Oracle Solaris Userland Cryptographic Framework

Software Version 1.0 and 1.1

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation
Version 1.3

2014-01-08

Table of Contents

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Oracle Solaris Userland Cryptographic Framework 1.0 and 1.1 from Oracle Corporation (Oracle). This Security Policy describes how the Solaris Userland Cryptographic Framework 1.0 and 1.1 meets the security requirements of FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. FIPS 140-2 details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/cryptval/.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Oracle Corporation website (http://www.oracle.com) contains information on the full line of products from Oracle.

- The CMVP website (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Oracle Corporation and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Oracle Corporation.

ORACLE SOLARIS USERLAND CRYPTOGRAPHIC FRAMEWORK 1.0 AND 1.1

Overview

The Oracle Solaris 11 and 11.1 SRU5.5 operating system (OS) is a highly configurable UNIX-based operating system that is optimized to quickly and securely deploy services in traditional enterprise data centers, large scale cloud environments and small personal desktop use. Oracle preserves the long-standing guarantee of binary compatibility – applications that run on previous Oracle Solaris releases can still run unchanged on Oracle Solaris 11 within the same processor architecture: x86 or SPARC[1].

The Oracle Solaris 11 and 11.1 SRU5.5 OS can be installed on either x86 or SPARC hardware architectures or run in a virtualized environment. The operating system allows one or more processors and multiple hardware peripheral and storage devices to be accessed by multiple users in order to meet user requirements.

Oracle Solaris 11 and 11.1 SRU5.5 provides a suite of technologies and applications that create an operating system with optimal performance. Oracle Solaris 11 and 11.1 SRU5.5 includes key technologies such as zones, ZFS file system, Image Packaging System (IPS), multiple boot environments, trusted extensions, and cryptographic framework.

The Oracle Solaris 11 and 11.1 SRU5.5 OS utilizes two cryptographic modules; one in the Userland space and the second in the Kernel space. The OS uses the Oracle Solaris Userland Cryptographic Framework module for cryptographic functionality for any applications running in user space. The Oracle Solaris Userland Cryptographic Framework exposes PKCS#11[2] API[3]s, uCrypto APIs, and libmd public interfaces to provide cryptography to any application designed to utilize it.

The Oracle Solaris 11 and 11.1 SRU5.5 OS also utilizes the Oracle Solaris Kernel Cryptographic Framework module to provide cryptographic functionality for any kernel-level processes that require it, via its Oracle-proprietary APIs.

This document will focus solely on the Oracle Solaris Userland Cryptographic Framework. The Oracle Solaris Kernel Cryptographic Framework is discussed in another FIPS 140-2 Non-proprietary Security Policy.

The module meets overall level 1 requirements for FIPS 140-2, and Table 1 describes the level achieved by the module in each of the eleven sections of FIPS 140-2 requirements.

[1] SPARC – Scalable Processor Architecture
[2] PKCS – Public Key Cryptography Standards
[3] API – Application Programming Interface

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

Table 1 – Security Level per FIPS 140-2 Section

Module Specification

The Oracle Solaris Userland Cryptographic Framework is a software module with a multi-chip standalone embodiment. The overall security level of the module is level 1. The following sections will define the physical and logical boundaries of the module.

The cryptographic module is a group of libraries that, collectively, are known as the Oracle Solaris Userland Cryptographic Framework. The module provides cryptographic functionality for any application that calls into it. The module provides encryption, decryption, hashing, signature generation and verification, certificate generation and verification, and message authentication functions. The module can leverage the AES-NI[4] instruction set, when operating on an Intel Xeon processor. Figure 1, below, is the logical block diagram for the module. It highlights the libraries that make up the module in orange, while illustrating the module boundary.

