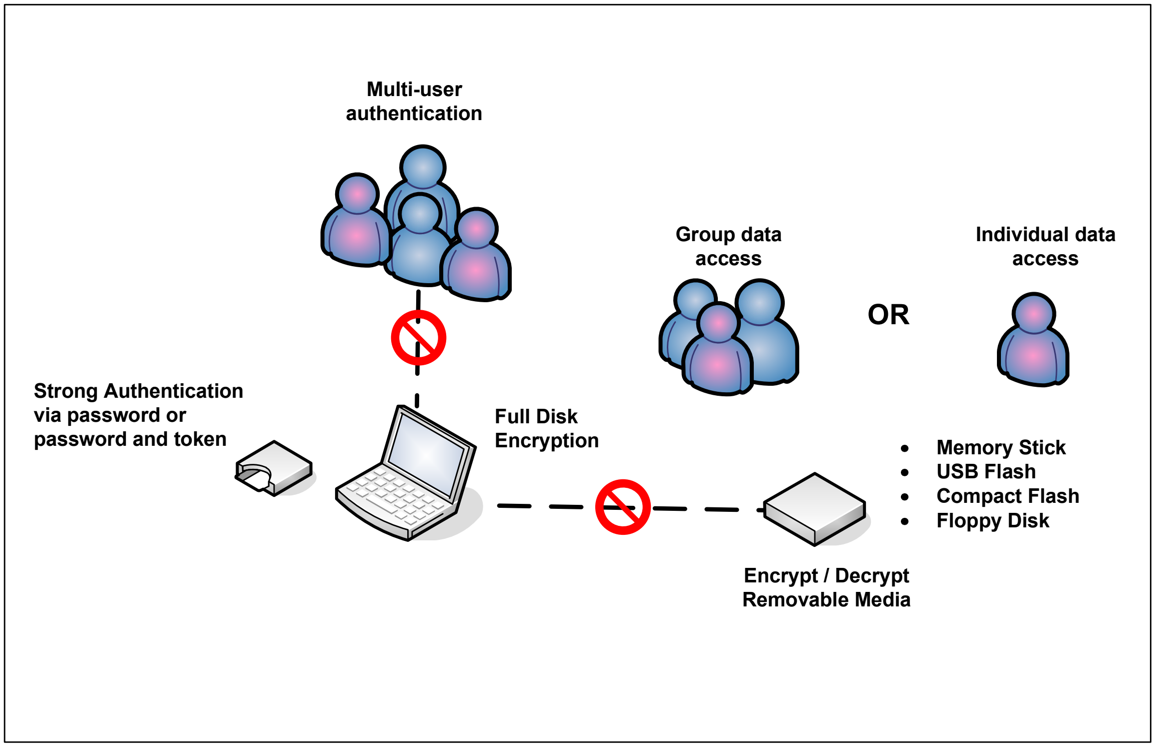

Multi-user authentication
Group data access
OR
Individual data access
Strong Authentication via password or password and token
Full Disk Encryption
• Memory Stick
• USB Flash
• Compact Flash
• Floppy Disk
Encrypt / Decrypt Removable Media

Figure 1. High Level Functional Overview

Module Description

The module is considered to be a multi-chip standalone cryptographic module with application software that executes on a Microsoft® Windows® PC general-purpose computing platform. The module is configured in single-user mode.

The module encrypts all data on a computer’s hard drive with a valid implementation of the AES algorithm using a 128 bit key. The module meets FIPS 140-2 level 1 security requirements.

The cryptographic module is comprised of three sub components viz. the pre-Operating System (pre-OS sub) component, the Operating System (OS) sub component and the User mode sub component. When the cryptographic module is powered up, the sub components load in the following order; pre-OS sub component, OS sub component and then User mode sub component. The cryptographic module is only operational when all sub-components have loaded.

The module provides authentication and software integrity services assuring operators of a valid software state within the module and privacy services for the secure storage of data. The module does not have a maintenance mode.

High Level Block Diagram

Figure 2 shows a block diagram of the cryptographic module that illustrates the physical boundary of the module and shows the module physical interfaces. The physical cryptographic boundary is the physical boundary of the PC case.

