Outset Medical, Inc.

Tablo Medical Informatics System

Hardware Version: 1.0
Hardware Part Number: PN-0002824
Firmware Version: MIES 4.9.12.6269

FIPS 140-3 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.2

Prepared for:

Outset Medical, Inc.
3052 Orchard Drive
San Jose, CA 95134
United States of America

Phone: +1 669 231-8200
www.outsetmedical.com

Prepared by:

Corsec Security, Inc.
12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
www.corsec.com

Abstract

This is a non-proprietary Cryptographic Module Security Policy for Tablo Medical Informatics System (firmware version: MIES 4.9.12.6269) from Outset Medical, Inc. (Outset). This Security Policy describes how Tablo Medical Informatics System meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-3, which details the U.S. and Canadian government requirements for cryptographic modules. More information about the FIPS 140-3 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website, which is maintained by the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS).

This document also describes how to run the module in a secure Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-3 validation of the module. Tablo Medical Informatics System is referred to in this document as Medical Informatics System or the module.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-3 cryptographic module security policy. More information is available on the module from the following sources:

- The Outset website (www.outsetmedical.com) contains information on Tablo from Outset.
- The search page on the CMVP website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search) can be used to locate and obtain vendor contact information for technical or sales-related questions about the module.

Document Organization

ISO/IEC 19790 Annex B uses the same section naming convention as *ISO/IEC 19790* section 7 - Security requirements. For example, Annex B section B.2.1 is named “General” and B.2.2 is named “Cryptographic module specification,” which is the same as *ISO/IEC 19790* section 7.1 and section 7.2, respectively. Therefore, the format of this Security Policy is presented in the same order as indicated in Annex B, starting with “General” and ending with “Mitigation of other attacks.” If sections are not applicable, they have been marked as such in this document.

Table of Contents

List of Tables

List of Figures

1. General

The Outset Tablo is a dialysis machine designed from the inside out to offer a better and easier experience for patients and providers. The Outset Tablo machine creates an all-in-one solution that reduces care and infrastructure costs, expands the variety of eligible users, and enables new care delivery models.

The Tablo Hemodialysis System is an automated machine designed to filtrate blood and offers multiple automated maintenance functions. It consists of a water purification system, Tablo cartridge, Non-invasive blood pressure cuff, and a two-way data communication.

The Tablo Hemodialysis System is a mobile indoor unit that establishes a two-way data communication that automatically sends treatment data as well as machine performance to the Outset Tablo Cloud. The Tablo machine includes touchscreen guidance that contains animations and conversational instructions. Figure 1 – Tablo Hemodialysis System Functions below shows the main functions of the Tablo system.

Figure 1 – Tablo Hemodialysis System Functions

The Tablo machine feature set includes inexpensive operations, direct connection to the Tablo Cloud, automated functions, and effective hemodialysis features:

- Blood flow rate of up to 400 mL/min
- Extracorporeal Circuit volume of 140 mL
- Maximum Ultrafiltration Rate of 2,000 mL/hour
- Dialysate Flow Rate of up to 300 mL/min
- Automated daily heat disinfection and weekly chemical disinfection
- Automatic Saline Bolus tracking
- Automated water purification system

The module is the Tablo Medical Informatics System, which is an internal component of the Outset Tablo and provides secure storage and transmission of patient data.

Tablo Medical Informatics System is validated at the FIPS 140-3 section levels shown in Table 1.

Table 1 – Security Levels

ISO/IEC 24579 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic Module Specification	1
3	Cryptographic Module Interfaces	1
4	Roles, Services, and Authentication	1
5	Software/Firmware Security	1
6	Operational Environment	1
7	Physical Security	1
8	Non-Invasive Security	N/A[1]
9	Sensitive Security Parameter Management	1
10	Self-tests	1
11	Life-Cycle Assurance	1
12	Mitigation of Other Attacks	N/A

The module has an overall security level of 1.

[1] N/A – Not Applicable

2. Cryptographic Module Specification

Tablo Medical Informatics System is a hardware module with a multi-chip embedded embodiment. The module is a single board computer (embedded within the Tablo dialysis machine) that securely protects and transmits patient data.

2.1 Operational Environments

Table 2 below lists the module configuration(s) used for validation testing.

Table 2 – Cryptographic Module Tested Configuration

Model	Hardware (Part number and version)	Firmware Version	Distinguishing Features
Tablo Medical Informatics System	PN-0002824 1.0	MIES 4.9.12.6269	High performance ARM processor (NXP i.MX 6Dual), onboard DDR3 and Flash memory, USB, Ethernet, and UART interfaces.

2.2 Algorithm Implementations

Table 3 lists the cryptographic algorithm sources employed by the module.

Table 3 – Cryptographic Algorithm Sources

Certificate Number	Implementation Name	Version	Use
A2699	Tablo Medical Informatics System Bouncy Castle Cryptographic Library	1.0	Provides implementations for general-purpose cryptographic primitives
A2700	Tablo Medical Informatics System CPU Jitter Library	1.0	Conditioning function used in entropy mechanism
A2701	Tablo Medical Informatics System OpenSSL Cryptographic Library	1.0	Provides implementations for general-purpose cryptographic primitives
A2702	Tablo Medical Informatics System TLS KDF Library	1.0	TLS key derivation function implementation
A2703	Tablo Medical Informatics System SSH KDF Library	1.0	SSH key derivation function implementation

Validation certificates for each approved security function are listed in Table 4.

