ORACLE
Communications

FIPS 140-3 Non-Proprietary Security Policy

# Oracle Communications

# Acme Packet 4600 and Acme Packet 6350

Prepared by:

Lightship Security

Applus

www.lightshipsec.com


This document may be reproduced whole and intact including the Copyright notice.

**Title:** Acme Packet 4600 and Acme Packet 6350
**Date:** May 29th, 2026
Contributing Authors:
Oracle Acme Packet Engineering
Security Evaluations – Global Product Security
Lightship Security, Inc.

Oracle Corporation
World Headquarters
2300 Oracle Way
Austin, TX 78741
U.S.A.
Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com

Oracle is committed to developing practices and products that help protect the environment

Copyright © 2026, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. Oracle specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may reproduced or distributed whole and intact including this copyright notice.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

**Hardware and Software, Engineered to Work Together**

ORACLE

# Table of Contents


**1 General** ..... 1

1.1 Overview ..... 1

1.2 Security Levels ..... 1

1.3 Additional Information ..... 1

**2 Cryptographic Module Specification** ..... 2

2.1 Description ..... 2

2.2 Tested and Vendor Affirmed Module Version and Identification ..... 2

2.3 Excluded Components ..... 2

2.4 Modes of Operation ..... 3

2.5 Algorithms ..... 3

2.6 Security Function Implementations ..... 5

2.7 Algorithm Specific Information ..... 7

2.8 RBG and Entropy ..... 7

2.9 Key Generation ..... 8

2.10 Key Establishment ..... 8

2.11 Industry Protocols ..... 8

**3 Cryptographic Module Interfaces** ..... 9

3.1 Ports and Interfaces ..... 9

**4 Roles, Services, and Authentication** ..... 12

4.1 Authentication Methods ..... 12

4.2 Roles ..... 12

4.3 Approved Services ..... 13

4.4 Non-Approved Services ..... 18

4.5 External Software/Firmware Loaded ..... 18

4.6 Bypass Actions and Status ..... 18

**5 Software/Firmware Security** ..... 19

5.1 Integrity Techniques ..... 19

5.2 Initiate on Demand ..... 19

5.3 Additional Information ..... 19

**6 Operational Environment** ..... 20

6.1 Operational Environment Type and Requirements ..... 20

**7 Physical Security** ..... 21

**8 Non-Invasive Security** ..... 22

**9 Sensitive Security Parameters Management** ..... 23

9.1 Storage Areas ..... 23

9.2 SSP Input-Output Methods ..... 23

9.3 SSP Zeroization Methods ..... 23

9.4 SSPs ..... 23
9.5 Transitions ..... 27
**10 Self-Tests** ..... 28
10.1 Pre-Operational Self-Tests ..... 28
10.2 Conditional Self-Tests ..... 28
10.3 Periodic Self-Test Information ..... 30
10.4 Error States ..... 31
**11 Life-Cycle Assurance** ..... 32
11.1 Installation, Initialization, and Startup Procedures ..... 32
11.2 Administrator Guidance ..... 32
11.3 Non-Administrator Guidance ..... 33
11.4 End of Life ..... 33
**12 Mitigation of Other Attacks** ..... 34

## List of Tables

Table 1: Security Levels ..... 1
Table 2: Tested Module Identification – Hardware ..... 2
Table 3: Modes List and Description ..... 3
Table 4: Approved Algorithms - Oracle Acme Packet Cryptographic Library ..... 4
Table 5: Approved Algorithms - Cavium Octeon II (CN6880) ..... 4
Table 6: Approved Algorithms - Cavium Octeon III (CN7890) ..... 4
Table 7: Approved Algorithms - Cavium Nitrox PX (CN1620) ..... 4
Table 8: Vendor-Affirmed Algorithms ..... 4
Table 9: Security Function Implementations ..... 7
Table 10: Entropy Certificates ..... 8
Table 11: Entropy Sources ..... 8
Table 12: Ports and Interfaces ..... 10
Table 13: Authentication Methods ..... 12
Table 14: Roles ..... 13
Table 15: Approved Services ..... 18
Table 16: Storage Areas ..... 23
Table 17: SSP Input-Output Methods ..... 23
Table 18: SSP Zeroization Methods ..... 23
Table 19: SSP Table 1 ..... 26
Table 20: SSP Table 2 ..... 27
Table 21: Pre-Operational Self-Tests ..... 28
Table 22: Conditional Self-Tests ..... 29
Table 23: Pre-Operational Periodic Information ..... 30
Table 24: Conditional Periodic Information ..... 31
Table 25: Error States ..... 31

## List of Figures

Figure 1: Acme Packet 4600 ..... 2
Figure 2: Acme Packet 6350 ..... 2
Figure 3: Acme Packet 4600 Front View ..... 10

Figure 4: Acme Packet 4600 Rear View ..... 10
Figure 5: Acme Packet 6350 Front View ..... 10
Figure 6: Acme Packet 6350 Rear View ..... 11

# 1 General

## 1.1 Overview

This document is the FIPS 140-3 Non-Proprietary Security Policy for the Acme Packet 4600 and Acme Packet 6350 appliances (running firmware version: S-Cz9.3) manufactured by Oracle Communications, hereafter 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 140-3 Overall Security Level 1. It also describes how the Acme Packet 4600 and Acme Packet 6350 appliances function to meet the FIPS requirements, and the actions that operators must take to maintain the security of the modules.

This Security Policy describes the features and design of the Acme Packet 4600 and Acme Packet 6350 modules using the terminology contained in the FIPS 140-3 specification. FIPS 140-3, 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/CCCS Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-3. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

## 1.2 Security Levels

| Section | Title | Security Level |
|---|---|---|
| 1 | General | 1 |
| 2 | Cryptographic module specification | 1 |
| 3 | Cryptographic module interfaces | 1 |
| 4 | Roles, services, and authentication | 2 |
| 5 | Software/Firmware security | 1 |
| 6 | Operational environment | 1 |
| 7 | Physical security | 1 |
| 8 | Non-invasive security | N/A |
| 9 | Sensitive security parameter management | 1 |
| 10 | Self-tests | 1 |
| 11 | Life-cycle assurance | 1 |
| 12 | Mitigation of other attacks | N/A |
| | Overall Level | 1 |

Table 1: Security Levels

## 1.3 Additional Information

Except for this Non-Proprietary Security Policy, the FIPS 140-3 Validation Documentation is proprietary to Oracle and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Oracle.

# 2 Cryptographic Module Specification

## 2.1 Description

**Purpose and Use:**

The Acme Packet 4600 and Acme Packet 6350 are Enterprise Session Border Controllers. The module is designed to securely manage, control, and protect real-time IP-based communications such as voice, video, and unified communications across trusted and untrusted network boundaries. The module is intended for use in government, enterprise, and carrier-grade environments.

**Module Type**: Hardware

**Module Embodiment**: Multi-Chip Standalone

**Cryptographic Boundary:**

The cryptographic boundary for the Acme Packet 4600 and Acme Packet 6350 is defined as the module case and all components within the case.

A representation of the cryptographic boundary is shown in the Figures below:

Figure 1: Acme Packet 4600

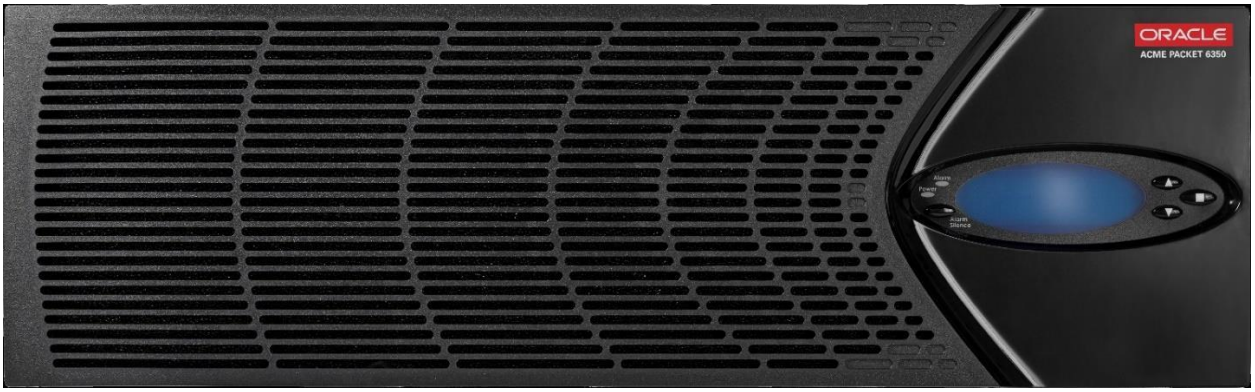


Figure 2: Acme Packet 6350

## 2.2 Tested and Vendor Affirmed Module Version and Identification

**Tested Module Identification – Hardware:**

| Model and/or Part Number | Hardware Version | Firmware Version | Processors | Features |
|---|---|---|---|---|
| Acme Packet 4600 | 4600 | S-Cz9.3 | Intel Core i3-3120ME | |
| Acme Packet 6350 | 6350 | S-Cz9.3 | Intel Xeon D-1548 | |

Table 2: Tested Module Identification – Hardware

## 2.3 Excluded Components

There are no components within the cryptographic boundary that are excluded from the FIPS 140-3 security requirements.