[4] AES-NI – Advanced Encryption Standard – New Insructions

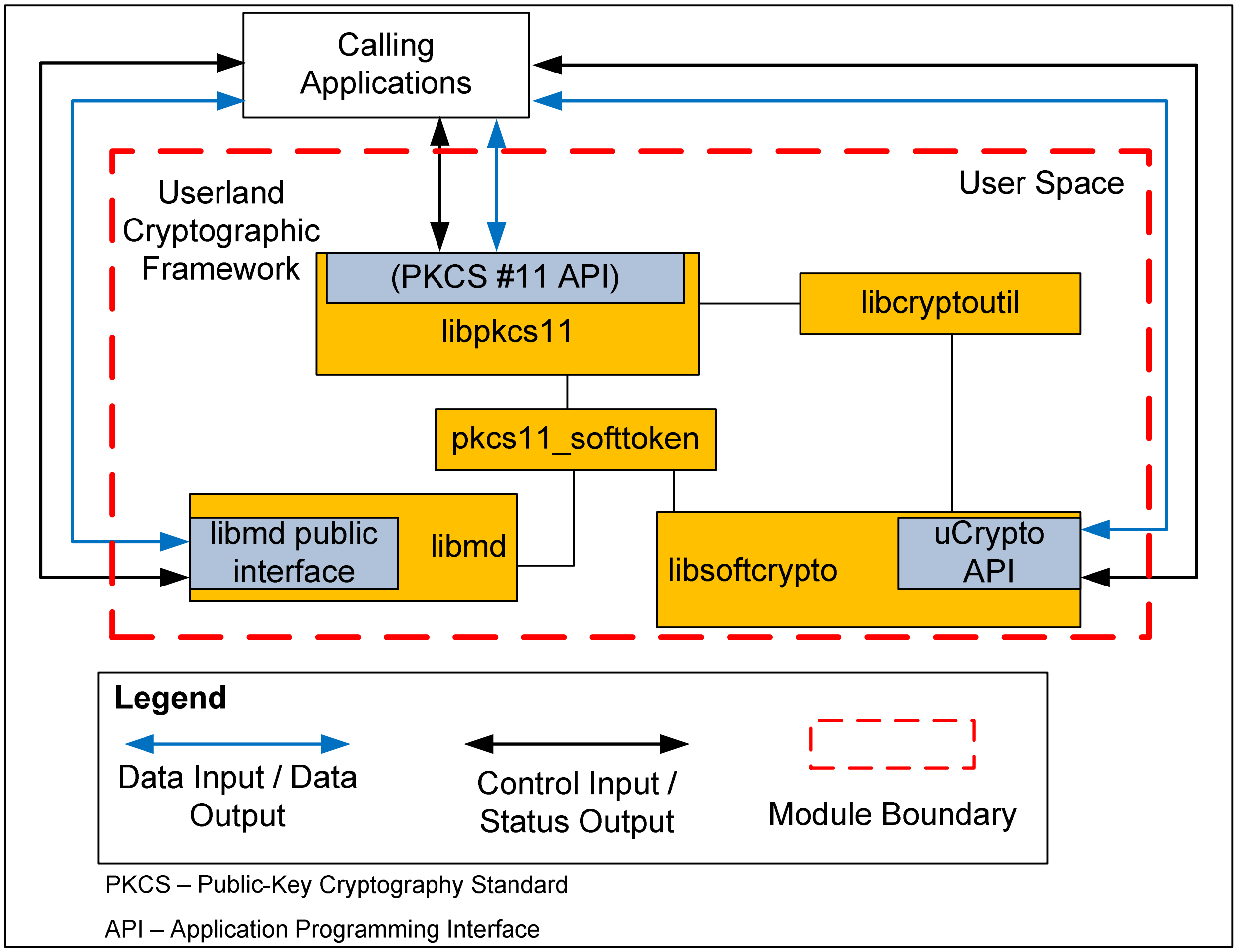
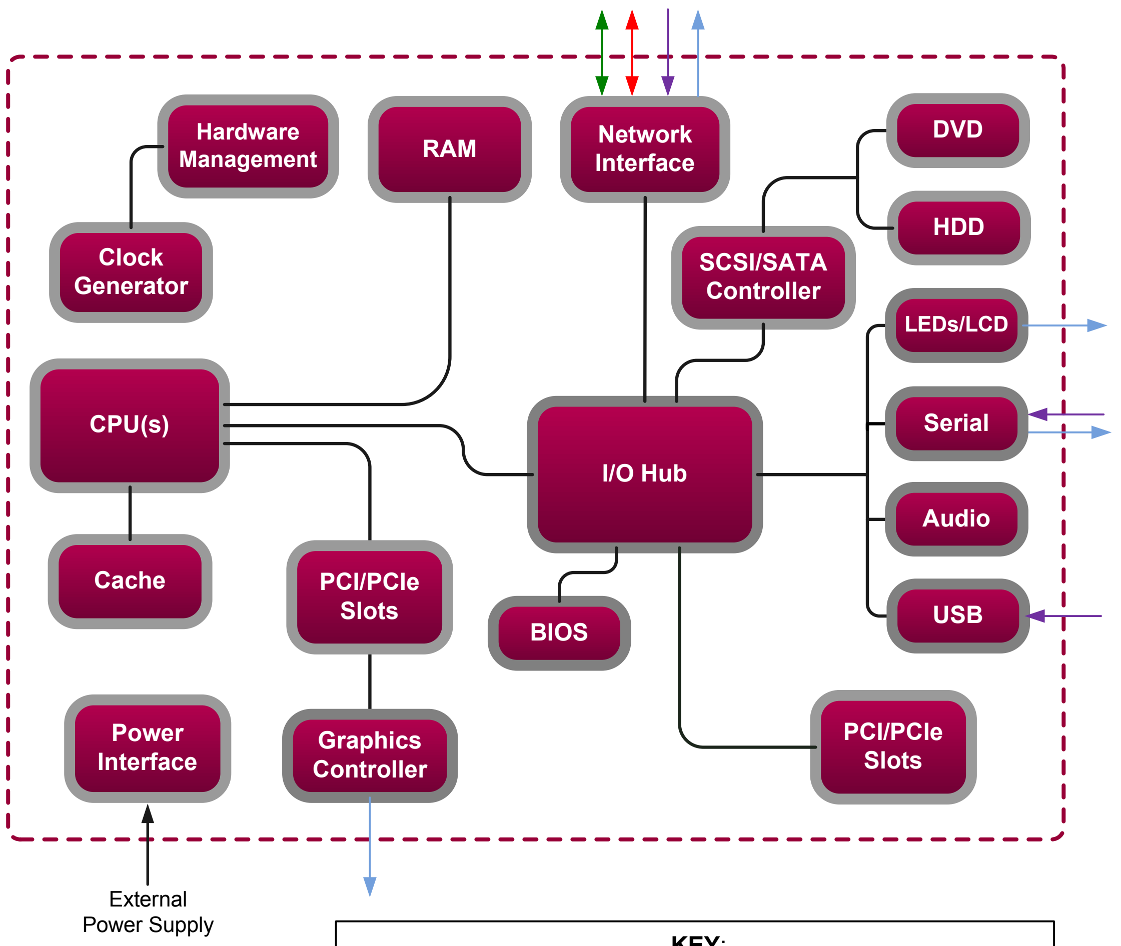


Figure 1 - Oracle Solaris Userland Cryptographic Framework Logical Block Diagram

Figure 2 and Figure 3, below, show the hardware block diagrams for the GPCs[5], utilizing Intel Xeon and SPARC64 processors that will execute the module.