Table 4 – Approved Algorithms Validation Certificates

CAVP Certificate[2]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strengths	Use / function
Tablo Medical Informatics System Bouncy Castle Cryptographic Library				
A2699	**AES** *FIPS PUB 197* *NIST SP 800-38A*	CBC, CTR	128, 256	Encryption/decryption
A2699	**AES** *NIST SP 800-38C*	CCM	128, 256	Encryption/decryption
A2699	**AES** *NIST SP 800-38D*	GCM	128, 256	Encryption/decryption
Vendor Affirmed	**CKG** *NIST SP 800-133rev2*	-	-	Cryptographic key generation
A2699	**CVL** *NIST SP 800-135rev1*	TLS 1.2 KDF	-	Key derivation[3]
A2699	**DRBG** *NIST SP 800-90Arev1*	Counter-based (derivation function – yes; prediction resistance – no)	128, 192, 256-bit AES-CTR	Deterministic random bit generation
A2699	**DSA** *FIPS PUB 186-4*	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	2048	Key generation
		SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	1024, 2048, 3072	Digital signature verification
A2699	**ECDSA** *FIPS PUB 186-4*	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571, P-192, P-224, P-256, P-384, P-521	Key generation, key verification, digital signature verification
A2699	**HMAC** *FIPS PUB 198-1*	SHA-1, SHA2-256, SHA2-384, SHA2-512	112 (minimum)	Message authentication
A2699	**KAS-SSC**[4] *NIST SP 800-56Arev3*	FFC DH	2048/224, 2048/256	Shared secret computation
		ECC CDH	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	Shared secret computation
A2699	**RSA** *FIPS PUB 186-4*	X9.31	1024, 2048, 3072, 4096 (SHA-1, SHA2-256, SHA2-384, SHA2-512)	Digital signature verification
		PKCS#1 v1.5 PSS	1024, 2048, 3072, 4096 (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital signature verification
A2699	**SHS** *FIPS PUB 180-4*	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	-	Message digest
Tablo Medical Informatics System CPU Jitter Library				
A2700	**SHA-3** *FIPS PUB 202*	SHA3-256	-	Conditioning function
Tablo Medical Informatics System OpenSSL Cryptographic Library				

[2] This table includes vendor-affirmed algorithms that are approved but CAVP testing is not yet available.
[3] No part of the TLS protocol, other than the KDF, has been tested by the CAVP and CMVP.
[4] The methods of shared secret computation are approved per FIPS 140-3 IG D.F

CAVP Certificate[2]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strengths	Use / function
A2701	**AES** *FIPS PUB 197 NIST SP 800-38A*	CBC, CTR	128, 256	Encryption/decryption
A2701	**AES** *NIST SP 800-38C*	CCM	128, 256	Encryption/decryption
A2701	**AES** *NIST SP 800-38D*	GCM	128, 256	Encryption/decryption
Vendor Affirmed	**CKG** *NIST SP 800-133rev2*	-	-	Cryptographic key generation
A2701	**DRBG** *NIST SP 800-90Arev1*	Counter-based (derivation function – yes; prediction resistance – no)	256-bit AES-CTR	Deterministic random bit generation
A2701	**DSA** *FIPS PUB 186-4*	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	1024, 2048, 3072	Digital signature verification
A2701	**ECDSA** *FIPS PUB 186-4*	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571, P-192, P-224, P-256, P-384, P-52	Digital signature verification
A2701	**HMAC** *FIPS PUB 198-1*	SHA-1, SHA2-256, SHA2-384, SHA2-512	112 (minimum)	Message authentication
A2701	**KAS-SSC** *NIST SP 800-56Arev3*	ECC CDH[5]	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	Shared secret computation
A2701	**RSA** *FIPS PUB 186-4*	X9.31	1024, 2048, 3072, 4096 (SHA-1, SHA2-256, SHA2-384, SHA2-512)	Digital signature verification
		PKCS#1 v1.5 PSS	1024, 2048, 3072, 4096 (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital signature verification
A2701	**SHS** *FIPS PUB 180-4*	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	-	Message digest
Tablo Medical Informatics System TLS KDF Cryptographic Library				
A2702	**CVL** *NIST SP 800-135rev1*	TLS 1.2 KDF	-	Key derivation[6]
Tablo Medical Informatics System SSH KDF Cryptographic Library				
A2703	**CVL** *NIST SP 800-135rev1*	SSH KDF	-	Key derivation[7]

The vendor affirms the following cryptographic security methods:

- Cryptographic key generation – The module implements cryptographic key generation (CKG) compliant to *NIST SP 800-133rev2* section 4. The module uses unmodified output from its Approved DRBGs (both

[5] ECC CDH – Elliptic Curve Cryptography Cofactor Diffie-Hellman
[6] No part of the TLS protocol, other than the KDF, has been tested by the CAVP and CMVP.
[7] No part of the SSH protocol, other than the KDF, has been tested by the CAVP and CMVP.

OpenSSL DRBG cert. A2701 and Bouncy Castle DRBG cert. A2699) as both symmetric keys and seeds for generating asymmetric key pairs. The module's DRBGs are seeded via entropy generated from the module's internal entropy mechanism.

The module implements the non-Approved but allowed algorithms shown in Table 5 below, in both the Tablo Medical Informatics System OpenSSL Cryptographic Library and Tablo Medical Informatics System Bouncy Castle Cryptographic Library.

Table 5 – Non-Approved Algorithms Allowed in the Approved Mode of Operation

Algorithm	Caveat	Use / Function
AES (Cert. A2701)	-	Key unwrapping

The module employs the non-Approved algorithms with no security claimed shown in Table 6 below.

