ICU Medical, Inc.

LifeCare PCA™ Infusion Pump

Non-Proprietary FIPS 140-2 Security Policy

Version: 1.2

Date: 29/09/2020

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the ICU Medical, Inc. LifeCare PCA™ Infusion Pump module, hereafter denoted the Module. The Module is a medical Patient Controlled Analgesia (PCA) device. The Module provides secure communications with ICU Medical MedNet™ Hospital Management Safety Software (HMSS) for infusion status reporting, configuration via updating of drug libraries, and auto-programs. The Module uses TLS protocol to ensure the secure communication with the HMSS as well as the Module configuration via a web interface using either wired or wireless network interfaces.

Table 1 – Cryptographic Module Configuration

	Module	HW P/Ns and Versions[1]	FW Versions
1	LifeCare PCA™	20837-04-03 with 810-04505-039 and 810-11438-018	CE v1.90.0.8 and MCU v7.4.0.5*
2		20837-04-04 with 810-04505-039 and 810-11438-018	

* The MCU firmware is excluded from the FIPS 140-2 requirements. The MCU firmware does not implement FIPS 140-2 security functions. Even if the MCU firmware malfunctions, it cannot cause a potential release of CSPs, plaintext data, or other information that if misused could lead to a compromise.

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-2 validated infusion pumps.

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	3
Cryptographic 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	1
Mitigation of Other Attacks	N/A
Overall	1

[1] Both models implement the same HW components, the different part numbers are related to different manufacturing dates. 810-04505-039 and 810-11438-018 are related to the internal component references.

1.1 Module Description and Cryptographic Boundary

The physical form of the Module is depicted in Figure 1 and Figure 2. The Module is a multi-chip standalone embodiment. The cryptographic boundary is the entire product and enclosure without the syringe (Figure 1 only).

Figure 1 – Picture of the 20837-04-03 Module

Figure 2 – Picture of the 20837-04-04 Module

The Module's ports and associated FIPS defined logical interface categories are listed in Table 3.

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
Barcode reader	Drug label reader	Data in
Display, LEDs, and speaker	Status output	Status out
Keypad	Keypad for device control and data input to MCU	Control in | Data in

Port	Description	Logical Interface Type
Maintenance port	Internal module port used to access diagnostic information. Available for maintenance operation only.	Status out
Network	Ethernet and Wi-Fi connection	Control in | Data in | Data out | Status out
Nurse Call	Signal to call nurse	Status out
Patient Pendant	Patient control to administer dose	Control in
Power	Power and Ground	Power
Flip switch	Internal module switch to enable a Factory reset. Available for maintenance operation only.	Control in

1.2 Modes of Operation

The Module is intended to operate in two modes:

A) FIPS Approved mode:
This mode is entered by enabling the configuration setting through the WebConfig interface (under the "HMSS" configuration tab on the web page, Configure and Show Status service), followed by a Module reset. In this mode of operation, the MedNet™ and WebConfig communications with the Module is mandated to use FIPS enabled TLS sessions.

- OpenSSL FIPS Canister version 2.0.16 is used along with OpenSSL 1.0.2n.
- Power-up self-tests and conditional self-tests are performed as per FIPS requirements.
- Approved DRBG is seeded with the non-Approved but allowed NDRNG. Only cryptographic algorithms listed in Table 4 and Table 5 are used. See Table 6 for details on Security Relevant Protocols used in the FIPS Approved mode of operation.
- Only algorithm certificates and keys that are allowed by the FIPS specifications can be uploaded.
- The Module does not provide any bypass capability in this mode of operation.
- The module does not provide any external cable or network-based shell access, or access to the file system or any of the internal services or data.
- Firmware load test is performed with the Approved RSA signature verification algorithm.

B) FIPS non-Approved mode:
This mode is the default factory mode of operation on the device. It can also be explicitly entered by enabling the configuration setting through the WebConfig interface, followed by a Module reset or by accessing the physical switch (maintenance operation). In this mode, the Module is not mandated to use a FIPS Enabled TLS session while communicating with the MedNet™ or the WebConfig (i.e., SSL can be disabled).

- OpenSSL 1.0.2n crypto protocols and ciphers are used
- Module uses a Non-Approved and non-allowed NDRNG

- See Table 6 for details on Security Relevant Protocols used in the non-Approved mode of operation
- Only algorithm certificates and keys that are allowed by the FIPS specifications are allowed to be uploaded.
- Power-On Self-Test (other than the 32-bit CRC firmware integrity and RAM integrity POST) and Conditional Tests are not performed
- The module provides a limited (non-root) shell access to assist in debug and diagnostics, without any capability to stop/add/remove/alter any existing services or access any portion of the filesystem with sensitive data.
- Firmware load test is performed with the Approved RSA signature verification algorithm.

Whenever the Module switches between FIPS Approved and non-Approved mode, it forces the zeroization of the CSPs (as clarified in Table 14). Switching the Module between the two modes also forces a Module Reset (Self-test) as specified in Table 12. Only the CO role and Maintenance role are authorized to switch the mode of operation of the Module.

