



Security Policy of the Kenwood Cryptographic Module

Author: John Batenhorst

Part Number: KWD-AE40

Hardware Version: 1

Firmware Version: 1.0.0

Date: 10/9/2024

Table of Contents

1	General	3
2	Cryptographic Module Specification	3
3	Cryptographic Module Interfaces.....	7
4	Roles, Services and Authentication	8
5	Software/Firmware Security	14
6	Operational Environment.....	15
7	Physical Security	15
8	Non-invasive Security	18
9	Sensitive Security Parameter Management.....	18
9.1	Generation	20
9.2	Entry.....	21
9.3	Output	21
9.4	Storage	21
9.5	Zeroization	21
10	Self-Tests	22
10.1	Pre-Operational Self-Tests	23
10.1.1	Pre-Operational Software/Firmware Integrity Test	23
10.2	Conditional Self-Tests.....	24
10.2.1	Conditional Cryptographic Algorithm Self-Tests	24
10.2.2	Software/Firmware Load Tests	25
10.2.3	Periodic Self-Tests	25
11	Life-Cycle Assurance	25
12	Mitigation of Other Attacks.....	26

1 General

This document is a non-proprietary FIPS 140-3 Security Policy for the EF Johnson Technologies’ Kenwood Cryptographic Module (KCM) version hardware version 1, firmware version 1.0.0. The KCM is a Level 3 hardware cryptographic module. Table 1 describes the security level of each section in this document.

Table 1: Security Levels

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	Level 3
2	Cryptographic Module Specification	Level 3
3	Cryptographic Module Interfaces	Level 3
4	Roles, Services and Authentication	Level 3
5	Software/Firmware Security	Level 3
6	Operational Environment	N/A
7	Physical Security	Level 3
8	Non-invasive Security	N/A
9	Sensitive Security Parameter Management	Level 3
10	Self-Tests	Level 3
11	Life-Cycle Assurance	Level 3
12	Mitigation of Other Attacks	N/A

2 Cryptographic Module Specification

The KCM is a multi-chip embedded FIPS 140-3 hardware cryptographic module. It provides access to basic cryptographic algorithms with available long-term key storage within the module itself. This module is intended for use cases where the additional security provided by a level 3 module is needed. The KCM has been designed for installation in Kenwood land mobile radio transceivers to provide them with secure storage for encryption keys and the cryptographic services needed for operation on encrypted P25 systems.

The cryptographic boundary of the KCM encompasses the entire KCM PCB and all hardware and firmware components contained therein. No components found on the KCM PCB are excluded from the

cryptographic boundary. Any keys stored in the module by a user reside in the boundary. The physical form of the Module is depicted in Figure 1.

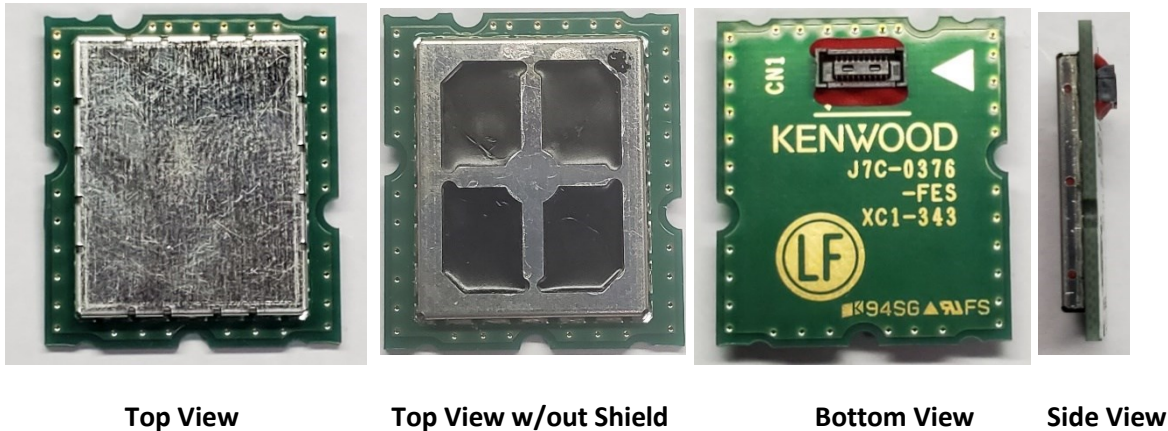


Figure 1: KCM Physical Form

The module itself consists of several ICs and discrete components installed on a PCB. An ARM-based microcontroller on the PCB holds the module’s firmware in FLASH memory. Table 2 lists the operating hardware and firmware versions for which the KCM has been tested.

Table 2: Cryptographic Module Tested Configuration

Module	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
Kenwood Cryptographic Module (KCM)	KWD-AE40 Hardware Version 1	V1.0.0	

The overall security rating of this module is Level 3.

The KCM only operates in a single mode of operation. This is an approved mode and is entered automatically KCM is powered on or reset. If a failure occurs, the module enters a failure mode which cannot be exited except by power-cycling or resetting the module. Other than the failure mode, the module does not operate in any degraded modes.

