Security Policy:

Secure Cryptographic Module (SCM)

Document Version 2.1.2

FIPS 140-2 Non-Proprietary
Kenwood Corporation

May be reproduced only in its original entirety [without revision].

Revision History

Date	Revision	Author	Description
2006/01/12	1.0.0	Yuichi Hagiwara	Initial release.
2006/01/18	1.1.0	Yuichi Hagiwara	Updated indicating how to ensure that the module is operating in FIPS mode.
2006/01/25	1.1.1	Yuichi Hagiwara	Updated the operations of FIPS and non-FIPS mode.
2006/02/07	1.2.0	Yuichi Hagiwara	Reflected comments from InfoGard.
2006/02/14	1.3.0	Yuichi Hagiwara	Added Sleep Mode as a service delivered to the operator.
2006/02/16	1.3.1	Yuichi Hagiwara	Inserted company logo, modified contact information and module name.
2006/02/20	1.3.2	Yuichi Hagiwara	Reflected comments from Kenwood USA.
2006/03/01	1.4.0	Yuichi Hagiwara	Added Calibration Service, delivered to the operator.
2006/03/13	1.5.0	Yuichi Hagiwara	Reflected comments from InfoGard.
2006/03/23	1.5.1	Yuichi Hagiwara	Reflected additional comments from InfoGard.
2006/04/04	1.5.2	Yuichi Hagiwara	Reflected additional comments from InfoGard.
2006/04/04	1.5.3	Yuichi Hagiwara	Revision reflecting comments from InfoGard.
2006/09/01	1.5.4	Yuichi Hagiwara	Reflected comments from CMVP.
2006/10/05	1.5.5	Tamaki Shimamura	Reflected comments from CMVP.
2008/09/12	2.0.0	Tamaki Shimamura	Included firmware version A2.0.0 which supports AES/DES-OTAR and firmware upgrade.
2008/12/03	2.1.0	Tamaki Shimamura	Reflected comments from CMVP.
2010/02/18	2.1.1	Tamaki Shimamura	Included firmware version A2.0.1.
2010/08/10	2.1.2	Tamaki Shimamura	Included firmware version A2.0.2.

Table of Contents

1. Module Overview

The Secure Cryptographic Module (SCM) is a hardware cryptographic module developed by Kenwood Corporation to provide FIPS 140-2 validated cryptographic securities for the TK-5XX0 series FM/P25 digital two way radios and NX-/NXR- series NEXEDGE digital two way radios. This Security Policy was prepared as one of the requirements of FIPS 140-2. If you have any technical questions, feel free to contact to fips@kenwood.co.jp. For sales contact, feel free to contact to JWatts@kenwoodusa.com.

SCM part number: KWD-AE20, hardware version 1.0.0, firmware versions A1.0.0, A1.0.1 (FIPS 140-2 Cert. #711), A2.0.0, A2.0.1 (FIPS 140-2 Cert #1076), and A2.0.2 (FIPS 140-2 Cert # pending) is a hardware cryptographic module targeted for FIPS 140-2 Security Level 1 overall. In FIPS 140-2 terms, SCM is a multi-chip embedded module and the physically contiguous cryptographic boundary is defined as the PC board including all hardware and firmware components to perform cryptographic functions. All of the I/O is managed by the board-to-board connector the module employs.

Image 1 – The SCM

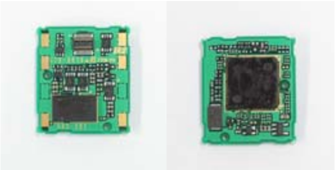

Table 1 - The module's function dependant on its firmware is as follows.

	FW ver. A1.0.0 and ver A1.0.1 (FIPS 140-2 Cert. #711)	FW ver. A2.0.0, ver A2.0.1 (FIPS 140-2 Cert #1076) FW ver A2.0.2 (FIPS 140-2 Cert # pending)	FIPS Approved
AES encryption	✓	✓	✓
DES encryption	✓	✓	
AES OTAR		✓	✓
DES OTAR		✓	
FW upgrade function		✓	✓[1]

[1] The targeted firmware to upgrade must be validated to FIPS 140-2.