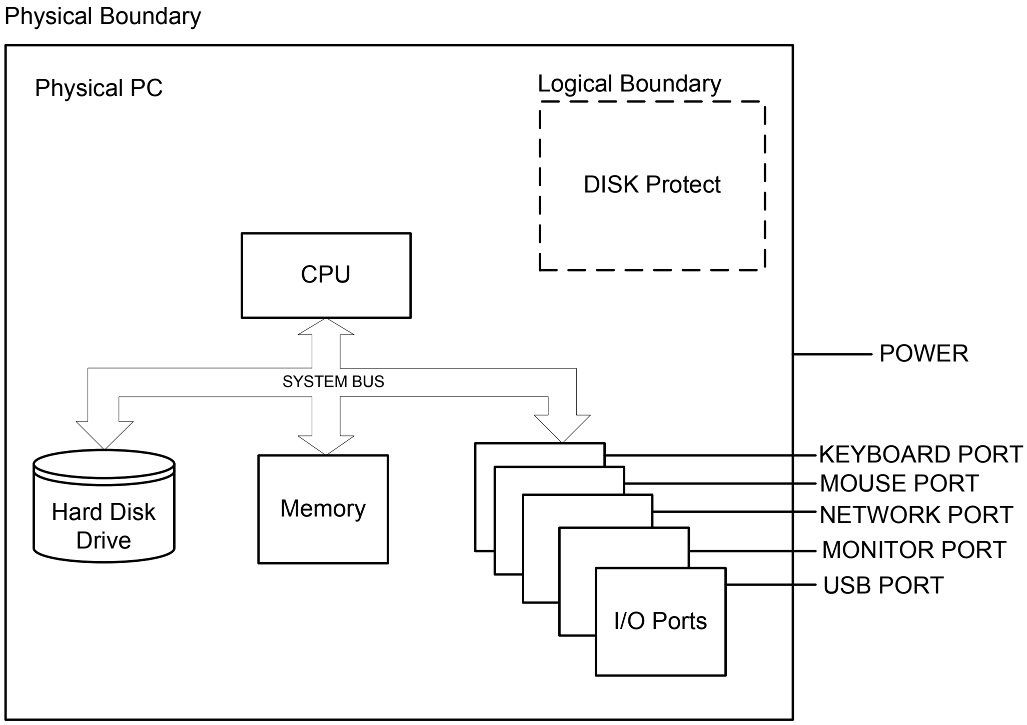


Figure 2. High Level Block Diagram Showing Physical Boundaries

Figure 3 shows a logical block diagram of the cryptographic module illustrating application components related to, and included within, the cryptographic boundary of the module.

The cryptographic boundary includes all application files as listed below:

- DiskProtectInstall.exe – Installation configuration wizard for the cryptographic module

- DPAgent.exe – NT service to control installation events, run user mode power up self tests, manage password change events and removable media key import
- DPRMTool.exe – used to encrypt a removable media when user selects encrypt-in-place
- DPRMExt.dll – used to assign or remove passwords from removable media
- DPUpdate.exe – application to update the MBR on installation
- DPTokenMan.exe – Token programming utility
- dpmgntool.exe – management tool
- INT13.EXE – real mode cryptographic implementation
- CRSGen2.dll – cryptographic interface for the token programming utility
- bcGina.dll – GINA implementation
- wxpenc.sys – Windows XP device driver

The following files are excluded from requirements of FIPS 140-2 as not security relevant:

- **Replacement Master Boot Record and configuration files**: BOOTSECT.EXE, MBR128.exe, CRYPTO.TAT, ETOKEN.TAT, LANGUAGE.INI, OCRYPTO.TAT, ORSA.TAT, OSETEC.TAT, RSA.TAT, SETEC.TAT, UCRYPTO.TAT, URSA.TAT, USETEC.TAT
- **Protected mode filter drivers**: bcscdftr.dll (filter for smartcard insertion events), bcupper.sys (upper level filter driver interface to protected mode encryption drivers)
- **Third Party Smartcard DLLs**: DupHashProxy.dll, NPsigplug.dll, SetCSP.dll, inst_ca.dll, sc.dll, settoki.dll, ssiasn1.dll, ssider.dll, ssides.dll, ssihash.dll, ssipk15.dll, ssirsa.dll, ssirsakg.dll, ssiutil.dll, unicows.dll
- **Program Files**: RecoveryConsole.exe, PacakageWiz.exe, BCSystray.exe, DISK Protect.chm, InstallHelpers.dll, bcscdftr.inf, becrypt.bmp, msvcp71.dll, msvcr71.dll, w2kenc.inf, wxpenc.inf, Language.ini

