Security Policy

for

C4CS Lite and CSL software cryptographic modules

Version 1.0.3

C4CS Lite Product Version 1.1.0
CSL Product Version 1.1.0

FIPS 140-2 Non-Proprietary

May be reproduced only in its original entirety [without revision].

Copyright © 2007 – 2008 SBI Net Systems Co.,Ltd.

Revision History

Date	Revision	Author	Description
2005/03/16	0.0.0	Yuichi Hagiwara	Initial release.
2005/04/06	0.1.0	Yuichi Hagiwara	Minor update.
2005/09/01	0.2.0	Yuichi Hagiwara	Reflected Atlan Laboratories' comments. Added Mac OS 9 and X for compliance.
2006/12/22	0.3.1	Takuya Iwamoto	Merged C4CS Lite and CSL.
2007/03/09	1.0.0	Takuya Iwamoto	Updated Access Control Policy and Security Rules.
2007/09/06	1.0.1	Takayuki Uchiyama	Reflected CMVP Comments
2007/12/19	1.0.2	Takayuki Uchiyama	Reflected CMVP Comments
2008/08/08	1.0.3	Takayuki Uchiyama	Reflected Company name change

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.

Table of Contents

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.

1. Module Overview

This Security Policy is prepared as one of the requirements of FIPS 140-2 validation. However, SBI Net Systems Co.,Ltd. intends other purposes also.
It allows entities to:

- Determine if the cryptographic modules are implemented as stated in the Security Policy.
- Describe how the FIPS 140-2 requirements are actually implemented in the cryptographic module.

C4CS Lite and CSL are two separate software cryptographic modules targeted for FIPS 140-2 Security Level 1 overall. In FIPS 140-2 terms, C4CS Lite and CSL are multi-chip standalone modules and the physically contiguous cryptographic boundary is defined as the outer enclosure of a general purpose computing system. As software-only cryptographic modules, the logical boundary is defined as the module itself. (C4CSLite.dll and CSL.dll) The two modules have a single binary in dll format. All I/O is managed through the cryptographic modules' API. An external user application (software outside of the logical boundary) links to the cryptographic module at runtime. The diagram below illustrates the cryptographic boundary.

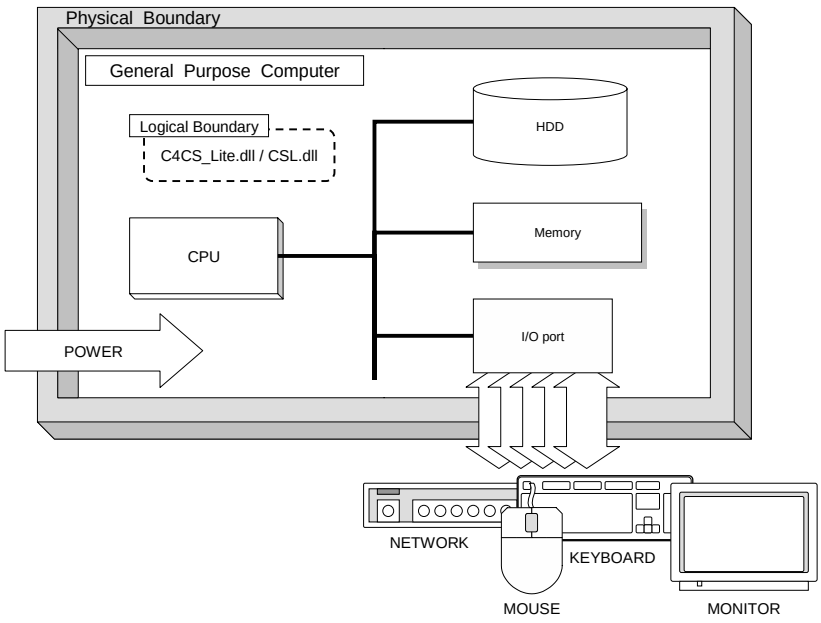

Diagram 1 - Cryptographic Boundary

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.

2. Security Level

The cryptographic modules meet the overall requirements applicable to Level 1 security of FIPS 140-2.

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	3
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.