## 2.4 Modes of Operation

**Modes List and Description:**

| Mode Name | Description | Type | Status Indicator |
|---|---|---|---|
| Approved Mode | When installed, initialized and configured as specified in Section 11 of the Security Policy, the module only runs in the approved mode of operation. | Approved | Global |

Table 3: Modes List and Description

## 2.5 Algorithms

**Approved Algorithms:**

Oracle Acme Packet Cryptographic Library

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| AES-CCM | A6582 | Key Length - 128 | SP 800-38C |
| AES-CFB128 | A6582 | Direction - Decrypt, Encrypt<br>Key Length - 128 | SP 800-38A |
| AES-CTR | A6582 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-ECB | A6582 | Direction - Decrypt, Encrypt<br>Key Length - 128, 256 | SP 800-38A |
| AES-GCM | A6582 | Direction - Decrypt, Encrypt<br>IV Generation - Internal<br>IV Generation Mode - 8.2.1<br>Key Length - 128, 256 | SP 800-38D |
| Counter DRBG | A6582 | Prediction Resistance - No<br>Mode - AES-256<br>Derivation Function Enabled - Yes | SP 800-90A Rev. 1 |
| ECDSA KeyGen (FIPS186-5) | A6582 | Curve - P-256, P-384<br>Secret Generation Mode - testing candidates | FIPS 186-5 |
| ECDSA SigGen (FIPS186-5) | A6582 | Curve - P-256, P-384<br>Hash Algorithm - SHA2-256, SHA2-384 | FIPS 186-5 |
| ECDSA SigVer (FIPS186-5) | A6582 | Curve - P-256, P-384<br>Hash Algorithm - SHA2-256, SHA2-384 | FIPS 186-5 |
| HMAC-SHA-1 | A6582 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-256 | A6582 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-384 | A6582 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-512 | A6582 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| KAS-ECC-SSC Sp800-56Ar3 | A6582 | Domain Parameter Generation Methods - P-256, P-384<br>Scheme -<br>ephemeralUnified -<br>KAS Role - initiator, responder | SP 800-56A Rev. 3 |
| KAS-FFC-SSC Sp800-56Ar3 | A6582 | Domain Parameter Generation Methods - ffdhe2048, MODP-2048, MODP-4096, MODP-8192<br>Scheme -<br>dhEphem -<br>KAS Role - initiator, responder | SP 800-56A Rev. 3 |
| KDF SNMP (CVL) | A6582 | Password Length - Password Length: 64-128 Increment 8 | SP 800-135 Rev. 1 |
| KDF SSH (CVL) | A6582 | Cipher - AES-128, AES-192, AES-256<br>Hash Algorithm - SHA-1, SHA2-256 | SP 800-135 Rev. 1 |
| RSA KeyGen (FIPS186-5) | A6582 | Key Generation Mode - probable<br>Modulo - 2048, 3072, 4096 | FIPS 186-5 |

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| | | Primality Tests - 2pow100<br>Private Key Format - standard | |
| RSA SigGen (FIPS186-5) | A6582 | Modulo - 2048, 3072, 4096<br>Signature Type - pkcs1v1.5, pss | FIPS 186-5 |
| RSA SigVer (FIPS186-5) | A6582 | Modulo - 2048, 3072, 4096<br>Signature Type - pkcs1v1.5, pss | FIPS 186-5 |
| Safe Primes Key Generation | A6582 | Safe Prime Groups - ffdhe2048, MODP-2048, MODP-4096, MODP-8192 | SP 800-56A Rev. 3 |
| Safe Primes Key Verification | A6582 | Safe Prime Groups - ffdhe2048, MODP-2048, MODP-4096, MODP-8192 | SP 800-56A Rev. 3 |
| SHA-1 | A6582 | Message Length - Message Length: 8-51200 Increment 8 | FIPS 180-4 |
| SHA2-256 | A6582 | Message Length - Message Length: 8-51200 Increment 8 | FIPS 180-4 |
| SHA2-384 | A6582 | Message Length - Message Length: 8-65536 Increment 8 | FIPS 180-4 |
| SHA2-512 | A6582 | Message Length - Message Length: 8-65536 Increment 8 | FIPS 180-4 |
| TLS v1.2 KDF RFC7627 (CVL) | A6582 | Hash Algorithm - SHA2-256, SHA2-384 | SP 800-135 Rev. 1 |
| TLS v1.3 KDF (CVL) | A6582 | HMAC Algorithm - SHA2-256, SHA2-384<br>KDF Running Modes - DHE | SP 800-135 Rev. 1 |

Table 4: Approved Algorithms - Oracle Acme Packet Cryptographic Library

Cavium Octeon II (CN6880)

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| AES-CTR | A6578 | Direction - Decrypt, Encrypt<br>Key Length - 128 | SP 800-38A |
| HMAC-SHA-1 | A6578 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| KDF SRTP (CVL) | A6578 | AES Key Length - 128 | SP 800-135 Rev. 1 |
| SHA-1 | A6578 | Message Length - Message Length: 8-51200 Increment 8 | FIPS 180-4 |

Table 5: Approved Algorithms - Cavium Octeon II (CN6880)

Cavium Octeon III (CN7890)

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| AES-CTR | A6579 | Direction - Decrypt, Encrypt<br>Key Length - 128 | SP 800-38A |
| HMAC-SHA-1 | A6579 | Key Length - Key Length: 112-524288 Increment 8 | FIPS 198-1 |
| KDF SRTP (CVL) | A6579 | AES Key Length - 128 | SP 800-135 Rev. 1 |
| SHA-1 | A6579 | Message Length - Message Length: 8-51200 Increment 8 | FIPS 180-4 |

Table 6: Approved Algorithms - Cavium Octeon III (CN7890)

Cavium Nitrox PX (CN1620)

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| RSA SigGen (FIPS186-5) | A6577 | Modulo - 2048, 4096<br>Signature Type - pkcs1v1.5 | FIPS 186-5 |
| RSA SigVer (FIPS186-5) | A6577 | Modulo - 2048, 4096<br>Signature Type - pkcs1v1.5 | FIPS 186-5 |

Table 7: Approved Algorithms - Cavium Nitrox PX (CN1620)

**Vendor-Affirmed Algorithms:**

| Name | Properties | Implementation | Reference |
|---|---|---|---|
| CKG | Key Type:Symmetric and Asymmetric | N/A | SP800-133rev2: Section 4, example 1 |

Table 8: Vendor-Affirmed Algorithms

**Non-Approved, Allowed Algorithms:**

N/A for this module.

**Non-Approved, Allowed Algorithms with No Security Claimed:**

N/A for this module.

**Non-Approved, Not Allowed Algorithms:**

N/A for this module.

