AS2-FIPS PIC
Security Policy

Document *Version 1.5*

Juniper Networks

November 27, 2006

TABLE OF CONTENTS

1. Module Overview

The Adaptive Services (AS) 2-FIPS Physical Interface Card (PIC), (HW Versions PB-AS2-FIPS, PE-AS2-FIPS, Rev. A and B, Bootloader Firmware Version 560-011740 (rev. 4.008), Run-time Image Software Versions 7.2R1.7 and 7.4R1.7), is a multi-chip embedded cryptographic module, which supports a new level of services integration and performance. The AS2-FIPS PIC supports compressed real time protocol (CRTP), high-speed Network Address Translation (NAT), stateful firewall, tunnel services, IPSec encryption and J-Flow accounting today while having built-in headroom to support additional services in the future. With high-speed NAT and stateful firewall, providers can protect their networks and simultaneously deploy network-based security and VPN solutions. The cryptographic boundary is defined as the outer perimeter of the module's printed circuit board.

Figure 1 – Image of the Cryptographic Module

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3

Module Ports and Interfaces	1
Roles, Services and Authentication	3
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

The cryptographic module supports an Approved and a non-Approved mode of operation. By default, the AS2-FIPS PIC operates in a non-Approved mode of operation and must be configured into the Approved mode. In order to configure the AS2-FIPS PIC into the Approved mode of operation, the Cryptographic Officer must issue the "Authorize PIC" service. In FIPS mode, the cryptographic module only supports the following algorithms:

- RSA with 2048-bit or 1024-bit keys for digital signature verification
- RSA with 1024-bit keys for key transport
- Triple-DES (Three Key, CBC Mode, Hardware implementation) for encryption/decryption
- Triple-DES (Three Key, CBC Mode, Software implementation) for encryption/decryption
- SHA-1 for hashing using a hardware implementation
- SHA-1 for hashing using a software implementation
- HMAC-SHA-1 (96 bit key) for message authentication using a hardware implementation

The cryptographic module relies on the implemented software deterministic random number generator (DRNG) that is compliant with *FIPS 186-2, Appendix 3.1, Change Notice 1* for key generation.

The user can determine if the cryptographic module is running in FIPS mode if the module returns "Authorized" upon execution of the "Show Status" service.

Non-FIPS mode of operation

The cryptographic module provides a non-FIPS mode of operation. The module operates in the non-FIPS mode of operation by default and may be configured into the FIPS mode of operation by issuing the "Authorize PIC" service. If the module is operating in the FIPS-mode of operation, then it may be configured to operate in non-FIPS mode by zeroizing the module. In non-FIPS mode, the cryptographic module supports the following additional algorithms (Please note that the following algorithms are not used in the Approved mode of operation):

- MD5
- DES (to support legacy systems only)
- RSA (PKCS#1, key wrapping, key establishment methodology provides 80-bits of encryption strength)

4. Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

- PICNIC Bus: status output, control input
- BD Interface (Bus): data input, data output, control input, status output
- I^2C: status output
- Power Interface
- LEDs: status output

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module shall support three distinct operator roles (User, Cryptographic-Officer, and Software Manager). The cryptographic module shall enforce the separation of roles using identity-based operator authentication.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	Username, 256-bit password
Cryptographic-Officer	Identity-based operator authentication	Username, 256-bit password OR

		1024-bit RSA Digital Signatures
Software Manager	Identity-based operator authentication	2048-bit RSA Digital Signatures

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password	The module uses passwords that are at least 256-bits in length. The probability of a successful random attempt is 1 / 2^256, which is less than 1/1,000,000. The module can process a maximum of 480,000 password authentication attempts within a given minute. The probability of successful authentication with multiple consecutive attempts in a one minute period is 480,000/ 2^256, which is less than 1/100,000.
1024-bit RSA Digital Signature	The module uses 1024-bit RSA keys which have at least 80-bits of equivalent strength. The probability of a successful random attempt is 1 / 2^80, which is less than 1/1,000,000. The module can process a maximum of 131 CO RSA verifications in a minute. The probability of successful authentication with multiple consecutive attempts in a one minute period is 131/ 2^80, which is less than 1/100,000.
2048-bit RSA Digital Signature	The module uses 2048-bit RSA keys which have 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. The module can process a maximum of 12,000 authentication attempts using the 2048-bit RSA key within a given minute. The probability of successful authentication with multiple consecutive attempts in a one minute period is

