TrellisWare Technologies, Inc.

TW-860-F TSM Spirit

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 9
2.3 Excluded Components 9
2.4 Modes of Operation 9
2.5 Algorithms 10
2.6 Security Function Implementations 12
2.7 Algorithm Specific Information 15
2.8 RBG and Entropy 15
2.9 Key Generation 15
2.10 Key Establishment 15
2.11 Industry Protocols 15
2.12 Additional Information 15
3 Cryptographic Module Interfaces 16
3.1 Ports and Interfaces 16
4 Roles, Services, and Authentication 17
4.1 Authentication Methods 17
4.2 Roles 18
4.3 Approved Services 18
4.4 Non-Approved Services 23
4.5 External Software/Firmware Loaded 23
4.8 Additional Information 24
5 Software/Firmware Security 25
5.1 Integrity Techniques 25
5.2 Initiate on Demand 25
6 Operational Environment 25
6.1 Operational Environment Type and Requirements 25
6.2 Configuration Settings and Restrictions 25
7 Physical Security 26
7.1 Mechanisms and Actions Required 26
7.2 User Placed Tamper Seals 26
8 Non-Invasive Security 28

8.1 Mitigation Techniques....28
9 Sensitive Security Parameters Management....28
9.1 Storage Areas....28
9.2 SSP Input-Output Methods....28
9.3 SSP Zeroization Methods....30
9.4 SSPs....30
10 Self-Tests....34
10.1 Pre-Operational Self-Tests....34
10.2 Conditional Self-Tests....34
10.3 Periodic Self-Test Information....34
10.4 Error States....35
10.5 Operator Initiation of Self-Tests....35
10.6 Additional Information....35
11 Life-Cycle Assurance....36
11.1 Installation, Initialization, and Startup Procedures....36
11.2 Administrator Guidance....37
11.3 Non-Administrator Guidance....37
12 Mitigation of Other Attacks....37

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Hardware 9
Table 3: Modes List and Description 10
Table 4: Approved Algorithms 10
Table 5: Non-Approved, Allowed Algorithms with No Security Claimed 12
Table 6: Security Function Implementations 14
Table 7: Ports and Interfaces 16
Table 8: Authentication Methods 17
Table 9: Roles 18
Table 10: Approved Services 23
Table 11: Mechanisms and Actions Required 26
Table 12: Required Locations and Number for Tamper Evidence per Module Type 26
Table 13: Storage Areas 28
Table 14: SSP Input-Output Methods 29
Table 15: SSP Zeroization Methods 30
Table 16: SSP Table 1 32
Table 17: SSP Table 2 33
Table 18: Pre-Operational Self-Tests 34
Table 19: Conditional Self-Tests 34
Table 20: Pre-Operational Periodic Information 34
Table 21: Conditional Periodic Information 35
Table 22: Error States 35

List of Figures

Figure 0-1: TW-860-F TSM Spirit Module 7
Figure 0-2: TW-860-F TSM Spirit Module Block Diagram 8

1 General

1.1 Overview

The TrellisWare Technologies, Inc Cryptographic module(s) covered by this Security Policy document are shown in the table below.

Product Ordering Number	Catalog Description	FW Version	Non-Security Features	Primary Use-Case	Env Rating
TW-860-F	TSM Spirit Radio	6.2.1-b74	Display, buttons	Body-worn	IP68

The module(s) are multi-chip standalone cryptographic module(s) designed to convert Plaintext Data to/from Ciphertext data using AES256-CTR mode. The module(s) also authenticate Crypto Officer access using a RSA2048/SHA256 Certificate.

The module(s) support distinct operator roles: Crypto Officer (CO) and User. Additionally, the module supports an unauthenticated Human Operator role. These are discussed further below.

1.2 Security Levels

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	2
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module(s) covered by this Security Policy act as nodes (‘radios’) on a Wireless network with a minimum of two (2) nodes or up to hundreds of nodes. Each node can produce data on the Wireless network and act as a relay, re-broadcasting data from nearby nodes.

The Wireless network implements TrellisWare's TSM waveform. The TSM waveform enables a self-forming, self-healing, infrastructure-less Mobile Ad-hoc Network (MANET) that provides wireless coverage in challenging environments or during critical situations.

The TSM mobile ad-hoc network is not dependent on a fixed infrastructure. No towers are required. No central control points, programmed routes or tables, access points, or directional antennas.

All data on the Wireless network is Ciphertext created with the approved Algorithm listed in this Security Policy. One or more Wired Plaintext data interfaces are provided on the module(s) to input or output the data passing through the Wireless Ciphertext network.

The flow of Plaintext to/from Ciphertext data is defined as the ‘User mode’. Only Plaintext data is present on the Wired interface(s). Only Ciphertext data is present on the Wireless interface.

Local Plaintext data is also created on each module and passed to/from the Wireless network as Ciphertext using the approved Algorithm. Local data includes Position-Location-Information (PLI), Voice, Video and Status.

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

For the module(s) covered by this Security Policy, the physical cryptographic boundary is defined as the module case.

The physical cryptographic boundary does not require any caps or covers on connectors.

Module Images:

- **Figure 0-1** below shows the physical cryptographic boundary of the TW-860-F TSM Spirit.

