Alaris™ PC Unit Model 8015 FIPS 140-2 Level 2 Non-Proprietary Security Policy

For Alaris™ PC Unit with v12.1.3 Firmware

2022-12
DME: 10000396895-00

Alaris™ PC Unit Model 8015 FIPS 140-2 Level 2 Non-Proprietary Security Policy

The information in this document is subject to change and does not represent a commitment on the part of BD to provide additional services or enhancements.

The intended audience of this document is any BD Alaris™ Systems user with PC Unit version 12.1.3 software and who is interested in supporting increased security of FIPS 140-2 in their environment.

This document is posted to the NIST website and is part of the open public domain.

CareFusion 303, Inc.
10020 Pacific Mesa Blvd.
San Diego, CA 92121
United States

888-876-4287

bd.com

Change Record

Revision	*Date*	*Author*	*Description of Change*
00	2022-12	BD	Initial FIPS certification for PC Unit v12.1.3 software.

Contents

1. Introduction

1.1. References

[FIPS 140-2] FIPS Publication 140-2 Security Requirements for Cryptographic Modules

[FIPS 180-2] FIPS Publication 180-2 *Secure Hash Standard*

[FIPS 197] FIPS Publication 197 *Advanced Encryption Standard*

FIPS Official Web Site: http://www.nist.gov/itl/fips.cfm

1.2. Definitions and Acronyms

Term	Definition
Advanced encryption standard (AES)	A cryptographic algorithm; a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.
BD Alaris™ System Maintenance software	A PC-based software tool that allows a hospital to perform routine maintenance, firmware upgrade, and data log downloads from the BD Alaris™ and Alaris™ PC Unit Model 8015 and attached expansion devices.
BD Alaris™ Systems Manager	BD Alaris™ Systems Manager software manages wireless communication with a PC Unit.
Critical security parameter (CSP)	From FIPS 140-2: Security-related information (for example, secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module.
Cryptographic boundary	From FIPS 140-2: An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.
Cryptographic module (CM)	From FIPS 140-2: The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.
Cryptographic officer (CO)	From FIPS 140-2: An operator or process (subject), acting on behalf of the operator, performing cryptographic initialization or management functions.
Cryptographic user (CU)	From FIPS 140-2: An individual or process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services.
FIPS	Federal Information Processing Standards
FIPS Approved	From FIPS 140-2: FIPS-Approved and/or NIST-recommended.
FIPS-Approved mode of operation	From FIPS 140-2: A mode of the cryptographic module that employs only approved security functions.

Term	Definition
FIPS-approved security function	From FIPS 140-2: A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is one of the following: • Specified in an approved standard • Adopted in an approved standard and specified either in an appendix of the approved standard or in a document referenced by the approved standard • Specified in the list of approved security functions
IG	Implementation guidance for FIPS 140-2 and the cryptographic module validation program
Inter-unit interface (IUI) port	Proprietary physical connector for data and power supply connection.
NIST	National Institute of Standards and Technology
Random number generator	From FIPS 140-2: Random number generators (RNGs) used for cryptographic applications typically produce a sequence of zero and one bits that may be combined into sub-sequences or blocks of random numbers. There are two basic classes: deterministic and nondeterministic. • Deterministic RNG (DRNG) consists of an algorithm that produces a sequence of bits from an initial value called a seed. • Nondeterministic RNG (NDRNG) produces output that is dependent on some unpredictable physical source that is outside human control.
Secure hashing algorithm (SHA)	An algorithm for computing a one-way, condensed representation of electronic data with secure properties.
Tamper evidence	From FIPS 140-2: The external indication that an attempt has been made to compromise the physical security of a cryptographic module. The evidence of the tamper attempt should be observable by an operator subsequent to the attempt.
Zeroization	From FIPS 140-2: A method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data.

1.3. Cryptographic Module Overview

The Alaris™ PC Unit Model 8015, (also named the BD Alaris™ PC Unit model 8015 and hereafter may also be referred to as the cryptographic module or CM) is the central point-of-care unit, which is the main component of the BD Alaris™ and Alaris™ System. The BD Alaris™ and Alaris™ System are modular systems intended for adult, pediatric, and neonatal care in a professional healthcare environment. The BD Alaris™ and Alaris™ System bring a higher level of medication error prevention to the point of patient care. The CM is multi-chip standalone embodiment validated to FIPS 140-2 level 2.

Figure 1-1 depicts the CM (outlined in red) in an operational context. The Systems Manager software controls communication and data transfer between the server and other systems and software resident on the network including the BD Alaris™ and Alaris™ System, BD Care Coordination Engine (CCE), and BD Alaris™ Guardrails™ continuous quality improvement (CQI) database. This browser-based software interface allows the hospital's data sets to be uploaded to the BD Alaris™ and Alaris™ System while providing device data reporting on successful uploads and downloads of CQI log data. The Systems Manager also provides data communication support for the CCE by providing interface capability to other hospital systems. CCE can provide subscription services to a broad range of hospital applications, including pharmacy, electronic medical records (EMR), clinical information systems, and other monitoring/patient tracking systems.

The CM cryptographic functions provide:

- Strong authentication of the Systems Manager by the CM.
- AES encryption of traffic from the CM to the Systems Manager.
- AES decryption of traffic from the Systems Manager to the CM.
- RSA signature verification to authenticate CM firmware.

The CM uses an off-the-shelf IEEE 802.11 wireless communication device to communicate with system wireless access points. No FIPS 140-2 security claim is made for 802.11-related functionality in accordance with implementation guidance (IG) 1.23.

Traffic is secured by AES encryption and decryption between the CM and the Systems Manager independent of the 802.11 protocol choices made on the intervening wireless access point.

Table 1-1: FIPS 140-2 Security Levels

Security requirements section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

The CM implements a limited operational environment. FIPS 140-2 Area 6 operational environment requirements are not applicable.

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

The following figure depicts the CM. The CM's cryptographic boundary is the external housing, which does not include the IUI ports and battery pack.

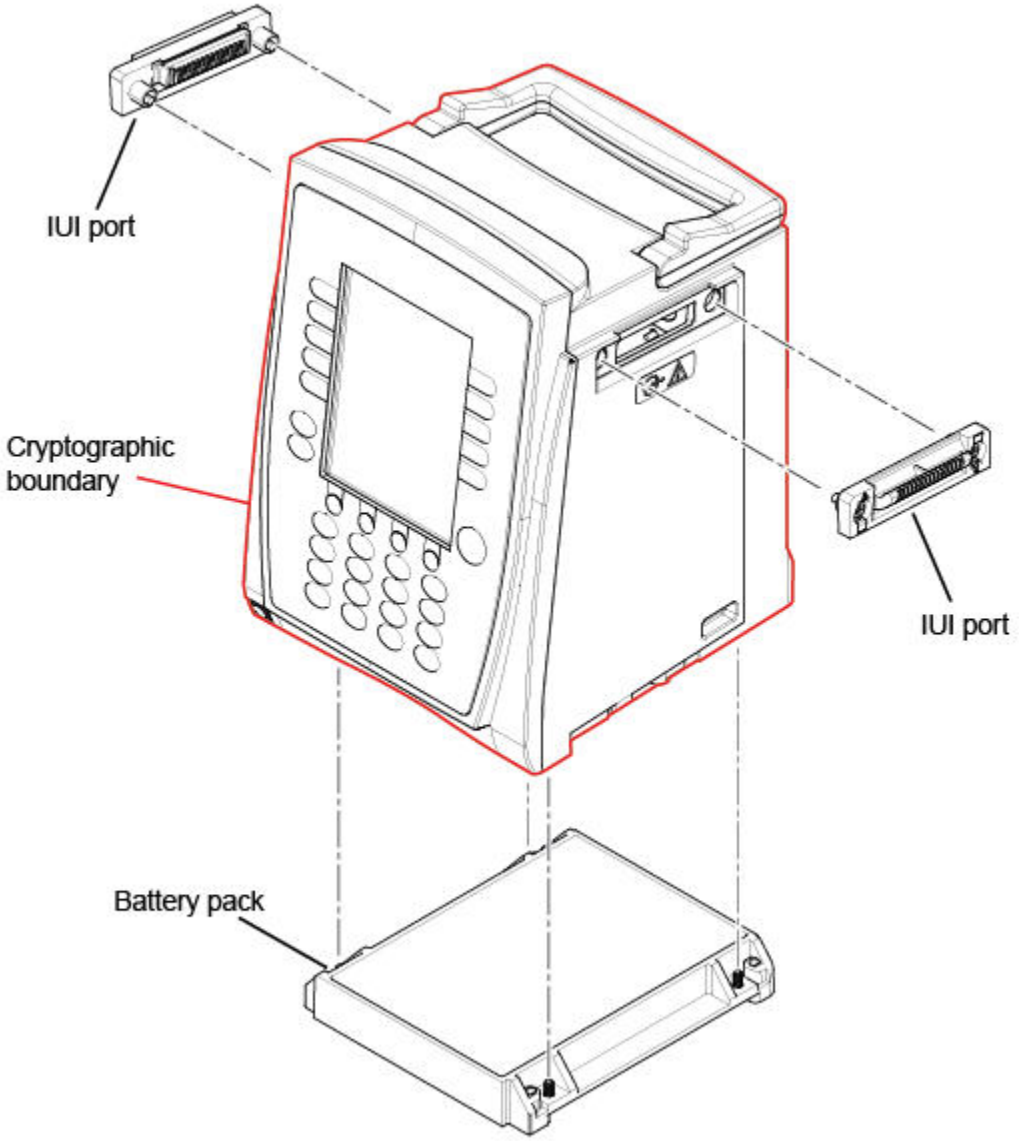

Figure 1-1: CM Front and Side View

The following figure depicts a rear view of the CM.

