TrellisWare Technologies, Inc.

TW-900/950 TSM Shadow and TW-870/875 TSM Ghost FIPS 140-2 Non-Proprietary Security Policy

Document Revision:	1.0			
H.W. Version:	ASY0750164 Rev.C	ASY0750090 Rev.C	ASY0750203 Rev.B	ASY0750220 Rev.B
S.W. Version:	N/A			
F.W. Version:	6.1.6-fips-b2			

Revision History		
Document Revision	Date	Description
1.0	10/20/2021	Initial release

Table of Contents

1 INTRODUCTION

The TrellisWare Technologies, Inc TW-900/950 TSM Shadow and TW-870/875 TSM Ghost Cryptographic Modules, F.W. Version 6.1.6-fips-b2, are multi-chip standalone cryptographic modules designed to convert Plaintext Data to/from Ciphertext data using AES256-CTR mode. The modules also authenticate Crypto Officer access using a RSA2048/SHA256 Certificate.

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

1.1 Module Identification

The modules described in this document are identified by a Product ordering numbering. The product label on the module case is applied in the factory and identifies the module by Assembly number. The following table provides a mapping of the Product number to Assembly number.

Table 1: Mapping of Product Numbers to Assembly Numbers

Product Ordering Number	Product Description	HW Assembly Number	HW Revision	FW Version
TW-950	TSM Shadow Radio. Handheld Cryptographic module, with Keypad/LCD	ASY0750164	C	6.1.6-fips-b2
TW-900	TSM Shadow Radio. Handheld Cryptographic module, no Keypad/LCD	ASY0750090	C	6.1.6-fips-b2
TW-875	TSM Ghost Radio. Embeddable Cryptographic module, internal battery	ASY0750203	B	6.1.6-fips-b2
TW-870	TSM Ghost Radio. Embeddable Cryptographic module, no internal battery	ASY0750220	B	6.1.6-fips-b2

2 CRYPTOGRAPHIC BOUNDARY

For the TW-900/950 TSM Shadow and TW-870/875 TSM Ghost, the physical cryptographic boundary is defined as the module case.

- **Figure 2-1** below shows the physical cryptographic boundary of the TW-950 TSM Shadow.
- **Figure 2-2** below shows the physical cryptographic boundary of the TW-900 TSM Shadow.
- **Figure 2-3** below shows the physical cryptographic boundary of the TW-875 TSM Ghost.
- **Figure 2-4** below shows the physical cryptographic boundary of the TW-870 TSM Ghost.

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

- The Red and Blue arrows in the figures show the locations of the Tamper Evidence, further discussed in Section 7.5 below.

Figure 2-1: TW-950 TSM Shadow Module

Figure 2-2: TW-900 TSM Shadow Module

Figure 2-3: TW-875 TSM Ghost Module

Figure 2-4: TW-870 TSM Ghost Module

2.1 Module Block Diagrams

The figures below show a simplified block diagram depicting major hardware components of the cryptographic modules, component interconnections, Plaintext data paths, Ciphertext data paths, Non-security Human Operator features and Crypto Officer control paths.

- ***Figure 2-5*** below is the Block Diagram for the TW-900/950 TSM Shadow modules.
  - Note that the Keypad/LCD interface is available on the TW-950 Only.
- ***Figure 2-6*** below is the Block Diagram for the TW-870/875 TSM Ghost modules.
  - Note that the RF Antenna connector type on the TW-875 is a TNC jack, while the TW-870 is a SMA jack.
  - Also, the LCD interface and internal battery are present on the TW-875 only. The LCD interface provides non-security status only.

All modules run the same Firmware. They differ only in case size and variations in connectors and controls mounted on the case.

