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

January 15, 2009

Revision Version 2.8

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
2.1. Roles 9
2.2. Authentication Mechanisms and Strength 10
3. Secure Operation and Security Rules 12
3.1. Security Rules 12
3.2. Physical Security Rules 12
3.3. Secure Operation Initialization Rules 12
4. Definition of SRDIs Modes of Access 15
4.1. Cryptographic Keys, CSPs, and SRDIs 15
4.2 Access Control Policy 16
5. Glossary 18

1. Introduction

The following describes the security policy for the multi-chip standalone module; the P7130^{IP} Select, 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 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 Select (P7130^{IP}) or Scan (P7150^{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 trunked 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.

- **Project 25 (P25) Over-the-Air Rekeying (OTAR)**

The P7100^{IP} portable provides P25 compliant OTAR support as described in TIA/EIA-102.AACA allowing the radio seamless digital interoperability with P25 compliant Key Management Facilities.

- **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

The hardware versions tested and validated are as follows:

- RU101188V1 – 136-174MHz, Mobile 7100
- RU101188V21 – 136-174MHz, Mobile 7100 (50 W)
- RU101188V12 – 378-430MHz, Mobile 7100
- RU101188V22 – 450-512MHz, Mobile 7100
- RU101188V231 – 806-870MHZ, Mobile 7100
- 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

Each validated hardware configuration supports the following three validated firmware configurations:

- H8 Version J2R14B02 and DSP Version F7R06A01
- H8 Version J2R15E05 and DSP Version F7R06F03
- H8 Version J2R16F01 and DSP Version F7R06F03

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-SHHXA	M7100, 136-174MHz – AES Algorithm
RU101188V21	MAHG-SHMXX	M7100 (50 W), 136-174MHz – Unencrypted
	MAHG-SHMXA	M7100 (50 W), 136-174MHz – AES Algorithm
RU101188V12	MAHG-SNMXX	M7100, 378-430MHz – Unencrypted
	MAHG-SNMXA	M7100, 378-430MHz – AES Algorithm
RU101188V22	MAHG-SUMXX	M7100, 450-512MHz – Unencrypted
	MAHG-SUMXA	M7100, 450-512MHz – AES Algorithm
RU101188V231	MAHG-S8MXX	M7100, 806-870MHz – Unencrytped
	MAHG-S8MXA	M7100, 806-870MHz – AES Algorithm

The following table identifies all of the validated hardware part numbers for the P7130^{IP} Select and P7150^{IP} Scan radios.

Validated Hardware Version Numbers	Validated Hardware Part Numbers	Description
RU101219V21	HT7170SH1X	P7150 Scan, 136-174MHz– Unencrypted
	HT7170SH1A	P7150 Scan, 136-174MHz – AES Algorithm
RU101219V51	HT7170AN1X	P7150 Scan (100 mW), 378-430MHz– Unencrypted
	HT7170AN1A	P7150 Scan (100 mW), 378-430MHz – AES Algorithm
RU101219V61	HT7170SN1X	P7150 Scan, 378-430MHz– Unencrypted
	HT7170SN1A	P7150 Scan, 378-430MHz – AES Algorithm
RU101219V63	HT7130EN1X	P7130 Select, 378-430MHz– Unencrypted
	HT7130EN1A	P7130 Select, 378-430MHz – AES Algorithm
RU101219V41	HT7170SU1X	P7150 Scan, 450-512MHz – Unencrypted
	HT7170SU1A	P7150 Scan, 450-512MHz – AES Algorithm
RU101219V71	HT7170S81X	P7150 Scan, 806-870MHz – Unencrypted
	HT7170S81A	P7150 Scan, 806-870MHz – AES Algorithm
RU101219V73	HT7130E81X	P7130 Select, 806-870MHz – Unencrypted
	HT7130E81A	P7130 Select, 806-870MHz – AES Algorithm

2. Roles, Services, and Authentication

The radio supports three roles: Crypto-Officer (CO), Key Management Facility (KMF), and User. By design, both the CO and User roles have access to a common set of services provided by the module, while the KMF role possess a separate set of services (OTAR). The module does not provide authentication of the User and CO operators, but does authentication OTAR messages. Thus, the Crypto-Officer and User roles are implicitly assumed based on the services selected, while OTAR messages must include a Message Authentication Code (a MAC). All the services of the module require the assumption of an authorized role or authenticated role (i.e., the CO, KMF, or User role).