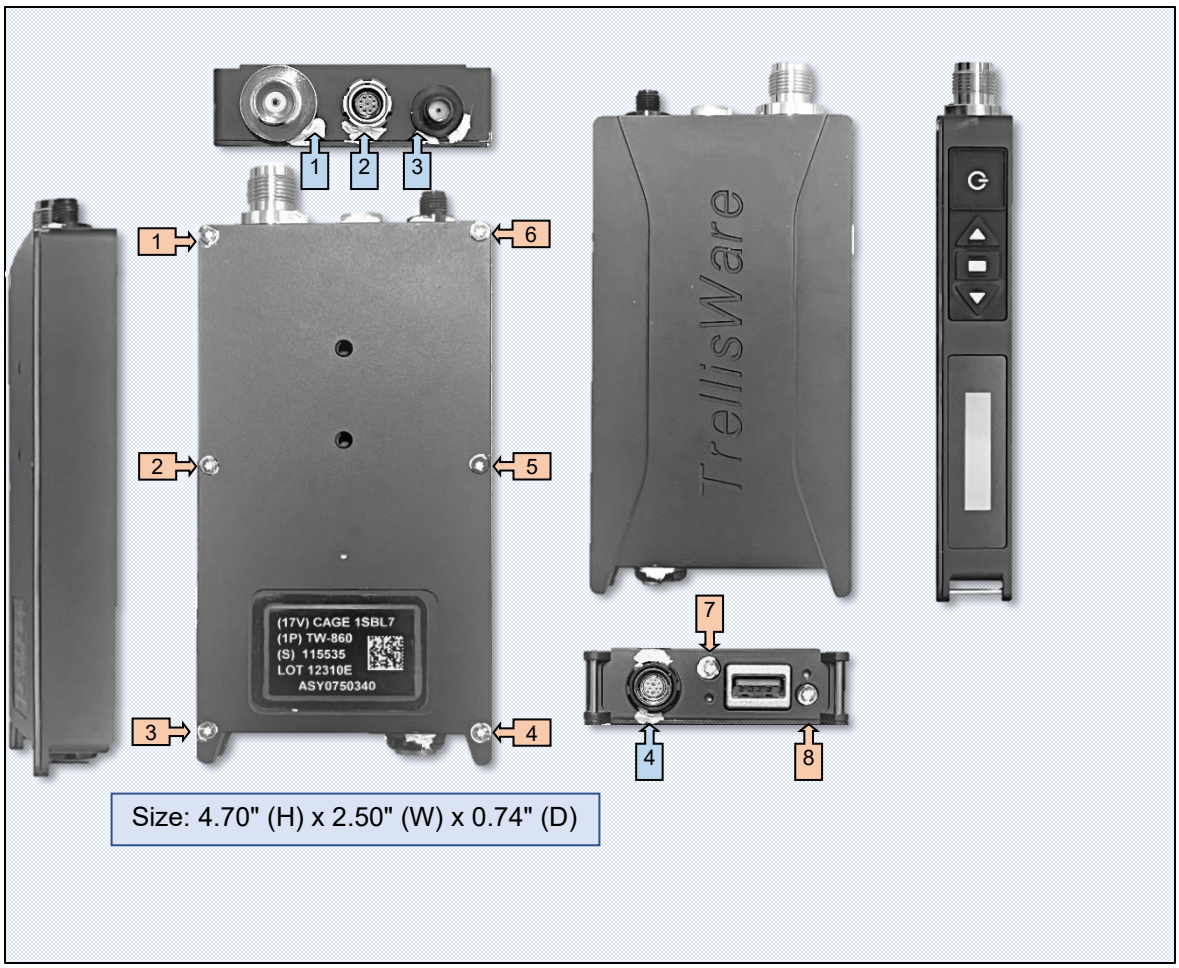


Figure 0-1: TW-860-F TSM Spirit Module

The cryptographic boundary is further identified in the following **block diagram**.

Figure 0-2 below shows a simplified block diagram depicting major hardware components of the TW-860-F TSM cryptographic module, component interconnections, Plaintext data paths, Ciphertext data paths, Non-security Human Operator features and Crypto Officer control paths.

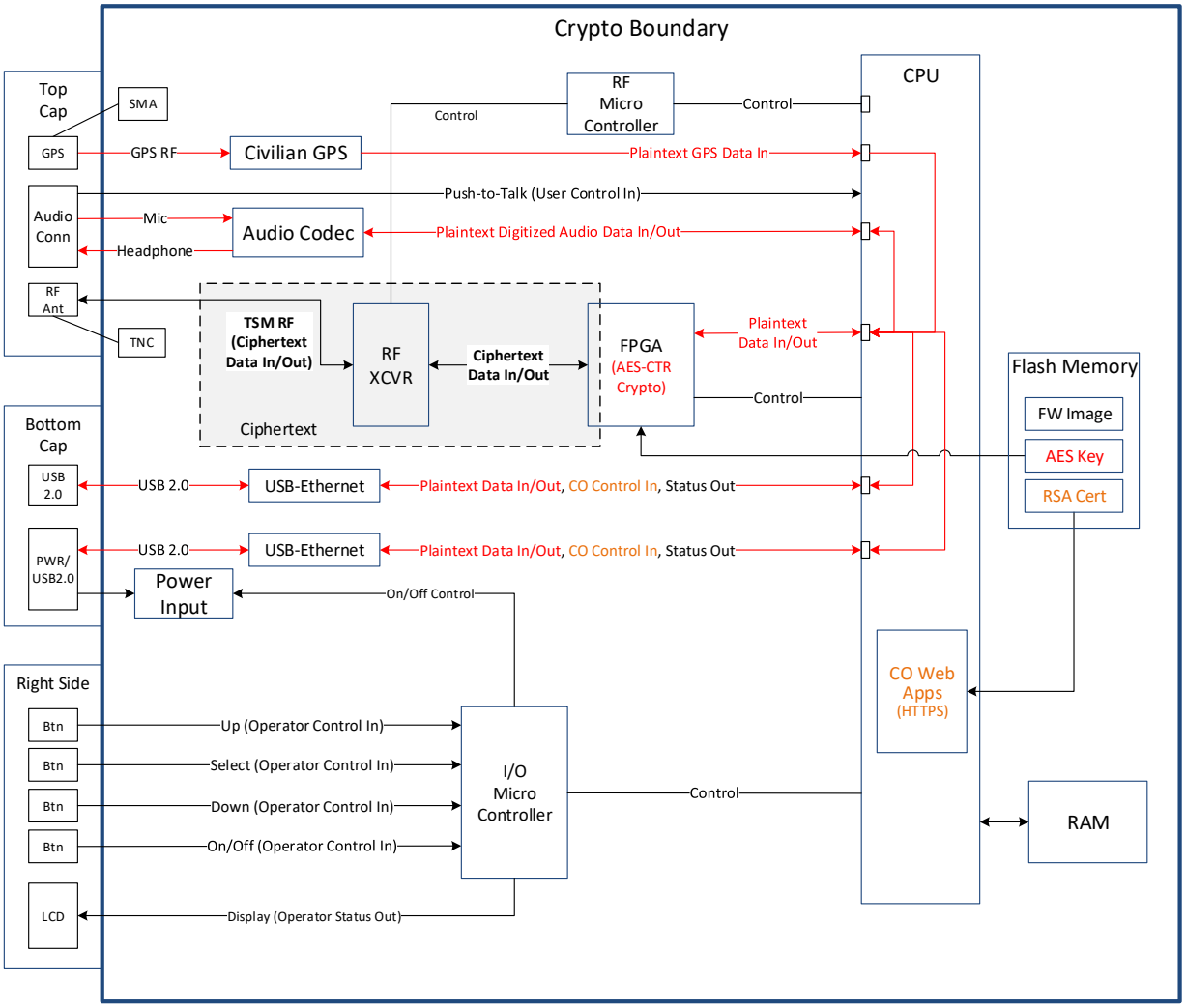


Figure 0-2: TW-860-F TSM Spirit Module Block Diagram

Tested Operational Environment's Physical Perimeter (TOEPP):

For the module(s) covered by this Security Policy, the TOEPP is equal to the module case because the physical cryptographic boundary is defined as the module case.

