# FIPS 140-2 Security Policy

## P7170$^{IP}$ System Portable Two-Way FM Radio

---

M/A Com, Inc.
221 Jefferson Ridge Parkway
Lynchburg, VA 24501

May 15, 2006

Revision Version 1.6

# 1. Introduction

The following describes the security policy for the multi-chip standalone module, the P7170$^{IP}$ System Portable Two-Way FM Radio (P7170$^{IP}$). This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

The P7100$^{IP}$ series portable radios are rugged, high-quality, high-performance two-way FM communication units. The P7100$^{IP}$ series portables are available in either Scan (P7150$^{IP}$) or System (P7170$^{IP}$) versions with or without the immersion option HTMR. These are M/A COM's most sophisticated, high specification portable radios. The P7100$^{IP}$ designs use custom integrated circuits to set new standards for size and weight in high power, feature-enriched two-way radios. The P7100$^{IP}$ series radios are Phase-Locked-Loop synthesized radios that can be programmed to operate on both EDACS® trunked or conventional communications systems.

Features include:

- **Lightweight, Rugged Construction**

  Features a molded front case made of a polycarbonate. This construction provides a lightweight yet durable housing designed to withstand years of rugged use.

- **High System/Group Capacity**

  The P7100$^{IP}$ series radios can manage up to 16 different EDACS system/group combinations (greater than 128 systems/groups with premium feature set) with up to 200 conventional channels. EDACS systems/groups can be configured in many different ways to meet specific user needs.

- **Dual Mode Capability**

  Conventional operation is obtained by simply selecting a pre-programmed conventional system.

- **Project 25 (P25) Interoperability**

  The P7100$^{IP}$ portable is P25 compliant and is ideal for use either as a primary P25 digital conventional portable or as a trunked portable with P25 Common Air Interface (CAI) for digital talkaround interoperability. The radio provides digital interoperability with other P25 users during critical communications situations.

- **Display**

  System and group information, status icons and menu operation is supported by the 3-line, 12-character, alphanumeric backlit Liquid Crystal Display (LCD).

- **Top-Mounted Rotary Knobs**

The rugged rotary knobs are designed for ease of operation by allowing tactile access to groups, systems, conventional channels, as well as volume and power control.

- **Keypad**

  The backlit keypad allows the user to access the many radio functions. The keypad provides easy access to preprogrammed telephone and individual radio IDs. A detailed description of the keypad and additional functions is found in the OPERATION section.

- **Emergency ID and Alarm**

  The user can alert the dispatcher to an emergency by pressing a recessed red button located on the top of the radio, which sends the user ID and an emergency signal.

- **Universal Device Connector (UDC)**

  The UDC provides the PC programmer and optional accessories access to the radio for ease and versatility of radio functionality.

- **Variable Power Control**

  Variable power control is PC programmable and keypad selectable for 1 or 3 watts.

- **Weatherproof**

  Radios operate reliably under adverse conditions. These portable radios meet military standards MIL-STD-810F specifications for high and low, operating and storage temperatures; low pressure extremes: thermal shock; solar radiation; driven rain; humidity; salt fog; blowing dust; shock and vibration. As mentioned, the P7100$^{IP}$ series models can also be purchased with a water immersion option HTMR.

- **Vibration**

  Meets TIA/EIA-603, U.S. Forest Service (USDA LMR Standard, Section 2.15), and MIL-STD-810F environmental and vibration-stability requirements.

- **Personality Programming**

  Can easily interface with a personal computer in the field, to allow system and radio parameters to be flexibly programmed as requirements change, without changing parts or opening the radio case.

## 1.1. Purpose

This document treats to cover the secure operation of the radio including the initialization, roles, and responsibilities of operating the product in a secure, FIPS 140-2 compliant manner.

## 1.2. Validated Configurations

All validated hardware configurations run the following firmware: H8 Version J2R06B03 and DSP Version F7R01A16.

The hardware versions tested and validated are as follows:

- RU101219V22 – 136-174MHz, Portable 7170 System Model
- RU101219V42 – 450-512MHz, Portable 7170 System Model
- RU101219V52 – 378-430MHz, Portable 7170 System Model (100mW)
- RU101219V62 – 378-430MHz, Portable 7170 System Model
- RU101219V72 – 806-870MHZ, Portable 7170 System Model

The following table identifies all of the validated hardware part numbers for the P7170$^{IP}$ System Portable Two-Way FM Radios.

