
# Johnson Encryption Machine 2 (JEM2)

## Security Policy

**Hardware Version**: 023-3900-183

**Firmware Version**: 2.0

**Author**: Christopher G. Hruby

**Document Version:** 1.5

**Date:** January 23, 2009

# 1 Module Overview

The Johnson Encryption Machine 2 (JEM2) is a PCIe-based multi-chip embedded cryptographic module. The primary purpose for this device is to provide cryptographic services to a host computer for the purpose of supporting Project 25 (P25) infrastructure equipment such as dispatch consoles and key management facilities. The JEM2 includes those services necessary to support FIPS-140-2 validated encryption and decryption of P25 voice and data and key management and storage. The JEM2 also includes non-validated legacy services to support P25 DES encryption operation.

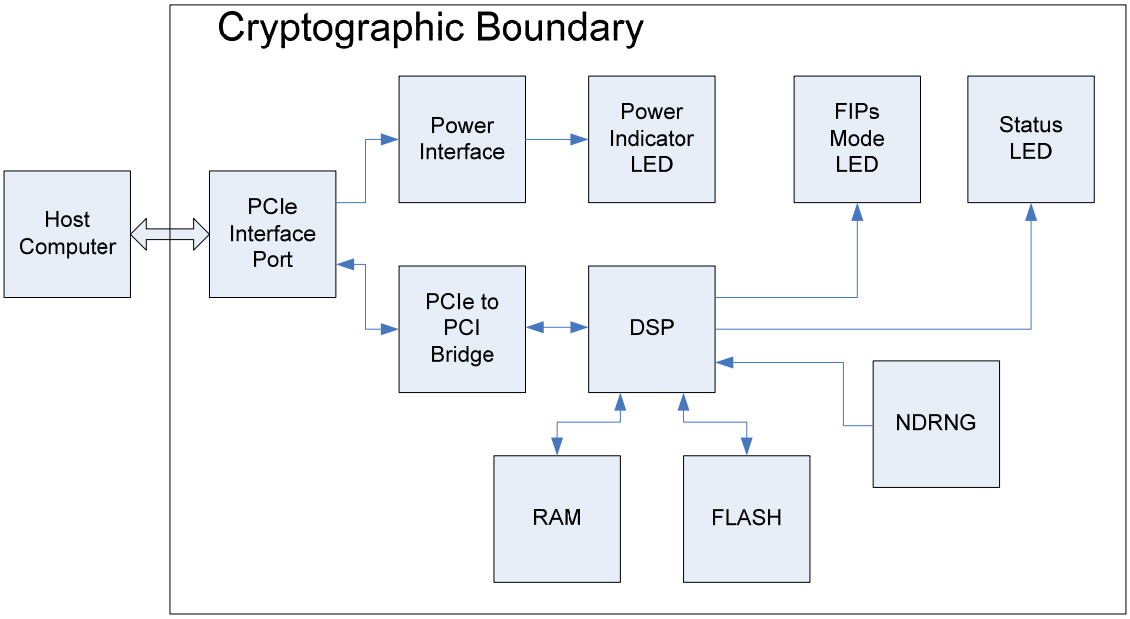
The JEM2 is designed to meet all applicable requirements of FIPS-140-2 for Level 1 security. The security rules specified in this document include rules derived from the FIPS-140-2 standard as well as requirements imposed by EJ Johnson.

The JEM2 crypto module (Hardware Version 023-3900-183, Firmware Version 2.0) is a multi-chip embedded module consisting of several integrated circuits and additional discrete components that are assembled onto a printed circuit board. The operator can determine the correct firmware version by reading the DCB and confirming the correct version. The operator can determine the correct hardware version by reading the printed version off the board.

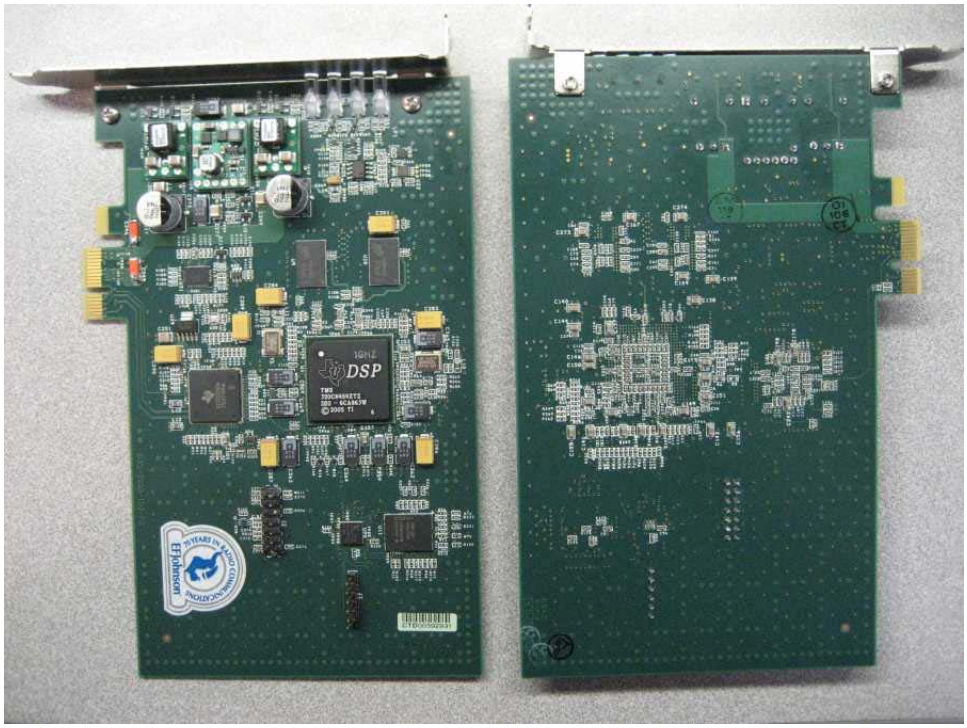
The JEM2 is a PCIe card that is designed to be installed into a compatible host computer. The JEM2 receives its power from the computer's PCIe interface port. The JEM2 communicates with the host computer through the PCIe interface. Processing is done on a digital signal processor (DSP). The JEM2 contains both volatile and non-volatile memory. Non-volatile memory stores the executable code of the DSP and the cryptographic keys of the JEM2 key store. The JEM2 will transfer both the executable code and the contents of the key store from non-volatile to volatile memory after power-up. Status output is provided via LEDs. A hardware NDRNG circuit provides random data.