Table 6 – Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm / Function	Use / Function
Blowfish	Decryption

2.3 Cryptographic Boundary

The cryptographic boundary of the module is defined by the physical perimeter of the Tablo Medical Informatics System (shown in Figure 2). A logical block diagram of the module's hardware components is provided in Figure 3 below.

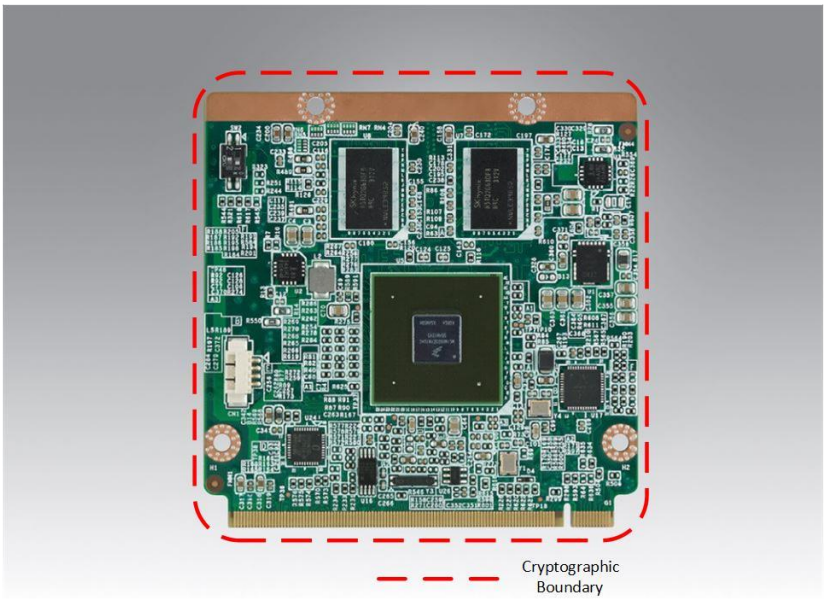

Figure 2 – Tablo Medical Informatics System PN-0002824

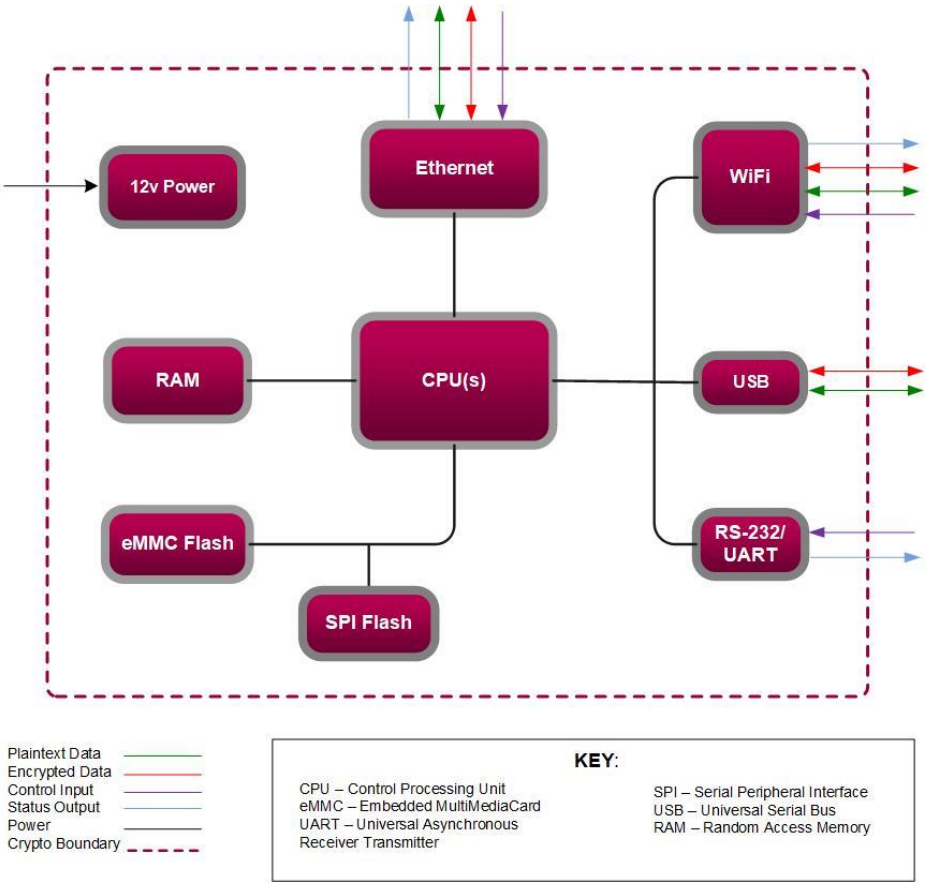

Figure 3 – Module Block Diagram (with Cryptographic Boundary)

2.4 Excluded Components

There are no excluded hardware or firmware components.

2.5 Modes of Operation

The module supports an Approved mode of operation only. When installed, configured, and operated according to this Security Policy, the module does not support a non-Approved mode of operation.

3. Cryptographic Module Interfaces

The module supports the following logical interfaces:

- Data Input
- Data Output
- Control Input
- Status Output
- Power

A mapping of the physical ports to the module's logical interfaces can be found in Table 7. Note that the module does not output control information, and thus has no specified control output interface.