The Module is shipped in non-Approved mode of operation by default. To operate the Module in a FIPS mode of operation, the WebConfig interface shall be enabled with the following operations:

- Unlock the front door
- Plug the Module to the power supply
- Press ON/OFF+ENTER key at the same time on the KeyPad
- Select DIAGNOSTICS->NETWORK->CE SETTINGS->WEB CONFIG-> ENABLE/DISABLE on the menu to enable the WebConfig interface

The Cryptographic Officer (FSE or Biomed) will authenticate to WebConfig interface with the default password of the non-Approved mode of operation. The mode of operation can be switched by the CO role by accessing the WebConfig interface “HMSS” page (Configure and Show Status service) and appropriately setting the “FIPS 140-2 Enabled:” check-box as shown below.

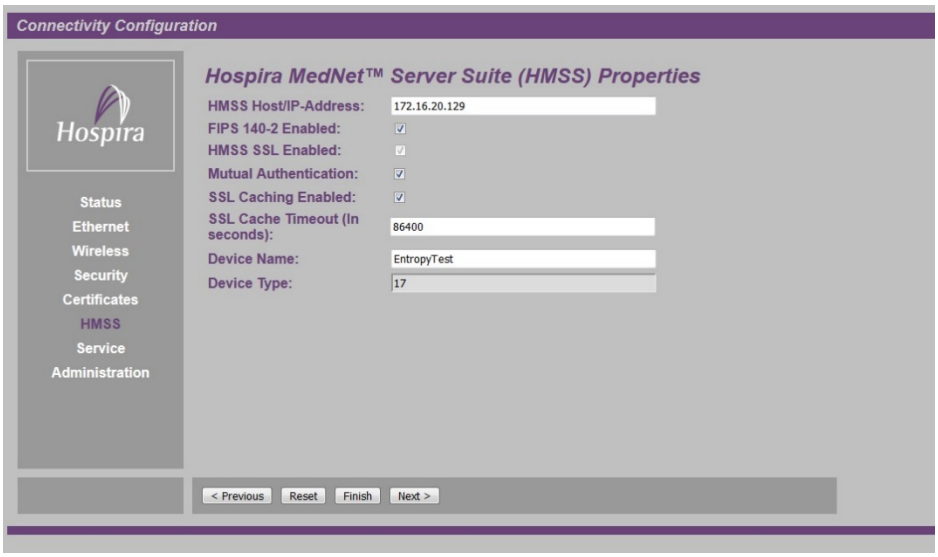

Figure 3 – FIPS-Mode Configuration

Whether the Module is operating in the FIPS Approved mode or not, it can be verified through the WebConfig interface and checking the "Status" page.

Under the "Status" page, the "FIPS 140-2 Mode:" shall be set to "Enabled" to indicate that the device is operating in FIPS Approved Mode, as shown below:

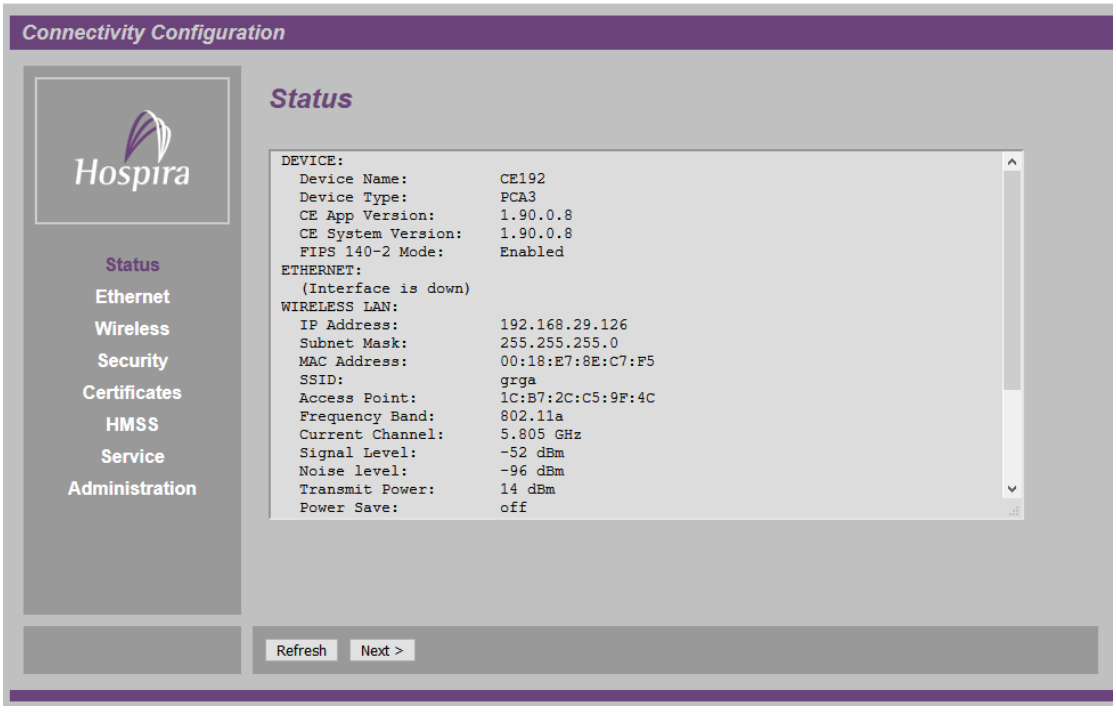

Figure 4 – Show Status – FIPS Mode Enabled

If the module is in a non-Approved mode of operation, the "FIPS 140-2 Mode:" will be set to "Disabled".

