FIPS 140-2 Non-Proprietary Security Policy

Oracle Solaris Userland Cryptographic Framework

FIPS 140-2 Level 1 Validation

Software Version:

1.3

Date: July 27, 2016

Title: Oracle Solaris Userland Cryptographic Framework
27 July 2016
Author: Acumen Security
Contributing Authors: N/A

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.
Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

ORACLE®

TABLE OF CONTENTS

List of Tables

List of Figures

ORACLE®

1 Introduction

1.1 Overview

This document is the Security Policy for the Oracle Solaris Userland Cryptographic Framework designed by Oracle Corporation. The Oracle Solaris Userland Cryptographic Framework is also referred to as 'the module' or 'module'. This Security Policy specifies the security rules under which the module shall operate to meet the requirements of FIPS 140-2 Level 1. It also describes how Oracle Solaris Userland Cryptographic Framework functions in order to meet the FIPS requirements, and the actions that operators must take to maintain the security of Oracle Solaris Userland Cryptographic Framework.

This Security Policy describes the features and design of the Oracle Solaris Userland Cryptographic Framework module using the terminology contained in the FIPS 140-2 specification. *FIPS 140-2, Security Requirements for Cryptographic Modules* specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST/CSE Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

1.2 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:

- Oracle Non-Proprietary Security Policy
- Oracle Vendor Evidence document
- Finite State Machine
- Entropy Assessment Document
- 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 and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Oracle.

2 Oracle Solaris Userland Cryptographic Framework

2.1 Functional Overview

The Oracle Solaris cryptographic framework is an architecture that enables applications in the Oracle Solaris operating system to use or provide cryptographic services. At a high level it consists of Userland Cryptographic Framework and Kernel Cryptographic Framework. This Security Policy is for the Userland Cryptographic Framework.

3 Cryptographic Module Specification

3.1 Definition of the Cryptographic Module

The Oracle Solaris Userland Cryptographic Framework module is a multiple-chip standalone cryptographic module as defined by the requirements of FIPS PUB 140-2. The module provides cryptographic functionality for any application that calls into it. The module provides encryption, decryption, hashing, secure random number generation, signature generation and verification, certificate generation and verification, message authentication functions, and key pair generation for RSA and DSA. The module can leverage the algorithm acceleration from SPARC and X86 processors when available.

3.2 Cryptographic Boundary

The cryptographic module is composed of two shared objects, PKCS11_softtoken.so and libucrypto.so, which together are known as the Oracle Solaris Userland Cryptographic Framework. A representation of the cryptographic boundary is defined below by the red dotted line:

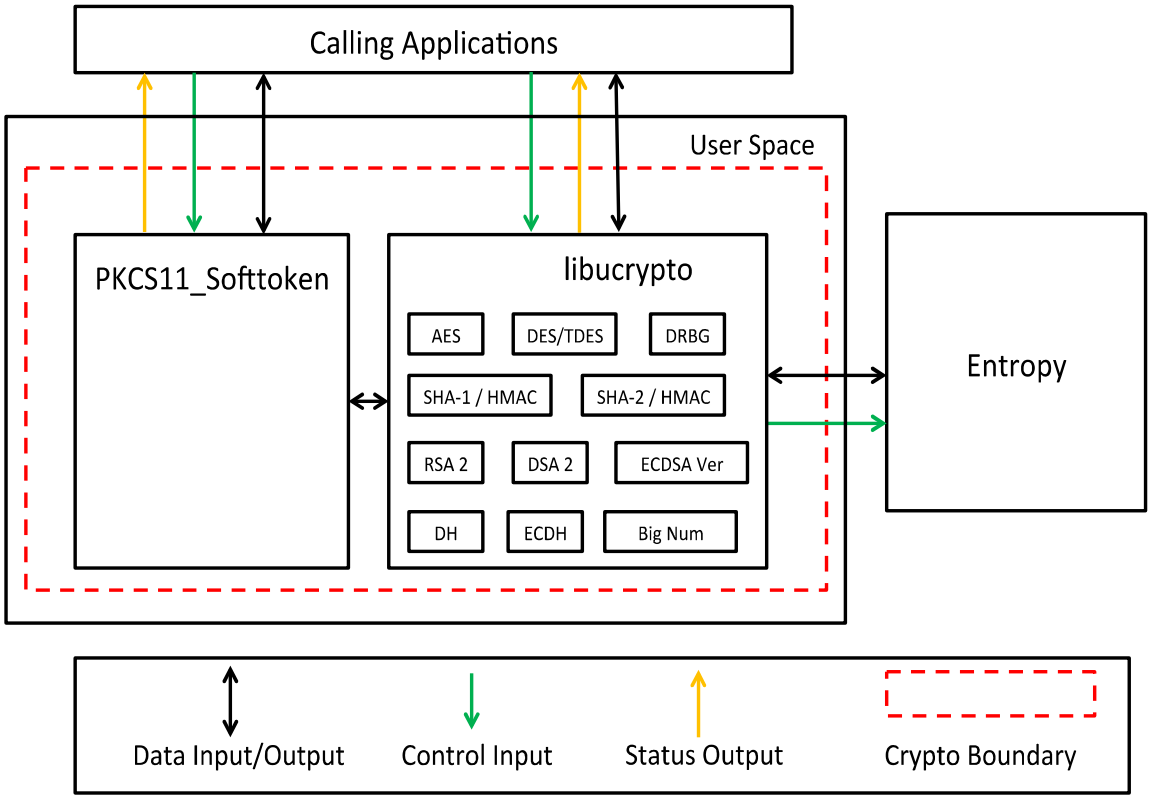

Figure 1: Solaris Cryptographic Framework Cryptographic Boundary

3.3 FIPS 140-2 Validation Scope

The Oracle Solaris Userland Cryptographic Framework is being validated to overall FIPS 140-2 Level 1 requirements. See Table 1 below.

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

Table 1: FIPS 140-2 Security Requirements

3.4 Security Functions

3.4.1 Approved or Allowed Security Functions

The Oracle Solaris Userland Cryptographic Framework module contains the following FIPS Approved Algorithms listed in Table 2:

Approved or Allowed Security Functions	Certificate
Symmetric Encryption/Decryption	
AES: (CBC, ECB, CFB128, CTR, CCM, GCM); Encrypt/Decrypt; Key Size = 128, 192, 256 XTS[1]; Encrypt/Decrypt; Full/Partial Block; Key Size = 128, 256	3936
Triple-DES: **TCBC**(KO 1 e/d) ; **TECB**(KO 1 e/d)	2159
Secure Hash Standard (SHS)	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512_224, SHA-512_256 (Byte Only)	3245
Data Authentication Code	
HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-SHA-512_224, HMAC-SHA-512_256, (KeySizes = KS < BS; KS = BS; KS > BS)	2558
Asymmetric Algorithms	
RSA: **FIPS186-4:** **186-4KEY(gen):** FIPS186-4_Random_e **ALG[RSASSA-PKCS1_V1_5] SIG(gen)** (2048 SHA(224, 256 , 384 , 512)) (3072 SHA(224, 256 , 384 , 512)) **SIG(Ver)** (1024 SHA(1, 224 , 256 , 384 , 512)) (2048 SHA(1, 224, 256 , 384 , 512)) (3072 SHA(1, 224, 256 , 384 , 512))	2011
ECDSA**: FIPS186-4:** SigVer: CURVES(P-192, P-224, P-256, P-384 P-521, K-163, K-233, K-283, K-409, K-571, B-163, B-233, B-283, B-571 : (SHA-1))	862
DSA: **FIPS186-4:** **KeyPairGen:** [(2048,224) ; (2048,256) ; (3072,256)] **SIG(gen)PARMS TESTED:** [(2048,224) SHA(224 , 256 , 384 , 512); (2048,256) SHA(224 , 256 , 384 , 512); (3072,256) SHA(224 , 256 , 384 , 512);] **SIG(ver)PARMS TESTED:** [(1024,160) SHA(1 , 224 , 256 , 384 , 512); (2048,224) SHA(1 , 224 , 256 , 384 , 512); (2048,256) SHA(1 , 224 , 256 , 384 , 512); (3072,256) SHA(1 , 224 , 256 , 384 , 512)]	1074
Random Number Generation	
NIST SP 800-90A Rev. 1: **Hash_Based DRBG**: [Prediction Resistance Tested: Enabled (SHA-512)]	1143

Table 2: FIPS Approved or Allowed Security Functions

[1] XTS mode can only be used for storage applications

Note that the DRBG requests 256 bits of entropy per GET function.

