Cisco 3271 High Performance Mobile Access Router Card (HMARC)

FIPS 140-2
Non-Proprietary Security Policy

Level 2 Validation
Version 1.2

May 12, 2009

© Copyright 2009 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Table of Contents

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

1 Introduction

1.1 Purpose

This is the non-proprietary Cryptographic Module Security Policy for the Cisco 3271 High Performance Mobile Access Router Card. This security policy describes how the 3271 High Performance Mobile Access Router Card (Hardware Version: A0; Firmware Version: 12.4(15)T7) meet the security requirements of FIPS 140-2, and how to operate in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the Cisco 3271 High Performance Mobile Access Router Card.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/index.html.

1.2 References

This document deals only with operations and capabilities of the 3271 High Performance Mobile Access Router Card in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the 3271 Mobile Access Router Card from the following sources:

- The Cisco Systems website contains information on the full line of products at www.cisco.com. The 3200 Series product descriptions can be found at: http://www.cisco.com/en/US/products/hw/routers/ps272/index.html.
- For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.
- The NIST Validated Modules website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) contains contact information for answers to technical or sales-related questions for the module

1.3 Terminology

In this document, the Cisco 3271 High Performance Mobile Access Router Card is referred to as the Cisco 3271 Mobile Access Router Card, 3271 Router, the router or the module.

1.4 Document Organization

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

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

This document provides an overview of the Cisco 3271 Mobile Access Router Card and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the 3271 Mobile Access Router

© Copyright 2009 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Card. Section 3 specifically addresses the required configuration for the FIPS-Approved mode of operation.

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

© Copyright 2009 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2 The Cisco 3271 High Performance Mobile Access Router Card

The Cisco 3271 High performance Mobile Access Router Cards (HMARC) are high-performance IOS Mobile Router cards that enable customers deliver solutions primarily for the DoD, Defense, Homeland Security, Commercial Transportation and Public Safety markets. These router cards use the Cisco IOS Mobile Networks feature as the foundation for delivering new mobile applications.

The Cisco 3271 Mobile Access Router Card along with the other Network interface cards (such as WMIC, FESMIC and SMIC) extend the edge of the IP network to a new frontier of Networks-in-Motion and facilitates new and existing applications in the defense, public safety, homeland security, and commercial transportation markets.

The Cisco 3271 High Performance Mobile Access Router Cards provide a scalable, secure, manageable router platform that meets FIPS 140-2 Level 2 requirements. This section describes the general features and functionality provided by the Cisco 3271 Mobile Access Router Card.

2.1 The 3271 Cryptographic Module

The 3271 High Performance Mobile Access Router card is a multi-chip embedded cryptographic module. The cryptographic boundary is the High Performance Mobile Access Router Card ("HMARC") and is defined by the exterior surfaces of the thermal plates surrounding the module and the module's connectors. The connectors include the 34-pin multifunction header, the 10-pin Ethernet header, the USB LEDs header ports, the upper and lower PCI bus, and the upper and lower ISA bus. All of the functionality discussed in this document is provided by components within this cryptographic boundary.

The evaluated platform of 3271 HMARC consists of two configurations: The configuration with Hardware Number C3271MARC-TP has two 10/100/1000 Mbps Copper Ethernet ports. The configuration with hardware number C3271MARC-FO-TP has one 10/100/1000 Mbps Copper Ethernet port and one 100/1000 Mbps Fiber Optic Ethernet port.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