Table 3 lists the security functions provided by the KCM.

Table 3: Approved Algorithms

CAVP Cert.	Algorithm and Standard	Mode/Method	Description/Key Size(s)/ Key Strength(s)	Use/Function
A2717	AES-CBC SP 800-38A	CBC	128, 192, 256	Encryption, Decryption
A2717	AES-ECB SP 800-38A FIPS 197	ECB	128, 192, 256	Encryption, Decryption
A2717	AES-KW (KTS) SP 800-38F	KW	128, 192, 256	Wrap, Unwrap SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G. 128 and 256-bit keys providing 128 or 256 bits of encryption strength
A2717	AES-OFB SP 800-38A	OFB	128, 192, 256	Encryption, Decryption
A2717	Hash DRBG SP 800-90Arev1	Hash DRBG	SHA2-512, no PR	Random Number Generation
A2717	HMAC-SHA2-512 FIPS 198-1	HMAC	SHA2-512	Verification
A2717	SHA2-512 FIPS 180-4	SHA2	SHA2-512	Hash
C1327	AES-CMAC SP 800-38B	Generation	128	Entropy Conditioning
N/A	ENT (P) SP 800-90B	N/A	N/A	DRBG Seed – 384 bits of entropy
Vendor Affirmed	CKG SP 800-133rev2	SP 800-133rev2 Section 6.1 Key Generation Method	128, 192, or 256	Key generation using direct output of approved DRBG

Table 4 Lists the non-approved algorithms supported by the KCM.

Table 4: Non-Approved Algorithms Allowed in the Approved Mode of Operation

Algorithm	Caveat	Use/Function
AES-CBC-MAC	Only allowed for use within OTAR per IG D.C	TIA-102.AACA-B P25 OTAR

The AES-CBC-MAC algorithm is provided for interoperability with the P25 OTAR standard. The algorithm uses AES keys and AES block encryption in a way that will not lead to the disclosure of the encryption keys.

The module does not implement any non-approved (not allowed) algorithms.

Figure 2 depicts the KCM logical block diagram in an operational context.