	12,000/ 2^112, which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User: This role shall provide service necessary to destroy the secrets contained within the cryptographic module.	• System Zeroize: This service actively destroys all plaintext critical security parameters contained within the physically contiguous cryptographic boundary. This service must be invoked and the module must be power cycled to complete zeroization.
Cryptographic-Officer: This role shall provide all of the services necessary for the secure transport of data over a network.	• Authorize PIC: initialize the cryptographic module to perform cryptographic services. • IPSec Traffic Processing: the cryptographic module performs IPSec traffic processing using TDES and HMAC-SHA-1. • Update Internal Session Key: This service enters an RSA wrapped TDES Internal Session Key into the cryptographic module. • Update SAs: This service enters TDES encrypted IPSec SAs (Security Associations) into the cryptographic module. • Update Password: This service will update the User's password to a new password.
Software Manager: This role shall provide the service necessary to update the cryptographic module software image via an Approved authentication technique.	• Software Image Load: This service loads a new software image and verifies the digital signature on the software image using 2048-bit RSA.

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- Show status: This service provides the current status of the cryptographic module.
- Self-tests: This service executes the suite of self-tests required by FIPS 140-2 and is invoked by rebooting the module.
- Offline: This service causes the AS2-FIPS PIC to be turned off.
- Reset: This service causes the AS2-FIPS PIC to perform a soft reset.
- Firewall: performs packet filtering operations.
- Compressed Real Time Processing (CRTP): enables high quality voice to be run over low speed links.
- Network Address Translation (NAT): supports static or dynamic translation of IP addresses.
- J-Flow Accounting: performs traffic monitoring functions.
- Tunneling: provides different encapsulations mechanisms to support transport of multiple types of traffic over existing links.
- Update Service Set Configuration: This service configures non-security relevant characteristics of network traffic.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

User Password: a 256-bit password used to authenticate the User role to the module for execution of the System Zeroize service.

CO Password: a 256-bit password used to authenticate the Cryptographic-Officer to the module during initialization.

Internal Session Key: TDES Key used to encrypt SAs and passwords during entry.

SA Traffic Keys: TDES Key used for IPSec traffic encryption/decryption.

SA HMAC-SHA-1 Keys: a 160-bit HMAC key used for generation and verification of message authentication codes for IPSec traffic.

Internal State of FIPS 186-2 DRNG: Used during the Continuous RNG Test.

FIPS 186-2 DRNG Seed Key: Used for generation of random numbers.

RSA Private Signing Key: a 1024-bit RSA key used for generation of digital signatures in order to authenticate to an external entity during the Update Internal Session Key service.

RSA Private Decrypting Key: a 1024-bit RSA key used for RSA key wrapping to support commercially available key establishment per FIPS 140-2 Annex D.

Definition of Public Keys:

The following are the public keys contained in the module:

Software Image Verification Key: a 2048-bit RSA public key used for digital signature verification of the software image during the conditional software load test.

Juniper Root CA Public key: a 2048-bit RSA public key used for digital signature verification of digital certificates.

PIC RSA verify key: a 1024-bit RSA public key used for verification of digital signatures in order to authenticate to an external entity during the Update Internal Session Key service.

PIC RSA encrypt key: a 1024-bit RSA key used for RSA key wrapping to support commercially available key establishment per FIPS 140-2 Annex D.

C.O. RSA verify key: a minimum 1024-bit RSA public key used for digital signature verification during C.O. authentication.

C.O. RSA encrypt key: a minimum 1024-bit RSA public key used for RSA key wrapping to support commercially available key establishment per FIPS 140-2 Annex D.

Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Enter (e): The CSP is entered into the cryptographic module.
- Default (d): The CSP is set back to the factory default.
- Generate (g): The CSP is generated using the Approved FIPS 186-2 DRNG.
- Use (u): The CSP is used per its corresponding security function.
- Zeroize (z): The CSP is actively destroyed.