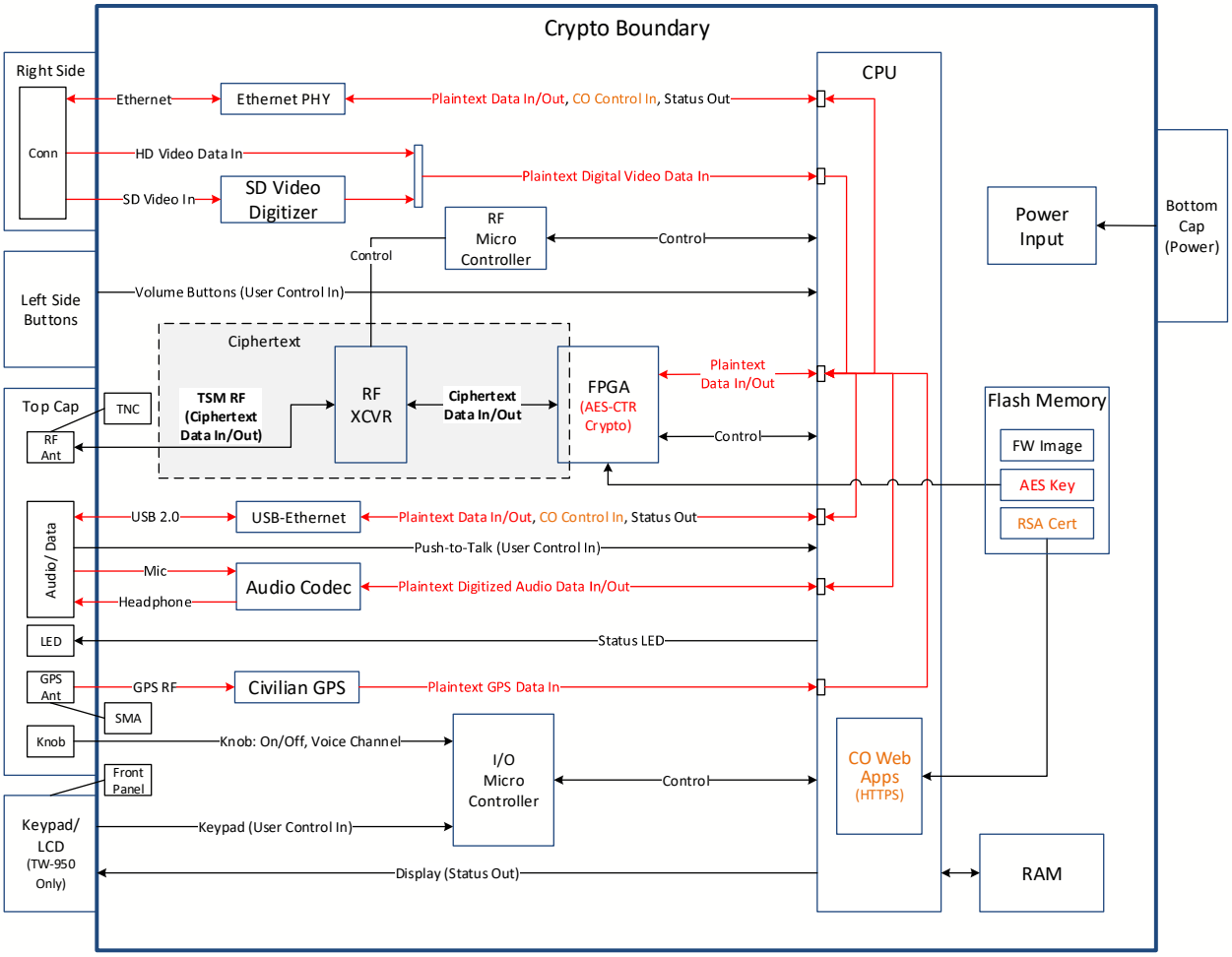

Figure 2-5: TW-900/950 TSM Shadow Module Block Diagram

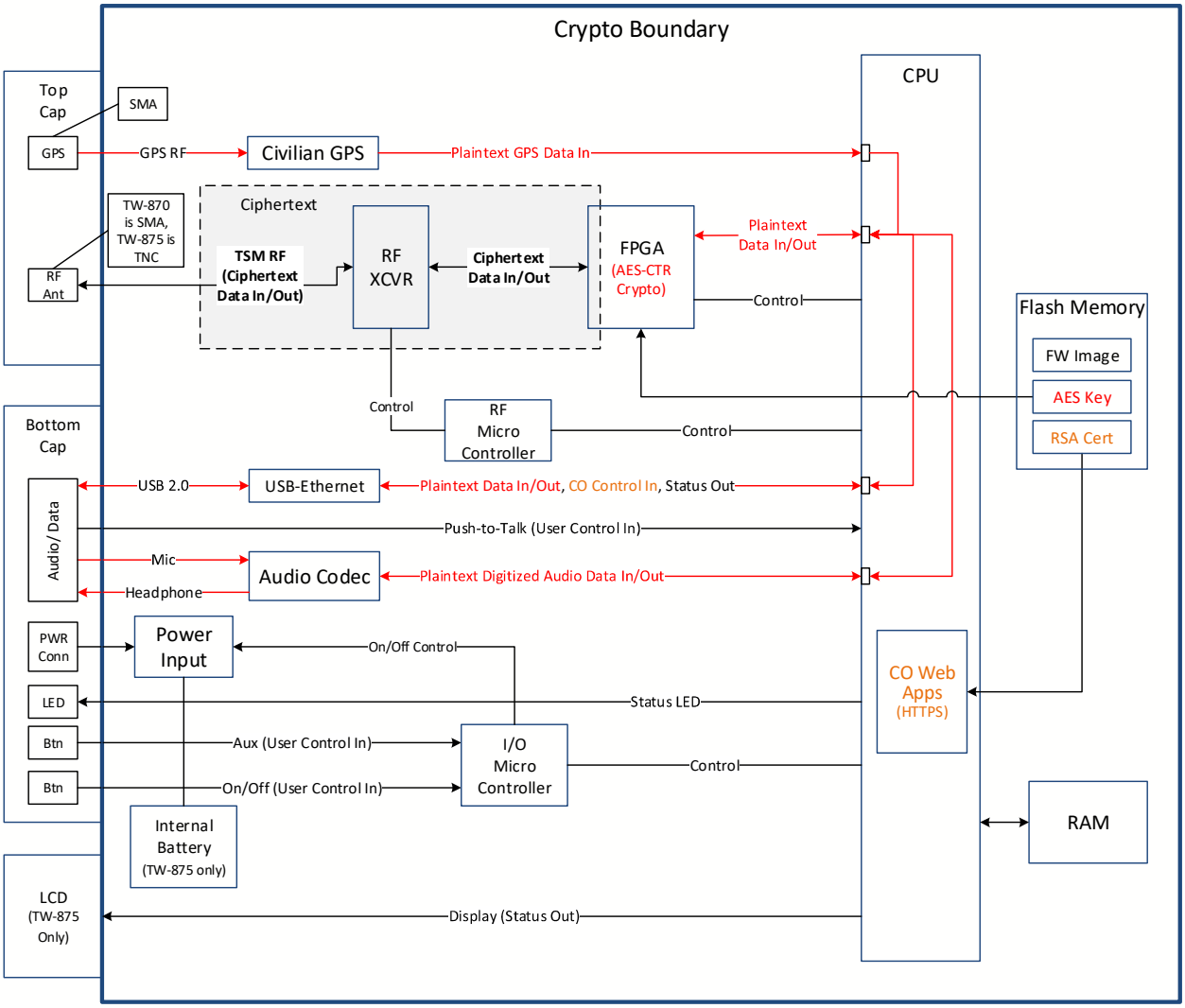

Figure 2-6: TW-870/875 TSM Ghost Module Block Diagram

2.2 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.

3 ACRONYMS

The following table specifies acronyms related to the cryptographic module that are referenced in this document.

Table 2: Specification of Acronyms and their Descriptions

Term	Definition	Description
AES	Advanced Encryption Standard	See FIPS 197. Developed by Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process circa 2001
ANSI	American National Standards Institute	Private nonprofit organization that oversees the development of voluntary consensus standard
CAVP	Cryptographic Algorithm Validation Program	Provides validation testing of Approved cryptographic algorithms and their individual components. Cryptographic algorithm validation is a prerequisite of cryptographic module validation
CMVP	Cryptographic Module Validation Program	A joint American and Canadian security accreditation program for cryptographic modules
CO	Crypto/Cryptographic Officer	An individual assigned to configure a FIPS 140-2 Approved Cryptographic Module
CRC	Cyclic-Redundancy Check	Typically, 3 to 64 bits. Error detection, but no correction. Not suitable as a signature hash
CSP	Critical Security Parameters	For example, Keys and Certificates
CT	Ciphertext	Encrypted data
CTR	Counter	In this context, a type of AES cipher using a counter as the key. Counter is typically initialized using a shared key.
ECB	Electronic Code Book	In the AES context, a cipher operation is done on each block of 16-bytes
EMC	Electro-Magnetic Compatibility	Device design features to ensure co-existence with other electronic devices
EMI	Electro-Magnetic Interference	Device design features to ensure proper operation in the presence of interfering signals from other electronic devices or nature
FIPS	Federal Information Processing Standards Publication	A set of publications issued by NIST
FW	Firmware	Software used in embedded systems
GPS	Global Positioning System	A satellite-based radio-navigation system operated by the US Air Force. It provides geolocation and time information
GUI	Graphical User Interface	Allows users to interact with electronic devices through graphical icons