| Validated Hardware Version Numbers | Validated Hardware Part Numbers | Description |
|---|---|---|
| RU101219V22 | HT7170TH1X | P7170 System, 136-174MHz– Unencrypted |
| | HT7170TH1E | P7170 System, 136-174MHz – DES Algorithm |
| | HT7170TH1A | P7170 System, 136-174MHz – AES Algorithm |
| RU101219V42 | HT7170TU1X | P7170 System, 450-512MHz – Unencrypted |
| | HT7170TU1E | P7170 System, 450-512MHz – DES Algorithm |
| | HT7170TU1A | P7170 System, 450-512MHz – AES Algorithm |
| RU101219V52 | HT7170YN1X | P7170 System (100 mW), 378-430MHz– Unencrypted |
| | HT7170YN1E | P7170 System (100 mW), 378-430MHz – DES Algorithm |
| | HT7170YN1A | P7170 System (100 mW), 378-430MHz – AES Algorithm |
| RU101219V62 | HT7170TN1X | P7170 System, 378-430MHz– Unencrypted |
| | HT7170TN1E | P7170 System, 378-430MHz – DES Algorithm |

| | | |
|---|---|---|
| | HT7170TN1A | P7170 System, 378-430MHz – AES Algorithm |
| RU101219V72 | HT7170T81X | P7170 System, 806-870MHz – Unencrypted |
| | HT7170T81E | P7170 System, 806-870MHz – DES Algorithm |
| | HT7170T81A | P7170 System, 806-870MHz – AES Algorithm |

# 2. Roles, Services, and Authentication

The radio supports two roles: Crypto-Officer and User. By design, both roles have access to all services provided by the module. A single PIN is used to gain access to services for both roles.

## *2.1. Roles*

The roles of the module include a Crypto-officer (CO) and User Role. All the services of the module require the assumption of an authorized role (i.e., either the CO or User role).

### *Crypto-Officer Role*

The Crypto-Officer is an operator who has access to all of the radios management tasks as well as all User services identified below. The CO services include:

- Putting the module into the FIPS mode
- Loading cryptographic keys and radio personality configuration
- Upgrading radio firmware
- Downloading H8 and DSP firmware, the personality file, Tracking Data and Feature Encryption Data from radio
- Using Direct Frequency Entry feature (see the section 6.5.5 of the Maintenance Manual)
- Loading Tracking Data and Feature Encryption Data

### *User Role*

The User is an operator who is not allowed to perform management tasks such as loading new firmware and loading keys. The following services are assigned to the User role.

- Turning the module on and initiating power-up self-tests
- Authenticating / changing PIN
- Sending/receiving encryption calls
- Sending/receiving plaintext calls
- Activating bypass mode
- Changing the current system and group
- Browsing through menus to view radio status information
- Zeroize encryption keys

## 2.2. Authentication Mechanisms and Strength

There are two kinds of authentication mechanisms in the module. The Crypto-Officer and the User authentication are done by entering a valid PIN, which is the first mechanism. Therefore, the CO and User authentication is role-based. When loading the DSP code, the module performs a DES-MAC based authentication on it and this is the second authentication mechanism. Only the CO is allowed to perform key management. Therefore, the DES-MAC based authentication is associated with the CO role.

### *PIN Authentication*

The Crypto-Officer and the User authenticate to the module using a valid 6-digit PIN. The CO must make sure that the PIN is at least six digits long. The false acceptance rate of one attempt in this PIN authentication is $1/10^6$. The false acceptance rate for multiple attempts is less than $1/10^5$ in a minute.

### *DES-MAC Authentication*

The DSP file that is loaded to the module contains an embedded DES-MAC. When loading the DSP file, the module calculates a DES-MAC of the file using the DES-MAC key stored in the module and compares it with the DES-MAC embedded in the file. If the comparison succeeds, the module resumes normal operation. If the comparison fails, the module continuously resets and does not resume normal operation.

The DES-MAC key, which is the authentication data in this case, is 64 bits long. Therefore, the false acceptance rate of one attempt is 1/18446744073709551616, which is much less than $1/10^6$. To make the false acceptance rate of multiple attempts to be equal to $1/10^5$ in one minute, one needs to load DSP files 184467440737095 times in one minute. Given the physical constraints, this many attempts in one minute are impossible (in fact, much less than this). Therefore, the false acceptance rate for multiple attempts is less than $1/10^5$ in a minute for this authentication.

# 3. Secure Operation and Security Rules

In order to operate the P7170$^{IP}$ System Portable Two-Way FM Radio securely, the operator should be aware of the security rules enforced by the module and should adhere to the physical security rules and secure operation rules required.

## *3.1. Security Rules*

The security rules enforced by the radio include both the security rules that the M/A Com has imposed and the security rules that result from the security requirements of FIPS 140-2.