The Red and Blue arrows in Figure 0-1 show the locations of the Tamper Evidence and are discussed in more detail in Section 7.2 below.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
TW-860-F	ASY0750340 G	6.2.1-b74	Mentor Graphics ModelSim PE 10.6c ARM Cortex A9	USB PD power, keypad, LCD, no LED, Civilian GPS, USB, Audio port, 2W RF output, IP68

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

There are two (2) additional microcontrollers within the Cryptographic Boundary which have no security functions.

- The I/O Micro Controller is used to service the Human Operator controls on the module case.
- The RF Micro Controller is used to control the RF Transceiver settings (e.g. Frequency, Bandwidth, Power Control, Tx/Rx switching).

These controllers have no access to Plaintext, Ciphertext and CSP storage or data paths and thus cannot compromise the module's security.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved	Initiated by following instructions in section 11.1 of the Security	Approved	Global / implicit indicator (i.e., successful completion of the

Mode Name	Description	Type	Status Indicator
	Policy		approved service).

Table 3: Modes List and Description

Mode Change Instructions and Status:

After initialization into the Approved mode, it is expected that the module(s) described in this Security Policy document will remain in the Approved mode for the remainder of the product life cycle. The instructions for initialization into the Approved mode are provided in section 11.1 below. The mode status indicators are shown in the table above. The CSP status services are accessible by the CO using TrellisWare provided tools.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	C1431	Direction - Encrypt Key Length - 256	SP 800-38A
RSA SigGen (FIPS186-5)	A5395	Hash Pair - Hash Algorithm - SHA2-256 Modulo - 2048 Signature Type - pkcs1v1.5	FIPS 186-5
RSA SigVer (FIPS186-5)	A5395	Hash Pair - Hash Algorithm - SHA2-256 Modulo - 2048 Signature Type - pkcs1v1.5 Public Exponent Mode - random	FIPS 186-5
SHA2-256	A5395	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms:

N/A for this module.

There are no functions within the scope of the module that rely on a non-approved cryptographic algorithm to support a claim of security.

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
AES	No security claimed	Used internally and separate from AES Cert # C1431. As per FIPS 140-3 IG 2.4.A, this is used to "obfuscate" data using proprietary implementations. All obfuscated data is treated as plaintext.
SRP	No security claimed	As per FIPS 140-3 IG 2.4.A, this is used between applications/web browser and the module; however, the module's purpose is to provide end-to-end secure communications over an insecure communications channel. Module does not rely on the security of this algorithm for this purpose.
DH	No security claimed	As per FIPS 140-3 IG 2.4.A, this is used between applications/web browser and the module; however, the module's purpose is to provide end-to-end secure communications over an insecure communications channel. Module does not rely on the security of this algorithm for this purpose.
ECDH	No security claimed	As per FIPS 140-3 IG 2.4.A, this is used between applications/web browser and the module; however, the module's purpose is to provide end-to-end secure communications over an insecure communications channel. Module does not rely on the security of this algorithm for this purpose.
DSA	No security claimed	As per FIPS 140-3 IG 2.4.A, this is used between applications/web browser and the module; however, the module's purpose is to provide end-to-end secure communications over an insecure communications channel. Module does not rely on the security of this algorithm for this purpose.
ECDSA	No security claimed	As per FIPS 140-3 IG 2.4.A, this is used between applications/web browser and the module; however, the module's purpose is to provide end-to-end secure communications over an insecure communications channel. Module does not rely on the security of this algorithm for this purpose.
Triple-DES	No security claimed	As per FIPS 140-3 IG 2.4.A, this is used between applications/web browser and the module; however, the module's purpose is to provide end-to-end secure communications over an insecure communications channel. Module does not rely on the security of this algorithm for this purpose.
Camellia	No security claimed	As per FIPS 140-3 IG 2.4.A, this is used between applications/web browser and the module; however, the module's purpose is to provide end-to-end secure communications over an insecure communications channel. Module does not rely on the security of this algorithm for this purpose.
SEED	No security claimed	As per FIPS 140-3 IG 2.4.A, this is used between applications/web browser and the module; however, the module's purpose is to provide end-to-end secure communications over an insecure communications channel. Module does not rely on the security of this algorithm for this purpose.
RC4	No security claimed	As per FIPS 140-3 IG 2.4.A, this is used between applications/web browser and the module; however, the module's purpose is to provide end-to-end secure communications over an insecure communications channel. Module does not rely on the security of this algorithm for this

Name	Caveat	Use and Function
		purpose.
MD5	No security claimed	As per FIPS 140-3 IG 2.4.A, this is used between applications/web browser and the module; however, the module's purpose is to provide end-to-end secure communications over an insecure communications channel. Module does not rely on the security of this algorithm for this purpose.
IDEA	No security claimed	As per FIPS 140-3 IG 2.4.A, this is used between applications/web browser and the module; however, the module's purpose is to provide end-to-end secure communications over an insecure communications channel. Module does not rely on the security of this algorithm for this purpose.
SHA-1	No security claimed	As per FIPS 140-3 IG 2.4.A, this is used between applications/web browser and the module; however, the module's purpose is to provide end-to-end secure communications over an insecure communications channel. Module does not rely on the security of this algorithm for this purpose.
SHA2-384	No security claimed	As per FIPS 140-3 IG 2.4.A, this is used between applications/web browser and the module; however, the module's purpose is to provide end-to-end secure communications over an insecure communications channel. Module does not rely on the security of this algorithm for this purpose.
KDF	No security claimed	As per FIPS 140-3 IG 2.4.A, this is used between applications/web browser and the module; however, the module's purpose is to provide end-to-end secure communications over an insecure communications channel. Module does not rely on the security of this algorithm for this purpose.