Table 7 – Ports and Interfaces

Physical Port	Logical Interface	Data That Passes Over Port/Interface
RS[8]-232/UART	• Control Input • Status Output	• System state information • Network configuration information • MIES firmware version • MIES operational status
Ethernet	• Data Input • Data Output • Control Input • Status Output	• Black box log data • Treatment data • Patient Data • License information
USB[9]	• Data Input • Data Output	• Wi-Fi configuration and status data • Patient data files • Provisioning
Wi-Fi	• Data Input • Data Output • Control Input • Status Output	• Black box log data • Treatment data • Patient Data • License information
12V DC[10]-Input	• Power	• N/A
LED	• Status Output	• N/A
GPIO[11]	• Status Output	• N/A
USB OTG[12]	(Not in Use)	
SD/MMC[13]	(Not in Use)	
SIM[14] Card slot	(Not in Use)	

[8] RS – Recommended Standard
[9] USB – Universal Serial Bus
[10] DC – Direct Current
[11] GPIO – General Purpose Input/Output
[12] USB OTG – Universal Serial Bus On-The-Go
[13] SD/MMC – Secure Digital Multi-Media Card
[14] SIM – Subscriber Identity Module

Physical Port	Logical Interface	Data That Passes Over Port/Interface
SATA[15]	(Not in Use)	
I²C[16]	(Not in Use)	
I²S[17]	(Not in Use)	
SPI[18]	(Not in Use)	
CAN[19]	(Not in Use)	
HDMI[20]	(Not in Use)	
VGA[21]	(Not in Use)	
Audio	(Not in Use)	

Table 8 – LED Indicator

LED	Meaning
1 blink	Module is loaded
2 blinks	Module is performing self-tests
3 blinks	Module has entered normal operation
4 blinks	Module has entered critical error state
8 blinks	Module performing “Import Legacy Data” operation

[15] SATA – Serial ATA
[16] I²C – Inter-Integrated Circuit
[17] I²S – Inter-IC Sound
[18] SPI – Serial Peripheral Interface
[19] CAN – Controller Area Network
[20] HDMI – High-Definition Multimedia Interface
[21] VGA – Video Graphics Array

4. Roles, Services, and Authentication

The sections below describe the module's authorized roles, services, and operator authentication methods.

4.1 Authorized Roles

The module supports a Crypto Officer (CO) role and a User role. The CO role performs cryptographic initialization or management functions and general security services. The User role performs general security services, including cryptographic operations and other approved security functions. The operator assumed a Crypto Officer role implicitly by invoking a service allocated to the Crypto Officer and assumes a User role implicitly by invoking a service allocated to the User. The module does not support multiple concurrent operators.

Table 9 – Roles, Service Commands, Input and Output

Role	Service	Input	Output
CO	Show Status	Command	Module operational status
CO	Perform Self-tests On-demand	Power-cycle	Status
CO	Show Module Version	Command	Module name and version
CO	Perform Zeroization	Command	Status
User	Import Provision File	Command, Provision File	Status
User	Import Patient Data	Command, Patient Data	Status
User	Export Patient Data	Command, Patient Data	Data, Status
User	Import License Info and Configuration File	Command, License Info, Configuration File	Status
User	Establish SSH Session	Command, Endpoint	Status
User	Establish TLS Session	Command, Endpoint	Status
User	Transmit Data to Cloud	Command, Data	Status, data

4.2 Operator Services

Descriptions of the services available to the authorized roles are provided in Table 10 below. Please note that the keys and Sensitive Security Parameters (SSPs) listed in the table indicate the type of access required using the following notation:

- G = Generate: The module generates or derives the SSP.
- R = Read: The SSP is read from the module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the module.
- E = Execute: The module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The module zeroizes the SSP.

Table 10 – Approved Services

Service	Description	Approved Security Function(s)	Keys/SSPs	Roles	Access rights to Keys/SSPs	Indicator
Show Status	Returns mode status	None	-	CO	-	N/A[22]
Perform Self-tests On-demand	Performs pre-operational self-tests	None	-	CO	-	N/A
Show Module version	Returns module versioning information	None	-	CO	-	N/A
Perform Zeroization	Zeroizes memory and storage locations containing keys and SSPs	None	Master Key	CO	Master Key – Z	"PHI related files are removed successfully SUCCESS"
Import Provision File	Imports provision file via USB	AES (CBC) CTR DRBG SHA-3	Master Key Provisioning File Decryption Key Treatment In-Progress Data Key CTR DRBG Entropy CTR DRBG Seed CTR DRBG 'V' Value CTR DRBG 'Key' Value	User	Master Key – E Provisioning File Decryption Key – E Treatment In-Progress Data Key – G CTR DRBG Entropy – W, E CTR DRBG Seed – G, E CTR DRBG 'V' Value – G, E CTR DRBG 'Key' Value – G, E	"Decrypting provisioning file"
Import Patient Data	Imports patient data via USB	AES CBC	Patient Data Encryption Key Prescription Key	User	Patient Data Encryption Key – E Prescription Key – W, E	"Decrypting patient data"
Export Patient Data	Exports patient data via USB	AES CBC	Patient Data Encryption Key Prescription Key	User	Patient Data Encryption Key – E Prescription Key – W, E	"Encrypting patient data"
Import License Info and Configuration File	Imports license info and configuration file from the Internet	AES (CBC, GCM)	License File Decryption Key Configuration File Decryption Key	User	License File Decryption Key – E Configuration File Decryption Key – E	"Finished downloading license file successfully" And "Retrieving remote config from {location} Retrieved config: {config text}"

[22] Note that the **Show Status**, **Perform Zeroization**, and **Show Module Version** services do not require an Approved security service indicator per FIPS 140-3 Implementation Guidance 2.4.C.