3.4.2 Non-Approved But Allowed Security Functions

The following are considered non-Approved but allowed security functions:

Non-Approved But Allowed	Use
Diffie-Hellman	key agreement, key establishment methodology between 112 and 192 bits of encryption strength
EC Diffie-Hellman	key agreement, key establishment methodology between 112 and 256 bits of encryption strength
RSA	key wrapping, key establishment methodology provides between 112 and 192 bits of encryption strength

Table 3: Non-Approved but Allowed Security Functions

3.4.3 Non-Approved Security Functions

The following are considered non-Approved security functions:

Non-Approved Security Functions	
MD5	HMAC MD5
MD4	RC4
DES	Blowfish
AES XCBC-MAC	ECDSA Key Generation and Signature Generation
Camelia	HMAC-SHA-1 (PKCS11_softtoken implementation, non-compliant)
SHA-1 (PKCS11_softtoken implementation, non-compliant)	Diffie-Hellman (key agreement, non-compliant less than 112 bits of encryption strength)
EC Diffie-Hellman (key agreement, non-compliant less than 112 bits of encryption strength)	RSA (key wrapping, non-compliant less than 112 bits of encryption strength)
Triple-DES(2-key option, encrypt/decrypt)	

Table 4: Non-Approved Security Functions

4 Module Ports and Interfaces

The module can be accessed by utilizing the API it exposes. Table 5 below, shows the interfaces provided by the module.

FIPS 140-2 Logical Interface	Logical Port
Data Input	Input arguments to PKCS#11 and uCrypto APIs
Data Output	Output arguments to PKCS#11 and uCrypto APIs
Control Input	PKCS#11 and uCrypto APIs
Status Output	Return variables of PKCS#11 and uCrypto APIs
Power	N/A

Table 5: Mapping of FIPS 140 Logical Interfaces to Logical Ports

5 Operating System

5.1 Definition of Operating System Embodiment

The module runs on a general purpose operating system as defined in section 4.6 of FIPS PUB 140-2. The module uses a strong integrity test using HMAC-SHA-256.

5.2 Tested Configurations

The module was tested on the following configurations:

Hardware	Processor	Operating System
Oracle SPARC T5-1B Server	SPARC T5 (with and without acceleration)	Solaris 11.3
Oracle SPARC T7-2 Server	SPARC M7 (with and without acceleration)	Solaris 11.3
Oracle Server X5-2	Intel Xeon E5 (with and without acceleration)	Solaris 11.3

Table 6: Tested Operational Environments

5.3 Vendor Affirmed Configurations

Additionally, Oracle affirms that the module will function the same way and provide the same security services on any of the systems listed below[2].

S3 Core Processors

- Oracle SPARC T4-1
- Oracle Netra SPARC T4-1B
- Oracle SPARC T4-2
- Oracle SPARC T4-4
- Oracle SPARC T4-1B
- Oracle Netra SPARC T5-1B
- Oracle SPARC T5-2
- Oracle SPARC T5-4 Server
- Oracle SPARC T5-8 Server
- Oracle SPARC M5-32 Server
- Oracle SPARC M6-32 Server

S4 Core Processors

- Oracle SPARC T7-1 Server
- Oracle SPARC T7-4 Server

[2] The CMVP makes no claims as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not listed on the validation certificate.

- Oracle SPARC M7-8 Server
- Oracle SPARC M7-16 Server
- Oracle SPARC S7-2 Server
- Oracle SPARC S7-2L Server
- Oracle MiniCluster S7-2 Engineered System

X86 Systems

- Oracle Sun Blade X3-2B
- Oracle Sun Server X3-2
- Oracle Sun Server X3-2L
- Oracle Sun Blade X4-2B
- Oracle Sun Server X4-2
- Oracle Sun Server X4-2L
- Oracle Sun Server X4-4
- Oracle Sun Server X4-8
- Oracle Sun Server X5-2
- Oracle Sun Server X5-2L
- Oracle Sun Server X5-4
- Oracle Sun Server X5-8
- Oracle Netra Server X3-2
- Oracle Netra Server X5-2
- Oracle Server X6-2
- Oracle Server X6-2L

Fujitsu further affirms that the module will function the same way and provide the same security services on any of the systems listed below.

Note: The following Fujitsu M10 SPARC systems using the SPARC64 processor are known by different product marketing names depending on locale and are otherwise identical:

- Fujitsu M10-1 is named the SPARC M10-1 in Japan.
- Fujitsu M10-4 is named the SPARC M10-4 in Japan.
- Fujitsu M10-4S is named the SPARC M10-4S in Japan.