2.1. Roles

The roles of the module include a Crypto-officer (CO), a Key Management Facility (KMF), and a User Role. All the services of the module require the assumption of an authorized role (i.e., the CO, KMF, 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 (H8 and DSP firmware)
- Downloading the personality file, Tracking Data and Feature Encryption Data to the radio
- Using Direct Frequency Entry feature (see the section 6.5.5 of the Maintenance Manual)
- Loading Tracking Data and Feature Encryption Data

KMF Role

The KMF sends OTAR key management messages to the radio to configure, update, and modify a given radio's Traffic and KEKs. All KMF services are described in the P25 OTAR standard (TIA/EIA-102.AACA)

- Change-RSI Procedure
- Changeover Procedure
- Delayed-Acknowledgment
- Delete-Key Procedure

- Modify-Key Procedure
- Negative-Acknowledgment
- Rekey Procedure
- Rekey-Acknowledgment
- Warm-Start Procedure
- Zeroize Procedure
- Hello Procedure
- Delete-Keyset Procedure
- No-Service Procedure

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

2.2. Authentication Mechanisms and Strength

The module authenticates loading code by verifying the accompanying CMAC checksum and also authenticates messages from the KMF by validating the accompanying AES-MAC checksum.

CMAC Authentication

The DSP file that is loaded to the module contains an embedded CMAC. When loading the DSP file, the module calculates a CMAC of the file using the CMAC key stored in the module and compares it with the CMAC 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.

AES-MAC Authentication

The module supports P25 KMF communication using the AES algorithm, and the KMF will include an AES-MAC with each message to allow the module to authenticate the validity of the message. The module will verify the AES-MAC before processing the message.

The KMF uses 256-bit AES-MAC keys to generate a 64-bit OTAR AES-MAC, and thus the false acceptance rate is $1/18x10^{19}$, which is far less than $1/10^{6}$. Additionally, one would need to authenticate $1.84x10^{14}$ times in one minute make the probability of a false acceptance greater than $1/10^{5}$. Therefore, the false acceptance rate for multiple attempts is less than $1/10^{5}$ in a minute for AES-MAC authentication.

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 DSP code with an embedded CMAC should be loaded to the module
2. A CMAC 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 "ZERO AES" should be configured on the personality file.

3.2. Physical Security Rules

The P7130^{IP}, P7150^{IP} and 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	64-bit, OFB	No
AES	256-bit, ECB, CBC, OFB	Yes, AES (Certs. #155 and #623)
VGE (M/A Com proprietary digital voice encryption algorithm)		No
Message Authentication Code		
CMAC		Yes, CMAC (Cert. #623)
AES-MAC		Allowed, AES MAC (Cert.

		#623, 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) 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 CMAC key and an AES 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) Before loading the DSP code into the radio [done in step (g) below], use the Keyadminconsole program to generate a CMAC of the code using the CMAC key and embed it in the DSP code. Generate the distribution key file based on the master key file.

(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 AES" as one of the menu items. Once this new personality is loaded to the radio, it gives a menu item called "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.

(2) Finally, operators should only load AES TEK's and not load any DES TEK's keys during operation (irrespective of whether the DES TEK's are manually distributed or sent via P25 OTAR), as DES is no longer a FIPS approved algorithm. Additionally, operators should not attempt to load any DES TEK's via P25 OTAR (which would only be possible if using a non-standard compliant KMF).

When initialized and operated 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 AES. The key sizes 256-bits, and the keys are stored in the DSP EEPROM in plaintext.
AES MAC (TEK)	This key is used by the module to authenticate messages sent by the KMF role and to generate AES MAC for response messages. The key is a specially designated 256-bit AES TEK.
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 AES), this key is also used to decrypt the new KEK. The encryption algorithms used is AES. The key size is 256 bits and it is stored in the DSP EEPROM in plaintext.
CMAC key	At power-up or after firmware loading, the module calculates a CMAC of the DSP firmware using this key and compares it with the CMAC embedded in the DSP firmware. If a new CMAC key is loaded (which is encrypted using AES), this key is also used to decrypt the new CMAC key. The key size is 256 bits and it is stored in the DSP EEPROM in plaintext.
Copy of CMAC key	This is a copy of the CMAC key mentioned in the above row. When the module performs power-up self-tests, this key is compared with the CMAC key of the above row. The key size is 256 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 stored in the SRAM at power up in plaintext. The size of a key is 256 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.

P7100^{IP} System Portable Two-Way FM Radio SRDI/Role/Service Access Policy	Security Relevant Data Item	TEK	KEK	CMAC key	Copy of CMAC 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
KMF Role										
Change-RSI Procedure										
Changeover Procedure										
Delayed-Acknowledgment										
Delete-Key Procedure		w	w							
Modify-Key Procedure		w	w							

Negative-Acknowledgment										
Rekey Procedure		w	w							
Rekey-Acknowledgment		r	r							
Warm-Start Procedure		w	w							
Zeroize Procedure		w	w	w	w	w	w			
Hello Procedure										
Delete-Keyset Procedure		w	w							
No-Service Procedure										
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
OTAR	Over the air rekey
KMF	Key Management Facility