Table 5: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

N/A for this module.

None

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Packet Creation and Forwarding	BC-UnAuth	Packet Creation and Forwarding	Keys:AES 256 bits keys with 256 of key strength	AES-CTR: (C1431) Algorithm Capabilities: AES-CTR
Firmware load test	DigSig-SigVer	Firmware load test	Keys:2048 bits with 112 bits of key strength	RSA SigVer (FIPS186-5): (A5395) Algorithm Capabilities:

Name	Type	Description	Properties	Algorithms
				RSA SigGen (FIPS186-5) SHA2-256: (A5395)
Authentication of CO	DigSig-SigVer	Authentication of CO	Keys:2048 bits with 112 bits of key strength	RSA SigVer (FIPS186-5): (A5395) Algorithm Capabilities: RSA SigVer (FIPS186-5) SHA2-256: (A5395)
FW Integrity Test	SHA	Verification of firmware integrity		SHA2-256: (A5395)
KTS - Key Wrapping/Unwrapping with AES-CTR and RSA	KTS-Unwrap KTS-Wrap	Key wrapping, key unwrapping using AES-CTR and RSA	Standard:SP 800-38F IG D.G:approved "combination" method from IG D.G and SP 800-38F Caveat:Key establishment methodology provides 256 bits of security strength	AES-CTR: (C1431) Algorithm Capabilities: AES-CTR RSA SigGen (FIPS186-5): (A5395) Algorithm Capabilities: RSA SigGen (FIPS186-5) RSA SigVer (FIPS186-5): (A5395) Algorithm Capabilities: RSA SigVer (FIPS186-5) SHA2-256: (A5395)
Local HTTPS	UNK	HTTPS Key Loader SSP input/output		AES: () Algorithm Capabilities: AES SRP: () Algorithm Capabilities: SRP DH: () Algorithm Capabilities: DH ECDH: ()

Name	Type	Description	Properties	Algorithms
				Algorithm Capabilities: ECDH DSA: () Algorithm Capabilities: DSA ECDSA: () Algorithm Capabilities: ECDSA Triple-DES: () Algorithm Capabilities: Triple-DES Camellia: () Algorithm Capabilities: Camellia SEED: () Algorithm Capabilities: SEED RC4: () Algorithm Capabilities: RC4 MD5: () Algorithm Capabilities: MD5 IDEA: () Algorithm Capabilities: IDEA SHA-1: () Algorithm Capabilities: SHA-1 SHA2-384: () Algorithm Capabilities: SHA2-384 KDF: () Algorithm Capabilities: KDF

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

Not applicable.

2.8 RBG and Entropy

N/A for this module.

N/A for this module.

There are no entropy sources or RNGs in the module(s) covered by this Security Policy document.

2.9 Key Generation

The module(s) do not generate Keys. To generate Network Keys and CO Certificates for the module(s), a supplied Windows PC Application must be used: TrellisWare Management Tool. This tool is outside the boundary and out-of-scope of this validation. The required tool is issued to the Crypto Officer(s) only by TrellisWare Technologies, Inc.

The tool will install and run on any Windows 7, 10 or 11 PC.

2.10 Key Establishment

The module(s) support key entry from the software tools that are outside of the module(s) physical and cryptographic boundary using a key loader. Key entry from the tools is via the Plaintext wired interfaces only.

After Keys are loaded on the module(s), network keys can be transferred over-the-air to other modules, using the Key Wrapping/Unwrapping with AES-CTR and RSA SFI. The network keys cannot be transferred to other modules via the Wired interfaces.

The transfer process is referred to as Over-the-Air Cloning (OTAC) in the module(s) User Guide. The transfer is initiated by a CO. One module is placed into OTAC transmit mode, and when one or more modules have been placed into OTAC receive mode, these modules will be updated over-the-air within a few seconds. To complete the process, the CO manually exits the OTAC mode on the transmit and receive modules.

2.11 Industry Protocols

The module(s) use HTTPS with TLS for the local connection. No protection of data is claimed for HTTPS with TLS.

2.12 Additional Information

The module(s) have been tested for RF Emissions and Electromagnetic Immunity per the requirements and procedures in MIL-STD 461F.

This document may be freely reproduced and distributed (without revision).

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
RF Antenna Connector	Data Input Data Output Control Input Status Output	All data is Ciphertext. User Mode data input/output. CO Mode authenticated control input/output. Non-security status output. Module identification output.
GPS Antenna Connector	Data Input	Civilian GPS, plaintext data.
USB 2.0 OTG	Data Input Data Output Control Input Status Output	All data is Plaintext. User Mode data input/output. CO mode authenticated control input/output. Non-security status output. Module identification output.
USB 2.0 Host	Data Input Data Output Control Input Status Output	All data is Plaintext. User Mode data input/output. CO mode authenticated control input/output. Non-security status output. Module identification output.
Audio Port	Data Input Data Output Control Input	Analog voice data input/output, Push-to-talk control input.
LCD	Status Output	Non-security status output only.
Pushbuttons	Control Input	Power on/off and non-security control input only.
Power Connector	Power	None.

Table 7: Ports and Interfaces

The interfaces for the cryptographic boundary include physical and logical interfaces. The physical interfaces provided by each module are mapped to FIPS 140-3 defined logical interfaces: Data Input (DI), Data Output (DO), Control Input (CI), Status Output (SO), and Power Interface (PI).

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
CO Public Key Certificate	The RSA certificate contains a 2048-bit key signed with a SHA-256 hash function. An RSA 2048-bit key provides an equivalent security strength of 112-bits.	RSA SigVer (FIPS186-5) (A5395)	The probability that a random attempt will succeed is 1/2^112, which is orders of magnitude less than the required 1/1,000,000 (ca. 1/2^20).	Each HTTPS attempt was observed to be 5,024 bytes (40,192 bits). At the module's maximum rate of 100 mbps, the maximum number of HTTPS attempts per second is 100e6/40192 bits, or 2,488 per second, ignoring packet overhead, equivalent to 149,280 (2,488x60) attempts per minute. Rounding up to the nearest power of 2, assume 2^18 attempts per minute is possible via a script or automated attack. The probability of a success with multiple attempts is 2^18/2^112 = 1/2^94, which is ca. 5.5 times better than the required 1/100,000 (ca. 1/2^17).
Network Key	AES-256 key provides an equivalent security strength of 256-bits.	AES-CTR (C1431)	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^256, which is orders of magnitude less than the required 1/1,000,000 (ca. 1/2^20).	AES-256 output blocks are 128-bits in length. The Ciphertext output port is capable of 16Mbps maximum, or 16M/128 = 125K blocks/sec that an attacker could analyze. Rounding up to a power of 2, results in 2^17 blocks per second. Thus, the probability of a success is 2^17/2^256=1/2^239, which is ca. 14 times better than the required 1/100,000 (ca. 1/2^17).
None	Access to non-security relevant functionalities	None	NA	NA

