FIPS 140-2 Non-Proprietary Security Policy

Acme Packet VME

FIPS 140-2 Level 1 Validation

Software Version: ECz 7.5.0

Date: December 11, 2017

Title: Acme Packet VME Security Policy
Date: December 11, 2017
Author: Acumen Security, LLC.
Contributing Authors:
Oracle Communications Engineering
Oracle Security Evaluations – Global Product Security

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

TABLE OF CONTENTS

Section **Title** **Page**

1. Introduction ... 1

1.1 Overview ... 1

1.2 Document Organization ... 1

2. Acme Packet VME ... 2

2.1 Functional Overview ... 2

3. Cryptographic Module Specification ... 3

3.1 Definition of the Cryptographic Module ... 3

3.2 Definition of the Physical Cryptographic Boundary ... 3

3.3 FIPS 140-2 Validation Scope ... 4

3.4 Approved or Allowed Security Functions ... 4

3.5 Non-Approved But Allowed Security Functions ... 5

3.6 Non-Approved Security Functions ... 6

4. Module Ports and Interfaces ... 7

5. Physical Security ... 7

6. Roles and Services ... 8

6.1 Operator Services and Descriptions ... 8

6.2 Unauthenticated Services and Descriptions ... 10

6.3 Operator Authentication ... 11

6.3.1 Crypto-Officer: Password-Based Authentication ... 11

6.3.2 User: Certificate-Based Authentication ... 11

6.4 Key and CSP Management ... 12

7. Self-Tests ... 16

7.1 Power-Up Self-Tests ... 16

7.1.1 Software Integrity Test ... 16

7.1.2 Mocana Self-tests ... 16

7.1.3 OpenSSL Self-Tests ... 16

7.2 Critical Functions Self-Tests ... 16

7.3 Conditional Self-Tests ... 17

8. Crypto-Officer and User Guidance ... 18

8.1 Secure Setup and Initialization ... 18

8.2 AES-GCM IV Construction/Usage ... 18

9. Mitigation of Other Attacks ... 19

10 Operational Environment ... 20

Appendices ... 21

Acronyms, Terms and Abbreviations ... 21

References ... 22

List of Tables

Table 1: FIPS 140-2 Security Requirements 4
Table 2: FIPS Approved or Allowed Security Functions 5
Table 3: Non-Approved but Allowed Security Functions 5
Table 4: Non-Approved Disallowed Functions 6
Table 5 – Mapping of FIPS 140 Logical Interfaces to Logical Ports 7
Table 6 – Service Summary 8
Table 7 – Operator Services and Descriptions 10
Table 8 – Unauthenticated Operator Services and Descriptions 10
Table 9 – Crypto-Officer Authentication 11
Table 10 – Crypto-Officer Authentication 12
Table 11 – CSP Table 15
Table 12 – Operating Environment 20
Table 13 – Acronyms 21
Table 14 – References 22

List of Figures

Figure 1 – VME Logical Cryptographic Boundary 3

1. Introduction

1.1 Overview

This document is the Security Policy for the Acme Packet VME developed by Oracle Corporation. Acme Packet VME 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 the Acme Packet VME functions in order to meet the FIPS requirements, and the actions that operators must take to maintain the security of the module.

This Security Policy describes the features and design of the Acme Packet VME module using the terminology contained in the FIPS 140-2 specification. FIPS 140-2, Security Requirements for Cryptographic Module specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST/CSEC Cryptographic Module Validation Program (CMVP) validates cryptographic module 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. Acme Packet VME

2.1 Functional Overview

The Acme Packet VME is specifically designed to meet the unique price performance and manageability requirements of the small to medium sized enterprise and remote office/ branch office. Ideal for small site border control and Session Initiation Protocol (SIP) trunking service termination applications, the Acme Packet VME deliver Oracle’s industry leading ESBC capabilities in binary packaged executable that can be run in a virtual environment.

Acme Packet VME addresses the unique connectivity, security, and control challenges enterprises often encounter when extending real-time voice, video, and UC sessions to smaller sites. The appliance also helps enterprises contain voice transport costs and overcome the unique regulatory compliance challenges associated with IP telephony. An embedded browser based graphical user interface (GUI) simplifies setup and administration.