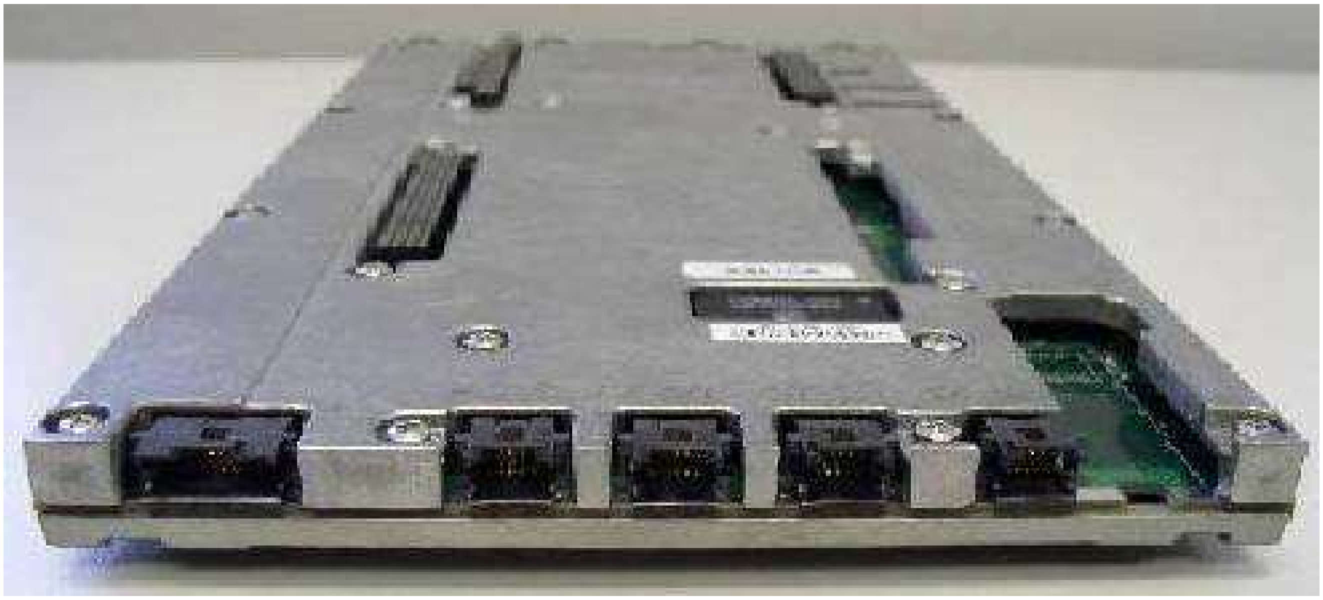

Figure 1 -The 3271 HMARC with two 10/100/1000 Mbps Copper Ethernet ports

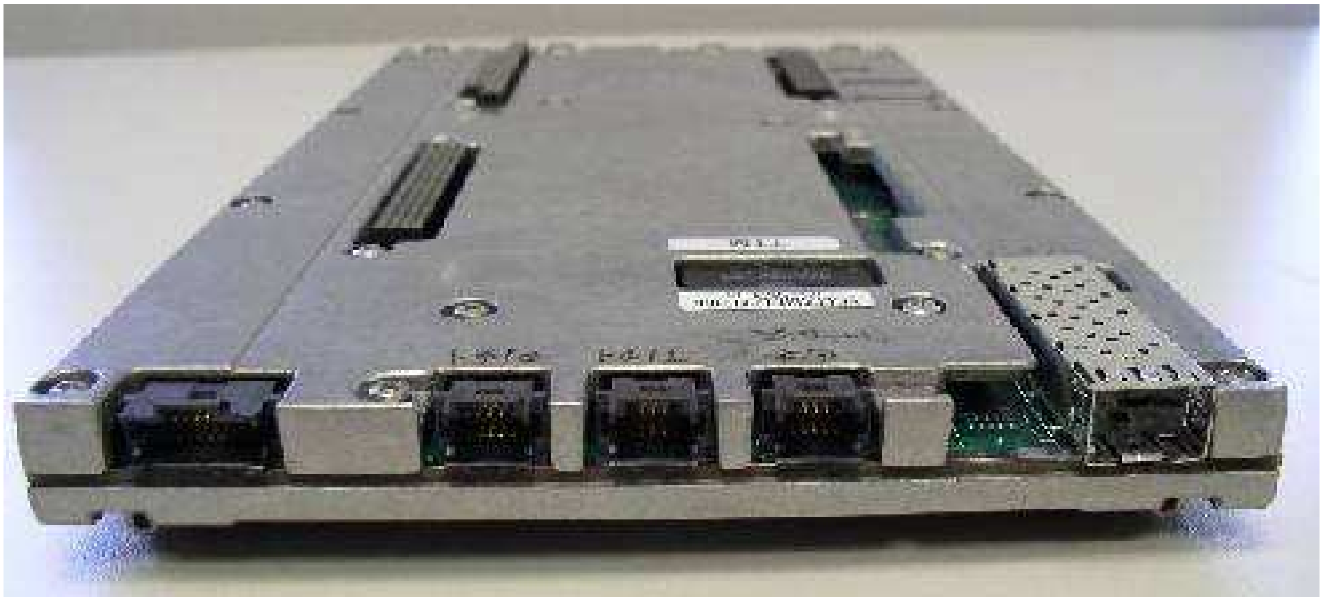

Figure 2 -The 3271 HMARC with one 10/100/1000 Mbps Copper Ethernet port and one 10/100/1000 Mbps Fiber Optics Ethernet port

2.2 Module Interfaces

The Cisco 3271 High Performance Mobile Access Router Cards feature a multifunctional header interface, which provides functionality to connect a console port, auxiliary ports, and system and network LEDs. The module also provides the ability to add network modules and other interface cards via the PC/104-Plus PCI interface.

© Copyright 2009 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

The physical interfaces include an ISA interface but the card does not send or receive any data, control, or status information via the ISA interface – it provides a physical connection only (although the module will allow data used by other units to pass through the ISA bus). The PC/104-Plus PCI interface provides power to the module from the power card, as well as communications with other units. The module also has an RS-232 connector for a console terminal for local system access. The router also has a multifunctional header interface which provides status via LED indicators whose status indicators are provided in Table 1:

LED	Indication	Description
ETHERNET LEDs	ON	Link with partner
	OFF	No Link with partner
	BLINKING	Transmitting or receiving packet
USB LEDs	ON	Link with downstream USB device
	OFF	No link with downstream USB device
	BLINKING	Transmitting or receiving packet
AUX/CONSOLE LEDs	ON	Link with partner
	OFF	No link with partner
	BLINKING	Transmitting or receiving packet
ZEROIZATION LED	ON	Zeroization complete
	OFF	Not activated
	BLINKING	Zeroization in process
THERMAL WARNING LED	ON	Thermal reading is out of range
	OFF	Thermal reading is within the range
	BLINKING	Thermal reading is far out of range such as high as 105C. At this stage all chips in the system may be exposed to permanent damages.

Table 1 – 3271 LEDs Descriptions

Each 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 Table 2

Router Card Physical Port	FIPS 140-2 Logical Interface