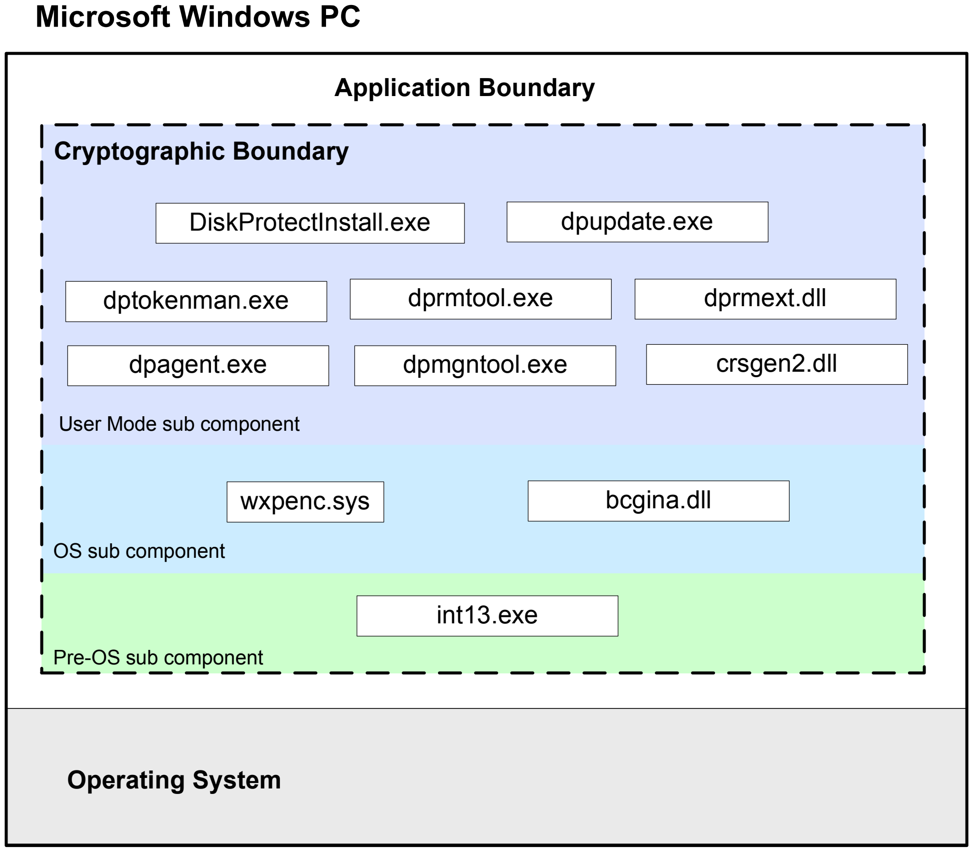


Figure 3. High Level Block Diagram Showing Logical and Cryptographic Boundaries.

Module Ports and Interfaces

The module is considered to be a multi chip standalone module with ten physical ports and five logical interfaces. The logical interfaces are described as:-

- **Data input interfaces;** consist of all parameters passed into functions that accept input data arguments.
- **Data output interfaces;** consist of all parameters passed out of functions that produce output arguments and return values.
- **Control input interfaces;** consist of all parameters passed into functions to administer the module.
- **Status output interfaces;** consist of return values from functions and output parameters that return information regarding module status, as well as values passed to the Application Event Log.

The physical ports have the functions described in Table 2.

Physical Ports	FIPS 140-2 Logical Interface
PC USB port, PCMCIA port, touch screen interface (Windows XP tablet), network port, Keyboard port, Mouse port, optical drive, floppy drive	Data input interfaces
PC USB port, PCMCIA port, network port, optical drive, floppy drive	Data output interfaces
Mouse port, Keyboard port, PC Power button	Control input interfaces
PC monitor	Status output interface
PC Power interface	Power interface

Table 2. Physical ports and Logical Interfaces.

Table 3 gives further details on the Logical Interfaces.

Logical Interface	Description
Data input interfaces	The data input is: • All plaintext data entering the Pre-OS subcomponent and OS subcomponent (driver API, encrypt block function) for the purpose of being encrypted and stored on the hard drive. • All ciphertext data entering the Pre-OS subcomponent and OS subcomponent (driver API, decrypt block function) for the purpose of being decrypted.
Data output interfaces	The data output is: • All plaintext data exiting the Pre-OS subcomponent and OS subcomponent (driver API, decrypt block function). • All ciphertext data exiting the Pre-OS subcomponent and OS subcomponent (driver API, encrypt block function).
Control input interfaces	The module accepts control input from the operator via applications that have Windows GUI interfaces including; • Setting password policy, including password length, format and lifetime (Management Tool) • Enabling / Disabling removable media encryption, including setting media and transport keys (Management Tool GUI) • Program user tokens for token based authentication (Management Tool and DPTokenMan) • Adding users to the machine so that they can have

	individual boot time access (Management Tool). Multiple concurrent users are not allowed to use the module, this is enforced via authentication. Users can only operate in Single user mode as per FIPS requirements. • Change Password (Systray Application and Management Tool) There are a number of control inputs that can only be carried out during installation of the module by an operator with administrative privileges on the PC. These include; • Setting authentication to password or token (Install Wizard Application) • Setting local machine policy including password lifetime, and type of password (Install Wizard Application) • Generating a fixed DISK encryption key (Install Wizard Application) • Re-starting installation (System Registry). This case only applies to DISK Protect for Afaria Security Manager which remains in a dormant state after running the InstallWizard. Installation needs to be re-started, as specified in Installation subsection of Section 9, in order to complete the process and start encryption.
Status output interface	The status output is: • all messages logged by the module • any messages returned by the module. • error messages are output to the display via messages on the screen.