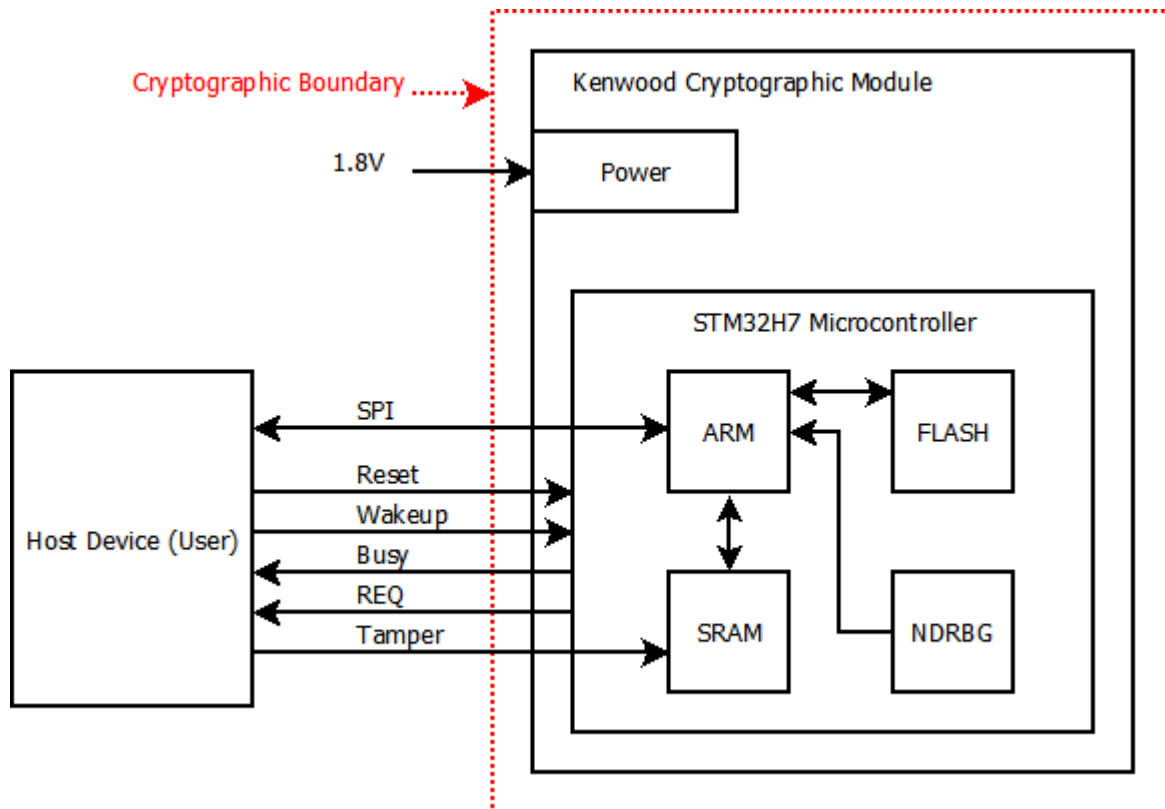


Figure 2: KCM Block Diagram

The security design and rules of operation are as follows: The module’s circuitry is protected against unauthorized modifications and tampering. A multi-pin connector on the module’s PCB is used to supply the module with power and allow bidirectional communication between the user and the module. This connector is the only interface to the module, allowing data to be passed across the cryptographic boundary. The specifics of the physical and logical interfaces available through the multi-pin connector are detailed in Section 3. After the module is initialized, users are required to assume an authenticated role in order to use cryptographic services and access CSPs. The bulk of user communication with the module is done using a proprietary serial messaging protocol. Data input, output, status, and most control for the module is done using the messaging protocol. When the module detects a critical error, it enters the failure state, and all cryptographic services will be unavailable until the module is power cycled or reset. The module initializes itself atomically on power on or reset, including all self-tests, integrity checks, and DRBG seeding. See Section 10 for a description of the self-tests that are run on load.

3 Cryptographic Module Interfaces

Table 5 lists the KCM’s ports and associated FIPS logical interfaces.

Table 5: Ports and Interfaces

Physical Port	Logical Interface	Data that passes over port/interface
SPI	Data Input Data Output Status Output Control Input	User data Status requests/responses Cryptographic service requests/responses Configuration requests/responses Firmware updates
Busy	Status Output	Indicates the KCM is ready to receive input
REQ	Status Output	Indicates the KCM has data to send
Wakeup	Control Input	Wakes/suspends the module
Tamper	Control Input	Indicates physical disconnection from user
Reset	Control Input	Resets the module without disconnecting power

The module does not utilize a trusted channel. Instead, all CSPs sent to or received from the module are encrypted with approved cryptographic algorithms. The module does not input or output plaintext CSPs.

Data input and output, some forms of status, and some forms of control input and output are done over SPI using a proprietary serial messaging protocol. The module will not respond to any incoming user requests or output data over SPI until it completes any task currently in progress, including pre-operational self-tests, zeroization, firmware load tests, and firmware upgrades. If the module goes into the failure mode, the output interface is disabled with a couple exceptions: User requests over SPI for the module’s status or the contents of the error log will still elicit a response from the module even while the module is in the error state since neither of those requests utilize cryptographic algorithms, and responses will not contain any sensitive information.

The SPI messages sent and received by the module are uniquely defined to logically separate the logical interfaces utilizing SPI.

4 Roles, Services and Authentication

The KCM supports the Crypto Officer role, a User role, and an Unauthenticated User role. There is no maintenance role. Authentication is required for the Crypto Officer and User roles, and the Unauthenticated User role requires no authentication. The module supports only a single operator assuming one of these roles.

Table 6 lists the KCM’s Roles and their available services.

Table 6: Roles, Service Commands, Input and Output

Role	Service	Input	Output
Crypto Officer	Firmware Update	MAC Encrypted Firmware	Success/Fail
User	Generate Random Value	Length	Random bytes
User	Import Keys	AES Key	Key Storage Identifier
User	AES Encryption	Plaintext Data	Ciphertext Data
User	AES Decryption	Ciphertext Data	Plaintext Data
User	Generate Random Key	Key Length	Key Storage Identifier

User	AES Key Wrap	Key Storage Identifier	Wrapped AES Key
User	Module Configuration	Configuration Settings	Configuration Settings
User	OTAR MAC Calculate	Key Storage Identifier Data Bytes	KMM MAC
User	P25 LLA Calculate	Key Storage Identifier Mode Seed Challenge	Response
User	Erase Key	Key Storage Identifier	N/A
User	Erase Keys of Length	Key Length	Zeroization Indicator
User	Clear Error Log	N/A	N/A
User Unauthenticated User	Zeroize	N/A	Zeroization Indicator
User Unauthenticated User	Reset Password	Password	Success/Fail
User Unauthenticated User	Get Status	N/A	Module Name Firmware Version Module Status
User Unauthenticated User	Show Version	N/A	Firmware Version
User Unauthenticated User	Get Error Log	N/A	Error Log
User Unauthenticated User	Reset	N/A	N/A
User Unauthenticated User	Wake/Suspend	N/A	N/A
Unauthenticated User	Self-Tests	N/A	Self-Tests Result
Unauthenticated User	User Login	Password	Success/Fail

Table 7 Lists the KCM's authorized roles and their associated authentication requirements.


	TITLE: Security Policy of the Kenwood Cryptographic Module		
	HARDWARE VERSION: 1	FIRMWARE VERSION: 1.0.0	DATE: 10/9/2024

Table 7: Roles and Authentication

Role	Authentication Method	Authentication Strength
Crypto Officer	Identity-based HMAC-SHA2-512	512-bit HMAC for Firmware Update Service Probability: $1/2^{512}$ Probability over one-minute period: $14,000/2^{512}$
User	Identity-based Password	32-digit hexadecimal number Probability: $1/16^{32}$ Probability over one-minute period: $5/16^{32}$

There are no ways to bypass any of these capabilities, and there is no self-initiated cryptographic output capability.

