Oceana Sensor Technologies
Fortress Cryptographic Library ™ V1.0
FIPS 140-2 Non-Proprietary
Security Policy
Level 1 Validation

August 22, 2005

Oceana Sensor Technologies
1632 Corporate Landing Parkway
Virginia Beach, VA 23454

Table of Contents

1 INTRODUCTION

1.1 Purpose

This is a non-proprietary FIPS 140-2 Security Policy for the Oceana Sensor Technologies (OST) Fortress Cryptographic Library™ v.1.0 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 testing 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 Standard:

- 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 Oceana Sensor Technologies please visit http://www.oceanasensor.com.

Author	**Title**
NIST	[1] FIPS PUB 140-2: Security Requirements For Cryptographic Modules, May 2001
NIST	[2] Derived Test Requirements for FIPS PUB 140-2, November 2001
NIST	[3] Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program, July 2001
OST	[4] Fortress Secure Interface™ User Guide, August 2004.
OST	[5] Fortress Secure Interface™ Installation Procedure, August 2004.
OST	[6] Fortress Secure Interface™ Functional Specification, September 2004
OST	[7] Fortress Secure Interface™ Ports and Interfaces, September 2004
OST	[8] Fortress Secure Interface™ Roles, Services and Authentication, September 2004
OST	[9] Fortress Secure Interface™ Finite State Model, September 2004
OST	[10] Fortress Secure Interface™ Physical Security, September 2004
OST	[11] Fortress Secure Interface™ Operational Environment, September 2004
OST	[12] Fortress Secure Interface™ Cryptographic Key Management, September 2004
OST	[13] Fortress Secure Interface™ Electromagnetic Interference/Electromagnetic Compatibility, September 2004
OST	[14] Fortress Secure Interface™ Self-Tests, September 2004

OST	[15] Fortress Secure Interface™ Design Assurance, September 2004
OST	[16] Fortress Secure Interface™ Mitigation of Other Attacks, September 2004
Dell	[17] Dell™ OptiPlex™ 160L Service Manual, Dell, Inc., 2003. http://support.dell.com/support/edocs/systems/op160L/en/index.htm
Dell	[18] Dell™ OptiPlex™ 160L Setup and Quick Reference Guide, Dell, Inc., 2003. http://support.dell.com/support/edocs/systems/op160L/en/index.htm
Dell	[19] Dell™ OptiPlex™ 160L User's Guide, Dell, Inc., 2003. http://support.dell.com/support/edocs/systems/op160L/en/index.htm
Microsoft	[20] Windows® 2000 Professional.

1.3 Document History

Authors	Date	Version	Comment
OST	Sept. 29, 2004	1.0	
OST	Jan. 14, 2005	2.0	
OST	Feb. 1, 2005	3.0	
OST	March 7, 2005	4.0	
OST	August 22, 2005	5.0	

2 PRODUCT INTRODUCTION

The Oceana Sensor Technologies Fortress Cryptographic Library™ (FCL) is a cryptographically secure interface to applications both internal and external to the OST product. It has many features and supports AES, Triple DES and RSA. It is entirely a software product. The cryptographic boundary includes the FCL and the host computer enclosure.

The module implements Triple DES and AES (encryption/decryption), RSA (signing/verifying), SHA-1 (Secure Hash Algorithm) and HMAC-SHA-1, 256, 384, 512 (Hashed Message Authentication Code) algorithms in the approved mode.

The product meets the overall requirements applicable to Level 1 security for FIPS 140-2 as indicated in Table 1, with Roles, Services and Authentication meeting the Level 2 requirements, and EMI/EMC and Design Assurance meeting the Level 3 requirements.

3 CRYPTOGRAPHIC MODULE SPECIFICATION

The cryptographic module is a multi-chip standalone as defined by FIPS pub 140-2. The module consists of the following generic components:

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	3
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	1
Overall Level of Certification	1

Table 1 Module Compliance Table

1. A commercially available general-purpose computing platform. A generic high-level block diagram for such a platform is provided in Figure 1.
2. A commercially available Operating System (OS) that runs on the above platform.
3. A software component, the Fortress Cryptographic Library™ (a set of dynamic link libraries) that runs on the above platform and operating system. This component is custom-designed and written by Oceana Sensor Technologies in the Java language and is identical, at the source code level, for all identified hardware platforms and operating systems. The source code is compiled into dynamic link libraries on the above OS. An application Programming Interface (API) is defined as the interface to the Fortress Cryptographic Library™. The Java runtime library used in testing is JRE 1.4.2.

