MIDLAND RADIO CORPORATION

SECURITY POLICY

Base Station Crypto Module

Revised: September 3, 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 Base Station Crypto Module product which is a multi-chip standalone cryptographic module validated at a FIPS 140-2 Security Level 1. The Module supports Project 25 (P25) digital voice and data encryption operation and key loading using a PC key loader.

This Security Policy covers the Midland Radio BTIII Base Station product line where the entire Base Station is the Cryptographic Module. The terms "Base Station" "Module" and "Cryptographic Module" are therefore used interchangeably. The UHF and VHF version of each Base Station product are identical to each other with the exception of certain RF frequency-dependent components. All Base Stations utilize the same architecture, processor, digital circuitry and use the same operational firmware.

The following Base Station Models are covered by this FIPS-140-2 validation:

FCC ID	Model #
No FCC ID (FEDERAL Use)	91-1060A
MMA911060B	91-1060B
No FCC ID (FEDERAL Use)	91-1110A
MMA911110B	91-1110B
No FCC ID (FEDERAL Use)	91-4050A
MMA914050B	91-4050B
No FCC ID (FEDERAL Use)	91-4100A
MMA914100B	91-4100B
MMA914100C	91-4100C
MMA914100D	91-4100D
MMA917100B	91-7100B
MMA918100B	91-8100B

Table 1 Base Station Model Numbers Included in FIPS-140-2 Validation

The Version of the Module Firmware covered by the FIPS-140-2 validation is:

- Digital Signal Processor (DSP) Firmware Version: FIPS_ver010b Dated 12/26/2008.

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

The Midland BTIII Base Stations provide Project 25 encrypted and clear voice, data and Short Message Service communications in accordance with the Project 25 Digital Land Mobile Radio standards suite. In addition, conventional analog radio voice communications are also supported.

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

The Midland Base Station is a multi-chip standalone module for FIPS 140-2 validation purposes where the cryptographic boundary includes the entire Base Station. The Critical Security Parameters (CSPs) are the AES Traffic Encryption and Key Encryption keys and HMAC authentication key. These parameters are described as used in the following sections.