10/100 Mbps Ethernet ports 10/100/1000 Mbps Copper Ethernet ports 100/1000 Mbps Fiber Optic Ethernet port Multifunctional Header PC/104-Plus PCI Interface USB header port	Data Input Interface
10/100 Mbps Ethernet ports 10/100/1000 Mbps Copper Ethernet pports 100/1000 Mbps Fiber Optic Ethernet port Multifunctional Header PC/104-Plus PCI Interface USB header port	Data Output Interface

© Copyright 2009 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Router Card Physical Port	FIPS 140-2 Logical Interface
10/100 Mbps Ethernet ports 10/100/1000 Mbps Copper Ethernet ports 100/1000 Mbps Fiber Optic Ethernet port Multifunctional Header PC/104-Plus PCI Interface	Control Input Interface
Multifunctional Header 10/100 Mbps Ethernet ports 10/100/1000 Mbps Copper Ethernet ports 100/1000 Mbps Fiber Optic Ethernet port PC/104-Plus PCI Interface USB LEDs header port	Status Output Interface
PC/104-Plus PCI Interface	Power Interface

Table 2 – FIPS 140-2 Logical Interfaces

2.3 Roles and Services

Authentication is role-based. There are two main roles in the router that operators may assume: the Crypto Officer role and the User role. The administrator of the router assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services. Both roles are authenticated by providing a valid password. The configuration of the encryption and decryption functionality is performed only by the Crypto Officer after authentication to the Crypto Officer role by providing a valid Crypto Officer username and password. Once the Crypto Officer configured the encryption and decryption functionality, the User can use this functionality after authentication to the User role by providing a valid User username and password. The Crypto Officer can also use the encryption and decryption functionality after authentication to the Crypto Officer role. The module supports RADIUS and TACACS+ for authentication and they are used in the FIPS mode. The RSA digital signature authentication mechanism is used to authenticate the User role via IPSec/IKE protocol implementation. A complete description of all the management and configuration capabilities of the Cisco 3271 High Performance Mobile Access Router Card can be found in the *Performing Basic System Management* manual and in the online help for the router.

