FIPS 140-2 Non-Proprietary Security Policy

Acme Packet 3820

Document Version 2.5

December 5, 2014

Prepared For:

Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065
www.oracle.com

Prepared By:

SafeLogic Inc.
530 Lytton Ave, Suite 200
Palo Alto, CA 94301
www.safelogic.com

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140-2

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic products to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment Canada (CSEC) jointly run the Cryptographic Module Validation Program (CMVP). The NIST National Voluntary Laboratory Accreditation Program (NVLAP) accredits independent testing labs to perform FIPS 140-2 testing; the CMVP validates test reports for all cryptographic modules pursuing FIPS 140-2 validation. *Validation* is the term given to a cryptographic module that is documented and tested against the FIPS 140-2 criteria.

More information is available on the CMVP website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the Acme Packet 3820 from Oracle Communications provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document also contains details on the cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS mode of operation.

The Oracle Communications Acme Packet 3820 may also be referred to as the “module” in this document.

1.3 External Resources

The Oracle Communications website (http://www.oracle.com) contains information on the full line of products from Oracle Communications, including a detailed overview of the Acme Packet 3820 solution. The Cryptographic Module Validation Program website contains links to the FIPS 140-2 certificate and Oracle Communications contact information.

1.4 Notices

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CSEC	Communications Security Establishment of Canada
CSP	Critical Security Parameter
DTR	Derived Testing Requirement
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GPOS	General Purpose Operating System
HMAC	Hashed Message Authentication Code
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
RSA	Rivest Shamir Adelman
SHA	Secure Hashing Algorithm

Table 1 – Acronyms and Terms

2 Oracle Communications Acme Packet 3820

2.1 Product Overview

Oracle Communications session border controllers (SBC) provide critical control functions to deliver trusted, first-class interactive communications—voice, video and multimedia sessions—across IP network borders. They support multiple applications in government, service provider, enterprise and contact center networks—from VoIP trunking to hosted enterprise and residential services to fixed-mobile convergence. Oracle Communications' SBC is configured on Acme Packet OS, which operates on both the Acme Packet 4500 and 3820 platforms.

The Acme Packet 3820 platform supports up to 4,000 simultaneous signaled sessions for government agencies, smaller service providers, small enterprises and smaller sites within larger organizations. Like the Acme Packet 4500, the Acme Packet 3820 features Acme Packet's custom hardware design tightly integrated with Acme Packet OS to satisfy the most critical infrastructure security requirements.

In government, enterprise and contact center environments, the 3820 secure SIP/H.323 trunking borders to service provider and other 3rd party IP networks and the Internet border to remote offices, teleworkers and mobile employees. In extremely security-conscious organizations, they secure the border to the private VPN connecting other sites. SIP and H.323 interworking capabilities ensure interoperability with and between legacy IP PBX equipment and next-generation unified communications platforms. They control session admission, IP PBX or UC server loads and overloads, IP network transport and SIP/H.323 session routing to assure SLAs and minimize costs. Regulatory compliance requirements are also satisfied with encryption ensuring session privacy and call/session replication for recording.

2.2 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interference / Electromagnetic Compatibility	2
Self-Tests	2
Design Assurance	3

FIPS 140-2 Section Title	Validation Level
Mitigation of Other Attacks	N/A

Table 2 – Validation Level by DTR Section

2.3 Algorithm Implementations

2.3.1 FIPS-Approved Algorithms

The module contains the following algorithm implementations:

- Hifn 8450: bump-in-the-wire, bulk IPSec processing (HMAC-SHA1, AES, TRIPLE-DES)
- Broadcom 5862 (BCM5862): DH, SHA-1, HMAC-SHA1, AES and Triple-DES for SSH and TLS
- Firmware running on Intel Core Duo T2500: random number generation, SHA-1, SHA-256, RSA, HMAC-SHA1, HMAC-SHA256, Hash_DRBG

These cryptographic algorithm implementations have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Keyed Hash	HMAC-SHA1	FIPS 198-1	519	Message verification
Hashing	SHA-1	FIPS 180-4	912	Message digest
Symmetric Key	Three key Triple-DES (CBC mode)	NIST SP 800-67	745	Data encryption / decryption
	AES 128 and 256(CBC, CTR modes)	FIPS 197	928	Data encryption / decryption

Table 3 – Algorithm Certificates for FIPS-Approved Algorithms in the Hifn 8450

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Hashing	SHA-1	FIPS 180-4	1378	Message digest
Keyed Hash	HMAC-SHA1	FIPS 198-1	907	Message verification
Symmetric Key	Three key Triple-DES (CBC mode)	NIST SP 800-67	1019	Data encryption / decryption
	AES 128 and 256(CBC, CTR modes)	FIPS 197	1555	Data encryption / decryption

Table 4 – Algorithm Certificates for FIPS-Approved Algorithms for the BCM5862

Algorithm Type	Algorithm	Standard	CAVP Certificate for Intel Core Duo T2500	Use
Hashing	SHA-1 SHA-256	FIPS 180-4	1372	Message digest

