Trulink Control Logic Module CL6882-M1
Security Policy

Document *Version 1.1*

Telephonics Corp.

Telephonics Corp.

TABLE OF CONTENTS

1. Module Overview

TruLink Control Logic Module CL6882-M1 (P/N 010.6882-01 Rev. B1 FW Versions Boot: SW7158 v2.4 and Application: SW7151 v1.12) (CL6882) is a hardware multi-chip embedded module as defined by FIPS 140-2. The CL6882's crypto boundary is defined as the entire CL6882 component (see Figure 1). It is comprised entirely of production grade components. It is the central component supporting TruLink's secure versatile wireless communication system. It is designed to operate in a variety of critical situations and extreme environments. The TruLink Control Module is designed to be embedded in portable short range radios or access points.

The TruLink system is a fully duplex system that permits multiple users to speak simultaneously without interrupting another user's voice transmission. Unlike conventional walkie-talkies, TruLink users can converse among themselves without pressing a "Push-to-Talk" button or waiting for another user to finish their transmission.

The system supports 50 channels (0-49). Depending on the system configuration, up to 31 users can be logged onto a channel which functions as an independent network. A TruLink network is composed of one TruLink unit designated as the "master" and all other TruLink units operating as "slaves". The master in the system acts as the central controller which handles network separation and routing of all user traffic.

Although the systems central purpose is the transmission of voice data, it also supports the wireless transmission of bulk user data over the same system. This allows the TruLink system to be highly flexible to a wide range of user needs.

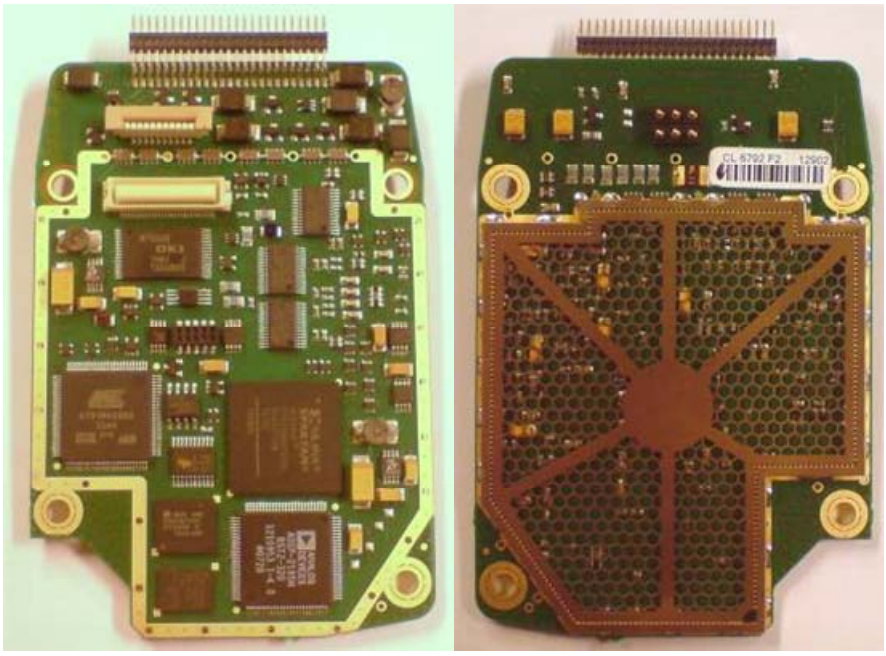

Figure 1 – Image of the Cryptographic Module

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

FIPS Security Requirements Section	Level
Cryptographic Module Specification	1
Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self Test	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Table 1 – Module Security Level Specification

3. Modes of Operation

FIPS Approved mode of operation

In FIPS mode, the cryptographic module only supports FIPS Approved algorithms as follows:

- AES 128 ECB (Cert. #872)
- HMAC-SHA-1 (Cert. #488)
- SHA-1 (Cert. #866)

The module can only enter FIPS mode after authenticated firmware has been successfully loaded via the HMAC-SHA-1 firmware load operation.

NOTE: While in the FIPS Approved mode of operation all security rules shall be enforced, see also reference [2].

Non-FIPS Approved Mode of Operation

The module supports a non-FIPS Approved mode of operation. This mode is invoked when the operator attempts to load in unauthenticated firmware into the module. Such an action permanently places the module into a non-FIPS Approved mode.

4. Ports and Interfaces

The CL6882 module provides the following physical ports and logical interfaces:

Physical Port	Qty	Logical interface definition	Description
50 PIN Port	1	- Power input - Status Output - Control Input - Data Input - Data Output	The main physical port provided by the module. It provides access to the majority of the supported interfaces.
Key Flex Port	1	- Control Input - Status Output	This interface provides the input and output to a key pad and LED. The LED and Key Pad are not included within the crypto boundary.
TR Port	1	- Data Input - Data Output - Status Input	This is the transceiver port which provides the input and output accessed by an attached radio interface. The radio interface is not included within the crypto boundary.
Battery (Power) Port	1	- Power - Status Input - Control Input	Provides power and status from an external battery. It also provides control Input while the module is in a battery charging state.

Table 2 – Ports and Interfaces

5. Identification and Authentication Policy

Assumption of roles

The module supports the FIPS required roles of Crypto-Officer and User as well as an Application User. The Operators of the module are not required to authenticate as this is a Level 1 module[1]. The assumption of a role can either be implicitly assumed in which case the assumption is per interface used or in the instance of the Crypto-Officer can be explicitly assumed by entering an 8 byte "password".