[5] GPC – General Purpose Computer

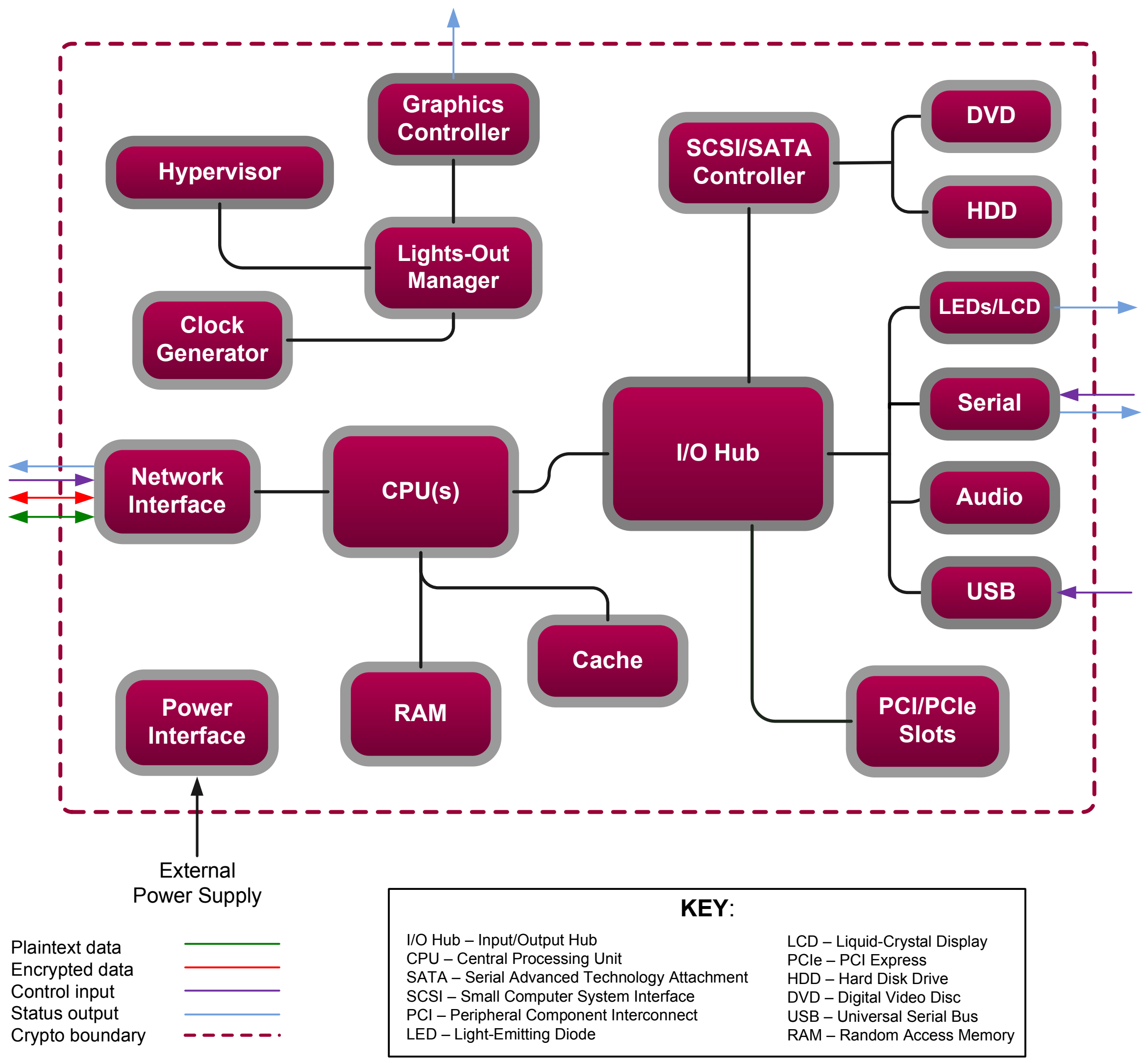


Plaintext data	🟩
Encrypted data	🟥
Control input	🟪
Status output	🟦
Crypto boundary	- - -

KEY:

BIOS – Basic Input/Output System	LCD – Liquid-Crystal Display
CPU – Central Processing Unity	PCIe – PCI express
SATA – Serial Advanced Technology Attachment	HDD – Hard Disk Drive
SCSI – Small Computer System Interface	DVD – Digital Versatile Disc
PCI – Peripheral Control Interface	USB – Universal Serial Bus
LED – Light-Emitting Diode	RAM – Random Access Memory

Figure 2 – Intel Xeon-based GPC Hardware Block Diagram



KEY:

I/O Hub – Input/Output Hub
CPU – Central Processing Unit
SATA – Serial Advanced Technology Attachment
SCSI – Small Computer System Interface
PCI – Peripheral Component Interconnect
LED – Light-Emitting Diode
LCD – Liquid-Crystal Display
PCIe – PCI Express
HDD – Hard Disk Drive
DVD – Digital Video Disc
USB – Universal Serial Bus
RAM – Random Access Memory

Figure 3 – SPARC64-based GPC Hardware Block Diagram

Module Interfaces

The module can be accessed in several different ways, depending on which library the calling application is accessing. The module provides three primary interfaces for requesting cryptographic functionality.

- libpkcs11 provides the PKCS #11 interface for accessing the majority of the cryptographic functions of the module, through pkcs11_softtoken, which provides key storage and cryptographic algorithm access.

- libsoftcrypto provides an interface known as uCrypto, which allows access to the cryptographic functions contained within libsoftcrypto, for pkcs11_softtoken and direct calls.