Algorithm Type	Algorithm	Standard	CAVP Certificate for Intel Core Duo T2500	Use
Keyed Hash	HMAC-SHA1 HMAC-SHA256	FIPS 198-1	899	Message verification and module integrity (via HMAC-SHA256)
Asymmetric Key	RSA	FIPS 186-2	754	Verify operations
Random Number Generation	Hash_DRBG	SP800-90A (hash based)	67	Random Number Generation

Table 5 – Algorithm Certificates for FIPS-Approved Algorithms for Firmware

2.3.2 Non-Approved Algorithms

The module implements the following non-approved algorithms:

- DES
- ARC4
- HMAC-MD5
- RSA (allowed for use in FIPS mode of operation)
  - Used in FIPS mode for TLS sessions key establishment in and provides 112-bits of encryption strength
- Diffie-Hellman
  - Used for key agreement in SSH and IPSEC sessions; key establishment methodology provides 112-bits of encryption strength (allowed for use in FIPS Mode of operation).
  - Used for key agreement in SSH and IPSEC sessions; key establishment methodology provides less than 112-bits of encryption strength (non-compliant).
- Hardware-based random number generator
  - This RNG is used in FIPS mode only to generate entropy_input to the firmware-based FIPS-approved Hash_DRBG.

Unless otherwise noted, Non-approved algorithms are not used in FIPS mode.

2.4 Cryptographic Module Specification

The module is the Oracle Communications Acme Packet 3820 running firmware version C6.3 on hardware version A1. The module is classified as a multi-chip standalone cryptographic module. The physical cryptographic boundary is defined as the module case and all components within the case. No firmware is excluded from validation.

The specific model included in the validation is as follows:

- Acme Packet 3820

- Running network processor AMCC NP3750 @400 Mhz and host processor Intel Celeron M 440
- Running Hifn 8450 and Broadcom 5862 for dedicated, hardware-based cryptographic processing

The physical boundary is pictured in the image below:

Figure 1 – Physical Boundary for Acme Packet 3820

2.5 Module Interfaces

The table below describes the main interfaces on the Acme Packet 3820:

Physical Interface	Description / Use
LEDs	Indicates if any alarms are active on the module. The LED can be three different colors to indicate the severity of the alarms. • Unlit—system is fully functional without any faults • Amber—major alarm has been generated • Red—critical alarm has been generated.
Console Ports	Provides console access to the module. The module supports only one active serial console connection at a time. The rear console port is useful for customers who want permanent console access; the front console port provides easy access to the module for a temporary connection. Console port communication is used for administration and maintenance purposes from a central office (CO) location. Tasks conducted over a console port include: • Creating the initial connection to the module • Accessing and using all functionality available via the ACLI • Performing in-lab system maintenance (services described below)
Alarm Port	Closes a circuit when a specific alarm level becomes active. The module features an alarm control signal interface that can be used in a CO location to indicate when internal alarms are generated. The appliances use alarm levels that correspond to three levels of service-disrupting incidents.
USB Ports	Provides access to external Flash based memory
Network Management Ports	Used for EMS control, RADIUS accounting, CLI management, SNMP queries and traps, and other management functions

Physical Interface	Description / Use
Signaling and Media Interfaces	Provide network connectivity for signaling and media traffic.

Table 6 – Acme Packet 3820 Interface Descriptions

The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the following table:

FIPS 140-2 Logical Interface	Module Physical Interface	Information Input/Output
Data Input	Network Management Ports Signaling and Media Interfaces	Ciphertext (IPSec, SSH, and TLS packets)
Data Output	Network Management Ports Signaling and Media Interfaces	Ciphertext (IPSec, SSH, and TLS packets)
Control Input	Console Port	Plaintext control input (configuration commands, operator passwords)
Status Output	Network Management Ports Console Ports LEDs	Plaintext status output. Plaintext key output during manual key generation and configuration.
Power	Power Plug On/Off Switch	N/A

Table 7 – Logical Interface / Physical Interface Mapping

2.6 Roles, Services, and Authentication

As required by FIPS 140-2 Level 2, there are two roles (a Crypto Officer role and User 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 table below provides a mapping of default roles in the module to the roles defined by FIPS 140-2:

Operator Role	Summary of Services	FIPS 140-2 Role
User	• View configuration versions and a large amount if statistical data for the system's performance • Handle certificate information for IPSec and TLS functions • Test pattern rules, local policies, and session translations • Display system alarms. • Set the display dimensions for the terminal	Crypto Officer

Operator Role	Summary of Services	FIPS 140-2 Role
Superuser	Allowed access to all system commands and configuration privileges	Crypto Officer
LI Admin	Allowed access to all system commands and configuration privileges, including LI features (if available)	Crypto Officer
Remote IT system	Connect to module for data transmission	User
Unauthenticated user	Allowed access to view status and perform self test	Crypto Officer-2

Table 8 – Role Mapping

2.6.1 Operator Services and Descriptions

The services available to the User and Crypto Officer roles in the module are as follows:

Service and Description	Service Input	Service Output	Key/CSP Access	Roles
Configure Initializes the module for FIPS mode of operation, configure manual keys	FIPS License, Image integrity (HMAC) value Manual key value.	None	HMAC 256-bit key, IPSec Session Keys (TRIPLE-DES) IPSec Session Keys (AES128) IPSec Session Keys (AES256) HMAC 160-bit key 1	Crypto Officer

Service and Description	Service Input	Service Output	Key/CSP Access	Roles
Decrypt Decrypts a block of data Using AES or TRIPLE-DES in FIPS Mode Decrypts a block of data using DES or ARC4 in Non-FIPS mode	Key Encrypted byte stream	Byte stream	TLS Session Keys (TRIPLE-DES) TLS Session Keys (AES128) TLS Session Keys (AES256) TLS Session Keys (DES,ARC4 in Non-FIPS Mode) IPSec Session Keys (TRIPLE-DES) IPSec Session Keys (AES128) IPSec Session Keys (AES256) SSH Session Key (TRIPLE-DES) SSH Session Key (AES128) SSH Session Key (AES256) SSH Session Keys (DES, ARC4 in Non-FIPS Mode) Private Key 2	User

Service and Description	Service Input	Service Output	Key/CSP Access	Roles
Encrypt Encrypts a block of data Using AES or TRIPLE-DES in FIPS Mode Encrypts a block of data using DES or ARC4 in Non-FIPS mode	Key Byte stream	Encrypted byte stream	TLS Session Keys (TRIPLE-DES) TLS Session Keys (AES128) TLS Session Keys (AES256) TLS Session Keys (DES, ARC4 in Non-FIPS Mode) IPSec Session Keys (TRIPLE-DES) IPSec Session Keys (AES128) IPSec Session Keys (AES256) SSH Session Key (TRIPLE-DES) SSH Session Key (AES128) SSH Session Key (AES256) SSH Session Keys (DES, ARC4 in Non-FIPS mode) Public Key 2	User

Service and Description	Service Input	Service Output	Key/CSP Access	Roles
Generate Keys Generates AES or TRIPLE-DES keys for encrypt/decrypt operations in FIPS mode Generates DES or ARC4 keys for encrypt/decrypt operations in Non-FIPS mode	Key Size	AES-Key TRIPLE-DES-Key in FIPS mode DES key and ARC4 Key in Non-FIPS mode	TLS Session Keys (TRIPLE-DES) TLS Session Keys (AES128) TLS Session Keys (AES256) TLS Session Keys (DES, ARC4 in non-FIPS mode) IPSec Session Keys (TRIPLE-DES) IPSec Session Keys (AES128) IPSec Session Keys (AES256) SSH Session Key (TRIPLE-DES) SSH Session Key (AES128) SSH Session Key (AES256) SSH Session Keys (DES, ARC4 in Non-FIPS mode) Public Key 2	User

Key Establishment DH public key for establishing AES or TRIPLE-DES session keys in FIPS mode DH public key for establishing DES or ARC4 session keys in Non-FIPS mode	Key Size	AES-Key TRIPLE-DES-Key in FIPS mode DES key and ARC4 Key in Non-FIPS mode	IPSec Session Keys (TRIPLE-DES) IPSec Session Keys (AES128) IPSec Session Keys (AES256) SSH Session Key (TRIPLE-DES) SSH Session Key (AES128) SSH Session Key (AES256) SSH Session Keys (DES, ARC4 in Non-FIPS mode) Public Key 2	User

Key Establishment DH private key for establishing AES or TRIPLE-DES session keys in FIPS mode DH private key for establishing DES or ARC4 session keys in Non-FIPS mode	Key Size	AES-Key TRIPLE-DES-Key in FIPS mode DES key and ARC4 Key in Non-FIPS mode	IPSec Session Keys (TRIPLE-DES) IPSec Session Keys (AES128) IPSec Session Keys (AES256) SSH Session Key (TRIPLE-DES) SSH Session Key (AES128) SSH Session Key (AES256) SSH Session Keys (DES, ARC4 in Non-FIPS mode) Public Key 2	User
Sign Signs a block with RSA	Data block to sign RSA Private key	RSA Signed data block	Private Key 1 Private Key 2 Public Key 2	User
Verify Verifies the signature of a RSA-signed block	RSA Signed data block RSA Public key	Verification success/failure	Public Key 1 Public Key 2	User
Hash_Drbg seed Generate a entropy_input for Hash_Drbg	HWRNG generated random bits.	entropy_input	entropy_input Public Key 2	User
Hash_Drbg Generate random number.	Working state C and V	Random number	Hash_DRBG V Hash_DRBG Public Key 2	User

Service and Description	Service Input	Service Output	Key/CSP Access	Roles
HMAC Hash-SHA hash based Message Authentication Code in FIPS mode HMAC-MD5 Hash based Message Authentication Code in Non-FIPS mode	Key, data block	HMAC value	HMAC 160-bit key 1 HMAC 160-bit key 2 HMAC 160-bit key 3 HMAC 256-bit key Public Key 2 HMAC-MD5 Key (non-FIPS mode)	User
Zeroize CSPs Clears CSPs from memory	Key, Key pair, entropy_input, password	Invalidated CSP	All CSPs	Crypto Officer

Table 9 – Operator Services and Descriptions

The module provides for the following unauthenticated services, which do not require authentication as they are not security relevant functions. These services do not affect the security of the module; these services do not create, disclose, or substitute cryptographic keys or CSPs, nor do they utilize any Approved security functions.

