ZOLL Medical Corporation

R Series Data Comm II

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Version: 1.5

Date: 1/6/2016

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the ZOLL R Series Data Comm II module, hereafter denoted the Module. The Module allows data to be wirelessly transmitted. The Module meets FIPS 140-2 overall Level 1 requirements.

The Module contains an embedded cryptographic module: OpenSSL FIPS Object Module validated to FIPS 140-2 under Cert. #1747 operating in FIPS mode.

Table 1 – Cryptographic Modules

Module	HW P/N and Revision	FW Revision
R Series Data Comm II	9214-00207 Rev A	03.02.007.1322 (includes OpenSSL FIPS Object Module Version 2.0.7)

The Module is intended for use by US Federal agencies and other markets that require a FIPS 140-2 validated IEEE 802.11-2007 Wireless Card. The Module is a multi-chip standalone embodiment; the cryptographic boundary is the entire Wi-Fi card, inclusive of the case.

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic 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

The Module implementation is compliant with:

Table 3 - Module Compliance

Specification	Date	Title/Scope	Organization
IEEE 802.11-2007	6/12/2007	*IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements* *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*	The Institute of Electrical and Electronic Engineers, Inc. (IEEE)
FCC CFR 47 Part 15—RADIO FREQUENCY DEVICES	10/01/2007	Emission requirements for radio frequency devices	Federal Communications Commission (FCC)
FCC CFR 47 Part 15, Subpart C—INTENTIONAL RADIATORS, §15.247	10/01/2007	RF requirements for radio frequency devices	Federal Communications Commission (FCC)

1.1 Hardware and Physical Cryptographic Boundary

The physical form of the Module is depicted in Figure 1; the red outline depicts the physical cryptographic boundary. The Module relies on a CF interface to connect to an R Series system as an input/output device. The module consists of production-grade components that include standard passivation techniques.

Figure 1 – Module

Table 4 – Ports and Interfaces

Port	Description	Logical Interface Type
CF Connector	Compact Flash interface.	Power | Control in | Data in | Data out | Status out
Wi-Fi	This is used to wirelessly transfer data collected within the R Series to an external server.	Control in | Data in | Data out | Status out
LED	The module will control the LED allowing it to indicate power and the transmission of a file to the DXS.	Status out

1.2 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment.

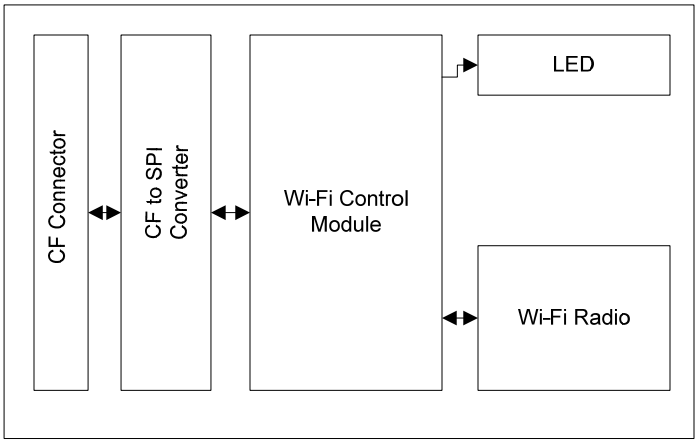

Figure 2 – Module Block Diagram

2 Modes of Operation

The Module supports a FIPS-Approved and non-Approved mode of operation. The mode of operation is based on the TLS cipher suite and key sizes negotiated. If any non-Approved function listed in Table 8 is used for TLS, the module is in the non-Approved mode. (All Approved algorithms are available in both the Approved and non-Approved modes.)

Although allowed for use in the Approved mode, the TLS protocol has not been reviewed or tested by the CAVP and CMVP.