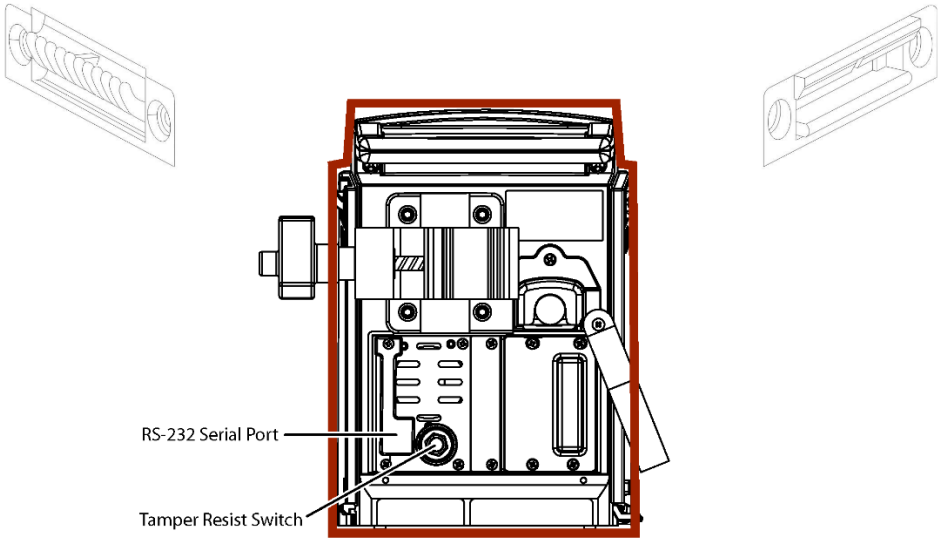

Figure 1-2: CM Rear View (Rear Panel May Look Slightly Different Depending on Model)

The tamper resist switch is designed as a clinical feature and does not refer to FIPS 140-2 physical security requirements. This tamper resist switch is used to inhibit a non-clinical person from making clinical changes to a programmed infusion. This switch is also used by biomedical engineers to initiate firmware upgrade functionality.

The CM's cryptographic boundary is indicated by the solid red line in the logical diagrams that follow. Figure 1-3 illustrates model 8015 b/g and model 8015 a/b/g. Figure 1-4 illustrates model 8015 a/b/g/n.

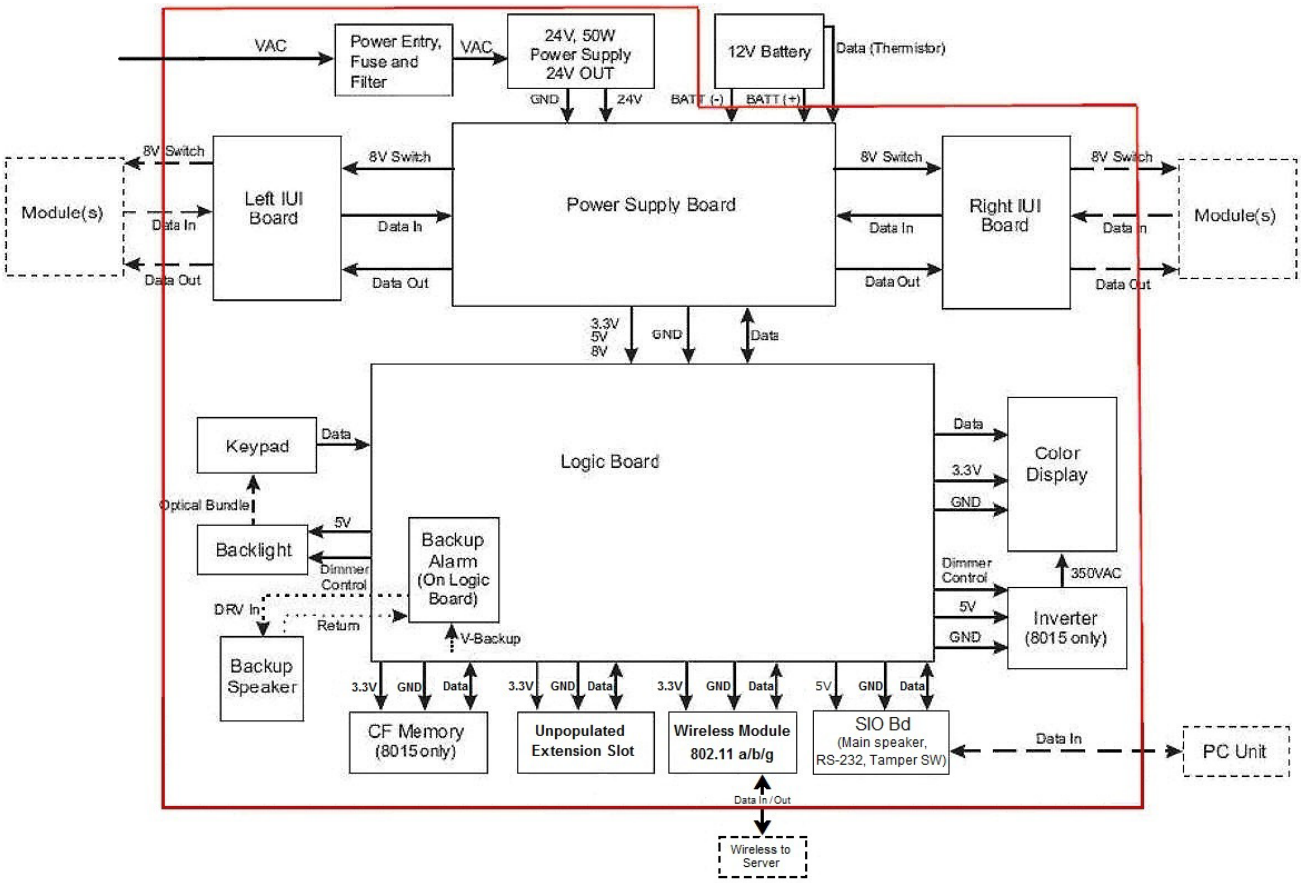

Figure 1-3: Block Diagram of CM Logic – Model 8015 b/g and Model 8015 a/b/g

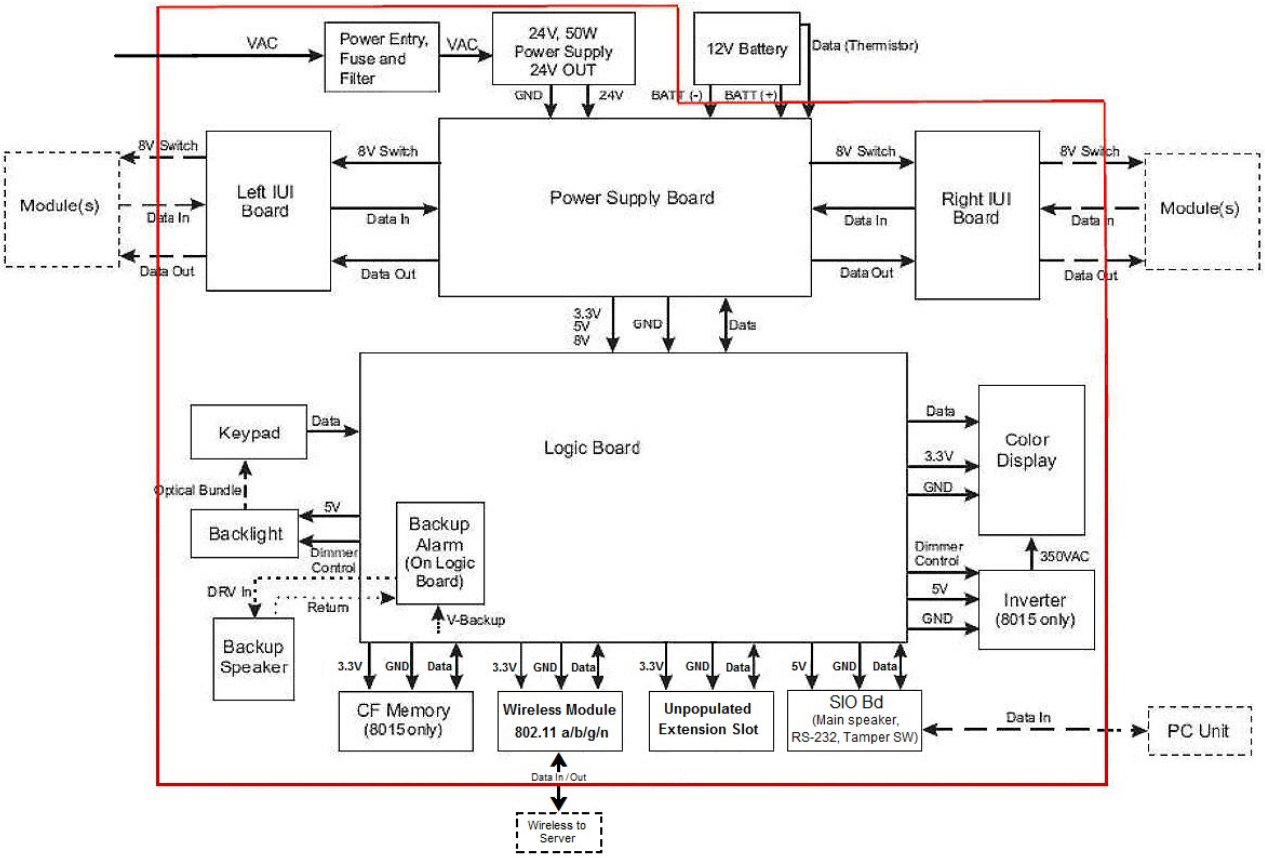

Figure 1-4: Block Diagram of CM Logic for both Model 8015 a/b/g/n and BD Alaris™ Model 8015 a/b/g/n

The CM comprises the components shown in the block diagrams above.