The User and Crypto Officer passwords and the RADIUS/TACACS+ shared secrets must each be at least 8 alphanumeric characters in length. See Section 3, Secure Operation of the Cisco 3271 High Performance Mobile Access Router, for more information. The probability of randomly guessing the correct sequence is 1 in 208,827,064,576. To have a 1 in 100,000 chance of guessing the password in one minute, an attacker would need to be able to guess 34000 passwords per second, which far exceeds the operational capability of the module. Including the rest of the alphanumeric characters drastically decreases the odds of guessing the correct sequence.

When using RSA based authentication, RSA key pair has modulus size of 1024 bit to 2048 bit, thus providing between 80 bits and 112 bits of strength. Assuming the low end of that range, an attacker would have a 1 in 2^{80} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of

© Copyright 2009 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

approximately 1.8x10^{21} attempts per minute, which far exceeds the operational capabilities of the modules.

2.3.1 Crypto Officer Services

During initial configuration of the router, the Crypto Officer password (the "enable" password) is defined. A Crypto Officer may assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration and maintenance of the router. The Crypto Officer services consist of the following:

- **Configure the router**: define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.
- **Define Rules and Filters**: create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- **Status Functions**: view the router configuration, routing tables, active sessions, use Gets to view SNMP MIB II statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status
- **Manage the router**: log off users, shutdown or reload the router, manually back up router configurations, view complete configurations, manager user rights, and restore router configurations.
- **Set Encryption/Bypass**: set up the configuration tables for IP tunneling. Set keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.
- **Change Interface Cards:** Insert and remove interface cards.
- **Perform Self Tests:** Perform self tests

The Crypto Officer role also has access to all user role services.

2.3.2 User Services

A User enters the system by accessing the console port CLI, or SSHv2, Telnet over IPSec and SNMP over IPSec. The module prompts the User for a password or authenticates them via RSA digital signatures. The services available to the User role consist of the following:

- **Status Functions**: view state of interfaces, state of layer 2 protocols, version of IOS currently running
- **Network Functions**: connect to other network devices (via outgoing telnet or PPP) and initiate diagnostic network services (*i.e.*, ping, mtrace)
- **Terminal Functions:** adjust the terminal session (e.g., lock the terminal, adjust flow control)
- **Directory Services**: display directory of files kept in flash memory

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.3.3 Unauthenticated Services

The only services available to someone without an authorized role are:

- **Viewing the status output from the module’s LED pins**
- **Power Cycling**
- **Bypass services**

2.4 Physical Security

The entire contents of the module, including all hardware, and firmware are enclosed in thermal plates that cover the circuitry of the module. In order to meet FIPS 140-2 Level 2 physical security requirements, the thermal plates must be sealed using tamper-evident labels, which prevent the plates from being removed without signs of tampering. To maintain FIPS 140-2 compliance, the Crypto Officer must attach tamper evident labels as shown in the photographs below.