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 2 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	3
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	1

3. Modes of Operation

The SCM cryptographic module employs both FIPS approved and non-FIPS approved modes of operation. By initializing AES encryption or decryption service, or AES-OTAR service with CBC-MAC or CMAC to confirm the KMM's integrity (both Legacy and Advanced), the module enters an ***Approved*** mode of operation. Any requests for DES encryption or decryption initialization service, or DES-OTAR service after AES/AES-OTAR services will result in the module transitioning to a ***non-Approved*** mode of operation, exiting the Approved mode of operation. An operator is capable of confirming the Approved mode of operation by calling the show-status function and verifying the bit flag given within the Cipher Status set to "1".

Approved Algorithms used in FIPS Approved Mode

The cryptographic module supports the following Approved algorithms in FIPS mode:

Table 3 - Approved Algorithms in FIPS Approved Mode

AES	As defined in **FIPS PUB 197** with 256 bit keys. FW version A2.0.0, A2.0.1, and A2.0.2 supports ECB, OFB, modes for encryption and decryption (AES Cert. #831)
AES CMAC (For use in Advanced AES-OTAR and SW/FW load test)	As defined in SP 800-38B and Project 25 TIA-102.AACA-1 for MAC generation and verification in Advanced AES-OTAR (AES CMAC), and SW/FW load test with modules loaded with FW version A2.0.0 A2.0.1, and A2.0.2 (AES Cert. #832).
SHA-256	As defined in **FIPS PUB 180-2** for creating message digests with 256 bits. SHA-256 (SHS Cert. #827) is provided for internal functions ***only***.

Non-Approved but Allowed Algorithms used in FIPS Approved Mode

The cryptographic module in FIPS Mode supports the following non-Approved algorithms:

Table 4 - Non-Approved but Allowed Algorithms in FIPS Approved Mode

AES OTAR (Legacy)	As defined in ANSI/TIA-102.AACA-1, "Project 25 – Digital Radio Over-the-Air-Rekeying (OTAR) Protocol Addendum 1 – Key Management Security Requirements for Type 3 Block Encryption Algorithms" using CBC-MAC based on AES (AES Cert. #831, vendor affirmed; P25 AES OTAR).

Non-Approved Algorithms in non-FIPS Mode

The cryptographic module supports the following non- Approved algorithms used in the non-FIPS mode:

Table 5 - Non-Approved Algorithms used in non-FIPS Approved Mode

DES	As defined in **FIPS PUB 46-3** with 56 bit keys. FW version A2.0.0, A2.0.1, and A2.0.2 supports ECB, OFB, and CBC mode.
DES-OTAR	As defined in TIA/EIA Telecommunications Systems Bulletin, “APCO Project 25, Over-The-Air-Rekeying (OTAR) Protocol”, New Technology Standards Project, Digital Radio Technical Standards, TSB102.AACA, January 1996
LFSR	The module employs a LFSR for generation of IV in OFB mode. The LFSR never generates encryption keys.

See Section 6 for Access Control Policy.

4. Ports and Interfaces

The SCM cryptographic module provides the following ports and interfaces:

- ■ 1 Board to board connector utilized for:
  - □ Data input
  - □ Data output
  - □ Control input
  - □ Status Output

The cryptographic module receives power from the radio system on which it executes.

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module supports both Crypto Officer and User role, implicitly selected by the operator from the services provided. The module does not support a maintenance role. The module keeps track of the radio it is utilized by, and upon detection of an invalid radio, it zeroizes all CSPs.

Table 6 - Roles and Required Identification and Authentication

Role	**Type of Authentication**	**Authentication Data**
User	N/A	N/A
Cryptographic-Officer	N/A	N/A

Table 7 - Strengths of Authentication Mechanisms

Authentication Mechanism	**Strength of Mechanism**
N/A	N/A

6. Access Control Policy

Roles and Services

Table 8 - Services Authorized for Roles

Role	Authorized Services
User: The entity that has access to all crypto related functions supported by the crypto module, including key entry.	• AES • AES-OTAR • DES • DES-OTAR • LFSR • Key entry • Sleep Mode / Wake Up
Cryptographic-Officer: The entity responsible for management activities including installing the module to the radio, deletion of keys, and checking status of the module.	• Show Status • Calibration Service • Key zeroization • Self tests • Firmware upgrade service