The cryptographic boundary of the JEM2 encompasses the JEM2 PCB and all the hardware, software and firmware components contained therein. No components within the confines of the JEM2 PCB are excluded from the cryptographic boundary. Note that all cryptographic keys stored in the JEM2 key store are contained within the cryptographic boundary.

The following diagram shows the block diagram of the JEM2.




The following image is a photo of the JEM2.



# 2 Security Level

The JEM2 cryptomodule is designed to meet FIPS-140-2 Security Level 1 criteria. The JEM2 security level for each requirements section is shown in the following table.

| Requirements Section | Security Level |
|---|---|
| Cryptographic Module Specification | Level 1 |
| Module Ports and Interfaces | Level 1 |
| Roles, Services, and Authentication | Level 1 |
| Finite State Model | Level 1 |
| Physical Security | Level 1 |
| Operational Environment | N/A |
| Cryptographic Key Management | Level 1 |
| EMI/EMC | Level 1 |
| Self Tests | Level 1 |
| Design Assurance | Level 1 |
| Mitigation of Other Attacks | N/A |

# 3 Modes of Operation

The JEM2 supports a FIPS-140-2 approved operational mode and a non-approved operational mode. Each mode offers cryptographic services to support P25 infrastructure security requirements. The host can set the desired operational mode of the JEM2 by issuing a *Continue FIPS* or *Continue NonFIPS* command while the JEM2 device is in a stopped condition. CSPs are not shared between the approved and non-approved modes.

The following lists enumerate the security functions available in each operational mode of the JEM2.

**FIPS-140-2 Approved Operational Mode Security Functions**

***Approved Security Functions***

1. AES-256 ECB
2. AES-256 CBC
3. AES-256 OFB
4. AES-192 ECB
5. AES-192 CBC
6. AES-192 OFB
7. AES-128 ECB

8. AES-128 CBC
9. AES-128 OFB
10. DSA Signature Verification: SHA-1, 1024-bit key
11. SHA-1
12. SHA-256
13. SHA-512
14. HMAC: SHA-256
15. DRNG: FIPS 186-2 Appendix 3.1: 160-bit Xkey, SHA-1

***Non-Approved Security Functions (allowed for use in FIPS Approved Mode)***

1. AES Key Wrap (key establishment methodology provides between 128 and 256 bits of encryption strength)
2. AES MAC (vendor affirmed; P25 AES OTAR)
3. NDRNG (used to generate seed values for the Approved DRNG)

**Non-Approved Operational Mode Security Functions**

1. DES ECB
2. DES CBC
3. DES OFB

**Note:** All security functions available in the FIPS-140-2 approved mode are also available in the non-approved mode.

# 4 Ports and Interfaces

The JEM2 incorporates four physical ports and five logical interfaces. The physical ports are the PCIe connection to the host computer and the power indicator LED, FIPS mode LED, and status LED on the back of the JEM2 PCB. The five logical interfaces include the data input interface, data output interface, control input interface, status output interface, and power interface. The following table shows which physical port supports each logical interface.

| | | **Physical Ports** | | | |
|---|---|---|---|---|---|
| | | **PCIe** | **Power Indicator LED** | **FIPS Mode LED** | **Status LED** |
| **Logical Interfaces** | Data Input | X | | | |
| | Data Output | X | | | |
| | Control Input | X | | | |
| | Status Output | X | X | X | X |
| | Power Input | X | | | |

**Data Input Interface**

The data input interface transfers data over the PCIe port from the host to the JEM2. The data input interface is disabled during self-test and error states.

**Data Output Interface**

The data output interface transfers data over the PCIe port from the JEM2 to the host. The data output interface is disabled during self-test and error states.

**Control Input Interface**

The control input interface transfers control data over the PCIe port from the host to the JEM2. Control input is achieved through direct buffer commands and messaging header information.

**Status Output Interface**

The status output interface transfers status data over the PCIe port from the JEM2 to the host and sets physical indicator LEDs. Status output is achieved over the PCIe port through direct buffer status reports and messaging status codes. The power indicator LED indicates the device has power. The FIPS mode LED indicates whether the device is currently in FIPS approved or FIPS non-approved mode. The FIPS mode LED is green when the device is in FIPS approved mode and unlit when the device is in FIPS non-approved mode. The status LED indicates whether the device is currently running normally or is in an error state. The status LED is green when the device is in normal operation and red when the device is in an error state.

**Power Interface**

The power interface consists of the +12 V and +3.3 V pins on the PCIe port. These pins supply power to voltage regulator circuitry on the JEM2 PCB that creates additional voltages needed by the active components of the JEM2. Reset circuitry holds the DSP in reset during under-voltage conditions.

# 5 Identification and Authentication Policy

The JEM2 supports two operator roles (User and Cryptographic Officer), but does not support operator authentication. Since the two roles are separated procedurally, the following authentication parameters are not applicable: type of authentication, authentication data, authentication mechanism and strength of authentication mechanism.

# 6 Access Control Policy

## *6.1 Roles*

The JEM2 cryptomodule supports a user role and cryptographic officer role. The services associated with each role are summarized in the table included in this section.