3. Modes of Operation

Approved mode of operation

In FIPS mode, the cryptographic modules will support the following algorithms:

Table 2 - Approved Mode of Operation

AES	As defined in **FIPS PUB 197** with 128, 192, or 256 bit keys. AES will support the following modes : ECB, CBC, CTR
DRNG	As defined in **FIPS 186-2, Appendix 3.1 with Change Notice 1** for generation of all cryptographic keys and random numbers used by the user application.
HMAC	As defined in **FIPS PUB 198** for performing the power-up software integrity test, and generating MAC values. HMAC will support the following hash algorithms : SHA-1, SHA-256
RSA	RSA will support the following schemes : ■ As defined in **RSAES OAEP** / **RSAES PKCS1v1.5** for encryption/decryption. This functionality is only supported for key wrapping as a commercially available key establishment technique allowed under **FIPS 140-2 Annex D**. Encryption of bulk data is ***not*** supported. If the operator forces the module to encrypt non-key data, this Security Policy is violated. The key establishment methodology provides between 80 and 150 bits of encryption strength. ■ As defined in **RSASSA PKCS1v1.5 / RSASSA PSS** for digital signature generation/verification.
SHS	As defined in **FIPS PUB 180-2** for generating message digests with 160 or 256 bit lengths. (SHA-1, SHA-256)
SSS	**Secret Sharing Scheme** is used for split-knowledge procedures. Encryption of bulk data is ***not*** supported. If the operator forces the module to split non-key data, this Security Policy is violated. SSS will support the following schemes : **(k, n) threshold scheme, (k, L, n) threshold scheme**

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.

The C4CS Lite and CSL cryptographic modules may be configured for FIPS mode by making function calls associated with the algorithms listed above. If any of the Non-Approved algorithms are accessed, the modules will immediately switch to non-FIPS mode, and violate this Security Policy. Note that the modules will ***not*** indicate if the module is operating in a FIPS approved mode or not.

Non-Approved mode of operation

In non-FIPS mode, the cryptographic modules provide non-FIPS Approved algorithms as follows:

Table 3 - Non-Approved Mode of Operation

C4Custom	The **C4Custom** algorithm is a proprietary stream cipher of SBI Net Systems Co.,Ltd. (Contained only in C4CS Lite)
RSA	As defined in **RSAES OAEP / RSAES PKCS1v1.5** for encryption/decryption of bulk data.
SSS	**Secret Sharing Scheme** used for splitting bulk data in the following schemes : (k, n) threshold scheme, (k, L, n) threshold scheme

The modules support both FIPS approved and non-approved modes of operation.
See Section 6 for Access Control Policy.

4. Ports and Interfaces

The C4CS Lite and CSL cryptographic modules provide the following logical interfaces:

- Data input
- Data output
- Control input
- Status Output

The general purpose computing system that the cryptographic module executes on receives power from an external power supply.

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.

5. Identification and Authentication Policy

Assumption of roles

The C4CS Lite and CSL cryptographic modules support two distinct operator roles (User and Cryptographic-Officer [C.O.]). The cryptographic modules do not support operator authentication or a maintenance role. The operator assumes a given role by making function calls associated with the role.

Table 4 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	N/A	N/A
C.O.	N/A	N/A

Table 5 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
N/A	N/A

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.

6. Access Control Policy

Roles and Services

Table 6 - Services Authorized for Roles

Role	Authorized Services
User: The entity that has access to all functions supported by the cryptographic module. The operator ***implicitly*** selects this role by making function calls associated with this role.	• AES • FIPS 186-2 DRNG • HMAC • RSA encrypt/decrypt (only supported for key wrapping) • RSA signature generation/verification • Self-tests • SHS • SSS (only supported for key splitting) • Zeroization • Show Status
Cryptographic-Officer: The entity is responsible for management activities including installing the software onto the platform and configuring the OS. Authentication is not required.	• Configuration of the Operating System • Installation of the module

Services - Purposes and Uses

Table 7 - Service names, purposes, and uses

Service Name	Purpose and Use
AES	Allows Users to encrypt / decrypt various data.
FIPS 186-2 DRNG	Allows Users to generate deterministic random numbers and generate keys for AES, RSA, and HMAC.
HMAC	Allows Users to generate MAC values.
RSA encryption/decryption	Allows Users to wrap / unwrap keys.
RSA signature/verification	Allows Users to sign / verify messages.

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.