The KCM can receive firmware updates, and these can be initiated by the Crypto Officer role any time after the successful completion of the self-tests. More information about the firmware update process can be found in Section 5.

The KCM supports only approved services and always operates in an approved mode. Approved services indicate their use by toggling hardware lines and sending serial messages conforming to the proprietary serial messaging protocol. Services indicated through serial messages have message payloads that are uniquely defined based on the service performed. All approved services provided by the KCM are listed in Table 8.

Table 8: Approved Services

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs*	Indicator
Firmware Update	Update the KCM firmware	HMAC-SHA2-512 AES-OFB	FVHK FVDK	Crypto Officer	W, E W, E	Serial Message Response
Generate Random Value	Use previously seeded DRBG	Hash DRBG	DRBG V DRBG C	User	W, E E	Serial Message Response



TITLE: Security Policy of the Kenwood Cryptographic Module

HARDWARE VERSION:
1

FIRMWARE VERSION:
1.0.0

DATE: 10/9/2024

Import Keys	Store wrapped AES key in KCM's FLASH or RAM	AES-KW	AES Key KSK KFK	User	W, E E E	Serial Message Response
AES Encryption	Encrypt blocks of data	AES-CBC AES-ECB AES-KW AES-OFB	AES Key KSK	User	E E	Serial Message Response
AES Decryption	Decrypt blocks of data	AES-CBC AES-ECB AES-KW AES-OFB	AES Key KSK	User	E E	Serial Message Response
Generate Random Key	Generates a Key from random bits	Hash DRBG AES-KW CKG	DRBG V DRBG C KSK AES Key	User	W, E E E G, W	Serial Message Response
AES Key Wrap	Exports wrapped AES key	AES-KW	AES Key KSK	User	E, R E	Serial Message Response
OTAR MAC Calculate	Calculate the KMM MAC as specified by the P25 standard	AES-CBC-MAC	AES Key KSK	User	E E	Serial Message Response
P25 LLA Calculate	Calculate the response to a P25 LLA challenge	N/A	AES Key KSK	User	E E	Serial Message Response
Module Configuration	Configure the module	N/A	N/A	User Unauthenticated User		Serial Message Response
Zeroize	Clear DRBG, stored keys, stored password hash	Hash DRBG SHA2-512 CKG	KSK Password Hash Entropy Input DRBG Seed DRBG V DRBG C	User Unauthenticated User	Z, G, W Z Z, G, W Z, G, W Z, G, W Z, G, W	Serial Message Response



TITLE: Security Policy of the Kenwood Cryptographic Module

HARDWARE VERSION:
1

FIRMWARE VERSION:
1.0.0

DATE: 10/9/2024

Get Status	Return module name, firmware version, hardware version, and status	N/A	N/A	User Unauthenticated User	-	Serial Message Response
Show Version	Return module name, firmware version, hardware version, and status	N/A	N/A	User Unauthenticated User	-	Serial Message Response
Get Error Log	Returns the most recent error	N/A	N/A	User Unauthenticated User	-	Serial Message Response
Clear Error Log	Clears the error log	N/A	N/A	User	-	Serial Message Response
Self-Tests	Runs cryptographic algorithm self-tests and verifies integrity of module firmware	AES-KW AES-CMAC ENT (P) Hash DRBG HMAC-SHA2-512 SHA2-512	N/A	Unauthenticated User	-	Serial Message
User Login	Allows a user to authenticate with the module	AES-OFB SHA2-512	PWK Password Password Hash	Unauthenticated User	E Z, W R	Serial Message Response
Reset Password	Zeroize the module and set a new username and password	AES-OFB SHA2-512 Hash DRBG CKG	PWK Password Password Hash KSK Entropy Input DRBG Seed DRBG V DRBG C	Unauthenticated User	E Z, W W Z, G, W Z, G, W Z, G, W Z, G, W	Serial Message Response



TITLE: Security Policy of the Kenwood Cryptographic Module

HARDWARE VERSION:
1

FIRMWARE VERSION:
1.0.0

DATE: 10/9/2024

Erase Key	Makes keys unavailable to the user. Keys still exist in module memory until zeroized	N/A	N/A	User	-	Serial Message Response
Erase Keys of Length	Zeroizes all keys of specified length	Hash DRBG CKG	KSK	User	Z, G, W	Serial Message Response
Reset	Reboots the module	N/A	Entropy Input DRBG Seed DRBG V DRBG C	User Unauthenticated User	Z, G, W Z, G, W Z, G, W Z, G, W	Serial Message
Wake/ Suspend	Command the module to enter or leave low power mode	N/A	N/A	User Unauthenticated User	-	Busy Line

**These access rights are defined as follows: (G)enerate, (R)ead, (W)rite, (E)xecute, and (Z)eroise.*

Installation requires connecting the KCM’s hardware lines to provide power, control, and to communicate with the module.

A single Crypto Officer is supported by the module and is able perform firmware updates, and that identity and role is authenticated using an approved keyed-hash message authentication code when a firmware update service is accessed. The User is identified and authenticated using a password that can be configured by the Unauthenticated User role. Switching between either of these authenticated roles requires that the operator authenticate as required by that role. The state of the operator’s authentication is held in volatile memory and will be cleared when the module is powered cycled or reset, requiring the operator to reauthenticate the next time they assume an authenticated role.

