

FIPS 140-2 Security Policy

P7130^{IP} Select, P7150^{IP} Scan Portable, and M7100^{IP} Mobile
Two-Way FM Radio

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

July 12, 2006

Revision Version 1.7



1.	Introduction.....	3
1.1.	P7130 ^{IP} Select and P7150 ^{IP} Scan.....	3
1.2.	M7100 ^{IP} System and Scan Radio.....	5
1.3.	Purpose.....	5
1.4.	Validated Configurations.....	6
2.	Roles, Services, and Authentication.....	9
3.	Secure Operation and Security Rules.....	10
3.1.	Security Rules.....	10
3.2.	Physical Security Rules.....	10
3.3.	Secure Operation Initialization Rules.....	11
4.	Definition of SRDIs Modes of Access.....	13
4.1.	Cryptographic Keys, CSPs, and SRDIs.....	13
4.2.	Access Control Policy.....	14
5.	Glossary.....	16

1. Introduction

The following describes the security policy for the multi-chip standalone module, the P7150^{IP} Scan Portable and M7100^{IP} Mobile Two-Way FM Radios. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

1.1. P7130^{IP} Select and P7150^{IP} Scan

The P7100IP series portable radios are rugged, high-quality, high-performance two-way FM communication units. The P7100^{IP} series portables are available in either Select (P7130^{IP}), 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 P7100IP 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.

Note – The Select radio does not include a backlit keypad.

- **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.

1.2. M7100^{IP} System and Scan Radio

The M7100^{IP} mobile is a digital two-way radio that operates on Project 25 conventional and trunked modes, as well as the Enhanced Digital Access Communications System (EDACS) and ProVoice digital trunked communications systems. The M7100^{IP} is also ideal for analog conventional communications systems. This rugged mobile was designed to work in rigorous environmental conditions and meets MIL-STD-810F, U.S. Forest Service vibration, and TIA/EIA-603 shock and vibration requirements. This leading edge mobile complement the P7100^{IP} portable family of radios designed to excel in the challenging public safety environment.

Features include:

- The standard M7100^{IP} incorporates the critical communications features Emergency and Dynamic Regroup to deliver advanced performance.
- Trunked systems/groups may be configured for up to 800 different combinations and up to 255 conventional channels.
- The Extended Network feature package upgrades capacity to 800 system/group combinations and includes ProScan. and ProFile.. Individual software options may also be added to meet user requirements.
- ProFile offers easy over-the-air programming for efficient updates of radios.
- ProScan provides the user smooth, automatic roaming between sites.
- The M7100^{IP} includes the full conventional feature set with dual priority scan and various tone signaling formats.

1.3. 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.

1.4. 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:

- RU101188V1 – 136-174MHz, Mobile 7100^{IP}
- RU101188V21 – 136-174MHz, Mobile 7100^{IP} (50 W)
- RU101188V12 – 378-430MHz, Mobile 7100^{IP}
- RU101188V22 – 450-512MHz, Mobile 7100^{IP}
- RU101188V31 – 806-870MHZ, Mobile 7100^{IP}
- KRY1011632/13 – System control head
- KRY1011632/11 – Scan control head
- RU101219V21 – 136-174MHz, Portable 7150 Scan Model
- RU101219V51 – 378-430MHz (100 mW), Portable 7150 Scan Model
- RU101219V61 – 378-430MHz, Portable 7150 Scan Model
- RU101219V63 – 378-430MHz, Portable 7130 Select Model
- RU101219V41 – 450-512MHz, Portable 7150 Scan Model
- RU101219V71 – 806-870MHZ, Portable 7150 Scan Model
- RU101219V73 – 806-870MHZ, Portable 7130 Select Model

The following table identifies all of the validated hardware part numbers for the M7100^{IP} radios.

Validated Hardware Version Numbers	Validated Hardware Part Numbers	Description
RU101188V1	MAHG-SHHXX	M7100, 136-174MHz – Unencrypted
	MAHG-SHHXE	M7100, 136-174MHz – DES ¹ Algorithm
	MAHG-SHHXA	M7100, 136-174MHz – AES Algorithm
RU101188V21	MAHG-SHMXX	M7100 (50 W), 136-174MHz – Unencrypted
	MAHG-SHMXE	M7100 (50 W), 136-174MHz – DES ² Algorithm
	MAHG-SHMXA	M7100 (50 W), 136-174MHz – AES Algorithm
RU101188V12	MAHG-SNMXX	M7100, 378-430MHz – Unencrypted
	MAHG-SNMXE	M7100, 378-430MHz – DES Algorithm
	MAHG-SNMXA	M7100, 378-430MHz – AES Algorithm
RU101188V22	MAHG-SUMXX	M7100, 450-512MHz – Unencrypted
	MAHG-SUMXE	M7100, 450-512MHz – DES Algorithm
	MAHG-SUMXA	M7100, 450-512MHz – AES Algorithm
RU101188V31	MAHG-S8MXX	M7100, 806-870MHz – Unencrypted
	MAHG-S8MXE	M7100, 806-870MHz – DES Algorithm
	MAHG-S8MXA	M7100, 806-870MHz – AES Algorithm

¹ DES algorithm is for legacy system use only, transitional phase only – valid until May 19, 2007

² DES algorithm is for legacy system use only, transitional phase only – valid until May 19, 2007

The following table identifies all of the validated hardware part numbers for the P7150^{IP} Scan radio.