- Power components: Power entry, fuse and filter, 24V power supply, 12V battery, and power supply board (power conversion and distribution)
- Communications: Wireless module (802.11 b/g, 802.11 a/b/g or 802.11 a/b/g/n), left and right IUI boards (communication with add-on clinical modules)
- Keypad, switches and annunciators: keypad, backlight, backup speaker, color display and inverter (display power); Tamper Resist Switch (used to lock keyboard from accidental key presses)
- Multi-function I/O board: SIO board, with serial communications to Alaris™ System maintenance (marked PC Unit in the diagram above)
- Processing and associated memory: Logic board, with CPU, RAM and flash memory, and compact flash memory card

The battery pack and outer replaceable IUI connectors are external to the cryptographic boundary. The IUI subsystem and battery subsystem do not implement any cryptographic function; they do not provide any access to CSPs. The IUI connectors and battery pack are replaceable as part of routine maintenance; removal does not affect CM opacity or provide unprotected entry points for probing or other access.

2. Versions and Modes of Operation

The configuration of hardware and firmware for this validation is:

- Hardware: Model 8015 b/g, Model 8015 a/b/g, or Model 8015 a/b/g/n
- FIPS Kit P/N: 49000550
- Firmware Version: 12.1.3

Model 8015 supports 802.11 b/g, 802.11 a/b/g, and 802.11 a/b/g/n.

The firmware version is displayed on the software versions page. To display the firmware version:

1. Press the **Options** button from the main page.
2. Press the **Page Down** soft key to display the **Systems Option 2 of 3** page.
3. Select the **Software Versions** option and press the **View** soft key for the PC Unit.

2.1. FIPS Approved Mode of Operation

The CM only provides a FIPS approved mode of operation, comprising all services described in the section Roles and Services.

The CM always performs all FIPS 140-2 required cryptographic self-tests at power up. The CM may perform public operator (unauthenticated) role services for the operation of the attached pump at any time following successful power on self-tests and configuration checks.

The following conditions must be met prior to operation:

- The cryptographic self-tests performed at power on passed.
- The tamper-evident seals (physical security) have been applied.
- FIPS 140-2 Mode flag has been enabled on the CM.
  NOTE:
  Informational purposes only and has no impact on CM functionality.

The operator can verify that the CM approved mode flag has been set on the display page titled **System Options 3 of 3**.

To display FIPS mode:

1. Press the **Options** button from the main page.
2. Press the **Page Down** soft key twice to display the **Systems Options 3 of 3** page containing the FIPS mode status.

The CM displays FIPS 140-2 Mode Enabled only if the FIPS mode flag has been set. The FIPS 140-2 mode indicator displays disabled otherwise.

FIPS 140-2 mode is set using the System Maintenance to enable FIPS mode service. After FIPS 140-2 mode is enabled, it cannot be set back to disable.

3. Ports and Interfaces

The CM implements the ports and interfaces shown in the following table.

Table 3-1: FIPS 140-2 Ports and Interfaces

Port	Number of Ports	Name and Description	FIPS 140-2 Designation
LCD display	1	LCD display located on the front panel, used to provide visual feedback to public operator (unauthenticated user).	Status output
System maintenance serial port	1	Rear panel RJ-45 connector used for administrative control of the CM.	• Data input • Data output • Control input • Status output
IUI ports	2	The IUI Right and IUI Left ports on the sides of the CM provide control over pump expansion devices. These interfaces provide no cryptographic function or access to CSPs.	• Data input • Data output • Control input • Status output • Power/ground
802.11 card antenna	1	Wireless communications interface, enabling communications with external wireless access point devices.	• Data input • Data output • Control input • Status output
Tamper resist switch	1	Rear panel button used to deter casual changes to infusion pump settings by disabling the front panel buttons. Tamper resist in this context is not related to cryptographic functions. No CSPs are affected by this switch.	Control input
Status LEDs	1	• Front panel status LEDs: AC power, battery, and communications. • Rear panel: 802.11 card LED for 802.11 status. These LEDs have no cryptographic relevance.	Status output
Speakers	1	Audio status output to indicate alarm status.	Status output
Keypad	1	Front panel keypad for local control of the CM.	Control input
Power port	1	AC power input.	Power/ground
Battery port	1	Battery pack connector.	Power/ground

The CM requires an external device (the System Maintenance) for module administrative configuration, including CSP entry. The System Maintenance software connects only to the RS-232 serial port depicted in Figure 1-2. No other connection port is used by the System Maintenance software.

CSPs entry can also be performed using Systems Manager over the encrypted network connection.

4. Cryptographic Functionality

The CM performs FIPS 140-2 Approved cryptography in three services:

- The authentication handshake between the CM and Systems Manager, using SHA-256 and externally established shared secret.
- Encryption and decryption of communications taking place over the network connection between the CM and the Systems Manager.
- Verification of authenticity using the RSA signature verification algorithm of firmware transferred to CM from the Systems Manager over network connection.

4.1. Approved Algorithms

The CM supports the following FIPS Approved and allowed algorithms.

Table 4-1: FIPS Approved Algorithms

Cert.	Algorithm	Mode	Description	Functions/Caveats
4428	AES	CBC	Key Sizes: 128, 192, 256	Encrypt, Decrypt Only 128-bit key size is used.
3560	HMAC	N/A	SHA-256	Data authentication, as used within KTS
N/A	KTS	CBC	AES Cert. #4428 HMAC Cert. #3560	Key establishment methodology provides 128 bits of encryption strength.
2410	RSA	X9.31 PKCS1_1.5 PSS	n = 1024 SHA-256 n = 2048 SHA-256 n = 3072 SHA-256	SigVer Only PKCS1_15 with 2048-bit key size is used.
3646	SHS	SHA-256	N/A	Message digest generation

4.2. Non-FIPS Approved, but Allowed Algorithms

The CM includes an embedded off-the-shelf 802.11 wireless module. The 802.11 module implements uncertified cryptographic algorithms to satisfy wireless communication protocols in the deployment environment; no FIPS 140-2 security claims are made for 802.11 communications cryptography. The wireless module and the library used for the 802.11 communications contain the non-approved algorithm implementations listed below. None of these algorithms are used by the module for any other purpose; the module encrypts all traffic with AES-128 independent of the 802.11 communications cryptography, which conforms with IG 1.23.

Table 4-2: Non-FIPS Approved, but Allowed Algorithms

Non-FIPS Approved Algorithm
Uncertified cryptographic functions implemented by the 802.11 RF module: • AES 128/192/256 (non-compliant) • Blowfish • CAST • DES—ECB, CFB, CBC, & OFB modes • DH (non-compliant) • DSA (non-compliant) • MD5 • RC2-CBC, RC2-ECB, RC2-CFB64, RC2-OFB64 • RC4 • RIPEMD • RSA (non-compliant) • SHA-1 (non-compliant) • SHA-256 (non-compliant) • Triple DES—ECB, CFB, CBC & OFB modes (non-compliant)
Uncertified cryptographic functions implemented by the standard C++ library: • RNG (non-compliant): Third-party supplied RNG to generate challenge values for CO authentication.

4.3. Critical Security Parameters (CSPs)

The CM implements the CSPs listed in the following table:

Table 4-3: Critical Security Parameters (CSPs)

CSP Name	Length and Type
ENC	AES 128-bit symmetric key used to encrypt and decrypt all traffic between the module and the Systems Manager. The module supports eight instances of this CSP.
CU-AUTH	CU authentication. A character string used in the CU authentication handshake with the Systems Manager hashed by SHA-256 along with a nonce. The module supports eight instances of this CSP. A six-character minimum string length is enforced by the CM.
CM-AUTH	CM authentication. A character string used in the optional CM authentication handshake to the Systems Manager hashed by SHA-256 along with a nonce. The module supports eight instances of this CSP. A six-character minimum string length is enforced by the CM.
CO1-AUTH	User name and password strings used in the CO authentication when communicating with the System Maintenance over the System Maintenance serial port for use in CSP-related transactions. A six-character minimum string length for user name and for password is enforced by the CM.
CO2-AUTH	User name and password strings used in the CO authentication when communicating with the Systems Manager over the network connection for use in CSP-related transactions or firmware upgrade. A six-character minimum string length for user name and password is enforced by the CM.
KEY-AUTH	HMAC-SHA-256 key used to authenticate CSPs during transfer via Systems Manager. A sixteen-character minimum string length is enforced by the CM.