Firmware is authenticated using the HMAC algorithm. The probability of a successful random attempt is 2^{512} , which is less than 1 in 1,000,000. The module is capable of processing no more than 14,000 firmware updates in a one-minute period, so the probability of a successful random attempt in a one minute period is 14,000 in 2^{512} which is less than 1 in 1,000,000.

A single authenticated User is supported by the module; any time the password is reset, the module is zeroized. If an operator fails to authenticate with a password five times sequentially, the module will be zeroized, and the password will need to be reset for the User role. The password reset service is also used to establish authentication data for the User role on new modules where no authentication data for that role has been set previously.

Passwords sent to the module are encrypted using an approved encryption method. The password is a memorized secret but does not adhere to all SP800-63B requirements for authentication assurance level 1. The KCM is designed to interact with another device, not a human user, so protections against compromised or weak ascii passwords are not present in the module. Passwords are 32-digit hexadecimal numbers, chosen by the device utilizing the KCM. A new password is hashed and stored in the KCM's memory using an approved hash function, and the hashes are used to authenticate users on subsequent authentication requests. Password hashes are not salted since the module has no way to separately store the salt from the hash inside the module's boundary. Instead, the hashes are protected in the module's memory by the module's firmware and the physical security mechanisms described in Section 7. The password length allows for 16^{32} possible passwords, so the possibility of a successful random attempt is 1 in 16^{32} , which is less than 1 in 1,000,000. Since the module allows for 5 failed password attempts, the probability of a successful random attempt in a one-minute period is 5 in 16^{32} which is less than 1 in 1,000,000.

5 Software/Firmware Security

The KCM automatically performs an integrity check on its executable code when powered on or reset. It computes a hash of the executable code in FLASH and compares it to an expected value that was written when the module's firmware was installed. If the two match, the integrity check passes. Otherwise, the module enters a failed state, and requests made to the module will either be ignored, or the module will respond with a message indicating an error condition. Any service utilizing a cryptographic algorithm will be unavailable.

The operator can initiate this integrity check on demand by power cycling or resetting the module.

Firmware updates are provided in the form of an encrypted firmware file and an HMAC. The keys used to encrypt the firmware and calculate the HMAC are known only to the KCM and the firmware author,



TITLE: Security Policy of the Kenwood Cryptographic Module

HARDWARE VERSION:
1

FIRMWARE VERSION:
1.0.0

DATE: 10/9/2024

EF Johnson. These keys are loaded into the module when an approved firmware is installed. Firmware updates are provided to the module using the proprietary SPI messaging protocol. When the module is provided with a firmware update, the update file is saved into volatile memory where the module decrypts it with its firmware decryption key. Then it performs a firmware load test by calculating an HMAC over the decrypted update file using its firmware HMAC key. If the HMAC calculated by the module matches the HMAC provided by the user, then the test is passed, and the update is understood to be a genuine update provided by EF Johnson. The module then replaces its executable code stored in FLASH with the updated code contained in the firmware file and resets. If the HMAC calculated by the module does not match the one provided by the user, the test is failed. The module will return an error to the user, and the firmware update will not be applied.

Any applied firmware update with a version that does not match what appears on the FIPS 140-3 validation certificate is outside the scope of this validation and requires a separate FIPS 140-3 validation.

This module is not open source.

6 Operational Environment

The KCM operates in a limited operational environment. The module can receive firmware updates, and firmware versions validated under FIPS 140-3 will appear on a validation certificate. Installing any firmware version not appearing in this Security Policy will result in the KCM operating in a non-compliant state.

7 Physical Security

Table 9 lays out the KCM's Physical Security Mechanisms.


	TITLE: Security Policy of the Kenwood Cryptographic Module		
	HARDWARE VERSION: 1	FIRMWARE VERSION: 1.0.0	DATE: 10/9/2024

Table 9: Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper-evident encapsulating material	Inspect before putting module into service. Further inspections may be conducted at the user’s discretion.	Look for damage to the epoxy coating on the module’s PCB. Any attempts to remove the epoxy coating have a high probability of damaging the module. If the epoxy coating shows damage but the module is still functioning, zeroize the module, remove it from service, and contact EF Johnson for assistance.
Tamper Line	Test before putting module into service. Routine tests may be conducted at the user’s discretion.	Set up user login credentials and configure module to store SSPs in volatile memory. Import a key to the module, then disconnect and reconnect power and the tamper line. After logging in, attempt to encrypt with the previously imported key – this will fail because the tamper event erased the key.

The KCM is a multi-chip embedded cryptographic module consisting of production grade components designed to meet Level 3 physical security requirements. All circuitry and components are protected by a hard, opaque epoxy coating that cannot be removed or penetrated without causing serious damage to the module. This coating discourages modifications and will show evidence if any such modifications are attempted.

Table 10 lays out the KCM’s environmental failure testing and protections.