**User Role**

The user role supports services associated with encryption and decryption of voice and data. The user role is implicitly assumed whenever the host requests a service associated with the user role.

**Crypto Officer Role**

The crypto officer role supports services associated with key management and firmware updates. The crypto officer role can generate, store, retrieve or delete keys, and can also update the JEM2

firmware. The crypto officer role is implicitly assumed whenever the host requests a service associated with the crypto officer role.

## 6.2 Critical Security Parameters

The JEM2 uses both symmetric and asymmetric cryptography. Symmetric keys for AES (including both traffic encryption keys (TEK) and key encryption keys (KEK)) and the key storage area key (KSAK) and are all stored in plaintext form in the flash and RAM memory inside the cryptographic boundary of the JEM2. The seed used by the FIPS 186-2 Appendix 3.1 DRNG is created through the hardware NDRNG. The state of the DRNG is stored in RAM memory. The JEM2 can store up to 65,536 AES keys. The JEM2 does not use or store any passwords or PINs. The JEM2 does not use or store asymmetric private keys.

**Definition of Critical Security Parameters (CSPs)**

The following are CSPs contained in the JEM2:

- AES Traffic Encryption Key (TEK): This is an AES key used to encrypt voice and data. Possible TEK sizes are 128-bit, 192-bit, and 256-bit.
- AES Key Encryption Key (KEK): This is an AES key used to encrypt TEKs and KEKs during the key management operations. Possible KEK sizes are 128-bit, 192-bit, and 256-bit. The KEK size must be greater than or equal to the size of the key to be encrypted.
- Key Storage Area Key (KSAK): This is used to compute the HMAC for a stored key. The KSAK is 256-bit.
- DRNG Seed: This is a FIPS 186-2 Appendix 3.1 DRNG seed used to generate pseudo-random numbers. The seed for the DRNG is obtained by sampling a hardware NDRNG circuit on the JEM2 device. This seed is used as the initial seed-key, XKEY. The optional user input seed, XSEED, is not used.

**Definition of Public Keys**

The following are public keys contained in the JEM2:

- DSA signature verification public key: This public key is used to verify the signature of the downloaded firmware.

**Definition of CSPs Modes of Access**

The relationship between access to CSPs and the different module services is shown in the table included in this section. The modes of access shown in the table are defined as follows:

- Associate Stored Key with Stream ID: Associate a stored key with a stream ID for subsequent crypto operations.
- Verify Key Exists: Verify that a key exists in the key store.
- Generate IV: Generate an Initialization Vector to initialize the encryption algorithm.
- Encrypt with TEK: Encrypt data using a TEK.
- Decrypt with TEK: Decrypt data using a TEK.

- Generate Key: Generate a random key.
- Delete Key: Delete key from key store.
- Unwrap Key with KEK: Decrypt a wrapped key with a KEK.
- Wrap Key with KEK: Encrypt a key with a KEK.
- Calculate HMAC with KSAK: Calculate the HMAC for a stored key with the KSAK.
- Generate DRNG Seed: Generate a random seed for the DRNG.
- Generate KSAK: Generate a random KSAK.
- Activate FIPS Approved Key Storage: Make the FIPS approved key storage area active.
- Activate FIPS Non-approved Key Storage: Make the FIPS non-approved key storage area active.
- Deactivate Key Storage: Deactivate the key storage area.
- Deactivate DRNG: Zeroize DRNG and deactivate.
- Verify Signature with public DSA Key: Calculate signature and verify provided signature using the public DSA key.
- Seed DRNG: Re-seeds the DRNG.
- Access DRNG: Access the DRNG to gather random data.

## *6.3 Services*

The JEM2 provides services to the host using a request/response based proprietary messaging protocol. The host will make a service request and the JEM2 will perform the service and issue a response to the host. For infrastructure operations that require multiple service calls for completion of the operation, a single stream ID is used for that operation. The JEM2 associates the stream ID with a particular key, algorithm state information, and other parameters. The JEM2 provides the services that are described in detail in the sections that follow and are summarized in the table included in this section.

**Note:** All the services below are also available in the non-approved mode of operation. In addition to the approved mode of operation services, the non-approved mode of operation offers the same services that require an AES key but with a DES key.

### 6.3.1 Load Key

The Load Key service commands the JEM2 to load an existing key from its key storage for subsequent use by other service commands. The desired key is specified by an index value that allows the JEM2 to retrieve the correct key from its key store and associate it with a stream ID for subsequent encryption or decryption operations. The JEM2 responds to this command by loading the desired key and issuing an acknowledgement, or by detecting and reporting an error.

### 6.3.2 Validate Key

The Validate Key service commands the JEM2 to verify the existence of a key in its key storage and report the results. The desired key is specified by an index value that allows the JEM2 to

identify the correct key and examine its properties. The JEM2 responds to this command by accessing the specified key and reporting success or failure at verifying the existence of the key.

### 6.3.3 Get Random Data

The Get Random Data Service commands the JEM2 to generate a specified number of cryptographic-quality pseudo-random bytes and return them to the host. The JEM2 responds to this command by generating the specified number of pseudo-random bytes and returning them, or by reporting an error if it is unable to generate the pseudo-random bytes.

### 6.3.4 Enter Voice Tx

The Enter Voice Tx Service commands the JEM2 to prepare for voice transmission. This service must be called prior to using any of the voice transmission related services: Encrypt LC, Encrypt Voice Frame, Encrypt LSD, Transcode Audio, and Generate Tone. If Encrypt LC, Encrypt Voice Frame, or Encrypt LSD are to used subsequently, the Load Key service must have been called prior to using this service. Use of Transcode Audio does not require a key therefore the Load Key service does not need to have been called prior. If subsequent Generate Tone service calls require encryption, the Load Key service must have been called prior to using this service. If specified in the service call, the JEM2 responds to this command by generating a 64-bit pseudo-random message indicator as specified in TIA-102.AAAD that is used as an initialization vector in the subsequent OFB encryption that follows. The JEM2 will return the generated MI if specified to the host, or report an error.

