Monaco Enterprises, Inc.

14820 E. Sprague Avenue, P. O. Box 14129, Spokane, Washington 99214-0129
Web Site: www.monaco-inc.com & Email: service@monaco-inc.com
Telephone: (509) 926-6277 Φ FAX: (509) 924-4980

# Monaco Enterprises Inc.

# Monaco Communication Cryptographic Module 1.0
# FIPS 140-2 SECURITY POLICY

H.W. Part Number: 314R0006
F.W. Version: 51.01

Document Revision: 1.1
Document Date: March 30, 2022

Non-proprietary Security Policy

## REVISION HISTORY

| Author(s) | Version | Updates |
|---|---|---|
| Don Skinfill | 1.0 | Initial release |
| John Webster | 1.1 | Minor clarifications |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# Contents

# 1 Introduction

The Monaco Enterprises Inc. Monaco Communication Cryptographic Module 1.0 (H.W. Part Number: 314R0006, F.W. Version: 51.01) is a single chip cryptographic module designed to provide FIPS 140-2 AES-256 encryption for secure RF radio communications. The Overall security level of the Monaco Communication Cryptographic Module 1.0 is Level 1.

# 2 Security Level Specification

| SECURITY REQUIREMENTS AREA | LEVEL |
|---|---|
| Cryptographic Module Specification | 1 |
| Cryptographic Module 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-tests | 1 |
| Design Assurance | 1 |
| Mitigation of Other Attacks | N/A |

*Table 1* **– Security Level of Security Requirements.**

# 3 Module Overview

## 3.1 Cryptographic Boundary

The following diagram defines the cryptographic boundary:

