FIPS140-2 Security Policy for IBM CryptoLite in C (CLiC)

FIPS140-2 Security Policy for CryptoLite in C (CLiC)

October 2003

Revision: 1. 3

NON CONFIDENTIAL

Status: Released

First Edition (October 2003)
This edition applies to the First Edition of the IBM BlueZ – FIPS140-2 Security Policy for Crypto Lite in C and to all subsequent versions until otherwise indicated in new editions. IBM welcomes your comments on this publication. Please address them to: bluez@zurich.ibm.com. When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

1. Document Information

1.1. Document Scope

This document is a non-proprietary FIPS 140-2 Security Policy for the IBM BlueZ 'CryptoLite in C' (CLiC), Version 3.0 (FIPS140/Prod) cryptographic module. It contains a specification of the rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-2 (Federal Information Processing Standards Publication 140-2) for a Level 1 multi-chip standalone module. This Policy forms a part of the submission package to the testing lab.

FIPS 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.

- For more information on the FIPS 140-2 standard and validation program please refer to the NIST website at http://csrc.nist.gov/cryptval/.
- For more information about IBM BlueZ software please visit http://bluez@zurich.ibm.com

1.2. Table of Contents

2. Applicable documents

Cryptography

RSA Laboratories PKCS #15 v1.0: Cryptographic Token Information Format Standard – April 23, 1999
RSA Laboratories PKCS#15 v1.0 Amendment 1 Draft #1 - October 20, 1999
FIPS 140-2 standard, the *Derived Test Requirements*, and on-line implementation guidelines
Digital Encryption Standard: FIPS PUB 46-3, FIPS PUB 74, and FIPS PUB 81
SHA-1: FIPS PUB 180-1
Digital Signature Standard : FIPS PUB 186-2 27 January 2000
Pseudo-random Number Generation: Appendix 3 of FIPS PUB 186.
Digital Signature Scheme Giving Message Recovery: ISO/IEC 9796
The 3DES standard, ANSI X9.52, *Triple Data Encryption Algorithm Modes Of Operation*
Advanced Encryption Standard (AES) FIPS Publication 197, November 26, 2001
Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry. ANSI X9.31-1998

3. CLiC Library

3.1. Module Components

The following table lists the module components:

Type	Name	Release
Software	CLiC– (jclic_sslite140.dll)	Version 3.0 (FIPS140/ Prod)
Documentation	CLiC User Guide	

Table 1a: Module Component List for MS Windows

Type	Name	Release
Software	CLiC – (jclic_sslite.so)	Version 3.0 (FIPS140/ Prod)
rDocumentation	CLiC User Guide	

Table 1b: Module Component List for Unix

3.2. Module Description

The IBM BlueZ CLiC Library, from hereon known as CLiC, consists of a single dynamically-linked library (DLL) named jclic_sslite140.dll under MS Windows and a single loadable module named jclic_sslite140.so on unix based systems. The cryptographic boundary for CLiC is defined as the enclosure of the computer system on which the cryptographic module is to be executed.

4. Security Levels

The IBM CLiC module meets the overall requirements applicable to Level 1 security of FIPS 140-2. The individual security requirements specified for FIPS 140-2 meets the level specifications indicated in the following table.

Security Requirements Section Level	
Cryptographic Module	1
Ports and Interfaces	1
Roles and Services	1
Finite State Model	1
Physical Security	1
Operational Environment	1
Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Table 2: FIPS 140-2 certification levels

5. Cryptographic Module Specification

The IBM CLiC module is classified as a multi-chip standalone module for FIPS 140-2 purposes. As such, the CLiC Module must be tested upon a particular operating system and computer platform. The actual cryptographic boundary thus includes the CLiC Module running upon an IBM-compatible PC running the Windows™ 2000 Operating System (OS) or Red Hat Linux (version 8.0). The CLiC Module running on this platform was validated as meeting all FIPS 140-2 level 1 security requirements. The CLiC Module is packaged in a single DLL, named jclic_sslite140.dll or loadable module named jclic_sslite140.so, which contains all the code for the module. IBM CLiC also runs upon many other platforms including Windows '95, '98, and NT, Sun/Solaris, HP-UX, Linux, and AIX; however, the CLiC Module was not implemented and tested upon each of these platforms as part of this effort.

