MIDLAND RADIO CORPORATION

SECURITY POLICY

Syn-Tech III P25
Portable Radio (VHF and UHF)

Syn-Tech III P25
Dash Mount Mobile Radio (VHF and UHF)

Syn-Tech III P25
Trunk Mount Mobile Radio (VHF and UHF)

Syn-Tech III Desk Top Radio (VHF and UHF)

Revised: August 5, 2009

MIDLAND RADIO CORPORATION
5900 Parretta Drive
Kansas City MO 64120
www.midlandradio.com

Table of Contents

List of Tables

CHAPTER 1.0 Introduction

This manual contains the non-proprietary security policy for the Midland Syn-Tech III P25 Portable, Mobile (dash and trunk mount) and Desktop Radio products which are multi-chip standalone cryptographic modules validated at a FIPS 140-2 Security Level 1. The radios support Project 25 (P25) digital voice and data encryption operation and encryption key loading using a Midland Proprietary PC Key Loader.

This Security Policy covers the following radio models:

DESCRIPTION	MODEL-NUMBER	FCC ID
VHF Portable Radio, 136-174 MHz	STP105B	MMA90105
UHF Portable Radio, 380-470 MHz	STP404A	MMA90404
UHF Portable Radio, 450-512 MHz	STP404B	MMA90404B
VHF Mobile Radio, Mid Power, Dash Mount, 136-174 MHz	STM1050B	MMA901050
VHF Mobile Radio, Mid Power, Trunk Mount, 136-174 MHz	STM1055B	MMA901050
VHF Mobile Radio, High Power, Trunk Mount, 136-174 MHz	STM1115B	MMA901115
UHF Mobile Radio, Mid Power, Dash Mount, 380-470 MHz	STM4040A	MMA904040
UHF Mobile Radio, Mid Power, Trunk Mount, 380-470 MHz	STM4045A	MMA904040
UHF Mobile Radio, Mid Power, Dash Mount, 450-512 MHz	STM4040B	MMA904040B
UHF Mobile Radio, Mid Power, Trunk Mount, 450-512 MHz	STM4045B	MMA904040B
UHF Mobile Radio, High Power, Trunk Mount, 380-470 MHz	STM4085A	MMA904085
UHF Mobile Radio, High Power, Trunk Mount, 450-512 MHz	STM4085B	MMA904085B
VHF Desktop Radio, 136-174 MHz	SDT1090	MMA901090
UHF Desktop Radio, 380-470 MHz	SDT4080A	MMA904080
UHF Desktop Radio, 450-512 MHz	SDT4080B	MMA904080B

Table 1 FIPS 140-2 Validated Module Model Numbers

The above units are shown in illustrations on the following pages. The Trunk Mount Mobile is identical to the Dash Mounted Mobile Radio but has the Control Head removed from the main unit chassis and mounted in the vehicle interior connected by a cable to the main unit mounted in the trunk. The Desk Top Mobile version is identical to the standard Mobile Radio with the exception that an additional RF power amplifier module and power supply is fitted.

The UHF and VHF version of each product are identical to each other with the exception of certain RF frequency-dependent components. All versions utilize the same architecture, firmware and processors.

With the exception of certain RF components and packaging, all of the above models have identical digital circuitry and use the same operational firmware.

The Firmware covered by the FIPS 140-2 Validation consists of the following three elements:

- Control Micro-Processor Boot Firmware Version: 1.00 Build:1080
- Control Micro-Processor Firmware Version: MDV 1.01 Build:3320
- Digital Signal Processor(DSP) Firmware Version: SPV 1.03 Build:0556

Loading of firmware that has not been validated to FIPS 140-2 will void the validation of the Module

The Midland Syn-Tech III R25 radios provide Project 25 encrypted and clear voice, data, Short Message Service and GPS Reporting Service communications in accordance with the Project 25 Digital Land Mobile Radio standards suite. In addition, conventional analog unencrypted radio voice communications are supported.

This Security Policy defines the rules that must be followed to allow the radio to be operated in a secure manner. This document does not provide detailed user guidance for the radio operation to follow these rules, but will refer to the Midland user documentation as needed.

The entire radio is considered the crypto module for FIPS 140-2 validation purposes. The terms "Radio" and "Cryptographic Module" are used interchangeably in this document. The Critical Security Parameters (CSPs) are the AES Traffic Encryption and Key Encryption keys, HMAC authentication key, User password and zone password. These parameters are described as used in the following sections.

Algorithm Certifications (CAVP) are as follows:

1. AES (Cert. #645) The module uses a previously certified AES implementation (SnapCrypt) provided by Snapshield LTD.
2. SHS (Cert. #916)
3. HMAC (Cert. #521)
4. DRBG (Cert. #5.)

The radio products are also capable of clear and DES operation as FIPS non-Approved modes.