The cryptographic module contains the following hardware computing platform and operating system:
1. A Dell Personal Computer system 51873-OEM-0045023-09136 with:
- An Intel Pentium 4 2.2 GHz processor
- 512 MB system RAM (DIMM)
- 2 serial ports, 1 parallel port and USB
- 40 GB hard drive
- A 3COM 3C509 Ethernet card

2. Windows 2000 service pack 4 operating system.

A detailed technical description of the Dell platform is included in the references.

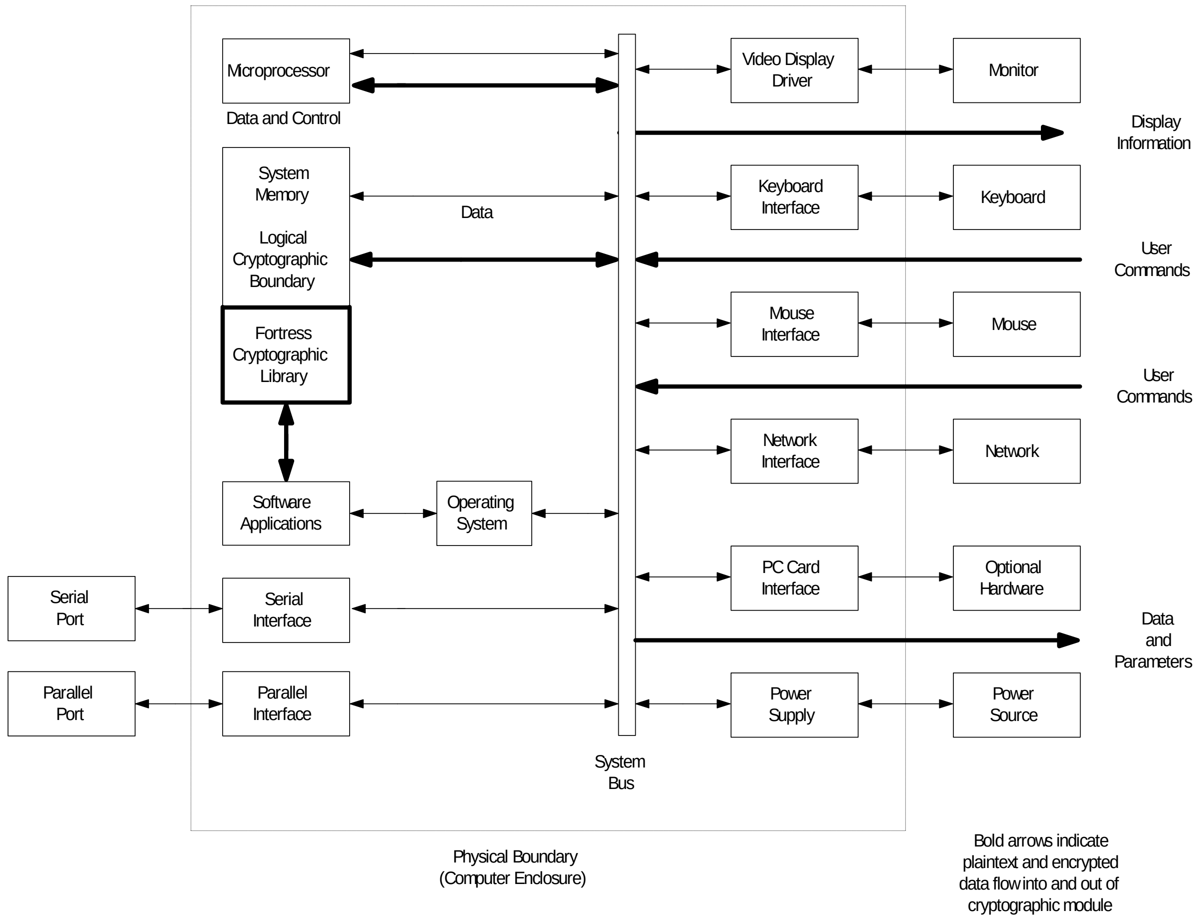

Figure 1. Cryptographic Module Diagram for Hardware

Oceana Sensor Technologies believes the implementation of its Fortress Cryptographic Library™ to be suitable for platforms from the same or other manufacturers, based on compatible processors with equivalent or greater system resources and equivalent or later operating system versions, including Windows 2000 SP4 and Windows XP.

4 CRYPTOGRAPHIC MODULE PORTS AND INTERFACES

The module is considered to be a software standalone module. The logical interface of the module is its Application Programming Interface (API). The module implements the required FIPS 140-2 interfaces as shown in Table 2.

FIPS 140-2 Interface	Module Implementation
Data Input	The module implements the Data Input Interface via the input parameters of each API function call.
Data Output	The module implements the Data Output Interface via the output parameters of each API function call.
Control Input	The module implements the Control Input Interface via the API function calls.
Status Output	The module implements the Status Output Interface via specific API function calls that return status information and the return code provided by each API function call after execution.

