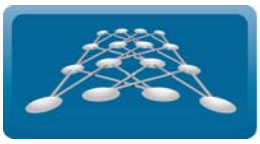

FIPS 140-2 Non-Proprietary Security Policy: TW-400 (CUB)

Level 2 Validation

Document: TWFIPS001
Version: 1.1
Revision Date: 2013/02/07

TrellisWare Technologies Inc.

CHANGE RECORD

Revision	Date	Author	Description of Change
1.0	2012/07/12	Chris Litvin	Initial release
1.1	2013/02/07	Chris Litvin	Incorporate CMVP Comments

Contents

1. Module Overview 5
2. Security Level 6
3. Initialization Procedures 7
3.1. Initializing Modules Received form the Factory 7
3.2. Reinitializing Modules After Zeroization 7
4. Modes of Operation 7
4.1. FIPS Approved Mode of Operation 7
4.2. Approved and Allowed Algorithms 7
***5.* Ports and Interfaces 8**
6. Identification and Authentication Policy 9
6.1. Assumption of Roles 9
7. Access Control Policy 10
7.1. Roles and Services 10
7.2. Definition of Critical Security Parameters (CSPs) 11
7.3. Definition of Public Keys 11
7.4. Definition of CSPs and Public Key Modes of Access 12
8. Operational Environment 12
9. Security Rules 13
10. Physical Security Policy 14
10.1. Physical Security Mechanisms 14
10.2. Operator Required Actions 14
11. Mitigation of Other Attacks Policy 14
12. References 15

Tables

Table 1 - Module Security Level Specification 6
Table 2 - FIPS Approved Algorithms Used in Current Module 7
Table 3 – FIPS Allowed Algorithms Used in Current Module 7
Table 4 - Logical Interface/Physical Interface Mapping 8
Table 5 - Roles and Required Identification and Authentication 9
Table 6 – Strengths of Authentication Mechanisms 9
Table 7 – Roles and Services 10
Table 8 - CSPs 11
Table 9 - Public Keys 11
Table 10 - CSP and Public Key Access Rights within Roles & Services 12
Table 11 - Inspection/Testing of Physical Security Mechanisms 14

Figures

Figure 1 – Physical Boundary of TW-400 5
Figure 2 – Locations of Blue Tamper Evident Coating 14

1. Module Overview

The module is the TrellisWare Technologies TW-400 (CUB) hand held unit. The module is a multi-chip standalone embodiment. For the TW-400, the physical cryptographic boundary is defined as the module case. Figure 1 shows the physical cryptographic boundary of the TW-400. The cryptographic boundary does not include any port caps. Additionally, the internal IO CPLD, RF Microcontroller, and RF CPLD have been excluded from the FIPS requirements.

Figure 1 – Physical Boundary of TW-400

The Module Configuration covered by this Security Policy is:
TW-400 (CUB)

- Hardware: ASY0540250 rev X1
- Firmware 4c-beta2-FIPS

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1 - 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	N/A
Overall Level	**2**

3. Initialization Procedures

3.1. Initializing Modules Received form the Factory

The TW-400 modules ship from the factory in an initialized state with a default set of User Certificates, Crypto Officer (CO) Certificates, and Network Key. Operators may use the module in the FIPS Approved mode right out of the box. TrellisWare recommends that the Crypto Officer apply a new Network Key to the module before operation as the default Network Key is common to all modules shipped from the factory.

3.2. Reinitializing Modules After Zeroization

The Crypto Officer must use the following procedure to re-initialize the module:

1) Load new certificates on the module using the "Certificate Update" service.

   Note: If the module has not already been zeroized, this service will zeroize all keys on the module.

2) Load the FIPS validated firmware on the module using the “Firmware Upgrade” service. Only the existing version can be reloaded.

3) Load a new Network Key onto the module using the “Wideband Configuration” service.

4. Modes of Operation

4.1. FIPS Approved Mode of Operation

The module provides only a FIPS Approved mode of operation. The module will enter FIPS Approved mode following successful power up initialization. An operator may check that the TW-400 module is in the FIPS approved mode by pressing the status buttons and observing the LED as blue, purple, green, or yellow at any time after power up initialization. An operator may confirm the hardware and firmware version of the module using the Status & Troubleshooting service.

4.2. Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithms.