Service	Description	Approved Security Function(s)	Keys/SSPs	Roles	Access rights to Keys/SSPs	Indicator
Establish SSH Session	Establishes a SSH session between the module and Wi-Fi module within Tablo	AES (CBC, CTR, GCM) CKG DRBG DSA ECDSA KAS-FFC-SSC KAS-ECC-SSC SSH KDF SHA-3	AES GCM IV SSH Password DH Private Key Component DH Public Key Component ECDH Private Key Component ECDH Public Key Component SSH Shared Secret SSH Session Key SSH Authentication Key CTR DRBG Entropy CTR DRBG Seed CTR DRBG 'V' Value CTR DRBG 'Key' Value	User	AES GCM IV – G, E SSH Password – E DH Private Key Component – G, E DH Public Key Component – G, W, R, E ECDH Private Key Component – G, E ECDH Public Key Component – G, W, R, E SSH Shared Secret – G, E, Z SSH Session Key – G, SSH Authentication Key – G, CTR DRBG Entropy – W, E CTR DRBG Seed – G, E CTR DRBG 'V' Value – G, E CTR DRBG 'Key' Value – G, E	"SSH command complete"
Establish TLS Session	Establishes a TLS connection	CKG DRBG DSA ECDSA KAS-FFC-SSC KAS-ECC-SSC RSA SHA-3 TLS KDF	DH Private Key Component DH Public Key Component ECDH Private Key Component ECDH Public Key Component TLS Premaster Secret TLS Master Secret TLS Session Key TLS Authentication Key AES GCM IV CTR DRBG Entropy CTR DRBG Seed CTR DRBG 'V' Value CTR DRBG 'Key' Value	User	DH Private Key Component – G, E DH Public Key Component – G, W, R, E ECDH Private Key Component – G, E ECDH Public Key Component – G, W, R, E TLS Premaster Secret – G, E, Z TLS Master Secret – G, E, Z TLS Session Key – G TLS Authentication Key – G AES GCM IV – G CTR DRBG Entropy – W, E CTR DRBG Seed – G, E CTR DRBG 'V' Value – G, E CTR DRBG 'Key' Value – G, E	"TLS transaction complete"
Transmit Data to Cloud	Transmits patient data to the cloud	AES (CBC, CCM, GCM) HMAC SHS	TLS Session Key TLS Authentication Key AES GCM IV Treatment In-Progress Data Key	User	TLS Session Key – E TLS Authentication Key – E AES GCM IV – E Treatment In-Progress Data Key – E	"TLS transaction complete"
Import Legacy Data	Import legacy patient data from previous format	AES CBC	Patient Data Encryption Key Prescription Key	User	Patient Data Encryption Key – E Prescription Key – W, E	"Decrypting patient data"

The operator can verify the module firmware version on the Tablo Status Screen:

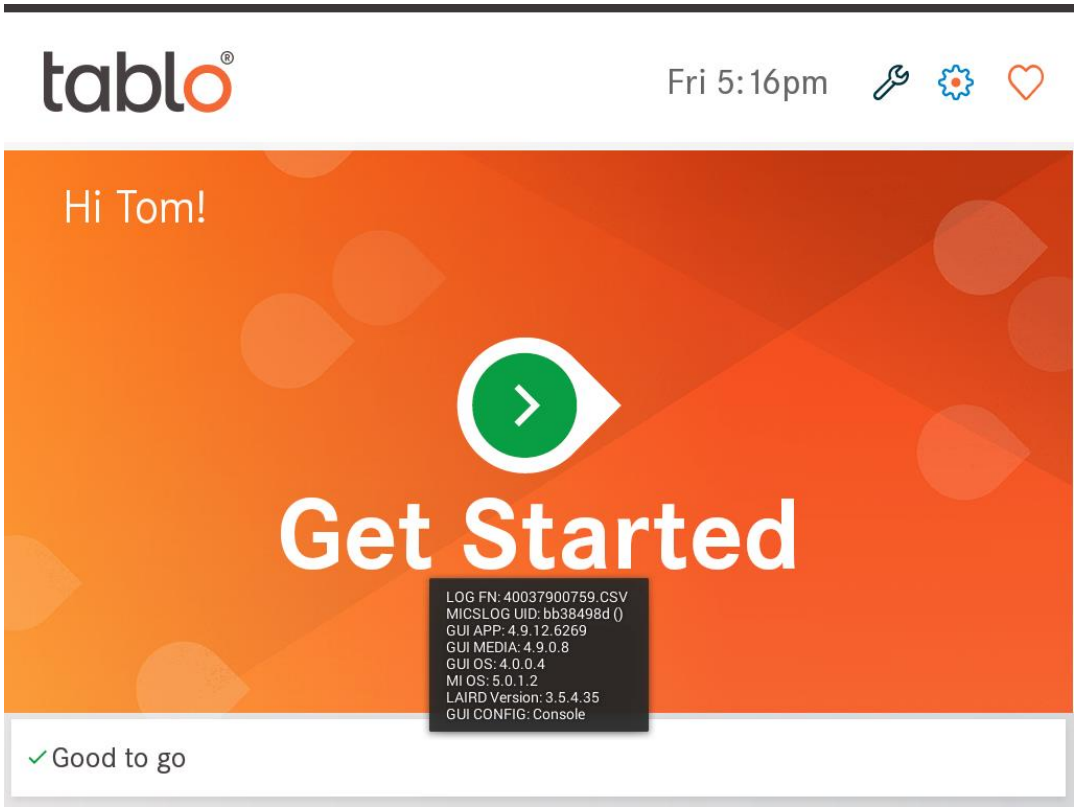

Figure 4 – Status/Show Version Screen

4.3 Authentication

The module does not support authentication mechanisms; roles are implicitly selected based on the service invoked. Refer to Table 10 above for a listing of the services associated with each authorized role.