Service - Purpose and Use

Table 9 - Service name, purpose, and use

Service Name	Purpose and Use
AES	Allows Users to encrypt/decrypt data.
AES-OTAR	Allows Users to load encrypted AES keys automatically. Legacy and Advanced AES-OTAR is supported.
DES	Allows Users to encrypt/decrypt data.
DES-OTAR	Allows Users to load encrypted DES keys automatically.
LFSR	Allows Users to generate IV used in OFB mode.
Key entry	Allows Users to enter cryptographic keys in plaintext using a manual electronic method.
Sleep Mode / Wake Up	Minimize the power consumption of the module
Key zeroization	Allows Crypto Officers to zeroize keys in RAM and FLASH ROM of the module, excluding the AES Firmware key.
Self-tests	Allows Crypto Officers to perform self-tests.
Calibration Service	Allows Crypto Officers to calibrate the module’s timing.
Show Status	Allows Crypto Officers to let the module indicate its status.

Firmware Upgrade Service	Allows Crypto Officers to update FIPS validated firmware, or entering a hard error state by loading a zeroization firmware image, zeroizing all keys including the AES Firmware Key.

Definition of Critical Security Parameters (CSPs)

The following **CSP**s are contained in the module:

- **AES key (AES):** Used for encryption and decryption of data in ECB and OFB modes with 256 bit keys.
- **AES OTAR key (AEO):** Used for calculating the integrity of the KMM in CBC-MAC mode (Legacy AES-OTAR) and CMAC mode (Advanced AES-OTAR).
- **AES Firmware key (AEF):** Used for calculating the integrity of the firmware in CMAC mode.

Definition of Public and Private Keys

The module does not contain any public/private keys.

Definition of CSPs Modes of Access

Table 10 defines the relationship between access to **CSP**s and the different module services. The modes of access shown in the table are defined as follows:

- **Write:** a cryptographic key is entered to the module using a manual or automatic electronic method with its attributes, and stored.
- **Read:** a cryptographic key is used to perform cryptographic operations with AES (as described in Section 3 of this document).
- **Zeroize:** a cryptographic key is destroyed.

Table 10 - CSP Access Rights within Roles & Services

Role		**Service**	**Cryptographic Keys and CSPs Access Operation**		
C.O.	**User**		**AES**	**AEO**	**AEF**
	✓	AES	Read	N/A	N/A
	✓	AES-OTAR	Write, Zeroize	Read, Write, Zeroize	N/A
	✓	DES	N/A	N/A	N/A
	✓	DES-OTAR	N/A	N/A	N/A
	✓	LFSR	N/A	N/A	N/A
	✓	Key entry	Write	Write	N/A
	✓	Sleep Mode / Wake Up	N/A	N/A	N/A
✓		Zeroization	Zeroize	Zeroize	N/A

Role		Service	Cryptographic Keys and CSPs Access Operation		
C.O.	User		AES	AEO	AEF
✓		Self-Tests	N/A	N/A	N/A
✓		Calibration Service	N/A	N/A	N/A
✓		FW Upgrade Service	N/A	N/A	Read, Zeroize[2]
		Show Status	N/A	N/A	N/A

7. Operational Environment

This section is not applicable since the module executes within a limited operation environment with no General Purpose Operating System upon which the operation environment resides.

8. Security Rules

The cryptographic module corresponds to its Security Rules derived from FIPS 140-2 and Kenwood Corporation. This section documents the Security Rules enforced by the cryptographic module.

1. The cryptographic module shall provide two distinct operator roles. These are the User role, and the Cryptographic-Officer role.
2. The cryptographic module shall not provide operator authentication.
3. The cryptographic module shall provide authentication for the radio in which it is installed.
4. Keys shall be entered via electronic key entry using manual methods (e.g. use of a radio and a compatible key variable loader, with keys entered in plaintext), or via OTAR using automated methods (with keys entered encrypted in accordance with APCO OTAR methods).
5. All keys are stored in encrypted format with a key derived from the radio's input, though this is assumed to be plaintext in FIPS 140-2 context.
6. In order to initiate an Approved mode of operation, the module shall initialize encryption or decryption with the AES algorithm, or start AES-OTAR services.
7. DES must not be used in an Approved mode of operation.
8. The crypto officer must ensure that the new firmware to load is also validated to FIPS 140-2 when upgrading the module's firmware components[3].

