Odyssey Security Component
Kernel Mode Security Policy

Software Version 2.50
Document Version 1.8

Juniper Networks, Inc.

March 14, 2014

TABLE OF CONTENTS

1. Module Overview

The Odyssey Security Component Kernel Mode (OSCKM) (SW Version 2.50), is a software module that implements a set of cryptographic algorithms for use by a software application. This Security Policy document details the OSCKM Version 2.50.

The Odyssey Security Component Kernel Mode comprises a kernel level module, odFIPS2.sys. The module has a multi-chip standalone embodiment as defined by FIPS 140-2.

The cryptographic module runs, and was operational tested on the following operating systems:

- Windows 7 Enterprise Edition 64-bit

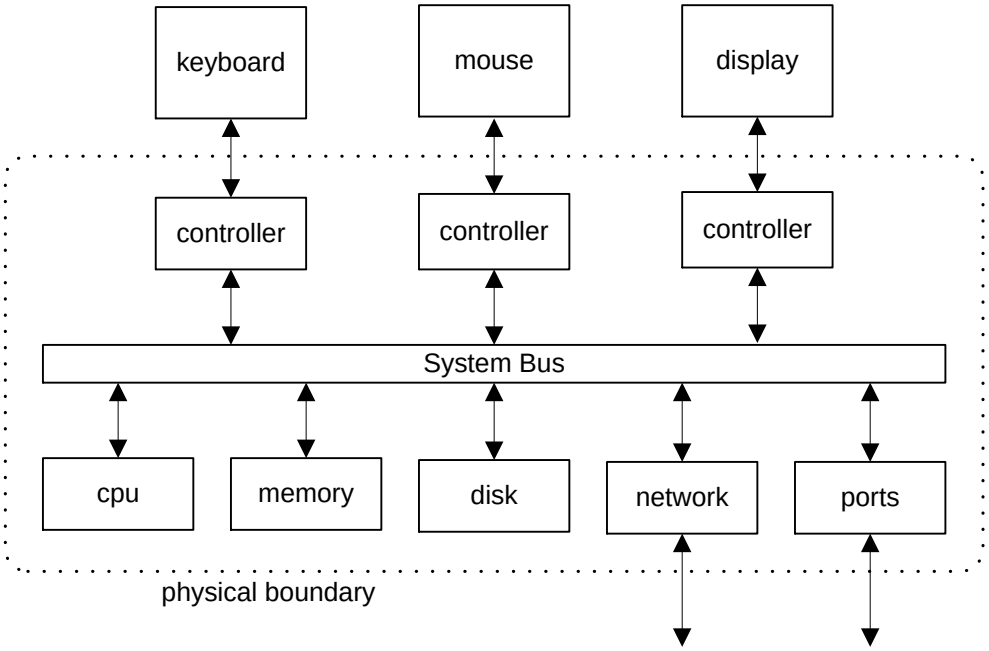

Figure 1: Hardware Diagram Showing PC Containing Cryptographic Module

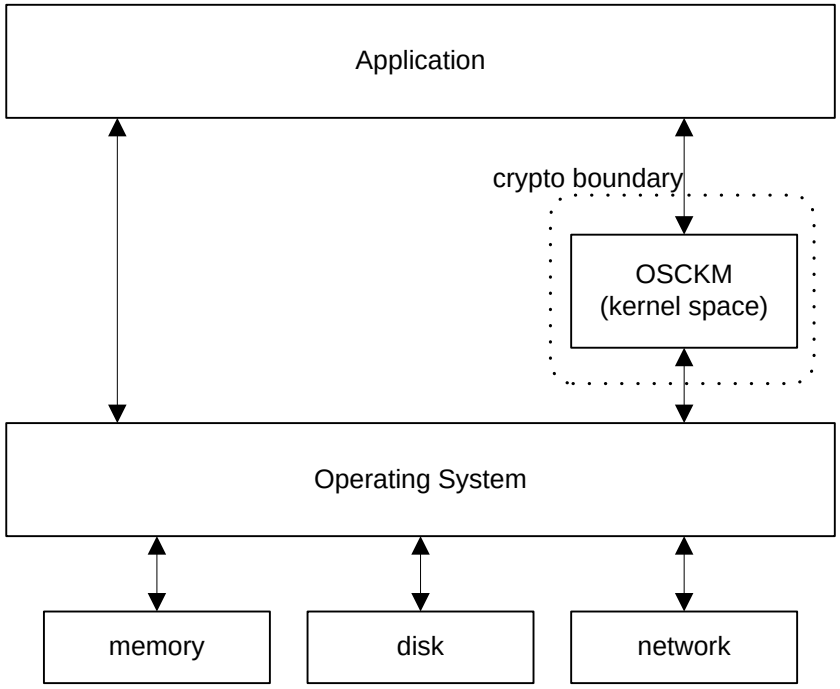

Figure 2: Software Diagram Showing Cryptographic Boundaries

2. Security Level

The OSCKM meets 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	1
Self-Tests	1
Design Assurance	2
Mitigation of Other Attacks	N/A

The FIPS modules are code signed and the HMAC SHA-512 hash values for these modules are compared at the load time to do the software integrity checks.

3. Modes of Operation

Approved mode of operation

In FIPS mode, the OSCKM supports the following FIPS Approved algorithms[1]:

- AES 128, 192, 256 – ECB, CBC, and Counter modes (See certificate #*1990*)
- AES-CCM – Key sizes 128, 192, and 256 (See certificate #*1990*)
- Triple-DES – TECB and TCBC modes (See certificate #*1291*)
- SHA -1, 224, 256, 384, 512 (See certificate #*1745*)
- HMAC-SHA-1, 224, 256, 384, 512 (See certificate #*1203*)
- DSA Verify (See certificate #*636*)
- RSA Verify (See certificate #*1032*)
- FIPS 186-2 RNG (See certificate #*1045*)

Once loaded into memory and executed, the module is running in FIPS mode. An operator of the module can verify that the module is running in the FIPS Approved mode of operation by first executing the "EnableFIPSModule" command, followed by the "Get State service, which shall return the following: OD_FIPS_STATE_ENABLED.

The cryptographic module provides the following allowed cryptographic key-wrapping algorithms:

- RSA Encrypt/Decrypt (for Key Transport only) (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength; non-compliant less than 112-bits of encryption strength)
- AES Key Wrap (AES Cert. #1990, key wrapping; key establishment methodology provides between 128 and 256 bits of encryption strength)

The following non-Approved algorithms are also available in the Approved mode of operation:

- RSA Encrypt/Decrypt (for bulk data) - No security is claimed for data that has been encrypted using this algorithm.