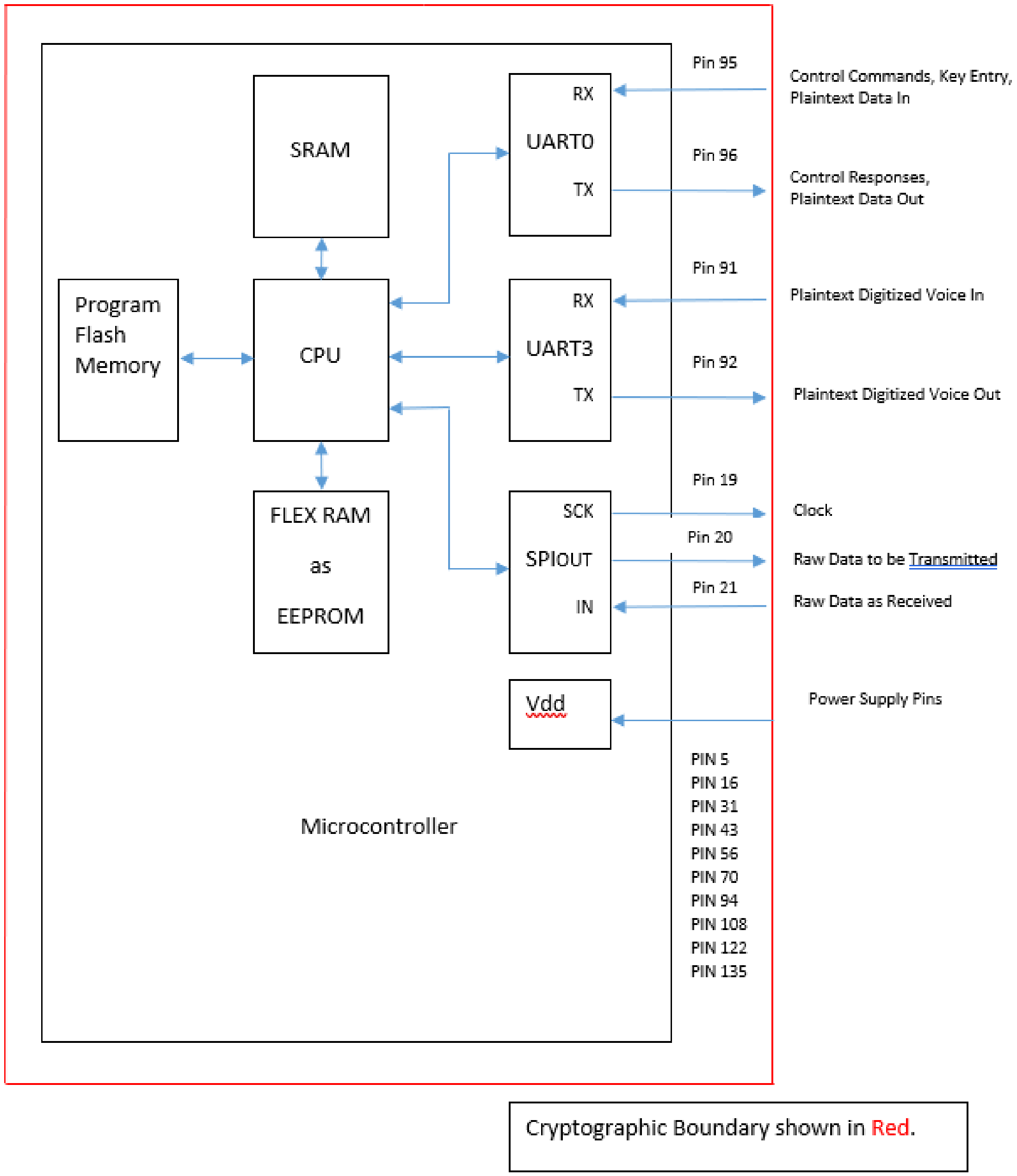

*Figure 1* **– Specification of Cryptographic Boundary**

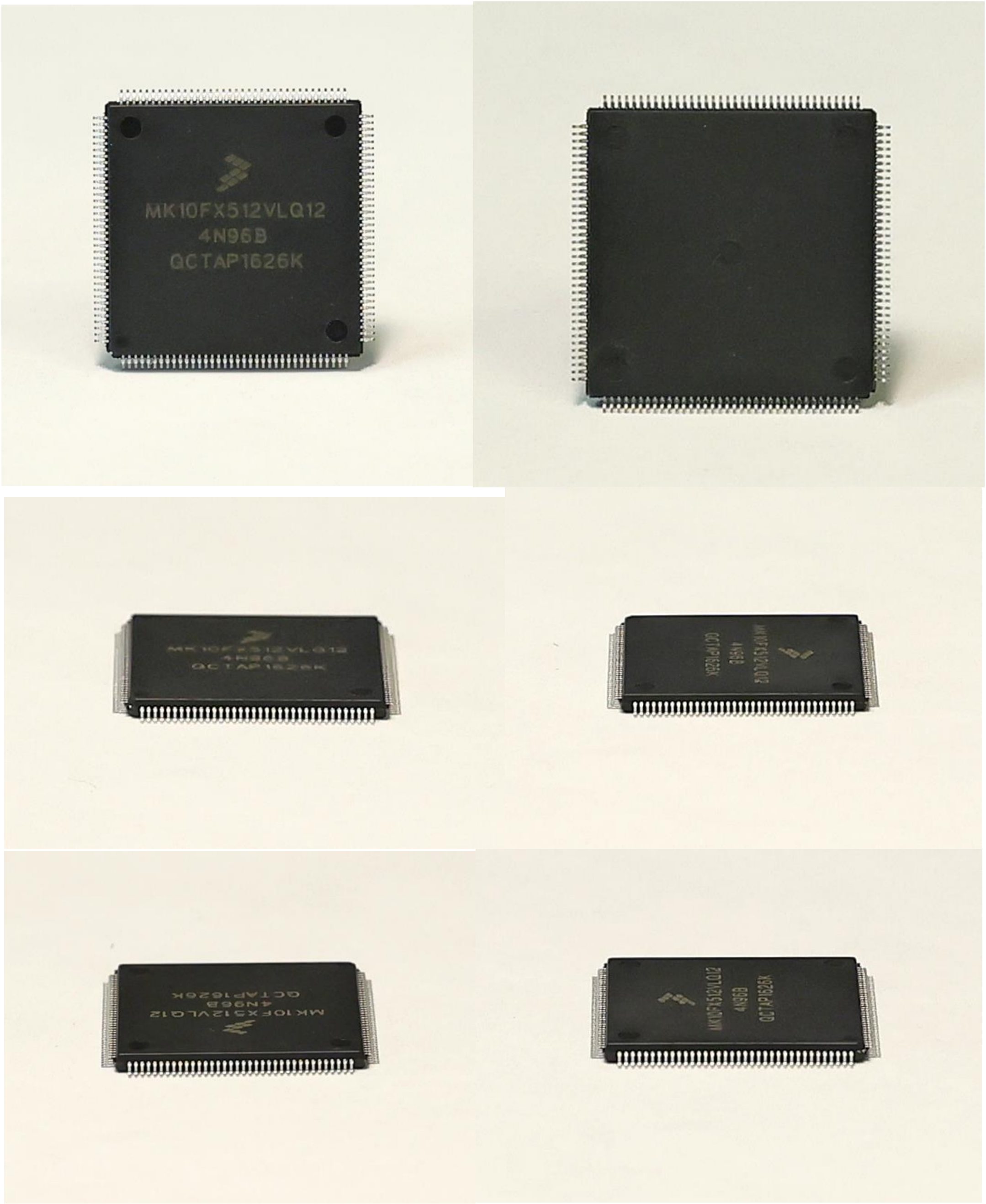

*Figure 2* **– The Monaco Communication Cryptographic Module 1.0**

## 3.2 Physical Ports and Logical Interfaces

The Cryptographic Module provides the following physical ports and interfaces.