	TITLE: Security Policy of the Kenwood Cryptographic Module		
	HARDWARE VERSION: 1	FIRMWARE VERSION: 1.0.0	DATE: 10/9/2024

Table 10: EFP/EFT

	Temperature or voltage measurement	Specify EFP or EFT	Specify if this condition results in shutdown or zeroization
Low Temperature	≤ -35°C	EFP	Shutdown
High Temperature	≥ +65°C	EFP	Shutdown
Low Voltage	< 1.62V	EFP	Shutdown
High Voltage	≥ 2.10V	EFP	Shutdown

Supply voltage and ambient temperature are monitored by the module. Exceeding the acceptable thresholds for either voltage or temperature will result in the module entering the failure state, and all cryptographic services will be unavailable until the module is power cycled or reset after temperature and voltage conditions return to an acceptable level.

Table 11 shows the temperatures extremes at which the epoxy coating has been tested for adequate hardness.

Table 11: Hardness testing temperature Ranges

	Hardness tested temperature measurement
Low Temperature	-30°C
High Temperature	+60°C

The module does not have any removable doors, covers, maintenance interface, or ventilation holes or slits that can be used to gain information about the module’s construction, components, or SSPs. The module does feature a tamper line that is used to retain a subset of SSPs in volatile memory. Loss of power to this line will result in the loss of any SSPs stored in that volatile memory. It should be noted that this tamper line is not used to meet any physical security requirements for a level 3 multi-chip embedded cryptographic module; those requirements are met by the epoxy coating.

No actions are required by users to maintain the module’s physical security mechanisms.

8 Non-invasive Security

No steps to mitigate non-invasive attacks have been made.

9 Sensitive Security Parameter Management

Table 12 lays out the KCM managed sensitive security parameters (SSPs).

Table 12: Sensitive Security Parameters (SSPs)

Key/SSP Name/Type	Strength	Security Function & Cert. Number	Generation	Import/Export	Establish-ment	Storage	Zeroisation	Use & Related Keys
AES Key	128, 192 or 256 bits	AES-ECB AES-CBC AES-OFB Cert# A2717 AES-CBC-MAC	Generate Random Key service using raw DRBG output	Input and output KTS using AES-KW	N/A	AES-KW Encrypted FLASH or Plaintext RAM	Zeroize for all keys ¹ , Reset Password for all keys ⁵ , power off or reset for RAM keys ³ , Erase Keys of Length for specified keys ⁴	AES Encryption, AES Decryption, Import Keys, AES Key Wrap, Generate Random Key, OTAR MAC Calculate, P25 LLA Calculate
KSK (Key Storage Key)	256-bits	AES-KW Cert# A2717	Generated using raw DRBG output	N/A	N/A	Plaintext FLASH or Plaintext Backup RAM	Zeroize ¹ , Reset Password ⁵ , tamper event ³ , Erase Keys of Length for specified keys ⁴	AES Encryption, AES Decryption, Import Keys, Generate Random Key, AES Key Wrap, OTAR MAC Calculate, P25 LLA Calculate



TITLE: Security Policy of the Kenwood Cryptographic Module

HARDWARE VERSION:
1

FIRMWARE VERSION:
1.0.0

DATE: 10/9/2024

KFK (Keyfill Key)	256-bits	AES-KW Cert# A2717	Pre-loaded	N/A	N/A	Plaintext FLASH	Firmware Update ²	Import Keys
PWK (Password Key)	256-bits	AES-OFB Cert# A2717	Pre-loaded	N/A	N/A	Plaintext FLASH	Firmware Update ²	User Login
Password	16 bytes	N/A	N/A	Input encrypted with AES-OFB	N/A	Plaintext RAM	Zeroize ¹ , power off ³ , Reset ³ , Reset Password ⁵	User Login
Password Hash	256-bits	SHA2- 512 Cert# A2717	Reset Password	N/A	N/A	Plaintext FLASH	Zeroize ¹ , Reset Password ⁵	User Login
FWDK (Firmware Decryption Key)	256-bits	AES-OFB Cert# A2717	Pre-loaded	N/A	N/A	Plaintext FLASH	Firmware Update ²	Firmware Update
FWHK (Firmware HMAC Key)	512-bits	HMAC- SHA2- 512 Cert# A2717	Pre-loaded	N/A	N/A	Plaintext FLASH	Firmware Update ²	Firmware Update
Entropy Input	384-bits	Hash DRBG Cert# A2717 ENT (P)	Generated per SP 800- 90B	N/A	N/A	Plaintext RAM	Zeroize ¹ , power off ³ , Reset ³ , Reset Password ⁵	Initialize DRBG V and C states
DRBG Seed	384-bits	Hash DRBG Cert# A2717 ENT (P)	Generated per SP 800- 90B	N/A	N/A	Plaintext RAM	Zeroize ¹ , power off ³ , Reset ³ , Reset Password ⁵	Initialize DRBG V and C states