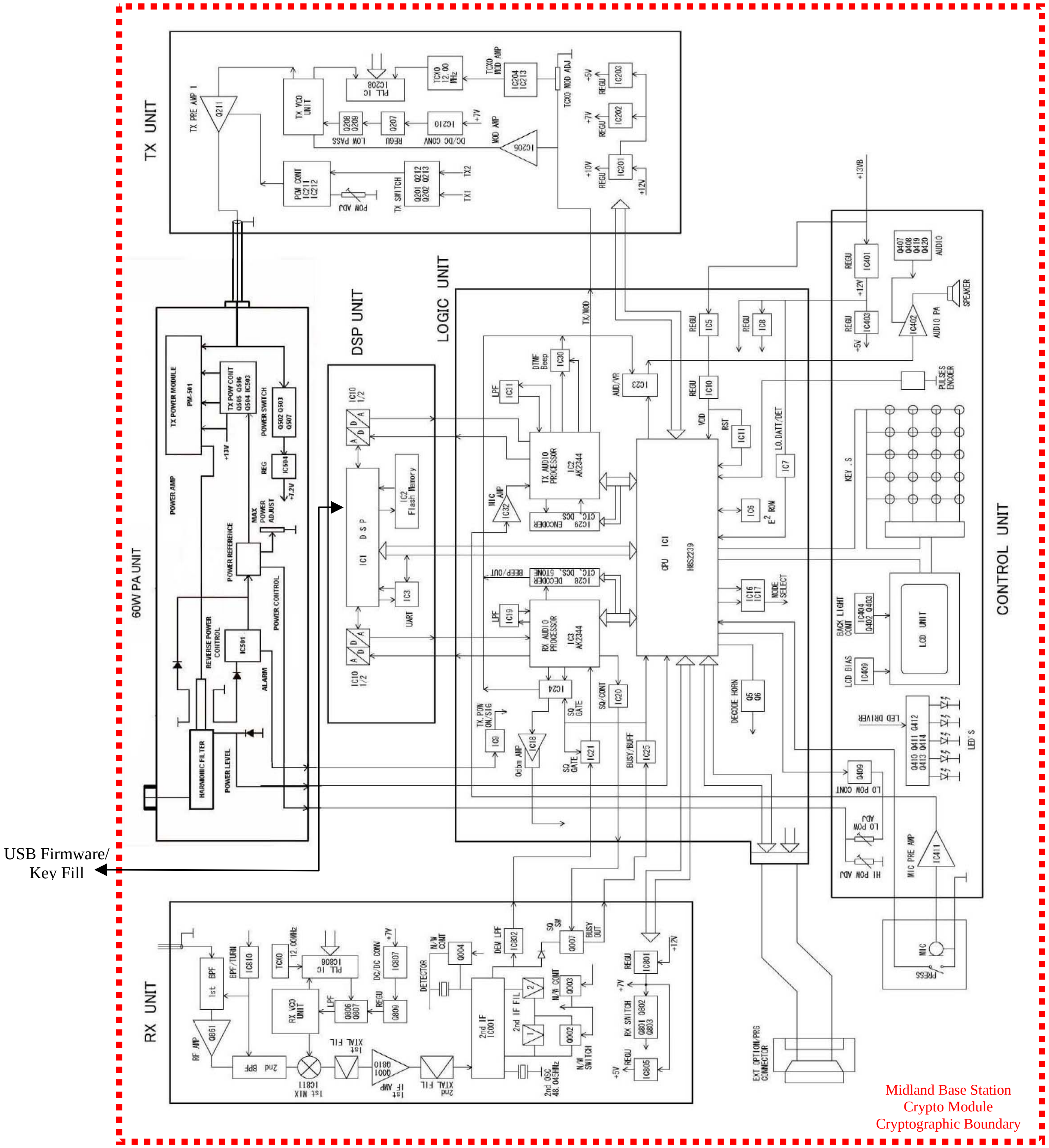
Algorithm Validations (CAVP) are as follows:

1. AES (Validation #485) The module uses a previously validated AES implementation (SnapCrypt) provided by Snapshield LTD.
2. SHS (Validation #945)
3. HMAC (Validation #548)
4. DRBG (Validation #7).

The Base Stations are also capable of clear and DES operation as a FIPS non-Approved modes.

Product Photograph

The following diagram shows the functional block elements of the Midland Base Station.



Block Diagram of the Midland Base Station Crypto Module

CHAPTER 2.0 Identification and Authentication

The Midland BTIII Base Stations Products include several security related roles and role-based authentication methods. However as a Public Safety tool the Base Station 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 Base Station to communicate with other Users	None	• Possession of the Base Station • Possession of valid Traffic Encryption Keys
Administrator/ Crypto Officer	• Loads firmware into the Base Station • Loads configuration data into the Base Station • Loads keys into the Base Station	None	• Possession of a valid PC Programmer • Possession of Authenticated firmware • Possession of PC Key Loader Software • Possession of valid Traffic Encryption Keys
Maintenance	• Adjusts and/or repairs Base Station • Erases HMAC key seed	None	• Possession of Base Station for service

Table 2. Roles and Authentication

CHAPTER 3.0 Access Control

Approved Modes of Operation

The Midland Base Stations 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. Only one mode of operation is permitted at a time (either clear, DES encrypted or Approved AES encrypted).

FIPS Approved Mode Indication

The Midland Base Station displays "AES" on the LCD status display to indicate it is operating in the sole FIPS 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. Whenever the AES encryption is enabled "AES" will be displayed on the LCD screen.

FIPS Non-Approved Modes of Operation

The Midland Base Stations also can support P25 DES encryption. NIST no longer supports validation of DES based modes of operation, so all of these modes are non FIPS approved. The LCD will display "DES", 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 License features. This allows a Midland Base Station to support only FIPS approved encryption operation if that is desired by a customer.