## 2.6 Security Function Implementations

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| SNMP Encrypt/Decrypt | BC-UnAuth | | | AES-CFB128: (A6582) |
| SNMP Message Authentication | MAC | | | HMAC-SHA2-256: (A6582)<br>HMAC-SHA2-512: (A6582)<br>SHA2-256: (A6582)<br>SHA2-512: (A6582) |
| TLS Encrypt/Decrypt | BC-UnAuth | | | AES-CCM: (A6582)<br>AES-GCM: (A6582) |
| TLS Message Authentication | MAC | | | HMAC-SHA2-256: (A6582)<br>HMAC-SHA2-384: (A6582)<br>SHA2-256: (A6582)<br>SHA2-384: (A6582) |
| SRTP Encrypt/Decrypt 1 | BC-UnAuth | | | AES-CTR: (A6578) |
| SRTP Encrypt/Decrypt 2 | BC-UnAuth | | | AES-CTR: (A6579) |
| SRTP Message Authentication 1 | MAC | | | HMAC-SHA-1: (A6578)<br>MAC: 80<br>SHA-1: (A6578) |
| SRTP Message Authentication 2 | MAC | | | HMAC-SHA-1: (A6579)<br>MAC: 80<br>SHA-1: (A6579) |
| SSH Encrypt/Decrypt | BC-Auth<br>BC-UnAuth | | | AES-CTR: (A6582)<br>AES-GCM: (A6582) |
| SSH Message Authentication | MAC | | | HMAC-SHA-1: (A6582)<br>MAC: 96, 160<br>HMAC-SHA2-256: (A6582)<br>SHA-1: (A6582)<br>SHA2-256: (A6582) |
| SSH Key Transport 1 | KTS-Wrap | | IG D.G:Approved Bullet 2 / Bit Strength: Provides 128 or 256 bits of encryption strength | AES-GCM: (A6582) |
| SSH Key Transport 2 | KTS-Wrap | | IG D.G:Approved Bullet 2 / Bit Strength: Provides between 128 and 256 bits of encryption strength | AES-CTR: (A6582)<br>HMAC-SHA-1: (A6582)<br>HMAC-SHA2-256: (A6582) |
| TLS Key Transport | KTS-Wrap | | IG D.G:Approved Bullet 2 / Bit Strength: Provides 128 or 256 bits of encryption strength | AES-GCM: (A6582) |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| DRBG | DRBG | | | Counter DRBG: (A6582)<br>AES-ECB: (A6582) |
| TLS Key Pair Generation | AsymKeyPair-KeyGen | | | ECDSA KeyGen (FIPS186-5): (A6582)<br>RSA KeyGen (FIPS186-5): (A6582)<br>Modulo: 2048, 4096 |
| TLS Digital Signature Generation | DigSig-SigGen | | | ECDSA SigGen (FIPS186-5): (A6582)<br>RSA SigGen (FIPS186-5): (A6582)<br>Signature Type: pss<br>Modulo: 2048, 4096<br>RSA SigGen (FIPS186-5): (A6577) |
| TLS Digital Signature Verification | DigSig-SigVer | | | ECDSA SigVer (FIPS186-5): (A6582)<br>RSA SigVer (FIPS186-5): (A6582)<br>Signature Type: pss<br>Modulo: 2048, 4096<br>RSA SigVer (FIPS186-5): (A6577) |
| Bypass Integrity Check | MAC | | | HMAC-SHA2-256: (A6582)<br>SHA2-256: (A6582) |
| TLS KAS 1 | KAS-Full | | IG D.F :Scenario 2 Path 2/ Bit Strength: Provides 128 or 192 bits of encryption strength | KAS-ECC-SSC Sp800-56Ar3: (A6582)<br>TLS v1.2 KDF RFC7627: (A6582)<br>TLS v1.3 KDF: (A6582) |
| TLS KAS 2 | KAS-Full | | IG D.F:Scenario 2 Path 2/ Bit Strength: Provides 112 bits of encryption strength | KAS-FFC-SSC Sp800-56Ar3: (A6582)<br>Domain Parameter Generation Methods: ffdhe2048<br>TLS v1.2 KDF RFC7627: (A6582)<br>TLS v1.3 KDF: (A6582) |
| SSH KAS | KAS-Full | | IG D.F:Scenario 2 Path 2/ Bit Strength: Provides between 112 and 200 bits of encryption strength | KAS-FFC-SSC Sp800-56Ar3: (A6582)<br>Domain Parameter Generation Methods: MODP-2048, MODP-4096, MODP-8192<br>KDF SSH: (A6582) |
| SNMP KDF | KAS-135KDF | | | KDF SNMP: (A6582) |
| SRTP KDF 1 | KAS-135KDF | | | KDF SRTP: (A6578) |
| SRTP KDF 2 | KAS-135KDF | | | KDF SRTP: (A6579) |
| SSH KDF | KAS-135KDF | | | KDF SSH: (A6582) |
| SSH Key Pair Generation | AsymKeyPair-KeyGen | | | RSA KeyGen (FIPS186-5): (A6582) |
| SSH Signature Generation | DigSig-SigGen | | | RSA SigGen (FIPS186-5): (A6582)<br>Signature type: pkcs1v1.5 |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| SSH Signature Verification | DigSig-SigVer | | | RSA SigVer (FIPS186-5): (A6582)<br>Signature type: pkcs1v1.5 |
| TLS KDF | KAS-135KDF | | | TLS v1.2 KDF RFC7627: (A6582)<br>TLS v1.3 KDF: (A6582) |
| Verify Firmware Integrity | DigSig-SigVer | | | RSA SigVer (FIPS186-5): (A6582)<br>Signature Type: pss<br>Modulus: 2048<br>Hash: SHA2-256 |
| Entropy Source | ENT-ESV | | | |
| KAS ECDSA KeyGen | AsymKeyPair-KeyGen | | | ECDSA KeyGen (FIPS186-5): (A6582) |
| KAS SafePrimes KeyGen | AsymKeyPair-KeyGen | | | Safe Primes Key Generation: (A6582)<br>Safe Primes Key Verification: (A6582) |
| Generate Symmetric Key | CKG | | | CKG: () |
| Password Hash/Verify | SHA | | | SHA2-512: (A6582) |

Table 9: Security Function Implementations

## 2.7 Algorithm Specific Information

The module's TLS v1.2 firmware AES-GCM implementation conforms to FIPS 140-3 IG C.H Scenario #1. The module is compatible with TLS v1.2 and provides support for acceptable GCM ciphersuites from SP 800-52 Rev2, Section 3.3.1. The counter portion of the IV is set by the module within its cryptographic boundary. The nonce_explicit management logic inside the module ensures that when the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key (in accordance with 7.4.1.1 and 7.4.1.2 RFC 5246). In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

The module's TLS v1.3 firmware AES-GCM implementation conforms to FIPS 140-3 IG C.H Scenario #1. The module is compatible with TLS v1.3 and provides support for acceptable GCM ciphersuites from SP 800-52 Rev2, Section 3.3.1. The counter portion of the IV is set by the module within its cryptographic boundary. The sequence number, and the client_write_iv or server_write_iv value (depending on role) are used to construct the per-record nonce, following the procedure in Section 5.3 of RFC 8446. Furthermore, as required by Section 5.3 of RFC 8446, the module ensures that when the sequence number would wrap, the first party, client or server, to encounter this condition rekeys (in accordance with Section 4.6.3 in RFC 8446) or terminates the connection. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

The module's SSHv2 firmware AES-GCM implementation conforms to FIPS 140-3 IG C.H Scenario #1. The IV generation is in compliance with the SSHv2 specification and only for use within the SSHv2 protocol, following the specifications defined in RFCs 4252, 4253 and 5647. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

The module's SRTP firmware AES-GCM implementation conforms to FIPS 140-3 IG C.H Scenario #5. The IV is generated and used within this SRTP protocol's implementation. The SRTP protocol and, specifically, the use of the AES-GCM encryption within the protocol are defined in RFC 7714.

## 2.8 RBG and Entropy

| Cert Number | Vendor Name |
|---|---|
| E235 | Oracle Corporation |

Table 10: Entropy Certificates

| Name | Type | Operational Environment | Sample Size | Entropy per Sample | Conditioning Component |
|---|---|---|---|---|---|
| Kernel CPU Time Jitter RNG Entropy Source | Non-Physical | Intel Core i3-3120ME Intel Xeon D-1548 | 64 bits | 59.119 | |

Table 11: Entropy Sources

The module employs a Deterministic Random Bit Generator (DRBG) based on [SP800-90Arev1] for random number generation. The DRBG used for the module is CTR_DRBG. The module performs the DRBG health tests as defined in Section 11.3 of [SP800-90Arev1]. The module uses an [SP 800-90B] compliant entropy source for seeding the DRBG.

## 2.9 Key Generation

Please see SFI Table entries for the following: TLS Key Pair Generation, SNMP KDF, SRTP KDF 1, SRTP KDF 2, SSH KDF, SSH Key Pair Generation, TLS KDF, KAS ECDSA KeyGen, KAS SafePrimes KeyGen, Generate Symmetric Key.

When the module generates symmetric keys or seeds used for generating asymmetric keys, unmodified DRBG output is used as the symmetric key or as the seed for generating the asymmetric keys.

## 2.10 Key Establishment

Key Agreement:

Please see SFI Table entries for the following: TLS KAS 1, TLS KAS 2, SSH KAS.

Key Transport:

Please see SFI Table entries for the following: SSH Key Transport 1, SSH Key Transport 2, TLS Key Transport.

## 2.11 Industry Protocols

No parts of the SSH, TLS, SNMP or SRTP protocols, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

# 3 Cryptographic Module Interfaces

## 3.1 Ports and Interfaces

| Physical Port | Logical Interface(s) | Data That Passes |
|---|---|---|
| Acme Packet 4600 USB Port | Control Input | The USB port is reserved for recovery only by Oracle, for a non-bootable system. |
| Acme Packet 4600 Console Port | Data Input<br>Control Input<br>Status Output | Provides console access to the module. The module supports only one active serial console connection at a time |
| Acme Packet 4600 Ethernet MGT (Mgmt0, Mgmt1, Mgmt2) Ports | Data Input<br>Data Output<br>Control Input<br>Status Output | Used for EMS control, CDR accounting, CLI management, and other management functions. High Availability (HA), use ports 1 and 2 |
| Acme Packet 4600 Signaling and Media (P0, P1, P2, P3) Ports | Data Input<br>Data Output | Provide network connectivity for signaling and media traffic. These ports are also used for incoming and outgoing data (voice) connections |
| Acme Packet 4600 Signaling and Media (P4, P5) Port | Data Input<br>Data Output | Provide network connectivity for signaling and media traffic. These ports are also used for incoming and outgoing data (voice) connections |
| Acme Packet 4600 LEDs | Status Output | Status information output from the module |
| Acme Packet 4600 Alarm Port | Status Output | Provides status output |
| Acme Packet 4600 LCD | Status Output | Provides status output |
| Acme Packet 4600 Power Switch | Control Input | Powers on the platform |
| Acme Packet 4600 Reset Button | Control Input | Provides reset functionality |
| Acme Packet 4600 Power Port | Power | Provides the power supply to the module |
| Acme Packet 6350 USB Port | Control Input | The USB port is reserved for recovery only by Oracle, for a non-bootable system. |
| Acme Packet 6350 Console Port | Data Input<br>Control Input<br>Status Output | Provides console access to the module. The module supports only one active serial console connection at a time |
| Acme Packet 6350 Ethernet MGT (Mgmt0, Mgmt1, Mgmt2) Ports | Data Input<br>Data Output<br>Control Input<br>Status Output | Used for EMS control, CDR accounting, CLI management, and other management functions. High Availability (HA), use ports 1 and 2 |
| Acme Packet 6350 Signaling and Media (P0, P1, P2, P3) Ports | Data Input<br>Data Output | Provide network connectivity for signaling and media traffic. These ports are also used for incoming and outgoing data (voice) connections |
| Acme Packet 6350 LEDs | Status Output | Status information output from the module |
| Acme Packet 6350 Alarm Port | Status Output | Provides status output |
| Acme Packet 6350 LCD | Status Output | Provides status output |
| Acme Packet 6350 Power Switch | Control Input | Powers on the platform |

| Physical Port | Logical Interface(s) | Data That Passes |
|---|---|---|
| Acme Packet 6350 Reset Button | Control Input | Provides reset functionality |
| Acme Packet 6350 Power Ports | Power | Provides the power supply to the module |

Table 12: Ports and Interfaces

The module does not support a Control Output interface. All data output via the data output interface is inhibited whenever the cryptographic module is performing pre-operational self-tests, zeroization, and when the module is in an error state.