As outlined in G.5 of the Implementation Guidance for FIPS 140-2, the module maintains its compliance on other operating systems, provided:

- the GPC uses the specified single user operating system/mode specified on the validation certificate, or another compatible single user operating system, and

- the source code of the cryptographic module does not require modification prior to recompilation to allow porting to another compatible single user operating system.

The IBM CLiC module for Windows was tested and validated on the Microsoft Windows 2000 with Service Pack 4 operating system. The software module maintains compliance when running on the Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT, and Microsoft Windows XP operating systems.

The IBM CLiC module for Linux was tested and validated on the RedHat (Version 8.0) distribution of the Linux operating system. The software module maintains compliance when running on other Linux based distributions such as Suse.

Hardware	Operating System
IBM PC Compatible	Windows 2000, SP3
IBM PC Compatible	RedHat Linux Version 8.0

Table 3: Platforms on which CryptoLite has been tested

The module provides no physical security features aside from the enclosure of the PC which the module runs on. Additionally, the computer that CryptoLite was tested on met the applicable FCC requirements. Finally, the module does not mitigate against any special attacks.

5.1. Cryptographic Standards

The IBM CLiC module supports the following approved and non approved FIPS algorithms.

HASH Services

Algorithm	Specification	FIPS Approved
MD2	**IETF RFC1319** Hash algorithm; hash size: 16 bytes; block size: 16 bytes. Used only for backward compatibility.	No

MD5	**IETF RFC 1321** Hash algorithm; hash size: 16 bytes; block size: 64 bytes. Used only for backward compatibility.	No
SHA-1	**FIPS180-1** Hash algorithm; hash size: 20 bytes; block size: 64 bytes.	Yes
SHA256	Hash algorithm; hash/block sizes: 32/64, bytes.	No
SHA384	Hash algorithm; hash/block sizes: 48/128 bytes.	No
SHA512	Hash algorithm; hash/block size 64/128 bytes.	No

Table 4: Hash Services

CIPHER Services

Algorithm	Specification & Description	FIPS Approved
RC2	**IETF: RFC2268** Symmetric block cipher. Block size 8 bytes. Key size 0-1024 bits. RC2 allows adjustment of the effective key strength independent of the input key length.	No
RC4	Stream cipher; key sizes: 0-2048 bits.	No
RC6	Symmetric block cipher; block size: 16 bytes; key sizes: 0-? bits. RSA DSI Inc. candidate for AES	No
DES, DES-CBC	**FIPS 46-3** Symmetric block cipher; block size: 8 bytes; key size: 56 bits.	Yes
3DES, 3DES-CBC	**FIPS 46-3** Triple DES has 112/168 bits key length depending on type of key.	Yes
MDC1, MDC-2, MDC-4	Owned by IBM., Patent: US4908861 Modification detection codes (MDC) based on DES cipher. There are different schemes called MDC-1, MDC-2, and MDC-4. Mainly used for backward compatibility with main frame systems. Modern hash algorithms are much faster.	No
UNIX_CRYPT	Unix password encryption based on a modified DES.	No
AES **AES CBC** **AES256**	FIPS197 Symmetric block cipher; block sizes: 16,24,32 bytes; key sizes: 16,24,32 bytes.	Yes
BLOWFISH	Blowfish encryption/decryption and macing; bock-size: 8 bytes	No
HMAC SHA-1	Hashed Message Authentication Codes (HMAC) based on the SHA-1 hash algorithm.	Yes

Table 5: Cipher Services

Public Key

Algorithm	Specification	FIPS Approved
RSA Sign/Verify	Public key encryption/signature scheme. Typical key/data sizes: 512, 768, 1024 (typical), 2048 bits.	Yes
RSA Encrypt/Decypt	RSA specification and padding scheme: PKCS#1	No

	OAEP Padding scheme for RSA encryption: RFC2437 PSS padding scheme for RSA signatures: Encryption, signing requires a padding scheme (typically PKCS#1, OAEP).	
DSA Sign/Verify	Public key signature scheme. Cannot be used for encryption. Key sizes: 512-1024 bits in steps of 64 bits.	Yes
DH	Public key crypto system. Typical key/data sizes: 512, 768, 1024 (typical), 2048 bits. Used for key agreement.	No

Table 6: Public Key Services

Random Number Generators

Algorithm	Specification	FIPS Approved
PSEUDO Random Number Generator	**FIPS 186-2** **ANSI X9.31 1998** .	Yes
Universal Software Based True Random Number Generator	Patented by IBM, EC Pat.No. EP1081591A2, True random number generator that works reliably on variety of platforms without exploiting platform specific features. Entropy evaluation through statistical analysis. Performance: 20-1000 bits/seconds.	No