All CSPs are entered in plain text over the serial port by the CO using the System Maintenance tool. The CSPs can also be updated wirelessly from Systems Manager, encrypted by ENC, and authenticated by KEY-AUTH. The CSP entity association is the network configuration profile identifier; each network configuration profile includes host name and port. The ENC key, CO1-AUTH, CO2-AUTH, CU-AUTH, and CM-AUTH are generated externally to the CM.

The CM does not display or otherwise provide any user feedback of CSPs. The CM does not implement any form of electronic or automated key establishment. The CM does not generate any keys or output any intermediate key values.

All CSPs are destroyed using the zeroize command, which actively overwrites the contents of the onboard flash.

4.4. Public Keys

The CM implements the public keys listed in the following table:

Table 4-4: Public Keys

Key Name	Length and Type
CO_PUB_KEY	Used to verify firmware upgrades using a RSA 2048-bit key.
ROOT_CA_PUB _Key	Used to verify the SUB_CA_PUB_KEY as part of the BD public certificate chain using RSA 2048-bit key.
SUB_CA_PUB_ KEY	Used to verify the CO_PUB_KEY as part of the BD public certificate chain using RSA 2048-bit key.

5. Roles and Services

5.1. Identification and Authentication

The CM supports four distinct operator roles as described in Table 5-1.

Table 5-1: Roles and Required Identification and Authentication

ID	Role Description	Authentication Type	Authentication Data
CO1	Cryptographic Officer 1: a System Maintenance user authorized to load CSPs.	Role-based authentication. See *CO1 authentication in Table 5-2.*	CO1-AUTH
CO2	Cryptographic Officer 2: a Systems Manager user authorized to load CSPs or firmware upgrades.	Role-based authentication. See *CO2 authentication in Table 5-2.*	CO2-AUTH
CU	Cryptographic User: the role used for communications between the module and the Systems Manager.	Role-based authentication See *CU Authentication in Table 5-2.*	CU-AUTH, CM-AUTH
PO	Public Operator: an implicit role for unauthenticated services	Not authenticated	N/A

An implicit role is defined for the CM: Public Operator (PO). The PO services are the clinical services accessible from the front panel and the subset of services using the System Maintenance tool using the serial port.

The CM enforces the separation of roles; the CO1, the CO2, and the CU roles require authentication and occur over different interfaces. The CO role is applicable to a subset of commands (see Table 5-3) invoked by the System Maintenance tool using CO1-AUTH. Each invocation of an authenticated service requires authentication of a CO. For the CU role, a session is initiated when communication with a Systems Manager is established. The session is destroyed when communication with Systems Manager is terminated.

All authenticated sessions are terminated at the CM power-cycle. The CM does not retain authentication across a power-cycle.

A separate set of credentials is required for each role. The CM does not allow switching of authenticated roles, as these roles are available only using a specific interface of the CM.

The CM allows multiple concurrent operators; however, only one operator per type is allowed at a given instance.

Each authentication mechanism implemented by the CM is listed in the following table, along with the FIPS 140-2 required strength of authentication rationale.

Table 5-2: Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
CO1 Authentication (authentication of CO using the System Maintenance serial port)	CM implements a user name and password-based authentication mechanism to authenticate the CO. A valid password is a minimum of six (6) characters in length and consists of a-zA-Z0-9_~@#%|&()-{} characters. These characters allow a minimum of 3.83E+57 possible combinations. The probability that a random attempt will succeed, or a false acceptance will occur is 1/3.83E+57, or 2.61E-58. It is estimated that the number of maximum number of authentication attempts that can be made is less than 10/minute. The probability of successfully authenticating to the module within one minute is 2.61E-57.
CO2 Authentication (authentication of CO using the Systems Manager network connection)	
CU Authentication (authentication of CU using the Systems Manager network connection)	CM implements a shared passphrase-based mechanism to authenticate the CU. A valid passphrase is a minimum of six (6) characters in length and consists of a-zA-Z0-9_~@#%|&()-{} characters. These characters allow a minimum of 3.83E+57 possible combinations. The probability that a random attempt will succeed, or a false acceptance will occur is 2.61E-58. It is estimated that the maximum number of authentication attempts that can be made is less than 10/minute. The probability of successfully authenticating to the module within one minute is 2.61E-57.

5.2. Services and Service Usage of CSPs

Table 5-3 lists all services performed by the CM, describing authorized roles and CSPs used for each service.

In the listing below:

- "executes using" means the CSP value is used when performing the service
- "update" means a new CSP value is entered into the CM
- "zeroization" means the CSP is overwritten with null values

Table 5-3: Services and Service Usage of CSPs

Service	Description	CO1	CO2	CU	PO
Self-test	Perform power up self-tests which are invoked by power cycling the module. Does not access any CSPs. KAT values are not CSPs.				X
System Manager authenticate	Performs the authentication of Systems Manager (CU) to the CM, and optionally, the CM to the Systems Manager. CU-AUTH is used for Systems Manager authentication to the CM; CM-AUTH is used for CM authentication to Systems Manager.			X	
Secure communication	Encryption and decryption of data between the module and the Systems Manager. Executes using ENC.			X	
Update System Maintenance Login Data	Change CO1 username and password using the System Maintenance. Updates CO1-AUTH and CO2-AUTH.	X			
Update Key Auth	Updates KEY-AUTH. Uses CO1-AUTH.	X			
Server CSP load	Updates ENC, CU-AUTH, and CM-AUTH. Uses CO1, CO2, and KEY-AUTH	X	X		
Zeroize	Overwrite all CSPs with null values.				X
Local show status	Performed using the front panel interface within the network configuration function.				X
Remote show status	Status/health test performed between the CM and the Systems Manager. Does not access any CSPs.			X	
Clinical device configuration and services	All clinical, non-cryptographic services provided by the CM. No CSPs are accessed by these services.				X

Service	Description	CO1	CO2	CU	PO
Enable FIPS mode	Set FIPS 140-2 Mode flag. (No operational impact)				X
Firmware upgrade	Verify authenticity of CM firmware transferred from Systems Manager. Uses CO2_AUTH.		X		
Display FIPS mode	Show FIPS 140-2 Mode flag status.				X
Power down	Power downs the CM.				X

Local show status and *Remote show status* information does not contain CSPs or sensitive data that if misused could lead to a compromise of the CM.

NOTE:
Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-2 evaluation.

6. Physical Security Policy

6.1. Physical Security Mechanisms

The CM is a multichip standalone embodiment with an opaque covering and tamper-evident seals at all potential access points and seams. The tamper-evident seals shall be installed for the module to operate in a FIPS Approved mode of operation.

See *Appendix—FIPS 140-2 Physical Security Considerations and Tamper Seal Installation* for figures that show the placement of the physical tamper-evident seals. These seals are designed to provide tamper evidence and have been tested as a part of the FIPS 140-2 validation process.

6.2. Operator Required Actions

The following table outlines the inspection and testing of the physical security mechanisms.

Table 6-1: Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper-Evident Seals	Annual inspection of the device for tamper evidence. On initial deployment, devices are configured with tamper-evident seals and the device is placed into clinical use.	Processes for inspection of Physical Security can be found in the *FIPS 140-2 Compliance Instructions for BD Alaris™ Products*. This process requires physical inspection of the tamper-evident seals to verify integrity and secure adhesion.

7. Self-Test

Power up cryptographic algorithm self-tests and software integrity test.

The operator can command the CM to perform the power-up self-test by cycling power. Power-up self-tests execute without operator action. The CM performs the following self-tests at power up:

- Verification of all CM firmware for integrity using CRC-32
- Verification of AES algorithm function using AES CBC encrypt and decrypt known answer tests
- Verification of SHA-256 algorithm function using a SHA-256 known answer test
- Verification of RSA signature verification algorithm using an RSA signature verification known answer test with a 2048-bit key
- Verification of HMAC-SHA256 generation algorithm function using a HMAC-SHA256 generation known answer test.

7.1. Conditional Cryptographic Tests

The DRNG is tested on each call for a stuck-fault, comparing the current DRNG output to the previous value to ensure that the previous value has not been repeated.

The CM also supports a firmware update test using RSA 2048-bit signature verification.

7.2 Critical Functions Tests

The CM performs the following tests at power-up.

- Memory test
- Audio-speaker test
- Power-supply test
- Keyboard test

In addition to the power-up tests, the CM performs continuous memory tests.

8. Electromagnetic Interference/Compatibility

The module conforms to the EMI/EMC requirements for intentional radiators.

9. Appendix—FIPS 140-2 Physical Security Considerations and Tamper Seal Installation

This procedure provides the steps for applying the tamper-evident seals on the BD Alaris™ and Alaris™ PC Unit Model 8015.

Part Number	Description
49000550	FIPS seal kit (includes tamper-evident seals and orange stick)
H0000418	Tamper-evident seals
10927242	Orange stick
N/A	Cotton tip applicator or soft cloth

The tamper-evident seals are provided in quantities of seven (7) seals per strip (Figure 9-1). When the tamper-evident seals are applied to the BD Alaris™ or Alaris™ PC Unit, they are valid until removed, damaged, or compromised. The expiration date of the tamper-evident seals is included in the packaging. When applied before the expiration date, the seals are valid for intended use.