### 6.3.5 Encrypt LC

The Encrypt LC service commands the JEM2 to encrypt 9 bytes of link control data. The host supplies 9 bytes of plaintext link control data that the JEM2 encrypts and returns as 9 bytes of ciphertext data. This data is encrypted using AES in OFB mode as specified in TIA-102.AAAD. The Load Key service and Enter Voice Tx service must have been called prior to using this service. The JEM2 will return the ciphertext to the host, or report an error.

### 6.3.6 Encrypt Voice Frame

The Encrypt Voice Frame service commands the JEM2 to encrypt 11 bytes of IMBE digital voice data. The host supplies 20ms of audio data in one of three formats: 11 bytes of plaintext IMBE data, 160 8kHz 16-bit linear PCM audio samples, or 160 8kHz 8-bit mu-law compressed PCM audio samples. For formats other than IMBE data, the JEM2 will first encode the samples into IMBE data. The JEM2 will then encrypt the 11 bytes of plaintext IMBE data and return 11 bytes of ciphertext IMBE voice data. This data is encrypted using AES in OFB mode as specified in TIA-102.AAAD. The Load Key service and Enter Voice Tx service must have been called prior to using this service. The JEM2 will return the ciphertext to the host, or report an error. Periodically, as specified in TIA-102.AAAD, the JEM2 will also return the next 64-bit MI to the host, along with the 11 bytes of ciphertext.

### 6.3.7 Encrypt LSD

The Encrypt LSD service commands the JEM2 to encrypt 2 bytes of low speed data. The host supplies 2 bytes of plaintext low speed data that the JEM2 encrypts and returns as 2 bytes of ciphertext data. This data is encrypted using AES in OFB mode as specified in TIA-102.AAAD. The Load Key service and Enter Voice Tx service must have been called prior to using this service. The JEM2 will return the ciphertext to the host, or report an error.

### 6.3.8 Enter Voice Rx

The Enter Voice Rx service commands the JEM2 to prepare for voice reception. This service must be called prior to using any of the voice reception related services: Decrypt LC, Decrypt Voice Frame, Decrypt LSD, Set MI, and Transcode Audio. Except for the Transcode Audio service, the Load Key service must have been called prior to using this service. Use of Transcode Audio does not require a key therefore the Load Key service does not need to have been called prior. The host must supply the JEM2 with the 64-bit MI that has been received, except in the case where only Transcode Audio is called subsequently. The MI will be used as an initialization vector in the subsequent OFB decryption that follows. The JEM2 will acknowledge receipt of the MI, or report an error.

### 6.3.9 Decrypt LC

The Decrypt LC service commands the JEM2 to decrypt 9 bytes of link control data. The host supplies 9 bytes of ciphertext link control data that the JEM2 decrypts and returns as 9 bytes of plaintext data. This data is decrypted using AES in OFB mode as specified in TIA-102.AAAD. The Load Key service and Enter Voice Rx service must have been called prior to using this service. The JEM2 will return the plaintext to the host, or report an error.

### 6.3.10 Decrypt Voice Frame

The Decrypt Voice Frame service commands the JEM2 to decrypt 11 bytes of IMBE digital voice data. The host supplies 11 bytes of ciphertext IMBE digital voice data that the JEM2 decrypts. This data is decrypted using AES in OFB mode as specified in TIA-102.AAAD. The Load Key service and Enter Voice Rx service must have been called prior to using this service. The JEM2 will return plaintext data to the host in the specified format, or report an error. The returned plaintext data will be 20ms of audio data in one of three formats: 11 bytes of plaintext IMBE data, 160 8kHz 16-bit linear PCM audio samples, or 160 8kHz 8-bit mu-law compressed PCM audio samples. Periodically, as specified in TIA-102.AAAD, the host may supply a received 64-bit MI to the JEM2, along with the 11 bytes of ciphertext.

### 6.3.11 Decrypt LSD

The Decrypt LSD service commands the JEM2 to decrypt 2 bytes of low speed data. The host supplies 2 bytes of ciphertext low speed data that the JEM2 decrypts and returns as 2 bytes of plaintext data. This data is decrypted using AES in OFB mode as specified in TIA-102.AAAD. The Load Key service and Enter Voice Rx service must have been called prior to using this service. The JEM2 will return the plaintext to the host, or report an error.

### 6.3.12 Set MI

The Set MI service commands the JEM2 to set the 64-bit MI to the value supplied by the host. This service provides an alternate way to load the MI, which is customarily loaded using the Enter Voice Rx service or Decrypt Voice Frame service. The JEM2 will accept the supplied MI and return and acknowledgement to the host, or report an error.

### 6.3.13 Transcode Audio

The Transcode Audio service commands the JEM2 to convert audio data from one format to another format. This service does not provide encryption or decryption functionality. The host supplies 20ms of audio data in one format and specifies the desired format of the returned audio data. The allowed formats are: 11 bytes of plaintext IMBE data, 160 8kHz 16-bit linear PCM

audio samples, or 160 8kHz 8-bit mu-law compressed PCM audio samples. The JEM2 will return 20ms of audio data in the specified format, or report an error.

### 6.3.14 Generate Tone

The Generate Tone service commands the JEM2 to generate a 20ms frame of IMBE digital voice data containing a specified tone which is optionally encrypted. If specified, the JEM2 will encrypt the 11 bytes of generated IMBE data using AES in OFB mode as specified in TIA-102.AAAD. If encryption is to be performed, the Load Key service must have been called prior to using this service. The Enter Voice Tx service must always be called prior to using this service. The JEM2 will return the plaintext or ciphertext to the host, or report an error. Periodically, as specified in TIA-102.AAAD, the JEM2 will also return the next 64-bit MI to the host, along with the 11 bytes of ciphertext.

