Security Policy:

Secure Cryptographic Module (SCM)

Document Version 1.5.6_1

FIPS 140-2 Non-Proprietary
JVC KENWOOD Corporation

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

Copyright© 2006 Kenwood Corporation
Copyright© 2011 JVC KENWOOD Corporation

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.
2006/10/20	1.5.6	Tamaki Shimamura	Added NX- series radios.
2011/11/12	1.5.6_1	Tamaki Shimamura	Reflected corporate name change.

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

Copyright© 2006 Kenwood Corporation
Copyright© 2011 JVC KENWOOD Corporation

Table of Contents

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

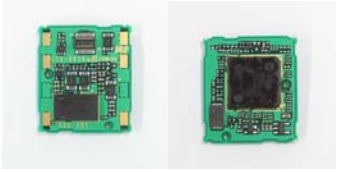
Copyright© 2006 Kenwood Corporation
Copyright© 2011 JVC KENWOOD Corporation

1. Module Overview

The Secure Cryptographic Module (SCM) is a hardware cryptographic module developed by JVC KENWOOD Corporation to provide FIPS 140-2 validated cryptographic securities for the TK-5XX0 and NX- series FM/P25 digital two way radios. This Security Policy was prepared as one of the requirements of FIPS 140-2, though the reader might find such information useful. If you have any technical questions, feel free to contact to fips140@jvckenwood.com. 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 and A1.0.1 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



2. Security Level

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

Table 1 - 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

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

Copyright© 2006 Kenwood Corporation
Copyright© 2011 JVC KENWOOD Corporation

Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

3. Modes of Operation

The SCM cryptographic module employs both FIPS approved and non-FIPS approved mode of operation. By initializing AES encryption or decryption service, the module enters an ***Approved*** mode of operation. Any requests for DES encryption or decryption initialization service after AES services will result the module to transit in 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 appropriate bit flag set to "1".

Approved Algorithms

The cryptographic module supports the following Approved algorithms:

Table 2 - Approved Algorithms

AES	As defined in **FIPS PUB 197** with 256 bit keys. ECB and OFB modes are supported. CBC mode is not made available with FW versions A1.0.0 and A1.0.1.
SHA-256	As defined in **FIPS PUB 180-2** for creating message digests with 256 bits. SHA-256 is provided for internal functions ***only***.

Non-Approved Algorithms

The cryptographic module supports the following non- Approved algorithms:

Table 3 - Non-Approved Algorithms

DES [non-compliant]	As defined in **FIPS PUB 46-3** with 56 bit keys. ECB and OFB modes are supported.
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

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

Copyright© 2006 Kenwood Corporation
Copyright© 2011 JVC KENWOOD Corporation

- 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 4 - Roles and Required Identification and Authentication

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

Table 5 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
N/A	N/A

6. Access Control Policy

Roles and Services

Table 6 - 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 • DES • 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	• Show Status • Calibration Service • Key zeroization • Self tests

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

Copyright© 2006 Kenwood Corporation
Copyright© 2011 JVC KENWOOD Corporation

checking status of the module.	

Service - Purpose and Use

Table 7 - Service name, purpose, and use

Service Name	**Purpose and Use**
AES	Allows Users to encrypt/decrypt data.
DES	Allows Users to encrypt/decrypt data.
LFSR	Allows Users to generate IV used in OFB mode.
Key entry	Allows Users to enter cryptographic keys 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.
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.

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.

Definition of Public and Private Keys

The module does not contain any public/private keys.

Definition of CSPs Modes of Access

Table 8 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 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 8 - CSP Access Rights within Roles & Services

Role		**Service**	**Cryptographic Keys and CSPs Access Operation**
C.O.	**User**		**AES**

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

Copyright© 2006 Kenwood Corporation
Copyright© 2011 JVC KENWOOD Corporation

	×	AES	Read
	×	DES	N/A
	×	LFSR	N/A
	×	Key entry	Write
	×	Sleep Mode / Wake Up	N/A
×		Zeroization	Zeroize
×		Self-Tests	N/A
×		Calibration Service	N/A
×		Show Status	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.
The module is not capable of upgrading its firmware components after the vendor's site.

8. Security Rules

The cryptographic module corresponds to its Security Rules derived from FIPS 140-2 and JVC 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. All keys shall be entered via electronic key entry using manual methods (e.g. use of a radio and a compatible key variable loader).
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.
7. DES must not be used in an Approved mode of operation.
8. The cryptographic module is not capable of upgrading its firmware components.

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

Copyright© 2006 Kenwood Corporation
Copyright© 2011 JVC KENWOOD Corporation

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.[1]
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. DES Known Answer Test
            c. LFSR Known Answer Test
            d. SHA-256 Known Answer Test
        3. Critical Functions Tests:
            a. N/A

    B. Conditional Self-Tests:
        1. Continuous Random Number Generator (RNG) test
           – performed on the LFSR

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

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

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

Copyright© 2006 Kenwood Corporation
Copyright© 2011 JVC KENWOOD Corporation

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 9 – 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 ***not*** been designed to specific attacks outside the scope of FIPS 140-2.

Table 10 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	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

12. Definitions and Acronyms

Table 11 – Definitions and acronyms

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

Copyright© 2006 Kenwood Corporation
Copyright© 2011 JVC KENWOOD Corporation

AES	**A**dvanced **E**ncryption **S**tandard
DES	**D**ata **E**ncryption **S**tandard
LFSR	**L**inear **F**eedback **S**hift **R**egister
SHA-256	**S**ecure **H**ash **A**lgorithm with **256** bits of message digest.

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

Copyright© 2006 Kenwood Corporation
Copyright© 2011 JVC KENWOOD Corporation