The locations for the tamper-evident seals is roughly the same for all models. Seals #1 and #2 are located on the sides of the models (see Figure 9-7) and Seal #7 is located on the back inside panel of the models (see Figure 9-16). However, for the specific placement locations of Seals #3, #4, #5, & #6 on each model, please refer to Figures 9-8 through 9-13 below.

Figure 9-1: Strip of FIPS Seals

9.1. Applying Tamper-Evident Seals

NOTE:
Placing the device face down on a work surface can result in damage to the operation panel. Lay a cloth down before placing the device on its front panel.

1. Before applying the tamper-evident seals, clean the surfaces where the seals will be applied with 70% isopropyl alcohol and ensure there is no residue. Allow the surface to dry.
2. Using finger/thumb pressure, slowly roll back the liner (backing material) to expose the adhesive side of the seal.

NOTE:
As much as possible, avoid touching the adhesive with your fingers, or the seal may tamper.

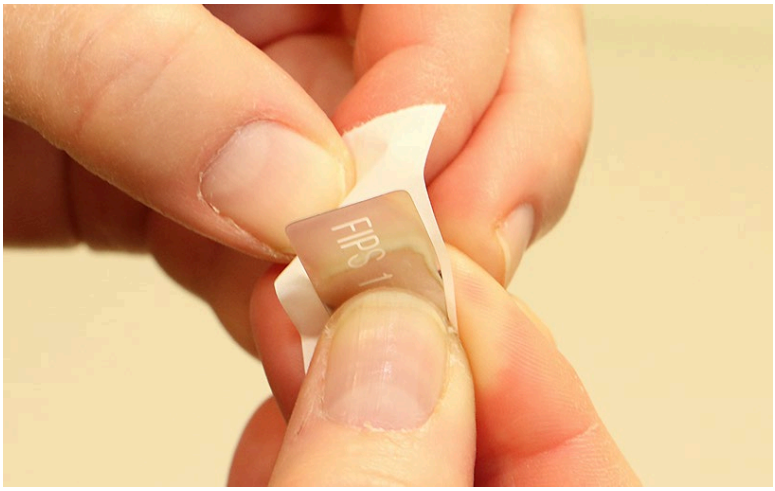

Figure 9–2: Rolling Back the Liner

3. Place the exposed adhesive side of the seal on the device, roll the backing off the label, and roll the seal onto the device.

Figure 9–3: FIPS Seal Application

4. Use the orange stick to ensure that the seal is affixed to cracks and crevices. Ensure full coverage. See detailed instructions in *Location of the FIPS Seal Labels* on *page* 28 for locations of the seals.

Figure 9–4: Using Orange Stick to Ensure Seal is Affixed

5. Apply firm pressure across the entire seal surface.

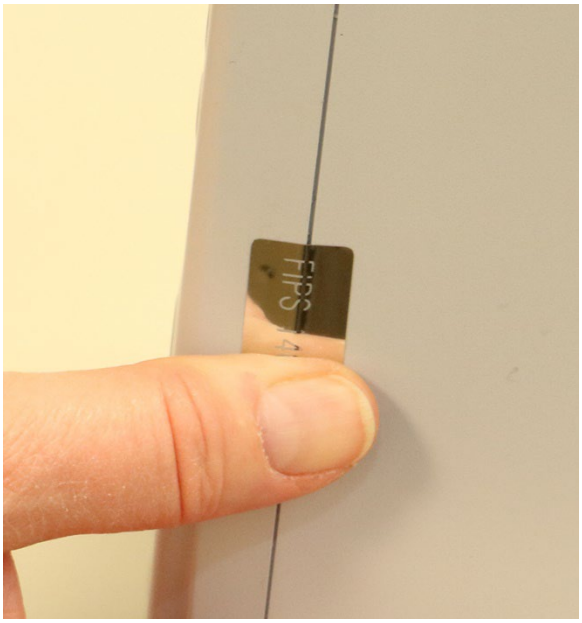

Figure 9–5: Applying Firm Pressure

6. Leave the seals to cure for 24 hours.

9.2. Location of the FIPS Seal Labels

Before applying the FIPS seal labels to the various locations on the device, carefully read and understand the instructions in *Applying Tamper-Evident Seals on page 26*.

NOTE:
It is important to place the seals in the correct locations, as described in this section. If the seals are incorrectly placed, the PC Unit may not be fully FIPS 140-2 compliant.

NOTE:
A small amount of wrinkles in the seals is expected and acceptable.

Figure 9–6: Acceptable Wrinkles

9.2.1. On the Seams on the Side of the Device

Figure 9-7 shows the location of the tamper-evident seals on the seams (grooves) that connect the rear and front cases of the device. Apply one seal on the left side and one seal on the right side of the device.

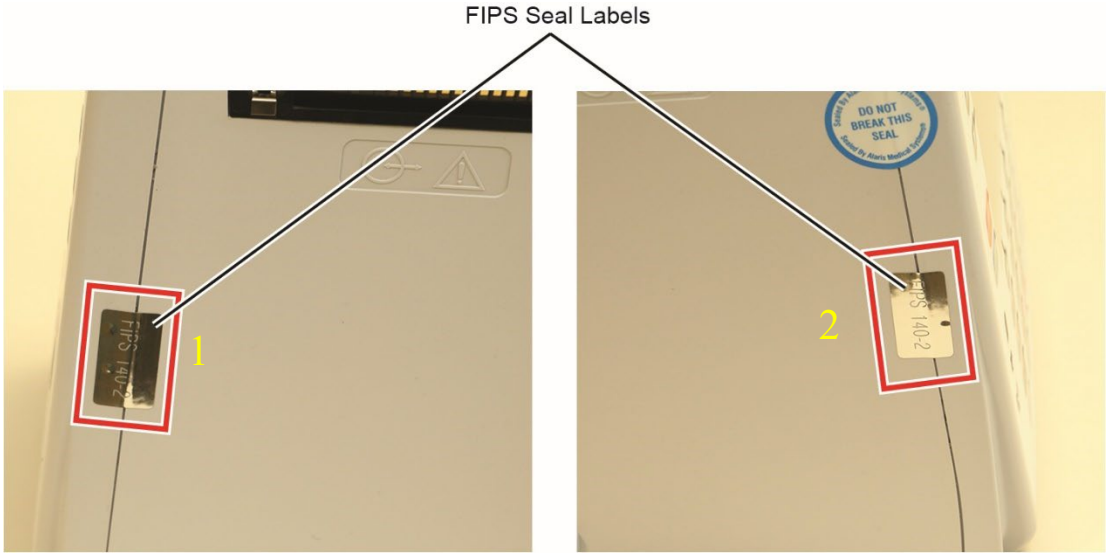

Figure 9–7: FIPS Seal on Seams

9.2.2. On the Back of the Device

Figures 9-8 and 9-13 show the location of the tamper-evident seals on the back (rear panel) of the device. Note that there are three different rear panels: Model 8015 (b/g), Model 8015 (a/b/g) and Model 8015 (a/b/g/n). Reference the figures with the back cover used on your model.

Model 8015 (b/g)