Table 2. Required Module Interfaces

5 ROLES AND SERVICES

A Crypto Officer and a User are implicitly assumed. The module explicitly supports a Crypto Officer and a User role. The Crypto-Officer is responsible for installing the module, since he has administrative rights in the Operating System to install software. The module does not support authentication mechanisms or a maintenance role.

The Fortress Cryptographic Library™ supports the services listed in Table 3. The table groups the authorized services by the operator roles and identifies 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.)

Approved Service	***Key, Algorithm or Operation***	***Certificate Number***	***Accessible Roles***	***Access Type***
Symmetric Encryption/Decryption	AES: 128, 192, 256 CBC, ECB	256	User/Crypto Officer	wrapped **R/E**
	Triple DES: 3-key CBC	337	User/Crypto Officer	wrapped **R/E**
Asymmetric Key Wrapping	RSA Public 1024 bits	65	User/Crypto Officer	**R/E**
	RSA Private PKCS-1 1024 bits	65	User/Crypto Officer	wrapped **R/E**
Digital Signature Generation/Verification	RSA Public PKCS-1 1024 bits	65	User/Crypto Officer	**R/E**
	RSA Private PKCS-1 1024 bits	65	User/Crypto Officer	wrapped **R/E**
Hash Generation	SHA-1, 256, 384, 512	331	User/Crypto Officer	**R/E**
MAC Generation	HMAC-SHA-1, 256, 384, 512	331	User/Crypto Officer	**R/E**
Random Number Generation	FIPS 186-2 Appendix 3.1	89	User/Crypto Officer	**R/W/E**
Module Initialization	n/a	n/a	Crypto Officer	**E**
Show Status	n/a	n/a	User/Crypto Officer	**R**
Key Agreement	Diffie-Hellman	n/a	User/Crypto Officer	**E**

Table 3. FIPS 140-2 Approved Services Authorized for Roles

6 FINITE STATE MODEL

The module has been designed to meet the requirements of the FSM. A detailed FSM and a Transition Table have been submitted as part of the validation process to the lab. The module consists of the following states: Uninitialized, Initialize, Self-Test, Error State, Idle/Operational, Crypto Officer, User and Key Management.

7 PHYSICAL SECURITY

Physical Security is Not Applicable as the module is a software cryptographic library tested to FIPS 140-2 Level 1 that runs on a general-purpose computer.

8 CRYPTOGRAPHIC KEY MANAGEMENT

Table 4 identifies the keys, key components, and CSPs utilized by the module.

Key/CSP	Description
AES Key	A symmetric key used to encrypt and decrypt data using the AES algorithm. The module supports AES key lengths of 128. 192 and 256 bits.
Triple DES Key	A symmetric key used to encrypt and decrypt data using the Triple DES algorithm. In accordance with the specification of Triple DES, all Triple DES keys are 192 bits in length.
HMAC Key	A key used to calculate a message authentication code using the HMAC algorithm. The length of the HMAC key is dependent upon the underlying hash algorithm.
Software Integrity Key	A 128-bit HMAC SHA-1 key used to calculate and verify the integrity of the module as specified in Self-Tests.
Rijndael Key	A symmetric key used to encrypt and decrypt data using the Rijndael algorithm. The module supports Rijndael key lengths of 160 and 224 bits. Rijndael is a non-approved service.
RSA Public PKCS-1 Key	A 1024-bit asymmetric key used for key wrapping and digital signature generation/verification.
RSA Private PKCS-1 Key	A 1024-bit asymmetric key used for key wrapping and digital signature generation/verification.

Table 4: Cryptographic Keys and CSPs

The module implements an RNG based on FIPS 186-2, Appendix 3.1.

8.1 Key Generation

The Fortress Cryptographic Library™ uses the FIPS 186-2 key generation method.

8.2 Key Input and Output

Secret and private keys may be electronically input or output from the module in encrypted form using FIPS approved algorithms. Key agreement is implemented with Diffie-Hellman using both public and private key lengths of 1024 bits.

8.3 Key Storage

The Fortress Cryptographic Library™ does not support key storage.

8.4 Key Destruction

All secret and private keys are zeroized with the zeroize command. All traces of the key are securely erased by writing over the key with ones and zeros.

9 EMI/EMC

The module complies with EMI/EMC requirements as specified by Title 47 of the Code of Federal Regulations, Part 15, Subpart B. The host computer is a Dell, Inc. PC, Model Number 3610KL-04W-B66, Serial Number CN-OD1534-70821-36B-20US, Rev A00.

