FIPS 140-2 Cryptographic Module Security Policy

Secure Cryptographic Module (SCM)

Document Version 3.0.9

FIPS 140-2 Non-Proprietary

JVC KENWOOD Corporation

Revision History

Date	Revision	Author	Description
2013/05/05	3.0.0	Tamaki Shimamura	Ported from version 2.1.2_1. This branch is developed for HW version 2.0.0, FW version A3.0.0.
2013/12/06	3.0.1	Tamaki Shimamura	Updated following onsite review and testing.
2014/01/24	3.0.2	Tamaki Shimamura	Included FW version A3.0.1.
2014/03/08	3.0.3	Tamaki Shimamura	Updated radio information.
2014/06/12	3.0.4	Tamaki Shimamura	Removed FW version A3.0.0.
2014/09/09	3.0.5	Tamaki Shimamura	Included FW version A3.0.2.
2015/4/1	3.0.6	Tamaki Shimamura	Updated supported radios.
2015/5/30	3.0.7	Tamaki Shimamura	Included FW version A3.0.3.
2017/04/11	3.0.8	Tamaki Shimamura	Included HW version 2.1.0, and updated supported radios.
2018/1/19	3.0.9	Tamaki Shimamura	Included FW version A3.0.4.

Table of Contents

List of Tables

List of Figures

1 Introduction

The Secure Cryptographic Module (SCM) is a hardware cryptographic module developed by JVC KENWOOD Corporation to provide FIPS 140-2 validated cryptographic security functionality for the radio series.

- TK-5XX0 series FM/P25 digital two way radios
- NX‐/NXR‐ series FM/P25/NEXEDGE digital radios
- VPxxx0 series FM/P25 digital two way radios
- VMxxx0 series FM/P25 digital two way radios

The SCM is a multi-chip embedded embodiment that meets FIPS 140-2 overall Level 1 requirements.

The validated module is identified as follows:

SCM part number: KWD-AE30
Hardware version: 2.0.0 and 2.1.0
Firmware version A3.0.1, A3.0.2, A3.0.3 and A3.0.4

Technical contact: fips140@kenwood.co.jp
Sales contact: fips@us.jvckenwood.com

The FIPS 140-2 security levels for the Module are as follows:

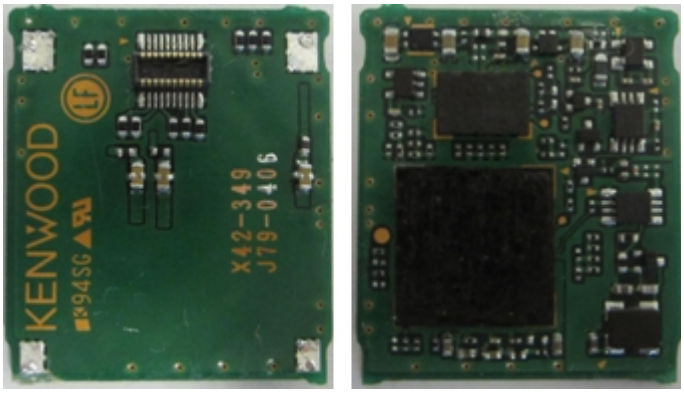
Table 1 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic 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	3
Mitigation of Other Attacks	1
Overall	**1**

1.1 Hardware and Physical Cryptographic Boundary

The SCM physical form is depicted in Figure 1, with the cryptographic boundary defined as the surfaces and edges of the assembled SCM printed circuit board.

Figure 1 - Physical Form of the SCM



The Module relies on external hardware: the carrier boards of the TK-5XX0 and NX-/NXR- series radios for system interaction, and on an external key loader device used in conjunction with the radio.

All physical ports are located on a single board-to-board connector J1.

Table 2 – Ports and Interfaces

Pin #	Pin Name	Description	Logical Interface Type
1	GND	Ground	Power
2	GND	Ground	Power
3	/RESET	Reset	Control Input
4	TXD	UART (key loader) data	Status Output
5	SCK	SPI shift clock	Control Input
6	RXD	UART (key loader) data	Control Input, Data Input
7	/REQ	Interrupt request	Status Output
8	BUSY	Busy indicator	Status Output
9	TAMPER2	Tamper detection	Control Input
10	NC	No Connect	N/A
11	TAMPER	Tamper detection	Control Input
12	Vcc	+3.3V	Power
13	MOSI	SPI data	Control Input, Data Input
14	BCLK	Clock	Control Input
15	/SS	SPI slave enable	Control Input

Pin #	Pin Name	Description	Logical Interface Type
16	MISO	SPI data	Data Output, Status Output
17	/WAKEUP	Wakeup from sleep mode	Control Input
18	/BFS	Frame sync	Control Input
19	GND	Ground	Power
20	GND	Ground	Power

1.2 Logical Function

Figure 2 depicts the SCM logical block diagram in an operational context. The SCM comprises a Processor (DSP), non-volatile memory (NVM), clock, tamper detection circuit and a board to board connector.