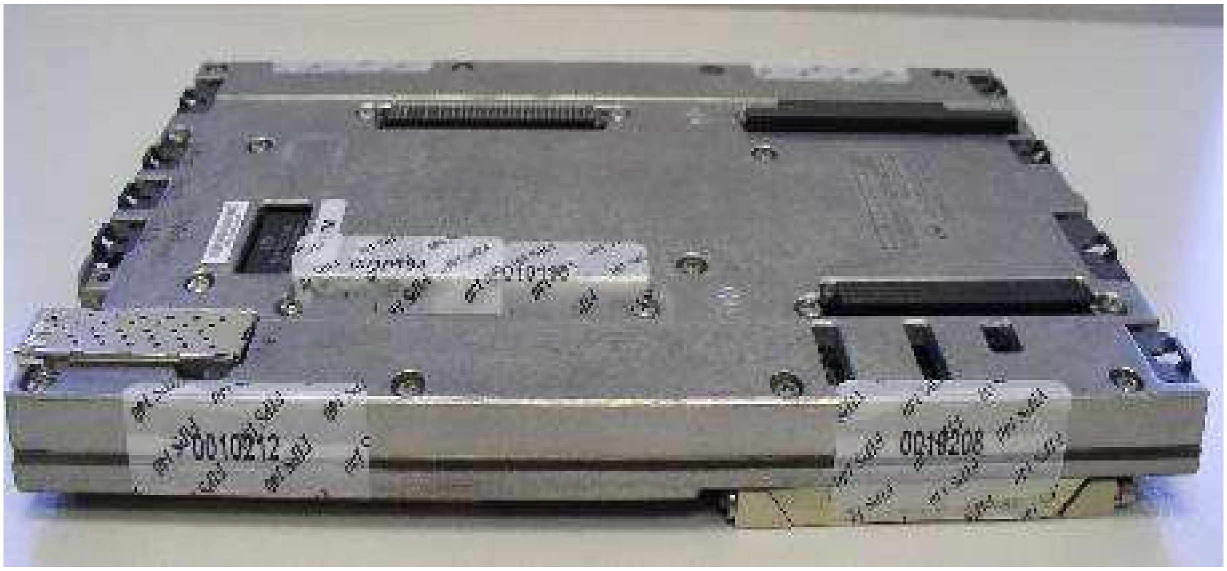

Figure 3 -The 3271 HMARC with Tamper Evidence Labels on the thermal plates

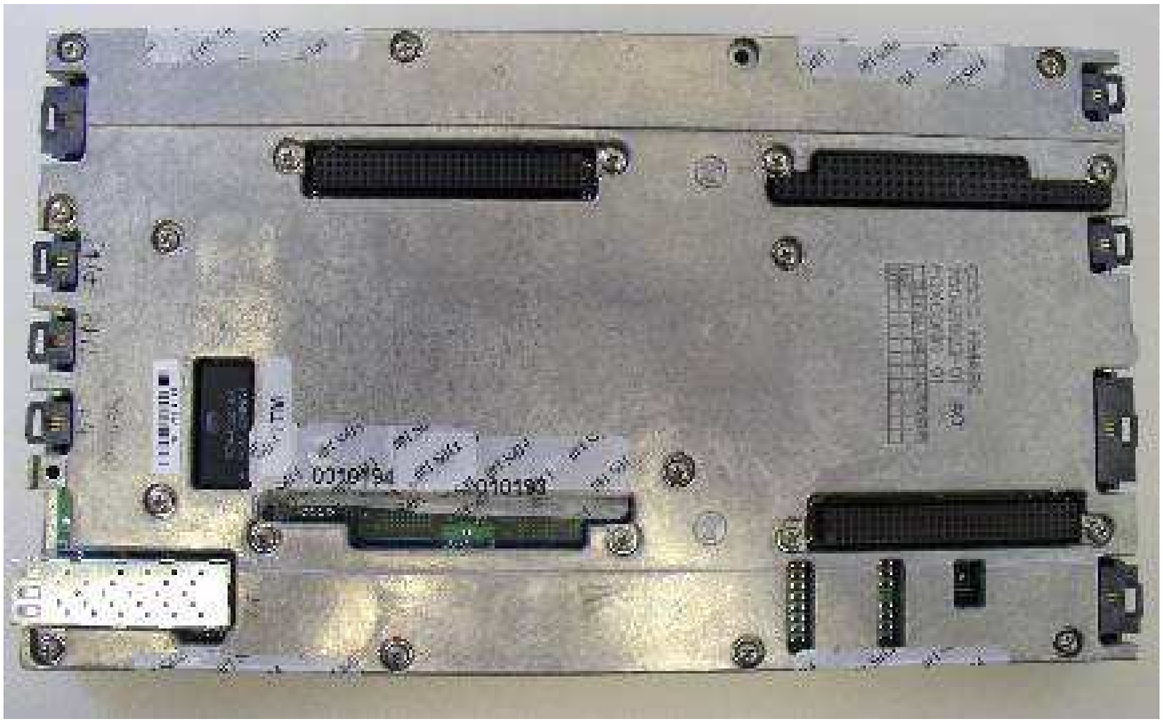

Figure 4 -The 3271 HMARC with Tamper Evidence Labels – Top View

The tamper evidence seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the thermal plates will damage the tamper evidence seals. Since the tamper evidence seals have non-repeated serial numbers, they can be inspected for damage and compared against the applied serial numbers to verify that the module has not been tampered. Tamper evidence seals can also be inspected for signs of tampering, which include the following: curled corners, bubbling, crinkling, rips, tears, and slices.

