FIPSCOM
Cryptographic Module
Security Policy

Document Version 1.2

RELM Wireless Corporation

December 5, 2007

TABLE OF CONTENTS

1. Module Overview

The FIPSCOM (HW P/N 7011-30967-000 Versions 050306 and 030207 FW Versions 0722-05072-000, 0722-05073-000, and 0722-05073-001) is a multi-chip embedded cryptographic module assembled on a PC board. The primary purpose for this device is to provide encryption functions for secure digital communication products. The diagram below illustrates the physically contiguous cryptographic boundary, which is defined as the bottom of the FIPSCOM board containing a processor, non-volatile memory, and their associated circuitry, and the nickel-silver enclosure.

Figure 1 – Image of the Cryptographic Module

2. Security Level

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

3. Modes of Operation

Approved mode of operation

The FIPSCOM cryptographic module supports a FIPS mode of operation and a non-FIPS mode of operation.

When operating in a FIPS 140-2 Approved mode, the FIPSCOM cryptographic module supports the following algorithms:

- RSA with 1024-bit keys implemented according to ANSI x9.31 for digital signature verification to support firmware upgrades
- AES with 256-bit keys in ECB (Encrypt) and OFB (Encrypt/Decrypt) mode for encryption/decryption of digital communication
- SHA-1 for hashing
- NDRNG to generate initialization vectors for DES and AES

When operating in a non-FIPS mode, the FIPSCOM cryptographic module supports the following algorithm:

- DES in ECB and OFB mode for encryption/decryption of digital communication (Note: DES is only used to support communication with legacy infrastructures and is non-compliant).

The host radio sends a Select Key command to the FIPSCOM module. Based on the type of key previously loaded into the FIPSCOM, the module will operate in either a FIPS 140-2 Approved mode or a non-FIPS mode.

4. Ports and Interfaces

The FIPSCOM cryptographic module provides the following physical ports and logical interfaces through a ten- pin connector:

Pin 1: 3.3V: power interface

Pin 2: -RESET: control input

Pin 3: GND: power interface

Pin 4: GND: power interface

Pin 5: FC DATA OUT: data output, status output

Pin 6: CLOCK: control input

Pin 7: -CHIPSEL: control input

Pin 8: FC DATA IN: control input, data input

Pin 9: K/F (keyloader interface): data input, control input, data output, status output

Pin 10: -HOST INT: control output

5. Identification and Authentication Policy

Assumption of roles

The FIPSCOM cryptographic module shall support two distinct, mutually exclusive, operator roles: User and Cryptographic-Officer. The User is defined as the host radio that incorporates the module and the Cryptographic-Officer is defined as the human operator. There are no Maintenance User Roles in the module. As a Level 1 cryptographic module, the FIPSCOM does not support authentication. The role is implicitly selected by the service that is initiated.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	N/A	N/A
Cryptographic-Officer	N/A	N/A

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
N/A	N/A

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User: This role shall provide all of the services necessary for secure digital communication.	• **Search for key:** This service allows the host to determine if the specified key is present. • **Select key:** Allows host to select the internally stored encryption key that will be used for encryption/decryption. • **Encrypt digital communication:** Uses AES 256 ECB and OFB and DES ECB and OFB (Note: DES is only used to support communication with legacy infrastructures and cannot be used in FIPS mode). • **Decrypt digital communication:** Uses AES 256 ECB and OFB and DES ECB and OFB (Note: DES is only used to support communication with legacy infrastructures and cannot be used in FIPS mode). • **Power-up Self-tests:** This service, which can be invoked by cycling power to the host radio, executes the suite of self-tests required by FIPS 140-2. • **Execute SHA:** This service can be invoked by the host to perform a SHA-1 computation. • **Show status:** This service provides the current status of the cryptographic module. • **Generate random number:** This service provides a random number.
Cryptographic-Officer: This role shall provide all of the services necessary for secure administration of the module.	• **Keyload:** Keys are manually established but electronically entered. • **Firmware Update:** Load firmware using RSA 1024 bit digital signature verification. • **Zeroize Key:** This service zeroizes the specified key. • **Zeroize All:** This service actively destroys all plaintext critical security parameters.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

Digital Communication AES Key: a 256-bit AES key used in ECB (encrypt only) and OFB (Output Feedback Mode) (encrypt/decrypt) of digital communication.

Definition of Public Keys:

The following are the public keys contained in the module:

Firmware Upgrade RSA Public Key: 1024-bit RSA key used to verify RSA signed binary images to support firmware upgrade once the radio is fielded.