In FIPS Approved mode only, the FSE (CO) will be able to zeroize all CSPs with the "Zeroize CSP" button (part of Configure and Show Status service), see Figure 5 below. This functionality can be used when entering and existing the maintenance mode.

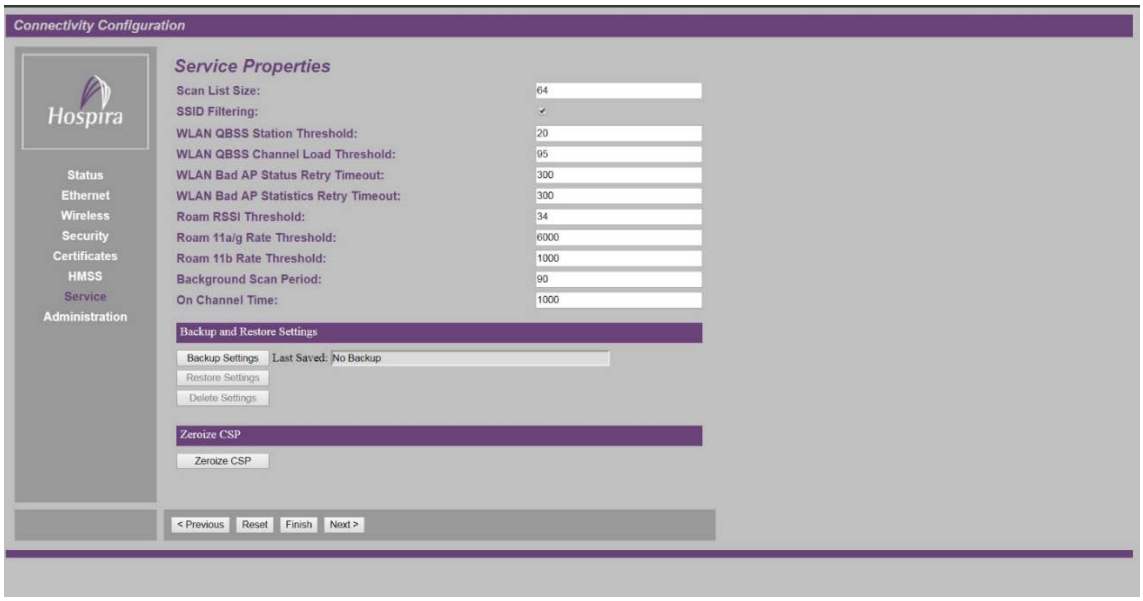

Figure 5 – Zeroize CSP for FSE

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 4 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
5766	AES [197]	ECB [38A]	Not used except for the self-test: AES-128 Not supported: AES-256	Self-test only
		CBC [38A]	Key Sizes: 128, 256	Encrypt, Decrypt
		GCM [38D]	Key Sizes: 128, 256	Authenticated Encrypt, Authenticated Decrypt
VA	CKG [IG D.12]	[133] Section 6.2 Asymmetric key establishment key generation using unmodified DRBG output		Key Generation
		[133] Section 7.1 Direct symmetric key generation using unmodified DRBG output		
		[133] Section 7.3 Derivation of symmetric keys from a key agreement shared secret.		
2088	CVL: KAS ECC [56A]	Ephemeral Unified, One-Pass DH	P-224, P-256, P-384, P-521	ECDH ephemeral shared secret generation
2089	CVL: TLS [135]	v1.0, v1.1	SHA-1	TLS key derivation

Cert	Algorithm	Mode	Description	Functions/Caveats
		v1.2	SHA-(256, 384) Not supported: SHA-512	
2090	CVL: RSADP [56B]		Key Size: 2048 bit	Decrypt encrypted keys for TLS with cipher suite using RSA key exchange, Signature generation.
2361	DRBG [90A]	HMAC_DRBG Not supported: Hash_DRBG	SHA-256 Not supported: SHA-(1, 512)	Deterministic Random Bit Generation Security Strength = 256 bits
1550	ECDSA [186]		P-224, P-256, P-384, P-521	TLS ECDHE Key Generation, no ECDSA keys are generated with this algorithm.
			P-224, P-256, P-384, P-521	TLS PKV
			P-224 SHA-(256, 384, 512) P-256 SHA-(256, 384, 512) P-384 SHA-(256, 384, 512) P-521 SHA-(256, 384, 512) Not supported: EC with SHA-1	TLS Signature Generation
			P-224 SHA-(256, 384, 512) P-256 SHA-(256, 384, 512) P-384 SHA-(256, 384, 512) P-521 SHA-(256, 384, 512) Not supported: EC with SHA-1	TLS Signature Verification
3814	HMAC [198]	SHA-1	Key Sizes: 256 bits λ = 160	TLS Message Authentication
		SHA-256	Key Sizes: 256 – 2048 bit λ = 256	
		SHA-384	Key Sizes: 384– 2048 bit λ = 384	
		SHA-512	Not supported	
VA	KAS [56Ar2]	CVL Certs. #2088 (KAS) and #2089 (KDF), IG D.1 rev2		TLS Key Agreement Scheme provides between 112 and 256 bits of encryption strength.
5766 3814	KTS	CBC	Key Sizes: 128, 256	Key Transport Scheme provides 128 or 256 bits of encryption strength
		HMAC	SHA-(1, 256, 384)	
5766	KTS	GCM	Key Sizes: 128, 256	Key Transport Scheme provides 128 or 256 bits of encryption strength
3069	RSA [186]	X9.31	Not supported	TLS Signature Generation
		PKCS1_v1.5	n = 2048 SHA-(256, 384, 512) Not supported: SHA-(1)	TLS Signature Generation
		X9.31	Not supported	TLS Signature Verification