6 Roles and Services

The Oracle Solaris Userland Cryptographic Framework implements two roles - a Crypto Officer Role (CO) and a User Role (U) that are implicitly assumed by operators based on the services they execute. Table 7 gives a high level description of all services provided by the module and lists the roles allowed to invoke each service. The following abbreviations are used for roles:

X – Execute (includes read and write operations), Z – Zeroize

U	CO	Service Name	Service Description	Keys and CSP(s)	Access Type(s)
	X	Run POSTs on-demand	Restarting the appliance will force the FIPS self-tests to run when the module is loaded. Alternatively the appropriate API can also be called to run the on-demand self-test.	Software Integrity Key	X
	X	Module Initialization	Use external cryptoadm utility to initialize the FIPS state.	N/A	N/A
	X	Module Configuration	Use external cryptoadm utility to configure the module.	N/A	N/A
	X	Zeroize Keys	Format operation on the host appliance's hard drive and power-cycle	All keys	Z
X		Symmetric Key Generation	Generate AES and Triple-DES keys	Symmetric Keys	X
X		Symmetric Encryption and Decryption	Encrypt/Decrypt data using a symmetric algorithm	Symmetric Keys	X
X		Asymmetric Key Generation	Generate RSA and DSA key pairs	Asymmetric Private Key (RSA and DSA)	X
X		Asymmetric Key establishment	Establish keys using RSA key wrapping, DH, or ECDH	Asymmetric Private Key (RSA) Diffie-Hellman and EC Diffie Hellman private key	X X
X		Signature Generation	Generate RSA and DSA signatures	Asymmetric Private Key (RSA and DSA)	X
X		Signature Verification	Verify RSA, DSA and ECDSA signatures	No Key/CSP access but uses Asymmetric Public Key (RSA, DSA and ECDSA)	N/A
X		Hashing	Perform a hashing operation on a block of data, using SHA algorithm	N/A	N/A
X		HMAC	Perform a hashing operation on a block of data, using a keyed Hashed Message Authentication Code with any of the hashing operations listed above	Keyed Hash Key (HMAC)	X
X		Random Number Generation	Generate random numbers using SP 800-90A DRBG	DRBG V value DRBG C value Entropy	X X X

Table 7: Services Authorized for Roles

Note: The services listed above can also be executed using non-approved algorithms (See Section 3.4.3) thereby making them non-approved services.

7 Key and CSP Management

The following keys, cryptographic key components and other critical security parameters are contained in the module.

CSP Name	Generation/Input	Input/Output	Storage	Use
Symmetric Keys (AES and Triple-DES)	Generated internally via DRBG and Entered via API	Input via API	RAM	Used for symmetric encryption and decryption
Asymmetric Key pairs	Generated internally via DRBG and entered via API	Input via API	RAM	Used for RSA and DSA signature generation and verification
Diffie-Hellman and EC Diffie Hellman key pairs	Generated internally via DRBG and entered via API	Input via API	RAM	Used for DH and ECDH key agreement
Keyed Hash Key (HMAC)	Generated internally via DRBG and Entered via API	Input via API	RAM	Used for keyed hashing (HMAC)
DRBG V value	Generated internally via entropy input	N/A	RAM	Used as part of SP 800-90A DRBG
DRBG C value	Generated internally via entropy input	N/A	RAM	Used as part of SP 800-90A DRBG
Entropy	Entered via API	N/A	RAM	Used as part of SP 800-90A DRBG
Software Integrity Key (HMAC)	N/A	N/A	Disk	Installed as part of crypto module installation

Table 8: Cryptographic Keys and CSPs

8 Self-Tests

8.1 Power-Up Self-Tests

Oracle Solaris Userland Cryptographic Framework performs the following power-up self-tests when power is applied to the module. These self-tests require no inputs or actions from the operator:

Libucrypto.so

- Software Integrity Test (HMAC-SHA-256)
- AES (Encrypt/Decrypt) KAT
- Triple-DES (Encrypt/Decrypt) KAT
- HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 KAT
- RSA sign/verify KAT
- DSA sign/verify test
- ECDSA sign/verify test
- DRBG KAT

PKCS11_Softtoken.so

- Software Integrity Test (HMAC-SHA-256)

When the module is in a power-up self-test state or error state, the data output interface is inhibited and remains inhibited until the module can transition into an operational state.

8.2 Conditional Self-Tests

The module performs the following conditional self-tests when called by the module:

- Pair Wise consistency test to verify that the asymmetric keys generated for RSA and DSA work correctly by performing a sign and verify operation;
- DRBG conditional test to verify that the output of DRBG is not the same as the previously generated value;
- DRBG Health Tests; and
- Entropy source conditional test to verify that the output of the entropy source to be used as seeding material into the FIPS Approved DRBG is not the same as the previously generated value.

