DPHx Radio with LZA0577 or LZA0577/LZA0578 Cryptographic Module Security Policy

Document Version 1.8

RELM Wireless Corporation

December 5, 2007

TABLE OF CONTENTS

1. Module Overview

The DPHx Radio with LZA0577 or LZA0577/LZA0578 Cryptographic Module (P/N DPHX5102X Versions 110504, 120104, 040805, 052005, 011606, 030206, 010507, 020707, 072007, FW Versions 722-05058-0000, 722-05058-0001, 722-05059-0000, 722-05059-0001, 722-05059-0002, 722-05059-0003, 722-05060-0000, 722-05061-0000) is a multi-chip standalone cryptographic module encased in an opaque commercial grade enclosure. As a secure radio, the primary purpose for this device is to provide encrypted digital communication. The diagram below illustrates the physically contiguous cryptographic boundary, which is defined as the outer perimeter of the radio's enclosure.

Figure 1 – Image of the Cryptographic Module

2. Security Level

The DPHx 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 DPHx cryptographic module supports a FIPS mode of operation and a non-FIPS mode of operation. With the LZA0578 kit installed (LZA0577/LZA0578), the DPHx supports AES Over-the-Air Rekeying (OTAR) of encryption keys.

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

- RSA (Cert. #31) with 1024-bit keys implemented according to ANSI x9.31 for digital signature verification to support firmware upgrades
- AES (Cert. #436): ECB mode (Encrypt/Decrypt; 256-bit), CBC mode (Encrypt; 256-bit), OFB mode (Encrypt/Decrypt; 256-bit)
- SHA-1 for hashing (Cert. #504)
- NDRNG to generate initialization vectors for AES

When operating in a non-FIPS mode, the DPHx cryptographic module supports the following algorithms:

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

Both AES and DES encryption keys can be loaded into the radio. Based on the type of key selected by the user, the radio will operate in either a FIPS 140-2 Approved mode or a non-FIPS mode.

4. Ports and Interfaces

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

RF link 1: control input, data input, data output, status output

RF link 2: control input, data input, data output, status output

Analog speaker output: data output, status output

Acoustic speaker output: data output, status output

Acoustic Microphone Input: data input

PTT Switch (Push to talk – high/low): control input

Touchpad input: control input, data input

Liquid Crystal Display: data output, status output

Channel Selector: control input

Function Yellow LED (on/off): Status output

Left Toggle Switch: control input

Middle Toggle Switch: control input

Right Toggle Switch: control input

On/Off & Volume: control input

Squelch & Monitor Switch: control input

Transmit Red LED: Status output (on/off)

Ground: power interface

Battery Connector: power interface

A six- pin accessories connector supports the following interfaces:

Pin 1: Switched A+: power interface

Pin 2: PTT (Push to talk - high/low): control input

Pin 3: Ground: power interface

Pin 4: Mic Hi (microphone): data input

Pin 5: supports two physically shared interfaces

Mon (monitor - high/low): control input

Serial: data output, status output

Pin 6: supports three physically shared interfaces

Prog (program – high/low): control input

Serial: data input, control input

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

The module also supports a maintenance interface through which an authorized maintenance operator can service the module. The interface can be accessed by removing the radio's outer case; the module must be zeroized upon entry and exit of the maintenance interface.

5. Identification and Authentication Policy

Assumption of Roles

The DPHx cryptographic module shall support three distinct operator roles (User, Cryptographic-Officer, and Maintenance). As a Level 1 cryptographic module, the DPHx 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
Maintenance	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.	• **Encrypt digital communication:** uses AES 256 OFB and DES 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 OFB and DES OFB (Note: DES is only used to support communication with legacy infrastructures and cannot be used in FIPS mode). • **Unencrypted communication:** transmits digital signals in plaintext. • **Bypass selection:** select encrypted or unencrypted transmission. • **Key tag selection:** select key used to encrypt digital transmissions. • **Power-up Self-tests:** This service, which can be invoked by cycling power to the radio, executes the suite of self-tests required by FIPS 140-2. • **Show status:** This service provides the current status of the cryptographic module. • **Request Re-Key:** transmits request to KMF for new encryption keys • **Key Set selection:** select active keyset from which key selection for transmit will be made
Cryptographic-Officer: This role shall provide all of the services necessary for secure administration of the module.	• **Initialize Radio:** load radio configurations into the module including bypass settings. • **Clone Radio:** copy configuration data from one radio to another including bypass settings. • **Program via touchpad:** manually set radio configurations using the radio's touchpad including bypass settings. • **Keyload:** keys are manually established but electronically entered. (e.g. via a key loader or KMF)