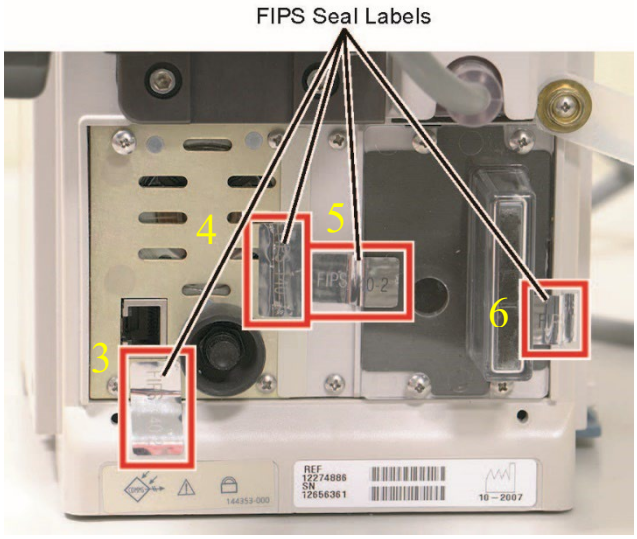

Figure 9–8: Model 8015 (b/g) FIPS Seals on Back of Device

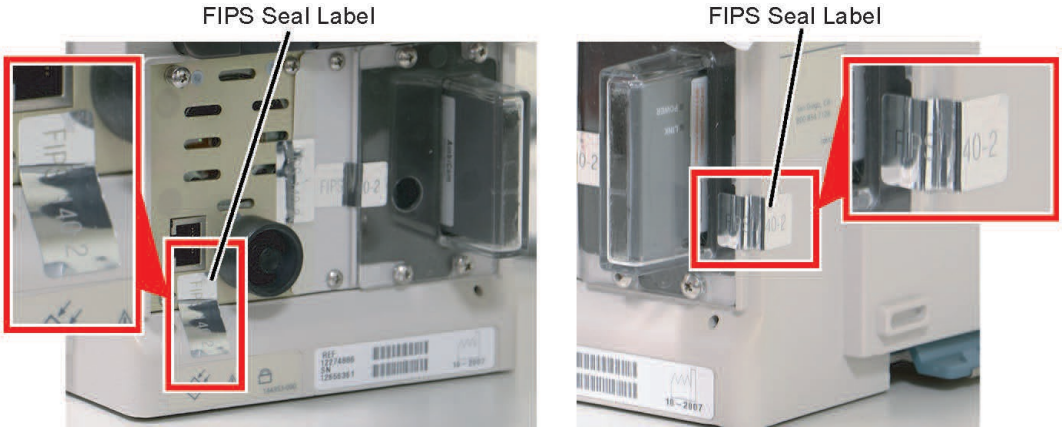

Figure 9–9: Model 8015 (b/g) Side Views

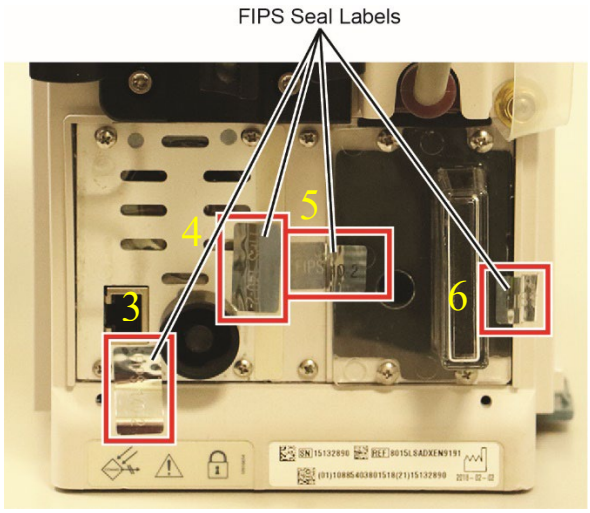

Figure 9–10: Model 8015 (a/b/g) FIPS Seals on Back of Device

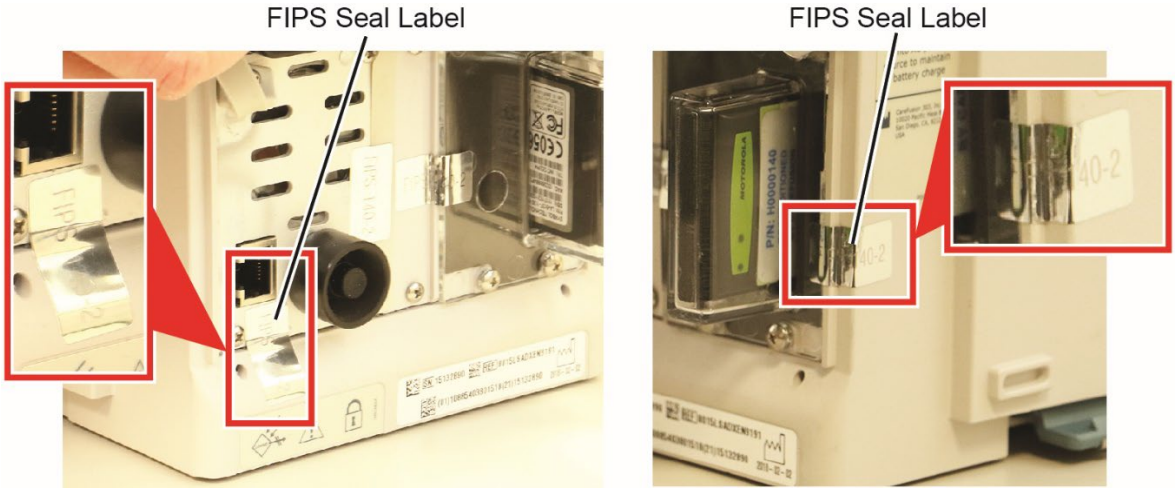

Figure 9–11: Model 8015 (a/b/g) Side Views

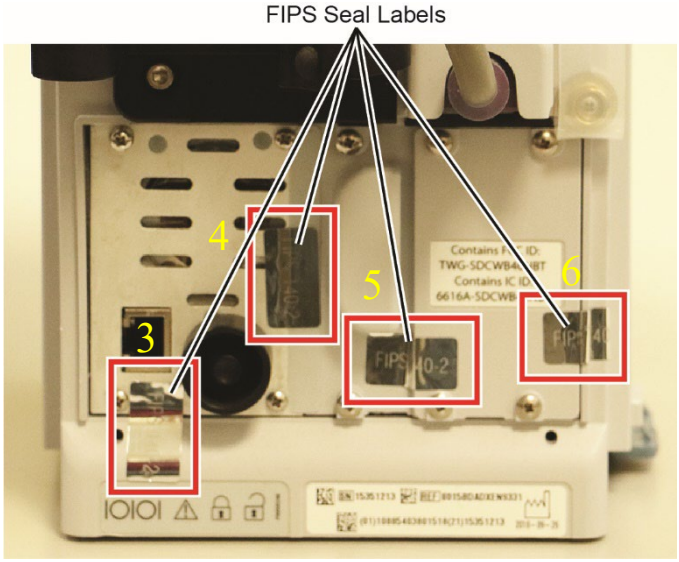

Figure 9–12: Model 8015 (a/b/g/n) FIPS Seals on Back of Device

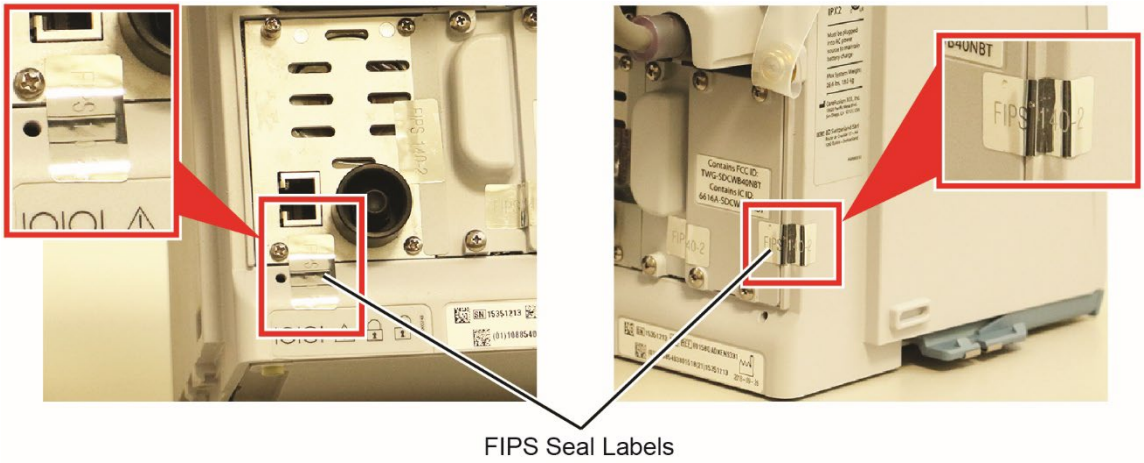

Figure 9–13: Model 8015 (a/b/g/n) Side Views

9.2.3. On the Battery Connector

Figure 9-17 shows the location of the tamper-evident seal on the battery connector.