DRBG V	256-bits	Hash DRBG Cert# A2717	Derived per SP 800- 90Arev1	N/A	N/A	Plaintext RAM	Zeroize ¹ , power off ³ , Reset ³ , Reset Password ⁵	Generate Random Value, Generate Random Key
DRBG C	256-bits	Hash DRBG Cert# A2717	Derived per SP 800- 90Arev1	N/A	N/A	Plaintext RAM	Zeroize ¹ , power off ³ , Reset ³ , Reset Password ⁵	Generate Random Value, Generate Random Key

1. *Explicitly zeroized by zeroization service – a uniquely defined message is sent by the module to indicate successful completion of the zeroize service.*
2. *Explicitly zeroized by firmware update – a uniquely defined message is sent by the module to indicate successful completion of the firmware update.*
3. *Implicitly zeroized when the volatile memory holding the SSP loses power.*
4. *Explicitly zeroized by Erase Keys of Length service – a uniquely defined message is sent by the module to indicate successful completion of the service.*
5. *Explicitly zeroized by Reset Password service – a uniquely defined message is sent by the module to indicate successful completion of the service.*

Table 13 lays out the KCM entropy sources.

Table 13: Non-Deterministic Random Number Generation Specification

Entropy Sources	Minimum number of bits of entropy	Details
Hardware RBG	384	Component of the module’s microcontroller using an analog entropy source conditioned by a SP800-90B approved conditioning state. One bit of entropy is output per bit output.

9.1 Generation

The approved random bit generator is a SHA2-512 DRBG. The source of entropy is a hardware random bit generator provided by the module’s microcontroller. The state of the DRBG exists in volatile memory only and is cleared when the module is powered off or reset. Any generated SSPs are created using unmodified output from this DRBG.

AES keys can be generated by the module at the request of the user.

9.2 Entry

All SSPs imported by the module by a user are sent through the module's serial messaging protocol and are protected by approved cryptographic methods. For the purpose of input using AES-OFB, the module utilizes manual distribution using electronic entry as per IG 9.5.A.

9.3 Output

All SSPs exported by the module by a user are sent through the module's serial messaging protocol and are protected by approved cryptographic methods.

9.4 Storage

All SSPs are stored in either volatile (RAM or backup RAM) or non-volatile (FLASH) memory.

An AES key can either be stored in volatile or non-volatile memory at the discretion of the user. AES keys stored in volatile memory are cleared when the module is zeroized, powered off, or reset. Keys stored in non-volatile memory are encrypted using the AES key wrapping algorithm with Key Storage Keys (KSKs) generated by the module. KSKs can be stored either in volatile or non-volatile memory at the discretion of the user.

Passwords are chosen by users and are not stored by the module. The module does generate a hash of the password using SHA2-512 which is stored in non-volatile memory.

9.5 Zeroization

The zeroize service is invoked using the module's serial messaging protocol. The module is always in approved mode.

The zeroize service will erase the KSKs, which will render the AES keys wrapped by them unrecoverable. The password hash and internal state of the DRBG are also erased. A uniquely defined serial message is returned by the module to indicate successful completion of the zeroize service.

KSKs stored in volatile memory can also be cleared by a tamper event, which occurs when the module's tamper line loses power.

AES keys stored in volatile memory can also be cleared by resetting the module or removing main power.

The FWDK, FWHK, PWK, and KFK are bound to the module’s firmware and can only be cleared by updating the module’s firmware. The module indicates completion of the firmware update by returning a uniquely defined serial message indicating successful completion of its pre-operational self-tests.

SSPs stored in the module are protected by the module’s physical security measures detailed in Section 7 and the user authentication requirements detailed in Section 4. Unauthenticated users do have the ability to zeroize the module using the zeroize service.

10 Self-Tests

The module runs pre-operational and conditional self-tests automatically on power up or reset, and the module operator can initiate these self-tests on demand by power cycling or resetting the module.

The module does not have or test any critical functions other than those that are tested as described in the subsections below.

If a test fails, the module enters the error state. Subsequent service requests made to the module will either be ignored, or the module will respond with a message indicating an error condition. Any service utilizing a cryptographic algorithm will be unavailable.

The module has a single error state that it enters in the event of an error, and it maintains an error log that contains what error event most recently occurred. Authorized roles can retrieve the error log, but roles must be authenticated in order to clear it. Table 14 contains the error codes that may be recorded by the module when an error occurs causing it to enter the error state.

Table 14: Error Code Values

Value (Hex)	Error	Reason
\$00	No Error	No error has occurred
\$01	AES Self Test Failed	The AES self test failed
\$02	DRBG Self Test Failed	The DRBG self test failed
\$03	HMAC Self Test Failed	The HMAC self test failed
\$04	Integrity Check Failed	Corruption was detected in the KCM's firmware
\$05	Stored Key Unwrap failed	A stored key could not be decrypted
\$06	Unexpected Load Key Failed	A KCM initiated key load operation failed
\$07	Unexpected Load Initialization Vector Failed	A KCM initiated initialization vector load operation failed
\$08	Unexpected Key Wrap Failed	A KCM initiated key wrap operation failed
\$09	Unexpected Encrypt Failed	A KCM initiated encryption operation failed
\$0A	Entropy Collection Failed	The KCM's RNG could not provide entropy
\$0B	DRBG Initialization Failed	The DRBG was unable to be seeded
\$0C	DRBG Reseed Required	The DRBG was unable to provide additional bytes
\$0D	Environmental Conditions Failure	The KCM's temperature and/or supply voltage exceeded its operational thresholds
\$0E	Flash Memory Failed	The KCM's flash memory could not be written