Service and Description	Service Input	Service Output	Key/CSP Access	Roles
Show Status Shows status of the module	None	Module status enabled/disabled	None	Crypto Officer-2
Initiate self-tests Restarting the module provides a way to run the self-tests on-demand	None	Console display of success/failure. Log entry of success/failure.	None	Crypto Officer-2

Table 10 – Unauthenticated Operator Services and Descriptions

2.6.2 Operator Authentication

2.6.2.1 Crypto-Officer: Password-Based Authentication

In FIPS mode of operation, the module is accessed via Command Line Interface over the Console ports or via SSH or SNMP over the Network Management Ports. Other than status functions

available by viewing LEDs and the LCD panel, the services described in Table 9 – Operator Services and Descriptions are available only to authenticated operators.

Passwords must be a minimum of 6 characters (see Guidance and Secure Operation section of this document). The password can consist of alphanumeric values, {a-zA-Z0-9], yielding 62 choices per character. The probability of a successful random attempt is $1/62^6$, 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 $600/62^6$, which is less than 1/100,000.

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 $3/62^6$ which is less than 1/100,000.

The module will permit an operator to change roles provided the operator knows both the User password and the Crypto Officer password.

2.6.2.2 Certificate-Based Authentication

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

2.7 Physical Security

The module is a multiple-chip standalone module and conforms to Level 2 requirements for physical security. For details on tamper evidence, please see Section 3.1.2 – Placement of Tamper Evidence Labels.

2.8 Operational Environment

The module operates in a limited operational model and does not implement a General Purpose Operating System.

The module meets Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B.

2.9 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters used within the module:

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
TLS Session Keys (TRIPLE-DES)	TRIPLE-DES CBC 168-bit key For encryption / decryption of TLS session traffic Source: Broadcom	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Resetting / rebooting the module or power cycling	Crypto Officer R W D
TLS Session Keys (AES128)	AES CBC 128-bit key For encryption / decryption of TLS session traffic Source: Broadcom	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Resetting / rebooting the module or power cycling	Crypto Officer R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
TLS Session Keys (AES256)	AES CBC 256-bit key For encryption / decryption of TLS session traffic Source: Broadcom	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Resetting / rebooting the module or power cycling	Crypto Officer R W D
IPSec Session Keys (TRIPLE-DES)	TRIPLE-DES CBC 168-bit key Source: HIFN	Manually entered	**Storage**: Non-Volatile RAM in plaintext **Type**: Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: Manual **Output**: None	Manually entering a new value and overwriting the old value	Crypto Officer R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
IPSec Session Keys (AES128)	AES CBC, CTR 128-bit key Source: HIFN	Manually entered	**Storage**: Non-Volatile RAM in plaintext **Type**: Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: Manual **Output**: None	Manually entering a new value and overwriting the old value	Crypto Officer R W D
IPSec Session Keys (AES256)	AES CBC, CTR 256-bit key Source: HIFN	Manually entered	**Storage**: Non-Volatile RAM in plaintext **Type**: Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: Manual **Output**: None	Manually entering a new value and overwriting the old value	Crypto Officer R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
SSH Session Key (TRIPLE-DES)	TRIPLE-DES CBC 168-bit key For encryption / decryption of SSH session traffic Source: Broadcom	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Resetting / rebooting the module or power cycling	Crypto Officer R W D
SSH Session Key (AES128)	AES CBC 128-bit For encryption / decryption of SSH session traffic Source: Broadcom	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Resetting / rebooting the module or power cycling	Crypto Officer R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
SSH Session Key (AES256)	AES CBC 256-bit key For encryption / decryption of SSH session traffic Source: Broadcom	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Resetting / rebooting the module or power cycling	Crypto Officer R W D
Diffie Hellman Public Key	y=g^x mod p component; Generator g is 2 and p is 1024 bits (group-2), 1536 (group-5) and 2048 (group-14) Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: y is ephemeral / p is static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Resetting / rebooting the module or power cycling	Crypto Officer R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
Diffie Hellman Private Key	x component of DH; x is 1024 bits (group-2), 1536 (group-5) and 2048 (group-14) Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Resetting / rebooting the module or power cycling	Crypto Officer R W D
HMAC 160-bit key 1	160-bit HMAC-SHA1 for message verification Source: HIFN	Manually entered	**Storage**: Flash RAM in plaintext **Type**: Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: Manual **Output**: None	Re-formatting flash memory	Crypto Officer R W D
HMAC 160-bit key 2	160-bit HMAC-SHA1 for message verification Source: Broadcom	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Flash RAM in plaintext **Type**: Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Re-formatting flash memory	Crypto Officer R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
HMAC 160-bit key 3	160-bit HMAC-SHA1 for message verification Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Flash RAM in plaintext **Type**: Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Re-formatting flash memory	Crypto Officer R W D
HMAC 256-bit key	80-bit HMAC-SHA256 for integrity check Source: Host Processor	Hard coded	**Storage**: RAM plaintext **Type**: Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Update firmware	Crypto Officer R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
Operator passwords	Alphanumeric passwords externally generated by a human user for authentication to the module. Source: Host Processor	Not generated by the module; defined by the human user of the module	**Storage**: Non Volatile RAM in plaintext **Type**: Static **Association**: controlled by the operating system	**Agreement**: NA **Entry**: Manual entry via console or SSH management session **Output**: In encrypted form only if using RADIUS authentication	Issue command secure_pwd_reset()	Crypto Officer R W D User R W D
Premaster Secret (48 Bytes)	RSA-Encrypted Premaster Secret Message Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: Input during TLS negotiation **Output**: Output to peer encrypted by Public Key	Resetting / rebooting the module or power cycling	Crypto Officer None User None
Master Secret (48 Bytes)	Used for computing the Session Key Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Resetting / rebooting the module or power cycling	Crypto Officer None User None