3. Cryptographic Module Specification

3.1 Definition of the Cryptographic Module

The logical cryptographic boundary of the module consists of the Oracle VME ISO image called nnECZ750-img.iso version ECz7.5.0.

Figure 1 shows the logical block diagram (red-dotted line) of the module executing in memory and its interactions with the hypervisor through the module's defined logical cryptographic boundary. The module interacts directly with the hypervisor, which runs directly on the host system.

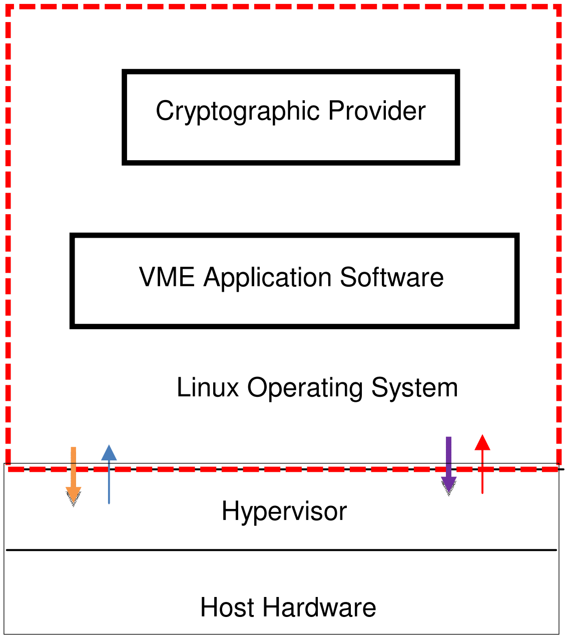

Figure 1 – VME Logical Cryptographic Boundary

→ Data Output
→ Data Input
→ Control Input
→ Status Output
- - - - - - - Cryptographic Boundary

3.2 Definition of the Physical Cryptographic Boundary

The module consists of binary packaged into an executable that can be run in a virtual environment. The module is classified as a multi-chip standalone cryptographic module. The physical cryptographic boundary is defined as the hard enclosure of the host system on which it runs and no components are excluded from the requirements of FIPS PUB 140-2.

3.3 FIPS 140-2 Validation Scope

The Acme Packet VME appliances are 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	2
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 Approved or Allowed Security Functions

The Acme Packet VME contains the following FIPS Approved Algorithms listed in Table 2:

Approved or Allowed Security Functions		Certificate
Symmetric Algorithms		
AES	OpenSSL: (CBC, GCM); Encrypt/Decrypt; Key Size = 128, 256	4577
	Mocana: (CBC); Encrypt/Decrypt; Key Size = 128, 256	4597
Triple DES	OpenSSL: (CBC); Encrypt/Decrypt; Key Size = 192	2460
	Mocana: (CBC); Encrypt/Decrypt; Key Size = 192	2447
Secure Hash Standard (SHS)		
SHS	OpenSSL: SHA-1, SHA-256, SHA-384	3754
	Mocana: SHA-1, SHA-256	3775
Data Authentication Code		
HMAC	OpenSSL: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	3028
	Mocana: HMAC-SHA-1, HMAC-SHA-256	3049
Asymmetric Algorithms		
RSA	OpenSSL: FIPS186-2: ALG[ANSIX9.31]: SIG(gen) (4096 SHS: SHA-256, SHA-384) RSA: FIPS186-4: 186-4KEY(gen): FIPS186-4_Random_e ALG[ANSIX9.31] SIG(gen) (2048 SHA(256 , 384)) SIG(Ver) (2048 SHA(1, 256, 384)) RSA: FIPS186-2 (not used by the module) Signature Generation 9.31:	2496

Approved or Allowed Security Functions		Certificate
	Modulus lengths: 4096 SHAs: SHA-256, SHA-384	
	Mocana: RSA: 186-4: 186-4KEY(gen): FIPS186-4_Random_e SIG(Ver) (1024 SHA(1); (2048 SHA (1))	2508
ECDSA	OpenSSL: FIPS186-4: PKG: CURVES(P-256 P-384 Testing Candidates) SigGen: CURVES(P-256: (SHA-256, 384) P-384: (SHA-256, 384) SigVer: CURVES(P-256: (SHA-256, 384) P-384: (SHA-256, 384))	1134
Random Number Generation		
DRBG	OpenSSL: **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256)] **Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1) Note: While implemented, CTR_DRBG is not used by the module.	1524
Key Establishment		
Key Derivation	OpenSSL: SNMP KDF, SRTP KDF, TLS KDF	CVL 1255
	Mocana: IKEv1 KDF (tested but not used by the module), SSH KDF	CVL 1269

