OpenSSL NPX Cryptographic Module FIPS 140-2 Non-Proprietary Security Policy

Adara Networks, Inc.

Document Name: OpenSSL NPX Cryptographic Module FIPS 140-2 Non-Proprietary Security Policy

Document Version: Ver1.0r4

Revision Date: December 6, 2010

CHANGE RECORD

Revision	*Date*	*Author*	*Description of Change*
Ver1.0r0	03/15/2010	Anthony Tso	Initial Draft.
Ver1.0r2	03/15/2010	Anthony Tso	Diagrams and Modification to Text.
Ver1.0r3	03/16/2010	Anthony Tso	Modifications.
Ver1.0r3	6/15/2010	Anthony Tso	Additional Modifications.
Ver1.0r4	12/06/2010	Anthony Tso	Modifications to Section 1.2 and Section 6.

Contents

Tables

Figures

1 Module Introduction

1.1 Overview

This document is the FIPS 140-2 security policy for the OpenSSL NPX Cryptographic Module to meet overall FIPS 140-2 level 1 requirements. This Security Policy details the secure operation of the OpenSSL FIPS Object as required in Federal Information Processing Standards Publication 140-2 (FIPS 140-2) as published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce.

1.2 Module Specification

The cryptographic module, Adara Networks OpenSSL NPX Cryptographic Module (SW Version 1.0) is a software library providing FIPS Approved cryptographic algorithms. This module provides an application program interface (API) for use by other processes that require cryptographic functionality.

For FIPS 140-2 purposes, the cryptographic module is classified as a multi-chip standalone module. The physical cryptographic boundary of the module is the enclosure of the system on which it is executing. The physical cryptographic boundary contains the general purpose computer (GPC) hardware of the system executing the application. This system hardware includes the central processing unit(s), cache and main memory (RAM), system bus, and peripherals including disk drives and other permanent mass storage devices, network interface cards, keyboard and console and any terminal devices.

The logical cryptographic boundary is defined by the object module. The logical cryptographic module is the specific compiled and tested discrete contiguous block of object code containing the machine instructions and data generated from the OpenSSL FIPS source, as used by the calling application.

The cryptographic module was tested on the following platform:

- HP Proliant DL360 G5 platform with an Intel Xeon processor with a FreeBSD 8.0 (x86-64 release p2) system

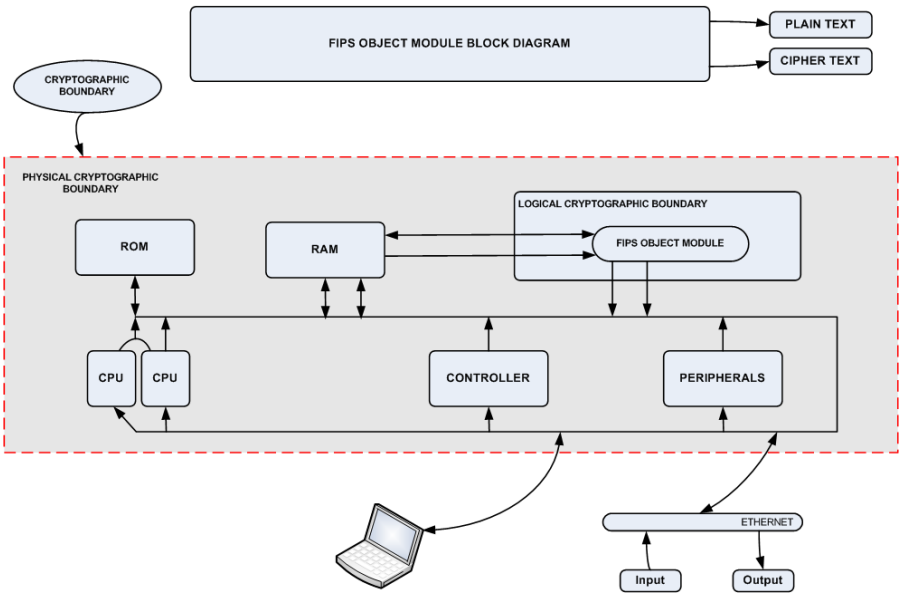

Figure 1 – Logical Diagram

2 Security Level

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

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

Table 1 – Module Security Level Specification

3 Modes of Operation

3.1 FIPS Approved Mode of Operation

The Cryptographic module operates in the FIPS 140- 2 Approved mode of operation when all Security Policy requirements have been met and the module's Approved mode of operation has been initialized.

A single initialization call is required to initialize the module for operation in the FIPS 140-2 Approved mode. When the module is in FIPS Approved mode of operation all security functions and cryptographic algorithms are performed in the Approved mode.