Table 7: Random Number Generator Services

5.2. Module Interfaces

As a multi-chip standalone module, the CLiC Module's physical interfaces consist of the keyboard, mouse, monitor, serial ports, network adapters, etc. However, the underlying logical interface to the CLiC Module is a C- language Application Program Interface (API) documented in the CLiC Library Reference Manual. The module provides for Control Input with the exported DLL library API calls. Data Input and Output are provided in the variables passed with API calls, and Status Output is provided in the returns and error codes that are documented for each call. The CLiC Module is accessed from C/C++-language programs using the same method as the CLiC static toolkit, via the inclusion of the include file "CLiC.h".

5.3. Cryptographic Module Self Tests

The CLiC module implements a number of self-tests to check the proper functioning of the Module. This includes power-up self-tests and conditional self-tests. Conditional tests are performed when symmetric or asymmetric keys are generated. These tests include a continuous random number generator test and pair-wise consistency tests of the generated RSA keys.

Startup Self-Tests
Power-up self-testing is initiated automatically when the CLiC module starts loading. (See the CLiC Finite State Machine for more details). These tests comprise of the software integrity test and the known answer tests of cryptographic algorithms. Should any of these tests fail; the CLiC module will terminate the loading process. The module cannot be used in this state.

The integrity of the module is verified by checking a HMAC SHA-1 of the all of the module file. The Initialization will only succeed if this HMAC SHA-1 is valid.

The CLiC module executes the following cryptographic algorithms tests:

- DES KAT
- 3DES KAT
- AES KAT
- SHA-1 KAT
- SHA256 KAT
- SHA384 KAT
- SHA512 KAT
- RSA_SIGN/VERIFICATION
- RSA_ENCRYPTION/DECRYPTION
- DSA PARAMETER GENERATION
- DSA_SIGN/VERIFICATION
- RNG KAT

Startup Recovery
Should the startup self tests fail during module initialization the crypto officer should reinstall the complete application.

Conditional Self-Testing
This includes continuous PRNG testing. The very first output block generated by the PRNG is never used for any purpose other than initiating the continuous PRNG test which compares every newly generated block with the previously generated block. The test fails if newly generated PRNG output block matches the previously generated block. In such a case, the Module enters the Conditional Error state and all data output from the responsible function during the error condition is inhibited. It is the responsibility of the calling application to handle the exception, for example by retrying the PRNG service.

Pair-wise Consistency Self-Testing
The test is run whenever the CLiC Module generates a private key. The private key structure of the Module always contains either the data of the corresponding public key or information sufficient for computing the corresponding public key.

5.4. Operational Environment

The CLiC security module is written mostly in the C programming language that allows for extensive review to confirm security. CLiC is developed and maintained according to IBM's internal development standards and tools including CVS (Version 1.11.1p1) are used for configuration management.
The CLiC module implements both approved and non-approved services. The calling application controls the cryptographic material as well as the services that use them. It is the applications responsibility to ensure that when in a FIPS compliant mode, only those FIPS approved algorithms are used.

5.5. Module Status

The module communicates any error status asynchronously through the use of return codes. It is the responsibility of the calling application to handle these exceptions.

6. Roles and Services

6.1. Roles

The CLiC module supports two roles, a cryptographic officer role and a user role.

- ROLE_CO: The Cryptographic Officer Role is purely an administrative role and does not involve the use of any of the modules cryptographic services. The role is not explicitly authenticated but assumed implicitly on implementation of the modules installation and usage sections defined in the security rules section.

- ROLE_USER: The User Role has access to all of the modules services. The role is not explicitly authenticated but assumed implicitly on access of any of the modules services.

Role	Type of Authentication	Authentication Data
Cryptographic Officer Role	None	None
User Role	None	None

Table 8: Roles and Required Identification and Authentication

6.2. Services

The modules services are accessed through API interfaces from the calling application.

