Data Encryption Systems Ltd.

DESlock+ Kernel Mode Crypto Core V1.0.0.2

FIPS 140-2 Non-Proprietary Security Policy

Status:	See Change History
Version:	2.0
Date:	25 January 2010
Author:	J. P. Baycock (DES)

Data Encryption Systems

Table of Contents

Table of Figures

1. Introduction

1.1. Purpose

This Document is a non-proprietary FIPS 140-2 Security Policy for the DESlock+ Kernel Mode Crypto Core V1.0.0.2 cryptographic module. It describes how this module meets all the requirements as specified in the FIPS 140-2 standard. 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 visit

http://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 FIPS 140-2 Standard.

For more information on the FIPS 140-2 standard and validation program please refer to the NIST website at

http://csrc.nist.gov/groups/STM/index.html

For more information about DESlock+ please visit

http://www.deslock.com

1.3. Schedule Change History

Version	Date	Author	Description
1.0	19/08/2009	J. Baycock	Updated following functional testing
2.0	25/01/2010	J. Baycock	Updated following CMVP first review

1.4. Vocabulary

- **DES** Data Encryption Systems Ltd.
- **Triple-DES** Implementation of the Data Encryption Standard
- **SHA** Secure Hash Algorithm
- **AES** Advanced Encryption Standard
- **Crypto Core** The DESlock^{+} Kernel Mode Crypto Core
- **The Module** The Crypto Core
- **CSP** Critical Security Parameters
- **KAT** Known Answer Test
- **CO** Crypto Officer
- **PRNG** Pseudo Random Number Generator

2. Product Description

The DESlock+ Kernel Mode Crypto Core is a FIPS 140-2 level 1 compliant software based cryptographic module residing at the kernel mode level of the Windows Operating System.

The cryptographic module is a Kernel Mode Device Driver in the form of a .sys system driver file. The module is designed to operate in a 32 bit operating environment.

The Module encapsulates several different cryptographic algorithms in an easy to use cryptographic module accessible by other Kernel Mode drivers and User Mode applications provided by DES (Data Encryption Systems Ltd).

The Crypto Core implements Triple-DES, AES, SHA-1, SHA-256, SHA-512, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512 and ANSI X9.31 PRNG algorithms in the FIPS mode.

In addition to the FIPS approved algorithms the Crypto Core can also implement Blowfish and MD5 algorithms when operating in non-FIPS Mode.

3. Module Compliance Table

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles Services and Authentication	1
Finite State Machine Model	1
Physical Security	N/A
Operational Environment	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	1
Overall Level of Certification	1

Figure 1 - Module Compliance Table

The module is a software module, and as such depends on its host system for its physical characteristics. However both the test and the host platforms have been tested for, and meet, applicable Federal Communications Commission (FCC) EMI and EMC requirements for residential and small office use as defined in Subpart B, Class B of FCC 47 Code of Federal Regulations Part 15.

4. Module Ports and Interfaces

The Crypto Core is classified as a multi chip stand alone module designed to meet FIPS 140-2 level 1 requirements. The physical interfaces of the module are the same as the computer system on which it is executing. The logical interfaces are the 'C' programming API calls through which the module is providing its services.

5. Cryptographic Hardware Boundary

For FIPS 140-2 purposes the Module has a physical cryptographic hardware boundary that comprises the contiguous enclosure of the computer system upon which the operating system and the crypto core execute (as the module is defined as a multi chip stand alone module).

The logical cryptographic boundary of the Module is the boundary which incorporates the .sys system driver.

