DeltaCrypt Solutions

DeltaCrypt FIPS Module, V1.0.0.0

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation

February 2010

© 2009 DeltaCrypt technologies inc. All rights reserved. www.deltacrypt.com
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table of Contents

1. INTRODUCTION

Since 2000, DeltaCrypt team of professionals has been concentrating on developing and adapting numerous software products related to corporate security and encryption. Prestigious, security-conscious customers from around the world have joined us over the years.

DeltaCrypt is a software company with a mission to secure mobile data. Mobile devices constantly travel out of the corporate offices and with them goes some of sensitive corporate information. No one can prevent mobile devices from being stolen or lost, however, DeltaCrypt can prevent the financial, legal and embarrassment costs such incidents may cause enterprises, their business partners and their clients. The DeltaCrypt products are detailed in the section 2 below.

Whether you use DeltaCrypt Encryption applications to secure your data-at-rest or to protect your sensitive files from eavesdropping while you work on your computer or mobiles devices, DeltaCrypt versatile encryption applications offer flexible protection.

1.1. Purpose

This is a non-proprietary FIPS 140-2 Security Policy for the “DeltaCrypt FIPS Module v1.0.0.0” cryptographic module. It describes how this module meets 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. FIPS 140-2 (Federal Information Processing Standards Publication 140-2) specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules, this standard identifies requirements in eleven sections. For more information about the standard please visit csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

1.2. References

This Security Policy describes how this module complies with the eleven sections of the Standard

- For more information on the FIPS 140-2 standard and validation program please refer to the NIST website at csrc.nist.gov/groups/STM/index.html
- For more information about DeltaCrypt Technologies inc. please visit www.deltacrypt.com

1.3. Document History

Authors	Date	Version	Comment
Olivier Fournier	29/09/2009	V1.0	Submission
Olivier Fournier	18/02/2010	V1.1	Updated following CMVP first review

1.4. Acronyms and Abbreviations

AES	Advanced Encryption Standard
CO	Crypto Officer
DLL	Dynamic Link Library
DRBG	Deterministic Random Bit Generator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
PUB	Publication
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman Public Key Algorithm
SHA	Secure Hash Algorithm

2. PRODUCT DESCRIPTION

2.1. Cryptographic Module Definition

DeltaCrypt FIPS Module provides core cryptographic functionality for software applications. It supports in the approved mode:

- AES-128, AES-192, AES-256 (encryption/decryption)
- SHA-1 (hashing), SHA-256(hashing), SHA-512(hashing)
- (NIST SP 800-90 DRBG), (Random Number Generation)
- HMAC-SHA1, HMAC-SHA256, HMAC-SHA512 (message integrity)
- RSA-1024 (signature verify only), RSA-2048, RSA-4096 (key generation/sign/verify)

The cryptographic module is comprised of three DLL’s (fips140_2.dll, dtimemory.dll, and plugin manager.dll) that is tested on:

- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows Server 2003

The module has the same structure for all Operating Systems listed above. The module is a multi-chip standalone cryptographic module as defined by FIPS PUB 140-2 consisting of software that executes on a general-purpose PC. It is not available as a separate product but is contained in different security software products such as:

- DUSK Corporate Edition Protection
- DUSK Home Edition Protection
- DUSK-CD Protection
- DUSK Suite
- One Click Home Edition
- Automatic Pro Encryption application
- Automatic Corporate Solution
- DEOS
- Encrypted Backup Solution

In this document, the DeltaCrypt FIPS Module is also referred to as “the Module”.
The Module meets the overall requirements applicable to Level 1 security for FIPS 140-2.

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
Cryptographic Module Security Policy	1
Overall Level of Certification	1

Table 1 : Module Compliance Table

2.2. High Level Block Diagram

Figure 1 shows a block diagram of the cryptographic module that illustrates the physical boundary of the module and shows the module physical interfaces.