Term	Definition	Description
HTTPS	Secure Hypertext Transfer Protocol	HTTP is a text-based messaging method that is used to access Web pages. Security is added using TLS, usernames and passwords.
HW	Hardware	Electronics circuit boards, components and modules
IP	Internet Protocol	As used herein. May also mean 'Intellectual Property' in other documents
KAT	Known Answer Test	Part of power-on self-tests of CSPs
LCD	Liquid Crystal Display	Flat-screen display technology
LED	Light Emitting Diode	As used herein, an indicator lamp. May be single-color or multi-colored
N	No	If not part of a word
N/A	Not Available or Not Applicable	Can be interpreted as Don't Care
NIST	National Institute of Standards and Technology	US Government agency which (among other things) defines requirements for and certifies compliance of Cryptographic Modules
OTAC	Over-the-Air Clearing	Wirelessly disable a key (but not destroyed)
OTAR	Over-the-Air Rekeying	Wirelessly change a key
OTAZ	Over-the-Air Zeroing	Wirelessly zero a key (must be reloaded)
PC	Personal Computer	Windows, Mac, Chrome or Linux
PLI	Position/Location Information	Small packets of formatted data typically added to data streams
PT	Plaintext	Non-encrypted machine or human readable data
PTT	Push-To-Talk	Button used to start sending voice over a Radio link
R	Read	If not used as part of a word
RF	Radio Frequency	Synonym for wireless communications
RSA	Rivest-Shamir-Adleman	Public key crypto algorithm named after its inventors
RW	Read and Write	If not used as part of a word
SHA	Secure Hash Algorithm	See FIPS PUB 180-2
SMA	Sub-Miniature version A	Radio Connector developed in the 1960s
SSL	Secure Socket Layer	Older version of TLS, but term is still used even when TLS is actually being used
SW	Software	Can be applicable to embedded, desktop or mainframe computers
TBD	To Be Determined	Indicates details will be added later
TN	Technical Note	Supplemental technical documents
TNC	Threaded Neill–Concelman	Radio Connector invented in the late 1950s, named after its inventors
TLS	Transport Layer Security	Provides communications security over a computer network
v or V	Version	If not used as part of a word
W	Write	If not used as part of a word
Y	Yes	If not used as part of a word

4 SECURITY LEVEL SPECIFICATION

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2, as shown in the table below.