Figure 3: Acme Packet 4600 Front View

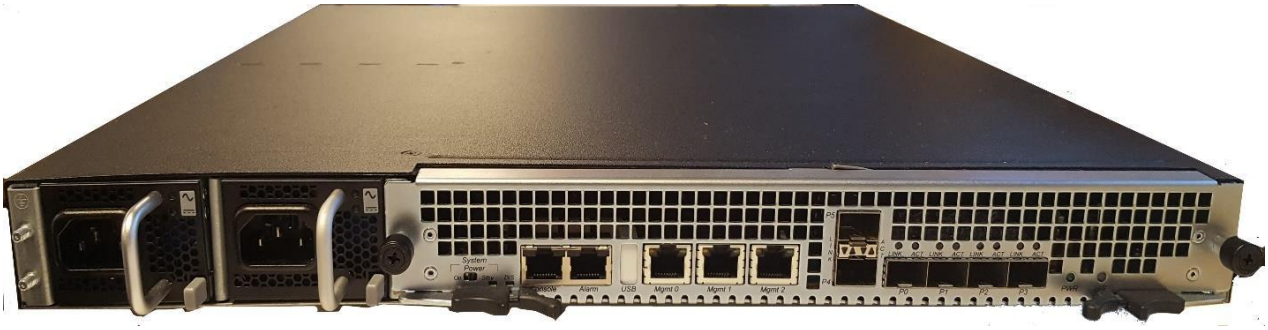

Figure 4: Acme Packet 4600 Rear View

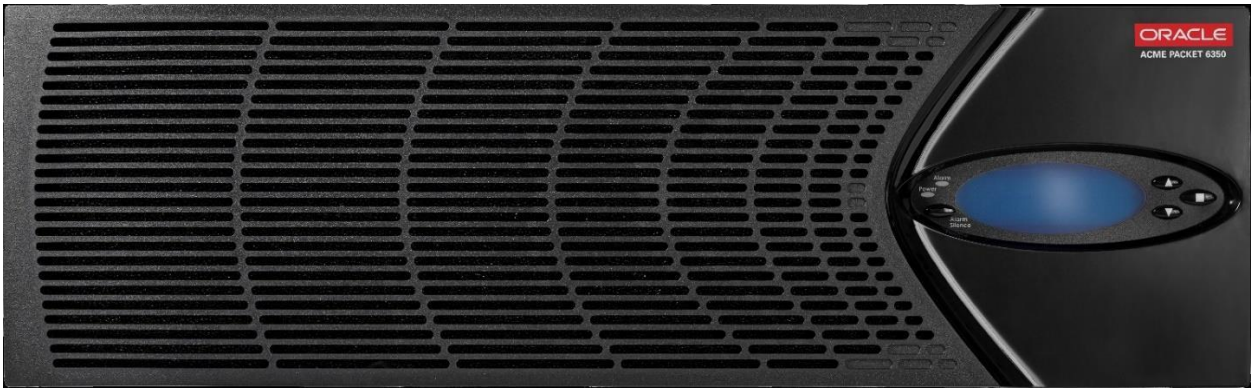


Figure 5: Acme Packet 6350 Front View

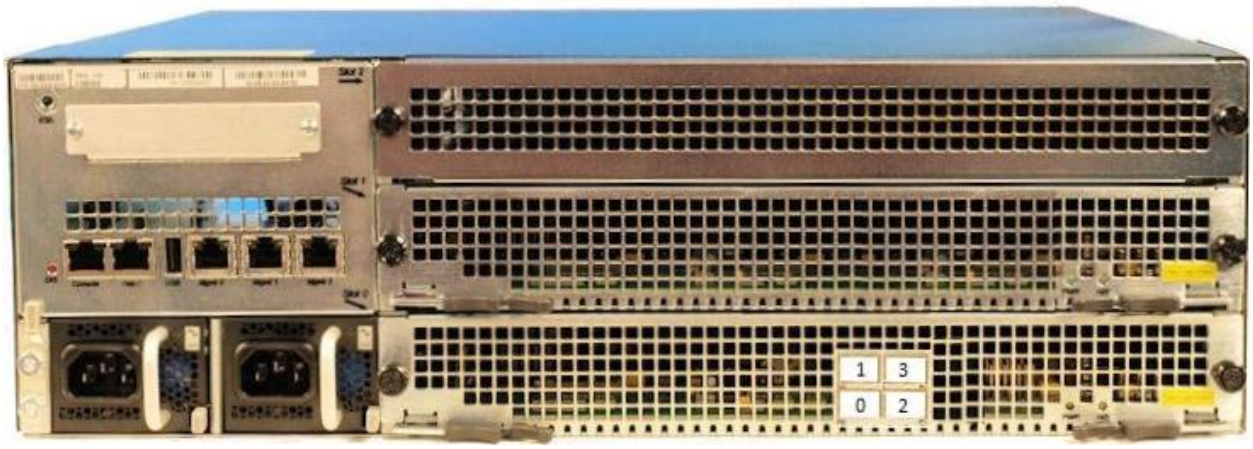

Figure 6: Acme Packet 6350 Rear View

# 4 Roles, Services, and Authentication

## 4.1 Authentication Methods

| Method Name | Description | Security Mechanism | Strength Each Attempt | Strength per Minute |
|---|---|---|---|---|
| Console Auth | | Username and Password | Passwords must be a minimum of 8 characters. The password can consist of alphanumeric values, [a-z, A-Z, 0-9, and special characters], yielding 94 choices per character. The probability of a successful random attempt is 1/94^8, which is less than 1/1,000,000. | Passwords must be a minimum of 8 characters. The password can consist of alphanumeric values, [a-z, A-Z, 0-9, and special characters], yielding 94 choices per character. Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple attempts in a one-minute period is 600/94^8, which is less than 1/100,000. |
| SSH Auth 1 | | Username and Password | Passwords must be a minimum of 8 characters. The password can consist of alphanumeric values, [a-z, A-Z, 0-9, and special characters], yielding 94 choices per character. The probability of a successful random attempt is 1/94^8, which is less than 1/1,000,000. | Passwords must be a minimum of 8 characters. The password can consist of alphanumeric values, [a-z, A-Z, 0-9, and special characters], yielding 94 choices per character. Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple attempts in a one-minute period is 600/94^8, which is less than 1/100,000. |
| SSH Auth 2 | | RSA SigVer (FIPS186-5) (A6582) | A 2048-bit RSA has at least 112-bits of equivalent strength. The probability of a successful random attempt is 1 /2^112, which is less than 1/1,000,000. | Assuming the module can support 60 authentication attempts in one minute, the probability of a success with multiple consecutive attempts in a one-minute period is 60/2^112, which is less than 1/100,000. |
| WebGUI Auth | | Username and Password | Passwords must be a minimum of 8 characters. The password can consist of alphanumeric values, [a-z, A-Z, 0-9, and special characters], yielding 94 choices per character. The probability of a successful random attempt is 1/94^8, which is less than 1/1,000,000. | Passwords must be a minimum of 8 characters. The password can consist of alphanumeric values, [a-z, A-Z, 0-9, and special characters], yielding 94 choices per character. Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple attempts in a one-minute period is 600/94^8, which is less than 1/100,000. |
| SNMP Auth | | Username and Password | Passwords must be a minimum of 8 characters. The password can consist of alphanumeric values, [a-z, A-Z, 0-9, and special characters], yielding 94 choices per character. The probability of a successful random attempt is 1/94^8, which is less than 1/1,000,000. | Passwords must be a minimum of 8 characters. The password can consist of alphanumeric values, [a-z, A-Z, 0-9, and special characters], yielding 94 choices per character. Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple attempts in a one-minute period is 600/94^8, which is less than 1/100,000. |

Table 13: Authentication Methods

## 4.2 Roles

| Name | Type | Operator Type | Authentication Methods |
|---|---|---|---|
| Crypto-Officer | Role | CO | Console Auth<br>SSH Auth 1<br>SSH Auth 2<br>WebGUI Auth<br>SNMP Auth |
| User | Role | User | Console Auth<br>SSH Auth 1<br>SSH Auth 2 |

| Name | Type | Operator Type | Authentication Methods |
|---|---|---|---|
| | | | WebGUI Auth<br>SNMP Auth |