10.1 Pre-Operational Self-Tests

10.1.1 Pre-Operational Software/Firmware Integrity Test

The module performs only one pre-operational self-test:

- Firmware Integrity Test - Integrity check using SHA2-512

The integrity check is done by calculating the SHA2-512 hash of all the module's executable code in FLASH against an expected hash that was written when the module's firmware was installed. The SHA2-512

implementation is validated by the HMAC-SHA2-512 KAT. After the test, all temporary values are cleared by overwriting their memory with zeroed bytes.

10.2 Conditional Self-Tests

10.2.1 Conditional Cryptographic Algorithm Self-Tests

The module performs the cryptographic algorithm self-tests shown in Table 15:

Table 15: Conditional Cryptographic Algorithm Self Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SP 800-90B RCT	40 consecutive bits	Fault-Detection	CAST	Self test SPI message	Performed on raw data	Bootup
SP 800-90B APT	684 repeated bits in 1024-bit window	Fault-Detection	CAST	Self test SPI message	Performed on raw data	Bootup
AES-CMAC	128-bit key 256-bit Message 128-bit MAC	KAT	CAST	Self test SPI message	MAC Generate	Bootup
AES-KW (KTS)	128-bit key	KAT	CAST	Self test SPI message	Wrap	Bootup
AES-KW (KTS)	128-bit key	KAT	CAST	Self test SPI message	Unwrap	Bootup
Hash DRBG	888-bit entropy input 128-bit nonce Two 1024-bit requests	KAT	CAST	Self test SPI message	Instantiate, Generate	Bootup
HMAC-SHA2-512	512-bit key 272-bit text	KAT	CAST	Self test SPI message	MAC Generate	Bootup

The hardware RBG is initialized and performs a repetition count test (RCT), an adaptive proportion test (APT), and AES CMAC known answer tests (KAT). The RBG completes its initialization when all tests pass.

The AES test performs known answer tests (KAT) with a 128-bit key, one KAT for wrapping a key and another KAT for unwrapping a key, in order to test the AES forward and reverse functions. The Hash DRBG KAT test is also an SP 800-90Arev1, Section 11.3 health test for the instantiate and generate functions. The HMAC test is another KAT that tests the generation of an HMAC using a key and input data. Since the HMAC is implemented with SHA2-512, the HMAC KAT verifies the SHA2-512 capabilities of the module as well. After each test, all temporary values are cleared by overwriting their memory with zeroed bytes.

10.2.2 Software/Firmware Load Tests

When new firmware is transferred to the module, the module will validate it using HMAC-SHA2-512. The HMAC-SHA2-512 implementation is validated by the HMAC-SHA2-512 KAT. After the test, all temporary values are cleared by overwriting their memory with zeroed bytes. The firmware is not applied if this test fails.

10.2.3 Periodic Self-Tests

The hardware RBG continuously runs RCT and APT tests as random bits are generated to ensure the amount of entropy provided remains high.

Additionally, the integrity check is run approximately every 30 minutes to detect any modification to the module's code that may arise during its operation. This test happens in the background between user requests as to not interrupt the user experience; user requests may be briefly delayed by the test, and the test could be briefly delayed by user requests.

Lastly, the DRBG continuously keeps track of requests and will put the module into the error state when the number of requests exceeds 2^{48} . With the module's limited performance capabilities, such a condition would take several thousand years to occur even in extreme use cases.

11 Life-Cycle Assurance

Modules should be physically examined for signs of modifications or tampering, such as damage to the PCB or the epoxy protecting it. Any modules exhibiting such signs should not be put into service. The connections and interfaces needed to operate the KCM are specified in Section 3.

Modules should also have their firmware version checked to ensure that the installed firmware has been validated against FIPS 140-3, updating the firmware to a validated version if necessary. The firmware version is checked by requesting it from the module using the module's serial messaging protocol. The name, firmware version, and hardware version output by the module should match the information provided in Table 2. Updates to the module's firmware are also done using its serial messaging protocol. Installing any firmware version not appearing in this Security Policy will result in the KCM operating in a non-compliant state.

Modules will require that a user set up password to access approved services requiring authentication. Modules with existing user credentials can be zeroized to erase stored CSPs and allow a new user to establish their own login credentials. If a module is taken out of service or repurposed, it can be zeroized in order to erase all CSPs. The module requires no maintenance, and no administrator or non-administrator guidance is needed outside of the services available through the module's serial messaging protocol.

If users wish to securely destroy a module, it is recommended that the module be shredded into small pieces using an electronics shredder designed to destroy electronic storage mediums such as solid-state drives and hard disk drives.

12 Mitigation of Other Attacks

The KCM is not designed for the mitigation of any attacks outside the scope of FIPS 140-3 Level 3.