### 6.3.15 Encrypt Data

The Encrypt Data service commands the JEM2 to encrypt a variable amount of data. The host supplies a variable amount of plaintext data (along with the length of the data) that the JEM2 encrypts and returns as ciphertext data. This data is encrypted using AES in OFB mode as specified in TIA-102.AAAD. The Load Key service must have been called prior to using this service. The host can optionally request the JEM2 to generate a 64-bit MI to accompany the ciphertext. The JEM2 will return the ciphertext and the optional MI to the host, or report an error.

### 6.3.16 Decrypt Data

The Decrypt Data service commands the JEM2 to decrypt a variable amount of data. The host supplies a variable amount of ciphertext data (along with the length of the data) that the JEM2 decrypts and returns as plaintext data. This data is decrypted using AES in OFB mode as specified in TIA-102.AAAD. The Load Key service must have been called prior to using this service. The host can optionally supply the JEM2 with a 64-bit MI to accompany the ciphertext. The JEM2 will return the plaintext to the host, or report an error.

### 6.3.17 Create Random Key

The Create Random Key service commands the JEM2 to generate a 256 bit AES pseudo-random key using the JEM2's DRNG and place it into its key store. The host provides an index value that instructs the JEM2 where to store the key. The JEM2 responds to this command by generating a 256 bit AES pseudo-random key, placing it in the key store and issuing an acknowledgement, or by reporting an error. The seed generation for the DRNG is discussed in the critical security parameters section.

### 6.3.18 Store Key

The Store Key service commands the JEM2 to accept a (plaintext or ciphertext) key from the host and place it into the key store. The host supplies a key and an index that tells the JEM2 where to store the key. If the key is encrypted with the AES Key Wrap algorithm, the host also supplies the index of a key encryption key that the JEM2 will use to decrypt the encrypted key before placing it into the key store. The JEM2 responds to this command by (decrypting an encrypted key), placing it into the key store and issuing an acknowledgement, or by reporting an error.

### 6.3.19 Delete Key

The Delete Key service commands the JEM2 to delete the key specified by the index provided by the host. The JEM2 responds to this command by deleting the specified key from the key store and issuing an acknowledgement, or by reporting an error.

### 6.3.20 Encrypt Key

The Encrypt Key service commands the JEM2 to retrieve a key from the key store, encrypt the key and supply the encrypted key to the host. The host supplies an index that tells the JEM2 where to retrieve the key. The host also supplies the index of a key encryption key that the JEM2 will use to encrypt the retrieved key before sending it to the host. The JEM2 responds to this command by retrieving the specified key from the key store, encrypting the key with the AES Key Wrap algorithm using the specified KEK and supplying the encrypted key to the host, or by reporting an error.

### 6.3.21 Calculate MAC

The Calculate MAC service commands the JEM2 to accept a variable length message and a key index and use the specified key to compute a 64-bit MAC of the message. The JEM2 responds to this command by using the specified key and the AES cipher in CBC mode to compute the MAC as specified in TIA-120.AACA-1. Once calculated, the JEM2 returns the 64-bit MAC to the host, or reports an error. Note that this algorithm is only allowed to be used within OTAR.

### 6.3.22 Clear Key Database (Zeroize)

The Clear Key Database service commands the JEM2 to zeroize all keys and CSPs within the cryptographic boundary of the JEM2.

### 6.3.23 Set Special Key

The Set Special Key service commands the JEM2 to create a copy of an existing key in it key store. The host supplies an index for the existing key to copy and an index of where to store the copy. The JEM2 responds to this command by copying the existing key to the new index and returning an acknowledgement to the host, or by reporting an error.

### 6.3.24 Test Load Key

The Test Load Key service commands the JEM2 to load an existing key from its key storage for use in algorithm tests. The desired key is specified by an index value that allows the JEM2 to retrieve the correct key from its key store and associate it with a stream ID for subsequent encryption or decryption operations. The host also specifies the mode of operation and an initialization vector. The JEM2 responds to this command by loading the desired key and issuing an acknowledgement, or by reporting an error.

### 6.3.25 Test Encrypt

The Test Encrypt service commands the JEM2 to encrypt 16 bytes of test data. The host supplies 16 bytes plaintext data that the JEM2 encrypts and returns as ciphertext data. The Test Load Key service must have been called prior to using this service. The JEM2 will return the ciphertext to the host, or report an error.

### 6.3.26 Test Decrypt

The Test Decrypt service commands the JEM2 to decrypt 16 bytes of test data. The host supplies 16 bytes of ciphertext data that the JEM2 decrypts and returns as plaintext data. The Test Load Key service must have been called prior to using this service. The JEM2 will return the plaintext to the host, or report an error.

### 6.3.27 Test DRNG

The Test DRNG Service commands the JEM2 to generate a cryptographic-quality pseudo-random number and return it to the host. The host supplies parameters for seeding and iterating the DRNG. The JEM2 responds to this command by generating a pseudo-random number and returning it, or by reporting an error if it is unable to generate the pseudo-random number.

### 6.3.28 Test Hash

The Test Hash service commands the JEM2 to generate a hash and return it to the host. The host specifies the hash algorithm to use (SHA-1, SHA-256, or SHA-512) and supplies the data. The JEM2 will return the hash to the host, or report an error.

### 6.3.29 Test HMAC

The Test HMAC service commands the JEM2 to generate an HMAC (using SHA-256) and return it to the host. The host supplies the key and data to perform the HMAC algorithm on. The JEM2 will return the HMAC to the host, or report an error.