Table 3. Logical Interfaces

3 Security Functions

The cryptographic module implements the following security functions described in Table 4:

Approved Security Function	**Certificate**
Symmetric Key Encryption	
AES (FIPS PUB 197) : Pre-OS implementation	667
AES (FIPS PUB 197) : OS implementation	247
Hashing	
SHA-256, FIPS 180-2 : Pre-OS implementation	700
SHA-256, FIPS 180-2: OS implementation	324
HMAC-SHA256 : Pre-OS implementation	351
Signature Generation and Verification	
RSA (ANSIX9.31 OS implementation)	309
Key Generation	
RNG (ANSI X9.31 User mode implementation)	386

Table 4. Module Security Functions

The cryptographic module does not implement any Non Approved security functions.

4 Identification and Authentication

The module supports a crypto officer role and a user role. The module implements role based authentication via password or password and token.

Crypto Officers must be configured to have both Windows and module Administrative Privileges. DISK Protect or DISK Protect for Afaria Security Manager Administrative privileges can be set up when configuring the module user properties during installation.

Crypto officer operations include configuring the PC in single user mode and running the setup program. The crypto officer is responsible for setting up DISK Protect or DISK Protect for Afaria Security Manager user accounts on the system including configuring password policy, recovery options and removable media support.

Users may operate the module once they have authenticated with their credentials.

Access to the authorized roles is restricted as explained in Table 5.

Role	Type of Authentication	Authentication Data
Crypto Officer	Role-based	The operator must enter the correct credentials at boot time before logging into Windows. The Crypto officer must have Administrative privileges assigned in order to perform crypto officer services.
User	Role-based	The operator must enter the correct credentials at boot time before logging into Windows. Users do not have Administrative privileges assigned.

Table 5. Roles and Required Identification and Authentication

The module does not require any physical maintenance. The strength of the operator authentication, for the Crypto Officer and User roles, is described in Table 6 below:

Authentication Mechanism	Strength of Mechanism
Password	Passwords for operator authentication are required to be at least 6 characters and at most 28 characters. Password characters must be from the ASCII character set. There are a minimum of 95^6 possible passwords for an exhaustive search of all six-character passwords. Therefore, the chance of correctly guessing a password is less than 1 in 1,000,000. Assuming 10,000 guesses per second, the possibility of guessing a password in a minute is

	less than 1 in 100,000.
Token + Password	Operators must authenticate using a token password that is required to be at least 6 characters and at most 21 characters. Password characters must be from the ASCII character set. There are a minimum of 95^6 possible passwords for an exhaustive search of all six-character passwords. Therefore, the chance of correctly guessing a password is less than 1 in 1,000,000. Assuming 10,000 guesses per second, the possibility of guessing a password in a minute is less than 1 in 100,000. The strength of this mechanism is at least as strong as the password authentication technique with the additional requirement of a physical token is physically required for two factor authentication.

Table 6. Strength of Authentication

5 Cryptographic Keys and CSPs

Table 7 below identifies the Cryptographic Keys and Critical Security Parameters (CSPs) used within the module.

Algorithm	Key	Key Length	Description
AES	Disk Encryption key (DEK)	16 bytes	Fix Disk Encryption Key. Disk Key to encrypt and decrypt the HDD and transport keys.
AES	Transport and Media Keys	16 bytes	Transport and Media Keys are used to encrypt media other than a machine's fixed disk (removable media).
RNG	RNG Seed	16 bytes	Seed used to generate random numbers during disk, transport, media and token key creation in FIPS mode.
RNG	RNG Seed key	16 bytes	Seed Key used to generate random numbers during disk, transport, media, and token key creation in FIPS mode.
HMAC	HMAC secret key	64 bytes	Private key for approved integrity technique for checking the Pre-OS binaries.
RSA	RSA private key	128 bytes	Private key for RSA signature generation and verification of binaries. Approved Integrity technique to be used for OS and User mode integrity checks based on ANSI x 9.31.
RSA	RSA public key	128 bytes	Public key for RSA signature verification of binaries. Approved Integrity technique to be used for OS and User mode integrity checks based on ANSI x 9.31.
AES	TKEK	16 bytes	The token key encryption key is used to protect the disk encryption key on the token if two factor authentication is used to access the module.
N/A	Password	6 – 28 characters	Passwords for user or crypto officer authentication at boot time. (Password only configuration)
N/A	Password	6 – 21 characters	Passwords for user or crypto officer authentication at boot time. (Password and Token based configuration)
AES	Key Encryption key	16 bytes	Key Encryption key used to protect the disk encryption key and media keys. However the disk encryption key and media keys are then considered to be stored in plaintext by FIPS 140-2.
AES	TKEK encryption key	16 bytes	Key used to protect the Token Key Encryption Key on the token. However the Token Key Encryption Key is then considered to be stored in plaintext by FIPS 140-2.