Table 2: FIPS Approved or Allowed Security Functions

3.5 Non-Approved But Allowed Security Functions

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

Algorithm	Usage
Diffie-Hellman	Key agreement, key establishment methodology provides 112-bits of encryption strength, non-compliant less than 112 bits of encryption strength.
RSA Key Wrapping	Key wrapping, key establishment methodology provides 112-bits of encryption strength, non-compliant less than 112 bits of encryption strength.
NDRNG	Used for seeding NIST SP 800-90A DRBG.
MD5	Used within the TLS protocol

Table 3: Non-Approved but Allowed Security Functions

3.6 Non-Approved Security Functions

The following services are considered non-Approved and may not be used in a FIPS-approved mode of operation:

Service	Non-Approved Security Functions
SSH	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES
TLS	MACing: HMAC MD5 Symmetric: DES
IKE/IPsec	Hashing: MD5, MACing: HMAC MD5
SNMP	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES
Diffie-Hellman	Key agreement, less than 112 bits of encryption strength.
RSA Key Wrapping	Key wrapping, less than 112 bits of encryption strength.

Table 4: Non-Approved Disallowed Functions

Services listed in the previous table make use non-compliant cryptographic algorithms. Use of these algorithms is prohibited in a FIPS-approved mode of operation. These services are allowed in FIPS mode when using allowed algorithms (as specified in section 8.1)

4. Module Ports and Interfaces

Oracle Virtual Machine edition is a virtualized cryptographic module that meets the overall Level 1 FIPS 140-2 requirements. The module interfaces can be categorized as follows:

- Data Input Interface
- Data Output Interface
- Control Input interface
- Status Output Interface
- Power Interface

The table below provides the mapping of ports as per FIPS 140-2 Standard.

FIPS 140 Interface	Physical Port	VM Port	Logical Interface	Information Input/Output
Data Input	Host System Ethernet (10/100/1000) Ports	• Virtual Ethernet Ports, • Virtual USB Ports, • Virtual Serial Ports.	API Input Data and Parameters,	Cipher text
Data Output	Host System Ethernet (10/100/1000) Ports	• Virtual Ethernet Ports, • Virtual USB Ports, • Virtual Serial Ports.	API Output Data and Parameters	Cipher text
Control Input	Host System Ethernet (10/100/1000) Ports	• Virtual Ethernet Ports, • Virtual USB Ports, • Virtual Serial Ports.	API Command Input Parameters	• Plaintext control input via console port (configuration commands, operator passwords) • Ciphertext control input via network management (EMS control, CDR accounting, CLI management)
Status Output	Host System Ethernet (10/100/1000) Ports	• Virtual Ethernet Ports, • Virtual USB Ports, • Virtual Serial Ports.	API Status Output Parameters	Plaintext Status Output.
Power	Power Plug	NA	N/A	N/A

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

5. Physical Security

The module is comprised of software only and thus does not claim any physical security.

6. Roles and Services

As required by FIPS 140-2 Level 2, there are three roles (a Crypto Officer Role, User Role, and Unauthenticated Role) in the module that operators may assume. The module supports role-based authentication, and the respective services for each role are described in the following sections.

The below table gives a high level description of all services provided by the module and lists the roles allowed to invoke each service.

Operator Role	Summary of Services
User	• View configuration versions and system performance data • Handle certificate information for TLS, IKE functions • Test pattern rules, local policies, and session translations • Display system alarms. • Set the display dimensions for the terminal • Connect to module for data transmission
Crypto-Officer	Allowed access to all system commands and configuration privileges
Unauthenticated	• Show Status • Initiate self-tests

Table 6 – Service Summary

6.1 Operator Services and Descriptions

The below table provides a full description of all services provided by the module and lists the roles allowed to invoke each service.