Services	User Role
Self Tests	Yes
AES encryption/decryption, MACing and internal key generation services	Yes
Blowfish encryption/decryption, MACing. And internal key generation services	Yes
DES/3DES encryption/decryption and internal key generation services	Yes
Diffie-Hellman key exchange and parameter generation	Yes
DSA signature generation, verification and parameter generation services.	Yes
Key Import and Export services	Yes
HMAC services	Yes
ISO 9796 message padding services	Yes
MARS encryption/decryption, MACing and internal parameter generation services.	Yes
MD2 secure hashing services	Yes
MD5 secure hashing services	Yes
Modification detection codes based on DES	Yes
RC2 encryption/decryption, MACing and internal parameter generation services	Yes
RC4 encryption and decryption and internal parameter generation services	Yes
RC5-W32 encryption/decryption, MACing and internal parameter generation services	Yes
RC5-W64 encryption/decryption, MACing and internal parameter generation services	Yes
RC6 encryption/decryption and MACing services	Yes
Random Number Services	Yes

RSA decryption, encryption and key generation services	Yes
RSA signature and verification services	Yes
SHA-1 secure hashing services	Yes
SHA-256 secure hashing services	Yes

Table 9: Services

Self Test Service

A calling application can access the self test service at any time using the CLiC_fips140SelfTests function.

7. Cryptographically Sensitive Material

7.1. Cryptographic Keys

Key Storage
The CLiC module does not provide long-term cryptographic key storage. If an application program makes use of CLiC service to implement cryptographic key storage functionality, it is a responsibility of the application program developers to ensure FIPS140-2 compliance of key storing techniques they implement.

Key Protection
The management and allocation of memory is the responsibility of the operating system. It is assumed that a unique process space is allocated for each request, and that the operating system and the underlying central processing unit (CPU) hardware control access to that space. Each instance of the cryptographic module is self-contained within a process space. All keys are associated with the User role.
It is the responsibility of application program developers to protect keys exported from the CLiC Module.

Key Import/Export
CLiC provides applications key import and export routines such that key material can be used in conjunction with cryptographic services. It is the responsibility of the applications to ensure that these services are used in a FIPS compliant manner.

Key Generation
Key generation uses the FIPS approved RNG algorithm which is based on SHA-1. The RNG has a maximum number of internal states of 2^160, this being limited by the compression function in SHA-1. The RSA and DH key generation algorithms use the RNG engine seeded with 20 bytes of true random data. This true random generator is based on IBM patented technology where statistical analysis used to estimate the entropy of the clock jitter. The internal RNG engine is enhanced using an automatic reseeding policy that insert a true random byte every 128 bytes of output if more than 30 seconds passed since last being reseeded. Applications can additionally provide their own seeding data and also increase the automatic reseeding policy of the internal RNG engine for example to add true random data every 8th byte without time constraint.

8. Security Rules

Physical Environment

1. The host system is expected to be assembled with commercial grade components,
2. The enclosure should be opaque,
3. The enclosure should be protected by tamper-evident seals when appropriate.
4. The system bus must be secure.
5. The disk drive that CLiC module is installed on must be in a secure environment.

Operating System

6. The cryptographic module is dependant on the operating system environment being set up in accordance with FIPS 140-2 specifications. This includes that the host operating system be restricted to a single operator mode.
7. Virtual (paged) memory must be secure (local disk or a secure network).

Application Usage

8. The application shall ensure that keys are exchange in a FIPS compliant manner
9. The application shall ensure that only FIPS approved algorithms are used.
10. The Module is to be used by a single human operator at a time and may not be actively shared among operators at any period of time.
11. All keys entered into the module must be verified as being legitimate and belonging to the correct entity by software running on the same machine as the module.
12. The above rules must be upheld at all times in order to ensure continued system security and FIPS 140-2 mode compliance after initial setup of the validated configuration. If the module is removed from the above environment, it is assumed to not be operational in the validated mode until such time as it has been returned to the above environment and re-initialized by the user to the validated condition.

Single User Guidelines

The following explains how to configure a Unix system for single user. The general idea is the same across all Unix variants:

- Remove all login accounts except "root" (the superuser).
- Disable NIS and other name services for users and groups.
- Turn off all remote login, remote command execution, and file transfer daemons.

The Windows Operating Systems can be configured in single user mode by disabling all user accounts except the administrator. This can be done through the Computer Management window of the operating system. Additionally, the operating system must be configured to operate securely and to prevent remote login. This is accomplished by disabling all services (within the Administrative tools) that provide remote access (e.g. – ftp, telnet, ssh, and server) and disallowing multiple operators to log in at once.

9. Notices

AIX, BlueZ, and IBM are trademarks or registered trademarks of IBM Corporation in the United States, other countries, or both.

Pentium and X-Scale are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.