Cryptographic Module Photographs

VHF Portable

UHF Portable

VHF Mobile-Dash Mount

UHF Mobile-Dash Mount

VHF Mobile-Trunk Mount

UHF Mobile-Trunk Mount

VHF Desk Top

UHF Desk Top

CHAPTER 2.0 Identification and Authentication

The Midland Syn-Tech III P25 radios include several security related roles and authentication methods (passwords or key data). However as a public safety tool the radio must be considered a limited access device and should be physically secured and in the possession of authorized users at all times.

Roles and Authentication Method

Role	Description	Identity Based Authentication	Role Based Authentication
User	Uses radio to communicate with other Users. Selects channel encryption key.	• User Password • Zone Password	• Possession of the radio • Possession of valid Traffic Encryption Keys • Encryption Feature License
Administrator/ Crypto Officer	Loads firmware and configuration data (channel setup/encryption toggle/passwords) into the radio. Loads encryption keys into the radio.	No passwords or other identity verification	• Possession of a valid PC Programmer • Possession of a valid Midland Firmware Loader • Possession of Authenticated firmware • Possession of PC Key Loader Software • Possession of valid Traffic Encryption Keys
Maintenance	Adjusts and/or repairs radio Configures Licensed Options Erase HMAC key seed	None	• Possession of radio for service • Possession of License Configuration Software and “Hard key lock’

Table 2 Roles and Authentication

Authentication Methods

Possession

The first layer of protection in the Midland radio is physical access to the radio. The radio includes several functions that require no authentication. For example until a configuration is loaded in the radio with a Zone password (see description below) anyone with the applicable PC Programmer software, cable, and access to the radio can program the radio. However these are all proprietary items and even a modest, common sense access control policy for the radios and accessories will go a long way in securing radio operation.

User Password

The Administrator must configure the Midland radio with a password. This is an 8 decimal digit stored internally to the radio. The User password prevents the radio from being operated by unauthorized Users.

User password entries are not provided for viewing on the Midland radio's LCD display. An asterisk (*) symbol will be displayed for each valid keypad entry of the password. Only five unsuccessful attempts at entering the correct password are allowed. After the fifth unsuccessful attempt, further password entries are locked out until the radio's power switch is cycled OFF then ON or the battery is removed and replaced. Successfully guessing the User password is very improbable (less than 1 in 10,000,000 attempts).

Once a User password is entered it is valid until power is cycled on the radio. Be sure to turn the radio OFF whenever it will be out of use to force the next user to have to enter the User password again. The User password can only be changed or zeroized by using the Midland Proprietary PC Programmer Software application.

Zone Password

The Zone password allows more complete protection of specific zones in the radio. Each zone (collection of up to 16 channels assigned to the channel selection knob) can be configured as a "Protected Zone". The Zone password is 5 decimal digits long. A single Zone password can also be assigned, and is applicable for all protected zones. The Zone password provides access protection with the following exceptions:

- Only applies to protected zones. Unprotected zones can be modified without requiring entry of the Zone password
- If ANY zone in the radio is protected the Administrator cannot reprogram the radio without first entering the Zone password. This allows the Zone password to provide the User with protection

against others, including Maintenance Personnel from modifying his configuration.

Zone password entries are not viewable on the Midland radio's LCD display. An asterisk (*) symbol is displayed for each valid keypad entry of the password. Five attempts can be made to enter the correct zone password. Successfully guessing the Zone password is improbable (less than 1 in 10,000 attempts).

Like the User password, the Zone password once entered remains in effect until power is cycled on the radio. The Zone password can only be changed or zeroized by the Administrator/Crypto Officer using the Midland Proprietary PC Programmer Software application.

CHAPTER 3.0 Access Control

Approved Mode of Operation

The Midland radios support Project 25 AES Output Feedback Encryption of voice, data and Short Message Service as the only FIPS 140-2 Level 1 Approved mode of operation.

FIPS Approved Mode Indication

The Midland radio uses a "padlock" ICON on the status display to indicate encrypted operation. When AES encryption is being used, the padlock ICON is displayed with an "A" indicating the Approved AES mode. Refer to the Midland Operators Manual for the location of this ICON. The module operates in a single encryption mode at a time; either Approved mode (AES) or non-Approved mode (DES).

FIPS Approved Mode Invocation

The FIPS approved mode (AES) is invoked by the User whenever a channel is selected that is configured for AES encryption and contains a valid AES encryption key resident in its AES key position. Additionally encryption may be enabled or disabled on an AES channel (see encryption toggle below). This encryption toggling is considered a manual bypass operation of the FIPS approved AES encryption mode. Whenever the AES encryption is enabled the "A" padlock ICON will be displayed on the LCD screen.