- While the hashing functions can be called from the PKCS#11 interface, libmd provides its own public interface for accessing hashing functions using SHA-1[6], SHA-224, SHA-256, SHA-384, and SHA-512. This interface can be utilized via direct calls to the library.

Figure 4 and Figure 5, below, show the host appliances for the module. These diagrams show the physical ports that are available on the hardware.

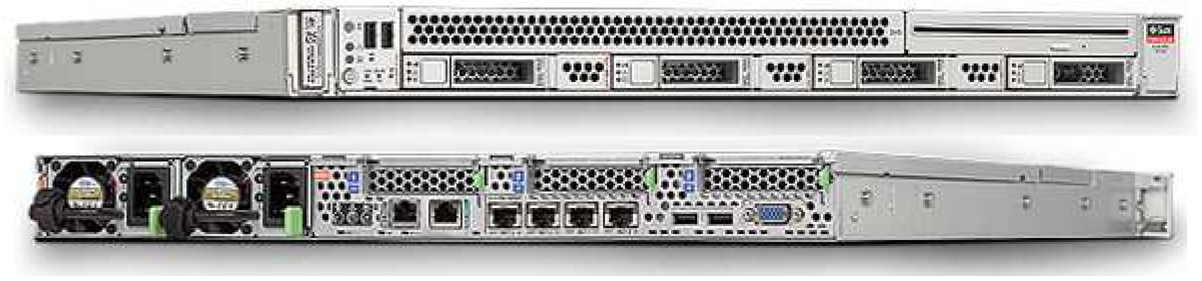


Figure 4 – Sun Server X3-2 (formerly the Sun Fire X4170 M3 server) Front and Rear Panel Ports (Intel-based)

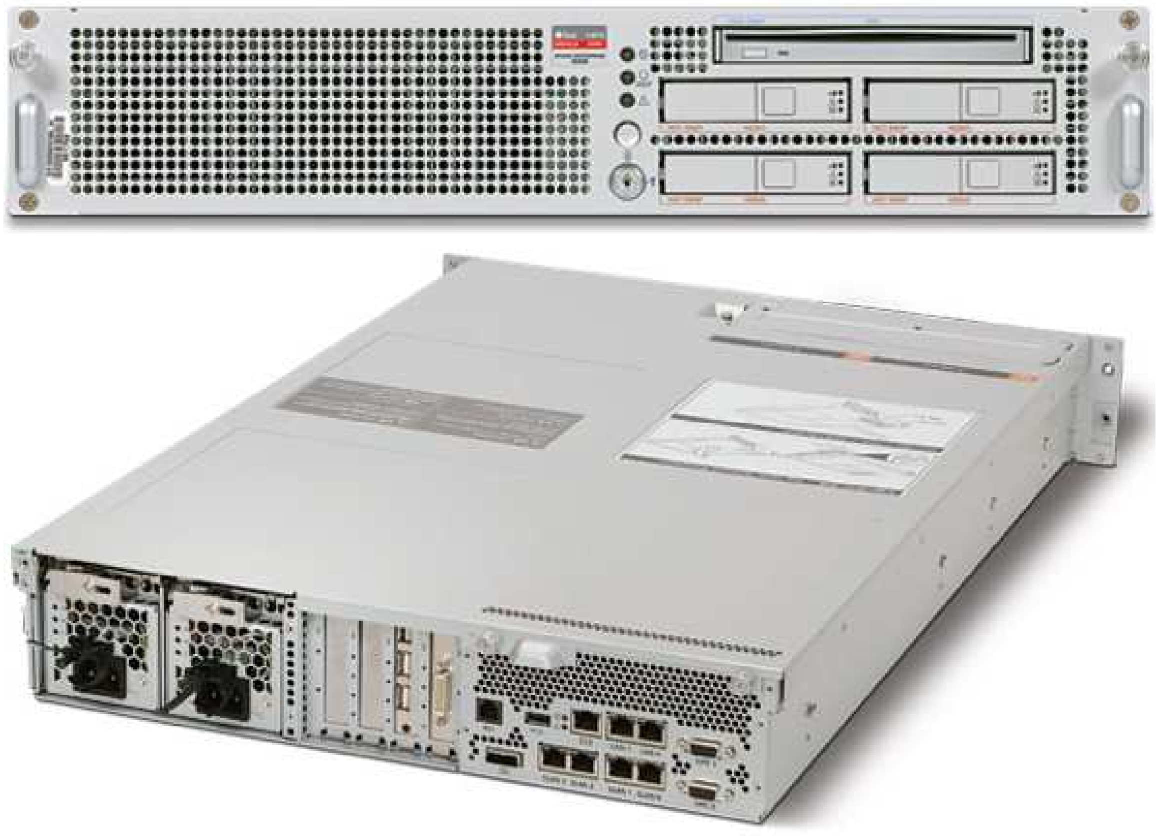


Figure 5 – M3000 Enterprise Server Front and Rear Panel Ports (SPARC64-based)

[6] SHA – Secure Hashing Algorithm

FIPS 140-2 Logical Interface	Module Logical Interface	Physical Port
Data Input	PKCS#11 API, uCrypto API, libmd public interface function calls	M3000 – Ethernet, USB[7], SAS[8] port, Serial port (RJ[9]-45), UPC[10] ports, RCI[11] port, DVD[12] optical drive
		Sun Server X3-2 – Ethernet, USB, Serial Port (RJ-45), DVD optical drive
Data Output	PKCS#11 API, uCrypto API, libmd public interface function returns	M3000 – Ethernet, USB, SAS port, Serial port (RJ-45)
		Sun Server X3-2 – Ethernet, USB, Serial Port (RJ-45)
Control Input	PKCS#11 API, uCrypto API, libmd public interface function calls	M3000 – Ethernet, USB, Power button
		Sun Server X3-2 – Ethernet, Serial (RJ-45) USB, Power button, Locator button
Status Output	PKCS#11 API, uCrypto API, libmd public interface function returns	M3000 – Ethernet, USB, VGA[13] port (HD[14]-15), status LEDs
		Sun Server X3-2 – LEDs, Serial (RJ-45), Ethernet, VGA port (HD-15)
Power Input	Not Applicable	Power Supply

Table 2 – FIPS 140-2 Logical Interfaces

Roles and Services

The module relies on the host OS for authentication. There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto Officer role and a User role.