Table 5 – CSP Access Rights within Roles & Services

Role			Service	Cryptographic Keys and CSPs Access Operation								
C.O.	User	Software Manager		User Password	CO Password	Internal Session Key	SA – TDES Traffic Keys	SA- HMAC-SHA-1 Keys	Internal State of FIPS 186-2 DRNG	FIPS 186-2 DRNG Seed Key	RSA Private Signing Key	RSA Private Decrypting Key
	x		System Zeroize	z	z, d	z	z	z	z	z	z	z
x			Authorize PIC		e, g, u	e, u			g, u	e, u	g	g
x			IPSec Traffic Processing				u	u				
x			Update Internal Session Key			e					u	u
x			Update SAs			u	e	e				
x			Update Password	e, g								
		x	Software Image Load									
			Show status									
			Self-tests			z	z	z	z	z		
			Offline									
			Reset									
			Firewall									
			Compressed Real Time Processing (CRTP)									
			Network Address Translation (NAT)									
			J-Flow Accounting									
			Tunneling									
			Update Service Set Config.				z	z				

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the cryptographic module contains a limited operational environment. The cryptographic module only supports the loading and execution of trusted code that is digitally signed with the appropriate 2048-bit Software Image Signature Key.

8. Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The cryptographic module shall provide three distinct operator roles. These are the User role, the Cryptographic-Officer role, and the Software Manager role.
2. The cryptographic module shall provide identity-based authentication.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. Data output shall be inhibited during self-tests, and error states. Data output shall be logically disconnected from zeroization and key generation.
5. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. The module shall not support concurrent operators.
7. The module shall maintain separation of roles and services.
8. The cryptographic module shall not support a bypass capability; IPSec null encryption shall not be supported.
9. Upon entering an error state, the cryptographic module shall not provide any cryptographic services and shall provide status of the error.
10. The cryptographic module shall perform the following tests:

    A. Power up Self-Tests:

    1. Cryptographic algorithm tests:
        a. TDES Known Answer Test
        b. FIPS 186-2, Appendix 3.1, Change Notice 1 DRNG Known Answer Test
        c. SHA-1 Known Answer Test
        d. HMAC-SHA-1 Known Answer Test
        e. RSA Known Answer Test (decrypt for key wrapping)
        f. RSA Known Answer Test (digital signature generation/verification)

2. Software Integrity Test
    a. Bootloader Integrity Test (32-bit CRC)
    b. Run-time Image Integrity Test (32-bit CRC)
3. Critical Functions Tests
    a. Memory Test
    b. Register Test
    c. ALU Test
    d. Memory Stress Test
    e. ASISA String Round-Robin Test
    f. ASISA DES/MD5 Round-Robin Test
    g. ASISA 3DES/SHA Round-Robin Test
    h. Core CPU ALL Instruction Test
    i. MMU Location Test
    j. MAC Tests
    k. MD5 Known Answer Test (latent functionality; beyond the self-test MD5 is not used internally nor exposed within any service)

B. Conditional Self-Tests:

1. Continuous Random Number Generator (RNG) test – performed on FIPS 186-2 DRNG.

2. Pairwise Consistency Test – performs encrypt/decrypt and sign/verify pairwise consistency tests on all generated RSA keys.

3. Software Load Test (2048-bit RSA Signature Verification)

9. Physical Security Policy

Physical Security Mechanisms

The multi-chip embedded cryptographic module includes the following physical security mechanisms:

Table 6 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Production-grade components	N/A	N/A
Standard passivation	N/A	N/A
Standard ICs with uniform exterior coating and standard connectors	N/A	N/A

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate against specific attacks beyond the scope of FIPS 140-2.

Table 7 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

11. Definitions and Acronyms

ALU	Arithmetic Logic Unit CA
AS	Adaptive Services
ASISA	Application Solutions and Integrated System Analysts
CA	Certificate Authority
CO	Cryptographic Officer
CPU	Central Processing Unit
CRC	Cyclic Redundancy Code
CRTP	Compressed Real Time Protocol
CSP	Critical Security Parameters
DES	Data Encryption Standard
DRNG	Deterministic Random Number Generator
HMAC	Keyed-Hash Message Authentication Code
IC	Integrated Circuit
IPSec	Internet Protocol Security
LED	Light Emitting Diode
MAC	Message Authentication Code
MD5	Message Digest (Version) 5
MMU	Memory Management Unit
NAT	Network Address Translation
PIC	Physical Interface Card
RSA	Rivest, Shamir, Adleman
SA	Security Associates
SHA	Secure Hash Algorithm
TDES	Triple Data Encryption Standard
VPN	Virtual Private Networking