FIPS Non-Approved Modes of Operation

The Midland radios also can support clear and P25 DES encryption. NIST no longer supports validation of DES based modes of operation, so all of these modes are non FIPS approved. The radio's encryption icon (a "padlock" icon) is displayed with a "D", indicating non-Approved DES operation. The non-Approved DES encryption modes can be disabled by not loading any DES encryption keys in the radio, or by not including the DES Licensed features. This allows a Midland radio to support only FIPS approved encryption operation if that is desired by a customer.

Services

The radios support the services specified in **Table 3 Services**. The table also lists the typical role that requires this service.

SERVICE	ROLE
Radio Maintenance	
Load Operational Firmware	Administrator/ Crypto Officer
Configure Licensed Options	Maintenance
Adjust/Repair Radio	Maintenance
Erase HMAC key seed	Maintenance
Configuration (Entered by PC Programmer)	
Encryption Key Load	Administrator/Crypto Officer
Channel Setup	Administrator/Crypto Officer
Enable Encryption Toggle	Administrator/Crypto Officer
Establish User and Zone Passwords	Administrator/Crypto Officer
Radio Operation	
Utilize User and Zone Passwords	User
Enable/Disable Encryption	User (if permitted in Channel Setup)
Select Channel Encryption Key	User (if permitted in Channel Setup)
Change Channel Parameters	User (if permitted in Channel Setup)
Zeroize keys	User, Administrator/Crypto Officer, Maintenance
Clear Analog Voice Service	User (if permitted in Channel Setup)
Clear/Encrypted Digital Voice Service	User (if permitted in Channel Setup)
Clear/Encrypted Data Service	User (if permitted in Channel Setup)
Clear/Encrypted SMS	User (if permitted in Channel Setup)
Clear/Encrypted GPS Service	User (if permitted in Channel Setup)
Show Status	
Display Firmware Revision Levels	Administrator/ Crypto Officer, User, Maintenance
Self-Test	
AES Key Wrap/Unwrap KAT	Administrator/Crypto Officer, User (Power on and menu selectable)
AES Algorithm KAT	Administrator/Crypto Officer, User (Power on and menu selectable)
SHA-256 KAT	Administrator/Crypto Officer, User (Power on and menu selectable)
HMAC-SHA-256 KAT	Administrator/Crypto Officer, User (Power on and menu selectable)
HMAC-DRBG KAT	Administrator/Crypto Officer, User (Power on and menu selectable)
HMAC-DRBG Continuous Test	User on each encrypted P25 transmit Administrator/Crypto Officer on key load
Firmware Check Sums Integrity Test	Administrator/Crypto Officer, User (Power on)
Operational Condition Test	
Bypass Operation Conditional Test	User on each encrypted P25 transmit
FIPS 140-2 External Software/Firmware Load Test	Administrator/Crypto Officer
Key Integrity Test	Administrator/Crypto Officer, User (Checked upon each key unwrap)

Table 3 Radio Services and Roles

Show Status Service

After a power on or User initiated self-test, the status of the radio will be displayed on the radio LCD. If the tests are all successful, a brief Test Passed indication will be given. During any error condition the error status of the radio will be displayed. The revision level of the firmware components can also be displayed via a menu entry request. During transmit and receive operation the encrypted/unencrypted status of the module is displayed using the Red/Green LEDs.

Self-Test Service

The radio contains the following self-tests that are run on power-up or on User initiation via a menu entry:

- AES Algorithm Known Answer Test (KAT)
- SHA-256 KAT
- HMAC-SHA-256 KAT
- HMAC-DRBG KAT
- HMAC-DRBG Continuous Test (Run on power-up and on each use of the HMAC-DRBG.)
- FIPS 140-2 External Software/Firmware Load Test (Run before operational firmware load. This test is run on any operational firmware load, regardless of supported (licensed) encryption algorithms.)
- Bypass Operation Conditional Test (This test is run before each transmission. It is run in all FIPS operational modes as well as non FIPS operational modes.)
- Firmware Check Sum Integrity Test
- Key Integrity Test (Run on each unwrap of encrypted key material.)

Failure of any KAT, Firmware Check Sum Integrity Test or the HMAC-DRBG Continuous Test will inhibit the operation of the radio.

Operational Condition Test Service

The following are operational condition tests where operation of the module is restricted if the test is failed:

- The FIPS 140-2 External Software/ Firmware Load Test is run before operational firmware load. A HMAC SHA-256 message digest calculation and verification is used to authenticate the firmware prior to loading. This test is run on any operational firmware load. Failure of the firmware update to authenticate using the HMAC Message Digest check will cause the Base

Station Crypto Module to reject the update and may necessitate the return of the Base Station to the Factory for service.