Table 8: Authentication Methods

The strength of each implemented authentication mechanism is described above.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer (CO)	Role	This role accesses the module via authenticated API services for initialization and configuration of the module. This role also has access to all other services offered by the module.	CO Public Key Certificate
User	Role	This role allows the module to perform Cryptographic data encryption/ decryption using Approved algorithms.	Network Key
Human Operator (HO, Non-security)	Role	An unauthenticated operator can control switches, dials, and other unauthenticated services of the module.	None

Table 9: Roles

The module supports distinct operator roles: Crypto Officer (CO) and User. Additionally, the module supports an unauthenticated Human Operator (HO) role.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Crypto Officer Authentication	Uses the CO Public Key Certificate to allow the CO to access the unit for	Management app receives a result	CO Public Key Certificate	Status of CO authentication	Authentication of CO	Crypto Officer (CO) - CO Public Key Certificate: R,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Security and Non-security configuration.					- TWT CA Public Key Certificate: R,E
Non-Security Configuration	Configure non-security settings and Wideband RF settings.	Management app receives a result	CO Public Key Certificate Non-security settings and Wideband RF settings	Status of CO authentication Status of Non-Security Configuration	Authentication of CO	Crypto Officer (CO) - CO Public Key Certificate: R,E - TWT CA Public Key Certificate: R,E
Security Configuration	Enter and select the FIPS-140 SSP's - CO Public Key Certificate and AES-256 CTR Network Key via manual distribution electronic entry. Prior to a certificate update, the module is automatically zeroized.	Management app receives a result	CO Public Key Certificate FIPS-140 SSP's - CO Public Key Certificate and AES-256 CTR Network Key	Status of Local HTTPS Key Loader Input/Output Status of Security Configuration	Local HTTPS	Crypto Officer (CO) - Network Key: R,W - CO Public Key Certificate: R,W,E - TWT CA Public Key Certificate: R
Packet Forwarding	Provides packet transfer between the RF Ciphertext	Management App shows # of nodes and network utilization	Network packets to be forwarded	Processed network packets to be forwarded	Packet Creation and Forwarding	User - Network Key: R,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	port and Plaintext Ethernet ports. Packets are encrypted and decrypted using the AES-256 Network Key.					
Packet Creation	Provides Ciphertext packet creation from internal Plaintext sources (GPS, Audio, Video). Packets are encrypted using the AES-256 Network Key. Encrypted packets are transmitted via RF.	Management app shows status and network utilization	Plaintext from internal sources	Encrypted network packets	Packet Creation and Forwarding	User - Network Key: R,E
Network Monitoring & Remote Control	Monitor network and individual radios. Remote control of radio non-security settings and stream control.	Management app shows status and network data	CO Public Key Certificate Radio non-security settings and stream control	Status of CO authentication Network monitoring data Status of radio non-security settings and stream configuratio	Packet Creation and Forwarding Authentication of CO	Crypto Officer (CO) - CO Public Key Certificate: R,E - TWT CA Public Key Certificat

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
				n		e: R,E
Firmware Upgrade	Upgrade firmware release. Note: If non-FIPS validated firmware is loaded, the module is no longer a FIPS validated module.	TSM Software Download PC app shows status	CO Public Key Certificate Firmware	Status of CO authentication Status of the upgrade	Firmware load test	Crypto Officer (CO) - CO Public Key Certificate: R,W,E - TWT CA Public Key Certificate: R,W,E - FW Load Public Key: R,E - CO Private Key: W
Power-on Module Self-Tests	Performs module's power-up self-tests. If failing, enters Error state.	Management app shows the status of the module	None	Status of the module's power-up self-tests	Packet Creation and Forwarding Authentication of CO FW Integrity Test KTS - Key Wrapping/Unwrapping with AES-CTR and RSA	Human Operator (HO, Non-security)
Module Status API	Provides CO Non-security Status API service for PC, Android and Web apps.	Management app shows status of the module	CO Public Key Certificate	Status of CO authentication Non-security status	Authentication of CO	Crypto Officer (CO) - CO Public Key Certificate: R,E - TWT CA Public Key Certificate: R,E
FIPS Zeroize (OTAC)	Remotely zeroize all CSPs in	Management apps do not see	CO Public Key	Status of CO authenticati	Authentication of CO Packet Creation	Crypto Officer (CO)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	the module. Once zeroized, the module must be reinitialized as described above.	the status of the module	Certificate Request to zeroize	on Status of zeroization	and Forwarding	- CO Public Key Certificate: R,E - TWT CA Public Key Certificate: R,E - Network Key: Z
Cloning of keys	Remotely clone Network Key	Management app receives a result	CO Public Key Certificate Request to clone	Status of cloning	KTS - Key Wrapping/Unwrapping with AES-CTR and RSA	Crypto Officer (CO) - CO Public Key Certificate: R,E - CO Private Key: R,E - Network Key: W
Manual Non-Security Configuration (devices with LCD only)	Selection of voice channel, volume and other non-security configuration parameters using the manual controls on the unit.	LCD	Keypad or buttons	LCD	None	Human Operator (HO, Non-security)
Show Status	Uses the CO Public Key Certificate to allow the CO to	Management app receives the status	CO Public Key Certificate	Status of CO authentication Status of the module	Authentication of CO	Crypto Officer (CO) - CO Public Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	access the unit to see the status					Certificate: R,E - TWT CA Public Key Certificate: R,E
Show Version	Uses the CO Public Key Certificate to allow the CO to access the unit to see the version of the module	Management app receives the version	CO Public Key Certificate	Status of CO authentication Version of the module	Authentication of CO	Crypto Officer (CO) - CO Public Key Certificate: R,E - TWT CA Public Key Certificate: R,E

Table 10: Approved Services

This table describes the services provided, along with which roles can access each service.