[2] The AEF (AES Firmware Key) is zeroized by use of the FW Upgrade Service with a zeroization firmware image (all memory locations zeroized)

[3] Note that Kenwood will only use the hard-coded CMAC key to generate MACs for FIPS validated firmware and a special firmware that will transit the module to a hard error state: the SW/FW Load test

9. The cryptographic module shall not output any CSPs.
10. Keys shall only be entered or modified by authorized operators.
11. The module employs a tamper mechanism governed by an attribute setting of the infinite flag. When the infinite attribute flags are not set at the detection of a tamper result, the module shall zeroize all CSPs. If infinite flags are set when a tamper result is detected, the module will only zeroize the keys stored in RAM.[4]
12. The cryptographic module shall perform the following tests:
    A. Power up Self-Tests:
    1. Software/Firmware Integrity Test (CRC 16 bit)
    2. Cryptographic algorithm tests:
        a. AES Known Answer Test
        b. SHA-256 Known Answer Test
        c. AES CMAC Known Answer Test
    3. Critical Functions Tests:
        a. DES Known Answer Test
        b. LFSR Known Answer Test

    B. Conditional Self-Tests:
    1. Continuous Random Number Generator (RNG) test
       – performed on the LFSR
    2. Firmware Load test
       – performed when updating firmware components.

13. If self-tests fail, the module shall enter an error state. The status of self-tests shall be available via the show status service. The error condition is ascertained from the output, by the index of a bit flag marked by "1".
14. To perform an on-demand self-test, the operator must re-boot the module.
15. Prior to each use, the internal RNG (LFSR) shall be tested using the conditional test specified in FIPS 140-2 §4.9.2.
16. Data output shall be inhibited during self-tests, zeroization, and error states.
17. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
18. The cryptographic module shall not support concurrent operators.

will fail if the crypto officer tries to upgrade the module’s firmware with non-FIPS validated firmware components.

[4] The implementation of the tamper mechanism is not intended to meet the Physical Security Requirements of FIPS 140-2.

19. The cryptographic module shall inhibit cryptographic operations and data output in all error states.

9. Physical Security Policy

Physical Security Mechanisms

All of the components within the module are production grade.

Operator Required Actions

There are no operator required actions

Table 11 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
N/A	N/A	N/A

10. Mitigation of Other Attacks Policy

The module has been designed to mitigate specific attacks as follows outside the scope of FIPS 140-2.

Table 12 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
Active Tamper	The module will detect removal from the radio while power is provided, and zeroize keys	N/A
Static Tamper	The module will detect removal from the radio while power is off and zeroize keys upon next boot.	N/A

11. References

- National Institute of Standards and Technology, "FIPS PUB 140-2, Security Requirements for Cryptographic Modules", 25 May, 2001
- National Institute of Standards and Technology, "Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules. Draft", March 24, 2004

- National Institute of Standards and Technology, “FIPS PUB 197, Advanced Encryption Standard (AES)”, November 26, 2001
- National Institute of Standards and Technology, “FIPS PUB 46-3, Data Encryption Standard (DES)”, October 25, 1999
- National Institute of Standards and Technology, “FIPS PUB 180-2, Secure Hash Standard (SHS)”, August 1, 2002
- TIA/EIA Telecommunications Systems Bulletin, “APCO Project 25, Over-The-Air-Rekeying (OTAR) Protocol”, New Technology Standards Project, Digital Radio Technical Standards, TSB102.AACA, January 1996

12. Definitions and Acronyms

Table 13 – Definitions and acronyms

AES	**A**dvanced **E**ncryption **S**tandard
DES	**D**ata **E**ncryption **S**tandard
ESN	**Electric Serial Number**
KMM	**K**ey **M**anagement **M**essage
LFSR	**L**inear **F**eedback **S**hift **R**egister
OTAR	**O**ver **T**he **A**ir-**R**ekeying
SHA-256	**S**ecure **H**ash **A**lgorithm with **256** bits of message digest.