Crypto-Officer Role

The Crypto-Officer is any operator on the host appliance with the permissions to utilize the external cryptoadm utility, or a program with the ability to access the module APIs. The Crypto-Officer role has the ability to enable and disable FIPS mode, check the status of the FIPS module, and configure cryptographic operations of the module, including which providers will be available. The Crypto-Officer is able to utilize these services via the cryptoadm commands.

[7] USB – Universal Serial Bus
[8] SAS – SCSI (Small Computer System Interface) Assisted Storage
[9] RJ – Registered Jack
[10] UPC – Usage Parameter Control
[11] RCI – Remote Cabinet Interface
[12] DVD – Digital Versatile Disc
[13] VGA – Video Graphics Array
[14] HD – High Density

Descriptions of the services available to the Crypto-Officer role are provided in Table 3, below.

The Crypto-Officer is also able to utilize all User services, described in Table 4.

Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

- Read: The CSP is read.
- Write: The CSP is established, generated, modified, or zeroized.
- Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism

Service	**Description**	**CSP**[15]	**Type of Access to CSP**
Run POST KATs on-demand	Restarting the appliance will force the FIPS self-tests to run when the module is loaded. Calling the fips140_post() function will call the Power-On Self-Tests.	Crypto-Officer credentials	Execute
Module Initialization	Use external cryptoadm utility to initialize the FIPS state.	Crypto-Officer credentials	Execute
Module Configuration	Use external cryptoadm utility to configure the module.	Crypto-Officer credentials	Execute
Zeroize keys	Format operation on the host appliance's hard drive	Crypto-Officer credentials	Execute

Table 3 – Crypto-Officer Services

The credentials for the Crypto-Officer are not considered CSPs, as requirements for module authentication are not enforced for Level 1 validation. The credentials are provided to the host OS, and are not part of the module.

User Role

The User role is able to utilize the cryptographic operations of the module, through its APIs. Descriptions of the services available to the User role are provided in the table below.

Service	**Description**	**CSP**	**Type of Access to CSP**
Symmetric encryption	Encrypt a block of data using a symmetric algorithm	AES[16] key Triple DES[17] key	Execute
Symmetric decryption	Decrypt a block of data using a symmetric algorithm	AES key Triple DES key	Execute

[15] CSP – Critical Security Parameter
[16] AES – Advanced Encryption Standard
[17] DES – Data Encryption Standard

Service	Description	CSP	Type of Access to CSP
Asymmetric key wrapping	Encrypt a block of data using an asymmetric algorithm	DSA[18] public key RSA[19] public key	Execute
Asymmetric key unwrapping	Decrypt a block of data using an asymmetric algorithm	DSA private key RSA private key	Execute
Signature Generation	Generate a signature	DSA public key RSA public key	Execute
Signature Verification	Verify a signature	DSA private key RSA private key	Execute
Asymmetric keypair generation	Generate a keypair for use in an asymmetric algorithm	DSA public key DSA private key	Write
Generate Elliptic-Curve keypair	Generate an asymmetric keypair for use in Elliptic-Curve DSA cryptographic operations	ECDSA[20] public key ECDSA private key	Write
Hashing	Perform a hashing operation on a block of data, using SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512	N/A	N/A
HMAC[21] signing	Perform a hashing operation on a block of data, using a keyed Hashed Message Authentication Code with any of the hashing operations listed above	HMAC key	Execute
Key derivation	Derive a session key using Elliptic-Curve Diffie-Hellman	Elliptic-Curve Diffie-Hellman keypair	Write
Random Number Generation	Generate random numbers	Userland FIPS 186-2 Seed Userland FIPS 186-2 Seed Key	Execute

Table 4 - User Services

Note that non-FIPS-Approved algorithms can also be used as part of these services, when the module is not operating in a FIPS-Approved mode.

Physical Security

Oracle Solaris Userland Cryptographic Framework is a software module, which FIPS defines as a multi-chip standalone cryptographic module. As such, it does not include physical security mechanisms. Thus, the FIPS 140-2 requirements for physical security are not applicable.

[18] DSA – Digital Signature Algorithm
[19] RSA – Rivest, Shamir, Adleman
[20] ECDSA – Elliptic-Curve Digital Signature Algorithm
[21] HMAC – (Keyed-) Hash-based Message Authentication Code

Operational Environment

The module operates as part of the Oracle Solaris 11.1 and 11.1 SRU5.5 Operating System. The module is programmed to utilize Intel special instruction sets for hardware-accelerated AES cryptography when running on the Intel processor. The module has been tested on Oracle Solaris 11.1 and 11.1 SRU5.5 OS, running on an M3000 Enterprise Server and Sun Server X3-2 (formerly the Sun Fire X4170 M3 server) appliance, using a SPARC64 and Intel Xeon 5600-series processor, respectively.