Cert	Algorithm	Mode	Description	Functions/Caveats
		PKCS1_v1.5	n = 2048 SHA-(256, 384, 512) Not supported: SHA-(1)	TLS Signature Verification
4588	SHS [180]	SHA-1 SHA-256 SHA-384 SHA-512	SHA-(1, 256, 384, 512)	Message Digest Generation
2855	Triple-DES [67]	TCBC [38A]	Key Size: 192	Self-test only

AES GCM IV: The AES GCM implementation meets Option 1 of IG A.5. The Module supports TLS 1.2 GCM Cipher Suites for TLS, as described in RFCs 5116, 5288 and 5289. The counter portion of the IV is set by the module within its cryptographic boundary.
The nonce_explicit part of the IV is incremented each time an AES GCM computation is performed. The module does not establish a new session key when the nonce_explicit part of the IV exhausts the maximum number of possible values (2^{64}). However, that would take hundreds of years to happen and the module enforces a TLS renegotiation (new session) after 24 hours.
AES GCM keys are zeroized when the module is power-cycled and for each new TLS session, a new AES GCM keys is established.

Table 5 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
Security Claimed	
MD5 within TLS	[IG D.2] Used only within TLS 1.0/1.1
NDRNG	[Annex C] Non-Deterministic RNG; the NDRNG provides a seed with a minimum entropy of 256 bits to the FIPS Approved DRBG.
RSA Encapsulation	[IG D.9] Cert. #2090 RSA based key encapsulation (for use in TLS), key establishment provides 112 bits of encryption strength
No Security Claimed	
AES (no security claimed)	[IG 1.23] • AES CCMP in WPA2 • AES encryption/decryption in EAP-TLS (802.1X) • AES CCM: self-test only • AES GCM: CSP obfuscation
CKG (no security claimed)	[IG 1.23] Asymmetric and symmetric key generation in EAP-TLS (802.1X)

Algorithm	Description
DH(E) (no security claimed)	[IG 1.23] Key Agreement Scheme in EAP-TLS (802.1X).
ECDH(E) (no security claimed)	[IG 1.23] Key Agreement Scheme in EAP-TLS (802.1X).
ECDSA (no security claimed)	[IG 1.23] Authentication in EAP-TLS (802.1X).
HMAC (no security claimed)	[IG 1.23] Authentication/Integrity in EAP-TLS (802.1X).
KDF (no security claimed)	[IG 1.23] Key derivation in EAP-TLS (802.1X).
RSA (no security claimed)	[IG 1.23] Authentication in EAP-TLS (802.1X).
SHA (no security claimed)	[IG 1.23] • SHA-1, -384, -256: Digest computation in EAP-TLS (802.1X). • SHA-1: Entropy pool conditioning
SHA-256 (no security claimed)	[IG 1.23] Passwords obfuscation
Storage encryption (no security claimed)	[IG 1.23] AES 128 in GCM mode: • Encrypting the sensitive information before saving in local storage (obfuscating local storage) • Decrypting the sensitive information after reading from local storage e.g., private key passwords, wireless configuration
Triple-DES (no security claimed)	[IG 1.23] • Triple-DES encryption/decryption in EAP-TLS (802.1X) • Triple-DES ECB decryption for obfuscation of certificate private key

Note that several algorithms which are identified in
Table 5 are used by the wireless interface (WPA2 and 802.1X EAP protocols). No security is claimed for the cryptographic algorithms implemented by the wireless interface. The security functions are those identified in Table 4 which are used by TLS for both the wireless and the wired interfaces.