The module is not in "FIPS mode" until the Approved mode of operation is initialized.

3.2 Approved and Allowed Algorithms

The cryptographic module supports the following Approved and allowed algorithms in the Approved mode of Operation

APPROVED ALGORITHMS				
Algorithm Type	**Algorithm**	**Standard**	**FIPS Validation Certificate Number**	**Utilization**
Asymmetric	RSA1024, 1536, 2048, 3072 and 4096	ALG [ANSIX9.31]; SIG (gen); SIG (ver); ALG [RSASSA-PKCS1_V1_5]; SIG (gen); SIG (ver); ALG [RSASSA-PSS]; SIG (gen); SIG (ver);	667	Sign and Verify Operations with private and public keys
	DSA 1024	FIPS 186-2	447	
Symmetric	Triple-DES – CBC, CFB8, CFB64, ECB, OFB Modes – 128 and 192 bit keys	FIPS 46-3	942	Encrypt / Decrypt Operations with symmetric encryption keys
	AES – CBC, CFB8, CFB128, ECB, OFB each with 128, 192 or 256 bit keys	FIPS 197	1367	

APPROVED ALGORITHMS				
Algorithm Type	**Algorithm**	**Standard**	**FIPS Validation Certificate Number**	**Utilization**
HMAC	HMAC–SHA-1 HMAC–SHA-224 HMAC–SHA-256 HMAC–SHA-384 HMAC–SHA-512	FIPS 198	801	Module Integrity Code Integrity Message Integrity with symmetric authentication HMAC keys
Hashing	SHA–1 SHA–224 SHA–256 SHA–384 SHA–512	FIPS 180-2	1248	Hashing
RNG	ANSI X9.31	ANSI X9.31	753	Random Number Generation with RNG Seed

Table 2 – Supported FIPS Approved Algorithms

3.3 Allowed Non-Approved Algorithms

The cryptographic module supports the following non-Approved algorithms in the Approved mode of operation as allowed.

ALLOWED ALGORITHMS		
Algorithm Type	**Algorithm**	**Utilization**
Key Agreement	DH primitives	Key establishment methodology provides between 80 and 219 bits of encryption strength
Asymmetric	RSA	Key establishment methodology provides between 80 and 256 bits of encryption strength

Table 3 – Allowed Algorithms

4 Ports and Interfaces

The module provides a logical interface via an Application Programming Interface (API). This logical interface exposes services that applications may utilize directly or extend to add support for new data sources or protocols. The API provides functions that may be called by the referencing application.

The logical interface provided by the module is mapped to each of the FIPS 140-2 logical interfaces, as follows:

- **Data Input** – input parameters to all functions that accept input from the Cryptographic Administrator or User entities;
- **Data Output** – Data output parameters from all functions that return data as arguments or return values to Cryptographic Administrator or User entities;
- **Control Input** – All API function input into the module by the Cryptographic Administrator and User entities;
- **Status Output** – Information returned via exception (return/exit codes) to Cryptographic Administrator or User entities.

4.1 Ports and Interfaces – Correlation

The physical ports of the module are the same as the computer system on which it is executing. The logical interface is a C language application program interface (API).

PORTS & INTERFACES		
FIPS Interface	**Physical Port**	**Module Interface**
Data Input	Ethernet Port	API input parameters
Data Output	Ethernet Ports	API output parameters
Control Input	Keyboard, Serial Port, Ethernet Port	API function calls
Status Output	Keyboard, Serial Port, Ethernet Port	API Return Codes
Power Input	Power Connector	N/A

Table 4– Ports & Interfaces – Correlation

5 Identification and Authentication Policy

5.1 Assumption of Roles

The User and Cryptographic Administrator (FIPS Crypto-Officer) roles are implicitly assumed by any entity that can access services implemented in the module. In addition the Cryptographic Administrator role can install and initialize the module.

5.2 Authenticated Services

All services may be performed in both User and Cryptographic Administrator roles.

AUTHENTICATED SERVICES				
Roles	**Services**	**Critical Security Parameters**	**Algorithm**	**Access**
User, Cryptographic Administrator	Symmetric Encryption / Decryption	Symmetric Key	AES	Read Write Execute
			3DES (2 Key)	
			3DES (3 Key)	
User, Cryptographic Administrator	Digital Signature	Asymmetric Private Key	RSA	Read Write Execute
			DSA	
User, Cryptographic Administrator	Message Digest	None	SHA–1 SHA–224 SHA-256 SHA-384 SHA-512	Read Write Execute
		HMAC Key	HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	
User, Cryptographic Administrator	Random Number Generation	RNG Seed Material	ANSI X9.31 RNG	Read Write Execute
User, Cryptographic Administrator	Show Status	None	N/A	N/A
User, Cryptographic Administrator	Module Initialization	None	N/A	N/A
User, Cryptographic Administrator	Self-Test (Includes integrity, Known answer and pair-wise consistency)	None	N/A	N/A
User, Cryptographic Administrator	Key Establishment	Asymmetric Private Key	RSA	Read Write Execute
			DH	