The table also defines the relationship between access to SSPs and the different module services. The modes of access shown in the table are defined as:

- **R** = Read: Role has privilege to read the SSPs.
- **W** = Write: Role has the privilege to write the SSPs.
- **Z** = Zeroize: Role has the privilege to zeroize the SSPs.
- **E**= Execute: Role has the privilege to perform a cryptographic operation

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

The module(s) ship with the validated firmware listed in this Security Policy document. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-3 validation. The Crypto Officer must use the following procedure to load the FIPS 140-3 compliant firmware:

- The Crypto Officer shall be physically present and in control of the module.

- The Crypto Officer shall authenticate into the module using the CO Certificate.
- Use the “Firmware Upgrade” service. The ***TrellisWare TSM Software Update Tool*** provides Crypto Officer access to the service.

4.8 Additional Information

Switches, buttons and status LEDs exist on the outside surface of the module’s enclosure and can only be used for unauthenticated non-security functions.

- These functions are available to the Human Operator role.
- The available non-security functions are summarized in the table below.

Non-Security Function	Access Method	Module State	Human Operator Service
Attach/Remove Power	Module Connector	Off	Manual Non-Security Config
Attach RF Antenna or Cable	Module Connector	Any	Manual Non-Security Config
Attach GPS Antenna or Cable	Module Connector	Any	Manual Non-Security Config
Attach USB OTG Data Cable	Module Connector	Operating	Manual Non-Security Config
Attach USB Host Data Cable	Module Connector	Operating	Manual Non-Security Config
Attach Audio Accessories	Module Connector	Operating	Manual Non-Security Config
Power On/Off	Module Button	Operating	Manual Non-Security Config
Voice Transmit (PTT)	Module Connector	Operating	Manual Non-Security Config
View RF Status	Module LCD	Operating	Manual Non-Security Config
View GPS Status	Module LCD	Operating	Manual Non-Security Config
View Battery Status	Module LCD	Operating	Manual Non-Security Config
View Non-Security Settings	Module LCD	Operating	Manual Non-Security Config
Change Non-Security on-the-fly User Settings	Module LCD and Keypad	Operating	Manual Non-Security Config

5 Software/Firmware Security

5.1 Integrity Techniques

The module(s) run the following integrity tests at startup:

- File system FW Integrity test, SHA-256
- FPGA FW Integrity test, SHA-256

5.2 Initiate on Demand

The integrity tests can be initiated on demand by running a power cycle on the module(s).

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

Only the validated version(s) of firmware identified in this Security Policy can be installed, while the module(s) are used in the Approved mode. Data output is inhibited prior to successful completion of the load test, self-tests and in the error state. The version of the installed firmware is indicated in the ***TrellisWare Management app*** and the ***TSM Software Download PC app***.

6.2 Configuration Settings and Restrictions

The operational environment is not configurable outside of settings and commands available through the ***CO-authenticated API Services***. TrellisWare provides customers with applications based on the API services. The API descriptions are also published to customers wanting to create custom applications.

No services are provided to view or read the File System, RAM or FPGA. Only executables compiled by TrellisWare Technologies, Inc. are properly formatted for writing to the module(s). Power-on integrity tests of the executables ensures tampering has not occurred.

Writing of executables and SSPs to the module(s) is done via CO-authenticated API services. The API descriptions and TrellisWare provided tools for CO services are only provided to individuals performing the CO role in the customer's organization. The Firmware will reject API commands that are not properly formatted.

This document may be freely reproduced and distributed (without revision).

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper Evident Coating	Daily	Inspect all screws and connector nuts. See figure(s) in Section 2 of the Security Policy. A magnifying glass or camera can be used as an aid for inspection.

Table 11: Mechanisms and Actions Required

The module is of production quality. Tamper evident coating is applied to all screws on each access panel by the Crypto Officer upon delivery. This makes it impossible to remove or move aside the access panel without resulting in damage to the tamper evident coating. If tampering is demonstrated, the local Crypto Officer is instructed to perform the zeroize operation prior to discarding the module or returning it to the manufacturer.

Tamper is evident by the presence of any 'dry-joints' or gaps between the adhesive and the protected components, or other inconsistencies in the applications. Inspect screw heads and connector nuts daily for chipped adhesive material. If any damage is present, remove the device from service.

7.2 User Placed Tamper Seals

Number:

Refer to Figure 0-1 above for required locations and examples of the proper technique for applying the sealant.

In the figure(s), the Red arrows indicate access screws that require sealant, and the Blue arrows indicate connector retaining nuts that require sealant. The table below summarizes the number of locations requiring sealant for access screws and connector retaining nuts per module type.

Table 12: Required Locations and Number for Tamper Evidence per Module Type

Module	Number of Access Screw Sealant Locations	Number of Retaining Nut Sealant Locations
TW-860-F Spirit	8	4

Placement:

Tamper evident coating is applied to all screws on each access panel by the Crypto Officer upon delivery. Locations of the screws are indicated in Figure 0-1 above.

- A magnifying glass or microscope is useful for controlling the application of the sealant.
    - Drying time is 20 seconds.

- Excess sealant may be removed with a wipe and/or Q-tip soaked with Isopropyl Alcohol.
    - Try to wipe each application within ~20 seconds for best results.
        - Note: When using solvents, extinguish all ignition sources.
    - Excess dried sealant may also be carefully scraped off as desired for aesthetics.
- Thicker sealant coverage of the fasteners is also acceptable if preferred, up to 1/8" thickness.
    - However, a thicker application may become chipped and appear to be tampered when in fact no tampering has occurred.

Surface Preparation:

Clean the application areas of any grease, dirt, or oil before applying sealant.

Operator Responsible for Securing Unused Seals:

One tube is sufficient for many radios, it is not included with every module. The goal is to cover the tool mating surfaces ('wells') on all access screws and a portion of the connector retaining nuts, such that it will be obvious if tampering has occurred.

Standard shelf life of the sealant is 12 months from date of manufacture when stored in a refrigerator. Shelf life is reduced to 9 months when stored at 60-80°C (16-27°C). The tube of sealant must be stored tip down.

The CO is responsible for storing the unused coating securely to prevent access to the coating by individuals not authorized to apply sealant to new radios.

Part Numbers:

The sealant is TrellisWare P/N 800AAA0036, 'Adhesive, Tamper-Poof Sealant, White'.

Once applied by the CO, the tamper-evident coating is not meant to be replaced during the life cycle of the module(s).