Table 7. Cryptographic keys and CSPs

6 Roles and Services

The module supports services that are available to crypto officers and users. The operator must enter the correct credentials at boot time to assume either the User or Crypto officer roles. Table 8 shows the services available to the various roles.

Service	Description
Users	
Boot Time Authentication	Provides boot time authentication
Manage User Properties for logged on user : Single Sign On	Users may elect to synchronise their disk encryption authentication details with Windows authentication details so that Single Sign On can be achieved from boot time
Review Encryption Status (Show status)	Users may Review the encryption status of the HD via the management tool utility
Review Event Logs (Show status)	Review status messages including errors
Configure Removable Media Encryption	Enable / Disable removable media encryption, including setting media and transport keys
Encrypt / Decrypt the HDD and or Removable Media	Encrypt or decrypt the hard disk and or removable media
Power up self tests	Perform Power up tests when module is rebooted
View Product Information (Show status)	Product version and build information
Secure Hibernation	Users may configure their PC power settings to hibernate securely. The module will automatically encrypt the image of the running system when hibernating and will automatically decrypt the image after successful boot time authentication.
Crypto Officers	
Install the module	Install, uninstall and configure the module
Manage Users	Add / Remove users
Set Local Machine Policy	Set password policy, including password length, format and lifetime
Configure Removable Media Encryption	Enable / Disable removable media encryption, including setting media and transport keys
View Encryption Status (Show status)	Review encryption progress as disk is encrypting
View Product Information (Show status)	Product version and build information
Boot Time Authentication	Provides boot time authentication
Review Event logs (Show status)	Review status messages including errors
Select Authentication Method	Installation only : Set authentication to password or token
Configure Fixed Disk encryption (generate encryption key)	Generate a DISK encryption key and use the key to encrypt the Fixed DISK
Add users	Add users to the machine so that they can have individual boot time access (FIPS level 1 only tests single user mode). Multiple concurrent users are not allowed to use the module, this is

	enforced via authentication.
Enable Single Sign On for the machine	Allow the user to synchronise module and Windows passwords
Program Tokens	Program user tokens for token based authentication or change the credentials held on the token.
Upgrade the product	Upgrade the product when a newer version is available
Encrypt / Decrypt HDD and or Removable Media	Encrypt or decrypt the hard disk and or removable media
Secure Hibernation	Described earlier in table – same functionality as for users
Power up self tests	Perform Power up self tests when module is rebooted
Zeroization	Zeroize all cryptographic keys and CSPs

Table 8. Roles and Services

7 Access Control

Table 9 groups the authorized services and the Cryptographic Keys and CSPs associated with the services. The modes of access are also identified per the explanation.

R - The item is read or referenced by the service.
W - The item is written or updated by the service.
E - The item is executed by the service. (The item is used as part of a cryptographic function.)
D – The item is deleted by the service

Key or CSP	Service	Access Control
Disk Encryption Key (DEK)	Boot time authentication	R,E
	Configure encryption during installation	R,W
	HDD and transport key encryption	R,E
Password	Boot time authentication	R,E
	Change password	R,W
	Single Sign On	R,E
Password (Token Authentication)	Boot time authentication	R,E
	Single Sign On	R,E
	Change password	R,W
HMAC secret key	Power Up Self Tests (Integrity tests for the Pre-OS component)	R,E
RSA public and private keys	Power Up Self Tests (Integrity tests for the OS and User Mode sub components)	R,E
Media and Transport Keys	Removable storage encryption	R,E,W
	Configure Removable Media Encryption	R,W,E,D
RNG Seed and Seed keys	Key Generation	R,E,W
Key Encryption key	Protection of disk encryption key and media keys (however the disk encryption key and media keys are then considered to be stored in plaintext by FIPS 140-2)	R,E
TKEK	Protection of disk encryption key on token	R,E
TKEK encryption key	Protection of Token Key Encryption Key on token (however the Token Key Encryption Key is then considered to be stored in plaintext by FIPS 140-2).	R,E
All keys and CSPs	Zeroize	D

Table 9. Access Control

8 Self Tests

The cryptographic module will perform the following power up tests that can be initiated by rebooting the system.