In addition, the Midland Base Stations can support clear analog voice communications which is a FIPS Non-Approved mode of operation. If this mode is not desired, the Base Station can be programmed on a channel-by-channel basis to require encrypted operation only.

Services

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

SERVICE	ROLE
Communication Services	
Clear Analog Voice Service	User (if permitted in channel setup)
Clear/Encrypted Voice Service-Digital	User (if permitted in channel setup)
Clear/Encrypted Data Service-Digital	User (if permitted in channel setup)
Clear/Encrypted SMS	User (if permitted in channel setup)
Non-Communication Services	
Base Station General	
Load Operational Firmware	Administrator/ Crypto Officer
Configure Licensed Options	Maintenance
Erase HMAC key seed	Maintenance
Configuration	
Encryption Key Entry-PC Key Loader	Administrator/Crypto Officer
Channel Configuration-PC Programmer	Administrator/Crypto Officer
Base Station Operation	
Enable/Disable Encryption	User (if permitted in channel setup)
Select Encryption Key	User (if permitted in channel setup)
Change Channel Parameters	User (if permitted in channel setup)
Zeorize keys	User, Administrator/Crypto Officer, Maintenance
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 transmit in P25 Administrator/Crypto Officer on key load
Firmware Check Sum Integrity Test	Administrator/Crypto Officer, User (Power on)
Bypass Operation Conditional Test	User on each transmit in P25
FIPS 140-2 External Firmware Load Test	Administrator/Crypto Officer
Key Integrity Test	Administrator/Crypto Officer, User (Checked upon each key unwrap)

Table 3. Base Station Services and Roles

Show Status Service

After a power on or User-initiated self-test, the status of the Base Station will be displayed on the Base Station LCD. If the tests are all successful, a brief "DSP Self-Test Passed" indication will be given. During any error condition the error status of the Base Station will be displayed on the Base Station LCD and the operation of the Base Station will be inhibited until power is cycled off and on forcing a retest.

Self Test Service

The Base Station 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 power-up and on each use of the HMAC-DRBG.
- Firmware Check Sum Integrity Test

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

In addition the following conditional tests are run as indicated:

- 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. 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 enter an Error State. After a failed or successful firmware load it is necessary to power down and re-power the Base Station to resume operation of the Module. If the firmware load was successful, once self-test are successfully completed, the Base Station will operate using the new firmware. If the firmware load was unsuccessful, once self-test are successfully completed, the Base Station will resume operation with the previously installed firmware.

- 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 enter an Error State. It is necessary to power down the Base Station to clear the Error State.

- The Key Integrity Test is 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 resume encrypted operation. The module will enter an Error State and it is necessary to power down the module and to load valid keys to resume operation of the Module

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. The User can select the current Traffic Encryption Key (TEK) to be used by selecting the Key ID, but is not able to view or extract the actual TEK data.

Encryption Key Load – PC Key Loader

Traffic Encryption Keys (TEKs) are loaded manually in plain-text hexadecimal form at the Midland PC Key Loader. Once TEK is entered and accepted it is sent to the Base Station in a clear text format. During Key Loading all Base Station 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 Base Station, the Base Station 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 Base Station and is generated after a zeroization using a HMAC-DRBG. The KEK, TEKs and other Critical Security Parameters cannot be read from the Base Station.

The Base Station can store two banks of up to 16 keys. Either bank can be designated as AES or DES keys. All keys are stored in an Approved AES key wrapped form wrapped using a 256 bit KEK and an Approved AES algorithm 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 Officer 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 Base Station.

Load Module Operational Firmware

Loading Module operational firmware is accomplished using PC Firmware Update software and a data file containing the updated firmware elements. The two operational firmware element blocks (Firmware and Table Data) each have an individual Message Digests calculated with a HMAC SHA-256 using a 256 bit secret key embedded in all Midland Base Stations. This key in a HMAC-DRBG seed form is loaded in the Module at manufacture. The key is not known or included in any form in the downloaded firmware image, or the update utility itself.