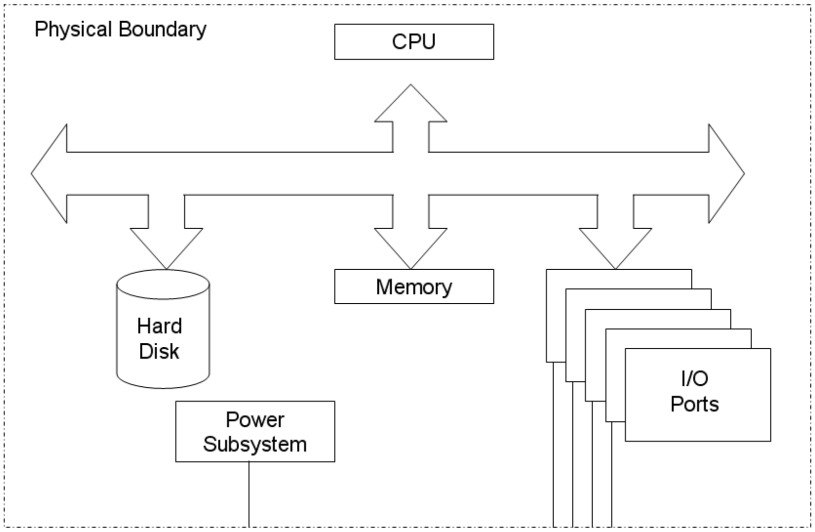

Figure 1 : High Level Block Diagram Showing Physical Boundaries.

2.3. Cryptographic Scheme

The following figure depicts the cryptographic module and its environment:

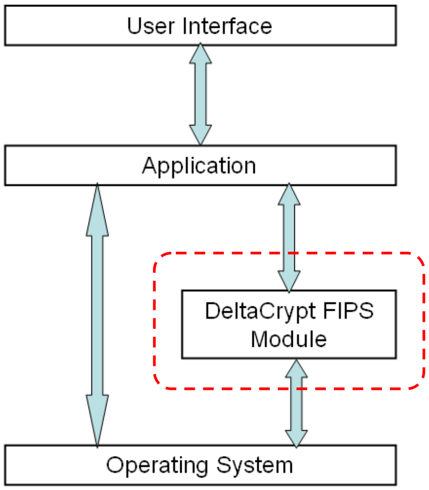

Figure 2 : Cryptographic Scheme

The Red dashed box enclosing the ‘DeltaCrypt FIPS Module’ in Figure 2 represents the ‘Logical Cryptographic Boundary’.

2.4. Cryptographic Algorithms

The Module provides the following FIPS-Approved algorithms:

Approved Security Function	***Certificate***
Symmetric Encryption/Decryption	
AES-128 bits (CBC, ECB, CFB128, OFB) (FIPS PUB 197)	1065
AES-192 bits (CBC, ECB, CFB128, OFB) FIPS PUB 197)	1065
AES-256 bits (CBC, ECB, CFB128, OFB) (FIPS PUB 197)	1065
Message Integrity	
HMAC-SHA-1 (FIPS PUB 198)	600
HMAC-SHA-256 (FIPS PUB 198)	600
HMAC-SHA-512 (FIPS PUB 198)	600
Hashing	
SHA-1 (FIPS PUB 180-3)	1008
SHA-256 (FIPS PUB 180-3)	1008
SHA-512 (FIPS PUB 180-3)	1008
Random Number Generation	
DRBG (SP 800-90A)	12
Signature Verification	
RSA-1024 (ANSI X9.31 and PKCS1.5) using SHA-1, SHA-256, and SHA-512	505
RSA-2048 (ANSI X9.31 and PKCS1.5) using SHA-1, SHA-256, and SHA-512	505
RSA-4096 (ANSI X9.31 and PKCS1.5) using SHA-1, SHA-256, and SHA-512	505

Approved Security Function	***Certificate***
FIPS 186-2 RSA Key Generation	
ANSI X9.31	505

Table 2 : Cryptographic Algorithms

In addition to the FIPS-Approved algorithms, the module includes an NDRNG that is used for seeding the module's SP 800-90A DRBG.