The following components are excluded from the FIPS 140-2 standard security requirements:

- Ethernet Transformer
- Capacitor (s)
- DC-DC Converters
- Pull Up/Down Resistors

2.5 Cryptographic Key Management

The router securely administers both cryptographic keys and other critical security parameters such as passwords. All keys and CSPs are also protected by the password-protection on the Crypto Officer role login, and can be zeroized by the Crypto Officer. Keys can be distributed manually or exchanged electronically via Internet Key Exchange (IKE).

The module supports the following critical security parameters (CSPs):

© Copyright 2009 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

CSP NAME	Algorithm	Description	Storage
PRNG seed	ANSI X9.31 Appendix A.2.4 using the 2-key Triple DES	This is the seed for the X9.31 PRNG. This key is stored in SDRAM and updated periodically after the generation of 400 bytes; hence, it is zeroized periodically. Also, the operator can turn off the router to zeroize this key.	SDRAM (plaintext)
PRNG seed key	ANSI X9.31 Appendix A.2.4 using the 2-key Triple DES	This is the seed key for X9.31 PRNG. This key is stored in SDRAM and updated periodically after the generation of 400 bytes; Again, the same zeroization method as above.	SDRAM (plaintext)
Diffie Hellman private exponent	DH (1024/1536/2048/4096 bits)	The public and private exponents used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated.	SDRAM (plaintext)
Diffie Hellman shared secret	Shared secret	This key is derived during DH algorithm implementation. The operator can turn off the router to zeroize this key	SDRAM (plaintext)
skeyid	Keyed SHA-1	Value derived from the shared secret within IKE exchange. Zeroized when IKE session is terminated.	SDRAM (plaintext)
skeyid_d	Keyed SHA-1	The IKE key derivation key for non ISAKMP security associations. The zeroization is the same as above.	SDRAM (plaintext)
IKE session encrypt key	TDES (Key Size 192 bits)/AES (AES Key Size 128/192/256 bits)	The IKE session encrypt key. The zeroization method is the same as above.	SDRAM (plaintext)
IKE session authentication key	HMAC-SHA-1	The IKE session authentication key. The zeroization method is the same as above.	SDRAM (plaintext)
RSA private key	RSA (Key Size 1024/1536/2048 bits)	The RSA private key. “Crypto key zeroize” command zeroizes this key.	NVRAM (plaintext)
IPSec encryption key	TDES (Key Size 192 bits)/AES (Key Size 128/192/256 bits)	The IPSec encryption key. Zeroized when IPSec session is terminated.	SDRAM (plaintext)
IPSec authentication key	HMAC-SHA-1	The IPSec authentication key. The zeroization method is the same as above.	SDRAM (plaintext)
Router authentication key 1	Shared secret (8+ characters)	This key is used by the router to authenticate itself to the peer. The router itself gets the password (that is used as this key) from the AAA server and sends it onto the peer. The password retrieved from the AAA server. It is zeroized upon completion of the authentication attempt.	SDRAM (plaintext)