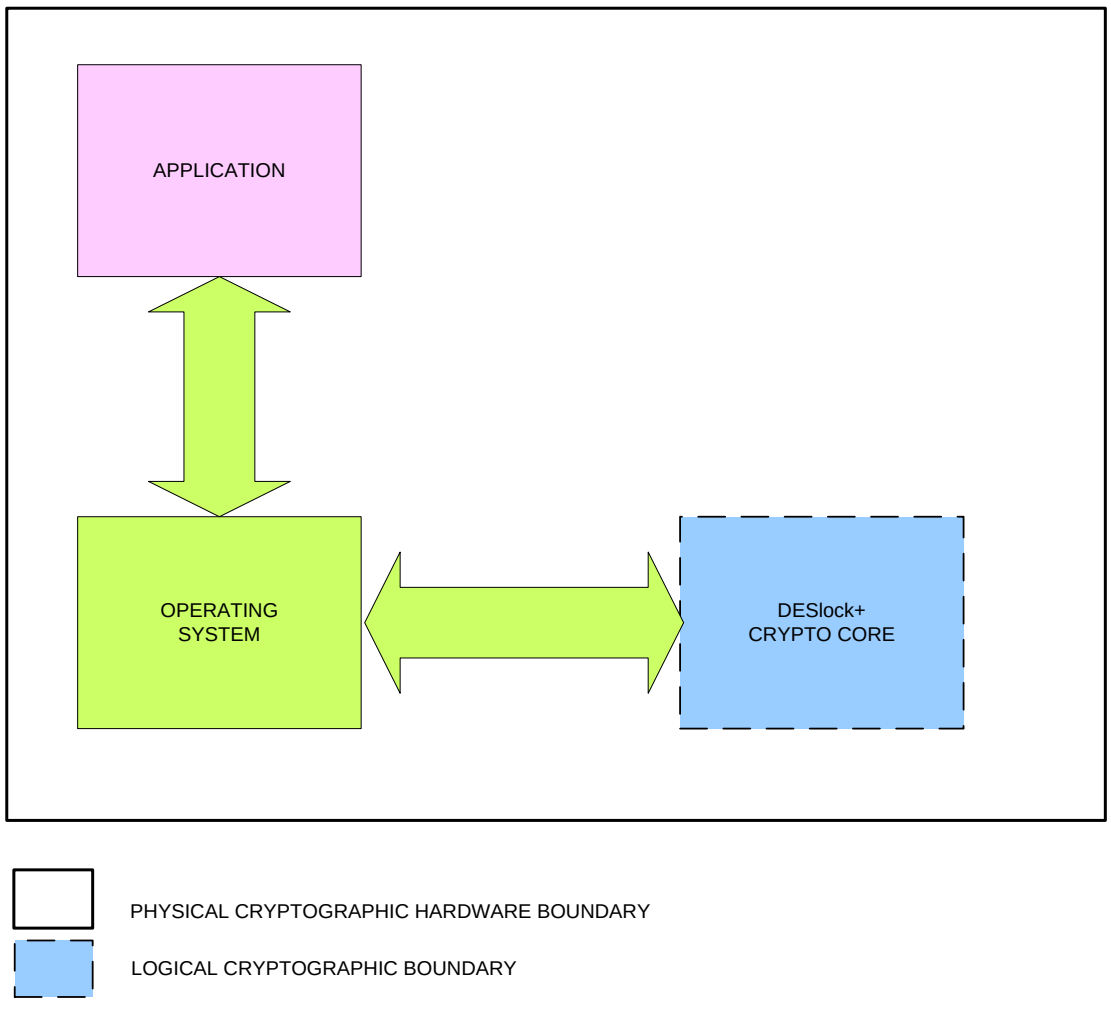

Figure 2 – Cryptographic Boundaries

6. Operational Environment

For the purposes of all FIPS140-2 testing, the Module was installed and tested on a Dell E520 System with the following specification:-

- Intel Core2 Duo 6300 1.86GHz processor
- 1GB DDR2 System RAM
- 80GB Hard Drive
- Windows XP Professional Service Pack 2 (Operating in single user mode)
- This system was approved to FCC standards Class B requirement

7. Mapping Physical and Logical Interfaces

The table below describes supported logical and physical interfaces as well as the relationships between them.