2.1 Approved Mode

When the following cipher suites and key sizes are used, the module is in the Approved mode:

Table 5 – TLS v1.0/v1.1/v1.2 Cipher Suites and Algorithms/Key Sizes Allowed in FIPS Mode

Cipher Suites[1] [IG D.8 and SP 800-135]	Key Exchange	Server Authentication
ECDHE-RSA-AES128-GCM-SHA256	Ephemeral EC-Diffie-Hellman: P-224, P-256, P-384, P-521 K-233, K-283, K-409, K-571 B-233, B-283, B-409, B-571	RSA Sig Ver: 1024, 1536, 2048, 3072, or 4096-bit with SHA-1 or SHA-2
ECDHE-RSA-AES256-GCM-SHA384		
ECDHE-RSA-AES128-SHA256		
ECDHE-RSA-AES256-SHA384		
ECDHE-ECDSA-AES128-GCM-SHA256		ECDSA Sig Ver: All P, K and B curves with SHA-1 or SHA-2
ECDHE-ECDSA-AES256-GCM-SHA384		
ECDHE-ECDSA-AES128-SHA256		
ECDHE-ECDSA-AES256-SHA384		
ECDH-RSA-AES128-GCM-SHA256	EC-Diffie-Hellman: P-224, P-256, P-384, P-521 K-233, K-283, K-409, K-571 B-233, B-283, B-409, B-571	RSA Sig Ver: 1024, 1536, 2048, 3072, or 4096-bit with SHA-1 or SHA-2
ECDH-RSA-AES256-GCM-SHA384		
ECDH-RSA-AES128-SHA256		
ECDH-RSA-AES256-SHA384		
ECDH-ECDSA-AES128-GCM-SHA256		ECDSA Sig Ver: All P, K and B curves with SHA-1 or SHA-2
ECDH-ECDSA-AES256-GCM-SHA384		
ECDH-ECDSA-AES128-SHA256		
ECDH-ECDSA-AES256-SHA384		
DHE-RSA-AES128-GCM-SHA256	Ephemeral Diffie-Hellman: 2048 or 3072-bit	RSA Sig Ver: 1024, 1536, 2048, 3072, or 4096-bit with SHA-1 or SHA-2
DHE-RSA-AES256-GCM-SHA384		
DHE-RSA-AES128-SHA256		
DHE-RSA-AES256-SHA256		
DHE-DSS-AES128-GCM-SHA256		DSA Sig Ver: 1024, 2048, or 3072-bit with SHA-1 or SHA-2
DHE-DSS-AES256-GCM-SHA384		
DHE-DSS-AES128-SHA256		
DHE-DSS-AES256-SHA256		

[1] **Cipher:** AES128-GCM = AES GCM 128-bit
AES256-GCM = AES GCM 256-bit
AES128 = AES CBC 128-bit
AES256 = AES CBC 256-bit

MAC: SHA256 = HMAC-SHA-256
SHA384 = HMAC-SHA-384
SHA = HMAC-SHA-1

Cipher Suites[1] [IG D.8 and SP 800-135]	Key Exchange	Server Authentication
DH-RSA-AES256-SHA256	Diffie-Hellman: 2048 or 3072-bit	RSA Sig Ver: 1024, 1536, 2048, 3072, or 4096-bit with SHA-1 or SHA-2
ADH-AES128-GCM-SHA256	Anonymous Diffie-Hellman: 2048 or 3072-bit	(function provided by ADH)
ADH-AES256-GCM-SHA384		
ADH-AES128-SHA256		
AES128-GCM-SHA256	RSA: 2048 to 15360-bit	RSA Sig Ver: 1024, 1536, 2048, 3072, or 4096-bit with SHA-1 or SHA-2
AES256-GCM-SHA384		
AES128-SHA		
AES256-SHA		
DES-CBC3-SHA (same as 3DES-CBC)		

Note: All algorithms used in TLS are implemented in the embedded OpenSSL module (see Table 6).