Table 3: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
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	2
Mitigation of Other Attacks	None
Overall Level	**2**

5 PHYSICAL PORTS AND LOGICAL INTERFACES

The interfaces for the cryptographic boundary include physical and logical interfaces. The physical interfaces provided by each module are mapped to four FIPS 140−2 defined logical interfaces: Data Input (DI), Data Output (DO), Control Input (CI), and Status Output (SO). The mapping of FIPS 140−2 logical interfaces to module physical interfaces is provided in the following tables.

The physical ports are identified in the module photos above - ***Figure 2-1***, ***Figure 2-2***, ***Figure 2-3***, ***Figure 2-4***. The ports are also shown in the block diagrams above - ***Figure 2-5*** and ***Figure 2-6***.

FIPS 140-2 Logical Interfaces	Physical Ports
Data Input	RF Antenna Connector, GPS Antenna Connector, Audio/Data Connector, Right-Side Connector Interface
Data Output	RF Antenna Connector, Audio/Data Connector, Right-Side Connector Interface
Control Input	RF Antenna Connector, Audio/Data Connector, Right-Side Connector Interface, Knob, Left-Side Volume Buttons, Left-Side Push-to-Talk Button, LCD, Keypad, Pushbuttons
Status Output	RF Antenna Connector, Audio/Data Connector, Right-Side Connector Interface, LCD, Status Indicator LED, Pushbuttons
Power	Power Connector, Internal Battery

The table below and notes that follow provide more details about each port, including:

- A description of each port
- The operator roles supported by each port
- Which ports transfer plaintext or ciphertext
- Which ports support CSP input

Table 4: Logical Interface/Physical Interface Mapping

Physical Port	Description	Human Operator Control	Crypto Officer Control Input	User Plaintext Data I/O	User Ciphertext Data I/O	Status Out	Power	CSP I/O
RF Antenna Connector Note 1	SMA (TW-870) or TNC (TW-875/900/950) RF connector		CI Note 1a		DI, DO	SO		
GPS Antenna Connector	Civilian GPS antenna SMA connector			DI				
Audio/Data Connector Note 2	12-pin audio, data in/out connector	CI Note 3	CI	DI, DO		SO		DI Only
Right-Side Connector Interface Note 2, 4	Multi-pin connector for dongle accessories		CI	DI, DO		SO		DI Only
Knob Note 4	16-position multi-function Power/ Channel Select	CI						
Left-Side Volume Buttons Note 4	Volume up/down push buttons	CI						
LCD Note 5	LCD display					SO		
Keypad Note 6	Standard touchtone-style numeric keypad	CI						
Status Indicator LED	Multi-color LED provides network status, signal strength and hop count					SO		
Pushbuttons Note 7	Buttons for On/Off, battery and RF status	CI	CI			SO		
Power Connector	Battery/power adapter						CI	
Internal Battery Note 8	Internal rechargeable battery						CI	

Notes:

1. All data I/O on the RF Antenna is Ciphertext.
   a. The Crypto Officer can perform over-the-air Zeroization, but not rekeying.
2. All data I/O on the Audio/Data connector and Side connector is Plaintext.
3. The Audio/Data connector has a Push-to-Talk (PTT) input pin for Audio transmit.
4. These ports are present on TW-900/950 TSM Shadow modules only.
5. The LCD is present on TW-950 TSM Shadow and TW-875 TSM Ghost modules only.
6. The Keypad is present on TW-950 TSM Shadow modules only.
7. Buttons are only used for non-security actions - On/Off, Volume and to report Non-security status (Link Quality and Battery).
   a. Security failure status is perpetual and requires no Human Operator actions.
      - No additional security status results from use of the buttons.
   b. TW-900/950 TSM Shadow: Volume buttons are located on the left-side of the module.
      - Press each button individually to change the Audio volume.
      - Press the two Volume buttons at the same time to view Link Quality on the Status LED for 5 seconds.
        - The LED emits colors ranging from blue (best), green, yellow, to red (worse).
   c. TW-870/875 TSM Ghost: On/Off and Aux buttons are located on the bottom cap.
      - Press the On/Off for 3 seconds to turn the module on/off.
      - Press the On/Off button for <1 second to view Battery status for 5 seconds.
        - The LED emits colors ranging from blue (best), green, yellow, to red (worse).
      - Press the Aux button for <1 second to view the Link Quality for 5 seconds.
        - The LED emits colors ranging from blue (best), green, yellow, to red (worse).
8. The internal battery is present on TW-875 TSM Ghost modules only.