U	CO	Service Name	Service Description	Keys and CSP(s)	Access Type(s)
	X	Configure	Initializes the module for FIPS mode of operation	HMAC-SHA-256 key, FIPS License	R, W, X
	X	Zeroize CSP's	Clears keys/CSPs from memory and disk	All CSP's	Z
	X	Software Update	Updates software	Software Integrity Key (RSA)	R, X
	X	Bypass	Configure bypass using TCP or UDP and viewing bypass service status	HMAC-SHA-256 Key	R, W, X
X	X	Decrypt	Decrypts a block of data Using AES or Triple-DES in FIPS Mode	TLS Session Keys (Triple-DES) TLS Session Keys (AES128) TLS Session Keys (AES256)	X X X

U	CO	Service Name	Service Description	Keys and CSP(s)	Access Type(s)
				SSH Session Key (Triple-DES) SSH Session Key (AES128) SSH Session Key (AES256) SRTP Session Key (AES-128) SNMP Privacy Key (AES-128)	X X X X X
X	X	Encrypt	Encrypts a block of data Using AES or Triple-DES in FIPS Mode	TLS Session Keys (Triple-DES) TLS Session Keys (AES128) TLS Session Keys (AES256) SSH Session Key (Triple-DES) SSH Session Key (AES128) SSH Session Key (AES256) SRTP Session Key (AES-128) SNMP Privacy Key (AES-128)	X X X X X X X X
X	X	Generate Keys	Generates AES or Triple-DES keys for encrypt/decrypt operations. Generates Diffie-Hellman and RSA keys for key transport/key establishment.	TLS Session Keys (Triple-DES) TLS Session Keys (AES128) TLS Session Keys (AES256) SSH Session Key (Triple-DES) SSH Session Key (AES128) SSH Session Key (AES256) SRTP Session Key (AES-128) SNMP Privacy Key (AES-128) Diffie-Hellman Public Key (DH) Diffie-Hellman Private Key (DH) SSH authentication private Key (RSA) SSH authentication public key (RSA) TLS authentication private Key (ECDSA/RSA) TLS authentication public key (ECDSA/RSA)	R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W

U	CO	Service Name	Service Description	Keys and CSP(s)	Access Type(s)
X	X	Verify	Used as part of the TLS, SSH, protocol negotiation	SSH authentication private Key (RSA) SSH authentication public key (RSA) TLS authentication private Key (ECDSA/RSA) TLS authentication public key (ECDSA/RSA)	X X X X X
X	X	Generate Seed	Generate an entropy_input for Hash_Drbg	DRBG Seed DRBG Entropy Input String	R, W, X
X	X	Generate Random Number	Generate random number.	DRBG C DRBG V	R, W, X R, W, X
X	X	HMAC	Generate HMAC	SNMP Authentication Key SRTP Authentication Key SSH Integrity Keys TLS Integrity Keys	X X X X

R – Read, W – Write, X – Execute, Z - Zeroize

Table 7 – Operator Services and Descriptions

6.2 Unauthenticated Services and Descriptions

The below table provides a full description of the unauthenticated services provided by the module:

Service Name	Service Description
On-Demand Self-Test Initialization	This service provides for the running of on-demand self-tests
Show Status	This service shows the operational status of the module

Table 8 – Unauthenticated Operator Services and Descriptions

6.3 Operator Authentication

6.3.1 Crypto-Officer: Password-Based Authentication

In FIPS-approved mode of operation, the module is accessed via Command Line Interface over the Console ports or via SSH or SNMPv3 over the Network Management Ports. Other than status functions available by viewing the Status LEDs, the services described are available only to authenticated operators.

Method	Probability of a Single Successful Random Attempt	Probability of a Successful Attempt within a Minute
Password-Based	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. 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.	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 module will lock an account after 3 failed authentication attempts; thus, the maximum number of attempts in one minute is 3. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is $3/94^8$ which is less than 1/100,000.
Password-Based (Challenge Response)	Passwords must be a minimum of 12 numeric characters. 0-9, yielding 10 choices per character. The probability of a successful random attempt is 1/10^12, which is less than 1/1,000,000. 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 600/10^12, which is less than 1/100,000.	Passwords must be a minimum of 12 numeric characters. 0-9, yielding 10 choices per character. The module will lock an account after 3 failed authentication attempts; thus, the maximum number of attempts in one minute is 3. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is $3/10^{12}$ which is less than 1/100,000.