8 Non-Invasive Security

8.1 Mitigation Techniques

The module doesn’t claim non-invasive security mitigation techniques.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
eMMC (Flash) File System - Executable Firmware	The eMMC Flash memory is organized as a File System. At power-on the ARM processor calls the Operating System at a fixed entry point in the Flash file system. The Firmware can be updated by authenticated CO services. No services exist to allow readback of Firmware from outside of the physical boundary.	Static
eMMC (Flash) File System - SSP storage	SSPs are also stored in the Flash file system. The stored SSPs can only be modified by authenticated CO services. Zeroization shreds and then deletes SSPs to fully prevent later recovery.	Static
RAM	SSPs are temporarily copied to RAM to support authentication of CO mode service requests. The temporary copy is overwritten after each service request. No services exist to allow access to the RAM from outside of the physical boundary.	Dynamic
FPGA	The FPGA implements the approved AES-CTR algorithm and provides faster processing compared to the ARM processor. AES-CTR keys are copied to FPGA to support the creation of User mode Ciphertext. No services exist to allow access to the FPGA from outside of the physical boundary.	Dynamic

Table 13: Storage Areas

The ***TrellisWare Management Tool*** is also used to download and store Keys in the module(s)' Flash memory. Keys are stored within the module as Plaintext in eMMC (Flash), File System, RAM, and FPGA.

The CO Public Key Certificate is used by the tool and module to verify that the transfer of keys is authenticated. If the authentication was not successful, the module will not store the new key.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Network Key Wireless	Outside the crypto	eMMC (Flash) File	Encrypted	Automated	Electronic	KTS - Key Wrapping/Unwrapping with AES-CTR and

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Entry	boundary	System - SSP storage				RSA
Network Key Wireless Output	eMMC (Flash) File System - SSP storage	Outside the crypto boundary	Encrypted	Automated	Electronic	KTS - Key Wrapping/Unwrapping with AES-CTR and RSA
Wired Entry via Key Loader	Outside the crypto boundary	eMMC (Flash) File System - SSP storage	Plaintext	Manual	Electronic	Local HTTPS
Wired Output via Key Loader	eMMC (Flash) File System - SSP storage	Outside the crypto boundary	Plaintext	Manual	Electronic	Local HTTPS

Table 14: SSP Input-Output Methods

The download occurs from the PC to any Plaintext I/O port listed in Table 6 ‘Ports and Interfaces’ above. The PC must be connected to one Plaintext I/O port on the module. Note that all Plaintext I/O ports on the module are wired connections only. The required cables are not included with each module and must be purchased separately.

- The table below is a list of the currently available cables that can be used with the ***TrellisWare Management Tool and TSM Software Download Tool***.

Cable P/N	TW-860-F
TW-1230	
TW-1255	
TW-1650	
TW-1665	
TW-1670	
TW-1710	
TW-1712	
TW-1750	
TW-1853	X
TW-2301	X
CBL0770066	
CBL0770067	
CBL0770072	

When using the ***TrellisWare Management Tool***, the module shall be on a Wired LAN with sufficient physical security controls to ensure that no other devices are analyzing or recording network traffic. It is required that the LAN have only one PC with TrellisWare tools and one or more radios to be configured.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Management Application 'Perform Clean'	External app sends an API command to the module	SSPs are stored in an industry-standard file system and temporary storage. Files containing SSPs are first zeroized by overwriting the file contents with zeroes, followed by a standard file 'remove' command. Finally, a hardware reset is commanded which erases the RAM and FPGA temporary contents.	Initiation of the CO API command can be manual or by an application outside of the physical and cryptographic boundary
Emergency	Human operator uses a combination of button presses	SSPs are stored in an industry-standard file system and temporary storage. Files containing SSPs are first zeroized by overwriting the file contents with zeroes, followed by a standard file 'remove' command. Finally, a hardware reset is commanded which erases the RAM and FPGA temporary contents.	Fast zeroization when needed.

Table 15: SSP Zeroization Methods

Zeroization is done by using the supplied ***Management Application***, available to Crypto Officer(s) only. This tool is outside the boundary and out-of-scope of this validation. The required tool is issued to the Crypto Officer(s) only by TrellisWare Technologies, Inc.

The application shows a list of all module(s) connected on the RF Wireless network. Any module listed can be Zeroized by selecting 'Perform Clean', this will invoke the FIPS Zeroize service. To re-initialize the module, follow the steps described in Section 11.1 of this Security Policy.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Network Key	AES-256 CTR mode encryption and decryption of network traffic. This	256 bits - 256	Symmetric key - CSP - CSP		KTS - Key Wrapping/Unwrapping with AES-CTR and RSA Local HTTPS	Packet Creation and Forwarding KTS - Key Wrapping/Unwrapping with AES-CTR and RSA

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	key authenticates the User of the module. The Crypto Officer may store up to 8 Network Keys on a crypto module, but only one key is used at a time.					
CO Private Key	RSA 2048 bit private key used to authenticate keys	2048 bits - 112	Private Key- CSP - CSP		Local HTTPS	KTS - Key Wrapping/Unwrapping with AES-CTR and RSA
CO Public Key Certificate	CO Certificate contains an RSA 2048 bit key used to authenticate Crypto Officer role.	2048 bits - 112	Public Key- PSP - PSP		Local HTTPS	Authentication of CO KTS - Key Wrapping/Unwrapping with AES-CTR and RSA
TWT CA Public Key Certificate	TrellisWare Technologies, Inc. CA Certificate contains an RSA 2048 bit key used to authenticate the Crypto Officer's certificate (certificate chain verification)	2048-bits - 112	Public Key- PSP - PSP		Local HTTPS	Authentication of CO

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	.					
FW Load Public Key	RSA 2048 bit public key used to authenticate Firmware Load.	2048-bits - 112	Public Key-PSP - PSP		Local HTTPS	Firmware load test