### *M/A Com Security Rules*

The following security rules are imposed by M/A Com:

1. A signed DSP code (i.e., a DSP code that has a DES-MAC embedded) should be loaded to the module
2. A DES-MAC key and a KEK should be loaded to the module
3. All the keys and the PIN should be loaded to the module in encrypted form

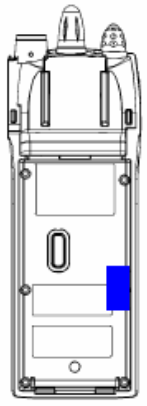
### *FIPS 140-2 Security Rules*

The following are security rules that stem from the requirements of FIPS PUB 140-2.

1. Enable FIPS mode
2. Only FIPS approved cryptographic algorithms to be used (this is automatically done by the module once the FIPS mode is enabled)
3. PIN should be at least 6-digits in length
4. The menu item "ZERO DES" or "ZERO AES" should be configured on the personality file.

## *3.2. Physical Security Rules*

The radio is physically protected by applying a tamper evident label as shown in the following figure. The tamper evident label is shown in blue.



The following steps shall be taken to apply the serialized tamper-evident label.

- Turn off the radio and remove the battery.
- Clean the surface surrounding the screw on which the tamper evident label will be applied (see the above figure). Alcohol-based cleaning pads can be used for the cleaning.
- Apply the tamper evident label covering the screw beneath it as shown in the above figure
- Record the serial number of the applied label in a security log
- Allow 24 hours for the adhesive in the tamper-evident seals to completely cure. The battery should be replaced only after this time period has been elapsed.

The CO is required to periodically inspect the tamper-evident label to ensure that it is not damaged.

## 3.3. Secure Operation Initialization Rules

The radio provides the following algorithms:

| Algorithm Type | Modes/Mod sizes | FIPS-approved |
|---|---|---|
| Symmetric Algorithms | | |
| DES (transitional phase only - valid until May 19, 2007) | 64-bit, OFB | Yes, DES (Cert. #241) |
| AES | 256-bit, OFB | Yes, AES (Cert. #155) |
| VGE (M/A Com proprietary digital voice encryption algorithm) | | No |
| Message Authentication Code | | |
| DES-MAC (transitional phase only - valid until May 19, 2007) | | Yes, DES MAC (Cert. #241, vendor affirmed) |

Because FIPS 140-2 prohibits the use of non-FIPS approved algorithms while operating in a FIPS compliant manner, the Crypto-Officer should follow the following rules to initialize a new radio to ensure FIPS level 2.

(1) Apply the tamper evident label as described in the section 2.4

(2) Enable FIPS mode on the radio in the following manner

(a) Make sure that the radio is turned off.

(b) Set up the radio in the configuration shown on Figure 8-2 of the Maintenance Manual.

(c) Make sure to define a PIN (equal to or greater than 6-digits in length), a DES-MAC key and a KEK on the master key file (The master key file is the file containing all the keys, PIN and the EnableFips parameter before encrypting keys and the PIN). Make sure to set the EnableFips parameter to 'true' on the master key file to enable FIPS mode.

(d) Generate a DES-MAC of the DSP code using the DES-MAC key and embed it in the DSP code. Generate the distribution key file based on the master key file. Use the Keyadminconsole program to do these tasks.

(e) Start the radio in the programming mode by pressing Option, Clear/Monitor and PTT buttons simultaneously and by powering on the module.

(f) Using the ProGrammer (this program runs on a PC as well; please refer to the section 8.5 of the Maintenance Manual and the Help menu on the ProGrammer for details on using it) read the personality from the radio. A window should pop up showing the personality settings of the radio. Under the Options tab, go to Programmable Menus. On the window popped up, under Conventional Menus, select "ZERO DES" or "ZERO AES" as one of the menu items. Once this new personality is loaded to the radio, it gives a menu item called "ZERO DES" or "ZERO AES" to zeroize all the keys and CSPs of the DSP EEPROM.

(g) Load the DSP code and the above personality to the module using the ProGrammer.

(h) Load the keys in the distribution key file to the module using the Keyloaderconsole program. This program runs on a PC.

(i) Power off and on the module; now the module should be in the FIPS (Approved) mode.

When initialized in this fashion, the radio will only use FIPS-approved algorithms.

# 4. Definition of SRDIs Modes of Access

This section specifies the radio's Security Relevant Data Items as well as the access control policy enforced by the radio.