10 SELF-TEST

The module performs the following self-tests at power on:

Cryptographic Algorithm Known Answer Tests (KATs): KATs are run at power-up for the Triple DES and AES (CBC mode) encryption/decryption, RSA digital signature signing/verifying, HMAC SHA-1, SHA-1, SHA-256, SHA-384, SHA-512, and RNG KAT to verify that the RNG works properly.

- **Software Integrity Tests:** The module checks the integrity of its various components using HMAC-SHA-1.

The module performs the following conditional self-tests:

Pair-wise Consistency Test: Pair-wise consistency tests are run on demand when the module generates key pairs. The module performs an encrypt operation with the private key and verifies it with the public key. The algorithm employed is RSA.

The module implements a continuous RNG test, as specified in FIPS 140-2 for the implemented RNG.

Table 5 describes the self-tests implemented by the module.

When an operator attempts to load the module into general purpose computer memory, the power-up self-tests are executed. During execution of the power-on self-tests, all data input/output is inhibited. The power-up self-tests comprise all the tests identified in Table 5. The Software Integrity Test is the first self-test executed; and if it fails, then the attempt to load the module fails. If a cryptographic algorithm known answer test fails, the module will enter an error state and data input/output is inhibited. The module will not transition to an operational state until all self-tests pass. The indication of test failure or success is a boolean API return signal: "true" for success and "false" for failure.

The operator may invoke the power-up self-tests by unloading and reloading the module into the computer memory. Clearing an error also is done by unloading and reloading the module from memory or, failing that, reinstalling the module by the Crypto-Officer.

The operator also may invoke all of the power-up self-tests, except the Software Integrity Test, by accessing the **Perform Self-Tests** service.

Test	Description
Software Integrity Test	The Software Integrity Test verifies the integrity of the module software using HMAC SHA-1.
Triple DES Known Answer Test	The Triple DES KAT verifies that the Triple DES encryption and decryption functions are operating correctly.
AES Known Answer Test	The AES KAT verifies that the AES encryption and decryption functions are operating correctly.
SHA-1 Known Answer Test	The SHA-1 KAT verifies that the SHA-1 hashing function is operating correctly.
HMAC Known Answer Test	The HMAC KAT verifies that the HMAC function is operating correctly.
RNG Known Answer Test	The RNG KAT verifies that the RNG is operating correctly
RSA Known Answer Test	The RSA KAT verifies that the RSA key algorithm is operating correctly

Table 5. Module Self-Tests

11 DESIGN ASSURANCE

The module satisfies the design assurance requirement as described in the standards by adopting the following methodologies.

Procedures for Secure Installation, Generation and Start-Up

All the files used by the Fortress Cryptographic Library™ (FCL) system will be installed on a local drive of a machine where the cryptographic module is intended to run. Those files shall include required Java class archive files, system property files, system resource files, system configuration files, system database files, system data files, and system script files. The folders containing those files must be protected either by using an encrypted folder (MS 2K environment), or by changing the access permission setting (Unix environment). Only authorized personnel shall have the access to those folders.

The FCL system provides a set of scripts to allow system users to start cryptographic modules. Only authorized personnel shall have permission to run those scripts.

Procedures for Maintaining Security

All the system source code, system property files, system configuration files, and system script files are maintained with a version control system (CVS in our case). Any new version of a cryptographic module to be distributed and delivered to an operator shall be tagged with the proper version number in the version control system. Change history file also shall be updated to reflect the change in the newly released version of the code.

Specification of the Source Code

The naming of the classes and methods, together with the comments in the code clearly depict the correspondence of the components to the design of the module.

The FCL system has a Functional Specification that defines the correspondence of its components to the design of the module. The FCL is designed in the Java Programming language.

Functional Specification

This specification is listed in the references. It is the Fortress Secure Interface™ Functional Specification.

Initialization and Start-Up

The Fortress Cryptographic Library™ module is initialized and started in accordance with the User Guide, as listed in the references.

User Behavior

The same user can't start two sessions on the system at the same time. This may cause the shortage of some critical resources, and also may lead to some security problems, such as unattended computer screens and potential public access to data. Keys and CSPs are not allowed to be output in clear text.

12 APPROVED MODE OF OPERATION

To operate the module in approved mode the Crypto Officer has to configure the module in the following manner.

1. Keys must be encrypted when input or output from the Fortress Cryptographic Library™.
2. The module must use approved cryptographic algorithms.
3. The operating system should be configured to operate in Single-User Mode.

13 USER RESPONSIBILITIES

Some user responsibilities are the following.

1. Never leave the cryptographic module unattended while it is running.

2. The same user should start only one session on the module at a time. The system limits the ability of a user to have no more than one session running at the same time.