Table 2 - FIPS Approved Algorithms Used in Current Module

FIPS Approved Algorithm	CAVP Cert. #
AES ECB mode encryption and AES CTR mode encryption/decryption with 256 bit keys [FIPS 197 and SP 800-138A]	1980
RSA 2048 bit signature verification for authentication and firmware load [FIPS 186-3 and ANSI X9.31]	1026
SHA-256 used with RSA signature verification [FIPS 180-3]	1734

The cryptographic module supports the following non-FIPS Approved algorithms which are allowed for use in FIPS mode.

Table 3 – FIPS Allowed Algorithms Used in Current Module

FIPS Allowed Algorithm
AES (Cert. #1980, key wrapping)
AES (“non-compliant”) used internally and separate from AES Cert # 1980 - no security claimed.
HTTPS using SSL v2, SSL v3, and SSL v3.1/TLS 1.0 using many ciphersuites – no security claimed.

5. Ports and 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, Data Output, Control Input, and Status Output. The mapping of logical interfaces to module physical interfaces is provided in the following table.

Table 4 - Logical Interface/Physical Interface Mapping

Physical Port	Description	Logical Interface Types
RF Antenna Connector	SMA wireless antenna connector	Data input, Data output, Control input, Status output
GPS Antenna Connector	SMA GPS antenna connector	Data input
Audio Connector	5-pin audio in/out connector	Data input, Data output
Side Connector Interface	Multi-pin connector for dongle accessory	Data input, Data output, Control input, Status output
Bottom Connector Interface	Battery/power adapter	Power input
Power/ Channel Select	16-position multi-function control knob	Control input
Volume Up	Volume up push button for audio output	Control input
Volume Down	Volume down push button for audio output	Control input
Status LED Indicator	Multi-color LED provides network status, signal strength and hop count	Status output
Status	Buttons used to access network signal strength and hop count status	Control input

6. Identification and Authentication Policy

6.1. Assumption of Roles

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

Table 5 - Roles and Required Identification and Authentication

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	2048 bit Certificate
User	This role accesses the module via Web Browser and has access to most services offered by the module; however it is not permitted to load keys to the module.	Role-based	2048 bit Certificate
Module	This role allows the module to perform “Packet Forwarding” using the Network Keys.	Role-based	256 bit AES key
Human Operator (Unauthenticated)	This role can control switches, dials, and other unauthenticated services on the module.	N/A	N/A

Table 6 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
2048 bit Certificate	The RSA certificate is 2048 bit and uses SHA-256. The probability that a random attempt will succeed is $1/2^{112}$ which is less than 1/1,000,000. The number of HTTPS sessions at a time is limited to 10. Assuming 10 attempts per second per session via a script or automated attack, the probability of a success with multiple attempts is $6000/2^{112}$ which is less than 1/100,000.
256 bit AES Key	The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{256}$ which is less than 1/1,000,000. Assuming 10 attempts per second via a script or automated attack, the probability of a success with multiple attempts is $600/2^{256}$ which is less than 1/100,000.

7. Access Control Policy

7.1. Roles and Services

Table 7 describes the services provided, along with which roles can access each service.

Table 7 – Roles and Services

Crypto Officer	User	Module	Human Operator (Unauthenticated)	Service	Description
X	X[a]			Initialize and Configure	Initialization and configuration of device. This is broken into two subsections (Device and Wideband Configuration) below.
X	X[a]			Device Configuration	Configure device specific parameters as well as external interfaces (dongles).
X	X[a]			Wideband Configuration	Configuration of wideband network, including definition of Network Key.
		X		Packet Forwarding	Provides packet forwarding and receipt. Forwarded packets are encrypted and incoming packets are decrypted.
X	X			Network Monitoring & Remote Control	Monitor network and individual radios. Remote control of radio settings and stream control.
X	X			COMSEC OTAZ/OTAR[b]	Over the air zeroize & rekey of COMSEC channel locks.
X	X			Firmware Upgrade	Upgrade firmware to newer release. *Note*: If non-FIPS validated firmware is loaded, the module is no longer a FIPS validated module.
N/A	N/A			Certificate Generate	This service is described in module documentation but has been disabled in this version of the module.
X	X			Certificate Update	Update the User and CO certificates on a unit. Prior to the certificate update, the module is automatically zeroized.
X	X		X	Self-Test	Performs self test of critical functions of the module. Run automatically at startup.
X	X		X	Status & Troubleshooting	Status of the module, refresh, reboot, run BIT & COMSEC zeroize.
X	X			OTAC (FIPS Zeroize)	Remotely zeroize all CSPs in the module. Once zeroized, the module must reinitialize as described in Section 3.2.
X	X		X	Local Zeroize (COMSEC)[b]	Zeroize COMSEC channel locks on module.
X	X		X	Manual Configuration	Selection of voice channel, volume and other system configuration parameters using the manual controls on the unit.

a. The User role can view Configurations but cannot write them.
b. COMSEC channel locks are not considered CSPs within the scope of this module.