Table 14: Roles

## 4.3 Approved Services

The abbreviations of the access rights to SSPs have the following interpretation:

**G = Generate:** The module generates or derives the SSP.

**R = Read:** The SSP is read from the module (e.g., the SSP is output).

**W = Write:** The SSP is updated, imported, or written to the module.

**E = Execute:** The module uses the SSP in performing a cryptographic operation.

**Z = Zeroise:** The module zeroises the SSP.

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Initialization | Initializes the module for Approved Mode of Operation. | N/A | Command and parameters | Command response/ Status output | | Crypto-Officer |
| Configure System Settings | Configure approved system parameters and operational settings | N/A | Command and parameters | Command response/Status output | | Crypto-Officer |
| Show Module's Versioning Information | Outputs the module name/identifier and the versioning information that can be correlated with the validation record. | N/A | Command | Module Versioning information | | Crypto-Officer<br>User |
| View Alarms | View system alarms | N/A | Command | Alarm information | | Crypto-Officer<br>User |
| View Performance | View system performance metrics | N/A | Command | Performance information | | Crypto-Officer<br>User |
| Manage Users | Create, edit, or delete user accounts | N/A | Command and parameters | Command response/Status output | | Crypto-Officer |
| Change Password | Change authentication credentials | Global and successful completion of service | Command and parameters | Command response/Status output | Password Hash/Verify | Crypto-Officer<br>- Operator Passwords: W<br>- Operator RSA public key: W |
| Authenticate | Authenticates users | Global and successful completion of service | Authentication data | Status output | Password Hash/Verify | Crypto-Officer<br>- Operator Passwords: W<br>- Operator RSA public key: W<br>User<br>- Operator Passwords: W<br>- Operator RSA public key: W |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Show Status | Outputs current status of the module. | N/A | Command | Command response/Status output | | Crypto-Officer<br>User |
| Certificates | Management and viewing of X.509 certificates | Global and successful completion of service | Command and parameters | Command response/Status output | | Crypto-Officer<br>- Web UI Certificate: R<br>User<br>- Web UI Certificate: R |
| Bypass | Configure bypass using TCP or UDP and viewing bypass service status | Global and successful completion of service | Command and parameters | Command response/Status output | Bypass Integrity Check | Crypto-Officer<br>- Bypass Key: G,E |
| SSH | Establish secure session | Global and successful completion of service | Command | Session establishment | SSH Encrypt/Decrypt SSH Message Authentication SSH Key Transport 1 SSH Key Transport 2 SSH KAS SSH KDF SSH Key Pair Generation SSH Signature Generation SSH Signature Verification KAS SafePrimes KeyGen | Crypto-Officer<br>- Diffie-Hellman Public Key: G,R,W,E<br>- Diffie-Hellman Private Key: G,E<br>- Diffie-Hellman Shared Secret: G,E<br>- SSH Authentication Public Key: G,R,E<br>- SSH Authentication Private Key: G,E<br>- SSH Session Keys: G,E<br>- SSH Integrity Keys: G,E<br>User<br>- Diffie-Hellman Public Key: G,R,W,E<br>- Diffie-Hellman Private Key: G,E<br>- Diffie-Hellman Shared Secret: G,E<br>- SSH Authentication Public Key: G,R,E<br>- SSH Authentication Private Key: G,E<br>- SSH Session Keys: G,E<br>- SSH Integrity Keys: G,E |
| TLS | Establish secure session | Global and successful | Command | Session establishment | TLS Encrypt/Decrypt TLS Message | Crypto-Officer<br>- Diffie-Hellman Public Key: |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | completion of service | | | Authentication<br>TLS Key Transport<br>TLS Key Pair Generation<br>TLS Digital Signature Generation<br>TLS Digital Signature Verification<br>TLS KAS 1<br>TLS KAS 2<br>TLS KDF<br>KAS ECDSA KeyGen<br>KAS SafePrimes KeyGen | G,R,W,E<br>- Diffie-Hellman Private Key: G,E<br>- Diffie-Hellman Shared Secret: G,E<br>- ECDH Public Key: G,R,W,E<br>- ECDH Private Key: G,E<br>- ECDH Shared Secret: G,E<br>- TLS Authentication Public Key: G,R,E<br>- TLS Authentication Private Key: G,E<br>- TLS Premaster Secret: G,E<br>- TLS Master Secret: G,E<br>- TLS Session Keys: G,E<br>- TLS Integrity Keys: G,E<br>User<br>- Diffie-Hellman Public Key: G,R,W,E<br>- Diffie-Hellman Private Key: G,E<br>- Diffie-Hellman Shared Secret: G,E<br>- ECDH Public Key: G,R,W,E<br>- ECDH Private Key: G,E<br>- ECDH Shared Secret: G,E<br>- TLS Authentication Public Key: G,R,E<br>- TLS Authentication Private Key: G,E<br>- TLS Premaster Secret: G,E<br>- TLS Master Secret: G,E<br>- TLS Session Keys: G,E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - TLS Integrity Keys: G,E |
| SRTP | Establish secure session | Global and successful completion of service | Command and parameters | Session establishment | SRTP Encrypt/Decrypt 1<br>SRTP Encrypt/Decrypt 2<br>SRTP Message Authentication 1<br>SRTP Message Authentication 2<br>SRTP KDF 1<br>SRTP KDF 2<br>Generate Symmetric Key | Crypto-Officer<br>- SRTP Master Key: G,W,E<br>- SRTP Session Key: G,E<br>- SRTP Authentication Key: G,E<br>User<br>- SRTP Master Key: G,W,E<br>- SRTP Session Key: G,E<br>- SRTP Authentication Key: G,E |
| SNMP | Secure network management | Global and successful completion of service | Command and parameters | Session establishment | SNMP Encrypt/Decrypt<br>SNMP Message Authentication<br>SNMP KDF | Crypto-Officer<br>- SNMPv3 Passwords (Privacy and Auth): W,E<br>- SNMP Privacy Key: G,E<br>- SNMP Authentication Key: G,E<br>User<br>- SNMPv3 Passwords (Privacy and Auth): W,E<br>- SNMP Privacy Key: G,E<br>- SNMP Authentication Key: G,E |
| On-Demand Self-tests | Initiates and runs the pre-operational self-tests. | N/A | Command | Command response/ Status output | Verify Firmware Integrity | Crypto-Officer<br>- Firmware Integrity Key: E |
| Zeroisation | Zeroises unprotected SSPs and key components. | Status | Command | Command response/ Status output | | Crypto-Officer<br>- Operator Passwords: Z<br>- Operator RSA public key: Z<br>- Firmware Integrity Key: Z<br>- DRBG Entropy Input String and Nonce: Z<br>- DRBG Seed: Z<br>- DRBG Internal State (V, Key): Z<br>- Diffie-Hellman Public Key: Z |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - Diffie-Hellman Private Key: Z<br>- Diffie-Hellman Shared Secret: Z<br>- ECDH Public Key: Z<br>- ECDH Private Key: Z<br>- ECDH Shared Secret: Z<br>- SNMPv3 Passwords (Privacy and Auth): Z<br>- SNMP Privacy Key: Z<br>- SNMP Authentication Key: Z<br>- SRTP Master Key: Z<br>- SRTP Session Key: Z<br>- SRTP Authentication Key: Z<br>- SSH Authentication Public Key: Z<br>- SSH Authentication Private Key: Z<br>- SSH Session Keys: Z<br>- SSH Integrity Keys: Z<br>- TLS Authentication Public Key: Z<br>- TLS Authentication Private Key: Z<br>- TLS Premaster Secret: Z<br>- TLS Master Secret: Z<br>- TLS Session Keys: Z<br>- TLS Integrity Keys: Z<br>- Web UI Certificate: Z<br>- Bypass Key: Z |
| Random Number Generation | Random Number Generation | Global and successful | Command | Command response/ Status output | DRBG Entropy Source | Crypto-Officer<br>- DRBG Entropy Input String and |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | completion of service | | | | Nonce: G,E<br>- DRBG Seed: G,E<br>- DRBG Internal State (V, Key): G,E<br>User<br>- DRBG Entropy Input String and Nonce: G,E<br>- DRBG Seed: G,E<br>- DRBG Internal State (V, Key): G,E |

Table 15: Approved Services

## 4.4 Non-Approved Services

N/A for this module.

## 4.5 External Software/Firmware Loaded

Not Applicable. The module does not support the capability of loading software of firmware from an external source.

## 4.6 Bypass Actions and Status

First, the Crypto-Officer must modify the SRTP configuration in order to enable the bypass capability for a specific SRTP profile. Then after the bypass settings for each SRTP profile have been set, the configuration must be saved. The module will prompt the operator to confirm the changes before committing them to the configuration. Status can be checked through configuration (show running-config media-sec-policy).

# 5 Software/Firmware Security

## 5.1 Integrity Techniques

The module performs a firmware integrity test over the entire firmware image using RSA 2048/SHA 256 signature verification.

## 5.2 Initiate on Demand

The integrity test can be invoked on demand by power cycling the module.

## 5.3 Additional Information

The temporary values generated during the module's integrity test are zeroised upon completion of the integrity test.