Table 9 – Crypto-Officer Authentication

6.3.2 User: Certificate-Based Authentication

The module also supports authentication via digital certificates for the User Role as implemented by the TLS and SSH protocols. The module supports a public key based authentication with 2048-bit RSA keys.

Method	Probability of a Single Successful Random Attempt	Probability of a Successful Attempt within a Minute
Certificate-Based	A 2048-bit RSA key 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.

Table 10 – Crypto-Officer Authentication

6.4 Key and CSP Management

The following keys, cryptographic key components and other critical security parameters are contained in the module. No parts of the SSH, TLS, or SNMP protocol, other than the KDF, have been tested by the CAVP and CMVP.

CSP Name	Generation/Input	Establishment/ Export	Storage	Use
Operator Passwords	Generated by the crypto officer as per the module policy	**Agreement**: NA **Entry**: Manual entry via console or SSH management session **Output**: Not Output	Virtual Hard Disk	Authentication of the crypto officer and user
Software Integrity Key (RSA)	Generated externally	**Entry**: RSA (2048 bits) entered as part of Software image	Virtual Hard Disk	Public key used to verify the integrity of software and updates
DRBG Entropy Input String	Generated internally from hardware sources	**Agreement**: NA **Entry**: NA **Output**: None	Virtual Hard Disk	Used in the random bit generation process
DRBG Seed	Generated internally from hardware sources	**Agreement**: NA **Entry**: NA **Output**: None	Virtual Hard Disk	Entropy used in the random bit generation process
DRBG C	Internal value used as part of SP 800-90a HASH_DRBG	**Agreement**: NA **Entry**: NA **Output**: None	Virtual Hard Disk	Used in the random bit generation process
DRBG V	Internal value used as part of SP 800-90a HASH_DRBG	**Agreement**: NA	Virtual Hard Disk	Used in the random bit generation process

CSP Name	Generation/Input	Establishment/ Export	Storage	Use
		Entry: NA **Output**: None		
Diffie-Hellman Public Key (DH)	Internal generation by FIPS-approved Hash_DRBG in software	**Agreement**: NA **Entry**: NA **Output**: None	Virtual Hard Disk	Diffie-Hellman secret key (2048 bits)
Diffie-Hellman Private Key (DH)	Internal generation by FIPS-approved Hash_DRBG	**Agreement**: NA **Entry**: NA **Output**: None	Virtual Hard Disk	Used to derive the secret session key during DH key agreement protocol
SNMP Privacy Key (AES-128)	NIST SP 800-135 KDF	**Agreement**: NIST SP 800-135 KDF **Entry**: NA **Output**: None	Virtual Hard Disk	For encryption / encryption of SNMP session traffic
SNMP Authentication Key (HMAC-SHA1)	Internal generation by FIPS-approved Hash_DRBG in software	**Agreement**: NA	Virtual Hard Disk	160-bit HMAC-SHA-1 for message authentication and verification in SNMP
SRTP Master Key (AES-128)	Internal generation by FIPS-approved Hash_DRBG in software	**Agreement**: Diffie-Hellman **Entry**: NA **Output**: encrypted	Virtual Hard Disk	Generation of SRTP session keys
SRTP Session Key (AES-128)	NIST SP 800-135 KDF	**Agreement**: NIST SP 800-135 KDF **Entry**: NA **Output**: None	Virtual Hard Disk	For encryption / decryption of SRTP session traffic