5. Software/Firmware Security

All firmware components within the cryptographic boundary are verified using an integrity technique implemented within the cryptographic module itself. The module implements a CRC-32 integrity test of the module firmware. Failure of the integrity check for the module will cause the module to enter a critical error state.

Tablo Medical Informatics System is not delivered to end-users as a standalone offering and is only used in conjunction with the Outset Tablo. The CO can initiate the pre-operational tests on demand by power-cycling the Outset Tablo. The module does not support firmware upgrade. In order to provision the module, the CO must first invoke the “Import Provision File” service and obtain the specified indicator that the service was executed successfully (note this step is not required to operate the module in Approved mode).

6. Operational Environment

The operational environment of the module does not provide access to a general-purpose operating system (OS). The module employs a non-modifiable operational environment. The operating system offers no mechanism whereby the operator can modify software/firmware components, nor can the operator load and execute software or firmware that was not included as part of the validation of the module. The module's operating system is Linux 4.1.15 LTS[23].

[23] LTS – Long Term Support

7. Physical Security

As a multi-chip embedded module, the module is composed of production-grade components necessary to meet FIPS 140-3 level 1 physical security requirements. All components of the hardware are coated with commercial standard passivation.

8. Non-Invasive Security

There are currently no approved non-invasive mitigation techniques referenced in *ISO/IEC 19790:2021* Annex F.

9. Sensitive Security Parameter Management

The module supports the keys and other SSPs listed in **Table 11 – SSPs** below.

Table 11 – SSPs

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use & Related Keys
Keys								
Master Key	256 bits	AES (CBC) (Cert. A2701)	No	No / No	Preloaded	Plaintext in non-volatile memory	"Perform Zeroization" service	Secure the module's main keystore
Patient Data Encryption Key	256 bits	AES (CBC) (Cert. A2701)	No	No / No	Preloaded	Encrypted by the Master Key in non-volatile memory	No	Encrypting and decrypting Patient Data
Provisioning File Decryption Key	256 bits	AES (Cert. A2701)	No	No / No	Preloaded	Encrypted by the Master Key in non-volatile memory	No	Decryption of Provision File
License File Decryption Key	256 bits	AES (Cert. A2701)	No	No / No	Preloaded	Encrypted by the Master Key in non-volatile memory	No	Decryption of License File
Configuration File Decryption Key	256 bits	AES (Cert. A2701)	No	No / No	Preloaded	Encrypted by the Master Key in non-volatile memory	No	Decryption of Configuration File
Prescription Key	256 bits	AES (Cert. A2701)	No	Import: Electronically via USB Export: No	No	Encrypted in non-volatile memory	No	Encryption and decryption of Patient Prescription Data
Treatment In-Progress Data Key	256 bits	AES (Cert. A2701)	Internally generated via DRBG	No / No	No	Encrypted in non-volatile memory	No	Encryption of Treatment Data. Used to encrypt data internally on the MIES.
Treatment Data Public Key	2048-bit	RSA (Cert. A2701)	No	No / No	Preloaded	Encrypted in non-volatile memory	No	Encryption of Treatment Data
SSH Session Key	128/192/256-bit	AES (Cert. A2701)	No	No / No	Derived internally via SSH KDF	Plaintext in volatile memory	Reboot; remove power; session termination	Encryption and decryption of SSH session packet
SSH Authentication Key	160/256/512-bit	HMAC (Cert. A2701)	No	No / No	Derived internally via SSH KDF	Plaintext in volatile memory	Reboot; remove power; session termination	Authentication of SSH session packets
DH Private Key Component	2048/224, 2048/256	KAS-SSC-FFC (Cert. A2699)	Generated internally via approved DRBG	No / No	No	Plaintext in volatile memory	Reboot; remove power; session termination	Generation of SSH and TLS shared secrets
DH Public Key Component	2048/224, 2048/256	KAS-SSC-FFC (Cert. A2699)	Generated internally via approved DRBG	No / Yes	No	Plaintext in volatile memory	Reboot; remove power; session termination	Generation of SSH and TLS shared secrets
ECDH Private Key Component	All approved P/B/K curves	KAS-SSC-ECC (Certs. A2699 and A2701)	Generated internally via approved DRBG	No / No	No	Plaintext in volatile memory	Reboot; remove power; session termination	Generation of SSH and TLS shared secrets