- The Bypass Operation Conditional Test is run before each transmission. Two separate and different commands are required from the control processor to permit clear transmission. It is run in the FIPS operational mode as well as non FIPS operational modes. Failure of the Bypass Test will produce a warning tone to alert the User that the module has rejected the clear transmission and the Base Station will not transmit in the clear mode.

- Key Integrity Test Run on each unwrap of encrypted key material. Failure of the Key Integrity Test will produce a warning to alert the User that a valid key is not available and new key(s) must be loaded to continue encrypted operation. If the current channel is designated as encrypted only, lack of a valid key will inhibit all transmission.

ROLES

The security related roles available were introduced in Roles and Authentication Method. This section details the available security services and the access to security parameters (cryptographic keys and Critical Security Parameters) that can be accessed by each role.

Administrator/Crypto Officer

The Administrator/Crypto Officer is responsible for key establishment. The person fulfilling this role will have access to the actual encryption key data. Other roles will have access to encryption key ID's and their use, but will not be able to access the actual encryption key data.

The Administrator/Crypto Officer also loads firmware and configuration data in the radio.

Encryption Key Load – PC Key Loader

Traffic Encryption Keys (TEKs) are entered manually in plain-text hexadecimal form using the Proprietary Midland PC Key Loader executable software running on a non-networked Personal Computer. Once TEK is entered and accepted it is sent to the radio in a clear text format. During Key Loading all radio operations except for key loading are disabled and no other inputs or outputs can occur on any other ports. When TEKs are received at the radio, the radio wraps the new key using an AES Key Wrap Algorithm and stores the wrapped key in non-volatile memory. The Key

Encryption Key (KEK) used in the wrapping is unique to the individual radio and is generated after a zeroization using a HMAC-DRBG. The KEK, TEKs and other Critical Security Parameters cannot be read from the radio.

The radio can store up to 48 AES keys and also up to 48 DES keys. All keys are stored in an AES key wrapped form (in accordance with "AES Key Wrap Specification" dated 16 November 2001) wrapped using a 256 bit KEK and an Approved AES algorithm (Cert. #645) in an Electronic Code Book operating mode. When keys are unwrapped for use, they are stored in volatile Random Access Memory in the Digital Signal Processor.

TEK generation must be by a FIPS Approved process that is outside the scope of this document. It is the responsibility of the Administrator/Crypto Offices to ensure that all key material is generated in a FIPS Approved process and that all key material is securely protected from the time it is generated until the time it is loaded into the radio.

Load Radio Operational Firmware

Loading FIPS 140-2 Validated radio operational firmware is accomplished using Midland Proprietary Firmware Update executable software running on a non-networked Personal Computer and a binary data file containing the FIPS 140-2 Validated updated firmware elements. The Firmware Update executable software also contains a application software identity code that is checked by the radio before commencing a firmware update. All operational firmware element blocks have an individual Message Digests calculated with a HMAC SHA-256 using a 256 bit secret key embedded in all Midland radios. This key is derived from a 440 bit HMAC-DRBG seed that is loaded in a read-protected Module Control Micro-Processor read-only memory area in the radio at manufacture. The key is not known or included in any form in the downloaded firmware image, or the update utility itself. The 440 bit HMAC-DRBG seed is the only CSP loaded at the factory. This seed can be zeroized by the Maintenance role using a proprietary PC executable software tool.

The Midland radio will ONLY accept firmware element blocks with HMAC Message Digests that each match the Message Digest calculated across the firmware block using the secret HMAC key stored in the radio. If the Message Digest of any block in a firmware element fails to match the Message Digest calculated using the HMAC and secret HMAC key, the entire firmware element update is rejected. If the update fails, the radio will revert to the

previous firmware or in some cases have to be returned to the Factory for repair.

In addition each firmware element has a Check Sum that is checked prior to committing the new firmware into the radio flash memory. These Check Sums are checked on each power-on. The check sum for the Module Control Micro- Processor firmware is 16 bits long and the Check Sum for the DSP firmware is 32 bits long.

User Password

The User password is entered by the Administrator/Crypto Officer with the PC Programmer. The Administrator/Crypto Officer can set, change or clear a radio's programming password, without needing to know the existing programming password.

Zone Password

The Zone Password, if enabled, is entered at the PC Programmer. The Administrator/Crypto Officer can set, change or clear a radio zone password. The Administrator/Crypto Officer must know a radio's existing Zone password before to be able to modify it. The radio checks its Zone password before accepting any configuration data from a PC Programmer. The Zone password must then be entered at the PC programmer before the radio will accept any changes (including changing the Zone password).

Channel Setup

The Administrator/Crypto Officer configures all radio channel parameters using the Midland Proprietary PC Programmer software application.

Encryption Toggle

The Administrator/Crypto Officer can program a side button to act as an encryption toggle using the Midland Proprietary PC Programmer software application.