1. Known answer tests for cryptographic algorithms
2. Software Integrity (using an Approved Algorithm) tests on all components in the cryptographic boundary

The cryptographic module is comprised of three sub components viz. the pre-Operating System (pre-OS sub) component, the Operating System (OS) sub component and the User mode sub component. When the cryptographic module is powered up, the sub components load in the following order; pre-OS sub component, OS sub component and then User mode sub component. The cryptographic module is only operational when all sub-components have loaded.

Each sub component will carry out Known Answer Tests (KAT) on the cryptographic algorithms they implement. The known answer tests will be performed before the algorithms are utilized.

Each of the sub-components implements the following FIPS approved algorithms:

- *Pre-OS sub component : AES, SHA-256, HMAC-SHA256*
- *OS sub component : AES, SHA-256, RSA signature generation and verification*
- *User mode sub component : RNG*

The following KAT tests are carried out per sub-component:

- *Pre-OS sub component : AES KAT encryption and decryption, HMAC-SHA256 KAT*
- *OS sub component : AES KAT encryption and decryption, SHA-256 KAT, RSA signature generation and signature verification KAT*
- *User mode sub component : RNG KAT*

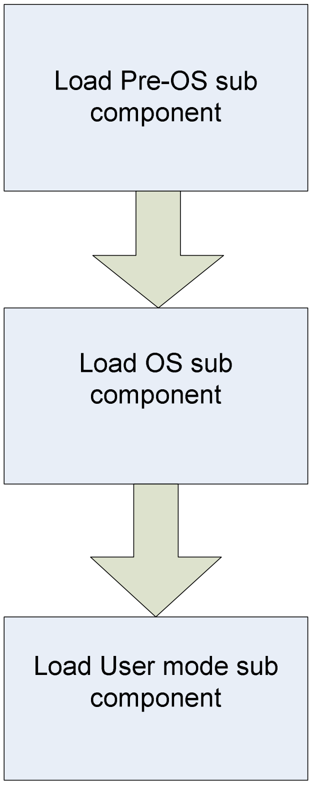
The following conditional tests are carried out:

- *User mode sub component : RNG test failure to a constant value (previous RNG blocks must not be equal to newly generated RNG blocks)*

Software integrity tests using an approved integrity technique will be run on all binaries in each sub component of the cryptographic module. These will be run when each of the three sub-components are loaded on the respective binaries that are contained within them.

- *Pre-OS sub component : HMAC-SHA256*
- *OS sub component : RSA*
- *User mode sub component : RSA*

Figure 4 shows the sequence of loading the sub components for the cryptographic module and the power up KATs and integrity tests performed per sub component.



- AES encryption and decryption KAT
- Software integrity check on pre-OS Sub Component Binaries using HMAC-SHA-256

- SHA256 KAT
- AES encryption and decryption KAT
- RSA sig gen and sig ver KAT
- Software integrity check (RSA) on OS and User Mode Sub Component Binaries as soon as the OS Sub Component has loaded using RSA signature validation.

- RNG KAT

Figure 4. Loading sequence for the Cryptographic module

Failure of any of the KAT tests or integrity tests will disable all cryptographic operations.

Should the integrity tests and algorithm KAT tests pass, the operator is allowed to log into Windows (if authentication credentials are valid) and use the system as normal in FIPS 140-2 mode and the event log status output will indicate that this is the case).

9 FIPS Approved Mode Of Operation

Fixed Disk Encryption

The module's Approved mode of operation is restricted to performing only FIPS-approved cryptographic algorithms and security functions. The module can be installed in either a non-Approved mode or an Approved mode. This is determined by the configuration parameters during installation. Details on installing the module in FIPS Approved mode are given in the Crypto Officers Guide below.

Crypto Officers Guide

The following limitations apply when the product is installed in FIPS mode.

Installation

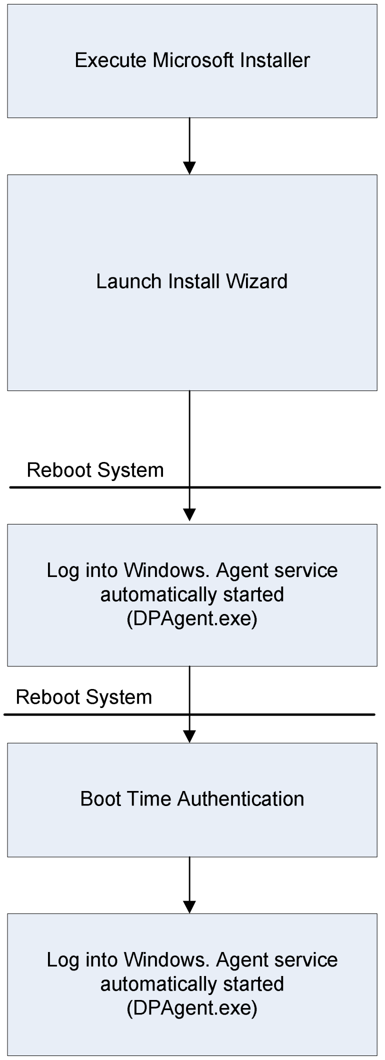
The Crypto Officer shall;