6 SECURITY RULES

This section specifies the security rules under which the cryptographic module shall operate:

1. The cryptographic module shall provide distinct operator roles:
   - User
   - Crypto Officer
   - Unauthenticated Human Operator
2. The cryptographic module shall provide role-based authentication.
3. The cryptographic module shall clear previous authentications on power cycle or closure of Web Browser GUI window.
4. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
5. The cryptographic module shall perform Power-up self-tests:
   - Integrity tests -
     - FW Environment Integrity test, CRC-32.
     - File system FW Integrity test, SHA-256.

    - FPGA FW Integrity test, SHA-256.
  - Security self-tests -
    - AES-256 CTR Encrypt and Decrypt Known Answer Tests (KAT).
    - RSA 2048 Verify KAT (includes SHA-256 KAT).
  - Critical Functions tests - none.

6. Power-up self-tests do not require any operator action.
   - During the power-on sequence, the Status LED will cycle through the following color sequence - White, Red, Yellow, Light Blue, Blue, followed by self-test results.
   - Self-test Pass/Fail indications shall be as follows:
     - Success of all self-tests will be indicated by Green for ~10 seconds on the Status LED.
     - Failure of Security self-tests will be indicated by a Red/Blue pattern on the Status LED, repeating twice per second.
     - On failure of FW Environment CRC-32 test, the Green color on the Status LED will not be displayed. Instead, the module will display a solid White color on the Status LED.
     - For all failures, the operator can attempt to power-cycle the module.
       - If the module returns to this state, the module must be RMA'd and sent back to TrellisWare Technologies, Inc.
7. The operator shall be capable of commanding the module to perform the power-up self-test by cycling power.
8. When loading new Firmware, the cryptographic module shall perform a Firmware load test on the new Firmware.
   - The Firmware load test uses RSA 2048 with SHA-256 Digital Signature Verification.
   - Failure of the Firmware load test will be indicated by a status message on the ***TrellisWare TSM Software Update Tool*** screen and the Status LED will blink Red/Green, repeating twice per second.
9. Data output shall be inhibited during self-tests, zeroization, and error states.
10. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
11. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
12. The module does not support a maintenance interface or role.
13. The module does not support Cryptographic bypass.
14. The module does not support cryptographic key generation.
15. The module supports electronically-distributed manual key entry using supplied applications that only function when the module is in Authenticated CO mode. This is covered below in Section 7.6.
16. The module does not output plaintext Keys or CSPs.
17. The following ***TrellisWare MMC web app*** command and related steps shall not be used in FIPS-approved operation - 'Certificate Update -> Generate Certificate'.

- If the ***TrellisWare MMC*** command is accidentally performed by the CO, the module will still be in FIPS-approved operation, 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 no longer be in FIPS-approved operation.
    - Note: Adding a certificate to a browser requires several manual steps and could not happen by accident.

18. 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 recommended that the LAN have only one PC with Trellisware tools and one or more radios to be configured.

7 CRITICAL SECURITY PARAMETERS, PUBLIC KEYS, AND PRIVATE KEYS

This section shows all Critical Security Parameters (CSPs), Public Keys, and Private Keys. The process of key generation, storage, and zeroization is also described.

7.1 List of Critical Security Parameters (CSPs) and Public Keys

The modules contain the following CSPs:

Table 5: List of CSPs and Public Keys

Algorithm	Name	Type	Description
AES-256 CTR Encryption/ Decryption	Network Key	Private Key	• AES-256 CTR mode encryption and decryption of network traffic. • This 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. • Generation: N/A • Storage: Plaintext in eMMC (Flash), File System, RAM, and FPGA • Zeroization: Actively overwritten via “FIPS Zeroize (OTAC)”
RSA-2048 with SHA-256	CO Public Key Certificate	Public Key	• CO Certificate contains an RSA 2048 bit key used to authenticate Crypto Officer role. • Generation: N/A • Storage: Plaintext in eMMC (Flash), File System, RAM • Zeroization: N/A
RSA-2048 with SHA-256	TWT CA Public Key Certificate	Public Key	• TrellisWare Technologies, Inc. CA Certificate contains an RSA 2048 bit key used to authenticate the Crypto Officer’s certificate (certificate chain verification). • Generation: N/A • Storage: Plaintext in eMMC (Flash), File System, RAM • Zeroization: N/A
RSA-2048 with SHA-256	FW Load Public Key	Public Key	• RSA 2048 bit public key used to authenticate Firmware Load. • Generation: N/A • Storage: Plaintext in eMMC (Flash), File System, RAM • Zeroization: N/A

7.2 Key Generation

The modules do not generate Keys. To generate Network Keys and CO Certificates for the modules, a supplied Windows PC Application must be used - ***TrellisWare TSM 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. via the TrellisWare support website (login account required).
- The tool will install and run on any Windows 7 or 10 PC.