Self-Test and Show Status

The Administrator/Crypto Officer can initiate the self-test either via powering on the module or via menu selection. The Administrator/Crypto Officer can also use the show Status menu selection to verify the correct level of firmware installed in the module.

USER

The User will operate the radio once it has been loaded and configured by the Administrator/Crypto Officer.

Communications Services

The following communication services are provided to the User:

Clear/Encrypted Digital Voice Service

Digital voice service is provided in accordance with the Project 25 Digital Land Mobile Radio standards suite. This digital voice service can be in the clear, AES Encrypted or DES Encrypted (FIPS non-Approved) mode. Voice communications can utilize external audio accessories or the internal speaker and microphone in the case of the Portable products.

Clear Analog Voice Service

Analog voice service is also provided. Voice communications can utilize external audio accessories or the internal speaker and microphone in the case of the Portable products.

Clear/Encrypted Digital Data Service

Digital Data Service using the Project 25 Packet Data protocol is provided through a RS-232 port and a Midland Proprietary Data Application Program running on a PC. This Digital Data Service can be in the clear text, AES Encrypted or DES Encrypted (Non-FIPS) mode.

Clear/Encrypted Short Message Service

Short Message Service is provided. This SMS can be in the clear, AES Encrypted or DES Encrypted (FIPS non-Approved) mode. The SMS can be either stored messages or messages entered from the radio keypad

Clear/Encrypted Global Position Message Service

If enabled by the User, the Serial Data Port (or second Serial Data Port in the case of the Non-Portable Radio Products) can be used to connect a standard GPS receiver to the radio. GPS messages can be in the clear, AES Encrypted or DES Encrypted (Non-FIPS) mode.

Input/Output Ports

Table 4 lists the ports used by the services provided by the Modules.

SERVICE	MODULE	PORT	USAGE
Encryption Key Load	All	RS-232 Serial Data	Control Input
Firmware Load	All	RS-232 Serial Data	Control Input
PC Program-Channel Setup/Encryption Toggle Enable/Enter Passwords	All	RS-232 Serial Data	Control Input
Configure Licensed Options	All	RS-232 Serial Data	Control Input
Clear/Encrypted Digital Data	All	RS-232 Serial Data	Data Input Data Output
Clear/Encrypted GPS Message Service	Portable	RS-232 Serial Data	Data Input
	• Dash Mount Mobile • Trunk Mount Mobile • Desk Top	Second RS-232 Serial Data	
Clear/Encrypted Short Message Service	All	LCD Output	Data Output
		Keypad Input	Data Input
• Clear Analog • Clear/Encrypted Digital Voice Data	Portable	Internal Speaker	Data Output
		Microphone	Data Input
	All	External Speaker	Data Output
		External Microphone	Data Input
• Clear/Encrypted Digital Data • Clear/Encrypted GPS Message Service • Clear/Encrypted Short Message Service • Clear Analog and Clear/Encrypted Digital Voice Data	All	Antenna	Data Input/Output
Encryption Toggle	All	Keypad/Side Button	Control Input
• Self-Test • Show Status • Utilize Passwords • Select Encryption Key	All	LCD Output	Display Module Status
		Keypad Initiate	Control Input
Zeroize	All	Keypad	Control Input

Table 4 Module Port Usage

External Input Devices

The following external input devices are utilized with the module:

- Personal Computer: A PC with proprietary Midland Radio software can be used to input configuration data in the radio, to set encryption key and keyset identifiers and to load keys themselves.
- Data Terminal: A PC with proprietary Midland Radio Data Application software can serve as a data terminal and input digital clear-text data into the Midland Radio.
- Audio Device: Any standard audio accessory can input audio data into the Midland Radio.
- GPS Data: If enabled by the User, GPS data can be input to the radio via the primary RS-232 Serial Data port or via the secondary RS-232 Serial Data Port in the case of the non-portable modules.

Encryption Toggle

The radio may have a side-key programmed to enable or disable encryption. Each press of the assigned side-key will toggle the setting. When disabled all channels will transmit in the clear regardless of the channel encryption configuration. However an encryption locked channel will always transmit encrypted regardless of this toggle setting.

Zeroize Keys

A User always has the ability to zeroize keys from the keypad regardless of the radio configuration. To zeroize keys, the User must hold down both the "Clear" button on the radio key pad and the red "Emergency" button for over 1 second. The radio LCD displays a zeroize message at the completion of the erasure of all keys. When zeroized, the radio-unique Key Encryption Key used to encrypt keys for internal storage is also erased. At next radio power up, the radio must generate a new KEK prior to loading new keys.

Change Channel Parameters

If permitted by the Administrator/Crypto Officer channel setup, the User can modify the radio channel parameters using the module keyboard to enter new channel data.