# 6 Operational Environment

## 6.1 Operational Environment Type and Requirements

**Type of Operational Environment**: Non-Modifiable

**How Requirements are Satisfied**:

The non-modifiable operational environment of the module prevents users from accessing SSPs which they are not authorized to access. There is no logical or physical access to the SSPs. The operating system provides process isolation and memory protection mechanisms that ensure appropriate separation for memory access among the processes on the system. Each process has control over its own data and uncontrolled access to the data of other processes is prevented.

As per ISO/IEC 19790:2012 7.6.3:

• The cryptographic module has control over its own SSPs.

• The operational environment provides the capability to separate individual application processes from each other to prevent uncontrolled access to CSPs and uncontrolled modifications of SSPs, regardless if this data is in the process memory or stored on persistent storage within the operational environment. This ensures that direct access to SSPs is restricted to the cryptographic module and the trusted parts of the operational environment.

• Processes that are spawned by the cryptographic module are owned by the module and are not owned by external processes/operators.

# 7 Physical Security

The module has a multi-chip standalone embodiment and is made of commercially available, production grade components meeting commercial specifications for power, temperature, reliability, shock and vibration. All production-grade components include standard passivation techniques, in the form of a coating applied over the module's circuitry to protect against environmental and other physical damage. The module is entirely contained within a production grade metal enclosure.

# 8 Non-Invasive Security

Currently, the ISO/IEC 19790:2012 non-invasive security area is not required by FIPS 140-3 (see NIST SP 800-140F). The requirements of this area are not applicable to the module.

# 9 Sensitive Security Parameters Management

## 9.1 Storage Areas

| Storage Area Name | Description | Persistence Type |
|---|---|---|
| Flash | Non-volatile memory | Static |
| VRAM | Volatile memory | Dynamic |

Table 16: Storage Areas

## 9.2 SSP Input-Output Methods

| Name | From | To | Format Type | Distribution Type | Entry Type | SFI or Algorithm |
|---|---|---|---|---|---|---|
| SSP Input 1 | External via SSH or TLS management session | Flash | Encrypted | Automated | Electronic | |
| SSP Input 2 | External via console | Flash | Plaintext | Manual | Electronic | |
| SSP Input 3 (Peer) | External | VRAM | Plaintext | Automated | Electronic | |
| SSP Output 1 | Flash | External via HA | Plaintext | Manual | Electronic | |
| SSP Output 2 | VRAM | External | Plaintext | Automated | Electronic | |
| SSP Output 3 | Flash | External | Plaintext | Automated | Electronic | |

Table 17: SSP Input-Output Methods

## 9.3 SSP Zeroization Methods

| Zeroization Method | Description | Rationale | Operator Initiation |
|---|---|---|---|
| Session Termination | Automatic zeroization upon session termination | Upon session termination, all respective SSPs stored in volatile memory are actively zeroized. | Operator closes protocol session |
| Power Cycle | Automatic zeroization upon power cycle | Upon power cycle, all SSPs stored in volatile memory are actively zeroized. | Operator power cycles the module |
| After Use | Automatic zeroization upon use | Upon crypto operation, all respective SSPs stored in volatile memory are actively zeroized. | |
| Factory Reset | Restores the module to factory defaults | Upon factory reset command, all SSPs stored in memory are actively zeroised by overwriting the memory locations with zeros. | Operator enters Factory Reset command |

Table 18: SSP Zeroization Methods

## 9.4 SSPs

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| Operator Passwords | Used for authentication of the crypto officer and user | 8-64 characters - Please see Authentication Methods table for details. | Authentication - CSP | | | |
| Operator RSA public key | Used for public key authentication of the crypto officer and user via SSH management session. | 2048 bits, 4096 bits - 112 bits, 152 bits | Authentication - CSP | | | |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| Firmware Integrity Key | Public key used to verify the integrity of firmware. | 2048 bits - 112 bits | Public Key - Neither | Factory Installed | | Verify Firmware Integrity |
| DRBG Entropy Input String and Nonce | Used in the random bit generation process | 384 bits - | Entropy - CSP | Entropy Source | | DRBG |
| DRBG Seed | Used in the random bit generation process | 384 bits - | Seed - CSP | DRBG | | DRBG |
| DRBG Internal State (V, Key) | Used in the random bit generation process (CTR DRBG) | V:16 bytes Key: 32 bytes - | Internal State - CSP | DRBG | | DRBG |
| Diffie-Hellman Public Key | Used as part of DH key agreement protocol | SSH: 2048 bits, 4096 bits, 8192 bits. / TLS1.2&3: 2048 bits. - SSH: 112 bits, 152 bits, 200 bits. / TLS1.2&3: 112 bits. | Public - PSP | KAS SafePrimes KeyGen | | TLS KAS 2<br>SSH KAS |
| Diffie-Hellman Private Key | Used as part of DH key agreement protocol | SSH: 2048 bits, 4096 bits, 8192 bits. / TLS1.2&3: 2048 bits. - SSH: 112 bits, 152 bits, 200 bits. / TLS1.2&3: 112 bits. | Private - CSP | KAS SafePrimes KeyGen | | TLS KAS 2<br>SSH KAS |
| Diffie-Hellman Shared Secret | Used as part of DH key agreement protocol | SSH: 2048 bits, 4096 bits, 8192 bits. / TLS1.2&3: 2048 bits. - SSH: 112 bits, 152 bits, 200 bits. / TLS1.2&3: 112 bits. | Shared Secret - CSP | | TLS KAS 2<br>SSH KAS | TLS KAS 2<br>SSH KAS |
| ECDH Public Key | Used as part of ECDH key agreement protocol | TLS1.2&3: P-256, P-384 - TLS1.2&3: 128 bits, 192 bits | Public - PSP | KAS ECDSA KeyGen | | TLS KAS 1 |
| ECDH Private Key | Used as part of ECDH key agreement protocol | TLS1.2&3: P-256, P-384 - TLS1.2&3: 128 bits, 192 bits | Private - CSP | KAS ECDSA KeyGen | | TLS KAS 1 |
| ECDH Shared Secret | Used as part of ECDH key agreement protocol | TLS1.2&3: P-256, P-384 - TLS1.2&3: 128 bits, 192 bits | Shared Secret - CSP | | TLS KAS 1 | TLS KAS 1 |
| SNMPv3 Passwords (Privacy and Auth) | Used in the derivation of SNMP keys | 8-64 characters - Please see Authentication Methods table for details. | Authentication string - CSP | | | SNMP KDF |
| SNMP Privacy Key | Used for encryption / decryption of SNMP session traffic | 128 bits - 128 bits | Symmetric - CSP | SNMP KDF | | SNMP Encrypt/Decrypt |
| SNMP Authentication Key | Used for message authentication and verification in SNMP | 256 bits, 512 bits - 256 bits, 512 bits | Symmetric - CSP | SNMP KDF | | SNMP Message Authentication |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| SRTP Master Key | Used in the derivation of SRTP session keys | 128 bits - 128 bits | Symmetric - CSP | Generate Symmetric Key | | SRTP KDF 1<br>SRTP KDF 2 |
| SRTP Session Key | Used for encryption / decryption of SRTP session traffic | 128 bits - 128 bits | Symmetric - CSP | SRTP KDF 1<br>SRTP KDF 2 | | SRTP Encrypt/Decrypt 1<br>SRTP Encrypt/Decrypt 2 |
| SRTP Authentication Key | Used for message authentication and verification in SRTP | 160 bits - 160 bits | Symmetric - CSP | SRTP KDF 1<br>SRTP KDF 2 | | SRTP Message Authentication 1<br>SRTP Message Authentication 2 |
| SSH Authentication Public Key | Used for SSH host/server authentication | 2048 bits, 3072 bits, 4096 bits - 112 bits, 128 bits, 152 bits | Public - PSP | SSH Key Pair Generation | | SSH Signature Verification |
| SSH Authentication Private Key | Used for SSH host/server authentication | 2048 bits, 3072 bits, 4096 bits - 112 bits, 128 bits, 152 bits | Private - CSP | SSH Key Pair Generation | | SSH Signature Generation |
| SSH Session Keys | Used for encryption/decryption of SSH session traffic | 128 bits, 192 bits, 256 bits - 128 bits, 192 bits, 256 bits | Symmetric - CSP | SSH KDF | | SSH Encrypt/Decrypt |
| SSH Integrity Keys | Used for message authentication and verification in SSH | 160 bits, 256 bits - 160 bits, 256 bits | Symmetric - CSP | SSH KDF | | SSH Message Authentication |
| TLS Authentication Public Key | Used for TLS host/server authentication | P-256, P-384, 2048 bits, 4096 bits - 128 bits, 192 bits, 112 bits, 152 bits | Public - PSP | TLS Key Pair Generation | | TLS Digital Signature Verification |
| TLS Authentication Private Key | Used for TLS host/server authentication | P-256, P-384, 2048 bits, 4096 bits - 128 bits, 192 bits, 112 bits, 152 bits | Private - CSP | TLS Key Pair Generation | | TLS Digital Signature Generation |
| TLS Premaster Secret | Used during the TLS handshake | 384 bits - | Secret - CSP | | TLS KAS 1<br>TLS KAS 2 | TLS KDF |
| TLS Master Secret | Used for computing the TLS keys | 384 bits - | Secret - CSP | TLS KDF | | TLS KDF |
| TLS Session Keys | Used for encryption/decryption of TLS session traffic | 128 bits, 256 bits - 128 bits, 256 bits | Symmetric - CSP | TLS KDF | | TLS Encrypt/Decrypt |
| TLS Integrity Keys | Used for message authentication and verification in TLS | 256 bits, 384 bits - 256 bits, 384 bits | Symmetric - CSP | TLS KDF | | TLS Message Authentication |
| Web UI Certificate | Used for secure, authenticated management connections | 2048 bits, 4096 bits - 112 bits, 152 bits | Certificate - CSP | | | |
| Bypass Key | Used to protect bypass table | 256 bits - 256 bits | Symmetric - CSP | Generate Symmetric Key | | Bypass Integrity Check |