| Physical Port | Logical Interface |
|---|---|
| UART3<br>SPI port<br>UART0 | Data Input |
| UART0 | Control Input |
| UART3<br>SPI port<br>UART0 | Data Output |
| UART0<br>Dedicated I/O pin for indicators | Status Output |
| Vdd | Power Input |

***Table 2 –*** Specification of Cryptographic Module Physical Ports and Logical Interfaces

All of the three ports are bidirectional i.e. the port can be used for both an input and output, however, the inputs and outputs are on separate physical lines. The firmware inside the cryptographic module is built around a state machine such that there are no states where confusion can exist between input data and control input information or between the data output and the status output signals.

In addition, control input signal and status output signals are formatted in such a way both in timing and in content to make them unique from general data input and output. This process also prevents key entry from interfering with general input digital data stream input which shares the same port.

The other two ports, the SPI port and UART3 are physically separate from the port, UART0, that handles digital data and input and output commands for control and status. The nature of the port control within the processor is such that the three ports may be operated simultaneously without interfering with each other or corrupting each other information stream.

# 4 Modes of Operation

## 4.1 Approved Mode of Operation

The module has only one mode of operation which is the Approved Mode. The module will remain operating in the Approved Mode if all the power-up self-tests and conditional self-tests pass.

## 4.2 Security Rules

The following specifies the security rules under which the cryptographic module shall operate:

- ❖ The module is initialized automatically the first time that it is powered up after having the firmware loaded.

- ❖ The module is embedded in another piece of equipment with no physical user access without disassembling. The module cannot be accessed before initialization and no other access points other than what is explicitly described in this document is provided.
- ❖ Maintenance (N/A): The module does not support a maintenance role.
  - There are no maintenance capabilities related to encryption or security, only normal radio operation and adjustments.

- ❖ Key Programming Rules (Key Entry) - When entering keys into the module the operator shall follow these rules:
  1- Key programming shall only be performed on the MCU Pin #95 interface,
  2- Configure MCU PIN #83 to High, and
  3- Configure MCU PIN #82 to non-active.

- ❖ Key rotation: The Crypto officer must perform KEY ROTATION once a year.
- ❖ The module will  always decrypt a received message if it has the active key for the received message and is not in an error state.
- ❖ The module will run the self-tests automatically upon power up (See section 7).
- ❖ If the module encounters an error the module will remain in that error state until an error recovery is performed.
- ❖ The Crypto-officer is responsible for
  - Maintaining module's operation
  - Managing the Keys
  - Firmware loading
- ❖ Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation
- ❖ To recover the module the Crypto-officer shall first power-cycle the module to rerun the self-test and observe that the self-tests have passed.

The following describes the status output indication when operating normally and when encountering a Self-test Error:

| Self-test | Status output | Module Status |
|---|---|---|
| No failure | Pin 66: N/A<br>Pin 67: N/A | The module operating normally |
| Bootloader CRC-32,<br>App CRC-32,<br>CMAC KAT,<br>or<br>CMAC Key CRC-32*: Fail | Pin 66 high<br>Pin 67 toggles every 24ms | The module is inoperable |
| App CRC-32: Pass<br>CMAC self-test: Pass<br>AES-KATs: Fail | Pin 66 toggles every 88ms<br>Pin 67 high | Pin 66 will toggle until the error is cleared (power-cycling the module) |
| Any failed conditional self-test | Pin 66 high<br>Pin 67 toggles every 1.4s | Pin 67 will toggle until the error is cleared (power-cycling the module) |

***Table 3* –** Power-up self-test Failures

Pin output Legend: High = 3.3V, Low = ground (0V), Toggle = transition from low to high or high to low

Note*: A Zeroized CMAC key will also cause a power-up self-test failure and the module will become inoperable.