The Midland Base Station Crypto Module 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 module. If the Message Digest of a firmware element fails to match the Message Digest calculated using the HMAC and secret HMAC key, the entire firmware element update is rejected and the Module enters an Error State. If the update fails, after power down and re-power, the Module will revert to the previous firmware or in some cases, may 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 Module flash memory. This Check Sum is checked on each power-on and when initiated by the Base Station operator using a menu selection. The check sum for the DSP is 16 bits long.

Channel Setup

The Administrator/Crypto Officer configures all Base Station channel parameters at the PC programmer.

Self-Test Service

The Administrator/Crypto Officer can initiate the Self-Test of the module through powering up the module or by a request from the Base Station menu.

Show Status Service

The Administrator/Crypto Officer can check the revision level of the module firmware by a request using the Base Station menu.

Zeroize

The Administrator/Crypto Officer is 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.

Maintenance

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

Self-Test Service

Maintenance can initiate the Self-Test of the module through powering up the module or by a request from the Base Station menu.

Show Status Service

Maintenance can check the revision level of the module firmware by a request using the Base Station menu.

Zeroize

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.

Erase HMAC Key

The maintenance personnel can also erase the HMAC key. This will prevent the module from being able to accept future module firmware updates and may necessitate return of the module to the Factory.

User

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

Communication Services

The following communication services are provided to the User:

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 (Non-FIPS), AES Encrypted or DES Encrypted (Non-FIPS) mode. Voice communications utilize external audio accessories.

Analog Voice Service

Analog voice service (Non-FIPS) is also provided. Voice communications utilize external audio accessories.

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 (Non-FIPS), AES Encrypted (FIPS-Approved) or DES Encrypted (Non-FIPS) mode.

Short Message Service

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

Non-Communication Services

The following non-communication services are provided to the User:

Self-Test Service

The User can initiate the Self-Test of the module through powering up the module or by a request from the Base Station menu.

Show Status Service

The User can check the revision level of the module firmware by a request using the Base Station menu.

Select Encryption Key

The User can select the encryption key to be used for Traffic (Communications) encryption/decryption by selecting the Key ID using the Base Station keypad. The actual key material cannot be viewed or extracted from the Module.

Change Channel Parameters

If permitted in the Channel Setup loaded the Administrator/Crypto Officer, the User can change the parameters (frequencies etc.) for each channel.

Enable/Disable Encryption

If permitted in the Channel Setup loaded the Administrator/Crypto Officer, the User can enable or disable encryption on each channel.

Zeroize

To zeroize keys, the User must depress the “Shift” button on the Base Station key pad and then the “C” red button. The Base Station LCD displays a “Cryptogram” menu. Entering a “9” will cause the display of an “Are You Sure” message. Entering a “9” again will initiate zeroization. When zeroized, the Base Station-unique Key Encryption Key used to encrypt keys for internal storage is also erased. At next Base Station power up, the Base Station Module will generate a new KEK prior to storing new keys.

Input/Output Port Usage

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

	SERVICE	PORT	USAGE
Communication Services			
	• Clear/Encrypted Digital Data	RS-232 Serial Data	Data Output
		RS-232 Serial Data	Data Input
	• Clear/Encrypted Short Message Service	LCD Output	Data Output
		Keypad Input	Data Input
	• Clear Analog • Clear/Encrypted Digital Voice	External Speaker	Data Output
		External Microphone	Data Input
	• Clear/Encrypted Digital Data • Clear/Encrypted Short Message Service • Clear Analog • Clear/Encrypted Digital Voice	Antenna	Data Input/Output
Non-Communication Services			
	• Encryption Key Load	USB	Control Input
	• Firmware Load	USB	Control Input
	• PC Program-Channel Setup	RS-232 Serial Data	Control Input
	• Configure Licensed Options	USB	Control Input
	• Self-Test • Show Status • Select Encryption Key • Change Channel Parameters • Enable/Disable Encryption	LCD Output	Display Module Status
		Keypad Initiate	Control Input
	Zeroize	Keypad	Control Input

Table 4. Input/Output Port Usage

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.