Table 6 – Approved & Allowed Algorithms Implemented in the Embedded OpenSSL Module[2]

Algorithms	Publications	Functions	Modes/Key Sizes/Options	Cert. #
Approved Algorithms (CAVP Validated)				
AES	[FIPS 197], [SP 800-38A]	Encryption, Decryption	CBC and EBC modes 128 and 256 bit	3276
GCM[3] with AES	[SP 800-38D]	Encryption, Decryption	128 and 256 bit	3276
Triple-DES	[FIPS 46-3], [ANSI X9.52-1998], [SP 800-20]	Encryption, Decryption	CBC mode 3-Key (192-bit)	1864
HMAC[4]	[FIPS 198]	MAC	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	2074
SHA	[FIPS 180-4]	Message Digest	SHA-1 SHA-2: SHA-256, SHA-384, SHA-512	2714
DRBG	[SP 800-90A]	Random Number Generation	CTR_DRBG AES-256	734
ECDSA	[FIPS 186-4]	Public Key Generation	P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571	631
		Signature Verification	All P, K and B curves SHA-1, SHA-2	
DSA	[FIPS 186-4]	Key Pair Generation	2048, 3072 bit	935
		Signature Verification	1024, 2048, 3072 bit SHA-1, SHA-2	

[2] The R Series Data Comm II does not use all of the algorithms and functions available in the embedded OpenSSL FIPS Object Module. Some functions tested during algorithm testing are not supported for this validation.

[3] AES GCM is only used in TLS. The IV is constructed per the TLS protocol. The TLS client operations are fully contained within the module. The TLS cipher suites using AES GCM are compliant with IG A.5 and SP 800-52.

[4] During TLS, the HMAC key size is 20 to 32 bytes.

Algorithms	Publications	Functions	Modes/Key Sizes/Options	Cert. #
RSA	[FIPS 186-2]	Signature Verification (PKCS #1 V1.5)	1024, 1536, 2048, 3072, and 4096-bit SHA-1, SHA-2	1688
TLS KDF	[SP 800-135]	Key Derivation	TLS 1.0/1.1 TLS 1.2: SHA-256, -384, -512	458 (CVL)
AES	[SP 800-38F]	Key Transport	AES 256-bit with HMAC for authentication Provides 256 bits of strength.	AES #3276, HMAC #2074
Non-Approved Algorithms Allowed in the Approved Mode				
MD5	[IG D.2]	Only allowed for use within TLS	N/A	N/A
EC Diffie-Hellman (ECDH)	N/A (not compliant with SP 800-56A)	Key Agreement	All NIST defined B, K and P curves ≥ 224 Provides 112 to 256 bits of strength.	N/A
Diffie-Hellman (DH)	N/A (not compliant with SP 800-56A)	Key Agreement	2048 or 3072 bit Provides 112 or 128 bits of strength.	N/A
RSA	N/A (not compliant with SP 800-56B)	Key Wrap	2048 to 15360 bit Provides 112 to 256 bits of strength.	N/A

Table 7 – Approved Algorithms Implemented in ZOLL Firmware

Algorithm	Standards/ Publications	Functions	Modes/Key Sizes/Options	Cert. #
SHA	[FIPS 180-4]	Message Digest	SHA-1	2715

The module also contains an untested WPA/WPA2 implementation. This includes RC4 (WPA) and an untested and non-compliant AES CCM implementation (WPA2). This is only used for communications purposes. The protocol and the cryptographic functions used are not Approved and are not being used for security purposes. All data transferred over the WiFi connection is encrypted using TLS, as described above in Section 2.1. Cipher suites used to encrypt data over the WiFi connection in the Approved mode are listed in Table 5.