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
Hash_DRBG V	440 bits long value V used for generating Hash_DRBG Source: Host Processor	Generated as per section 10.1.1.2 of SP 800-90	**Storage**: Volatile RAM in plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Resetting / rebooting the module or power cycling	Crypto Officer None User None
Hash_DRBG C	440 bits long constant C used for generating Hash_DRBG Source: Host Processor	Generated as per section 10.1.1.2 of SP 800-90	**Storage**: Volatile RAM in plaintext **Type:** Ephemeral **Association**: The operating environment is the one and only owner. Relationship is maintained by the operating environment via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Resetting / rebooting the module or power cycling	Crypto Officer None User None
Hash_DRBG Entropy Input String	Input string for DRBG Source: Host Processor	Generated as per section 10.1.1.2 of SP 800-90	**Storage**: Volatile RAM in plaintext **Type:** Ephemeral **Association**: The operating environment is the one and only owner. Relationship is maintained by the operating environment via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Resetting / rebooting the module or power cycling	Crypto Officer None User None

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
Hash_DRBG Seed Value	Seed value for DRBG Source: Host Processor	Generated as per section 10.1.1.2 of SP 800-90	**Storage**: Volatile RAM in plaintext **Type:** Ephemeral **Association**: The operating environment is the one and only owner. Relationship is maintained by the operating environment via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Resetting / rebooting the module or power cycling	Crypto Officer None User None
Public Key 1	RSA Public 2048-bit for verify operations. Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Flash in plaintext **Type:** Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via certificates.	**Agreement**: NA **Entry**: NA **Output**: NA	Not destroyed as it is a public key	Crypto Officer R W D User R

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
Public Key 2	RSA Public 2048-bit for key establishment for TLS sessions. Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Flash in plaintext **Type:** Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via certificates.	**Agreement**: NA **Entry**: NA **Output**: NA	Not destroyed as it is a public key	Crypto Officer R W D User R
Private Key 1	RSA Private 2048-bit for sign operations. Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Flash in plaintext **Type**: Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Re-formatting flash memory	Crypto Officer R W D User R
Private Key 2	RSA Private 2048-bit for key establishment [1] for TLS sessions Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Flash in plaintext **Type**: Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Re-formatting flash memory	Crypto Officer R W D User R

R = Read W = Write D = Delete

[1] Key establishment methodology provides at least 112-bits of encryption strength

Table 11 – Key/CSP Management Details

Public keys are protected from unauthorized modification and substitution. The module ensures only authenticated operators have access to keys and functions that can generate keys. Unauthenticated operators do not have write access to modify, change, or delete a public key. For the session certificate, the module generates a PKCS10 certificate request (PKCS 10), and a standard Certificate Authority (CA) generates the certificate.

All keys can be zeroized by the Crypto Officer using the Zeroize CSPs service. The Crypto Officer can also return the module to Oracle Communications, where it can be reimaged. The reimaging process at Oracle also zeroizes all CSPs but is a different feature than the Zeroize CSPs service that is available to the Crypto Officer.

2.10 Self-Tests

The module includes an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly. In the event of any self-test failure, the module will output an error dialog and will shutdown. When the module is in an error state, no keys or CSPs will be output and the module will not perform cryptographic functions.

The module does not support a bypass function.

The following sections discuss the module's self-tests in more detail.

2.10.1 Power-On Self-Tests

Power-on self-tests are run upon every initialization of the module and if any of the tests fail, the module will not initialize. The module will enter an error state and no services can be accessed by the users. The module implements the following power-on self-tests:

Implementation	Self Tests Run
Hifn 8450	• TRIPLE-DES known answer test • AES known answer test • HMAC-SHA1 known answer test[2]
BCM5862	• TRIPLE-DES known answer test • AES known answer test • SHA1 known answer test • HMAC-SHA1 known answer test
Intel Celeron M 440	• SHA1 and SHA256 known answer test • HMAC-SHA1 and HMAC-SHA256 known answer test • Hash_DRBG test • DRBG Health Test as specified in SP 800-90 Section 11.3 • Module integrity check using HMAC-SHA256 • RSA known answer test

Table 12 - Power-On Self-Tests

The module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module in FIPS Mode of Operation.