CSP Name	Generation/Input	Establishment/ Export	Storage	Use
SRTP Authentication Key (HMAC-SHA1)	derived from the master key	**Agreement**: NA	Virtual Hard Disk	160-bit HMAC-SHA-1 for message authentication and verification in SRTP
SSH Authentication Private Key (RSA)	Internal generation by FIPS-approved Hash_DRBG	**Agreement**: RSA (2048 bits)	Virtual Hard Disk	RSA private key for SSH authentication
SSH Authentication Public Key (RSA)	Internal generation by FIPS-approved Hash_DRBG	**Agreement**: RSA (2048 bits)	Virtual Hard Disk	RSA public key for SSH authentication.
SSH Session Keys (Triple-DES, AES-128, AES-256)	Derived via SSH KDF. Note: These keys are generated via SSH (IETF RFC 4251). This protocol enforces limits on the number of total possible encryption/decryption operations.	**Agreement**: Diffie-Hellman	Virtual Hard Disk	Encryption and decryption of SSH session
SSH Integrity Keys (HMAC-SHA1)	Derived via SSH KDF.	**Agreement**: NA	Virtual Hard Disk	160-bit HMAC-SHA-1 for message authentication and verification in SSH
TLS Authentication Private Key (ECDSA/RSA)	Internal generation by FIPS-approved Hash_DRBG	**Agreement**: RSA (2048bits); ECDSA (P- 256/P-384)	Virtual Hard Disk	ECDSA/RSA private key for TLS authentication
TLS Authentication Public Key (ECDSA/RSA)	Internal generation by FIPS-approved Hash_DRBG	**Agreement**: RSA (2048bits); ECDSA (P- 256/P-384)	Virtual Hard Disk	ECDSA/RSA public key for TLS authentication.
TLS Premaster Secret (48 Bytes)	Internal generation by FIPS-approved Hash_DRBG in software	**Agreement**: NA **Entry**: Input during TLS negotiation **Output**: Output to peer encrypted by Public Key	Virtual Hard Disk	Establishes TLS master secret
TLS Master Secret (48 Bytes)	Derived from the TLS Pre-Master Secret	**Agreement**: NA	Virtual Hard Disk	Used for computing the Session Key

CSP Name	Generation/Input	Establishment/ Export	Storage	Use
TLS Session Keys (Triple-DES, AES-128, AES-256)	Derived from the TLS Master Secret Note: These keys are generated via TLS (IETF RFC 5246). This protocol enforces limits on the number of total possible encryption/decryption operations.	**Agreement**: RSA key transport	Virtual Hard Disk	Used for encryption & decryption of TLS session
TLS Integrity Keys (HMAC-SHA1)	Internal generation by FIPS-approved Hash_DRBG in software	**Agreement**: NA	Virtual Hard Disk	160-bit HMAC-SHA-1 for message authentication and verification in TLS

Table 11 – CSP Table

Note: 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.

Note: All keys generated by the module use the direct output of a FIPS approved DRBG. This meets the requirements of SP 800-133.

7. Self-Tests

The modules include an array of self-tests that are run during startup and conditionally during operations to prevent any secure data from being released and to ensure all components are functioning correctly. Self-tests may be run on-demand by power cycling the module.

7.1 Power-Up Self-Tests

Acme Packet VME appliance performs the following power-up self-tests when the virtual machine is started. These self-tests require no inputs or actions from the operator:

7.1.1 Software Integrity Test

- RSA 2048 Software Integrity Test

7.1.2 Mocana Self-tests

- AES (Encrypt/Decrypt) Known Answer Test;
- Triple-DES (Encrypt/Decrypt) Known Answer Test;
- SHA-1 Known Answer Test;
- HMAC-SHA-1 Known Answer Test;
- HMAC-SHA-256 Known Answer Test; and
- RSA verify Known Answer Test.

7.1.3 OpenSSL Self-Tests

- SHA-1 Known Answer Test;
- SHA-256 Known Answer Test;
- HMAC-SHA-1 Known Answer Test;
- HMAC-SHA-256 Known Answer Test;
- HMAC-SHA-384 Known Answer Test;
- AES (Encrypt/Decrypt) Known Answer Test;
- AES GCM (Encrypt/Decrypt) Known Answer Test;
- Triple-DES (Encrypt/Decrypt) Known Answer Test;
- SP 800-90A DRBG Known Answer Test;
- RSA sign/verify Known Answer Test; and
- ECDSA sign/verify Known Answer Test.

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. While the user may attempt to restart the module in an effort to clear an error, the module will require re-installation in the event of a hard error such as a failed self-test.

7.2 Critical Functions Self-Tests

Acme Packet VME performs the following critical self-tests. These critical function tests are performed for each SP 800-90A DRBG implemented within the module.