Key Load

The primary access control should be to load only the encryption keys needed for a particular mission into a Base Station. This ensures that the Base Station can only communicate with others on the same mission, and limits the amount of key data that could be compromised if the Base Station was lost.

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 by a LCD "SECURE" indication 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.

Access Control

The first layer of protection in the Midland Base Station Crypto Module is physical access to the Base Station. Base Stations are typically installed in secure locations with access limited to authorized personnel. The Base Station includes several functions that require no authentication. For example, anyone with the applicable PC Programmer software, cable, and access to the Base Station can program the Base Station. However these are all proprietary items and even a modest, common sense access control policy for the Base Station and accessories will go a long way in securing Base Station operation.

Initial Installation

When the Base Station Module is first received and installed in a Base Station, the following steps must be followed to ensure compliance with FIPS and Midland Security Policy requirements:

1. **Zeroize (Administrator/Crypto Officer)** The Base Station 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 Base Station to develop a fresh Key Encryption Key to wrap the encryption keys with when entered.
2. **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 Module was manufactured. Since the firmware updates may address important Base Station performance and security issues, these updates must be installed prior to putting the Base Station into service. The Module will automatically authenticate the new firmware and will reject any firmware that is damaged or produced by anyone other than Midland Radio Corporation.
3. **Configure the Base Station Channels/Features (Administrator/Crypto Officer)** Attach a PC with the Midland Radio PC Programmer software installed to the Base Station. 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.
4. **Load Cryptographic Keys (Administrator/Crypto Officer)** Using the Midland PC Key Loader software application load keys into the Base Station. Up to two banks of 16 keys loaded into the Base Station. Either bank can be designated as AES or DES keys. The Base Station will store the keys internally in an AES key wrapped form and keys cannot be viewed or extracted from the Base Station after being entered.
5. **Cycle Power (Administrator/Crypto Officer)** Turn the Base Station off and then back on. A “test passed” indication will be briefly displayed on the Base Station LCD
6. **Test (Administrator/Crypto Officer)** Using a test set or a known good radio with the same channel configuration, verify the programming of the Base Station.
7. **Initiate Service (Administrator/Crypto Officer)** The Administrator can now issue the Base Station to the intended User.

Critical Security Parameters (CSPs)

The following table lists the Critical Security Parameters contained in the Base Station 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-Key is stored as the HMAC-DRBG 440 bit seed that produces the HMAC key and is stored when the Base Station is manufactured in flash memory in a split/interleaved form. 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 Base Station. The KEK is zeroized along with any Traffic Encryption Keys (TEKs). The KEK is stored as the 440 bit HMAC-DRBG seed that produces the KEK and is stored in flash memory in a split/interleaved form.	Stored Key Protection	Zeroize only	Zeroize only	Zeroize only
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 a default value of initialization that is recovered and checked on unwrapping thus verifying the integrity of the stored key material. TEKs are unwrapped at Base Station power on and are stored internally to the DSP in volatile memory and are lost once the Base Station is powered off.	Voice, Data, and SMS Encryption and Decryption	Use and zeroize only Cannot be extracted from Base Station Module	Load and zeroize only Cannot be extracted from Base Station Module	Zeroize only

Table 5. Critical Security Parameters

CHAPTER 4.0 Physical Security

TAMPER

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

ZEROIZE

The Midland Base Station can be zeroized by holding down both the "SHIFT" and "C" 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 Base Station 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 KEK is also erased on zeroization. The Base Station will automatically generate a new KEK when the Base Station is next powered on after a zeroizaton. The new KEK is generated using an Approved HMAC-DRBG algorithm and a 440 bit entropy source and is therefore unique to the Base Station and is different from any other KEK the Base Station has generated previously.

SUMMARY

The primary means of physical security for the Base Station is the possession of the device. A customer security policy should be based on ensuring that only authorized personal have access to the Base Station 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 Base Station, or having it repaired. The Base Station must be sent to Midland customer service for repair or replacement, and Midland as a policy clears all user data from the Base Station before performing any repair activities. In general a policy of limited Base Station, 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 Base Station does not contain any specific mitigation of other attacks.