## *4.1. Cryptographic Keys, CSPs, and SRDIs*

While operating in the level 2 FIPS-compliant manner, the radio contains the following security relevant data items:

| Security Relevant Data Item | SRDI Description |
|---|---|
| TEK (Traffic Encryption Keys) | These keys are used in the encryption and decryption of voice and data calls. The encryption algorithm used is DES or AES. The key sizes are 64 bits or 256-bits respectively, and the keys are stored in the DSP EEPROM in plaintext. |
| KEK | When the key loading is performed, this key decrypts the encrypted TEKs and the PIN that are being loaded. If a new KEK is loaded (which is encrypted using DES), this key is also used to decrypt the new KEK. The encryption algorithms used is DES. The key size is 64 bits and it is stored in the DSP EEPROM in plaintext. |
| DES-MAC key | At power-up or after firmware loading, the module calculates a DES-MAC of the DSP firmware using this key and compares it with the DES-MAC embedded in the DSP firmware. If a new DES-MAC key is loaded (which is encrypted using DES), this key is also used to decrypt the new DES-MAC key. The key size is 64 bits and it is stored in the DSP EEPROM in plaintext. |
| Copy of DES-MAC key | This is a copy of the DES-MAC key mentioned in the above row. When the module performs power-up self-tests, this key is compared with the DES-MAC key of the above row. The key size is 64 bits and it is stored in the DSP EEPROM in plaintext. |
| PIN | This is the PIN that is used for CO and User authentication. The PIN is exactly 6-digits. It is stored in the DSP EEPROM in plaintext. |
| Seed of the RNG | This is the random number last generated by the non-Approved RNG before powering off the module. After powering on, the first iteration of the RNG uses this seed. The size is 64 bits and it is stored in the DSP EEPROM in plaintext. |
| Feature Encryption Data | This data defines various features (including if the FIPS is enabled and if the DES or AES algorithm is used) enabled on the radio. This data is stored in the Flash and the H8 EEPROM in encrypted form. However, the encryption algorithm is not FIPS approved. Therefore, according to FIPS, this data is considered plaintext. The size of the data is 128 bits. |
| Instance of Feature Encryption Data | An instance of the Feature Encryption Data mentioned above is stored in the SRAM (after decryption) at power up in plaintext. The M/A Com proprietary encryption algorithm is used for this decryption. |
| P25 Key Instance | An instance of the TEK keys that belongs to the P25 system is |

| | |
|---|---|
| | stored in the SRAM at power up in plaintext. The size of a key is 64 bits. |

## 4.2 Access Control Policy

The radio allows controlled access to the SRDIs contained within it. The following table defines the access that an operator or application has to each SRDI while operating the radio in a given role performing a specific service. The permissions are categorized as a set of three separate permissions: read, write, delete. If no permission is listed, then an operator has no access to the SRDI.

| P7170$^{IP}$ System Portable Two-Way FM Radio<br><br>SRDI/Role/Service Access Policy | Security Relevant Data Item | TEK | KEK | DES-MAC key | Copy of DES-MAC key | PIN | Seed of the RNG | Feature Encryption Data (FED) | Instance of FED | P25 Key Instance |
|---|---|---|---|---|---|---|---|---|---|---|
| Role/Service | | | | | | | | | | |
| Crypto-Officer Role | | | | | | | | | | |
| Placing module in FIPS mode | | w | w | w | w | w | | | | |
| Loading keys and radio personality configuration | | w | w | w | w | w | | | | |
| Upgrading radio firmware | | r | r | r | r | r | | r | w | w |
| Downloading H8 and DSP firmware, the personality file, Tracking Data and Feature Encryption Data from radio | | | | | | | | r | | |
| Using Direct Frequency Entry feature | | | | | | | | | r | |
| Loading Tracking Data and Feature Encryption Data | | r | r | r | r | r | | r | w | w |
| User role | | | | | | | | | | |
| Turning the module on and initiate power-up self-tests | | r | r | r | r | r | | r | r | r |
| Authenticating/modifying PIN | | | | | | r/w | | | | |
| Sending/receiving encrypted calls | | r | r | | | | r | r | r | r |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Sending/receiving plaintext calls | | r | r | | | | r | r | r | r |
| Activating bypass mode | | | | | | | | | | |
| Changing the current system and group | | | | | | | | r | | |
| Browsing through menus to view status information | | | | | | | | r | | |
| Zeroize encryption keys | | w | w | w | w | w | w | | | w |

# 5. Glossary

| Term/Acronym | Description |
|---|---|
| CO | Cryptographic-officer or Crypto-officer |
| EDACS | Enhanced Digital Access Communications System |
| KEK | Key Encryption Key |
| MDT | Mobile Data Terminal |
| PC | Personal Computer |
| PTT | Push-to-talk |
| RF | Radio Frequency |
| SRDI | Security Relevant Data Items |
| TEK | Traffic Encryption Key |