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use & Related Keys
ECDH Public Key Component	All approved P/B/K curves	KAS-SSC-ECC (Certs. A2699 and A2701)	Generated internally via approved DRBG	No / Yes	No	Plaintext in volatile memory	Reboot; remove power; session termination	Generation of SSH and TLS shared secrets
TLS Session Key	AES AES-GCM	AES (Certs. A2699 and A2701) AES-GCM (Cert. A2701)	No	No / No	Derived internally using the TLS Master Secret	Plaintext in volatile memory	Reboot; remove power; session termination	Encryption and decryption of TLS session packets; AES GCM IV is used with the TLS Session key.
TLS Authentication Key		HMAC (Certs. A2699 and A2701)	No	No / No	Derived internally using the TLS Master Secret	Plaintext in volatile memory	Reboot; remove power; session termination	Authentication of TLS session packets
Other SSPs								
SSH Password	-	SSH KDF (Cert.)	No	No / No	Preloaded	Encrypted in non-volatile memory	No	Password used to authenticate MIES to Wi-Fi module
SSH Shared Secret	-		No	No / No	Computed via DH/ECDH shared secret computation	Plaintext in volatile memory	Reboot; remove power; session termination	Derivation of the SSH Session and authentication Keys; AES GCM IV is used with the SSH Session key.
TLS Premaster Secret	-	TLS 1.2 KDF (Cert. A2702)	No	No / No	Computed via DH/ECDH shared secret computation	Plaintext in volatile memory	Reboot; remove power; session termination	Derivation of the TLS master secret
TLS Master Secret	-	-	No	No / No	Derived internally using the TLS Premaster Secret via TLS KDF	Plaintext in volatile memory	Reboot; remove power; session termination	Derivation of the TLS session (AES) and authentication (HMAC) keys, and the GCM IV.
AES GCM IV	-	AES GCM (Certs. A2699 and A2701)	No	No / No	Derived internally using the TLS Master Secret[24] or generated for SSH in compliance with RFC 5647[25].	Plaintext in volatile memory	Reboot; remove power; session termination	Initialization vector for AES GCM
DRBG entropy input	-	DRBG (Certs. A2699 and A2701)	N/A	No / No	Produced internally via Approved entropy source	Plaintext in RAM	Upon module reboot Upon session termination	Establishment of seed for CTR_DRBG
DRBG seed	-	DRBG (Certs. A2699 and A2701)	N/A	No / No	Established internally using entropy input string via DRBG	Plaintext in RAM	Upon module reboot Upon session termination	Generation of random number
DRBG 'V' value	-	DRBG (Certs. A2699 and A2701)	Generated internally within DRBG	No / No	N/A	Plaintext in RAM	Upon module reboot Upon session termination	State value for CTR_DRBG

[24] The IV generation method complies with technique #1 (for TLS 1.2 GCM Cipher Suites) in FIPS 140-3 IG C.H. *RFC 5246* defines the TLS 1.2 protocol; *RFC 5288* defines the use of the AES-GCM encryption with the TLS protocol. Each IV is generated and used only within each protocol's implementation.
[25] The IV generation method complies with technique #1 (for SSHv2 protocol) in FIPS 140-3 IG C.H. Each IV is generated and used only within each protocol's implementation.

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use & Related Keys
DRBG 'Key' value	-	DRBG (Certs. A2699 and A2701)	Generated internally within DRBG	No / No	N/A	Plaintext in RAM	Upon module reboot Upon session termination	State value for CTR_DRBG

9.1 Algorithm Specific Information

9.1.1 AES-GCM

The AES-GCM IV is used in the following protocols:

- TLS – The AES-GCM IV is used in the TLS protocol. The TLS AES-GCM IV is generated in compliance with TLS v1.2 GCM cipher suites as specified in RFC[26] 5288 and section 3.3.1 of NIST SP 800-52rev1. Per RFC 5246, when the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key, the module will trigger a handshake to establish a new encryption key. The AES-GCM IV is a random 96-bit value generated with available entropy provided by the available entropy source.

- SSH – The module's SSHv2 implementation is compliant with RFCs 4252, 4253 and 5647. The AES GCM IV generation is in compliance with RFC 5647 and is only used for the SSHv2. When an SSH session gets terminated for any reason, all keying material will be re-negotiated by the module.

9.1.2 KAS

The module performs all applicable key assurances for its DH and ECDH implementations as specified in section 9 of *NIST SP 800-56Arev3*. These tests are performed as conditional tests.

9.2 SSP Zeroization

In order to zeroize all keys and CSPs present within the module, the operator shall decommission the module by performing the following steps:

1. Upload patient log files to the cloud and clear from MI board
2. Erase volatile storage in MIES unit
3. Clear log files from black box USB

For further detailed information on each step please refer to the "Tablo X Hemodialysis System De-Installation Procedure", steps 4, 5, and 6.

For the zeroization of keys in volatile memory, module operators can power-cycle the Tablo machine.

9.3 RBG Entropy Sources

Table 12 below specifies the module's entropy sources.

[26] RFC – Request For Comment

Table 12 – Non-Deterministic Random Number Generation Specification

Entropy Source	Minimum number of bits of entropy	Details
CPU Time Jitter Based Non-Physical TRNG version 3.3	256	The module requests 256 bits of entropy per call and receives 256 number of bits of entropy. Seed material is provided to the module's DRBG by the CPU jitter mechanism residing within the module's cryptographic boundary.