2.2 Non-Approved Mode

When the following key sizes are used in TLS, the module is in the non-Approved mode:

Table 8 – Non-Approved Mode Algorithms/Key Sizes Implemented in the Embedded OpenSSL Module

Cipher Suites (see Table 5)	Key Exchange Algorithms	Disallowed Key Sizes
ECDHE cipher suites, ECDH cipher suites	EC DH key agreement, not compliant with SP 800-56A	All P, K, or B curves < 224 (provides < 112 bits of strength; non-compliant)
DHE cipher suites, ADH cipher suites, DH cipher suites	DH key agreement, not compliant with SP 800-56A	All sizes < 2048 (provides < 112 bits of strength; non-compliant)
RSA cipher suites	RSA key transport, non-compliant with SP 800-56B	All sizes < 2048 (provides < 112 bits of strength; non-compliant)

Note: The Approved algorithms listed above in Section 2.1 are also available in the non-Approved mode.

2.3 Changing Between Modes

In order to change between modes, the following procedure must be followed:

1. Perform the "Firmware Upgrade/Zeroize" service to zeroize all keys on the module.
2. Perform the "Power Up Self-Tests" service by power cycling the module to run all self-tests.

3 Cryptographic Functionality

3.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 9 – Critical Security Parameters (CSPs)

CSP	Algorithms / Sizes	Description / Usage
Upgrade Encryption Key	AES256-ECB, 256 bit key	AES 256 key used to decrypt firmware during firmware updates.
Upgrade Signature Key	HMAC-SHA1 digest, 2048 bit key	HMAC-SHA1 digest for firmware upgrade verification.
DRBG Entropy	256 bit	Entropy material for approved DRBG
TLS Pre-Master Secret	384 bit pre-master secret	Pre-master secret for TLS.
TLS Session Key	AES-128 or 256 bit key or 3 key Triple-DES	Session key for TLS.
TLS Ephemeral DH private components	Ephemeral DH keys, 2048 or 3072 bit.	Ephemeral DH private components used for TLS
TLS Ephemeral ECDH private components	Ephemeral ECDH keys, min 224 bit.	Ephemeral ECDH private components used for TLS
DRBG internal state	V and Key; Managed by the embedded OpenSSL module	Internal state of DRBG, contained within the embedded OpenSSL module

3.2 Public Keys

Table 10 – Public Keys

Key	Description / Usage
ZOLL Root Key	RSA 2048 bit cert. This is used when establishing a HTTPS (TLS) connection to the ZOLL Data DXS server.
User Keys	RSA 2048 bit certs. The end user can add public root CA and SSL certificates as required.
TLS Ephemeral DH public components	Ephemeral DH keys, 2048 or 3072 bit.
TLS Ephemeral ECDH public components	Ephemeral ECDH keys, NIST curves $\geq$ 224.

4 Roles, Authentication and Services

4.1 Assumption of Roles

The module supports two distinct operator roles, User and Cryptographic Officer (CO). Roles are assumed implicitly based on service.

The Module does not support a maintenance role or bypass capability. The Module does not support concurrent operators. The Module does not implement authentication.

Table 11 – Roles Description

Role ID	Role Description
CO	Cryptographic Officer – see Table 12.
User	User – Transmission of data.

4.2 Services

All services implemented by the Module are listed in the table below. Each service description also describes all usage of CSPs by the service. See appendix D for services commands.

Note: The Module services are the same in the Approved and non-Approved modes of operation.

Table 12 – Services

Service	Description / CSPs	CO	User
Write Configuration	Configure the module and load User keys. Write: User keys, DRBG Entropy	X	
Read Configuration	Read the WiFi configuration stored on the module. This does not return any CSPs or certificates. Does not use CSPs.	X	
Show Status	Prints out the configuration and Version number of the module. Does not use CSPs.	X	
Firmware Upgrade/Zeroize	The R Series Defib will provide the Upgrade Key to the Module at the initiation of the Firmware Upgrade operation. The Module uses the Upgrade Key to decrypt the firmware upgrade file. The Module will then do a signature verification of the input image. Once a valid firmware image is present the upgrade is initiated. The firmware update process provides the option to zeroize all CSPs in the process. Zeroize performs the same operation that firmware upgrade does and it also destroys all CSPs and does a factory install of the firmware image. Write: Upgrade Encryption Key, Upgrade Signature Key, ZOLL Root Key Execute: Upgrade Encryption Key, Upgrade Signature Key Zeroize: All CSPs	X	