1. Using screwdriver, remove the screws on the bottom panel.

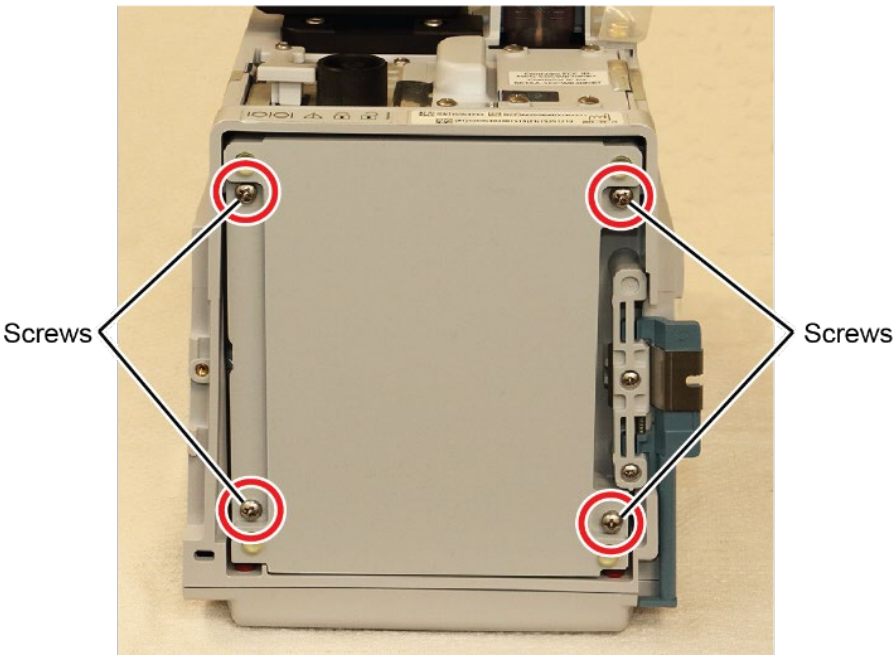

Figure 9–14: Bottom of Device with Battery Pack Installed

2. Remove the battery pack.

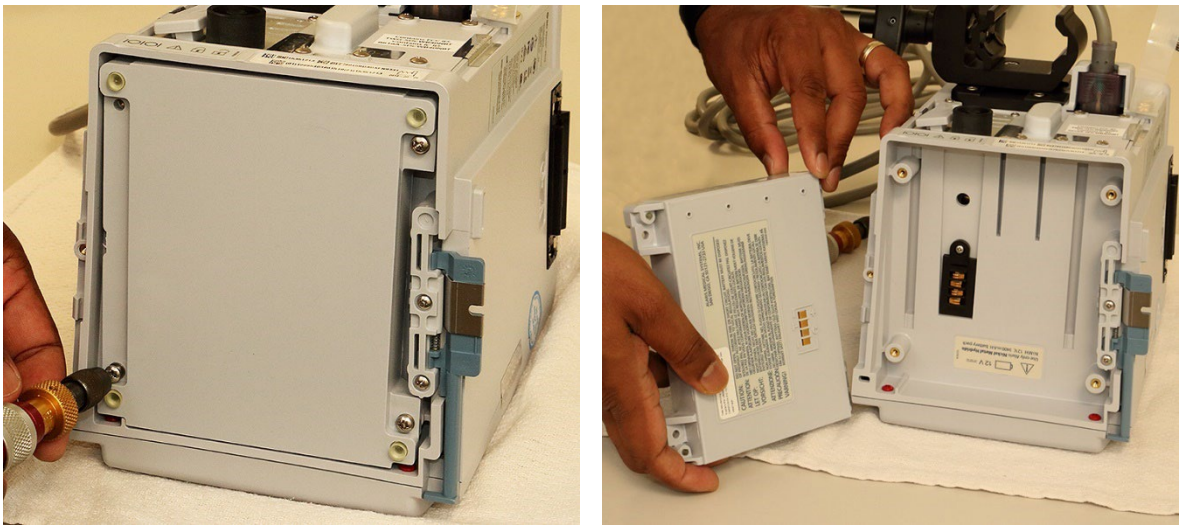

Figure 9–15: Battery Pack being Removed

3. Place the seal on the panel, with enough label overhanging so it fits into the groove on the black battery connector.

Figure 9–16: FIPS S on Battery Connector

4. Use the orange stick to press the seal into the groove. Apply pressure to the seal to affix it to the panel.

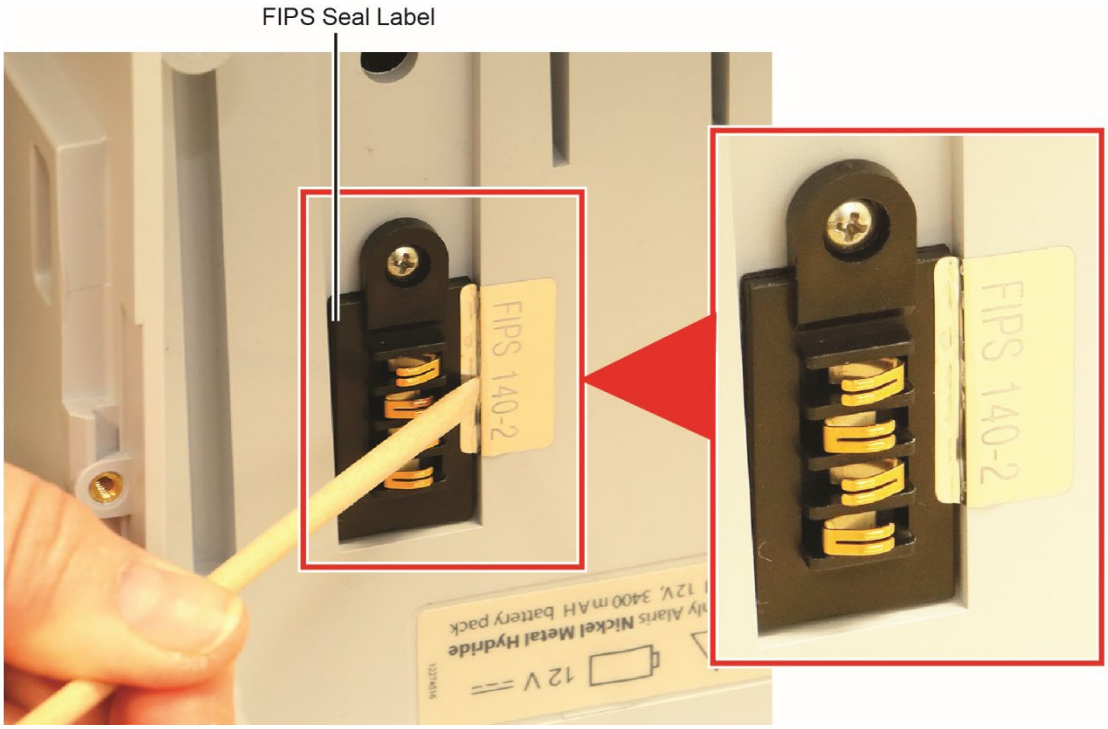

Figure 9–17: Seal on Battery Connector

WARNING

Do not allow the tamper-evident seal to touch the battery metal connector. This metalized seal is conductive. If the tamper-evident seal touches the battery connector it may short the battery causing overheating and damage.

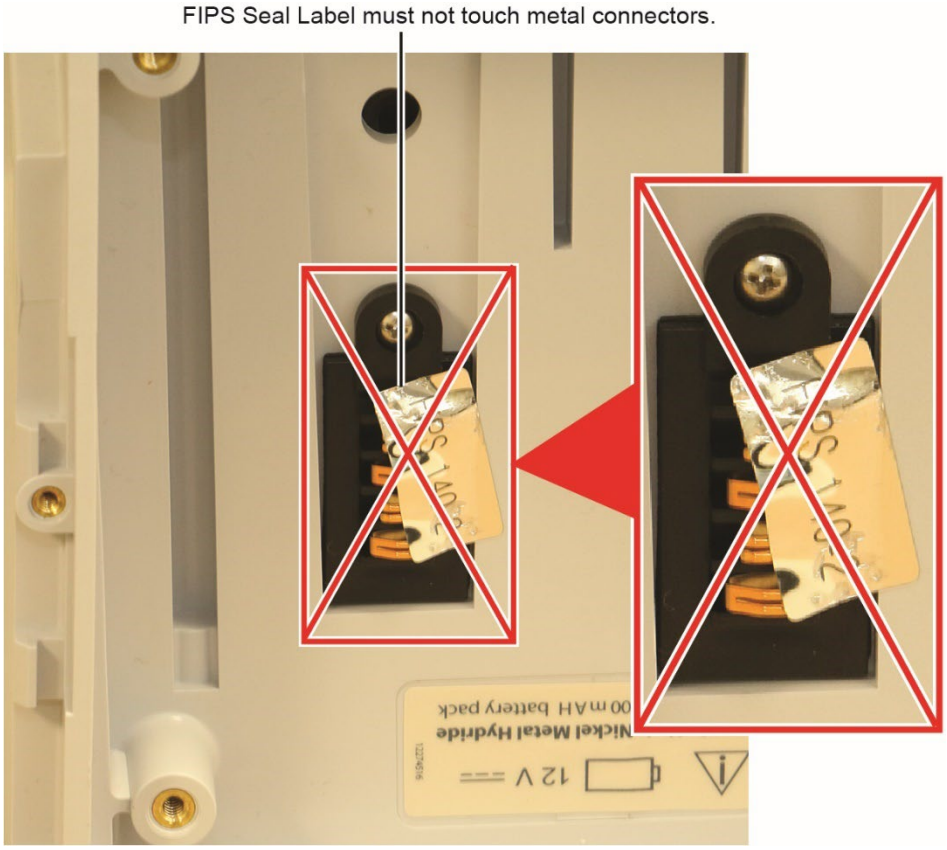

Figure 9–18: FIPS Seal Must Not Touch Metal Connectors

5. Reinstall the battery pack.

WARNING

Failure to correctly follow the battery installation instructions may lead to intermittent battery connection, which could result in a loss of power and interruption in patient therapy.

   a. Verify that the battery connectors are not corroded, damaged or partially covered by the FIPS seal.
   b. Line up the battery connectors.
   c. Carefully place the battery inside the battery well.
   d. Add a washer to each of the four battery screws.
   e. Place one screw with a washer in each of the four battery screw wells.
   f. Tighten each of the four battery screws to 6 in/lb.

6. Perform battery conditioning. Refer to the BD Alaris™ or Alaris™ technical service manual.

9.2.4. Cure Time

NOTE:
After applying the tamper-evident seals, allow the seals to cure for 24 hours. Until the 24-hour curing process has occurred, the PC Unit is not compliant with recommended security practices. Hospital policy will determine if PC Unit can be placed into clinical service during this curing time. BD makes no claim as to the efficacy of tamper-evident seals that are not allowed to cure for 24 hours.

NOTE:
It is recommended that the tamper-evident seals be replaced if applied incorrectly or if the seals show any sign of wear and tear. Ensure that the device is zeroized every time a tamper-evident seal is replaced.

9.3. Removing the Tamper-Evident Seals

BD cannot guarantee the performance of the tamper-evident seals if new seals are placed on top of old seals or if residue or remains of previous seals are not properly removed before the application of new seals.

When the tamper-evident seals are applied to the device, it is up to your facility to decide when to replace the seals. They do not need to be replaced unless they show signs of wear and tear and/or tampering. The seals are destroyed when removed and cannot be reused.

Ensure that the device is zeroized every time a tamper-evident seal is replaced.