- SP 800-90A Instantiation Test
- SP 800-90A Generate Test
- SP 800-90A Reseed Test
- SP 800-90A Uninstantiate Test

7.3 Conditional Self-Tests

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

- Pair Wise consistency tests to verify that the asymmetric keys generated for RSA, and ECDSA work correctly by performing a sign and verify operation;
- Continuous Random Number Generator test to verify that the output of approved-DRBG is not the same as the previously generated value;
- Continuous Random Number Generator test to verify that the output of entropy is not the same as the previously generated value;
- Bypass conditional test using HMAC-SHA-256 to ensure the mechanism governing media traffic is functioning correctly, and;
- Software Load test using a 2048-bit/SHA-256 RSA-Based integrity test to verify software to be updated.

8. Crypto-Officer and User Guidance

FIPS Mode is enabled by a license installed by Oracle, which will open/lock down features where appropriate. This section describes the configuration, maintenance, and administration of the cryptographic module.

8.1 Secure Setup and Initialization

The operator shall set up the device as defined in the Session Border Controller ACLI Configuration Guide. The Crypto-Officer shall also:

- Verify that the software version of the module is Version 7.5.0.
- Ensure all traffic is encapsulated in a TLS, SSH, or SRTP tunnel as appropriate.
- Ensure that SNMP V3 is configured with AES-128.
- Ensure all management traffic is encapsulated within a trusted session (i.e., Telnet should not be used in FIPS mode of operation).
- All operator passwords must be a minimum of 8 characters in length.
- Ensure use of FIPS-approved algorithms for TLS:
    - TLS_RSA_WITH_Triple-DES_EDE_CBC_SHA
    - TLS_DHE_RSA_WITH_Triple-DES_EDE_CBC_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_AES_256_CBC_SHA
    - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
    - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- Ensure RSA keys are at least 2048-bit keys. No 512-bit or 1024-bit keys can be used in FIPS mode of operation.
- When configuring High Availability (HA), only a local HA configuration on the same host is allowed in FIPS Approved Mode. Remote HA is not allowed in FIPS Approved mode.

8.2 AES-GCM IV Construction/Usage

In case the module's power is lost and then restored, the key used for the AES GCM encryption or decryption shall be redistributed. The AES GCM IV generation is in compliance with the [RFC5288] and shall only be used for the TLS protocol version 1.2 to be compliant with [FIPS140-2_IG] IG A.5, provision 1 ("TLS protocol IV generation"); thus, the module is compliant with [SP800-52].

9. Mitigation of Other Attacks

The module does not mitigate attacks beyond those identified in FIPS 140-2.

10 Operational Environment

The module is installed using a common base image distributed in a compatible hypervisor format (i.e ova, ovm, qcow2). The software image that is used to deploy the VME is common across all models. The tested configuration include:

Operating Environment	Processor	Hardware
Oracle Linux 7 running on VMware ESXi version 6.0	Intel Xeon Processor E5-2600 V3	Oracle Server X5-2

Table 12 – Operating Environment

This is considered a modifiable OE as defined by FIPS 140-2. The tested operating environments isolate virtual systems into separate isolated process spaces. Each process space is logically separated from all other processes by the operating environments software and hardware. The module functions entirely within the process space of the isolated system as managed by the single operational environment. This implicitly meets the FIPS 140-2 requirement that only one entity at a time can use the cryptographic module.

Appendices

Acronyms, Terms and Abbreviations

Term	Definition
AES	Advanced Encryption Standard
BBRAM	Battery Backed RAM
CDR	Call Data Record
CMVP	Cryptographic Module Validation Program
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DHE	Diffie-Hellman Ephemeral
DRBG	Deterministic Random Bit Generator
ECDSA	Elliptic Curve Digital Signature Algorithm
ESBC	Enterprise Session Border Controller
EDC	Error Detection Code
EMS	Enterprise Management Server
HMAC	(Keyed) Hash Message Authentication Code
IKE	Internet Key Exchange
KAT	Known Answer Test
KDF	Key Derivation Function
LED	Light Emitting Diode
MGT	Management
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
SNMP	Simple Network Management Protocol
SRTP	Secure Real Time Protocol
TDM	Time Division Multiplexing
TLS	Transport Layer Security
VME	Virtual Machine Edition

Table 13 – Acronyms

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 module can be found on the Oracle web site at https://www.oracle.com/industries/communications/enterprise/products/session-border-controller/index.html.

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
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	NIST	Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes
PKCS#1	RSA Laboratories	PKCS#1 v2.1: RSA Cryptographic Standard

Table 14 – References