Definition of CSPs Modes of Access

Table 6 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- **Read (R):** This operation reads the parameter from memory.
- **Write (W):** This operation writes the parameter to memory.
- **Input (I):** This operation supports the input of the parameter into the cryptographic module's physical boundary.
- **Output (O):** This operation supports the output of the parameter from the cryptographic module's physical boundary.
- **Update Reference (U):** This operation updates the reference to a parameter.
- **Destroy (D):** This operation actively overwrites the parameter, thus destroying the item.

Table 6 – CSP Access Rights within Roles & Services

Role		Service	Type of Access
C.O.	**User**		**Digital Communication AES Key**
	X	**Search for Key**	
	X	**Select Key**	
	X	**Encrypt digital communication**	R, W
	X	**Decrypt digital communication**	R, W
	X	**Power-up Self-tests**	
	X	**Execute SHA**	
	X	**Show status**	
	X	**Generate Random Number**	
X		**Key load**	I, R, W
X		**Firmware Update**	
X		**Zeroize Key**	D
X		**Zeroize All**	D

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the FIPSCOM device has a limited operational environment. The module only supports firmware updates using 1024 bit RSA digital signature verification; the cryptographic module does not support the loading or execution of untrusted code.

8. Security Rules

The FIPSCOM cryptographic module's design corresponds to the FIPSCOM 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, and additional security rules enforced by RELM Wireless Corp.

Security Rules

1. The cryptographic module shall provide two distinct operator roles. These are the User role and the Cryptographic-Officer role.
2. The operator shall assume a role based upon the service that is initiated; the cryptographic module shall not support authentication.
3. The cryptographic module shall support only encrypted digital communications. A bypass mode is not supported.
4. The cryptographic module shall perform the following tests:

   A. <u>Power up Self-Tests:</u>

   1. Cryptographic algorithm tests:
      a. AES Encrypt Known Answer Test
      b. SHA-1 Known Answer Test
      c. RSA Verification Known Answer Test

   2. Software Integrity Tests (16 bit CRC verification)
      a. Bootloader Firmware Integrity Test
      b. Application Firmware Integrity Test

   3. Critical Functions Tests
      a. Key Table Integrity Test
      b. NDRNG Generator Test

B. Conditional Self-Tests:

1. Continuous Random Number Generator (RNG) test – performed on the NDRNG.
2. Firmware load test using 1024-bit RSA.
3. Key Table Integrity Test – performed when any key is modified.

5. Data output shall be inhibited during self-tests, zeroization, and error states.
6. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. Key generation is not supported.
8. The module shall not support concurrent operators.
9. DES is only present to support communication with legacy infrastructures.

9. Physical Security Policy

Physical Security Mechanisms

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

- Production-grade components and opaque enclosure.

Operator Required Actions

Since the cryptographic module does not provide any physical security beyond the use of production grade components and an opaque enclosure, the host radio operator is not required to inspect the device.

Table 7 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
N/A	N/A	N/A

10. Mitigation of Other Attacks Policy

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

Table 8 – Mitigation of Other Attacks

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

11. References

FIPS PUB 140-2: Security Requirements for Cryptographic Modules

FIPS PUB 197: Advanced Encryption Standard (AES)

FIPS PUB 81: DES Modes of Operation

FIPS PUB 180-2: Secure Hash Standard

ANSI x9.31: Digital Signature Using Reversible Public Key Cryptography

TIA/EIA 102.BAAA: Project 25 FDMA Common Air Interface

TIA/EIA 102.BAAC: Project 25 Common Air Interface Reserved Values

TIA/EIA 102.AABF: APCO Project 25 Link Control Word Formats and Messages

TIA/EIA 102.AAAA: Project 25 DES Encryption Protocol

TIA/EIA 102.AAAC: Conformance Test for the Project 25 DES Encryption Protocol

TIA/EIA 102-AACA: Project 25 Digital Radio Over-the-Air Rekeying (OTAR) Protocol

TIA/EIA 102-AACD: APCO Project 25 Digital Land Mobile Radio Key Fill Device (KFD) Interface Protocol

12. Definitions and Acronyms

AES	Advanced Encryption Standard
CO	Cryptographic Officer
CRC	Cyclic Redundancy Code
CSP	Critical Security Parameter
DES	Data Encryption Standard
ECB	Electronic Code Book
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
FIPS	Federal Information Processing Standards
OFB	Output Feedback
RSA	Rivest, Shamir, Adleman Algorithm
SHA-1	Secure Hash Algorithm-1
NDRNG	Non-Deterministic Random Number Generator