Table 5- Authenticated Services

The following Public Keys are available in the module:

1. RSA Verifying Public Key (used to verify digitally signed data)
2. RSA Wrapping Key (used to perform RSA key transport of keys)

6 Operational Environment

The OpenSSL NPX Cryptographic Module v1.0 is a compiled module available for use on a wide variety of computer hardware and operating system platforms. Applications referencing the cryptographic module run as processes under the control of the host GPC and operating system.

The OpenSSL NPX Cryptographic Module was built and tested on specific hardware and software environments. The cryptographic module was tested on the following platform:

1) HP Proliant DL360 G5 platform with an Intel Xeon processor with a FreeBSD 8.0 (x86-64 release p2) system

7 Secure Operation

7.1 Security rules

1) The integrity of the logical module boundary shall be verified at runtime using a HMAC-SHA-1 hash.
2) The module shall be initialized into the FIPS 140-2 Approved mode of operation using the initialization service. The logical module shall not perform non-Approved algorithms or security functions in the Approved mode of operation.
3) The module shall not make network or inter-process connections and create files. The FIPS Object Module functions completely within the process space of the process which loads it. It does not communicate with any processes other than the one that loads it, and satisfies the FIPS 140-2 requirement for a single user mode of operation.
4) The writable memory areas of the module (data and stack segments) shall only be accessible by a single application so that the module is in "single user" mode, i.e. only the one application has access to that instance of the module.
5) The referencing application accessing the module shall run in a separate virtual address space with a separate copy of the executable code. The unauthorized reading, writing, or modification of the address space of the module is prohibited.
6) All host system components may contain sensitive cryptographic data (main memory, system bus, disk storage). The calling process or operator shall be responsible for the protection and zeroization of plaintext critical security parameters.
7) Secret or private keys that are input to or output from the physical boundary must be input or output in encrypted form using a FIPS Approved algorithm. Note: Keys established between an application and the logical cryptographic modules are considered plaintext.

8) For the generation of cryptographic key components, the operator shall ensure that the seeding material provides sufficient entropy. The entropy should be greater than the strength requirement for the key being generated. This can be done by seeding the Approved random number generator with at least 128 bits of entropy.

7.2 Critical Security Parameters

A Critical Security Parameter (CSP) is information, such as passwords, symmetric keys, asymmetric private keys, etc., that must be protected from unauthorized access. Since the module is accessed via an API from a referencing application, the module does not manage CSPs. For most applications CSPs will be found in multiple locations external to the logical cryptographic boundary of the module, such as in application buffers, primary (RAM) memory, secondary disk storage, CPU registers, and on the system bus. The operator should ensure the protection of these parameters.

7.3 Self-Tests

The module performs a number of power-up and conditional self-tests to ensure proper operation of the module.

The failure of any power-up self-test or continuous test causes the module to enter the Self-Test Failure state, and all cryptographic operations are disabled until the module is reinitialized with a successful initialization service request.

Power-up tests include cryptographic algorithm test and integrity tests. The power-up self-tests for the following algorithms:

POWER-UP SELF-TEST	
Algorithm	**Power-Up Self test**
AES	Encryption and Decryption KAT
Triple-DES	Encryption and Decryption KAT
DSA	Pairwise Consistency tests
RSA	Sign and Verify KAT
HMAC and SHAs	HMAC-SHA-1 KAT HMAC-SHA-224 KAT HMAC-SHA-256 KAT HMAC-SHA-384 KAT HMAC-SHA-512 KAT
RNG	Random Number Generation KAT

Table 6 – Power-Up Self-Test

In addition to the power-up tests, the module performs several conditional tests including pair-wise consistency tests on newly generated public and private key pairs.

Conditional tests are performed automatically as necessary and cannot be turned off.

CONDITIONAL TESTS	
Algorithm	**Conditional Test**
DSA	Pairwise Consistency test
RSA	Pairwise Consistency test.
RNG	Continuous RNG test

Table 7 – Conditional Tests

7.4 Critical Function Tests

The module does not implement any critical function tests.

8 Physical Security

The module does not claim to enforce any physical security as it is implemented entirely in software.

9 Mitigation of Other Attacks

The module does not mitigate against any specific attacks outside the scope of FIPS 140-2.