Self Test and Show Status

The User can initiate the self test either via powering on the module or via menu selection. The User can also use the show Status menu selection to verify the correct level of firmware installed in the module.

Encryption Key Selection

If permitted by the Administrator/Crypto Officer channel setup, the User can select the encryption key to be utilized for transmit operation using the module keyboard.. The receive key selection is automatic in that module will utilize the key indicated in the Project 25 frame header provided that key is available in the module.

Maintenance

Should the radio require maintenance, it must be returned to a Midland Authorized Maintenance Facility.

The maintenance personnel are required to erase all configuration and User data as well as to zeroize the radio when it is received and also to zeroize the radio again prior to returning the radio. When the radio is returned it will be necessary for the Administrator/Crypto Officer to reconfigure the radios and re-establish User and Zone passwords.

Configure Licensed Options

The radio licensed features are configured at the factory by a Midland Proprietary license software program requiring a “hard key lock” that runs on a PC. The Administrator must order specific features for specific radio serial numbers through their Midland customer service or sales representative. The PC software utility automatically loads the encrypted feature file and sends it to the radio thus enabling the feature. The Administrator/Crypto Officer has no other means for changing any licensed features. All license changes must be made by a Midland customer service or sales representative using the Midland Proprietary license software and the “hard key lock” hardware.

The FIPS 140-2 validation of the radios includes all of these licensed features, although only the AES encryption feature is part of the validated FIPS approved mode of operation. The radio includes indicators (described elsewhere in this document) to show if it is operating in a FIPS approved mode. The user cannot directly tell which features are licensed in a particular radio, however if a license is disabled, the feature is fully disabled including removal of menu items related to the feature. Each license description below includes a brief description of how the radio’s operation differs if the license is disabled. (Midland Customer Support also has a database of all licenses based on the radio’s serial number).

Project 25 DES Encryption Feature License

The Project 25 DES Encryption Feature License allows DES encrypted voice and data operations on P25 digital conventional

channels. This is a FIPS non-Approved mode of operation for interoperability on P25 systems that use this encryption method. For situations where this feature is not needed or only FIPS approved modes are allowed the feature can be fully disabled by not including this feature license

When disabled:

- DES Encryption cannot be enabled on a P25 digital channel through the channel programming menu, or PC Programmer.
- The radio menus will not display a DES choice for key management operations.
- If P25 DES is disabled DES keys cannot be loaded into the Midland radio.

Project 25 AES Encryption Feature License

The Project 25 AES Encryption Feature License allows AES encrypted voice and data operations on P25 digital conventional channels. This is the FIPS approved mode of operation, so this license must be included for any FIPS approved operation.
When disabled:

- Encryption cannot be enabled on a P25 digital channel through the channel programming menu, radio menus, or PC Programmer.
- The radio menus will not display an AES choice for key management operations.
- AES keys cannot be loaded into the Midland radio

Self Test and Show Status

The Maintenance role can initiate the self test either via powering on the module or via menu selection. The Maintenance role can also use the show Status menu selection to verify the correct level of firmware installed in the module.

General

Access control is generally concerned with ensuring the Users have access to only the channels and encryption parameters to which they are authorized. This section lists the typical and recommended means of using the parameters described in this section.

Encryption Key Load

The primary access control should be to load only the encryption keys authorized for an individual radio User. This ensures that the radio can only communicate with other Users authorized to use the encrypted channel.

Encryption Lock and Bypass Description

The use or non-use of encryption is controlled exclusively by the User, subject to the User selection being consistent with programming entered by the Administrator/Crypto Officer. The bypass mode is therefore exclusive. The User action sets a flag in the Control Micro-Processor indicating the selection of encrypted or non-encrypted operation.

In the Project 25 mode (the only encrypted mode supported by the Midland radios), if a RF signal is received that is encrypted, the radio checks to see if it has the encryption key indicated in the receiver Project 25 Encryption Header Frame and further that the channel has been programmed for encrypted operation and that the User has enabled encryption. If these two independent internal actions (checks) are successful, the radio will decrypt the message and provide decrypted voice or data to the User.

The User is also notified that the receive signal is encrypted both by a flashing Receive LED and a LCD Icon depicting encrypted receive operation.

Each channel in the Midland radio can be programmed by the Administrator/Crypto Officer, using the PC Programmer for "Encryption Lock". Sensitive missions where all communications must be encrypted should have channel encryption lock enabled. This prevents intentional or accidental disabling of encryption on the sensitive channels.

When "Encryption Lock" is enabled a User cannot disable encryption on a channel that is configured for encrypted operation. This ensures that the User cannot transmit on the secure channel without using encryption. This parameter can only be changed by the Administrator/Crypto Officer using the PC Programmer.