## 4.3 Cryptographic Algorithms

### Approved Algorithms

The following is a list of the Approved Algorithms:

| ACVTS Cert | Algorithm | Standard | Mode/Method | Key Lengths, Curves, Or Moduli | Use |
|---|---|---|---|---|---|
| A1230 | AES<br>ECB<br>OFB | FIPS 197<br>SP 800-38A | Encrypt<br>Decrypt | 256 | Encryption<br>Decryption |
| A1230 | AES-CMAC | SP800-38B | Verify | 256 | Firmware Integrity |

***Table 4*** **–** Table of Approved Algorithms

# 5 Cryptographic Key Management

## 5.1 List of Keys and CSPs

| Description /Usage | Type | Generation/ Establishment | Input/Output | Storage Persistent (NVM)/ Working Memory (RAM) | Zeroization |
|---|---|---|---|---|---|
| Short data keys (12-bytes or less) | AES-256 ECB | | Input: Plaintext, Manual distribution, electronic entry<br>Output: N/A | persistent, working memory | Zeroize Service: actively overwriting memory |
| Long data keys | AES-256 OFB | | Input: Plaintext, Manual distribution, electronic entry<br>Output: N/A | persistent, working memory | Zeroize Service: actively overwriting memory |
| Voice keys | AES-256 OFB | | Input: Plaintext, Manual distribution, electronic entry<br>Output: N/A | persistent, working memory | Zeroize Service: actively overwriting memory |
| Key CRC | CRC-32 | | Input: Plaintext, Manual distribution, electronic entry<br>Output: N/A | persistent, working memory | Zeroize Service: actively overwriting memory |
| Firmware Upgrade Key | AES-CMAC-256 | | Input: N/A<br>Output: N/A | persistent, working memory | Zeroize Service: actively overwriting memory |

*Table 5* – **Cryptographic Keys and CSPs Management Table**

# 6 Roles, Services and Access Control Policy

## 6.1 Roles

The module has two roles that are implicitly assumed by the operator. The module does not support concurrent operators.

The Crypto-Officer Role: is the operator that manages the Encryption Keys and can also perform all of the functions and responsibilities of a User. The CO is responsible for generating and safeguarding the encryption keys.

The User Role: is an operator who manages the configuration of the radios. This includes injecting the Keys, managing the status of the encryption keys and configuring the non-security relevant radio parameters.

## 6.2 Services and Access Control

| Service | Description | Role(s)* | Access Type(s) of Keys and CSPs** |
|---|---|---|---|
| Data Encryption | This service encrypts outgoing data such as short data, long data, and voice data. | CO, U | Short data keys (E)<br>Long data keys (E)<br>Voice keys (E) |
| Data Decryption | This service decrypts incoming data such as short data, long data, and voice data. | CO, U | Short data keys (E)<br>Long data keys (E)<br>Voice keys (E) |
| Keying/unkeying the transmitter | This service toggles on/off the transmitter | CO, U | Short data keys (R)<br>Long data keys (R)<br>Voice keys (R) |
| Change Channel Key number<br>(Bypass Toggle) | The radio four communication channels that can be configured for use. Only one channel is active at a time. Each channel can be configured for encrypted communication or non-encrypted communication (bypassed). If encrypted, a key from a table of 64 possible keys needs to be | CO, U | Short data keys (R)<br>Long data keys (R)<br>Voice keys (R) |

| | | | |
|---|---|---|---|
| | configured to use for encryption. This command allows the current key number (not key value) that is use on a channel to be changed. | | |
| Change Channel (Bypass Toggle) | This service will change the current channel. The new channel could be another encrypted channel or a non-encrypted channel (bypass) | CO, U | Short data keys (R)<br>Long data keys (R)<br>Voice keys (R) |
| Key Programming | This service allows the CO to change the 256-bit key value for any of the 64 keys in the key table | CO | Short data keys (W)<br>Long data keys (W)<br>Voice data keys (W)<br>Key CRC (W) |
| Activate/Deactivate Key | A non-zeroized key can be marked as Active or Inactive. | CO, U | N/A |
| Self-test | Preforms the power-up self-tests (via power cycling) | CO, U | N/A |
| Show Status | Shows the status of the module | CO, U | N/A |
| Test Tone | This service keys up the radio with a modulated 1031Hz test tone if on a digital channel | CO, U | Voice keys (E) |
| Zeroize | This service can zeroize a specific set of keys (Short key, Long key, and Voice Key for a key number), or all existing keys and CSPs in the module. | CO, U | Short data keys (Z)<br>Long data keys (Z)<br>Voice keys (Z)<br>Key CRC (Z)<br>Firmware Upgrade Key (Z) |
| Firmware Upgrade | This service allows loading new firmware to the module. | CO | Firmware Upgrade Key (R, E) |
| Field Use<br>(Non-FIPS related) | This service allows the operator to perform non-security relative operations in the field such as radio configuration. | CO, U | N/A |

***Table 6*** – Services Authorized for Roles, Access Rights within Services

Note*: CO = Crypto-Officer, U = User
Note**: R=read, W=write, E=execute, Z=zeroize

## 6.3 Bypass capability

The module has four communication channels that can be configured for use.  Only one channel is active at a time.  Each channel can be configured for encrypted communication or non-encrypted communication (bypassed).