Table 6 – Security Relevant Protocols[2] Used in FIPS Approved and non-Approved Mode of operations

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
TLS [IG D.8 and SP 800-135]	TLS_RSA_WITH_AES_128_CBC_SHA			TLS v1.0, v1.1, v1.2
	RSA	RSA	AES-128 CBC	HMAC-SHA-1
	TLS_RSA_WITH_AES_128_CBC_SHA256			TLS v1.0, v1.1, v1.2
	RSA	RSA	AES-128 CBC	HMAC-SHA-256
	TLS_RSA_WITH_AES_256_CBC_SHA			TLS v1.0, v1.1, v1.2
	RSA	RSA	AES-256 CBC	HMAC-SHA-1
	TLS_RSA_WITH_AES_256_CBC_SHA384			TLS v1.0, v1.1, v1.2
	RSA	RSA	AES-256 CBC	HMAC-SHA-384
	TLS_RSA_WITH_AES_128_GCM_SHA256			TLS v1.2
	RSA	RSA	AES-128 GCM	AEAD
	TLS_RSA_WITH_AES_256_GCM_SHA384			TLS v1.2
	RSA	RSA	AES-256 GCM	AEAD
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384			TLS v1.2
	ECDHE	RSA	AES-256 GCM	AEAD
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384			TLS v1.2
	ECDHE	ECDSA	AES-256 GCM	AEAD
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384			TLS v1.0, v1.1, v1.2
	ECDHE	RSA	AES-256 CBC	HMAC-SHA-384
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384			TLS v1.0, v1.1, v1.2
	ECDHE	ECDSA	AES-256 CBC	HMAC-SHA-384
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA			TLS v1.0, v1.1, v1.2
	ECDHE	RSA	AES-256 CBC	HMAC-SHA-1
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA			TLS v1.0, v1.1, v1.2
	ECDHE	ECDSA	AES-256 CBC	HMAC-SHA-1
	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384			TLS v1.2
	ECDH	RSA	AES-256 GCM	AEAD
	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384			TLS v1.2

[2] No parts of these protocols, other than the cryptographic algorithms, have been tested by the CAVP and CMVP

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
	ECDH	ECDSA	AES-256 GCM	AEAD
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384			TLS v1.0, v1.1, v1.2
	ECDH	RSA	AES-256 CBC	HMAC-SHA-384
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384			TLS v1.0, v1.1, v1.2
	ECDH	ECDSA	AES-256 CBC	HMAC-SHA-384
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA			TLS v1.0, v1.1, v1.2
	ECDH	RSA	AES-256 CBC	HMAC-SHA-1
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA			TLS v1.0, v1.1, v1.2
	ECDH	ECDSA	AES-256 CBC	HMAC-SHA-1
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256			TLS v1.2
	ECDHE	RSA	AES-128 GCM	AEAD
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256			TLS v1.2
	ECDHE	ECDSA	AES-128 GCM	AEAD
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256			TLS v1.0, v1.1, v1.2
	ECDHE	RSA	AES-128 CBC	HMAC-SHA-256
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256			TLS v1.0, v1.1, v1.2
	ECDHE	ECDSA	AES-128 CBC	HMAC-SHA-256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA			TLS v1.0, v1.1, v1.2
	ECDHE	RSA	AES-128 CBC	HMAC-SHA-1
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA			TLS v1.0, v1.1, v1.2
	ECDHE	ECDSA	AES-128 CBC	HMAC-SHA-1
	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256			TLS v1.2
	ECDH	RSA	AES-128 GCM	AEAD
	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256			TLS v1.2
	ECDH	ECDSA	AES-128 GCM	AEAD
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256			TLS v1.0, v1.1, v1.2
	ECDH	RSA	AES-128 CBC	HMAC-SHA-256
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256			TLS v1.0, v1.1, v1.2
	ECDH	ECDSA	AES-128 CBC	HMAC-SHA-256
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA			TLS v1.0, v1.1, v1.2

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
	ECDH	RSA	AES-128 CBC	HMAC-SHA-1
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA			TLS v1.0, v1.1, v1.2
	ECDH	ECDSA	AES-128 CBC	HMAC-SHA-1

The Module supports the RADIUS protocol in the context of 802.1X EAP protocols only to connect the Wireless devices. Users are not authenticated with the support of the RADIUS protocol.

In the non-Approved mode of operation, the following non-Approved algorithms are supported:

- Non-Approved and non-allowed NDRNG

2.1 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 7 – Critical Security Parameters (CSPs)

CSP	Description / Usage
Cached Entropy	Unused random data reads from NDRNG and saved in internal storage
Cached Nonce	128-bit unique nonce value saved in internal storage
DRBG-EI	DRBG entropy input: seed with a minimum entropy of 480 bits and 128-bit unique nonce value
DRBG-State	DRBG internal state (V and K for HMAC – see SP800-90A)
Private Keys Passwords	8-48 character passwords to protect the HMSS and WebConfig Static Private keys access
WebConfig Credentials	8-48 character user authentication password for the Cryptographic Officer to access the WebConfig interface (both BIOMED and FSE sub-roles). This also includes the Challenge and Response to recover forgotten passwords for the BIOMED User sub-role.
TLS-DH-Priv	TLS EC Diffie-Hellman P-224, P-256, P-384, and P-521 Ephemeral Private Key
TLS-Static-Priv	TLS RSA 2048-bit or EC Diffie-Hellman P-224, P-256, P-384, and P-521 HMSS and WebConfig Static Private Keys
TLS-MS	TLS Master Secret 384-bit, secret key material
TLS-PMS	TLS Pre-Master Secret, secret key material
TLS-SENC	TLS Session Encryption Key AES CBC or GCM 128/256-bit key
TLS-SMAC	TLS Session Authentication Keys HMAC-SHA-1, 256, 384 or AES-128, -256 GCM hash sub-key.