Service	Description / CSPs	CO	User
Power Up Self-Tests	See Table 13. Triggered by application of power to the Card, no commands involved. Does not use CSPs.	X	
File Transfer	Receives a file from the R-Series then transmits it to the ZOLL Data Systems Exchange Server. Execute: DRBG Internal State, TLS Pre-Master Secret, TLS Session Key, TLS Ephemeral DH/ECDH Private Components, ZOLL Root Key, User Keys Generate: TLS Pre-Master Secret, TLS Session Key, TLS Ephemeral DH/ECDH components		X

5 Self-tests

5.1 Power up Self-Tests

Each time the Module is powered up, it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power-up self–tests are available on demand by power cycling the module.

On power up or reset, the Module performs self-tests described in Table 13 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the Soft Error State.

Table 13 – Power Up Self-tests

Test Target	Description
Firmware Integrity test	An integrity test to validate the integrity of the running image. This is a HMAC-SHA-1 digest. The key is 256 bytes in length. The value of the HMAC-SHA-1 digest is calculated at compile time of the firmware image.
Python SHA-1	KAT: Python SHA-1
Critical Functions Test: OpenSSL Verification Test	Verification that embedded OpenSSL module successfully completes its self-tests and enters FIPS mode. The power up self-tests performed by the embedded OpenSSL module are listed in the module's Security Policy: csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1747.pdf

5.2 Conditional Self-tests

Table 14 – Conditional Self-Tests

Test Target	Description
Firmware Load test	HMAC-SHA-1 verification of all firmware updates.

The embedded OpenSSL module includes conditional self-tests that are run each time that the cryptographic algorithms are called.

Table 15 – OpenSSL Module Conditional Self-tests

Test Target	Description
DRBG	Tested as required by [SP 800-90A] Section 11
DRBG	FIPS 140-2 continuous test for stuck fault
DSA	Pairwise consistency test on each generation of a key pair
ECDSA	Pairwise consistency test on each generation of a key pair

6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware upgrade service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Security Rules and Guidance

The Module design corresponds to the Module 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 module shall provide two distinct operator roles: User and Cryptographic Officer.
2. The operator shall be capable of commanding the module to perform the power up self-tests by cycling power of the module.
3. Power up self-tests do not require any operator action.
4. Data output shall be inhibited during self-tests, Zeroization, and error states.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. There are no restrictions on which keys or CSPs are zeroized by the zeroization services.
7. The module does not support concurrent operators.
8. The module does not support a maintenance interface or role.
9. The module does not support manual key entry.
10. The module does not output CSPs.
11. The module does not output intermediate key values.

8 References and Definitions

The following standards are referred to in this Security Policy.

Table 16 – References

Abbreviation	Full Specification Name
[FIPS 140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP 800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011

Table 17 – Acronyms and Definitions

Acronym	Definition
CF	CompactFlash is a mass storage device format used in portable electronic devices.
Wi-Fi	Refers to the IEEE 802.11 communications standard.
LED	Light-emitting diode.
CSP	Critical Security Parameter
SPI	The "Serial Peripheral Interface" (SPI) is a synchronous four wire serial link used to connect microcontrollers to sensors, memory, and peripherals.
DXS	ZOLL Data Systems Exchange Server
Zeroization	Erasing sensitive parameters (electronically stored data, cryptographic keys, and CSPs)
OpenSSL	Toolkit implementing the Secure Sockets Layer (SSLv2/v3) and Transport Layer Security (TLS v1) protocols
R Series Defibrillator	R Series DATA COMM II R Series Defibrillator
Module	R Series DATA COMM II WIFI Card