### 6.3.30 Test DSA

The Test DSA service commands the JEM2 to verify a digital signature. The host supplies the parameters for the DSA algorithm, the text, and signature. The JEM2 will verify the signature. The JEM2 will return whether the signature is verified, or report an error.

### 6.3.31 Test RNG

The Test RNG service commands the JEM2 to retrieve random data from the JEM2's hardware NDRNG and return them to the host. The JEM2 responds to this command by retrieving raw samples from the hardware NDRNG and processing those samples into random bits and returning them, or by reporting an error if it is unable to generate the random data.

### 6.3.32 Test Bias RNG

The Test Bias RNG Service commands the JEM2 to retrieve raw (unprocessed) samples data from the JEM2's hardware NDRNG and return them to the host. The JEM2 responds to this command by retrieving raw samples from the hardware NDRNG and returning them, or by reporting an error if it is unable to generate the random data.

### 6.3.33 Continue FIPS

The Continue FIPS service commands the JEM2 to enter its FIPS approved mode of operation. The JEM2 responds to this service by going into its FIPS approved mode of operation. The JEM2 will signal the host that it has successfully entered its FIPS approved mode of operation.

### 6.3.34 Continue NonFIPS

The Continue NonFIPS service commands the JEM2 to enter its FIPS non-approved mode of operation. The JEM2 responds to this service by going into its FIPS non-approved mode of

operation. The JEM2 will signal the host that it has successfully entered its FIPS non-approved mode of operation.

### 6.3.35 Stop

The Stop service commands the JEM2 to go into a stopped state. The JEM2 responds to this service by going into a stopped state where it will only process the Continue FIPS, Continue NonFIPS, and Code Update services. The JEM2 will signal the host that it successfully entered its stopped state.

### 6.3.36 Code Update

The Code Update service allows the crypto officer to provide the JEM2 with a digitally signed firmware update that the JEM2 will verify and authenticate. If the signature verifies and the firmware update is authentic then the JEM2 will update its firmware as requested and report success. If the signature fails to verify or if the operation does not successfully complete, the JEM2 will report an error. Note only EF Johnson can generate valid signatures.

### 6.3.37 Self-Test

The Self-Test service commands the JEM2 to perform the power-up tests to verify proper secure operation. All JEM2 cryptographic and security functions are tested using known answer tests. When the self-tests are complete the JEM2 will report success or failure.

**Note:** The Self-Test Service is initiated by cycling power or resetting the JEM2.

### 6.3.38 Show Status

The Show Status Service commands the JEM2 to display its current status and mode of operation. Status is returned at completion of each service. The status LED also indicates the status of the device.

**Note:** The Show Status Service is inherent in the operation of the JEM2 and is not an explicit service.

## *6.4 Summary of Services*

The following table summarizes:

- Services Authorized for Roles
- Specification of Service Inputs and Outputs
- CSP Access Rights within Services