As part of CSP Zeroization of the flash persistent items, the module overwrites the plaintext CSP allocated memory range and then deallocate the memory range from the flash persistent storage. Transient CSPs are zeroized by the OpenSSL Stack, and also when the module restarts and powers-up.

2.2 Public Keys

Table 8 – Public Keys

Key	Description / Usage
TLS-DH-Pub	TLS EC Diffie-Hellman on P-224, P-256, P-384, and P-521 Ephemeral Public Key
TLS-Static-Pub	TLS RSA 2048-bit or EC Diffie-Hellman on P-224, P-256, P-384, and P-521 Static Public Key
CA-Root	CA-Root key, RSA 2048-bit or ECDSA on P-224, P-256, P-384, and P-521 signature verification public key for both server and client modes.
FW-Load-Pub	RSA 2048 Public Key for firmware signature verification

3 Roles, Authentication and Services

3.1 Assumption of Roles

The Module supports three (3) distinct operator roles, User, Cryptographic Officer (CO), and the Physical Maintenance Role. The cryptographic Module enforces the separation of CO and User roles using TLS sessions; maintenance role is not authenticated, and it does not access to CSPs.

The CO is authenticated to the Module with the password authentication method through the Web Configuration interface (WebConfig). Within the CO role, we have two sub-roles:

1. BIOMED role
2. Field Service Engineer (or also named as Super-User) role: in addition to BIOMED role settings (part of Configure and Show Status service), the FSE role has access to additional settings: Wi-Fi configuration, setting backup/restoration, and Super-User role password management. Only ICU Medical Field Engineer personnel would have access to this role.

Both sub-roles have their own passwords.

The User is authenticated to the Module with a certificate authentication mechanism through the HMSS interface.

Only the maintenance role (ICU Medical authorized Field Service Engineer (FSE) or Manufacturing Technician (MT)) provides maintenance services, where they need to open up the Module for various services like replacing components, flipping the CE reset switch, or enabling logging and diagnostics. The Module users do not have Maintenance access.

Table 9 lists all operator roles supported by the Module. The Module does not support a bypass capability. The CO and User roles work in mutual exclusion with each other. The Module clears authentications with the closure of the session including on power cycle. Access to private keys and CSPs requires authentication and is only done over an encrypted TLS session.

Table 9 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer – Access to the WebConfig interface by BIOMED role or Field Service role	Identity-based	Login/Password and certificate
User	User – HMSS connected user/machine.	Identity-based	Certificate
Maintenance	Physical Maintenance – Field Service personnel opening up the Module to replace components, or to flip the reset switch, or to get diagnostics or logging information from console access. The Module needs to be opened by unscrewing the case.	N/A	N/A

3.2 Authentication Methods

CO password

The Module is shipped with default CO passwords that the Module requires to be changed upon initial authentication when logged in using the BIOMED User sub-role. The Field Service Engineer role will have to change the default password. The password is sent to the Module through a TLS connection and its value is compared with the value stored in the Module. If the comparison succeeds, the CO is authenticated, otherwise the authentication has failed. After three (3) failed authentication attempts the Module must be reset which requires more than a minute. The default minimum password length is eight (8) characters composed of:

- At least one (1) lowercase letter (a…z),
- At least one (1) uppercase letter (A…Z),
- At least one (1) decimal numerals (0…9),
- At least one (1) special character among the following 33 characters: **SPACE ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~**

The Module also provides a ten (10) minute inactivity timeout on the CO session and forces the CO to log back in again.

The Module CO session also supports a Challenge and Response to recover forgotten passwords for the BIOMED User sub-role. For the BIOMED sub-role, the default Challenge and Response can be chosen and needs to be changed on the first login. The response does adhere to the same minimum password length and special characters requirements as mentioned above.

Certificate

The User is authenticated to the Module with the TLS authentication mechanism. The strength of the authentication mechanism is related to the selected TLS cipher suite.

The Module supports certificates with the following authentication algorithms: RSA 2048, ECDSA P-224, ECDSA P-256, ECDSA P-384, and ECDSA P-521.

The minimum equivalent strength supported is 112 bits. The Module can open up 1000 TLS new sessions per one-minute period.

Table 10 – Authentication Description

Authentication Method	Probability
Password	The character set contains 95 characters, the minimum size of the password is eight (8) characters, and the password shall include diversified characters. It is assumed that the characters of the password are independent with each other, and the probability of guessing an individual character of the password is less than 1/10; the smallest class of characters being the digit class (0-9) which a size of 10. The probability for guessing every character is smaller than the probability of guessing a digit, which is 1/10. Thus, the probability of guessing the password is less than 1/10^8 lower than 1/1,000,000. After three (3) failed authentication attempts the Module must be reset which requires more than a minute. The probability that a random attempt will succeed over a one minute interval is 3/(10^8) which is less than 1/100,000.
Certificate	The minimum equivalent strength supported is 112 bits. The probability that a random attempt will succeed using the certificate authentication method is 1/(2^112) which is lower than 1/1,000,000. Up to 1000 TLS new sessions can be opened per one-minute period. The probability that a random attempt will succeed over a one minute interval is 1000/(2^112) which is lower than 1/100,000.