Self-tests	Allows Users to determine if the module is functioning properly. (This service is obtained only upon the re-loading of the module.)
SHS	Allows Users to generate message digests.
SSS	Allows Users to split / rebuild keys.
Zeroization	Allows Users to zeroize key data.
Show Status	Allows Users to let the module indicate its status.

Definition of Critical Security Parameters (CSPs)

The following **CSP**s are contained in the modules:

- **AES key (128, 192, 256):**
  Used for encryption and decryption of various data in ECB, CBC, and CTR modes.
- **HMAC Key (HMAC SHA-1, HMAC SHA-256):**
  Used for generating MAC values.
- **FIPS 186-2 DRNG Seed and Seed key (FDS / FDSK):**
  Used within the Approved FIPS 186-2 DRNG for generation cryptographic keys, and random numbers used within crypto processes, or by the user application.
- **RSA Private Key (decrypt) (RPKD):**
  Used to unwrap keys as a commercially available key establishment technique allowed under FIPS PUB 140-2 Annex D. This key is not supported for decryption of bulk data.
- **RSA Private Key (sign) (RPKS):**
  Used to digitally sign data passed into the module by the User.
- **SSS Split Data (SSD):**
  Key data split by using SSS.

Definition of Public Keys

The following are the public keys contained in the modules:

- **RSA Public Key (encrypt):**
  Used to wrap keys as a commercially available key establishment technique

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.

allowed under FIPS PUB 140-2 Annex D. This key is not supported for encryption of bulk data.

- **RSA Public Key (verify):**
  Used to verify digitally signed data passed into the module by the User.

Definition of CSPs Modes of Access

Table 8 defines the relationship between access to **CSP**s and the different module services. The modes of access shown in the table are defined as follows:

Generate (g) : a cryptographic key or a random number is generated using the Approved FIPS 186-2 DRNG.
Enter (e) : a cryptographic key is entered into the module.
Use (u) : a cryptographic key is used to perform cryptographic operations within its corresponding algorithm (as described in Section 3 of this document).
Output (o) : a cryptographic key is output from the module.
Zeroize (z) : a cryptographic key is destroyed.

Table 8 - CSP Access Rights within Services

Service	Cryptographic Keys and CSPs Access Operation						
	AES	**FDS**	**FDSK**	**HMAC**	**RPKD**	**RPKS**	**SSD**
AES	e, g, u						
DRNG	g, o	e, u	e, u	g, o	g, o	g, o	g, o
HMAC				e, g, u			
RSAES					e, g, u		
RSASSA						e, g, u	
Self-Tests							
SHS							
SSS							e, g, u
Zeroization	z	z	z	z	z	z	z
Show Status							

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are applicable since both the C4CS Lite and CSL software execute on general purpose Operating Systems.
The cryptographic modules were tested and validated on Windows XP Service Pack 2.

As a 32-bit DLL, the modules will have compatibility with other 32-bit Windows Operating Systems. Also, the modules will have compatibility as a shared object on Solaris, Linux, HP-UX, AIX, and Mac OS X Operating Systems, since item G.5 of Implementation Guidance will apply.

The Cryptographic-Officer must ensure that the Operating System is configured to run in a single user mode.

8. Security Rules

The C4CS Lite and CSL cryptographic modules' design corresponds to the C4CS Lite and CSL cryptographic modules' security rules. This section documents the security rules enforced by the cryptographic modules to implement the security requirements of these FIPS 140-2 Security Level 1 modules.

1. The cryptographic modules shall provide two distinct operator roles. These are the User role, and the Cryptographic-Officer role.
2. The cryptographic modules shall not perform authentication.
3. The cryptographic modules shall support RSAES for key wrapping, and not bulk data encryption.
4. The cryptographic modules shall support SSS for splitting key data and not for bulk data. Values of k, L, n should be $n \geq k > 0$ for (k, n) threshold scheme and $n \geq k > L > 0$ for (k, L, n) threshold scheme.
5. The output of plaintext cryptographic keys shall require two independent internal actions.
6. The seed and seed key shall not assume the same value.
7. The seed and seed key shall have total entropy of at least 20 bytes.

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.