- Diffie Hellman (primitives only) non-approved, allowed in FIPS mode.

The following non-Approved algorithms shall not be used by the module. The module is not considered to be in a FIPS approved mode if the algorithms are used.

[1] The user of the module should review the Algorithm Transition Tables, available at the CMVP website and SP 800-131A (http://csrc.nist.gov/groups/STM/cmvp/) to determine the current status of algorithms and key lengths used in the module.

- DSA Sign, Key Gen, and PQG Gen
- RSA Sign
- RSA Encrypt/Decrypt (for Key Transport only) (key wrapping; key establishment methodology 80 bits of encryption strength)

4. Ports and Interfaces

All FIPS ports and interfaces are defined as the API of the cryptographic module. The API contains all data input, data output, control input, and status output interfaces to and from the module.

5. Identification and Authentication Policy

Assumption of roles

The OSCKM cryptographic module shall support two distinct roles, User and Cryptographic Officer. The system administrator implicitly assumes the Crypto Officer role, and is responsible for installing the module.

Table 2 - Roles and Required Identification and Authentication

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

6. Access Control Policy

Roles and Services

Table 3 lists each role and the services authorized for each role.

Table 3 – Services Authorized for Roles

Role	Authorized Services
User and Cryptographic Officer:	• AES Encrypt/Decrypt • Triple-DES Encrypt/Decrypt • RSA Verify • DSA Verify • Generate RNG • AES CCM • HMAC-SHA-1, 224, 256, 384, and 512 • RSA Encrypt/Decrypt (for key transport only), (key wrapping; key establishment methodology using 112 *or* 128 bits of encryption strength) - Note: This service is also used for encrypting/decrypting bulk data. However, no security is claimed for data that has been protected by RSA. • AES Key Wrap • Generate Prime Number – Generates a prime number using the FIPS 186-2 RNG • Modular Exponentiation • EnableFIPSModule – Puts the module in a FIPS Approved mode of operation • DisableFIPSModule – Disables the module, and allows only the 'EnableFIPSModule' and 'Run Self-tests' API commands to be called • GetState – Returns the current state of the cryptographic module • GetError – Returns a specific error code when the module is in an error state • Run Self-tests – This service executes the suite of self-tests required by FIPS 140-2 by calling the odFIPS_RunSelfTestsAsynch API command. • Context Termination –Zeroize CSPs/keys

Services disallowed in FIPS mode

The following services contain algorithms or keys sizes that are part of the SP800-131A transition and shall not be used in the module. If the algorithms are used the module is no longer in a FIPS Approved mode.