3.3 Services

All services implemented by the Module are listed in the tables below.

Table 11 – Authenticated Services

Service	Description	CO	User
Configure and Show Status	Establishes WebConfig via TLS for setting the network and security parameters, and for displaying the status. This service is also used to switch between the FIPS Approved and non-Approved modes of operation. The Field Service technician could also use the restricted Super-User sub-role to backup and restore the settings within the module during servicing, or to explicitly zeroize all the CSPs on the module. No HMSS interaction is permitted during these operations.	X	-
HMSS Request	Module receives drug libraries, auto-programs, and firmware update over TLS protocol from HMSS. Module acts as TLS server.	-	X
Module Request	Module sends data and system status over TLS to HMSS. Module acts as TLS client.	-	X

Table 12 – Unauthenticated Services

Service	Description
Factory Reset Settings (Unauthenticated)	Resets to factory settings via KeyPad. The CSPs will be zeroized.
KeyPad entry	KeyPad entry data input to MCU and for device control other than Factory Reset Settings service.
Module Reset (Self-test)	Resets the Module by power cycle.
Barcode reading	Barcode on pharmacy filled drug vials input to MCU.

Table 13 – Maintenance Services

Service	Description
Factory Reset Settings (Maintenance)	Resets to factory settings via the flip switch. Physical access required to unscrew the Module and open it up to access the reset flip switch. The CSPs will be zeroized.
Component replacement	Replacement of the components by unscrewing the chassis. Physical access required.
CE Diagnostic and logs collection	Retrieves diagnostic logs from an attached serial console cable. This requires unlocking and opening the front Security Door to the MCU using a physical key, and then enabling the serial debug mode through MCU menu control input to collect the logs. The serial console does not provide a shell access, or access to any module filesystem or services in the FIPS Approved mode of operation.

The services listed above do not include the normal infusion pump related functionality which is not related to the security related functionality of the Module and are implemented by the MCU firmware (excluded from the FIPS requirements).

Services are the same in the Approved and Non-approved modes of operation except that in a non-Approved mode of operation the Module will used non-Approved algorithms, see Section 1.2 for more detail, and the CE Diagnostic and logs collection service allows an access to the CE diagnostic console (limited filesystem access, information collection, and network configuration; the operational environment cannot be changed).

Table 14 defines the relationship between access to Security Parameters and the different Module services. The modes of access shown in the table are defined as:

- G = Generate: The service generates the CSP or Public Key.
- O = Output: The Module does not output CSPs or Public Keys.
- E = Execute: The service uses the CSP or Public Key in an algorithm.
- I = Input: The service inputs the CSP or Public Key in a protected form (KAS, KTS, or RSA encapsulation).
- Z = Zeroize: The service zeroizes the CSP or Public Key.

Table 14 – Security Parameters and Public Key Access by Service

Service	CSP												Public Key			
	Cached Nonce	Cached Entropy	DRBG EI	DRBG-State	Priv. Keys Password	WebConfig Credentials	TLS-DH-Priv	TLS-Static-Priv	TLS-MS	TLS-PMS	TLS-SENC	TLS-SMAC	TLS-Static-Pub	TLS-DH-Pub	CA-Root	FW-Load-Pub
Authenticated																
Configure and Show Status	Z	Z	Z	GEZ	IZ	IEZ	GEZ	IEZ	GEZ	GEZ	GEZ	GEZ	IEZ	GEZ	IZ	-
HMSS Request	-	-	-	GE	E	-	GE	E	GE	GE	GE	GE	E	GE	E	IE
Module Request	-	-	-	GE	E	-	GE	E	GE	GE	GE	GE	E	GE	E	-
Unauthenticated																
Factory Reset Settings (Unauthenticated)	Z	Z	G	GE	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	-
KeyPad entry	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Module Reset (Self-test)	GE	E	GZ	GEZ	-	-	Z	-	Z	Z	Z	Z	-	Z	-	-
Barcode reading	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Maintenance																
Factory Reset Settings (Maintenance)	Z	Z	G	GE	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	-
Component replacement	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CE Diagnostic and logs collection	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

4 Self-Tests

The Module performs self-tests to ensure the proper operation of the Module. Per FIPS 140-2, these are categorized as either power-up self-tests or conditional self-tests. Power up self–tests are available on demand by power cycling the Module.

All algorithm Known Answer Tests (KATs) must be completed successfully prior to any other use of cryptography by the Module. If the power-up self-tests succeed, the Module will indicate this status by displaying the network settings in the Diagnostics-Network screen in MCU BIOMED mode, otherwise it will fail the test and will restart the Module (KAT) or the module will not respond to any request (Firmware and RAM integrity tests failure).