FIPS 140-2 Interface	Logical Interface	Physical Port
Data Input	API functions that accept input data arguments	PC USB port, Network port, Keyboard port, Mouse port, optical drive floppy drive.
Data Output	API functions that produce output in arguments	PC USB port, Network port, optical drive, floppy drive.
Control Input	API functions to initialize and control the operation of the module	Keyboard port, Mouse port, PC power button
Status Output	API functions return values which return information regarding module status	PC monitor
Power	N/A	N/A

Figure 3 - Mapping Physical and Logical Interfaces

8. Roles Services and Authentication

The Crypto Core implements the following two roles: Crypto-Officer and User. Maintenance role is not supported. The roles are implicitly assumed and the module does not provide an authentication mechanism that would allow to explicitly distinguish users between the supported roles.

FIPS-140-2 mandates that a cryptographic module be limited to a single user at a time, as such the operating system within which the module functions must be configured in Single User mode.

8.1. Identification and Authentication

Described here are the types of authentication implemented

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

Figure 4 - Authentication Types Supported

8.2. Roles and Services

The table below lists supported FIPS approved and Non-FIPS approved authorised services. For each service it specifies which role the service can be used in, what cryptographic keys and critical security parameters (CSP's) the service can access and how.

Access Types

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 (this item is used as part of the cryptographic function)

Role		Approved or Allowed Services	Access Type
CO	**User**		
FIPS Approved Mode			
X		Installation	E
X	X	Initialization	E
X	X	Show status	R
X	X	Power-on Self Test	E
X	X	Random Number Generation	W/E
X	X	Key zeroization	W/E
X	X	Symmetric Encryption/Decryption • AES • Triple-DES	W/E
X	X	Digest Algorithms • SHA-1 • SHA-256 • SHA-512	W/E
X	X	Message Authentication • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-512	W/E
Non-FIPS Approved Mode			
X	X	Symmetric Encryption/Decryption • Blowfish	W/E
X	X	Digest Algorithms • MD5	W/E

Figure 5 – Roles and Services Table

9. Cryptographic Key Management

9.1. Implemented Algorithms

The Crypto Core provides random number generation routines for all the algorithms listed in the Roles and Services table above. Since the module implements both FIPS approved and Non-FIPS approved algorithms, it is the responsibility of the user to ensure only the FIPS approved services are being used.

9.2. Key Generation

The module provides services to generate pseudo-random symmetric according to the FIPS Approved ANSI X9.31 standard.

9.3. Key Entry and Output

The module does not import or export keys. It is the responsibility of the application that loads the Module to protect keys when they're being exported or imported across the physical cryptographic boundary. It is also the responsibility of the application to ensure that only FIPS Approved cryptographic algorithms are being used for key protection.

9.4. Key Storage

The module does not provide any long-term key storage. Keys are zeroized when they are no longer required.

9.5. Zeroization of Keys

The following precautions are taken to make sure that all keys and seeds are being destroyed properly:

- Module zeroizes all intermediate security sensitive material.
- Module zeroizes all keys passed to the authorised services when the services are no longer needed and are being destroyed.

9.6. Supported Keys

The following table identifies the Cryptographic Key and Critical Security Parameters employed within the module.

Key	Generation	Storage	Use
Triple-DES AES	Generated internally using a PRNG compliant to ANSI x9.31	Key not stored	Used to encrypt/decrypt data
ANSI X9.31 PRNG Seed Key	Generated internally using OS provided data	Key not stored	Used to generate random numbers during key creation in FIPS mode
Integrity Check key HMAC-SHA-256	Hard coded with the module at compile time	Compiled in the binary	Used to verify modules integrity at initialisation
HMAC	Generated internally using a PRNG compliant to ANSI x9.31	Key not stored	Used as part of the HMAC generation process

Figure 6 – Cryptographic Keys, CSP's and HMAC

9.7. Algorithm Certification

The following table details the algorithms available within the module and the corresponding FIPS-140-2 Validation Numbers

Algorithm	Validation Number	Modes / Keying Opts. / Description / Notes
Triple-DES	790	TECB(e/d; KO 2); TCFB8(e/d; KO 2); CTR (int only; KO2)
AES	1042	ECB(e/d; 128,192,256); CTR (int only; 128,192,256)
SHA-1 SHA-256 SHA-512	992	SHA-1 (BYTE-only) SHA-256 (BYTE-only) SHA-512 (BYTE-only)
RNG	593	ANSI X9.31 [AES-256Key]
HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512	584	(Key Sizes Ranges Tested: KS=BS) MAC Sizes Supported 20, 32 & 64 SHS Val 992

Figure 7 – FIPS Approved Algorithm Certification Table

The following table details the non FIPS approved algorithms available within the module.