The Crypto-Officer shall ensure that the OS is configured to a Single-User mode of operation. Each calling application calls its own instance of the module. During execution of this instance, the calling application will be the only operator of the module. This instance cannot be called by other applications. Therefore the calling application is the single-user of the module.

Cryptographic Key Management

The module implements the following FIPS-approved algorithms:

Key or CSP	**Certificate Number**	
	11.1 SRU 3	**11.1 SRU5.5**
Symmetric Key		
AES: ECB[22], CBC[23], CFB[24]-128, CCM[25], GCM[26], and CTR[27] modes for 128, 192, and 256-bit key sizes	#2308	*#2569*
Triple DES: CBC and ECB mode for keying option 1	#1455	#1556
Asymmetric Key		
RSA PKCS#1.5 signature generation: 2048-bit (SHA-256, SHA-384, SHA-512) RSA PKCS#1.5 signature verification: 1024- , 2048-bit (w/ SHA-1, SHA-256, SHA-384, SHA-512)	#1191	*#1317*
DSA 2048-, 3072-bit Key generation; Signature generation: 2048-, 3072-bit Signature verification: 1024-, 2048-, 3072-bit	#726	*#785*
ECDSA key generation, signature generation/verification: P-192, -224, -256, -384, -521; K-163, -233, -283, -409, -571; B-163, -233, -283, -409, -571	#373	*#443*
Secure Hashing Standard (SHS)		
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	#1992	*#2165*

[22] ECB – Electronic Codebook
[23] CBC – Cipher-Block Chaining
[24] CFB – Cipher Feedback
[25] CCM – Counter with CBC-MAC
[26] GCM – Galois/Counter Mode
[27] CTR – Counter

Key or CSP	**Certificate Number**	
	11.1 SRU 3	**11.1 SRU5.5**
Message Authentication		
HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	#1422	#1586
Random Number Generation		
Userland FIPS 186-2 Random Number Generator	#1150	#1221
Key Agreement Scheme (KAS)		
Diffie-Hellman (2048 – 8192-bit)	Allowed	Allowed
Elliptic-Curve Diffie-Hellman (224 – 571-bit)	Allowed	Allowed

Table 5 – FIPS-Approved Algorithm Implementations

NOTE: The following security functions have been deemed "deprecated" or "restricted" by NIST. Please refer to NIST Special Publication 800-131A for further details.

- After December 31, 2013, key lengths providing less than 112 bits of security strength shall not be used in the Approved mode of operation to generate keys or digital signatures.
- RSA (encrypt/decrypt, sign/verify operations) provides 112 bits of encryption strength, for 2048-bit keys. RSA provides higher bits of encryption strength with higher key sizes; non-compliant with less than 112 bits of encryption strength.
- RSA (key wrapping; key establishment methodology) provides 112 bits of encryption strength, for 2048-bit keys. RSA provides higher bits of encryption strength with higher key sizes; non-compliant with less than 112 bits of encryption strength.
- Diffie-Hellman (key agreement; key establishment methodology) provides 112 bits of encryption strength, for 2048-bit public keys. Diffie-Hellman provides higher bits of encryption strength with higher key sizes; non-compliant with less than 112 bits of encryption strength. After December 31, 2013, $|n| \leq 223$ bits shall not be used in a key agreement scheme. Please see NIST Special Publication 800-131A for further details.
- Elliptic-Curve Diffie-Hellman (key agreement; key establishment methodology) provides between 112 and 256 bits of encryption strength; non-compliant less than 112 bits of encryption strength. After December 31, 2013, the use of $|n| \geq 224$ is deprecated. Values of $|n| < 224$ shall not be used. Please see NIST Special Publication 800-131A for further details.
- As of January 1, 2014, the use of the RNGs specified in FIPS 186-2, [X9.31] and ANS [X9.62] are deprecated from 2011 through December 31, 2015, and disallowed after 2015.

The module implements the following FIPS-Approved algorithm, however the implementation has not been validated and, as such, shall not be used in the FIPS-Approved mode of operation:

- Two-key Triple-DES
- SHA-512/224
- SHA-512/256

Additionally, the module implements the following non-FIPS-approved algorithms:

- MD5[28]
- MD4
- RC4[29]

[28] MD5 – Message Digest Algorithm 5

- DES
- Blowfish
- AES XCBC-MAC[30] – 128-, 192-, 256-bit
- DSA key generation – 512-, 1024-bit
- DSA signature generation – 512-, 1024-bit
- DSA signature verification – 512-bit
- RSA signature generation – 256-, 512-, 1024-bit
- RSA signature verification – 256-, 512-bit
- Diffie-Hellman – 64-, 128-, 256-, 512-, 1024-bit public keys
- Elliptic-Curve Diffie-Hellman – 112 to 223-bit public keys

The module generates cryptographic keys whose strengths are modified by available entropy. The CSPs that the module supports are listed in Table 6, below.

[29] RC4 – Rivest Cipher 4

[30] XCBC-MAC – Extended Cipher-Block Chaining Message Authentication Code

Key or CSP	Key type	Generation	Output	Storage	Zeroization	Use
AES key	AES 128-, 192-, 256-bit key	Imported (passed as an attribute in an argument)	Output from module through Data Output interface	Reference Pointer Stored in volatile memory during execution Exported to hard drive of GPC	Zeroized upon completion of operation or reboot Zeroized via format hard-drive service	Symmetric encryption
AES GCM IV	Random data	Imported (passed as an attribute in an argument)	Never output from module	Reference Pointer Stored in volatile memory during execution	Zeroized upon completion of operation or reboot	IV input to AES GCM function
Triple DES key	Triple DES 168-bit key	Imported (passed as an attribute in an argument)	Output from module through Data Output interface	Reference Pointer Stored in volatile memory during execution Exported to hard drive of GPC	Zeroized upon completion of operation or reboot Zeroized via format hard-drive service	Symmetric encryption
RSA public key	RSA 1024[31]-, 2048-, 4096-, 8192-bit key	Imported (passed as an attribute in an argument)	Output from module through Data Output interface	Reference Pointer Stored in volatile memory during execution Exported to hard drive of GPC	Zeroized upon completion of operation or reboot Zeroized via format hard-drive service	Key wrapping, certificate generation, certificate verification, signature verification

[31] Please note that RSA 1024-bit key used for signature verification is considered legacy-use after 2010, and is disallowed for signature generation and key transport after 2013.