7.2. Definition of Critical Security Parameters (CSPs)

The module contains the following CSPs:

Table 8 - CSPs

Key Name	Type	Description
Network Keys	Encryption	AES-256 bit key for CTR mode encryption and decryption of network traffic. The Crypto Officer may store up to 8 Network Keys on a crypto module by configuring multiple wideband loads, but only one key is used at a time.
KEK	Encryption	AES-256 bit key for CTR mode decryption of Network Keys.

7.3. Definition of Public Keys

The module contains the following public keys:

Table 9 - Public Keys

Key Name	Type	Description
User Certificate (RSA Public Key)	Verify	2048 bit key used to authenticate User Role
Crypto Officer Certificate (RSA Public Key)	Verify	2048 bit key used to authenticate Crypto officer role
FW Certificate (RSA Public Key)	Verify	2048 bit used to verify Firmware load

7.4. Definition of CSPs and Public Key Modes of Access

Table 10 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 - CSP and Public Key Access Rights within Roles & Services

Service	Network Keys	KEK	User Certificate	Crypto Officer Certificate	FW Certificate
Crypto Officer Authentication (not a service - occurs prior to CO services)				R	
User Authentication (not a service - occurs prior to User services)			R		
Module Authentication (not a service - occurs prior to Module services)	R				
Initialize and Configure	RW	R			
Device Configuration					
Wideband Configuration	RW	R			
Packet Forwarding	R				
Network Monitoring & Remote Control					
COMSEC OTAZ/OTAR					
Firmware Upgrade		W	W	W	RW
Certificate Update			W	W	
Self-Test					
Status & Troubleshooting					
OTAC (FIPS Zeroize)	Z	Z	Z	Z	
Local Zeroize (COMSEC)					
Manual Configuration					

8. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the module does not contain a modifiable operational environment.

9. Security Rules

The module's design corresponds to the module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1) The cryptographic module shall provide three distinct operator roles. These are the User role, the Cryptographic Officer role, and Module role. The module also supports an unauthenticated Human Operator role.
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 the following tests

    A. Power-up Self-Tests

        1. Cryptographic Algorithm Tests
            a. AES-256 ECB Encrypt Known Answer Tests (KAT) (Note: ECB Encrypt only required because CTR Encrypt/Decrypt both make use of that function)
            b. RSA 2048 Verify KAT (includes SHA-256 KAT)
        2. Firmware Integrity Test - CRC16 and SHA-256
        3. Critical Functions Tests – N/A

    B. Conditional Self-Tests

        1. Firmware Load Test – RSA 2048 with SHA-256 verify

6) The operator shall be capable of commanding the module to perform the power-up self-test by cycling power. Failure of self-test will be indicated by a reboot of the module.
7) Power-up self-tests do not require any operator action.
8) Data output shall be inhibited during self-tests, zeroization, and error states.
9) Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10) There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
11) The module supports concurrent operators.
12) The module does not support a maintenance interface or role.
13) The module does not support bypass.
14) The module does not support manual key entry.
15) The module does not enter or output plaintext CSPs.
16) The module does not output intermediate key values.

TrellisWare imposed Security Rules are as follows:

1) The Human Operator shall not turn off the module during the OTAC (FIPS Zeroize) service.
2) No more than 10 active HTTPS sessions are allowed to be connected to the module at a time.

10. Physical Security Policy

10.1. Physical Security Mechanisms

The module is of production quality. Blue tamper evident coating is applied to all screws (qty. 13) on each access panel (performed at the factory). 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 evidence 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 daily for chipped adhesive material. If any damage is present, remove the device from service.

Top/Left/Front View

Bottom/Right/Back View

Figure 2 – Locations of Blue Tamper Evident Coating

10.2. Operator Required Actions

Table 11 - Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Coating	Daily	TW-400: Inspect all screws (13). See Figure 2.

11. Mitigation of Other Attacks Policy

The module does not mitigate other attacks.

12. References

FIPS Publication 140-2: *Security Requirements for Cryptographic Modules*

FIPS Publication 180-3: *Secure Hash Signature Standard (SHS)*

FIPS Publication 197: *Advanced Encryption Standard (AES)*

PKCS #1: *RSA Cryptographic Standard*