3. MODULE PORTS AND INTERFACES

The below table describes the relationship between the logical and physical interfaces:

FIPS 140-2 Interface	Logical Interface	Physical Interface
Data Input interface	Input data as parameters to API function calls	Keyboard Interface, , Hard Drive, CD Drive, USB Interface, Network Interface, RS-232 Interface, Parallel Interface
Data Output interface	Output data as parameters from API function calls.	Hard Drive, CD Drive, USB Interface, Network Interface, RS-232 Interface, Parallel Interface
Control Input interface	Any commands that are input that are used to configure or control the operation of the module	Mouse Interface, Keyboard Interface,
Status Output interface	Return values of certain API function calls	Monitor Interface
Maintenance Interface	Not applicable	Not applicable
Power Interface	Not applicable	PC power interface

Table 3 : Mapping Physical and Logical Interfaces

4. ROLES, SERVICES AND AUTHENTICATION

The module supports a crypto officer role and a user role that are implicitly assumed by each role depending on the service executed by the role:

- The Crypto Officer role has the responsibility of correctly installing, deploying and configuring the security of the data encryption. The crypto officer is also responsible for running self-tests and displaying "Status".
- The User Role performs basic operations as encryption/decryption, hashing, signature.

4.1. Identification and Authentication

The Module does not deploy authentication mechanisms.

4.2. Roles and Services

The Module supports the services listed in the following table. The table groups the authorized services by the operator roles and identifies the Cryptographic Keys associated with the services.

Authorized Services	CO	User	Cryptographic Keys and CSPs	Access
Symmetric Encrypt/Decrypt	X	X	AES-128, AES-192 or AES-256	Execute
RSA Key Generation	X	X	RSA-2048 or RSA-4096	Execute
RSA Verify	X	X	RSA-1024, RSA-2048 or RSA-4096	Execute
Hash Calculation	X	X	None	Execute
HMAC Generation	X	X	HMAC Key	Execute
Generate Random Number	X	X	DRBG Key	Execute
Zeroization	X	X	All keys and Critical Security Parameters	Execute
Show Status and Version	X		None	Read
Run Self-Test	X	X	None	Execute

Table 4 : Roles and Services

5. CRYPTOGRAPHIC KEY MANAGEMENT

The module contains the following keys within the module:

Key	Generation	Storage	Use	Role
AES Key	Generated internally using the DRBG	Stored in NVRAM	Used for data encryption and decryption.	User CO
HMAC Key	Generated internally using the DRBG	Stored in NVRAM	Used as part of the keyed hash function	User CO
DRBG Key	Hard coded	Stored in NVRAM	Used as part of the DRBG function	CO User
DRBG “V” Value	Internal state of DRBG	Stored in NVRAM	Used as part of the DRBG function	User CO
RSA Integrity Key	Generated outside of the module.	Hard coded	Used as part of the software integrity test	CO
RSA Public/Private Key Pair	Generated internally using the DRBG	Stored in NVRAM	Used for verify operations	User CO

Table 5 : Keys and CSPs

DeltaCrypt FIPS Module provides the underlying functions to support FIPS 140-2 Level 1 key management.

5.1. Key generation

DeltaCrypt FIPS Module provides FIPS 140-2 compliant key generation for asymmetric keys using ANSI X9.31.

The underlying random number generation uses a FIPS Approved method, SP 800-90A algorithm for generating symmetric keys

5.2. Key storage

The HMAC key is stored at the same place the module is stored. All the other keys are temporarily stored in RAM memory until the keys are zeroized as soon as the module does not use it anymore.

5.3. Key entry and Output

Keys are passed to the module as API parameters from function calls in either plaintext or encrypted form. Keys are output in encrypted form. It is a function of an application to output keys.

5.4. Key zeroization

All keys are zeroized when no longer needed. When executing the function *"memset(&(v),0,sizeof(v));" "v" is the variable to zeroize.*

6. SELF-TESTS

The Module performs the following self tests before opening the application:

6.1. Power-up Tests

6.1.1. Tests upon Power-up

Self-tests are initiated automatically by the module at start-up.

6.1.1.1. Known Answer Tests (KATs)

Known Answer Tests are performed on:

- AES-128 bit, AES-192 bit and AES-256 bit (encrypt/decrypt). All key sizes are tested.
- RSA-1024, RSA-2408, RSA-4096 (verifying). Only RSA-1024 is tested.
- HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512
- SHA-1, SHA-256, SHA-512
- SP 800-90A DRBG

Known Answer Tests for encryption/decryption or hashing, function by encrypting (or hashing) a string for which the calculated output is known and stored within the cryptographic module. An encryption or hashing test passes when the newly calculated output matches the expected (stored) value. A test fails when the calculated outmatch does not match the expected value. The test then decrypts the cipher text string. A decryption test passes when the freshly calculated output matches the plaintext value. A test fails when the calculated output does not match the plaintext value.