Key or CSP	Key type	Generation	Output	Storage	Zeroization	Use
RSA private key	RSA 2048-, 4096-, 8192-bit key	Imported (passed as an attribute in an argument)	Output from module through Data Output interface	Reference Pointer Stored in volatile memory during execution Exported to hard drive of GPC	Zeroized upon completion of operation or reboot Zeroized via format hard-drive service	Key wrapping, certificate generation, certificate verification, signature generation
RSA signature	RSA 2048-, 4096-, 8192-bit signature	Imported (passed as an attribute in an argument) Generated internally	Output from module through Data Output interface	Reference Pointer Stored in volatile memory during execution Exported to hard drive of GPC	Zeroized upon completion of operation or reboot Zeroized via format hard-drive service	Signing data, signature verification
DSA public key	DSA 2048-, 3072-bit key	Imported (passed as an attribute in an argument) Generated internally	Output from module through Data Output interface	Reference Pointer Stored in volatile memory during execution Exported to hard drive of GPC	Zeroized upon completion of operation or reboot Zeroized via format hard-drive service	Signature verification
DSA private key	DSA 224-, 256-bit private key	Imported (passed as an attribute in an argument) Generated internally	Output from module through Data Output interface	Reference Pointer Stored in volatile memory during execution Exported to hard drive of GPC	Zeroized upon completion of operation or reboot Zeroized via format hard-drive service	Signature generation

Key or CSP	Key type	Generation	Output	Storage	Zeroization	Use
ECDSA public key	ECDSA 163-, 192-, 224-, 233-, 256-, 283-, 384-, 409-, 512-, 571-bit public key	Imported (passed as an attribute in an argument) Generated internally	Output from module through Data Output interface	Reference Pointer Stored in volatile memory during execution Exported to hard drive of GPC	Zeroized upon completion of operation or reboot Zeroized via format hard-drive service	Encrypting data, verifying signature
ECDSA private key	ECDSA 163-, 192-, 224-, 233-, 256-, 283-, 384-, 409-, 512-, 571-bit private key	Imported (passed as an attribute in an argument) Generated internally	Output from module through Data Output interface	Reference Pointer Stored in volatile memory during execution Exported to hard drive of GPC	Zeroized upon completion of operation or reboot Zeroized via format hard-drive service	Decrypting data, digitally signing data
HMAC key	Secret key for HMAC	Imported	Never output from module	Reference Pointer Stored in volatile memory during execution Exported to hard drive of GPC	Zeroized upon completion of operation or reboot	Message Integrity/Authentication

ECDH[32] private key	P-192, -224, -256, -384, -521;
	K-163, -233, -283, -409, -571;
	B-163, -233, -283, -409, -571 private key
		Imported (passed as an attribute in an argument)
		
		Generated internally
			Output from module through Data Output interface	Reference Pointer Stored in volatile memory during execution
				
				Exported to hard drive of GPC
					Zeroized upon completion of operation or reboot
					
					Zeroized via format hard-drive service
						Decryption

[32] ECDH – Elliptic-Curve Diffie-Hellman

Key or CSP	Key type	Generation	Output	Storage	Zeroization	Use

ECDH public key	P-192, -224, -256, -384, -521;
	K-163, -233, -283, -409, -571;
	B-163, -233, -283, -409, -571 public key
		Imported (passed as an attribute in an argument)
		
		Generated internally
			Output from module through Data Output interface	Reference Pointer Stored in volatile memory during execution
				
				Exported to hard drive of GPC
					Zeroized upon completion of operation or reboot
					
					Zeroized via format hard-drive service
						Encryption

Diffie-Hellman private key	224-, 256-, 384-bit private key	Generated internally	Output from module through Data Output interface	Plaintext in volatile memory	Cleared on session close	Decryption
Diffie-Hellman public key	2048-, 4096-, 8192-bit public key	Generated internally	Output from module through Data Output interface	Plaintext in volatile memory	Cleared on session close	Encryption
Userland RNG[33] Seed	20-byte Hexadecimal string	Generated internally	Never output from module	Plaintext in volatile memory	Zeroized upon completion of operation or reboot	To calculate SHA-1 string in FIPS 186-2 RNG
Userland RNG Seed Key	20-byte SHA-1 Digest	Generated internally	Never output from module	Plaintext in volatile memory	Zeroized upon completion of operation or reboot	To calculate SHA-1 string in FIPS 186-2 RNG

Table 6 - Listing of Key and Critical Security Parameter

[33] RNG – Random Number Generator

Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to ensure all components are functioning correctly.