TrellisWare Tech Note TN-0091– TSM Management Tool (v.1.0.3.16) is the User Guide for the tool and is available to existing customers via the TrellisWare support website or to prospective customers by contacting TrellisWare customer service.

7.3 Key Storage

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

The CO Public Key Certificate shown in Table 5 above is used by the tool and module to verify that the transferred key has a valid signature. If the signature is not valid, the module will not store the new key.

The download occurs from the PC to any Plaintext I/O port listed in Table 4 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.

- Here is a list of the currently available cables that can be used with the ***TrellisWare TSM Management Tool***:
  - P/N TW-1650
  - P/N TW-1665
  - P/N TW-1670
  - P/N TW-1212
  - P/N TW-1230
  - P/N TW-1250
  - P/N TW-1255

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

7.4 Zeroization

Zeroization is done by using the supplied ***TTV-C Web 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 modules connected on the RF Wireless network. Any module listed can be Zeroized by selecting 'Perform Clean', this will invoke the FIPS Zeroize (OTAC) service. To re-initialize the module, follow the steps in ***'Reinitializing Modules After Zeroization'*** below.

7.5 Initializing Modules Received from the Factory

To operate in a FIPS-Approved mode, the following actions are required by a Crypto Officer when modules are received from the Factory:

- Apply anti-tamper sealant, TrellisWare P/N 800AAA0036 to all access fasteners.
- Load the FIPS-Approved firmware, a non-default CO Certificate and non-default Network Key(s).

7.5.1 Applying anti-tamper sealant

Obtain TrellisWare P/N 800AAA0036, 'Adhesive, Tamper-Poof Sealant, White'. Since 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.

- Refer to ***Figure 2-1, Figure 2-2, Figure 2-3 and Figure 2-4 above*** for required locations and examples of the proper technique for applying the sealant.
    - In the figures, 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.
- Clean the application areas of any grease, dirt, or oil before applying.
- 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.
- 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.

Table 6: Required Locations for Tamper Evidence per Module Type

Module	Quantity of Access Screw Sealant Locations	Quantity of Retaining Nut Sealant Locations
TW-950 TSM Shadow	19	2
TW-900 TSM Shadow	19	2
TW-875 TSM Ghost	8	3
TW-870 TSM Ghost	14	3

7.5.2 Load FIPS-Approved firmware, non-default CO Certificate and non-default Network Key(s)

The modules do not ship with the FIPS-Approved firmware. Also, the modules ship from the factory with a default CO Certificate and Network Key. To operate in a FIPS-approved state, follow the steps in ***'Reinitializing Modules After Zeroization'*** below.

7.6 Reinitializing Modules After Zeroization

The Crypto Officer must use the following procedure to re-initialize a module in the FIPS Approved mode of operation:

- Setup
  - The Crypto Officer shall be physically present and in control of the module.
  - The Crypto Officer shall inspect the module as per Section 12 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 the Audio/Data Connector physical port available on all module types.
    - On the TW-900/950 TSM Shadow modules, the Right-Side Connector physical port may also be used.
    - Remote access is a strict violation of this Security Policy.
- Cycle power using the Channel knob on the TW-900/950 TSM Shadow or Power button on the TW-870/875 TSM Ghost.
- Verify the FIPS validated firmware 6.1.6-fips-b2 is installed on the module.
  - Use the “Firmware Upgrade” service. The ***TrellisWare TSM Software Update Tool*** provides Crypto Officer access to the service.
  - The Crypto Officer shall authenticate into the module using the default CO Certificate.
  - Note that the module is not shipped from the factory with the FIPS validated firmware 6.1.6-fips-b2.
    - Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation.
  - If firmware 6.1.6-fips-b2 is not installed, the CO shall install the firmware using the tool.
- The Crypto Officer shall replace the default certificate.
  - Manually load a new CO Certificate on the module via electronic distribution manual key entry.

    - Use the Security Configuration service "Certificate Update" API. The ***TrellisWare TSM Software Update Tool*** provides Crypto Officer access to the API.
- The Crypto Officer shall replace the default Network Key.
    - Manually load a new Network Key onto the module via electronic distribution manual key entry.
        - Use the Security Configuration service “TWW Configuration” API. The required API is called from the ***TrellisWare TSM Management Tool***, a Windows PC application supplied with the module.
        - The Crypto Officer shall authenticate into the module using the CO Public Key.
- Power-cycle the module. The module will enter FIPS Approved mode of operation following successful power up initialization.
    - For FIPS Approved mode of operation, the Crypto Officer shall ensure the Module LED is enabled by un-checking the 'Light Discipline' checkbox in the ***TrellisWare MMC*** utility application. 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. via the TrellisWare support website (login account required).
        - Note: The module is shipped from the Factory with the LED enabled.
        - Re-installing the FIPS Approved firmware enables the LED by default.

8 IDENTIFICATION AND AUTHENTICATION POLICY

The module supports distinct operator roles: Crypto Officer (CO) and User. Additionally, the module supports an unauthenticated Human Operator role. These roles and the required identification and authentication are described below.