6.1.1.2. Software Integrity Test

The module checks the integrity of all cryptographic components listed above using an RSA 2048-bit signature verification. The module is provided with a pre-computed RSA Signature as part of the software integrity check. The entire module shared library (DLL) is verified against this signature. If the signature verification fails, the module is transitioned to the error state and is finally set back to the non-initialized state, where no further cryptographic operations are possible. In this case the user should retry initialization, if this doesn't fix the error, he will have to uninstall and re-install the module from the original installation media.

6.1.2. On-Demand Self-Tests

On-demand self tests may be invoked by the Cryptographic Officer or User and will run all the KATs. The test is done by the function *sFIPSGUI_StartTest*.

6.2. Conditional Tests

6.2.1. Conditional Tests

A test is run each time the DRBG generates a random number. The test involves comparing the generated value with the previously generated value. DRBG discards the first value generated after a power reset where every value after the first number generated is checked against the previously generated value. If the test fails, the module enters an error state. In addition, the module performs the SP 800-90A Health Tests for the Instantiate, Generate, and Reseed functions.

6.2.2. Pair wise Consistency Test

Pair wise consistency tests are run on demand when the module generates key pairs. The module performs a sign with the private key and verifies it with the public key. If the test fails, the module will enter the error state.

6.3. Self-Tests Result

To indicate failure of self-tests; the module displays an error message box containing a description of the error. In this case, the Module will be placed in Error State and the application will not start.

7. Cryptographic Module Security Policy

As the Module only contains FIPS Approved Cryptography, each product with the Module is running in FIPS Mode. Although the module does not support key entry or output by itself, it is recommended that any keys to be output from the physical cryptographic boundary be output in encrypted form.

7.1. Module installation

The module is one part of the software product. It is installed during the product installation process as well as all other DLLs.

The Module is distributed from the Internet using a link to download it. In order to install the product correctly, you must follow download installation instructions. You must have sufficient amount of space on the hard disk, enough memory and have administrative privileges on the computer where the product is being installed.

To validate that the Module has been successfully installed and is operated in the FIPS Approved Mode, you should follow these steps:

- For the DUSK, DUSK-CD, One Click Home Edition, Automatic Pro, Automatic Corporate Solution, Encrypted Backup Solution applications
  - Open the application
  - Go to the Help menu
  - Select the About menu
  - Make sure that FIPS version appears
- For the DUSK Suite (DUSKWatch) application:
  - Go to Start menu
  - Select All Programs > DeltaCrypt > DUSKWatch menu
  - Make sure that the FIPS version appears

7.2. Module initialization

The module must be initialized with successful completion of all self tests as documented in section 6 above. The self tests must be performed as part of the module initialization and can also be performed on demand by either COs or Users.

The steps to securely initialize the module are as follows:

- Configure the host PC in single user mode by disabling the guest account
- Initialize the module to run Self Tests
- After successful initialization, users may operate the module and access the cryptographic services implemented by the module.
- The CO must verify that they have a FIPS validated module by verifying the version of the module as 1.0.0.0 in the About section of the application. If the module fails the power on self-test or on demand self-test, the module will not return the version of the FIPS module indicating that the module is not loaded.
- Operators of the module shall not use RSA Signature Generation.
- Operators of the module shall not use 1024-bit RSA Key Pair Generation

8. Design Assurance

The Module is designed and developed using C and C++ languages. Integration build is performed every day. Each function (at creation or at modification) is validated by self-tests and user tests in order to run regression tests. Every release of products is specifically tagged with a build version number. Microsoft Visual SourceSafe (VSS) version 6.0 is used to provide configuration management. This software provides access control and versioning. VSS also maintains an internal revision history of each file of the module’s.

When new software is received by an organization or individual, the procedures outlined in the Quick Start Guide and the Administration manual should be followed. The Module can be installed or deployed using an EXE or a MSI.

9. Mitigation of Other Attacks

The module does not claim to mitigate any attacks.

Appendix: CKG as per SP800-133

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP800-133 (vendor affirmed). The resulting RSA key, is a modified output from the SP800-90A DRBG generated seed.