TruLink Control Logic Module CL6792-M1
Security Policy

Document *Version 2.5*

Telephonics Sweden AB.

Telephonics Sweden AB.Doc no:93857

TABLE OF CONTENTS

1 Module Overview

TruLink Control Logic Module CL6792-M1 (P/N 010.6792-01 Rev. H3 FW Versions Boot: SW7098 v2.5 and Application: SW7099 v9.13.1) (CL6792) is a hardware multi-chip embedded module as defined by FIPS 140-2. The CL6792's cryptographic boundary is defined as the entire CL6792 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 100 channels (0-99). 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.

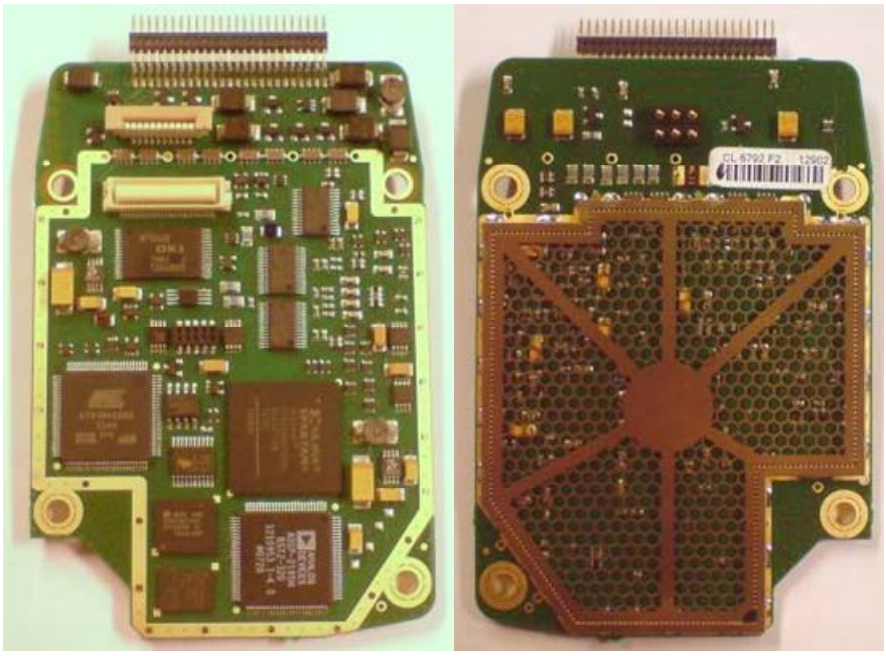

Figure 1 – Image of the Cryptographic Module

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

2 Modes of Operation

FIPS Approved mode of operation

The module only supports a FIPS Approved mode of operation, which is entered at the Telephonics Sweden AB factory. In FIPS mode, the cryptographic module only supports FIPS Approved algorithms as follows:

- AES 128 and 256 ECB for encryption and decryption (Cert. #2113)
- HMAC-SHA-1 for firmware verification (Cert. #1285)
- SHA-1 for use within HMAC (Cert. #1837)

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

3 Ports and Interfaces

The CL6792 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	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 - Data 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

4 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.

Role	Type of Authentication	Description
Crypto-Officer	No Authentication is provided (not required at Level 1).	Administrator of the module, with full access to configurations. This role is assumed when an operator accesses the module using a GPC.
User	No Authentication is provided (not required at Level 1).	The "day-to-day" user of the module, with limited access to services provided by the module. This role is assumed when a human operator holds and uses the physical radio in which this module is installed.
Application User	No Authentication is provided (not required at Level 1).	A user, with access via the application programming interface (API). This role is assumed when an operator accesses the module using a GPC, over the RS-232 interface and in data mode. This gives the user of the external application access to a part of the system configuration and also to the functions granted to the Crypto-Officer.

Table 3 – Roles and Required Identification and Authentication

5 Access Control Policy

Roles and Services

The following table defines the supported roles and services.

Crypto-Officer	User	Application User	Authorized Services	Description
X	X	X	**Unit Configuration**	Module functional configuration service. Provides a very limited part of configurable parameters for the module.
X	X	X	**Data Transmit and Receive**	Transmit or Receive data either encrypted or in plaintext
X	X	X	**Bypass**	Enable or Disable encryption
X	X	X	**Status Output**	Receive Status Output
X	X	X	**Zeroize**	Actively write over all plaintext CSPs.
X		X	**Key Entry and Output**	Manually Enter or Output the Traffic Encryption Key (TEK)
X		X	**Load Firmware**	Load external firmware
		X	**Application Services**	Application specific configuration service (via an API). Provides access to part of the configurable parameters and the behavior for the module. This cannot affect the crypto functionality except for key handling. Full access is limited to Telephonics.

Table 4 – FIPS Approved Mode Services Authorized for Roles

Definition of Critical Security Parameters (CSPs)

The following CSPs are contained within the module:

Key	Description/Usage
Traffic Encryption Key (TEK)	AES 128 or 256 bit key used to encrypt and decrypt user data within the system.
Firmware Authentication Key	64 bit HMAC-SHA-1 key used to authenticate externally loaded firmware.

Table 5 – CSPs

Public Keys

The module does not employ 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	Data Transmit and Receive	Bypass	Status Output	Zeroize	Key Entry and Output	Load Firmware	Application Services
TEK		*E*			*Z*	*RWEZ*		*RWEZ*
Firmware Authentication Key					*Z*		*E*	

Table 6 – CSP Access Rights within Roles & Services

6 Operational Environment

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

7 Security Rules

The cryptographic module's design corresponds to the 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 module does not support concurrent operators.
4. The cryptographic module shall encrypt message traffic using the AES-128 or 256 ECB algorithm.
5. The cryptographic module shall perform the following tests:
    A. Power up Self-Tests:
        1. Cryptographic algorithm tests:
            a. AES ECB Known Answer Test (KAT) (encrypt and decrypt)
            b. HMAC-SHA-1 Known Answer Test (SHA-1 KAT included)
        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 (Boot and Application FW): HMAC-SHA-1
6. At any time an operator can power cycle the module to initiate self tests.
7. Data output shall be inhibited during self-tests, zeroization, and error states.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. The operator is made aware of self-test errors via the Key Flex Port status output interface.
10. The operator is made aware of the bypass state via the 50 Pin Port and Key Flex Port status output interfaces.
11. The module supports exclusive bypass as defined by FIPS 140-2.

This section documents the security rules imposed by the vendor:

1. If a non-FIPS validated firmware version is loaded onto the module, then the module is no longer a FIPS validated module. If this is done, the module will no longer be able to be used in an environment which requires FIPS 140-2 Approved encryption.
2. The Crypto-Officer and Application User shall use the Key Entry and Output service using manual distribution/electronic entry per FIPS 140-2 IG7.7. I.e., the Crypto-Officer or Application User must be directly connected to the module when entering/outputting keys.
3. The Crypto-Officer and Application User shall use a Telephonics provided RNG or another Approved RNG when using the Key Entry service.

8 Physical Security Policy

Physical Security Mechanisms

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

9 Mitigation of Other Attacks Policy

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

10 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

11 Definitions and Acronyms

AES – Advanced Encryption Standard

ECB – Electronic Code Book

GPC – General Purpose Computer

HMAC – Hash Message Authentication Code

KAT – Known Answer Test

SHA – Secure Hash Algorithm

TEK – Traffic Encryption Key