- ensure that the Windows XP operating environment is configured in single user mode. This is done by disabling remote login capabilities, closing any shared resources and restricting user privileges so that the system cannot be accessed as a server.
- select FIPS-compliant mode by checking the FIPS mode check box
- select either password or token based authentication.
- configure local machine password policy including minimum length, minimum uppercase and minimum numeric characters. Passwords are required to be at least 6 characters and at most 28 characters.
- configure the type of disk encryption key to be used. The module encrypts the computer's hard drives using a disk encryption key (the DISK Keys). FIPS mode only allows use of a generated key produced using an approved Key generation algorithm. Construction of a Disk key from a keyphrase or import from a keyfile is not permitted in FIPS mode and this option is disabled if the Crypto Officer has already selected FIPS-compliant mode earlier in the configuration wizard.
- Confirm that the module has been installed correctly in FIPS Approved mode by reviewing the status of the module in the Application Event Log. The event log will show the following messages to indicate that installation in FIPS mode has been successful and that all sub components of the crypto module have been initialized correctly:
    - "DISK Protect has been installed in FIPS mode"
    - "FIPS User Mode Power Up tests passed: Operating in FIPS mode"
    - "FIPS Pre-OS Power Up tests passed: Operating in FIPS mode"
    - "FIPS OS Power Up tests passed: Operating in FIPS mode"

The Crypto Officer may not;

- use the Recovery Console; In environments where a non-approved product may be used, Crypto Officers can use the device recovery process via a Recovery Console. This is a mechanism that allows an authorized user to regain control of a computer after he or she has accidentally entered the wrong password. This type of recovery process is not permitted for use in FIPS mode and must be disabled by ensuring that the 'Enable Device Recovery' checkbox is left unchecked.
- use BeCrypt client installation packages for remote installation of the module via enterprise management tools; Creation of a client deployment package using the PackageWiz utility is not permitted in FIPS approved mode since this feature was excluded during FIPS compliance testing.

The procedure to install the module (DISK Protect) in FIPS compliant mode is detailed in Figure 5. below.


Execute Microsoft Installer
Launch Install Wizard
Reboot System
Log into Windows. Agent service automatically started (DPAgent.exe)
Reboot System
Boot Time Authentication
Log into Windows. Agent service automatically started (DPAgent.exe)

- Copy product components to target machine
- Install Protected mode drivers

Configure Crypto Module for FIPS mode

- Enable FIPS Approved Mode via checkbox
- Select Authentication method: (either password or token)
- Generate Disk Encryption Key
- Configure the initial user
- Configure Single Sign On for the registered user
- Optionally Enable Removable Media Encryption
- Complete the installation : User prompted to reboot the system

- Verify the Protected Mode Driver is installed successfully
- MBR and Real Mode Drivers installed

- User prompted for username and password or token and password
- Log user into Windows if user is authenticated

- Fixed Disk Encryption Starts
- Operators check the Application Event logs to confirm that the module has been successfully initialised in FIPS mode

Figure 5. Install sequence for FIPS approved mode

The installation procedure for DISK Protect for Afaria Security Manager is slightly modified as the module is left in a dormant state after running the Install Wizard before the first reboot. The Crypto Officer is required to re-enable the installation process by setting the StallRMInstallation registry key to 0 (zero) in HKLM/Software/BeCrypt/DISK Protect/. Following this, the system must be rebooted and installation will continue as normal.

Use of Removable Media

Encryption and decryption of removable storage media requires use of a Transport Key. A Transport key is a system key that is owned by all users of a particular computer allowing them to share their encrypted removable devices and the data stored on them. These keys must be generated using an approved random number generator. The procedure to do this is:

- navigate to the Removable Media tab in the Management Tool
- ensure removable media encryption is enabled (if it is not enabled, please enable and restart the machine for the settings to take effect)
- add a key to the user by right clicking the user icon
- generate a random key (this uses an approved random number generator)
- the new key appears as an icon under the user icon
- save the key to a location on disk (Windows user password authentication is required. Please set a password if no passwords are set – logoff / logon required for new password settings to take effect).
- set the newly generated key as the Transport key
- delete or overwrite the generated key that is stored on disk as this is no longer required

Removable media may also be encrypted and decrypted with a Media key that is generated using an approved method. As opposed to Transport keys, Media keys are personal user keys that are not shared system wide.

Since the module does not implement an approved key transport mechanism, Media keys may only be used in FIPS approved mode if they are used on the local PC i.e., they must not be shared between different PC's.