The Module performs the following Power-On Self-Test algorithm on power-up:

- CE Firmware Integrity[3]: 32-bit CRC
- Crypto Library integrity[4]: HMAC-SHA1
- AES-ECB-128, separate encrypt and decrypt KATs
- AES-GCM-256, separate encrypt and decrypt KATs with 128-bit tag
- RSA, sign and verify KATs using 2048 bit key, SHA-256, and PKCS#1 v. 1.5; inclusive to RSADP POST
- ECDSA, Key Pair, PKV, and separate signature generation and signature verification using P-224 curves and SHA-512
- SP 800-90A HMAC_DRBG KAT using SHA-256
- HMAC - One KAT per SHA-1, SHA-256, SHA-384, and SHA-512; inclusive to SHA POST requirements
- EC Diffie-Hellman KAT using P-224
- SHA-1 KAT
- Critical function: RAM integrity verification

The following KATs are also performed but the cryptographic algorithms are not reachable:

- Triple-DES, separate encrypt and decrypt KAT, CBC mode, 3 Keys
- AES-CMAC, sign and verify KATs, with AES-128, AES-192, AES-256
- AES-CCM-192, separate encrypt and decrypt KATs
- AES PRNG KAT based on ANSI X9.31
- AES XTS, encrypt and decrypt KATs with AES 128 and AES 256
- DSA KAT, sign and verify KATs with 2048-bit key and SHA-384
- SP 800-90A Hash_DRBG (SHA-256)
- HMAC - SHA-224 KAT

The Module performs the following conditional self-tests as indicated.

- NDRNG CRNGT using 160-bit block size
- DRBG CRNGT using 128-bit block size
- DRBG: SP800-90A Health Tests (every 2^{24} generations).

[3] Performed in both Approved and non-Approved modes of operation.

[4] Performed in the Approved mode of operation only.

- ECDSA Pairwise consistency test on ECDSA key pair generation, inclusive to SP 800-56A Conditional Test on Prerequisite Algorithms and Assurances (Domain Parameter Validity and Arithmetic Validity of a Public Key) per IG 9.6
- Firmware Load: RSA 2048 signature verification of SHA-256 based signature.

5 Physical Security Policy

The cryptographic boundary is the entire product and enclosure of LifeCare Patient-Controlled Analgesia™ (PCA™) Infusion system. It consists of production-grade components that include standard passivation techniques. Additional protection from environmental exposure is accomplished by the PCA enclosure.

6 Operational Environment

The Module has a non-modifiable operational environment under the FIPS 140-2 definitions. The Module includes a firmware update service to support necessary updates. The software image is signed with 2048-bit RSA key and SHA-256.

Firmware versions validated through the FIPS 140-2 CMVP will be explicitly identified on a validation certificate. Any firmware not identified in this Security Policy does not constitute the Module defined by this Security Policy or covered by this validation.

7 Mitigation of Other Attacks Policy

The Module does not implement mitigation of other attacks outside the scope of [FIPS 140-2].

8 Security Rules and Guidance

This section documents the security rules for the secure operation of the cryptographic Module to implement the security requirements of FIPS 140-2.

1. The Module provides three (3) distinct operator roles: Cryptographic Officer, User, and Maintenance.
2. The Module provides identity-based authentication.
3. The Module clears previous authentications on power cycle.
4. The Module allows the operator to initiate power-up self-tests by power cycling or resetting the Module.
5. Power-up self-tests do not require any operator action.
6. Data output are inhibited during key generation, self-tests, zeroization, and error states.
7. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
8. The Module does not support manual key entry.
9. The Module does have proprietary external input/output devices used for entry/output of data.
10. The Module does not enter or output plaintext CSPs.

11. The Module does not output intermediate key values.
12. The Module does not provide bypass services or ports/interfaces.
13. The Module will support RSA certificates with modulus size greater or equal to 2048 bits.
14. The Module will support EC certificates with curve P-224, P-256, P-384, and P-512.
15. The module does not provide any external cable or network-based shell access, or access to the file system or any of the internal services or data in the FIPS Approved mode of operation.

The conditions for using the Module in the Approved mode of operation are:

1. Client and Server certificates shall be generated using FIPS 140-2 approved key generation methods and loaded into the Module.
2. TLS and FIPS approved mode shall be enabled in the HMSS settings using WebConfig.
3. The Field Service personnel is responsible for zeroizing the CSP when entering or exiting the maintenance role by calling Factory Reset Settings (unauthenticated of Maintenance) service.
4. The Field Service personnel shall replace the default Super-User password during the Module initialization.
5. The CO shall replace the default TLS certificates used for CO and User access during the Module initialization.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 15 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, August 16, 2019*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, revision 2, *March 2019*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 1, July 2019*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56A]	*NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007*
[56Ar2]	*NIST Special Publication 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, May 2013*
[56Br1]	*NIST Special Publication 800-56A Revision 1, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, September 2014*

Abbreviation	Full Specification Name
[67]	*National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, Revision 2, July 2017*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*

Table 16 – Acronyms and Definitions

Acronym	Definition
AEAD	Authenticated Encryption with Additional Data
CE	Communications Engine
HMSS (or MedNet™)	ICU Medical Hospital Management Safety Software
MCU	Motor Control Unit
FSE	ICU Medical Field Service Engineer or Personnel