© Copyright 2009 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

CSP NAME	Algorithm	Description	Storage
PPP authentication key	Shared Secret (8+ characters)	The authentication key used in PPP. This key is in the SDRAM and not zeroized at runtime. One can turn off the router to zeroize this key because it is stored in SDRAM.	SDRAM (plaintext)
Router authentication key 2	Shared Secret (8+ characters)	This key is used by the router to authenticate itself to the peer. The key is retrieved from the local database (on the router itself). Issuing the "no username password" zeroizes the password (that is used as this key) from the local database.	NVRAM (plaintext)
SSH RSA private key	RSA (Key Size 1024/1536/2048 bits)	This key is used for signature signing when performing SSH authentication. "Crypto key zeroize" command zeroizes this key.	NVRAM (plaintext)
SSH session key	TDES (Key Size 192 bits)/AES (Key Size 128/192/256 bits)	This is the SSH session key. It is zeroized when the SSH session is terminated.	SDRAM (plaintext)
SSH session authentication key	HMAC-SHA-1	This key is used to perform authentication between the SSH client and SSH server. It is zeroized when the SSH session is terminated.	SDRAM (plaintext)
User password	Shared secret	The password of the User role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
Enable password	Shared secret	The plaintext password of the CO role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
Enable secret	Shared secret	The ciphertext password of the CO role. However, the algorithm used to encrypt this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
RADIUS secret	Shared secret (8+ characters)	The RADIUS shared secret. This shared secret is zeroized by executing the "no" form of the RADIUS shared secret set command.	NVRAM (plaintext)
TACACS+ secret	Shared secret (8+ characters)	The TACACS+ shared secret. This shared secret is zeroized by executing the "no" form of the TACACS+ shared secret set command.	NVRAM (plaintext)

Table 3 – Critical Security Parameters

The services accessing the CSPs, the type of access and which role accesses the CSPs are listed below.

© Copyright 2009 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

SRDI/Role/Service Access Policy	Security Relevant Data Item	PRNG seed	PRNG seed key	Diffie Hellman private exponent	Diffie Hellman shared secret	skeyid	skeyid_d	IKE session encrypt key	IKE session authentication key	RSA private key	ISAKMP preshared	IPSec encryption key	IPSec authentication key	Router authentication key 1	PPP authentication key	Router authentication key 2	SSH Private key	SSH session key	SSH session authentication key	User password	Enable password	Enable secret	RADIUS secret	TACACS+ secret
Role/Service																								
User role																								
Status Functions																								
Network Functions		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r				
Terminal Functions																								
Directory Services																								
Crypto-Officer Role																								
Configure the Router																r w d								
Define Rules and Filters																								
Status Functions																								
Manage the Router		d	d											r w d	d					r w d	r w d	r w d	r w d	r w d
Set Encryption/Bypass		r w d	r w d	rwd	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d		r w		r w d	r w d	r w d					
Change Interface Cards																								
Perform Self Tests																								

Table 4 – Role and Service Access to CSPs

© Copyright 2008 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.6 Approved Cryptographic Algorithms

The module supports firmware IOS implementations of the following FIPS approved algorithms:

- AES (Cert. #890)
- HMAC SHA-1 (Cert. #497)
- RNG based on ANSI X9.31 Appendix A.2.4 Using the 2-Key Triple DES algorithm. (Cert. #511)
- RSA (Sign/Verify) (Cert. #432)
- SHA-1 (Cert. #881)
- Triple-DES (Cert. #727)

The module supports hardware implementations of the following FIPS approved algorithms:

- AES (Cert. #945)
- SHA-1 (Cert. #920)
- Triple-DES (Cert. #749)
- HMAC SHA-1 (Cert. #530)

2.7 Non-FIPS Approved Algorithms Allowed in FIPS Mode

The module supports the following non-FIPS approved algorithms which are permitted for use in the FIPS approved mode:

- Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 156 bits of encryption strength)

2.8 Non-FIPS Approved Algorithms

The module supports the following non-FIPS approved algorithms and hence these are disabled when operating in the FIPS mode:

- DES (IOS)
- DES-MAC (IOS)
- TDES-MAC (IOS)
- MD5 (IOS, hardware)
- MD4 (IOS)
- HMAC MD5 (IOS)

2.9 Key Management Schemes

The module supports three types of key management schemes:

1. Pre-shared key exchange via electronic key entry. Triple-DES/AES key and HMAC-SHA-1 key are exchanged and entered electronically.

2. The IKE method with support for exchanging pre shared keys manually and entering electronically.
    - The pre-shared keys are used with Diffie-Hellman key agreement technique to derive Triple-DES or AES keys.
    - The pre-shared key is also used to derive HMAC-SHA-1 key.

© Copyright 2008 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

3. The Internet Key Exchange with RSA-signature authentication.

The module supports commercially available methods of key establishment, including Diffie-Hellman and IKE.