- RSA Sign
- DSA Sign
- DSA Key Generation
- RSA Encrypt/Decrypt (for key transport only), (key wrapping; key establishment methodology using 80 bits of encryption strength)

Definition of Critical Security Parameters (CSPs)

The Critical Security Parameters (CSPs) defined for the OSCKM consist of cryptographic keys and random numbers used as seeding material. The module does not persistently store CSPs within the logical boundary.

The following CSPs are supported by the module:

- AES Keys: 128, 192 and 256 bit keys used to AES encrypt/decrypt data.
- Triple-DES Keys: 3 separate 56 bit DES keys used to Triple-DES encrypt/decrypt data.
- AES CCM Key: 128, 192, or 256 bit AES Key used for AES CCM operations.
- HMAC Keys: For use during HMAC operations.
- AES Key Wrap Key: 128 bit AES key for use in AES key wrapping operations.
- FIPS 186-2 PRNG Seed and Seed Key: Used for the generation of CSPs and Keys.
- DH Primitives: Used for the generation of keys.

Definition of Public Keys:

The following are the public keys contained in the module:

- RSA Verifying Public Key: This is the public part of the cryptographic module's RSA Public/Private key pair used to verify RSA signatures.
- DSA Public Key: This is the public part of the cryptographic module's DSA Public/Private key pair used to verify DSA signatures.
- RSA Wrapping Key: Used to perform RSA key transport of keys.

Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Read
- Write
- Execute
- Zeroize

Each service's API indicates the type of access to CSPs defined by that API. When a CSP is used by the API call to perform particular services, read and execute access is indicated. When a CSP is generated, modified or deleted by the API call, write access is indicated.

Table 4 – Services and CSPs

Approved Services	**CSPs**	**Authorized Roles**	**Type of Access**
Symmetric Encryption/Decryption Services			
AES Encrypt/Decrypt	AES Key	User/CO	read, execute
Triple-DES Encrypt/Decrypt	Triple-DES Key	User/CO	read, execute
Asymmetric Encryption/Decryption for Key Wrapping Services			
RSA Encrypt	RSA Wrapping Public Key	User/CO	read, execute
RSA Decrypt	RSA Private Key	User/CO	read, execute
Message Authentication Service			
AES-CCM	AES-CCM Key	User/CO	read, execute
HMAC-SHA-1, 224, 256, 384, 512	HMAC Key	User/CO	read, execute
Digital Signature Verification Services			
RSA Verify	RSA Verifying Public Key	User/CO	read, execute
DSA Verify	DSA Public Key	User/CO	read, execute
Symmetric Key Wrapping			
AES Key Wrap	AES Key Wrap Key	User/CO	read, execute
Symmetric Key Generation Service			
Generate RNG	FIPS 186-2 PRNG Seed and Seed Key	User/CO	read, execute

Approved Services	CSPs	Authorized Roles	Type of Access
Other Services			
Generate Prime Number	FIPS 186-2 PRNG Seed and Seed Key	User/CO	read, execute
Modular Exponentiation	N/A	User/CO	N/A
EnableFIPSModule	N/A	User/CO	N/A
DisableFIPSModule	N/A	User/CO	N/A
Run Self-Tests	N/A	User/CO	N/A
GetState	N/A	User/CO	N/A
GetError	N/A	User/CO	N/A
Context Termination	All	User/CO	Zeroize

7. Cryptographic Key Management

Key generation

Key generation shall not be performed in the FIPS mode. The cryptographic module contains generation of DSA public and private keys, using the Approved FIPS 186-2 deterministic random number generator but the DSA algorithm used for the key generation is part of the SP800-131A transitioning of algorithms and key lengths and shall not be used in the FIPS approved mode.