Table 7: Roles and Required Identification and Authentication (FIPS 140-2 Table C1)

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

The strength of each implemented authentication mechanism is described below.

Table 8: Strengths of Authentication Mechanisms (FIPS 140-2 Table C2)

Authentication Mechanism	Strength of Mechanism
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. Thus, the probability that a random attempt will succeed is $1 \div 2^{112}$, which is less than the required 1/1,000,000 (~$1/2^{20}$). • Each HTTPS attempt was observed to be 5024 bytes (40192 bits). At the module's maximum 100 mbps rate, the maximum number of HTTPS attempts per second is 100e6 ÷ 40192 bits, or 2488 per second, ignoring packet overhead. Multiply x 60 = 149280 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 $1 \div 2^{(112-18)}$ => $1/2^{94}$, which is ~5.5 times better than the required 1/100,000 (~$1/2^{17}$).
Network Key	• An AES key provides an equivalent security strength of 256-bits. The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{256}$, which is less than the required 1/1,000,000 (~$1/2^{20}$). • AES-256 output blocks are 128-bits in length. The Ciphertext output port is capable of 16M bps maximum, or 16M ÷ 128 blocks/sec = 125K blocks/sec that an attacker could analyze. Rounding up to a power of 2 = 131K (2^{17}) blocks per second. Thus, the probability of a success is $1 \div 2^{(256-17)}$ => $1/2^{239}$, which ~14 times better than the required 1/100,000 (~$1/2^{17}$).

9 ACCESS CONTROL POLICY

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

Table 9: Services Authorized for Roles (FIPS 140-2 Table C3)

Crypto Officer	User	Human Operator	Service	Description
X			Crypto Officer Authentication	Uses the CO Public Key Certificate to allow the CO to access the unit for Security and Non-security configuration.
X			Non-Security Configuration	Configure non-security settings and Wideband RF settings.
X			Security Configuration	Enter and select the FIPS-140 CSP's - CO Public Key Certificate and AES-256 CTR Network Key via electronic distribution manual key. Prior to a certificate update, the module is automatically zeroized.
	X		Packet Forwarding	Provides packet transfer between the RF Ciphertext port and Plaintext Ethernet ports. Packets are encrypted and decrypted using the AES-256 Network Key.
	X		Packet Creation	Provides Ciphertext packet creation from internal Plaintext sources (GPS, Audio, Video). Packets are encrypted using the

Crypto Officer	User	Human Operator	Service	Description
				AES-256 Network Key. Encrypted packets are transmitted via RF.
X			Network Monitoring & Remote Control	Monitor network and individual radios. Remote control of radio non-security settings and stream control.
X			Firmware Upgrade	Upgrade firmware release. *Note*: If non-FIPS validated firmware is loaded, the module is no longer a FIPS validated module.
		X Note 1	Power-on Module Self-Tests	Performs module's power-up self-tests. If failing, enters Error state.
		X Note 2	Module Status LED	Provides Security and Non-Security Status LED indications.
X			Module Status API	Provides CO Non-security Status API service for PC, Android and Web apps.
X			FIPS Zeroize (OTAC)	Remotely zeroize all CSPs in the module. Once zeroized, the module must be reinitialized as described above.
		X Note 2	Manual Non-Security Configuration	Selection of voice channel, volume and other non-security configuration parameters using the manual controls on the unit.

Note 1. See Section 6, Security Rules for more details about Power-on Module Self-Tests.

Note 2. See Table 14 below for more details.

The table below defines the relationship between access to CSPs or Public Keys and the different module services. The modes of access shown in the table are defined as:

- **R** = Read: Role has privilege to read the CSP or Public Key.
- **W** = Write: Role has the privilege to write the CSP or Public Key.
- **Z** = Zeroize: Role has the privilege to zeroize the CSP or Public Key.

Table 10: Access Rights within Services (FIPS 140-2 Table C4)

Service	Network Key	CO Public Key Certificate	TWT CA Public Key Certificate	FW Load Public Key
Crypto Officer Authentication		R	R	
Non-Security Configuration [Note 1]		R	R	
Security Configuration	RW	RW	R	
Packet Forwarding	R			
Packet Creation	R			
Network Monitoring & Remote Control		R	R	
Firmware Upgrade		RW	RW	R
Power-on Module Self-Tests	N/A	N/A		
Module Status LED	N/A	N/A		
Module Status API		R	R	
FIPS Zeroize (OTAC)	Z	N/A		
Manual Non-Security Configuration [Note 2]	N/A	N/A		

Note 1. Non-security configuration that is done via PC, Android and Web applications requires CO Authentication, as only a CO shall have access to these tools. This includes RF Settings, Voice Settings, Video Streaming setup, IP Settings and Position-Location-Info (PLI) Settings.

Note 2. Manual configuration from the module's knobs and buttons does not require Authentication. A Human Operator is permitted to do manual configuration.

10 ALGORITHMS

10.1 APPROVED ALGORITHMS

The following table is a list of approved algorithms along with their corresponding CAVP certificates, standards, modes/methods, key lengths, curves, or moduli, and how they are used.