Maintenance: This role shall provide all of the services necessary for secure maintenance of the module.	• **Firmware Update:** load firmware using RSA 1024 bit digital signature verification. • **Zeroize:** This service actively destroys all plaintext critical security parameters.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- **Traffic Encryption Key:** a 256-bit AES key used in OFB (Output Feedback Mode) for encryption/decryption of digital communication.
- **Key Encryption Key:** a 256-bit AES key used to unwrap AES Traffic Encryption keys.
- **Group Touchpad Programming Secrets:** a maximum of twenty-five 6-digit secrets used to enable a subset of touchpad configuration capabilities.
- **Master Touchpad Programming Secret:** a 6-digit secret used to enable all of the touchpad configuration capabilities.

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 5 – CSP Access Rights within Roles & Services

Role			Service	Cryptographic Keys and CSPs Access Operation		
Maint.	**C.O.**	**User**		**Digital Communication AES Key**	**Group Touchpad Programming Secrets**	**Master Touchpad Programming Secret**
		X	**Encrypt digital communication**	R, W		
		X	**Decrypt digital communication**	R, W		
		X	**Unencrypted communication**			
		X	**Bypass selection**			
		X	**Key tag selection**	U		
		X	**Key set selection**	U		
		X	**Power-up Self-tests**			
		X	**Show status**			
	X		**Initialize Radio**		I, O, R, W	I, O, R, W
	X		**Clone Radio**		I, O, R, W	I, R, W
	X		**Program via touchpad**		I, O, R, W	I, R, W
	X		**Key load**	I, R, W		
X			**Firmware Update**			
X			**Zeroize**	D	D	D

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the DPHx 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 DPHx cryptographic module's design corresponds to the DPHx 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 three distinct operator roles. These are the User role, Cryptographic-Officer role, and Maintenance role.
2. The operator shall assume a role based upon the service that is initiated; the cryptographic module shall not support authentication.
3. When assuming the Maintenance role, the operator shall procedurally invoke zeroization upon entering and exiting the maintenance interface. Invoking the zeroization service will cause all CSPs stored within the module to be actively overwritten with zeroes.
4. The cryptographic module shall support both encrypted digital communications and unencrypted communications.
5. The cryptographic module shall perform the following tests:

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

   1. Cryptographic algorithm tests:
      a. AES Known Answer Test
      b. SHA-1 Known Answer Test
      c. RSA Known Answer Test
   2. Software Integrity Tests (16 bit CRC verification)
   3. Critical Functions Tests
      a. Bypass Test
      b. Key Table Integrity Test

   B. <u>Conditional Self-Tests:</u>

   1. Continuous Random Number Generator (RNG) test – performed on the NDRNG.

2. Bypass tests

3. Firmware load test using 1024-bit RSA.

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

9. Physical Security Policy

Physical Security Mechanisms

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

- Production-grade components and production-grade opaque enclosure.

Operator Required Actions

Since the cryptographic module does not provide any physical security beyond the use of production grade components, the User is not required to inspect the device.

Table 6 – 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 7 – 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

12. Definitions and Acronyms

AES	Advanced Encryption Standard
C.O.	Cryptographic Officer
CRC	Cyclic Redundancy Code
CSP	Critical Security Parameter
DES	Data Encryption Standard
DPHx	Digital Portable VHF Radio, Expanded Band
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
FIPS	Federal Information Processing Standards
LCD	Liquid Crystal Display
LED	Light Emitting Diode
OFB	Output Feedback
OTAR	Over-the-Air Rekeying
PTT	Push to Talk
RF	Radio Frequency
RSA	Rivest, Shamir, Adleman Algorithm
SHA-1	Secure Hash Algorithm-1
NDRNG	Non-Deterministic Random Number Generator