8. The same RSA key pair shall not be used for both key wrapping and digital signature operations.
9. The key establishment methods must employ 80 bits of security at minimum. i.e., RSA key size shall be 1024 bits at minimum.
10. The cryptographic modules shall perform the following tests without any operator actions:
    A. Power up Self-Tests:
        (1) Software Integrity Test (HMAC-SHA-1 verification)
        (2) Cryptographic algorithm tests:
            a. AES Known Answer Test
            b. SHS Known Answer Test
            c. HMAC Known Answer Test
            d. FIPS 186-2 DRNG Known Answer Test
            e. RSAES Known Answer Test
            f. RSASSA Known Answer Test
        (3) Critical Functions Tests:
            a. SSS Critical Function Test
    B. Conditional Self-Tests:
        (1) Continuous Random Number Generator (RNG) test
            – performed on FIPS 186-2 DRNG
        (2) RSA Pair-wise consistency test
            – performed on RSAES and RSASSA key generation
11. If the operator wishes to perform the power up self-tests, he/she should re-load the module. i.e., there are no function calls that will perform power-up self-tests on demand.
12. If the modules enter an error state due to failing of self-tests, the module shall be reloaded in order to perform its service.
13. The operator shall seed the DRNG with random numbers generated with a FIPS validated cryptographic module, or with at least 80 bits of entropy.
14. Prior to each use, the internal DRNG shall be tested using the conditional test specified in FIPS 140-2 §4.9.2.
15. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
16. Status information shall not contain CSPs or sensitive data that if misused could lead

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.

to a compromise of the module.

17. The modules shall not support concurrent operators as a Security Level 1 module.
18. The modules shall be operated with an Operating System configured in Single User mode.
19. The modules shall inhibit cryptographic operations and data output while in all error states.

9. Physical Security Policy

Physical Security Mechanisms

Physical security requirements are not applicable to these software-only modules. However, when installing the modules, the Cryptographic-Officer must ensure that the computer system is stored in a secure environment. Since a software cryptographic module cannot equip physical security, the Cryptographic-Officer should stress on the physical environment of the computer system.

Operator Required Actions

There are no operator required actions, as physical security is not applicable.

Table 9 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
N/A	N/A	N/A

10. Mitigation of Other Attacks Policy

The modules have ***not*** been designed to mitigate specific attacks outside the scope of FIPS 140-2.

Table 10 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.

11. References

- National Institute of Standards and Technology, “FIPS PUB 140-2, Security Requirements for Cryptographic Modules”, May 25, 2001
- National Institute of Standards and Technology, “Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules. Draft”, March 24, 2004
- National Institute of Standards and Technology, “Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program”, September 22, 2004.
- National Institute of Standards and Technology, “FIPS PUB 197, Advanced Encryption Standard (AES)”, November 26, 2001
- National Institute of Standards and Technology, “FIPS PUB 186-2, Digital Signature Standard (DSS)”, October 5, 2001
- RSA Laboratories, “PKCS #1: RSA Encryption Standard. Version 2.1”, June 14, 2002.
- National Institute of Standards and Technology, “FIPS PUB 180-2, Secure Hash Standard (SHS)”, August 1, 2002
- National Institute of Standards and Technology, “FIPS PUB 198, Keyed-Hash Message Authentication Code (HMAC)”, March 6, 2002
- Adi Shamir, “How to share a secret”, Communications of the ACM, 612-613, 1979.
- Hirosuke Yamamoto, “Secret Sharing System Using (k, L, n) Threshold Scheme”, IEICE Trans., vol.J68-A, no.9, pp.945-952, September 1985.

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.

12. Definitions and Acronyms

Table 11 – Definitions and Acronyms

AES	Advanced Encryption Standard
C4CS Lite	C4 Certified Suite Lite (developed by SBI Net Systems Co.,Ltd.)
C4Custom	A proprietary stream cipher developed by SBI Net Systems Co.,Ltd.
CSL	Compact Secure Library (developed by SBI Net Systems Co.,Ltd.)
DRNG	Deterministic Random Number Generator
HMAC	Keyed Hash Message Authentication Code
RSA	A public key cryptosystem invented by Rivest, Shamir, and Adleman
RSAES	RSA Encryption Standard
RSASSA	RSA Secure Signature Algorithm
SHS	Secure Hash Standard – the message digest will be 160, 224, 256, 384, or 512 bits (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512).
SSS	Secret Sharing Scheme

Copyright © 2007 2008 SBI Net Systems Co.,Ltd.