9.3.1. Cleaning Products Recommended by BD

BD recommends the use of 70% isopropyl alcohol (IPA) on the device to clean the residue left behind when the tamper-evident seals are removed.

For more cleaning agents, go to the link below and select the Alaris™ System recommended cleaning products tip sheet: *www.bd.com/alarissystemcleaning*

9.3.2. Removing Tamper-Evident Seals

NOTE:
Do not use tools that may scratch or damage the surface of device.

The following procedure explains how to remove the seals.

1. Start the removal process using a fingernail or other thin tool that can peel up a corner of the seal.

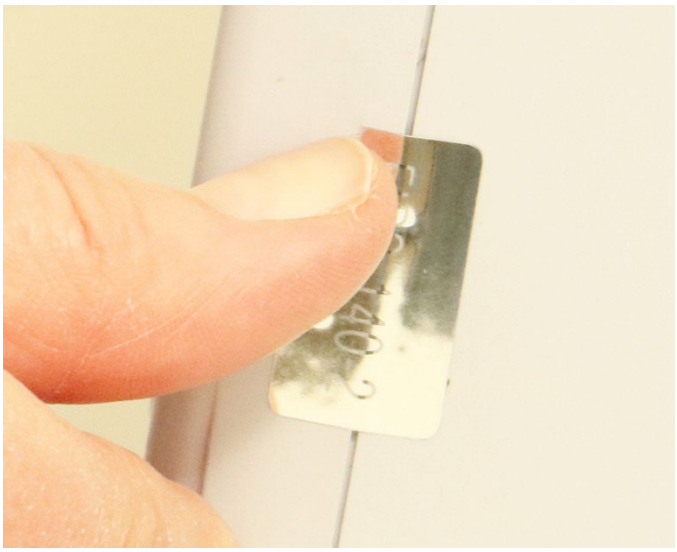

Figure 9–19: Fingernail Removing the Edge of Seal

2. Use tweezers to pull the seal off the device. Leave no portion of the seal on the device. The seal cannot be reused.

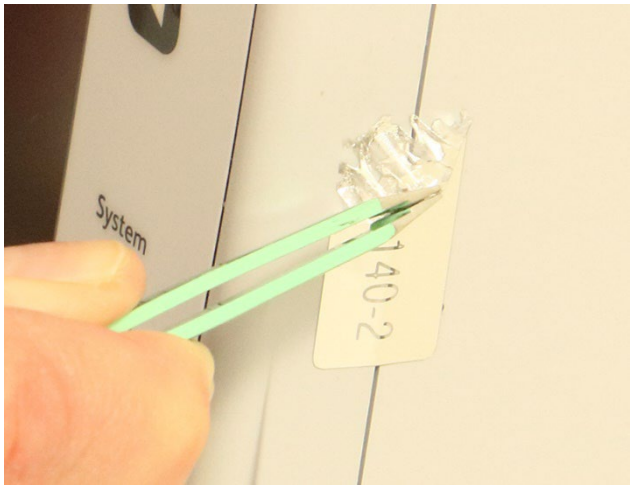

Figure 9–20: Tweezers Removing a FIPS Seal

3. Dampen a soft cloth or cotton-tipped applicator with 70% isopropyl alcohol. Ensure that the soft cloth or applicator is not dripping wet.
4. Remove the seal residue with soft cloth or applicator.

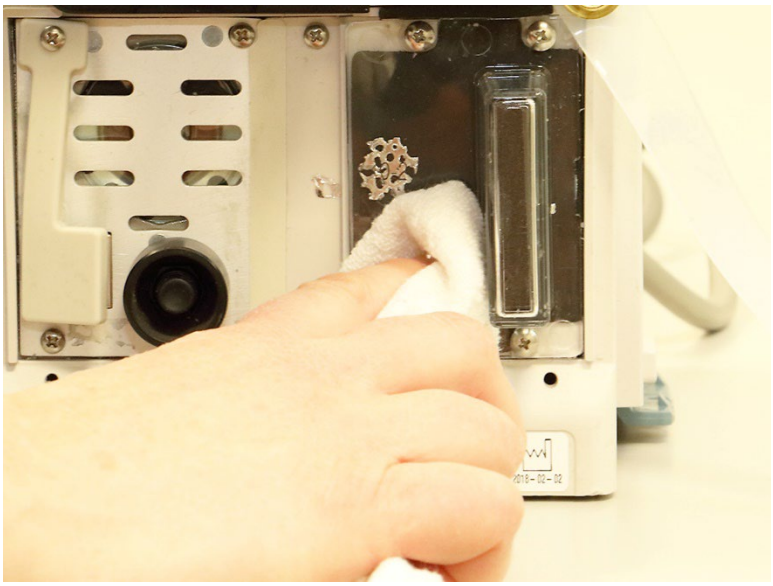

Figure 9–21: Removing Residue

See *Location of the FIPS Seal Labels* on *page 28* for all locations of the seals. Include the seal on the battery connector.

5. Wait 10 minutes for the device to dry before applying new seals.
6. Ensure that battery connector and surrounding areas are dry.
7. Refer to section *Applying Tamper-Evident Seals on page 26* to apply new seals.

NOTE:
Before reinstalling the tamper evident seals, ensure that the screws on the rear panel of the Alaris™ PC Unit are properly torqued to 6 in. lb. according to the BD Alaris™ or Alaris™ technical service manual.

9.4. Signs of Tampered Seals

Inspect PC Unit on a regularly scheduled basis as determined by the security officer of your hospital. If a PC Unit has been verified as tampered with, alert the hospital security officer to the situation because hospital network configurations may vary. This breach of security must be evaluated by the security officer and appropriate action must be taken. For assistance with CSP reconfiguration on the system, please consult with BD technical support.

Below are some examples of tampered seals.

- The tamper-evident seal has been sliced through the groove with a razor or other sharp object (Figure 9-22).

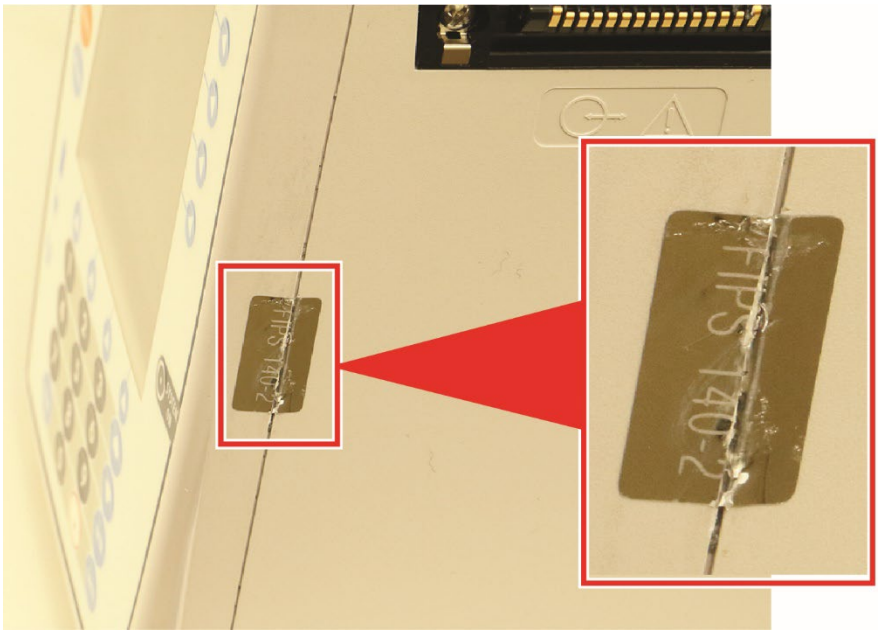

Figure 9-22: Seal Sliced through Sharp Object

- The tamper-evident seal has been partially removed. The tamper evidence is when the seal looks honeycombed and the seal might leave behind residue (Figure 9-23).

  Some seals may not leave behind residue. Signs of seal residue depends on how long the seal is left on the device.

Figure 9-23: Tampered FIPS Seal

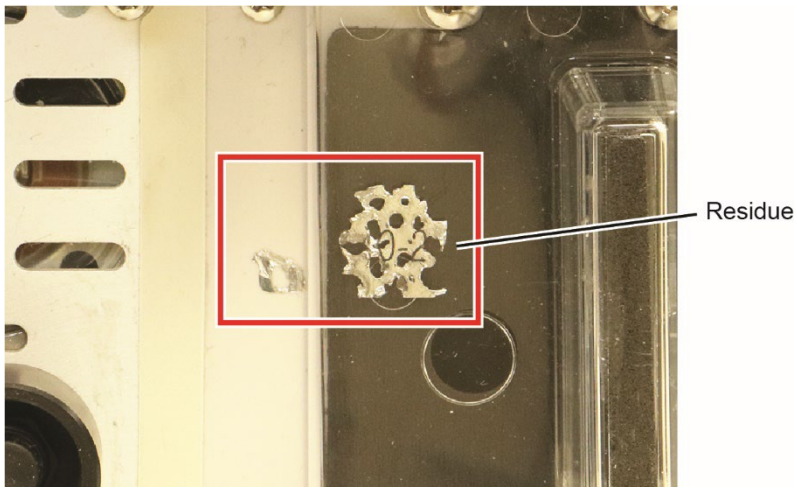

Figure 9-24: Residue from Removed Seal (Sign of Tampering)