Key Storage

The module does not persistently store keys. Key material is provided for use through a defined API, stored in RAM, and then destroyed once processing is terminated. If the operator wishes to store keys they are responsible for doing so outside of the cryptographic module's logical boundary.

Zeroization

All key data exists in data structures allocated within memory provided by the caller or data structures allocated within the cryptographic module, and can only be returned to an authorized user using the defined API. Context data which may contain sensitive data/CSPs/keys are automatically zeroized using the service termination API. It is the responsibility of consuming applications to manage zeroization of their own sensitive data because it is outside the logical boundary of the cryptographic module.

8. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are applicable because the module operates in a modifiable operational environment. The software module was operational tested on the following platform:

- Dell Optiplex 755, Intel Core 2 Duo E8400 @ 3.00 GHz processor, 2GB RAM with Windows 7 Enterprise SP1 64-bit operating system.

9. Security Rules

The OSCKM cryptographic module's design corresponds to the module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The cryptographic module shall provide two distinct roles. These are the User role, and the Cryptographic Officer role.
2. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

   Cryptographic algorithm tests:

   - AES Encrypt/Decrypt KAT
   - AES CCM Encrypt/Decrypt KAT
   - Triple-DES Encrypt/Decrypt KAT
   - RSA Sign/Verify KAT
   - RSA Encrypt/Decrypt KAT (for key transport only)
   - DSA Sign/Verify KAT
   - HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 KATs
   - SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 KATs
   - FIPS 186-2 DRNG KAT

   Software Integrity Test (HMAC SHA-512)

   B. Conditional Self-Tests:

   - Continuous Random Number Generator (RNG) test – performed on DRNG
   - DSA pairwise consistency test

3. To instantiate the module, the *odFIPS_enableFIPSModule* is called which will initiate the power-on self-tests. Upon successful instantiation, the caller is provided context data through which all other services of the module can be accessed. There is no way to bypass the requirement to call *odFIPS_EnableFIPSModule*. Subsequently, the user may optionally call *odFIPS_RunSelfTestAsynch* to re-run the power-on self-tests at any time.
4. Prior to each use, the internal RNG shall be tested using the conditional test specified in FIPS 140-2 §4.9.2.
5. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.

6. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. The module does not support concurrent operators.
8. In case of power-up or conditional test failure, the operator (calling application) is notified by receiving a return value of *OD_FIPS_ERROR_NOT_OPERATIONAL* and the module is not operational.

10. Physical Security

The FIPS 140-2 Area 5 Physical Security requirements are not applicable because the device is a software-only module.

11. Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks outside the scope of FIPS 140-2 requirements.

12. Crypto Officer Guidance

The crypto-officer is responsible for the installation of an application and using the module on an operational environment on which the module has been validated. The module is a binary module linked to an application.

The module should be installed on a Windows 7 Enterprise edition SP1 64 bit OS and that the crypto-officer should set the operating system to single user mode by performing the following functions:

- disable remote desktop,
- disable server service,
- disable fast user switching, and
- disable any other application that allows remote control of the computer.

13. User Guidance

The user is the application process that performs the function calls to the module's API's. There are no special set-up or operation instructions. The module does not input or output keys or other CSPs from the GPC and does not store keys or other CSPs inside the logical boundary of the module. It is the user's (application's) responsibility to provide secure storage of any keys or other CSPs inside the GPC and to ensure that any keys transmitted outside the boundary of the GPC are transmitted in a secure manner.

14. Design Assurance

The vendor uses Perforce for configuration management. The Source code and module documents are managed in Perforce. The user manual for Perforce states "Every time anyone edits a file and uploads it to Commons, Commons saves it as a new version, while keeping all previous versions so that you know who did what and when."

The module is only used in Juniper products and is maintained by Juniper. It is not distributed outside of Juniper. The module is only used in Juniper products. The module is binary object linked library module and the code has a computed HMAC SHA-512 embedded in the code for the security of the module and is used in the software integrity test. Any changes to the code or HMAC SHA-512 will cause the software integrity test to fail.

15. Definitions and Acronyms

AES	Advanced Encryption Standard
API	Application Program Interface
CO	Cryptographic Officer
CSP	Critical Security Parameter
DLL	Dynamic Link Library
DRNG	Deterministic Random Number Generator
DSA	Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
HMAC	Keyed-Hash Message Authentication Code
OSCKM	Odyssey Security Component Kernel Mode
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman Algorithm
SHA	Secure Hash Algorithm