Table 16: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Network Key	Network Key Wireless Entry Network Key Wireless Output Wired Entry via Key Loader Wired Output via Key Loader	eMMC (Flash) File System - SSP storage:Plaintext RAM:Plaintext FPGA:Plaintext	Power-on to Power-off	Management Application 'Perform Clean' Emergency	Network Key:Wraped By CO Private Key:Wrapped By Network Key:Wraps
CO Private Key	Wired Entry via Key Loader	eMMC (Flash) File System - SSP storage:Plaintext RAM:Plaintext	Each API service call	Management Application 'Perform Clean' Emergency	CO Public Key Certificate:Paired With Network Key:Wraped By
CO Public Key Certificate	Wired Entry via Key Loader Wired Output via Key Loader	eMMC (Flash) File System - SSP storage:Plaintext RAM:Plaintext	Each API service call	Management Application 'Perform Clean' Emergency	CO Private Key:Paired With
TWT CA Public Key Certificate	Wired Entry via Key Loader Wired Output via Key	eMMC (Flash) File System - SSP storage:Plaintext RAM:Plaintext	Each API service call	Management Application 'Perform Clean' Emergency	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Loader				
FW Load Public Key	Wired Entry via Key Loader	eMMC (Flash) File System - SSP storage:Plaintext RAM:Plaintext	Each FW Load API service call	Management Application 'Perform Clean' Emergency	

Table 17: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
SHA2-256 (A5395)	SHA2-256	Secure Hash	SW/FW Integrity	Module becomes operational	File system FW Integrity test, FPGA FW Integrity test

Table 18: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CTR (C1431)	256-bit AES key	Separate Encrypt and Decrypt KAT	CAST	Module is operational	Encryption, Decryption (Separately)	Power up
RSA SigGen (FIPS186-5) (A5395)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	Sign KAT	CAST	Module is operational	Sign	Power up
RSA SigVer (FIPS186-5) (A5395)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	Verify KAT	CAST	Module is operational	Verify	Power up
RSA SigVer (FIPS186-5) (A5395)	PKCS#1 v1.5 with 2048 bit key and SHA2-256	Verify KAT	SW/FW Load	TSM Software Download PC app shows status	Verify	FW Load

Table 19: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (A5395)	Secure Hash	SW/FW Integrity	On demand	Power cycling the module

Table 20: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CTR (C1431)	Separate Encrypt and Decrypt KAT	CAST	On demand	Power cycling the module
RSA SigGen (FIPS186-5) (A5395)	Sign KAT	CAST	On demand	Power cycling the module
RSA SigVer (FIPS186-5) (A5395)	Verify KAT	CAST	On demand	Power cycling the module
RSA SigVer (FIPS186-5) (A5395)	Verify KAT	SW/FW Load	On FW Load	FW Load

Table 21: Conditional Periodic Information

The self-tests are not repeated during module's operation.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
1st failure	All pre-operational and conditional self-tests run at power-on are not completed within 2-minutes.	At power-on reset, wait 2 minutes for tests to complete	Manually power cycle and subsequent start up without errors	Implicit: No I/O with User and CO modes
2nd failure	All pre-operational and conditional self-tests run at power-on are not completed within 2-minutes.	At power-on reset, wait 2 minutes for tests to complete	No recovery	Implicit: No I/O with User and CO modes

Table 22: Error States

10.5 Operator Initiation of Self-Tests

The operator can initiate self-tests by putting the module through a power cycle.

10.6 Additional Information

When self-test is completed with no failures, the CO and User mode data interfaces will be enabled. The CO can run the Management App to display the overall BIT results, including non-security related tests.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module(s) ship with the validated firmware. Also, the module(s) ship from the factory with a unique, vendor supplied, operator-specific CO Certificate and Network Key credentials. Instructions are shown in the table below.

To operate in the Approved mode, the following actions are required by a Crypto Officer when module(s) are received from the Factory: • Apply anti-tamper sealant, TrellisWare P/N 800AAA0036 to all access fasteners.   ○ The instructions for sealant application are discussed in Section 7.2 of this Security Policy
The following load procedure can be used at any time it becomes necessary or desired: • Re-initialize a module after zeroization. • Upgrade to the latest validated FW version.
After successful completion of this procedure, the module operates in the Approved mode. The instructions are listed below:

• Setup: Plaintext physical port available on all module types.
  ○ The Crypto Officer shall be physically present and in control of the module.
  ○ The Crypto Officer shall inspect the module as per Section 7 in this policy to ensure the Physical Security Mechanisms are not tampered.
  ○ For all steps in this section, the Crypto Officer shall connect directly to any Wired Interface.
  ○ Remote access to the wired interface is a strict violation of this Security Policy. The wired interface must only be accessed locally.

• Cycle power on the module: ○ Using Power button

• Use the “Firmware Upgrade” service. The ***TrellisWare TSM Software Update Tool*** provides Crypto Officer authenticated access to the service.
  ○ Note that the module is shipped from the factory with the validated firmware.
  ○ From the tool, observe that the validated firmware version identified in this Security Policy document is installed on the module.
  ○ Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-3 validation.

• Power-cycle the module. The module will enter the Approved mode of operation following successful power up initialization.
  ○ The ***TrellisWare TSM Software Update Tool*** and ***Management App*** will indicate the Approved mode is enabled, FW version and CO Certificate name.
  ○ Crypto Officer access to these tools indicates that power-on and conditional self-tests are not failing.

11.2 Administrator Guidance

- Each customer shall assign one or more persons to act as Crypto Officers.
- Only Crypto Officers shall be provided access to the TrellisWare Technologies, Inc configuration tools and API documentation.
- Crypto Officers and other administrators shall be familiar with this Security Policy document and follow the startup procedures in Section 11.1 above.
- The following TrellisWare TNC web app command and related steps shall not be used in the Approved mode of operation: 'Certificate Update -> Generate Certificate'.
    - If the Generate Certificate command is accidentally performed by the CO, the module will still be in the Approved mode, as the generated certificate will not be used as a CSP without also performing the following disallowed manual steps.
        - The CO shall not add 'generate.p12' to Firefox or other browser used to access the module's web apps, as the module will subsequently no longer be in the Approved mode.

  Note: Adding a certificate to a browser requires several manual steps and could not happen by accident.
- When using the Crypto Officer role, the module shall be on a LAN with sufficient security controls to ensure that no other devices are analyzing or storing network traffic. It is required that the LAN have only one PC with TrellisWare tools and one or more radios to be configured.

11.3 Non-Administrator Guidance

- All persons who have access to the Cryptographic module(s) covered by this Security Policy document shall take care to keep the module(s) secure from loss and tampering.
- All persons who have access to the module(s) shall be trained to inspect the module(s) and shall report to administrators any evidence of tampering, damage or loss.

12 Mitigation of Other Attacks

The module does not mitigate other attacks