The module can be configured to operate from normal operation to bypass mode and vice versa using the following two services:

**1-  Change Channel Key number:**

Normal operation to Bypass mode configuration:

The operator must use the “Change Chanel Key number” service and remove the assigned key. The module will request confirmation from the user before executing the command.

Bypass mode to Normal operation configuration:

The operator must use the “Change Channel Key number” service and set a key to be used for this channel.

**2-  Change Channel:**

Normal operation to Bypass mode configuration:

The operator must use the “Change Chanel” service and switch to a non-encrypted channel . The module will request confirmation from the user before executing the command.

Bypass mode to Normal operation configuration:

The operator must use the “Change Channel” service and switch to an encrypted channel.

When switching to non-bypass mode the module will perform the alternating bypass mode self-test which will verify the Keys CRCs and run the AES Known Answer Tests listed in section 7.

The operator can use the status command to check if a given channel is in bypass mode or not. If the module is in bypass mode it will return “Using software channel # bypass mode”.

# 7 Self-Tests

## Power-up self-tests

| ALGORITHM | Test Description |
|---|---|
| AES-ECB-256 | Encrypt ECB KAT |
| AES-ECB-256 | Decrypt ECB KAT |
| AES-OFB-256 | Encrypt OFB KAT |
| AES-CMAC-256 | Verify KAT |
| CRC-32 | Bootloader Firmware integrity test |
| CRC-32 | App Firmware integrity test |

***Table 7* - Power-up Self-test Table**

## Conditional Self-tests

| Self-Test | Test Description |
|---|---|
| Manual key Entry Test | CRC-32 |
| Firmware Load Test | AES-CMAC-256 |
| Alternating Bypass Test | CRC-32 with AES-OFB KAT and AES-ECB KATs |

***Table 8* - Conditional Self-test Table**

# 8 Identification and Authentication Policy

The Module does not implement Authentication of the operator roles.

| Role | Authentication Type | Authentication Data |
|---|---|---|
| Cryptographic Officer | N/A | N/A |
| User | N/A | N/A |

***Table 9*** - Roles and Required Identification and Authentication

| Authentication Mechanism | Strength of Mechanism |
|---|---|
| N/A | N/A |
| N/A | N/A |

Table **10 - *Strengths of Authentication Mechanisms***

# 9 Physical Security Policy

The module is a single chip cryptographic module which meets the Security Level 1 production-grade components requirement.

| Physical Security Mechanisms | Recommended Frequency of Inspection/Test | Inspection/Test Guidance Details |
|---|---|---|
| N/A | N/A | N/A |

***Table*** 11- Inspection/Testing of Physical Security Mechanisms

## 10 Operational Environment

The module runs in a limited operational environment.

## 11 EMI/EMC

The module is part of a device that meets 47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).

## 12 Mitigation of Other Attacks

The module provides no additional mitigation of other attacks.

| Other Attacks | Mitigation Mechanism | Specific Limitations |
|---|---|---|
| N/A | N/A | N/A |

*Table 12* **– Table of Mitigation of Other Attacks**

## 13 Acronyms

| TERM | DESCRIPTION |
|---|---|
| **ACVP** | Automated Cryptographic Validation Program |
| **AES** | Advanced Encryption Standard, as specified in [FIPS 197] |
| **CAVP** | Cryptographic Algorithm Validation Program |
| **CBC** | Cipher Block Chaining |
| **CCCS** | Canadian Centre for Cyber Security |
| **CERT** | Certificate |
| **CMVP** | Cryptographic Module Validation Program |
| **CO** | Crypto Officer |
| **CST** | Cryptographic and Security Testing |
| **FIPS** | Federal Information Processing Standard |
| **FISMA** | Federal Information Security Management Act |
| **FSM** | Finite State Model |
| **IG** | Implementation Guidance |
| **NIST** | National Institute of Standards and Technology |
| **NVLAP** | National Voluntary Laboratory Accreditation Program |
| **OFB** | Output Feedback |
| **PUB** | Publication |

*Table 13* – **Specification of Acronyms and their Descriptions**