Table 19: SSP Table 1

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| Operator Passwords | SSP Input 1<br>SSP Input 2<br>SSP Output 1 | Flash:Obfuscated | | Factory Reset | |
| Operator RSA public key | SSP Input 1 | Flash:Plaintext | | Factory Reset | |
| Firmware Integrity Key | | Flash:Plaintext | | Factory Reset | |
| DRBG Entropy Input String and Nonce | | VRAM:Plaintext | | Power Cycle | |
| DRBG Seed | | VRAM:Plaintext | | Power Cycle | DRBG Entropy Input String and Nonce:Derived From |
| DRBG Internal State (V, Key) | | VRAM:Plaintext | | Power Cycle | DRBG Seed:Derived From |
| Diffie-Hellman Public Key | SSP Input 3 (Peer)<br>SSP Output 2 | VRAM:Plaintext | | After Use | Diffie-Hellman Private Key:Paired With |
| Diffie-Hellman Private Key | | VRAM:Plaintext | | After Use | Diffie-Hellman Public Key:Paired With |
| Diffie-Hellman Shared Secret | | VRAM:Plaintext | | After Use | Diffie-Hellman Public Key:Computed Using<br>Diffie-Hellman Private Key:Computed Using |
| ECDH Public Key | SSP Input 3 (Peer)<br>SSP Output 2 | VRAM:Plaintext | | After Use | ECDH Private Key:Paired With |
| ECDH Private Key | | VRAM:Plaintext | | After Use | ECDH Public Key:Paired With |
| ECDH Shared Secret | | VRAM:Plaintext | | After Use | ECDH Public Key:Computed Using<br>ECDH Private Key:Computed Using |
| SNMPv3 Passwords (Privacy and Auth) | SSP Input 1<br>SSP Input 2<br>SSP Output 1 | Flash:Plaintext | | Factory Reset | |
| SNMP Privacy Key | | VRAM:Plaintext | | Session Termination | SNMPv3 Passwords (Privacy and Auth):Derived From |
| SNMP Authentication Key | | VRAM:Plaintext | | Session Termination | SNMPv3 Passwords (Privacy and Auth):Derived From |
| SRTP Master Key | SSP Input 1 | VRAM:Plaintext | | Session Termination | |
| SRTP Session Key | | VRAM:Plaintext | | Session Termination | SRTP Master Key:Derived From |
| SRTP Authentication Key | | VRAM:Plaintext | | Session Termination | SRTP Master Key:Derived From |
| SSH Authentication Public Key | SSP Output 1<br>SSP Output 3 | Flash:Plaintext | | Factory Reset | SSH Authentication Private Key:Paired With |
| SSH Authentication Private Key | | Flash:Plaintext | | Factory Reset | SSH Authentication Public Key:Paired With |
| SSH Session Keys | | VRAM:Plaintext | | Session Termination | Diffie-Hellman Shared Secret:Derived From |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| SSH Integrity Keys | | VRAM:Plaintext | | Session Termination | Diffie-Hellman Shared Secret:Derived From |
| TLS Authentication Public Key | SSP Output 1<br>SSP Output 3 | Flash:Plaintext | | Factory Reset | TLS Authentication Private Key:Paired With |
| TLS Authentication Private Key | | Flash:Plaintext | | Factory Reset | TLS Authentication Public Key:Paired With |
| TLS Premaster Secret | | VRAM:Plaintext | | After Use | |
| TLS Master Secret | | VRAM:Plaintext | | Session Termination | TLS Premaster Secret:Derived From |
| TLS Session Keys | | VRAM:Plaintext | | Session Termination | TLS Master Secret:Derived From |
| TLS Integrity Keys | | VRAM:Plaintext | | Session Termination | TLS Master Secret:Derived From |
| Web UI Certificate | SSP Output 3 | Flash:Plaintext | | Factory Reset | |
| Bypass Key | | Flash:Plaintext | | Factory Reset | |

Table 20: SSP Table 2

## 9.5 Transitions

Please see the latest revision of SP 800-131A and CMVP Programmatic Transitions page for transitions that may affect this module.

# 10 Self-Tests

The modules include an array of self-tests that are run during startup and during operations to prevent any secure data from being released and to ensure all components are functioning correctly.

## 10.1 Pre-Operational Self-Tests

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details |
|---|---|---|---|---|---|
| RSA SigVer (FIPS186-5) (A6582) | pss Modulus: 2048 Hash: SHA2-256 | Approved Integrity Technique | SW/FW Integrity | Status | Applied to all firmware components |
| Bypass Test | - | - | Bypass | Status | Ensures the correct operation of the logic governing activation of the bypass capability. |

Table 21: Pre-Operational Self-Tests

Pre-Operational Self-Tests are run upon the power up/initialization of the module. The module transitions to the operational state only after the pre-operational self-tests (and the cryptographic algorithm self-tests (CASTs)) are passed successfully. The design of the modules ensures that all data output, via the data output interface, is inhibited whenever the module is in a pre-operational self-test condition.

## 10.2 Conditional Self-Tests

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| RSA SigGen (FIPS186-5) (A6577) | pkcs Modulus: 2048 Hash: SHA2-256 | KAT | CAST | Status | Sign | Power Up |
| RSA SigVer (FIPS186-5) (A6577) | pkcs Modulus: 2048 Hash: SHA2-256 | KAT | CAST | Status | Verify | Power Up |
| AES-CTR (A6578) | 128-bit | KAT | CAST | Status | Separate Encrypt and Decrypt | Power Up |
| HMAC-SHA-1 (A6578) | HMAC-SHA-1 | KAT | CAST | Status | MAC | Power Up |
| KDF SRTP (A6578) | - | KAT | CAST | Status | SP 800-135 Key Derivation | Power Up |
| SHA-1 (A6578) | SHA-1 | KAT | CAST | Status | Message Digest | Power Up |
| AES-CTR (A6579) | 128-bit | KAT | CAST | Status | Separate Encrypt and Decrypt | Power Up |
| HMAC-SHA-1 (A6579) | HMAC-SHA-1 | KAT | CAST | Status | MAC | Power Up |
| KDF SRTP (A6579) | - | KAT | CAST | Status | SP 800-135 Key Derivation | Power Up |
| SHA-1 (A6579) | SHA-1 | KAT | CAST | Status | Message Digest | Power Up |
| AES-CCM (A6582) | 128-bit | KAT | CAST | Status | Separate Encrypt and Decrypt | Power Up |
| AES-GCM (A6582) | 128-bit | KAT | CAST | Status | Separate Encrypt and Decrypt | Power Up |
| Counter DRBG (A6582) | AES-256 | KAT | CAST | Status | SP 800-90Arev1 Section 11.3 | Power Up |
| ECDSA KeyGen (FIPS186-5) (A6582) | P-256, P-384 SHA2-256 | PCT | PCT | Status | Sign, Verify | Key Pair Generation |
| ECDSA SigGen (FIPS186-5) (A6582) | P-256 SHA2-256 | KAT | CAST | Status | Sign | Power Up |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| ECDSA SigVer (FIPS186-5) (A6582) | P-256 SHA2-256 | KAT | CAST | Status | Verify | Power Up |
| HMAC-SHA-1 (A6582) | HMAC-SHA-1 | KAT | CAST | Status | MAC | Power Up |
| HMAC-SHA2-256 (A6582) | HMAC-SHA2-256 | KAT | CAST | Status | MAC | Power Up |
| HMAC-SHA2-512 (A6582) | HMAC-SHA2-512 | KAT | CAST | Status | MAC | Power Up |
| KAS-ECC-SSC Sp800-56Ar3 (A6582) | P-256 | KAT | CAST | Status | Ephemeral Unified Shared Secret (Z) Computation | Power Up |
| KAS-FFC-SSC Sp800-56Ar3 (A6582) | FFDHE2048 | KAT | CAST | Status | dhEphem Shared Secret (Z) Computation | Power Up |
| KDF SNMP (A6582) | SHA-1 | KAT | CAST | Status | SP 800-135 Key Derivation | Power Up |
| KDF SSH (A6582) | Key Length: 256-bit, Hash: SHA2-256 | KAT | CAST | Status | SP 800-135 Key Derivation | Power Up |
| RSA KeyGen (FIPS186-5) (A6582) | Modulus: 2048, 3072, 4096 Hash: SHA2-256 | PCT | PCT | Status | Sign, Verify | Key Pair Generation |
| RSA SigGen (FIPS186-5) (A6582) | pkcs Modulus: 2048 Hash: SHA2-256 | KAT | CAST | Status | Sign | Power Up |
| RSA SigVer (FIPS186-5) (A6582) | pkcs Modulus: 2048 Hash: SHA2-256 | KAT | CAST | Status | Verify | Power Up |
| Safe Primes Key Generation (A6582) | FFDHE2048, MODP-2048, MODP-4096, MODP8192 | PCT | PCT | Status | SP 800-56A Rev3 Section 5.6.2.1.4 | Key Pair Generation |
| SHA-1 (A6582) | SHA-1 | KAT | CAST | Status | Message Digest | Power Up |
| SHA2-256 (A6582) | SHA2-256 | KAT | CAST | Status | Message Digest | Power Up |
| SHA2-512 (A6582) | SHA2-512 | KAT | CAST | Status | Message Digest | Power Up |
| TLS v1.2 KDF RFC7627 (A6582) | SHA2-256 | KAT | CAST | Status | SP 800-135 Key Derivation | Power Up |
| TLS v1.3 KDF (A6582) | SHA2-256 | KAT | CAST | Status | SP 800-135 Key Derivation | Power Up |
| RCT | - | FD | CAST | Status | SP 800-90B Section 4 | Power Up, On Demand and Continuously |
| APT | - | FD | CAST | Status | SP 800-90B Section 4 | Power Up, On Demand and Continuously |
| Bypass Test | HMAC-SHA2-256 | - | Bypass | Status | Ensures the correct operation of the services providing cryptographic processing when the mechanism governing the switching procedure is modified. | Bypass modification |