Each time transmit is initiated by the User the Module Digital Signal Processor requires that the Module Control Micro-Processor performs a bypass test prior to transmitting. This test involves the Control Micro-Processor overtly checking the programming on the channel to see if clear operation is permitted and checking the stored User selection (flag) to verify that the operator has selected a clear transmit mode. If either check indicates a conflict with the clear transmit operation, the Digital Signal Processor inhibits transmit operation and the User is given an audible and visual error indication. These two independent internal actions (checks) are performed prior to each transmit operation.

It is a requirement of Public Safety radio that unencrypted transmissions from another radio be received. If the channel is designated as encrypted only, the User radio will receive the transmission but will insert a loud, repetitive "Beep" warning tone to alert the User that the received transmission is unencrypted. This is not a bypass mode in that no sensitive

data is transmitted by the radio and the received information is “tagged” with a tone indicating that the information was received unencrypted.

The User is also notified when encrypted mode has been selected both by a flashing Transmit LED and a LCD Icon depicting encrypted transmit operation.

User/Zone Passwords

The User can be further restricted by setting User and/or Zone passwords. These prevent restricted users from being able to change any channel settings. From a security standpoint this prevents the users from being able to manually enter un-authorized frequencies or other channel parameters which could be used to monitor or block (interfere) with those channels.

Initial Installation

When the radio is first received the following steps must be followed to ensure compliance with FIPS 140-2 and Midland Security Policy requirements:

1. **Enter User Password (Administrator/Crypto Officer)** When the radio is first turned on, the operator will be prompted to enter a User password. The Administrator must enter this password and ensure that it is given to the intended User of the radio.
2. **Zeroize (Administrator/Crypto Officer)** The radio must be zeroized prior to configuring. This will ensure that any keys that may have been previously entered will be erased and also will force the radio to develop a fresh Key Encryption Key to wrap the encryption keys with when entered. Zeroization does not erase the User password entered above.
3. **Check for Firmware Updates (Administrator/Crypto Officer)** Check with your Midland Service Representative to see if there have been any firmware updates released since the radio was manufactured. Since the firmware updates may address important radio performance and security issues, these updates must be installed prior to putting the radio into service. The radio will automatically authenticate the new firmware and will reject any firmware that is damaged or produced by anyone other than Midland Radio Corporation.
4. **Configure the radio Channels/Features (Administrator/Crypto Officer)** Attach a PC with the Midland Radio PC Programmer software installed to the radio. Configure the channels to the desired arrangement. Keep in mind that AES is the only FIPS Approved mode and limit the use of Non-Approved DES for backward compatibility and interoperability only. The encrypted-only feature should be programmed on all critical security channels.
5. **Load Encryption Keys (Administrator/Crypto Officer)** Using the Midland PC Key Loader software application load keys into the radio. Up to 48 AES and 48 DES keys can be loaded into the radio. The radio will store the keys internally in an AES key wrapped form and keys cannot be viewed or extracted from the radio after being entered.
6. **Cycle Power (Administrator/Crypto Officer)** Turn the radio off and then back on. A “test passed” indication will be briefly displayed on the radio LCD. The operator will be required to enter the User password prior to use of the radio.
7. **Test (Administrator/Crypto Officer)** Using a test set or a known good radio with the same channel configuration, verify the programming of the radio.
8. **Initiate Service (Administrator/Crypto Officer)** The Administrator can now issue the radio to the intended User along with the User password.

CRITICAL SECURITY PARAMETERS (CSPs)

The following table lists the Critical Security Parameters contained in the radio and the access to each CSP for the various roles:

Critical Security Parameter	CSP Description	Service Utilizing the CSP	User Access	Admin./ Crypto Officer Access	Maint. Access
HMAC Key	The HMAC key is 256 bits long. The HMAC-DRBG 440 bit seed that produces the HMAC key is stored when the radio is manufactured in a read-protected flash ROM in the Module Control Micro- Processor. The HMAC is used to authenticate the firmware elements prior to accepting the firmware update.	Firmware Authentication	None Return to Maintenance to zeroize	None Return to Maintenance to zeroize	Load at Factory Zeroize
Key Encryption Key (KEK)	The KEK is generated at key load using an approved HMAC-DRBG. The KEK is unique to each radio. The KEK is zeroized along with any Traffic Encryption Keys (TEKs). The 440 bit HMAC-DRBG seed that produces the KEK is stored in a read-protected Module Control Micro-Processor ROM area and is provided to the DSP only just prior to unwrapping encrypted TEKs.	Stored Key Protection	Zeroize only	Zeroize only	None
Traffic Encryption Keys (TEKs)	TEKs are stored in serial flash memory in an encrypted form using an AES key wrap. The key wrap is done with the default value of initialization that is recovered and checked on unwrapping thus verifying the integrity of the stored key material. TEKs are unwrapped at radio power on and are stored internally to the DSP in volatile memory and are lost once the radio is powered off.	Voice, Data, and SMS Encryption and Decryption	Use and zeroize only Cannot be extracted from radio	Load and zeroize only Cannot be extracted from radio	None
User Password	This 8 digit Password prevents the radio from being operated by an unauthorized user.	User Authentication	Enter for Authentication	Set	Reset
Zone Password	If enabled, the zone password prevents unauthorized modification of the programming for a protected zone	Protect Zone Programming	Enter for Authentication	Set	Reset