Algorithm	Description
Blowfish	Symmetric encryption/decryption
MD5	MD5 hashing

Figure 8 – Non FIPS Approved Algorithms

10.Self Test

10.1. Power-On Self Tests

Software Integrity Test

The module is shipped with a pre-computed HMAC. As part of the software integrity check, the entire system driver file (.sys file) is verified against this HMAC-SHA-256. At load time the Driver is checked for integrity by calculating a HMAC-SHA-256 of the file on disk and comparing the result against both an embedded HMAC value and an external HMAC value.

Known Answer Tests

During initialisation the module performs a series of known answer tests for all FIPS approved algorithms according to the following table.

Algorithm Type	Known Answer Test Executed
Random number generator	ANSI X9.31 PRNG is initialized with a hard coded seed and internal values. A request to generate random numbers is then issued and the result compared to a pre-computed value.
Hash Functions • SHA-1 • SHA-256 • SHA-512	For each of the supported hash functions, a hard coded sample of text of various lengths is hashed, and the result compared to the pre-computed hashes.
Message Authentication • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-512	For each of the supported HMACs, a hard coded sample of text of various lengths and hard coded keys is used to generate HMAC. The results are compared to the pre-computed values.

Algorithm Type	Known Answer Test Executed
Symmetric Encryption/Decryption • Triple-DES TCFB • AES ECB	For each of the supported algorithms, a hard coded plaintext is encrypted with a hard coded key and the result compared to the pre-computer ciphertext. If the comparison is successful then the ciphertext is decrypted and compared to the original plaintext.

Figure 9 – Known Answer Tests

Conditional Tests

Conditional tests are executed after the module has been successfully initialised.

ANSI X9.31 PRNG Conditional Test

This test is executed each time the next 256-bit block of pseudo random numbers is generated. The first random number generated is not used, but stored and compared with the next random number generated. If the two values are equal the random number will not be used and a new random number will be generated and compared. If the same value is generated five times the module considers the random number generator to be stuck and enters the error state whereupon no other cryptographic operations are possible.

11. Crypto-Officer and User Guidance

11.1. Setup and Initialisation

The Crypto Core is distributed as part of the DESlock+ protection system. In order to install the Crypto Core correctly you must follow installation instructions included with the DESlock+ protection system. You must have sufficient disk space, enough memory, and poses Administrator Rights on the target machine.

It is the responsibility of the Crypto-Officer to configure the Operating System so as to operate securely and to prevent possible remote login. In order to configure the Operating System in single user mode the following steps should be taken:-

Disable “Server” and “RunAsService” services in the computer system (unless these are not installed or have already been disabled). To do that, the Crypto-Officer runs the “Services” applet in the Control Panel of the computer system, select the services to be disabled from the list one by one, and set their Startup Type to “Disabled”. The Crypto-Officer must have administrative privileges in the computer system being configured.

To validate that the module has been installed correctly and is operating in the FIPS approved mode, you should do the following:

1. Open a command line console
2. Navigate to the installation directory of the software
3. Execute dlcc_ver.exe and verify that the version displayed is 1.0.0.2 and that the FIPS approved mode indicator reads ‘YES’

Alternatively you may use the DESlock+ protection system about dialog to verify this information. This can be accessed from the windows tray bar.

11.2. Cryptographic Module Security Policy

When operating in FIPS mode the module must operate under the following rules.

1. Only FIPS approved algorithms will be used.
2. The Operating System must be configured in Single User Mode where all guest user accounts are disabled.
3. Any encryption keys exported outside of the module physical boundary must be encrypted using FIPS approved algorithms.

12. Mitigation of Other Attacks

The module does not mitigate against any specific attacks.