Table 11: FIPS Approved Algorithms Used in the Module

CAVP Cert. #	FIPS Approved Algorithm	Standard	Mode/ Method	Key Len	Use
C1431	AES	FIPS 197 and SP 800-38A	ECB[1], CTR	256-bits	RF Over-the-Air Encryption/Decryption
C1430	RSA	FIPS 186-4 and PKCS 1.5	RSA Signature Verification	2048-bits	For CO authentication and firmware load
C1430	SHS	FIPS 180-4	SHA-256		For CO authentication, firmware load and integrity tests at power-on

Note 1. AES-CTR mode uses ECB mode Encryption for both AES-CTR Encryption and Decryption. Thus, it is typical to obtain approval for ECB Encryption together with AES-CTR.

10.2 ALLOWED ALGORITHMS

The following table is a list of allowed algorithms, caveats and how they are used.

Table 12: FIPS Allowed Algorithms Used in the Module

FIPS Allowed Algorithm	Caveat	Use
AES (“non-compliant”)	No security claimed[1]	Used internally and separate from AES Cert # C1431. As per FIPS 140-2 IG 1.23, this is used to “obfuscate” data using proprietary implementations. All obfuscated data is treated as plaintext.
HTTPS using SSL v2, SSL v3, and SSL v3.1/TLS 1.2 using any ciphersuites	No security claimed[1]	As per FIPS 140-2 IG 1.23, this is used to support a secure channel between applications/web browser to 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 HTTPS for this. • Certificate Update service • Firmware Upgrade service • RF Network Configuration service • Module Status API service

Note 1. CSPs cannot be read back from the module. Thus, these additional algorithms are not considered part of the FIPS Cryptographic functionality. For FIPS, all internally stored CSPs are considered plaintext.

10.3 NON-APPROVED ALGORITHMS

The following table is a list of non-approved algorithms and how they are used.

Table 13: FIPS Non-Allowed Algorithms Used in the Module

FIPS Non-Allowed Algorithm
There are no Non-Allowed Algorithms used in the Module

11 UNAUTHENTICATED SERVICES

Within the Cryptographic boundary, the module provides only a FIPS Approved mode of operation. The module will enter FIPS Approved mode following successful power up initialization.

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

- These services are available to the Human Operator role.
- The available non-security services are summarized in the table below.
- Not all services are available on every module type, as shown in the table.

Table 14: List of Unauthenticated Services

Non-Security Service	Access Method	Module State	Human Operator Service
Attach/Remove Power	Module Connector	Off	Manual Non-Security Config
Attach Side Accessories [Note 1] (TW-900/950 TSM Shadow only)	Module Connector	Off	Manual Non-Security Config
Attach 12-pin Conn Cable	Module Connector	Operating	Manual Non-Security Config
Power On/Off (TW-900/950 TSM Shadow only)	Module Knob	Operating	Manual Non-Security Config
Power On/Off (TW-870/875 TSM Ghost only)	Module Button	Operating	Manual Non-Security Config
Change Voice Channel (TW-900/950 TSM Shadow only)	Module Knob	Operating	Manual Non-Security Config
Change Voice Volume (TW-900/950 TSM Shadow only)	Module Buttons	Operating	Manual Non-Security Config
Voice Transmit (PTT)	Module 12-pin Conn	Operating	Manual Non-Security Config
View RF Status (TW-950 TSM Shadow only)	Module LCD	Operating	Manual Non-Security Config
View RF Status	Module LED	Operating	Module Status LED
View GPS Status (TW-875 TSM Ghost, TW-950 TSM Shadow only)	Module LCD	Operating	Manual Non-Security Config
View Battery Status (TW-875 TSM Ghost, TW-950 TSM Shadow only)	Module LCD	Operating	Manual Non-Security Config
View Battery Status (TW-870/875 TSM Ghost only)	Module LED	Operating	Module Status LED
View Non-Security Settings (TW-950 TSM Shadow only)	Module LCD	Operating	Manual Non-Security Config
Change Non-Security on-the-fly User Settings (TW-950 TSM Shadow only)	Module LCD and Keypad	Operating	Manual Non-Security Config
View LED Status Indicator	Module LED	Operating	Module Status LED

Note 1. Side accessories do not access CSP's or Ciphertext data and use of the side accessories cannot lead to a compromise of the module.

12 PHYSICAL SECURITY POLICY

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.

Table 15: Inspection/Testing of Physical Security Mechanisms (FIPS 140-2 Table C5)

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Coating	Daily	Inspect all screws and connector nuts. See figures in Section 2 above. A magnifying glass or camera can be used as an aid for inspection.

13 EMI/EMC

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

14 MITIGATION OF OTHER ATTACKS POLICY

The following table specifies a security policy for mitigation of other attacks, including the security mechanisms implemented to mitigate the attacks.

Table 16 - Mitigation of Other Attacks (FIPS 140-2 Table C6)

Other Attacks	Mitigation Mechanism	Specific Limitations
The module does not mitigate other attacks	N/A	N/A