10. Self-Tests

Both pre-operational and conditional self-tests are performed by the module. Pre-operational tests are performed between the time a cryptographic module is powered on or instantiated (after being powered off, reset, rebooted, cold-start, power interruption, etc.) and before the module transitions to the operational state. Conditional self-tests are performed by the module during module operation when certain conditions exist. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

10.1 Pre-Operational Self-Tests

The module performs the following pre-operational self-test(s):

- Firmware integrity test (using CRC-32)

10.2 Conditional Self-Tests

The module performs the following conditional cryptographic algorithm self-tests (CASTs):

- Tablo Medical Informatics System CPU Jitter Library:
  - SHA-3 Known Answer Test
  - Stuck test on entropy source
  - Repetition Count Test on entropy source
  - Adaptive Proportion Test on entropy source

- Tablo Medical Informatics System OpenSSL Cryptographic Library:
  - AES ECB encrypt and decrypt KATs[27] (128-bit)
  - AES CCM encrypt and decrypt KATs (192-bit)
  - AES GCM encrypt and decrypt KATs (128-bit)
  - CTR_DRBG KAT (256-bit AES-CTR with derivation function)
  - CTR_DRBG Health Tests (Instantiate, Generate, Reseed)
  - DSA Digital Signature Verification KAT (2048-bit; SHA2-256)
  - ECDSA Digital Signature Verification KAT (P-224 and K-233 curve, SHA2-256)
  - HMAC KATs (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)
  - RSA Digital Signature Verification KAT (2048-bit; SHA2-256; PKCS#1.5 scheme)
  - SHA KATs (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)
  - ECC CDH Shared Secret “Z” Computation KAT (P-224 curve)

- Tablo Medical Informatics System Bouncy Castle Cryptographic Library:
  - AES ECB encrypt and decrypt KATs (128-bit)
  - AES CCM encrypt and decrypt KATs (128-bit)
  - AES GCM encrypt and decrypt KATs (128-bit)
  - CTR_DRBG KAT
  - CTR_DRBG Health Tests (Instantiate, Generate, Reseed)
  - DSA Digital Signature Verification KAT (2048-bit)

[27] KAT – Known Answer Test

- ECDSA Digital Signature Verification KAT (P-256)
- HMAC KATs (SHA2-256, SHA2-512)
- RSA Digital Signature Verification KAT (2048-bit)
- SHA KATs (SHA-1, SHA2-256, SHA2-512)
- FFC Shared Secret "Z" Computation KAT (Parameter Sets/Key sizes: FB)
- ECC CDH Shared Secret "Z" Computation KAT (P-256)

The module performs the following conditional pair-wise consistency tests (PCTs):

- Tablo Medical Informatics System OpenSSL Cryptographic Library:
  - ECDH key generation PCT

- Tablo Medical Informatics System Bouncy Castle Cryptographic Library):
  - DH key generation PCT
  - ECDH key generation PCT

10.3 On-Demand Self-Tests

The CO can initiate the pre-operational self-test (as well as the conditional CASTS) on demand for periodic testing of the module by power-cycling the Tablo machine. The LED will blink 2 times to indicate that self-tests are running.

10.4 Self-Test Failure Handling

Upon failure of any self-test, the module will set an internal flag and enter a critical error state. In this state, the module will no longer perform cryptographic services or output data over the data output interfaces. For any subsequent request for cryptographic services, the module will return a failure indicator.

To recover, the module must be reinitialized by power-cycle of the Tablo machine. If the pre-operational self-tests complete successfully, then the module can resume normal operations. If the module continues to experience self-test failures after reinitializing, then the module will not be able to resume normal operations, and the CO should contact Outset Medical, Inc. for assistance.

11. Life-Cycle Assurance

The sections below describe how to ensure the module is operating in its validated configuration. **Module operators shall follow all guidance provided guidance in this section to ensure the module is operating in a compliant manner. Operating the module without following this guidance (including the use of undocumented services) will result in non-compliant behavior and is outside the scope of this Security Policy**.

11.1 Secure Installation

The Medical Informatics System is delivered to the end user contained within the larger Outset Tablo machine, and there are no further installation procedures required by the operator.

11.2 Initialization

No initialization steps are required to be performed by end-users.

11.3 Startup

No setup steps are required to be performed by end-users.

11.4 Administrator Guidance

There are no specific management activities required of the CO role to ensure that the module runs securely. However, if any irregular activity is noticed or the module is consistently reporting errors, then Outset Customer Support should be contacted.

Module operators can view the module's operational status via the Tablo machine GUI.

11.5 Non-Administrator Guidance

The following list provides guidance for the User role:

- In case the module's power is lost and then restored, the key used for the AES GCM encryption or decryption shall be re-established.

11.6 Common Vulnerabilities and Exposures

There are no known CVEs associated with the cryptographic module.

12. Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-3 Level 1 requirements for this validation.

13. Acronyms and Abbreviations

Table 13 provides definitions for the acronyms and abbreviations used in this document.

Table 13 – Acronyms

Term	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CAST	Cryptographic Algorithm Self-Test
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CCM	Counter with Cipher Block Chaining - Message Authentication Code
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CMAC	Cipher-Based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DEP	Default Entry Point
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMI/EMC	Electromagnetic Interference /Electromagnetic Compatibility
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode

Term	Definition
GMAC	Galois Message Authentication Code
GPC	General-Purpose Computer
HMAC	(keyed-) Hash Message Authentication Code
KAS	Key Agreement Scheme
KAT	Known Answer Test
KTS	Key Transport Scheme
KW	Key Wrap
KWP	Key Wrap with Padding
MD	Message Digest
NIST	National Institute of Standards and Technology
OCB	Offset Codebook
OFB	Output Feedback
OS	Operating System
PBKDF	Password-Based Key Derivation Function
PCT	Pairwise Consistency Test
PKCS	Public Key Cryptography Standard
PSS	Probabilistic Signature Scheme
PUB	Publication
RC	Rivest Cipher
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
SHAKE	Secure Hash Algorithm KECCAK
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SP	Special Publication
TLS	Transport Layer Security
XEX	XOR Encrypt XOR
XTS	XEX-Based Tweaked-Codebook Mode with Ciphertext Stealing

Prepared by:
Corsec Security, Inc.

2600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com