All pre-shared keys are associated with the CO role that created the keys, and the CO role is protected by a password. Therefore, the CO password is associated with all the pre-shared keys. The Crypto Officer needs to be authenticated to store keys. All Diffie-Hellman (DH) keys agreed upon for individual tunnels are directly associated with that specific tunnel only via the IKE protocol.

2.10 Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The router includes an array of self-tests that are run during startup and periodically during operations. If any of the self-tests fail, the router transitions into an error state. Within the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

Power-up tests on IOS firmware

- Firmware integrity test
- RSA KAT (both signature and verification)
- AES KAT
- Triple-DES KAT
- SHA-1 KAT
- PRNG KAT
- Power-up bypass test
- HMAC SHA-1 KAT

Conditional tests on IOS firmware

- Conditional bypass test
- Pairwise consistency test on RSA key generation
- Continuous random number generator tests

Power-up tests on the hardware security engine

- AES KAT
- Triple-DES KAT
- Diffie-Hellman self-test
- HMAC SHA-1 KAT

© Copyright 2008 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

3 Secure Operation of the Cisco 3271 High Performance Mobile Access Router Cards

The Cisco 3271 High Performance Mobile Access Router Card meets all of the Level 2 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in FIPS mode. Operating this router without maintaining the following settings will remove the module from the FIPS approved mode of operation.

3.1 Initial Setup

1. The Crypto Officer must disable IOS Password Recovery by executing the following commands:

   ```
   configure terminal
   no service password-recovery
   end
   show version
   ```

   NOTE: Once Password Recovery is disabled, administrative access to the module without the password will not be possible.

3.2 System Initialization and Configuration

1. The Crypto Officer must perform the initial configuration. IOS version 12.4(15)T7 is the only allowable image; no other image may be loaded.
2. The value of the boot field must be 0x0101 (the factory default). This setting disables break from the console to the ROM monitor and automatically boots the IOS image. From the “configure terminal” command line, the Crypto Officer enters the following syntax:

   ```
   config-register 0x0101
   ```

3. The Crypto Officer must create the “enable” password for the Crypto Officer role. The password must be at least 8 characters and is entered when the Crypto Officer first engages the “enable” command. The Crypto Officer enters the following syntax at the “#” prompt:

   ```
   enable secret [PASSWORD]
   ```

4. The Crypto Officer must always assign passwords (of at least 8 characters) to users. Identification and authentication on the console port is required for Users. From the “configure terminal” command line, the Crypto Officer enters the following syntax:

   ```
   line con 0
   password [PASSWORD]
   login local
   ```

5. The Crypto Officer shall only assign users to a privilege level 1 (the default).
6. The Crypto Officer shall not assign a command to any privilege level other than its default.

7. The Crypto Officer may configure the module to use RADIUS or TACACS+ for authentication. Configuring the module to use RADIUS or TACACS+ for authentication is optional. If the module is configured to use RADIUS or TACACS+, the Crypto-Officer must define RADIUS or TACACS+ shared secret keys that are at least 8 characters long.
8. Loading any IOS image onto the router is not allowed while in FIPS mode of operation.

3.3 IPSec Requirements and Cryptographic Algorithms

1. There are two types of key management method that are allowed in FIPS mode: Internet Key Exchange (IKE) and IPSec manually entered keys.
2. Although the IOS implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:
    - ah-sha-hmac
    - esp-sha-hmac
    - esp-Triple-DES
    - esp-aes
3. The following algorithms are not FIPS approved and should be disabled:
    - MD-5 for signing
    - MD-5 HMAC
    - DES

3.4 Protocols

1. SNMP v3 over a secure IPSec tunnel may be employed for authenticated, secure SNMP *gets* and *set*s. Since SNMP v2C uses community strings for authentication, all SNMP v2C operations must be performed within a secure IPSec tunnel between the remote system and the module.

3.5 Remote Access

1. Telnet access to the module is only allowed via a secure IPSec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections via telnet are secured through IPSec.
2. SSH access to the module is only allowed if SSH is configured to use a FIPS-approved algorithm. The Crypto officer must configure the module so that SSH uses only FIPS-approved algorithms.

© Copyright 2008 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.