Role	Type of Authentication	Description
Crypto-Officer	No Authentication is provided and/or required at Level 1.	Administrator of the module, with full access to configurations.
User	No Authentication is provided and/or required at Level 1.	The "day-to-day" user of the module, with limited access to services provided by the module.
Application User	No Authentication is provided and/or required at Level 1.	A full access user, allowing access via the application programming interface (API).

Table 3 – Roles and Required Identification and Authentication

[1] Authentication is required per module design, although the provided mechanism does not fully comply with FIPS authentication requirements and so cannot be claimed as Authentication in this context.

6. Access Control Policy

Roles and Services

The following table defines the supported roles and supported services. The column on the left lists the supported roles with the services available to that role shown in the column directly to the right. The services are described further using a bulleted list which can be found in the column at the far right of the table.

Role	Authorized Services	Description
User	**Unit Configuration**	Module functional configuration service.
	Data Transmit and Receive	Transmit or Receive data either encrypted or in plaintext
	Bypass	Enable or Disable encryption
	Status Output	Receive Status Output
	Zeroize	Actively write zeroes over all plaintext CSPs.
Cryptographic-Officer	**Unit Configuration**	Module functional configuration service.
	System Configuration	Module system configuration service.
	Data Transmit and Receive	Transmit or Receive data either encrypted or in plaintext
	Bypass	Enable or Disable encryption
	Status Output	Receive Status Output
	Key Entry and Output	Manually Enter or Output the Traffic Encryption Key(TEK)
	Zeroize	Actively write zeroes over all plaintext CSPs.
	Load Firmware[2]	Load external firmware
Application User	**Unit Configuration**	Module functional configuration service.
	System Configuration	Module system configuration service.
	Application Services	Application specific configuration service.
	Data Transmit and Receive	Transmit or Receive data either encrypted or in plaintext
	Bypass	Enable or Disable encryption
	Status Output	Receive Status Output
	Key Entry and Output	Manually Enter or Output the Traffic Encryption Key(TEK)
	Zeroize	Actively write zeroes over all plaintext CSPs.
	Load Firmware[2]	Load external firmware

Table 4 – FIPS Approved Mode Services Authorized for Roles

[2] The Load Firmware service is a non-FIPS mode service if not performed with the HMAC-SHA-1 integrity test.

Definition of Critical Security Parameters (CSPs)

The following CSPs are contained within the module:

Key	Description/Usage
Traffic Encryption Key (TEK)	This is an AES 128 bit key used to encrypt and decrypt user data within the system.
Software Authentication Key	A SHA-1 HMAC key which is used to authenticate externally loaded firmware.

Table 5 – CSPs

Public Keys

The module does not employ the use of public keys.

Definition of CSPs Modes of Access

The implemented key establishment method is manual. Keys are entered in plaintext via a direct connection with a key loading device.

Table 6 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Read: the data item is read from memory.
- Write: the data item is written into memory.
- Zeroize: the data item is actively overwritten.
- Execute: Utilize the key within an approved security function.

CSP	Unit Configuration	System Configuration	Data Transmit and Receive	Status Output	Key Entry and Output	Application Services	Zeroize	Load Firmware
TEK			*E*		*WZ*	*RWEZ*	*Z*	
Software Authentication Key			*E*				*Z*	*E*

Table 7 – CSP Access Rights within Roles & Services

7. Operational Environment

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

8. Security Rules

The example cryptographic module's design corresponds to the example cryptographic 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 1 module.

1. The cryptographic module shall provide three distinct operator roles. These are the User role, Crypto-Officer role, and Application User role.
2. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
3. The cryptographic module shall encrypt message traffic using the AES-128 ECB algorithm.
4. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

   1. Cryptographic algorithm tests:
      a. AES Known Answer Test
      b. HMAC-SHA-1 Known Answer Test.
   2. Firmware Integrity Test (16 bit Checksum)

   B. Conditional Self-Tests:

   1. Bypass test: Ensures proper application of encryption to data after a switch has been made from clear text transmit and receive to encrypted transmit and receive.
   2. Manual key entry test: Duplicate entry
   3. Firmware Load Test (FW Versions Boot: SW7158 v2.4 and Application: SW7151 v1.12): HMAC-SHA-1
5. At any time an operator can power cycle the module to initiate self tests.
6. Data output shall be inhibited during self-tests, zeroization, and error states.
7. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. The operator is made aware of self-test errors via the Key Flex Port status output interface.
9. The operator is made aware of the bypass state via the 50 Pin Port status output interface.
10. The module supports exclusive bypass as defined by FIPS 140-2.

This section documents the security rules imposed by the vendor:

1. The user shall not externally load unauthenticated firmware. If this is done it will invalidate the certificate and the module will no longer be able to be used in an environment which requires FIPS 140-2 Approved encryption.

9. Physical Security Policy

Physical Security Mechanisms

The module employs production grade components which meet Level 1 FIPS 140-2 requirements.

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate against other attacks, outside of the scope of FIPS 140-2.

11. References

[1] FIPS PUB 140-2, Security Requirements for Cryptographic Modules / National Institute of Standards and Technology (NIST), May 2001

[2] Telephonics Sweden PR2060F0, User's manual TruLink

12. Definitions and Acronyms

AES – Advanced Encryption Standard

ECB – Electronic Code Book

HMAC – Hash Message Authentication Code

KAT – Known Answer Test

SHA – Secure Hash Algorithm

TEK – Traffic Encryption Key