| Service Name | Algorithms Used | Key Parameters | Inputs & Outputs | | | | Role | | CSP Access |
|---|---|---|---|---|---|---|---|---|---|
| | | | Control Input | Data Input | Data Output | Status Output | User | CO | |
| Load Key | None | 256 AES<br>192 AES<br>128 AES | Header Info | Key Index | None | Success/ Fail | X | | Associate Stored Key with Stream ID |
| Validate Key | None | 256 AES<br>192 AES<br>128 AES | Header Info | Key Index | None | Success/ Fail | X | | Verify Key Exists |
| Get Random Data | DRNG | None | Header Info | None | DRNG output data | Success/ Fail | X | | None<br>Access DRNG |
| Enter Voice Tx | DRNG | 64 IV | Header Info | None | MI data | Success/ Fail | X | | Generate IV<br>Access DRNG |
| Encrypt LC | AES OFB | 256 AES | Header Info | Plaintext LC data | Ciphertext LC data | Success/ Fail | X | | Encrypt with TEK |
| Encrypt Voice Frame | AES OFB | 256 AES | Header Info | Plaintext voice data | - MI data<br>- Ciphertext voice data | Success/ Fail | X | | Encrypt with TEK |
| Encrypt LSD | AES OFB | 256 AES | Header Info | Plaintext LSD data | Ciphertext LSD data | Success/ Fail | X | | Encrypt with TEK |
| Enter Voice Rx | None | 64 IV | Header Info | MI data | None | Success/ Fail | X | | None |
| Decrypt LC | AES OFB | 256 AES | Header Info | Ciphertext LC data | Plaintext LC data | Success/ Fail | X | | Decrypt with TEK |
| Decrypt Voice Frame | AES OFB | 256 AES | Header Info | - MI data<br>- Ciphertext voice data | Plaintext Voice data | Success/ Fail | X | | Decrypt with TEK |
| Decrypt LSD | AES OFB | 256 AES | Header Info | Ciphertext LSD data | Plaintext LSD data | Success/ Fail | X | | Decrypt with TEK |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Set MI | None | 64 IV | Header Info | MI data | None | Success/ Fail | X | | None |
| Transcode Audio | None | None | Header Info | Plaintext voice data | Plaintext voice data | Success/ Fail | X | | None |
| Generate Tone | AES OFB | 256 AES | Header Info | Tone parameters | - MI data<br>- Plaintext or Ciphertext voice data | Success/ Fail | X | | Encrypt with TEK |
| Encrypt Data | AES OFB | 256 AES | Header Info | Plaintext data | - MI data<br>- Ciphertext data | Success/ Fail | X | | Generate IV<br>Encrypt with TEK<br>Access DRNG |
| Decrypt Data | AES OFB | 256 AES | Header Info | - MI data<br>- Ciphertext data | Plaintext data | Success/ Fail | X | | Decrypt with TEK |
| Create Random Key | DRNG | 256 AES | Header Info | Key Index | None | Success/ Fail | | X | Generate Key<br>Access DRNG |
| Store Key | AES Key Wrap | 256 AES | Header Info | - Key Index for key to store<br>- Key Index for KEK<br>- Key data | None | Success/ Fail | | X | Unwrap Key with KEK<br>Calculate HMAC with KSAK |
| Delete Key | None | 256 AES | Header Info | Key Index | None | Success/ Fail | | X | Delete Key |
| Encrypt Key | AES Key Wrap | 256 AES | Header Info | - Key Index for key to encrypt<br>- Key Index for KEK | Ciphertext key data | Success/ Fail | X | | Wrap Key with KEK |
| Calculate MAC | AES CBC | 256 AES | Header Info | - Key Index<br>- Plaintext data | MAC data | Success/ Fail | X | | Encrypt with Key |
| Clear Key Database (Zeroize) | None | All | Header Info | None | None | Success/ Fail | | X | Delete Key<br>Generate DRNG Seed |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Seed DRNG |
| Set Special Key | None | 256 AES<br>192 AES<br>128 AES | Header Info | - Key Index for existing key<br>- Key Index for copied key | None | Success/ Fail | | X | Calculate HMAC with KSAK |
| Test Load Key | None | 256 AES<br>192 AES<br>128 AES | Header Info | - Key Index<br>- IV | None | Success/ Fail | | X | Associate Stored Key with Stream ID |
| Test Encrypt | AES ECB<br>AES CBC<br>AES OFB | 256 AES<br>192 AES<br>128 AES | Header Info | Plaintext data | Ciphertext data | Success/ Fail | | X | Encrypt with TEK |
| Test Decrypt | AES ECB<br>AES CBC<br>AES OFB | 256 AES<br>192 AES<br>128 AES | Header Info | Ciphertext data | Plaintext data | Success/ Fail | | X | Decrypt with TEK |
| Test DRNG | DRNG | None | Header Info | - Modulus data<br>- Seed data | DRNG output data | Success/ Fail | | X | Generate DRNG Seed<br>Seed DRNG |
| Test Hash | SHA-1<br>SHA-256<br>SHA-512 | None | Header Info | Data to be hashed | Hash output data | Success/ Fail | | X | None |
| Test HMAC | HMAC<br>SHA-256 | 256 HMAC | Header Info | - HMAC key<br>- Data to perform HMAC on | MAC data | Success/ Fail | | X | None |
| Test DSA | DSA<br>SHA-1 | 1024 DSA | Header Info | - Signature parameters<br>- Data to be signed<br>- Expected signature | Signature valid/non-valid | Success/ Fail | | X | None |
| Test RNG | None | None | Header Info | None | NDRNG debiased | Success/ | | X | None |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | output data | Fail | | | |
| Test Bias RNG | None | None | Header Info | None | NDRNG raw output samples | Success/ Fail | | X | None |
| Continue FIPS | DRNG<br>HMAC<br>SHA-512 | 256 HMAC | Command | None | None | Success/ Fail<br>FIPS LED | | X | Generate DRNG Seed<br>Generate KSAK<br>Activate FIPS Approved Key Storage<br>Calculate HMAC with KSAK<br>Seed DRNG |
| Continue NonFIPS | DRNG<br>HMAC<br>SHA-512 | 256 HMAC | Command | None | None | Success/ Fail<br>FIPS LED | | X | Generate DRNG Seed<br>Generate KSAK<br>Activate FIPS Non-Approved Key Storage<br>Calculate HMAC with KSAK<br>Seed DRNG |
| Stop | DRNG | none | Command | None | None | Success/ Fail | | X | Deactivate DRNG<br>Deactivate Key Storage |
| Code Update | DSA<br>SHA-1 | 1024 DSA | Command | Firmware data | None | Success/ Fail | | X | Verify Signature with public DSA key |
| Self-test | All | All | - Not an explicit service<br>- Inherent to device<br>- Self-initiated on reset | None | None | Success/ Fail | X | X | None |
| Show Status | None | None | - Not an explicit service<br>- Inherent to device | None | None | Success/ Fail | X | X | None |

# 7 Operational Environment

The FIPS-140-2 operational environment requirements are not applicable because the JEM2 does not contain a modifiable operational environment.

# 8 Security Rules

The design of the JEM2 corresponds to the security rules specified in FIPS-140-2 and the additional rules imposed by EF Johnson. This section documents the security rules enforced by the JEM2.

1. The JEM2 provides two distinct operator roles: user and the crypto officer.
2. The JEM2 performs the following tests:
    - Power-Up Self-Tests
        - RAM Test: this is a critical function test
        - Software/Firmware Integrity Test: software integrity is verified using SHA-512
        - Cryptographic Algorithm Tests
            - AES encrypt/decrypt KAT: KATs are performed for AES 256, 192, and 128 in the Electronic Codebook (ECB) mode.
            - SHA-1 KAT
            - SHA-256 KAT
            - SHA-512 KAT
            - HMAC-SHA-256 KAT
            - DSA signature verification KAT
            - DRNG KAT
    - Conditional Self-Tests
        - Firmware Verification Test (Software/Firmware Load Test): During code update, the DSA code signature is verified before applying the code update
        - Key Integrity Test: the integrity of each key and its associated parameters are verified using the key storage key with HMAC-SHA-256. This is a critical function test.
        - DRNG Continuous Test: test is performed over 20 bytes
        - NDRNG Continuous Test: test is performed over 20 bytes
3. Data output is inhibited during self-tests, zeroization, and error states.
4. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
5. The JEM2 does not support concurrent operators or maintenance operators.