Table 5 Critical Security Parameters

The following table lists the Non-Critical Security Parameters contained in the module and the access to each NCSP for the various roles:

Non-Critical Security Parameter	NCSP Description	Service Utilizing the NCSP	User Access	Admin./ Crypto Officer Access	Maint. Access
HMAC-DRBG Entropy Seed	The HMAC-DRBG Entropy Seed is a 440 bit long value that is continuously updated several times a second by concatenating the lowest 3 bits of 10 bit samples of four noisy analog voltages sampled at random times. The last 440 bit value is stored in serial flash memory when the radio is powered down thus ensuring availability of a high entropy seed even just after radio power on.	Random Bit generation for Key Wrap and Project 25 Encryption Message ID	None	None	None
HMAC-DRBG Last Value	The last 256 bit value produced by the HMAC_DRBG is stored in serial flash memory. This value is compared with the next value produced by the HMAC_DRBG to provide a continuous test of the HMAC_DRBG.	HMAC-DRBG Integrity Check	None	None	None
Check Sum-Digital Signal Processor	The DSP has a 32 bit Check Sum Check that is used to verify the integrity of each firmware element prior to usage. This is calculated and checked on each power-up	Digital Signal Processor Firmware Integrity Check	None	None	Read
Check Sums-Control Micro-Processor	Each of the two elements of the Module Control Micro-Processor firmware has a 16 bit Check Sum Check that is used to verify the integrity of each firmware element prior to usage. This is calculated and checked on each power-up	Control Micro-Processor Firmware Integrity Check	None	None	Read
Firmware Update Software Identity Code	The identity of the Midland Proprietary Firmware Update software is checked prior to initiating any firmware updates.	Firmware Update Software Validation	None	Use	Set at Factory

Table 6 Non- Critical Security Parameters

CHAPTER 4.0 Physical Security

Tamper

The radio does not include physical security mechanisms such as tamper evident seals or locks.

Zeroize

The Midland radio can be zeroized by holding down both the “Clear” and red “Emergency” Push Buttons (See Technical Service Manual). If a User is in a situation where the encryption keys may be compromised, the Zeroize feature should be used to allow rapid dumping of the encryption keys. This feature can also be used as a convenient means of clearing encryption keys from a radio before storage.

Zeroization erases all clear text Traffic Encryption Keys (TEKs) and the Key Encryption Key (KEK) stored in volatile memory as well as all wrapped TEKs stored in non-volatile memory. The seed used to generate the previous KEK is also erased on zeroization. The radio will automatically generate a new KEK when the radio is next powered on after a zeroizaton. The new KEK is generated using an Approved HMAC-DRBG algorithm and a continuously updated 440 bit entropy source and is therefore unique to the radio and is different from any other KEK the radio has generated previously.

The User and Zone passwords can only be changed or zeroized by the Administrator/Crypto Officer using the Midland Proprietary PC Programmer Software application.

The Firmware Update Software Identity Code and the HMAC key are loaded into the module at the factory and can only be changed or zeroized by Maintenance personnel. Erasure of the HMAC key will make firmware updates impossible. Attempting to load new firmware without a valid HMAC key in the module will cause erasure of the existing firmware and will make it necessary to return the module to the factory to restore operation of the module

The HMAC-DRBG Entropy Seed is continuously overwritten with a newly generated value and is not separately zeroized. The HMAC-DRBG Last Value is overwritten each time the HMAC-DRBG is called and is not separately zeroized.
c
The DSP and Control Processor Check Sums are imbedded in the firmware images and are checked on each power-up. They are not separately zeroized.

Summary

The primary means of physical security for the radio is the possession of the device. A customer security policy should be based on ensuring that only authorized personnel have access to the radio at all times. To further secure the

system Users should be directed to zeroize encryption keys whenever they are not immediately needed for a mission. This is especially important when storing the radio, or having it repaired. The radio must be sent to a Midland Authorized Maintenance Facility for repair or replacement, and Midland as a policy zeroizes all User and cryptographic data from the radio before performing any repair activities. In general a policy of limited radio, PC Programmer access, along with periodically changing encryption keys should be implemented to minimize potential compromises.

CHAPTER 5.0 Mitigation of Other Attacks

The Midland radios do not contain any specific mitigation of other attacks.