Table 22: Conditional Self-Tests

## 10.3 Periodic Self-Test Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| RSA SigVer (FIPS186-5) (A6582) | Approved Integrity Technique | SW/FW Integrity | On Demand | Power Cycle |
| Bypass Test | - | Bypass | On Demand | Power Cycle |

Table 23: Pre-Operational Periodic Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| RSA SigGen (FIPS186-5) (A6577) | KAT | CAST | On Demand | Power Cycle |
| RSA SigVer (FIPS186-5) (A6577) | KAT | CAST | On Demand | Power Cycle |
| AES-CTR (A6578) | KAT | CAST | On Demand | Power Cycle |
| HMAC-SHA-1 (A6578) | KAT | CAST | On Demand | Power Cycle |
| KDF SRTP (A6578) | KAT | CAST | On Demand | Power Cycle |
| SHA-1 (A6578) | KAT | CAST | On Demand | Power Cycle |
| AES-CTR (A6579) | KAT | CAST | On Demand | Power Cycle |
| HMAC-SHA-1 (A6579) | KAT | CAST | On Demand | Power Cycle |
| KDF SRTP (A6579) | KAT | CAST | On Demand | Power Cycle |
| SHA-1 (A6579) | KAT | CAST | On Demand | Power Cycle |
| AES-CCM (A6582) | KAT | CAST | On Demand | Power Cycle |
| AES-GCM (A6582) | KAT | CAST | On Demand | Power Cycle |
| Counter DRBG (A6582) | KAT | CAST | On Demand | Power Cycle |
| ECDSA KeyGen (FIPS186-5) (A6582) | PCT | PCT | N/A | N/A |
| ECDSA SigGen (FIPS186-5) (A6582) | KAT | CAST | On Demand | Power Cycle |
| ECDSA SigVer (FIPS186-5) (A6582) | KAT | CAST | On Demand | Power Cycle |
| HMAC-SHA-1 (A6582) | KAT | CAST | On Demand | Power Cycle |
| HMAC-SHA2-256 (A6582) | KAT | CAST | On Demand | Power Cycle |
| HMAC-SHA2-512 (A6582) | KAT | CAST | On Demand | Power Cycle |
| KAS-ECC-SSC Sp800-56Ar3 (A6582) | KAT | CAST | On Demand | Power Cycle |
| KAS-FFC-SSC Sp800-56Ar3 (A6582) | KAT | CAST | On Demand | Power Cycle |
| KDF SNMP (A6582) | KAT | CAST | On Demand | Power Cycle |
| KDF SSH (A6582) | KAT | CAST | On Demand | Power Cycle |
| RSA KeyGen (FIPS186-5) (A6582) | PCT | PCT | N/A | N/A |
| RSA SigGen (FIPS186-5) (A6582) | KAT | CAST | On Demand | Power Cycle |
| RSA SigVer (FIPS186-5) (A6582) | KAT | CAST | On Demand | Power Cycle |
| Safe Primes Key Generation (A6582) | PCT | PCT | On Demand | Power Cycle |
| SHA-1 (A6582) | KAT | CAST | On Demand | Power Cycle |
| SHA2-256 (A6582) | KAT | CAST | On Demand | Power Cycle |
| SHA2-512 (A6582) | KAT | CAST | On Demand | Power Cycle |
| TLS v1.2 KDF RFC7627 (A6582) | KAT | CAST | On Demand | Power Cycle |
| TLS v1.3 KDF (A6582) | KAT | CAST | On Demand | Power Cycle |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| RCT | FD | CAST | On Demand | Power Cycle |
| APT | FD | CAST | On Demand | Power Cycle |
| Bypass Test | - | Bypass | On Demand | Power Cycle |

Table 24: Conditional Periodic Information

## 10.4 Error States

| Name | Description | Conditions | Recovery Method | Indicator |
|---|---|---|---|---|
| Hard Error | The module halts operation, where all data output is inhibited. | Failed pre-operational self-test or CAST. | Attempt reboot, if reboot does not clear error, return to manufacturer. | Error Status and module halts operation |
| Soft Error | The module continues operation and repeats test. | Failed PCT | Module returns to operational state once error is logged. | Error Status returned |

Table 25: Error States

# 11 Life-Cycle Assurance

This section describes the configuration, maintenance, and administration of the cryptographic module. If the steps outlined in Section 11.1 below are not followed, the module will be operating in a non-compliant state that is out of scope of the validation.

## 11.1 Installation, Initialization, and Startup Procedures

Approved Mode is enabled by implementing the following steps:

1. Open CLI: type “setup entitlements”
2. Select “5 Data Integrity (FIPS 140-3)” option and type “enabled”
3. Type “s” to save the above modified entitlements.
4. Then reboot the module for Approved Mode to take effect.

Once the secure setup and the secure initialization and configuration is complete, the module is in Approved Mode. The steps outlined in Section 11.2 can be performed to ensure that the Approved Mode was correctly configured.

## 11.2 Administrator Guidance

The crypto-officer can verify FIPS settings by following these steps:

- Verify that the firmware version of the module is S-Cz9.3 (“show version” section in Session Border Controller ACLI Configuration Guide)
- A new account for the Crypto-Officer and User shall be created as part of Setup and Initialization process. Upon creation of the new CO and User accounts the “default” accounts shipped with the module shall be disabled (“local-accounts” section in SBC Guide).
- Ensure all management traffic is encapsulated within a trusted session by encapsulating in a TLS, SSH, or SRTP tunnel as appropriate (“TLS-profile”, “SSH-config” and “Sdes-profile” sections in SBC Guide).
- HTTPS shall be enabled and configure the web server certificate prior to connecting to the WebUI over TLS (“http-config” section in SBC Guide).
- Ensure that SNMP V3 is configured with AES-128/HMAC only (“SNMP-Group-Entry” section in SBC Guide).
- Ensure SSH is configured to use AES CTR/GCM mode for encryption (“Configure SSH Ciphers” section in SBC Guide).
- Ensure SSH uses at least Diffie-Hellman group 14 in Approved mode (“SSH-config” section in SBC Guide).
- Ensure RSA keys are at least 2048-bit keys for TLS. No 512-bit or 1024-bit keys can be used in Approved mode of operation (“Certificate-record” section in SBC Guide - 2048 is the default RSA modulus).
- All operator passwords must be a minimum of 8 characters in length (“password-policy” section in SBC Guide).
- Ensure use of FIPS-approved algorithms for TLS (“TLS-profile” in SBC Guide):
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_AES_128_CCM_SHA256
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
- Be aware that when configuring High Availability (HA), only a local HA configuration to a directly connected box via a physical cable over the management port is allowed in Approved Mode. Remote HA is not allowed in Approved mode.
- Be aware that HA configuration data that contains SSPs must never be transported over an untrusted network. Ensure that the HA ports used for the transport of HA data (including SSPs) are bound to a private IP address range during setup.
- Be aware that only the HA state transactions between the two devices over the direct physical connection are permitted over those dedicated ports.
- RADIUS and TACACS+ shall not be used in Approved Mode.

For more details, please refer to the Session Border Controller ACLI Configuration Guide (SBC Guide).

## 11.3 Non-Administrator Guidance

The User does not have the ability to configure sensitive information on the module, with the exception of their password. The module enforces a strong password, and the user must not reveal their password to anyone. Additionally, the User should be careful to protect any secret or private keys in their possession.

Additional non-administrator guidance is available in the FIPS Compliance Guide.

## 11.4 End of Life

The procedure for secure sanitization of the module at the end of life is to factory reset the platform, which performs the zeroization of the SSPs. This should be performed so that the module can be disposed or shipped back to Oracle.

# 12 Mitigation of Other Attacks

The module does not offer mitigation of other attacks and therefore this section is not applicable.