Power-Up Self-tests

To confirm correct functionality, the software library performs the following self-tests:

- Software Integrity Test (HMAC SHA-1)
- Known Answer Tests (KATs)
  - AES KAT
  - Triple-DES KAT
  - RSA sign/verify KAT
  - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 HMAC KAT
  - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
  - FIPS 186-2 RNG KAT
- Pairwise Consistency Tests
  - DSA sign/verify pairwise consistency test
  - ECDSA sign/verify pairwise consistency test

Conditional Self-tests

The Solaris Userland Cryptographic Framework performs the following conditional self-tests:

- DSA key generation pairwise consistency test
- ECDSA key generation pairwise consistency test
- FIPS 186-2 continuous random number generator test

Data output from the module is inhibited, while running self-tests. Should any of the power-up self-tests or conditional self-tests fail, the modules will cease operation, inhibiting any further data output from the modules. The modules will need to reboot and perform power-up self-tests. Successful completion of the power-up self-tests will return the module to normal operation.

Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

Secure Operation

The Oracle Solaris Userland Cryptographic Framework meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in a FIPS-approved mode of operation.

Initial Setup

The Oracle Solaris Userland Cryptographic Framework module is part of the Oracle Solaris operating system. Immediately after initial installation of the Oracle Solaris operating system, the Crypto-Officer must install a specific service to ensure sufficient entropy for random number generation functions within the module. The "fips-random service" is available from Oracle's standard support repository.

The fips-random service must be loaded onto the operating system's host appliance. The Crypto-Officer must ensure the package repository is up to date using:

```
http://pkg.oracle.com/solaris/support
```

The Crypto-Officer will then install the package by running the following command:

```
pkg install pkg:service/security/fips-random
```

Once the package is added, the Oracle Solaris operating system must be rebooted. It should be noted that this package can alternatively be listed in the Auto Install manifest so that it will be added and run at the initial operating system install time.

The next time that the Solaris operating system is booted, the Crypto-Officer must use the external cryptoadm utility to make the changes necessary to enable FIPS mode.

The Crypto-Officer must verify that pkcs11_softtoken is present in the list of providers, and is not disabled, using the "cryptoadm list" command. If it is not present, the Crypto-Officer must use the "cryptoadm enable <*provider name*> <*mechanism list*>" command to enable /usr/lib/security/$ISA/pkcs11_softtoken.so. The host OS will not boot properly without pkcs11_softtoken being enabled. The pkcs11_softtoken provider is the only provider installed in the validated configuration. MD5 is included as part of this provider, for TLS[34] uses only. The use of MD5 is allowed in the TLS or

[34] TLS – Transport Layer Security

DTLS[35] protocol only. MD5 shall not be used as a general hash function in an Approved mode of operation.

The Crypto-Officer must input the command "cryptoadm disable provider='/user/lib/security$ISA/pkcs11_kernel.so' all". This command disables the module's direct access to functions operating in the kernel.

Next, the Crypto-Officer must create a new boot environment, using the "beadm create <name>" command, where the name is one provided by the Crypto-Officer. This creates a boot environment which is a clone of the currently running environment, to be used if there is a panic or other error with initialization. The Crypto-Officer must then input the command "cryptoadm enable fips-140", in order to enable FIPS mode. The module must then be restarted by a full system reboot. Once the module loads, it will perform power-on cryptographic self-tests. Once all tests are successful, the module will begin to operate in a FIPS-Approved mode.

Crypto-Officer Guidance

The Crypto-Officer is responsible for making sure the module is running in FIPS-Approved mode of operation and to ensure that only FIPS-Approved algorithms are utilized. The following algorithms and key sizes, provided by the module, cannot be used in FIPS-Approved mode of operation:

- MD5 – for non-TLS uses
- MD4
- RC4
- DES
- Blowfish
- 2-key Triple DES
- AES XCBC-MAC (128-, 192-, 256-bit)
- DSA key generation – 512-, 1024-bit
- DSA signature generation – 512-, 1024-bit
- DSA signature verification – 512-bit
- RSA signature generation – 256-, 512-, 1024-bit
- RSA signature verification – 256-, 512-bit

Initialization

It is the Crypto-Officer's responsibility to configure the module into the FIPS-Approved mode.

Management

Using the commands available to the Crypto-Officer, outlined in Table 3, the cryptoadm utility can be used to configure and manage the module.

[35] DTLS – Datagram Transport Layer Security

Zeroization

As shown in Table 6, certain keys are stored on the host appliance's hard drive. A format of the host appliance's hard-drive will zeroize all keys.

User Guidance

It is the responsibility of the User calling applications to ensure that only FIPS-Approved algorithms and providers are being utilized by their commands. The User is required to operate the module in a FIPS-Approved mode of operation. In order to maintain FIPS-mode, the User must do the following:

- Only utilize the module interfaces to call FIPS-Approved algorithms

ACRONYMS

AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard – New Instruction
API	Application Programming Interface
CBC	Cipher-Block Chaining
CCM	Counter with CBC-MAC
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DVD	Digital Versatile Disc
DTLS	Datagram Transport Layer Security
ECB	Electronic Codebook
ECDH	Elliptic-Curve Diffie-Hellman
ECDSA	Elliptic-Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GPC	General Purpose Computer
HD	High Density
HMAC	(Keyed-) Hash-based Message Authentication Code
KAT	Known Answer Test
LED	Light Emitting Diode
MAC	Message Authentication Code
MD5	Message Digest Algorithm 5
NIST	National Institute of Standards and Technology
OS	Operating System
PKCS	Public Key Cryptography Standards
RCI	Remote Cabinet Interface
RJ	Registered Jack
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SAS	Small Computer System Interface-Assisted Storage
SHA	Secure Hash Algorithm
SPARC	Scalable Processor Architecture
UPC	Usage Parameter Control
USB	Universal Serial Bus
VGA	Video Graphics Array
XCBC-MAC	Extended Cipher-Block Chaining Message Authentication Code