2.10.1.1 Status Output

An operator can discern that all power-on self-tests have passed via normal operation of the module and the following log message.

[2] Note: According to the CMVPFAQ p.57 "If a KAT is implemented for the HMAC-SHA-1, a KAT is not needed for the underlying SHA-1."

```
FIPS: KAT self test completed successfully.
FIPS: System is currently operating in FIPS 140-2
compatible mode.
```

In the event a POST fails, the module will output the following log message:

```
FIPS: ERROR - System is not in FIPS 140-2 compatible mode
FIPS: ERROR - <Test Name> failed.
```

For example:

```
FIPS: ERROR - RSA pair wise consistency test failed.
```

Note that data output will be inhibited while the module is in an error state (i.e., when a POST fails). No keys or CSPs will be output when the module is in an error state.

2.10.2 Conditional Self-Tests

Conditional self-tests are test that run continuously during operation of the module. If any of these tests fail, the module will enter an error state. The module can be re-initialized to clear the error and resume FIPS mode of operation. No services can be accessed by the operators. The module performs the following conditional self-tests:

Implementation	Self Tests Run
Hifn 8450	• None (not applicable)
BCM5862	• Continuous HWRNG test
Intel Core Duo T2500	• Manual key entry test on manually-entered IPSec hash authentication and data encryption keys via duplicate entry verification • Continuous Hash_DRBG test • Continuous test on output of seed mechanism • RSA pairwise consistency test for sign/verify and encrypt/decrypt

Table 13 – Conditional Self-Tests

The module does not perform a firmware load test because no additional firmware can be loaded in the module while operating in FIPS mode.

2.10.2.1 Status Output

In the event a conditional self-test fails, the module will output the following log message:

```
FIPS: ERROR - System is not in FIPS 140-2 compatible mode
FIPS: ERROR - <Conditional Test Name> failed.
```

For example:

```
FIPS: ERROR - Continuous RNG test failed.
```

Note that data output will be inhibited while the module is in this error state. The module will self-correct this use case as follows:

Test	Remediation
Pairwise consistency test for RSA implementations	Generate a new RSA keypair and rerun test
Continuous test run on output of FIPS-approved Hash_DRBG in firmware	Generate a new value and rerun test
Continuous test on output of FIPS-approved Hash_DRBG in firmware seed mechanism	Generate a new value and rerun test
Manual key entry test on manually-entered IPSec hash authentication and data encryption keys	Prompt operator to re-enter value

Table 14 – Conditional Self Tests and Module Remediation

No keys or CSPs will be output when the module is in an error state.

2.11 Mitigation of Other Attacks

The module does not mitigate attacks.

3 Guidance and Secure Operation

This section describes how to configure the module for FIPS mode of operation. Operating the module without maintaining the following settings will remove the module from the FIPS mode of operation.

3.1 Crypto Officer Guidance

3.1.1 Enabling FIPS Mode and General Guidance

FIPS Mode is enabled by a license key installed by Oracle, which will open/lock down features where appropriate.

Additionally, the Crypto Officer must configure and enforce the following initialization procedures in order to operate in FIPS mode of operation[3]:

- Verify that the firmware version of the module is Version C6.3. No other version can be loaded or used in FIPS mode of operation.
- Ensure all media traffic is encapsulated in an IPSec or TLS tunnel as appropriate.
- Ensure all management traffic is encapsulated within an SSH session (i.e., Telnet should not be used in FIPS mode of operation).
- Ensure USB ports are not used in FIPS mode of operation.
- Ensure that the tamper evidence labels are applied by Oracle as specified in Section 3.1.2 – Placement of Tamper Evidence Labels. The tamper evident labels shall be installed for the module to operate in a FIPS mode of operation.
- Inspect the tamper evident labels periodically to verify they are intact and the serial numbers on the applied tamper evident labels match the records in the security log.
- All operator passwords must be a minimum of 6 characters in length.
- When using RADIUS for authentication, ensure a secure tunnel (via IPSec or TLS) is established between the module and the RADIUS server.
- Booting from an external device is not allowed in FIPS mode of operation. The image must be booted from flash memory, which is configured with the following command:

[3] The licensing may ensure most of these are met. The Crypto Officer should verify all details prior to operation in FIPS mode.

```
ACMEPACKET# configure terminal
ACMEPACKET# bootparam
```

- Ensure use of FIPS-approved algorithms for TLS v1.0:

```
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.

- Ensure only FIPS-approved algorithms are used for IPSec sessions:

```
Triple-DES
AES128CBC
AES256CBC
AES128CTR
AES256CTR
HMAC-SHA1
```

- Ensure the console windows used while manually entering keys are closed immediately after the configuration is complete.

- Do not disclose passwords and store passwords in a safe location and according to his/her organization's systems security policies for password storage.

3.1.2 Placement of Tamper Evidence Labels

To meet Physical Security Requirements for Level 2, the module enclosure must be protected with tamper evidence labels. The tamper evident labels shall be installed for the module to operate in a FIPS mode of operation. Oracle Communications applies the labels at time of manufacture; the Crypto Officer is responsible for ensuring the labels are applied as shown below. Once applied, the Crypto Officer shall not remove or replace the labels unless the module has shown signs of tampering. In the event of tampering or wear and tear on the labels, the Crypto Officer shall return the module to Oracle Communications, where it will be reimaged and returned with a new set of labels.

The Crypto Officer is responsible for

- Verifying the five labels are attached to the appliance as shown in the diagrams below,

- Maintaining the direct control and observation of any changes to the module such as reconfigurations to ensure the security of the module is maintained during such changes.

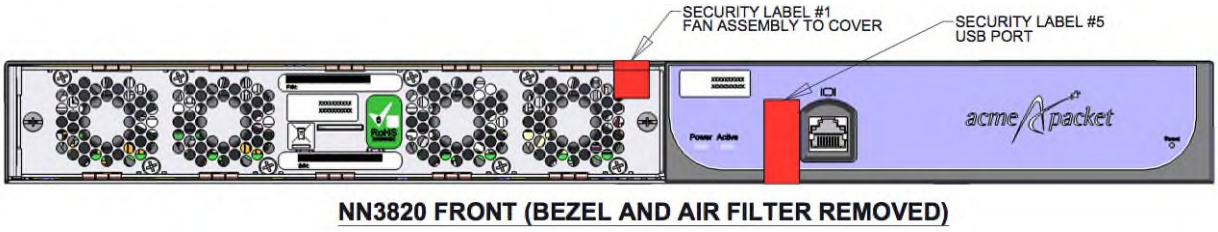

Figure 2 – Tamper Evidence Label Placement / Front

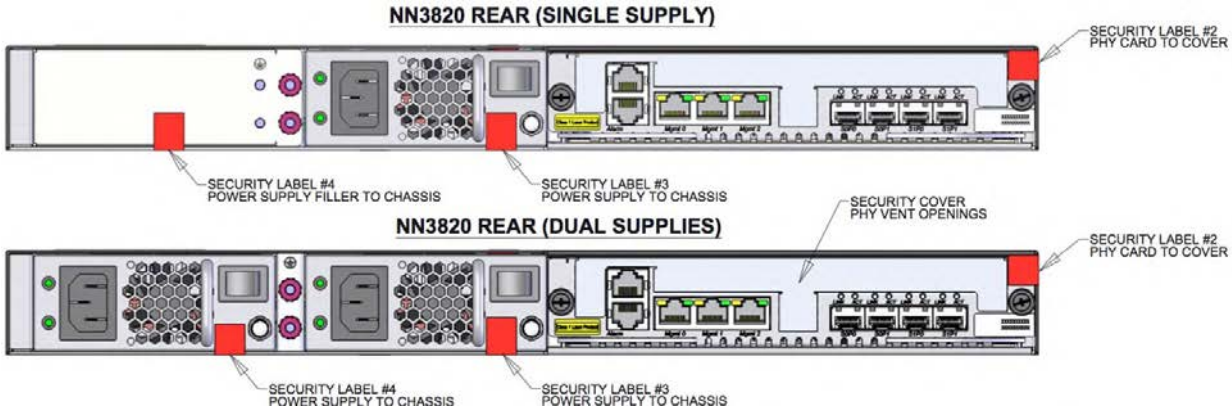

Figure 3 – Tamper Evidence Label Placement / Rear

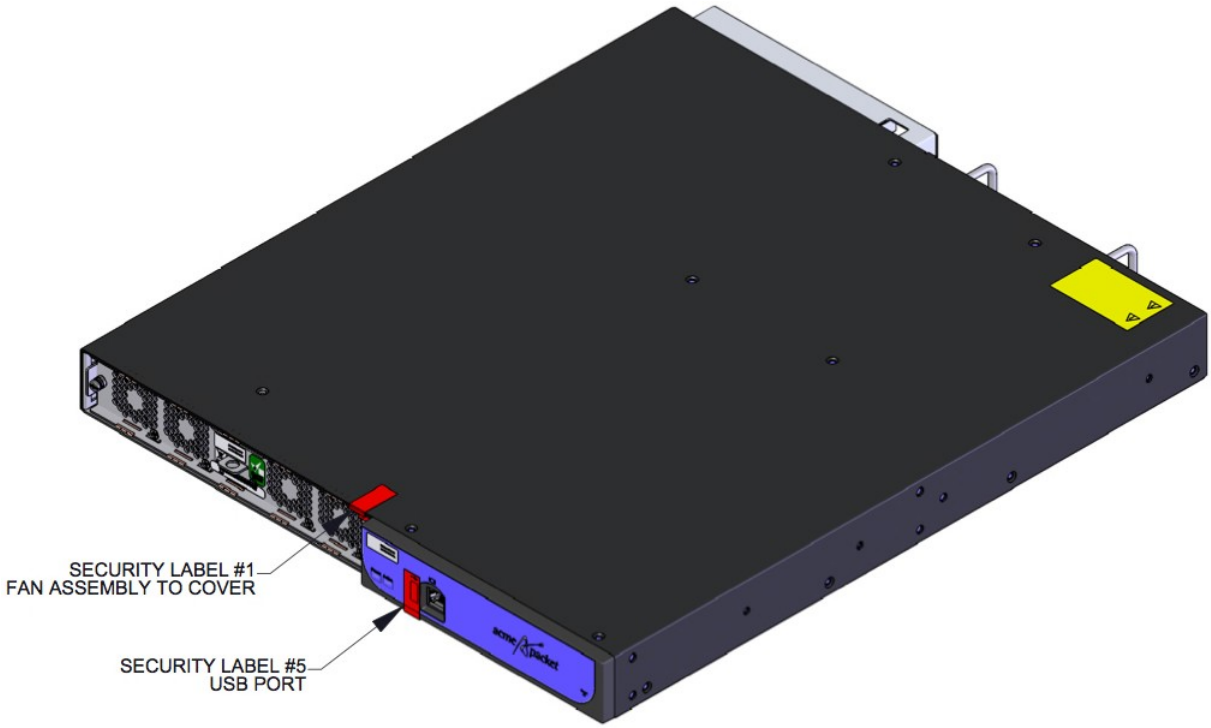

Figure 4 – Tamper Evidence Label Placement Top/Front

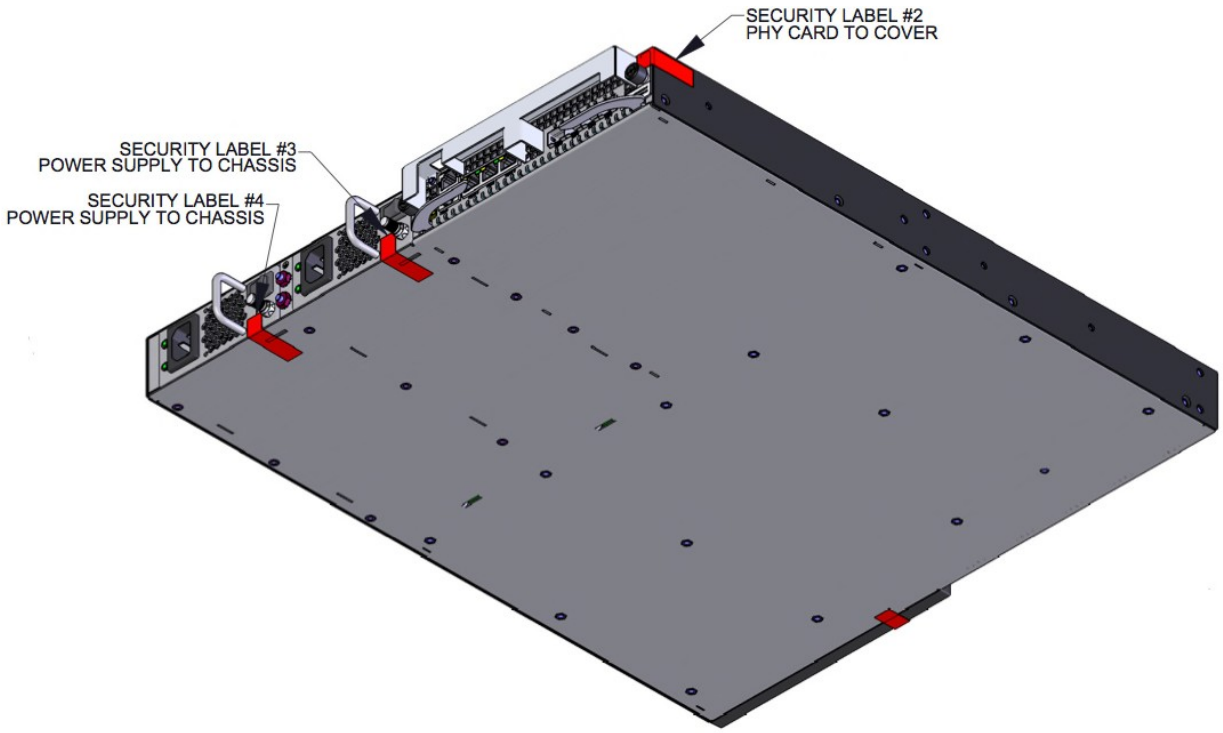

Figure 5 – Tamper Evidence Label Placement Bottom/Rear

Note that Oracle Communications does offer the purchase of additional labels. If labels need to be replaced, please contact Oracle Communications to return the module for reimaging, and Oracle Communications will reimage the module and provide additional label (internal part number LBL-0140-60). To apply replacement labels, see instructions at the beginning of this section.

3.2 User Guidance

3.2.1 General Guidance

The User must not disclose passwords and must store passwords in a safe location and according to his/her organization's systems security policies for password storage.

End of Document