Validated Hardware Version Numbers	Validated Hardware Part Numbers	Description
RU101219V21	HT7170SH1X	P7150 Scan, 136-174MHz– Unencrypted
	HT7170SH1E	P7150 Scan, 136-174MHz – DES Algorithm
	HT7170SH1A	P7150 Scan, 136-174MHz – AES Algorithm
RU101219V51	HT7170AN1X	P7150 Scan (100 mW), 378-430MHz– Unencrypted
	HT7170AN1E	P7150 Scan (100 mW), 378-430MHz – DES Algorithm
	HT7170AN1A	P7150 Scan (100 mW), 378-430MHz – AES Algorithm
RU101219V61	HT7170SN1X	P7150 Scan, 378-430MHz– Unencrypted
	HT7170SN1E	P7150 Scan, 378-430MHz – DES Algorithm
	HT7170SN1A	P7150 Scan, 378-430MHz – AES Algorithm
RU101219V63	HT7130EN1X	P7130 Select, 378-430MHz– Unencrypted
	HT7130EN1E	P7130 Select, 378-430MHz – DES Algorithm
	HT7130EN1A	P7130 Select, 378-430MHz – AES Algorithm
RU101219V41	HT7170SU1X	P7150 Scan, 450-512MHz – Unencrypted
	HT7170SU1E	P7150 Scan, 450-512MHz – DES Algorithm
	HT7170SU1A	P7150 Scan, 450-512MHz – AES Algorithm
RU101219V71	HT7170S81X	P7150 Scan, 806-870MHz – Unencrypted
	HT7170S81E	P7150 Scan, 806-870MHz – DES Algorithm
	HT7170S81A	P7150 Scan, 806-870MHz – AES Algorithm
RU101219V73	HT7130E81X	P7130 Select, 806-870MHz – Unencrypted
	HT7130E81E	P7130 Select, 806-870MHz – DES Algorithm
	HT7130E81A	P7130 Select, 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. The module does not provide authentication of its operators. Thus, the Crypto-Officer and User roles are implicitly assumed based on the services selected. 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
- 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

3. Secure Operation and Security Rules

In order to operate the radios 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 the M/A Com:

1. A signed DSP code (i.e., a DSP code that has a DES-MAC³ 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 should be loaded to the module in encrypted form

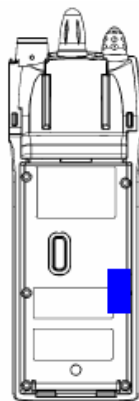
FIPS 140-2 Security Rules

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. The menu item "ZERO DES" or "ZERO AES" should be configured on the personality file.

3.2. Physical Security Rules

The P7150IP radio meets the Level 2 Physical security requirements through the application of a tamper evident label. The tamper evident label is shown in blue.



³ DES-MAC algorithm is for legacy system use only, transitional phase only – valid until May 19, 2007

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.

The M7100^{IP} radios meet the Level 1 physical security requirements. The physical enclosure of the radio provides the physical protection mechanisms.

3.3. Secure Operation Initialization Rules

The radio provides the following algorithms:

Algorithm Type	Modes/Mod sizes	FIPS-approved
Symmetric Algorithms		
DES (for legacy system use only, 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 (for legacy system use only, 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 140-2 compliance.

- (1) Apply the tamper evident label only to the P7150IP radio as described in the section 3.2
- (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 DES-MAC key and a KEK on the master key file (The master key file is the file containing all the keys and the EnableFips parameter before encrypting keys). 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 1 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 ⁴ 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 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 ⁵ 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.
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

⁴ DES algorithm is for legacy system use only, transitional phase only – valid until May 19, 2007.

⁵ DES-MAC algorithm is for legacy system use only, transitional phase only – valid until May 19, 2007.

	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.

P7150 ^{IP} and M7100 ^{IP} SRDI/Role/Service Access Policy	Security Relevant Data Item								
	TEK	KEK	DES-MAC ⁶ key	Copy of DES-MAC key	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					
Loading keys and radio personality configuration	w	w	w	w					
Upgrading radio firmware	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	w	w	
User role									
Turning the module on and initiate power-up self-tests	r	r	r	r		r	r	r	
Sending/receiving encrypted calls	r	r			r	r	r	r	

⁶ DES-MAC algorithm is for legacy system use only, transitional phase only – valid until May 19, 2007.

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

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