6. The JEM2 is incorporated into a host computer that is part of a Project 25 infrastructure. An authorized user of the host has the ability to select either a FIPS-140-2 approved mode of operation or a non-approved mode of operation for the JEM2. Critical Security Parameters are segregated for approved and non-approved modes of operation, and only the applicable set of Critical Security Parameters are in use at any given time.
7. The JEM2 FIPS-140-2 approved mode of operation provides AES cryptographic services for current Project 25 infrastructure systems. The JEM2 non-approved mode of operation provides DES cryptographic services for legacy Project 25 infrastructure systems.
8. When operating in the FIPS-140-2 approved mode, the JEM2 uses the AES block cipher as specified in FIPS-197 for encryption and decryption of voice and data, and AES CBC MAC.
9. When operating in the FIPS-140-2 approved mode, the JEM2 uses the AES Key Wrap Algorithm as specified in RFC-3394 for encryption and decryption of cryptographic keys.
10. When operating in the FIPS-140-2 approved mode, the JEM2 uses the DRNG specified in FIPS186-2 Appendix 3.1 as amended in Change Notice 1 of 5-October-2005 to generate cryptographic-quality pseudo-random numbers.
11. When operating in the FIPS-140-2 approved mode, the JEM2 uses the SHA-1 hash function as specified in FIPS-180-2 and the DSA signature algorithm as specified in FIPS-186-2 as amended in Change Notice 1 of 5-October-2005 to verify digital signatures of firmware updates.
12. When operating in the non-approved mode, the JEM2 uses the DES block cipher for encryption and decryption of voice and data.
13. The JEM2 provides for storage of keys (both traffic encryption keys and key encryption keys) in plaintext form within the cryptographic boundary of the JEM2.
14. The JEM2 has an LED output indicator that informs the user of the status of the crypto module and its operating mode (FIPS-140-2 approved or non-approved).

# 9 Physical Security Policy

The JEM2 is a multi-chip embedded cryptographic module that uses commercial-grade production components. Since the JEM2 is designed to meet the requirements of FIPS-140-2 Security Level 1, it does not employ environmental failure protection (EFP) features nor will it undergo environmental failure testing (EFT). The operator is not required to perform any physical security inspections.

# 10 Mitigation of Other Attacks

The JEM2 is not designed to mitigate against other attacks not specifically mentioned in this document, including but not limited to power analysis, timing analysis, fault indication or TEMPEST.

# 11 References

The following external documents contain information relevant to this document, the inclusions of which are incorporated by reference herein.

1. FIPS-140-2 Security Requirements for Cryptographic Modules
2. Implementation Guidance for FIPS-140-2 and the CMVP 5/22/08
3. FIPS-180-3 DRAFT 6/12/07 Secure Hash Standard (SHS)
4. FIPS-186-2 Digital Signature Standard (DSS)
5. FIPS-186-3 Digital Signature Standard (DSS)
6. FIPS-197 Advanced Encryption Standard
7. FIPS-198-1 DRAFT 6/8/07 Keyed-Hash Message Authentication Code (HMAC)
8. SP-800-38-A Recommendation for Block Cipher Modes of Operation - Methods and Techniques
9. SP-800-56-A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
10. SP-800-57 Recommendation for Key Management
11. SP-800-90 Recommendation for Random Number Generation Using Deterministic Random Bit Generators
12. RFC-3394 Advanced Encryption Standard (AES) Key Wrap Algorithm
13. TIA-102.AAAB-A Security Services Overview
14. TIA-102.AAAD Block Encryption Protocol
15. TIA-102.AACA-1 Key Management Security Requirements

# 12 Definitions and Acronyms

The following acronyms and abbreviations may appear in this document:

| | |
|---|---|
| **AES** | Advanced Encryption Standard |
| **CBC** | Cipher Block Chaining |
| **CMVP** | Cryptographic Module Validation Program |
| **CSP** | Critical Security Parameter |
| **DCB** | Device Control Block |
| **DES** | Data Encryption Standard |
| **DRNG** | Deterministic Random Number Generator |
| **DSA** | Digital Signature Algorithm |
| **DSP** | Digital Signal Processor |
| **DSS** | Digital Signature Standard |
| **DTR** | Derived Test Requirements |
| **ECB** | Electronic Codebook |
| **EDC** | Error Detection Code |

| | |
|---|---|
| **EFP** | Environmental Failure Protection |
| **EFT** | Environmental Failure Testing |
| **EMC** | Electromagnetic Compatibility |
| **EMI** | Electromagnetic Interference |
| **ESYNC** | Encryption Synchronization |
| **FCC** | Federal Communications Commission |
| **FIPS** | Federal Information Processing Standard |
| **HMAC** | Hash-Based Message Authentication Code |
| **IC** | Integrated Circuit |
| **IMBE** | Improved Multi-Band Exciter (P25 standard vocoder) |
| **IV** | Initialization Vector |
| **JEM2** | Johnson Encryption Machine 2 |
| **KAT** | Known Answer Test |
| **KEK** | Key Encryption Key |
| **KSAK** | Key Storage Area Key |
| **LC** | Link Control |
| **LED** | Light Emitting Diode |
| **LSD** | Low Speed Data |
| **MAC** | Message Authentication Code |
| **MI** | Message Indicator |
| **NDRNG** | Non-Deterministic Random Number Generator |
| **NIST** | National Institute of Standards and Technology |
| **OFB** | Output Feedback |
| **OTAR** | Over-the-Air Rekeying |
| **PCB** | Printed Circuit Board |
| **PCI** | Peripheral Component Interconnect |
| **PIN** | Personal Identification Number |
| **RAM** | Random Access Memory |
| **RFC** | Request For Comments |
| **RNG** | Random Number Generator |
| **ROM** | Read-Only Memory |
| **SHA** | Secure Hash Algorithm |
| **SHS** | Secure Hash Standard |

**TIA** Telecommunications Industry Association

**TEK** Traffic Encryption Key