9 Crypto-Officer and User Guidance

The module 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.

9.1 Secure Setup and Initialization

1. Firstly, the Crypto Officer must create a BE based on current configuration and boot it:
 # beadm create S11.3-FIPS-140
 # beadm activate S11.3-FIPS-140
 # reboot

2. Upon successful reboot, in the new BE, enable FIPS 140 mode in the Cryptographic Framework:
 # cryptoadm enable fips-140

If the fips-140 package is not yet loaded, this command also loads the package.

3. After the consumers are configured, reboot the BE.

 # reboot

At this time the system should be in FIPS mode of operation. This can be verified by issuing the following command:

 # cryptoadm list fips-140

In the output pkcs11_softtoken should indicate that FIPS 140 mode is enabled.

9.2 Module Security Policy Rules

This section describes the rules for operating the module in FIPS-approved mode of operation.

9.2.1 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. Algorithms listed in Table 4 shall not be used in FIPS-Approved mode of operation.

9.2.1.1 Initialization

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

9.2.1.2 Management

Using the commands available to the Crypto-Officer outlined in Table 7, the cryptoadm utility can be used to configure and manage the module.

9.2.1.3 Zeroization

As shown in Table 8, certain keys are stored on the host appliance's hard drive. A format of the host appliance's hard-drive will zeroize all keys. Additionally keys in RAM can be zeroized via a power-cycle.

9.2.2 User Guidance

It is the responsibility of the User to ensure that only FIPS-Approved algorithms and providers are being utilized. The User is required to operate the module in a FIPS-Approved mode of operation. In order to maintain FIPS-mode, the User must only utilize the module interfaces to call FIPS-Approved algorithms. Moreover for AES GCM, IVs must be generated internally only and must be at least 96-bits.

10 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.

ORACLE

Appendices

Acronyms, Terms and Abbreviations

Term	Definition
AES	Advanced Encryption Standard
BE	Boot Environment
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment of Canada
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
ECDSA	Elliptic Curve Digital Signature Algorithm
EDC	Error Detection Code
HMAC	(Keyed) Hash Message Authentication Code
KAT	Known Answer Test
LED	Light Emitting Diode
NIST	National Institute of Standards and Technology
POST	Power On Self Test
PUB	Publication
RAM	Random Access Memory
ROM	Read Only Memory
SHA	Secure Hash Algorithm
AES-NI	Advanced Encryption Standard – New Instructions
TLS	Transport Layer Security
SPARC	Scalable Processor Architecture

References

The FIPS 140-2 standard, and information on the CMVP, can be found at http://csrc.nist.gov/groups/STM/cmvp/index.html. More information describing the Oracle Solaris Userland Cryptographic Framework can be found on the Oracle web site at www.oracle.com .

This Security Policy contains non-proprietary information. All other documentation submitted for FIPS 140-2 conformance testing and validation is "Oracle - Proprietary" and is releasable only under appropriate non-disclosure agreements.

Document	Author	Title
FIPS PUB 140-2	NIST	FIPS PUB 140-2: Security Requirements for Cryptographic Modules (Dec. 2002)
FIPS IG	NIST	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program
FIPS PUB 140-2 Annex A	NIST	FIPS 140-2 Annex A: Approved Security Functions
FIPS PUB 140-2 Annex B	NIST	FIPS 140-2 Annex B: Approved Protection Profiles
FIPS PUB 140-2 Annex C	NIST	FIPS 140-2 Annex C: Approved Random Number Generators
FIPS PUB 140-2 Annex D	NIST	FIPS 140-2 Annex D: Approved Key Establishment Techniques
DTR for FIPS PUB 140-2	NIST	Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules
NIST SP 800-67	NIST	Recommendation for the Triple Data Encryption Algorithm TDEA Block Cypher
FIPS PUB 197	NIST	Advanced Encryption Standard
FIPS PUB 198-1	NIST	The Keyed Hash Message Authentication Code (HMAC)
FIPS PUB 186-4	NIST	Digital Signature Standard (DSS)
FIPS PUB 180-4	NIST	Secure Hash Standard (SHS)
NIST SP 800-131A Rev. 1	NIST	Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes
NIST SP 800-90A Rev. 1	NIST	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
PKCS#1	RSA Laboratories	PKCS#1 v1.5: RSA Cryptographic Standard

All of the above references are available at URL: http://csrc.nist.gov/groups/STM/cmvp/index.html.