Sharing of Media Keys by groups or users between different PC's is only possible in non-FIPS approved mode.

Please follow the first five steps of process above to generate a media key.

Zeroization

The module provides a decommissioning feature, via the management tool, that allows authenticated crypto officers to purge (zeroize) the disk key (DEK) for the system.

The decommissioning utility is used as part of the zeroization process. In order to zeroize cryptographic keys and CSPs Crypto officers are required to;

1. reprogram any tokens if they are being used
2. purge (zeroize) the disk key (DEK) for the system
3. reformat the HDD and power down the computer

Device Recovery

Recovery using BeCrypt decryption utilities is not permitted in event of irrecoverable self test failure.

The FIPS standard does not allow use of any keys and cryptographic security parameters used in FIPS approved mode to be re-used in non-approved mode. If FIPS self tests fail (and re-running the tests does not resolve the issue), users are asked to power down the module and retry the power up self tests. In environments where only FIPS approved mode is allowed and the FIPS self tests have failed the only recourse is to power down, reformat the disk, rebuild the PC and re-install the product. This approach requires regular back ups of data.

In environments where a non FIPS approved product may be used, a non approved decryption utility may be provided to change the disk key if any of the self tests fail. The decryption utility is required to be run from a separate bootable device (USB storage device, recovery floppy disk or bootable CD). Once the disk has been decrypted, users must remove the boot device with the decryption utility, restart Windows and re-run the Install Wizard to re-generate a key and add users to the system.

Required Practice

Only Crypto Officers with DISK Protect or DISK Protect for Afaria Security Manager Administrative Privileges may carry out configuration (crypto module operational policy and user policy) and recovery tasks. It is required that standard users should not be given sufficient rights to:

- change the cryptographic module local security policy settings;
- stop or start services on the system;
- install or uninstall services;
- install or uninstall system software;
- modify registry settings.

Please note: It is not allowed to start the PC in safe mode.

Users Guide

Users must use the module configured to run in FIPS mode during installation by Crypto Officers as described earlier. The following limitations apply to users when the product is installed in FIPS mode.

- users are requested to make regular backups of data. Data can be securely backed up to removable media storage and encrypted with a transport or media key. Please refer to the Removable media user guide for further instructions on how removable media can be used.
- in the event the PC fails a FIPS test irrecoverably, users must request their administrator or crypto officer to re-build their machine and re-install the cryptographic module. Please note that BeCrypt disk decryption tools cannot be used for recovery in FIPS approved mode.

.

Security Requirements on the Environment

Users and Crypto Officers must observe conventional good security practices as per their organisations security policies when using the module, including:

- using strong passwords and not writing passwords down;
- changing passwords on a regular basis;
- not sharing credentials between users or Crypto Officers;
- not sharing tokens between users or Crypto Officers;
- not leaving the system unattended and logged-in in environments that are unsecured. It is recommended that the machine should be powered down or hibernated when the system is not being used;
- to minimise data leakage in an organisation, it is recommended that removable media should be used with encryption turned on. However, users are to be made aware that all media that appears to Windows as removable storage, will be encrypted (including flash and hard disk mp3 players, memory cards etc.);
- auditing the use of Disk, transport and media keys.

10 References

[1] National Institute of Standards and Technology, *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, available at URL: http://www.nist.gov/cmvp.

[2] National Institute of Standards and Technology, *FIPS 140-2 Annex A: Approved Security Functions*, available at URL: http://www.nist.gov/cmvp.

[3] National Institute of Standards and Technology, *FIPS 140-2 Annex C: Approved Random Number Generators*, available at URL: http://www.nist.gov/cmvp.

[4] National Institute of Standards and Technology and Communications Security Establishment, *Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, available at URL: http://www.nist.gov/cmvp.

[5] National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, available at URL: http://www.nist.gov/cmvp.

[6] National Institute of Standards and Technology, *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-1, available at URL: http://www.nist.gov/cmvp.

11 Glossary

AES Advanced Encryption Standard

CMVP Cryptographic Module Validation Program

CSP Critical Security Parameter

EDC Error Detection Code

EMC Electromagnetic Compatibility

EMI Electromagnetic Interference

FCC Federal Communication Commission

FIPS Federal Information Processing Standard

GINA Graphical Identification and Authentication library

HDD Hard Disk Drive

HMAC Keyed-Hash Message Authentication Code

KAT Known Answer Test

LAN Local Area Network

MBR Master Boot Record

NIST National Institute of Standards and Technology

PUB Publication

RAM Random Access Memory

ROM Read Only Memory

RNG Random Number Generator

RSA Rivest Shamir and Adleman Public Key Algorithm

SHA Secure Hash Algorithm