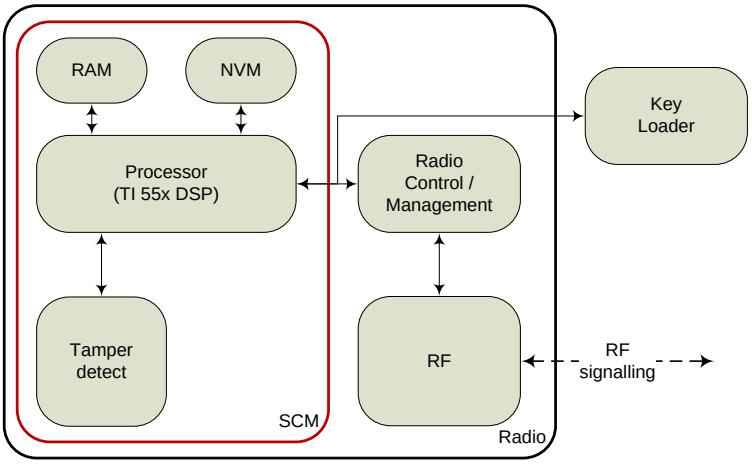


Figure 2 – SCM Block Diagram

1.3 Modes of Operation

The SCM cryptographic module employs both FIPS approved and non-FIPS approved modes of operation. By initializing AES 256-bit encryption or decryption service, or using the AES-OTAR service with CBC-MAC or CMAC to confirm the KMM's integrity, the module enters an Approved mode of operation. Any requests for DES or AES 128-bit 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. Other than the use of non-Approved algorithms as described below, there are no other differences in the functionality of the Module between the Approved mode and the non-Approved mode.

An operator (via radio controller functions) is capable of confirming the Approved mode of operation by calling the *Show Status* service and verifying the *Cipher Status* flag is set to "1".

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed below.

Table 3 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38A] Encryption and Decryption in ECB and OFB modes using a 256-bit key.	2696
CMAC	[SP 800-38B] [Project 25 TIA-102AACA-1] CMAC generation and verification using a 256-bit key.	2696
SHA	[FIPS 180-3] SHA-256 used for radio pairing.	2285

Table 4 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
AES MAC (OTAR)	[ANSI/TIA-102.AACA-1] AES MAC (AES Cert. #2696, vendor affirmed, P25 AES OTAR).

Non-Approved Cryptographic Functions for use in non-FIPS mode only:

- DES
- DES- MAC
- AES 128 / ECB (for use in Link Layer Authentication)
- LFSR (used for IV generation)

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 5 – Critical Security Parameters (CSPs)

CSP	Description / Usage
EDK	256 bit AES key used for encryption and decryption.
FWI	256 bit AES key used for firmware load testing.
KMMI	256 bit AES key used for KMM integrity.

The module does not utilize public keys.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The cryptographic module supports both Cryptographic Officer (CO) and User roles, implicitly selected by the operator from the services provided. The module does not support a maintenance role.

The CO role is responsible for management activities including installing the module to the radio, deletion of keys, and checking status of the module. The User role has access to all crypto related functions supported by the crypto module, including key entry.

3.2 Services

All services implemented by the Module are listed in the table(s) below. Each service description also describes all usage of CSPs by the service.

Table 6 – Authenticated Services

Service	Description	User	CO
Calibrate	Calibrate SCM timing.		X
Firmware Upgrade	Update validated firmware. Loading the Zeroization Image zeroizes all keys (including FWI).		X
Show status	Report SCM status.	X	X
Self-test	Perform self-tests. If any of the self-tests fail, an indicator showing which self-test(s) have failed will be returned.	X	X
Zeroize	Zeroizes all CSPs except FWI and RAND.		X
Secure Communication	Encrypted communications using AES (Approved mode) or DES (non-Approved mode).	X	
OTAR	Rekeying per P25 AES OTAR using AES CMAC or AES MAC (Approved mode), or DES OTAR using DES MAC (non-Approved mode).	X	
Key load	Load keys via a key loader.	X	
Sleep / Wake-up	Enable or disable sleep mode (power consumption reduction).	X	

Table 7 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- -- = No access to the CSP.
- G = Generate: The SCM generates the CSP.
- R = Read: The SCM outputs the CSP.
- E = Execute: The SCM executes using the CSP.
- W = Write: The SCM writes the CSP.
- Z = Zeroize: The module zeroizes (destroys) the CSP.

Table 7 – CSP Access Rights within Services

Service	CSPs		
	EDK	FWI	KMMI
Calibrate	--	--	--
Show status	--	--	--
Self-test	--	--	--
Firmware Upgrade	Z	E, W, Z	Z
Zeroize	Z	--	Z
Secure Communication	E	--	--
OTAR	W, Z	--	E, W, Z
Key load	W	--	W
Sleep / Wake-up	--	--	--

4 Self-tests

Each time the SCM is powered up, it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power-up self–tests are available on demand by power cycling the module, and are performed prior to any usage of SCM services.

On power-up or reset, the Module performs the self-tests described in Table 8 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the SCM enters an error state (returning "AA01" and a bit field indicating which self-test has failed) and only the show-status function will be functional. By using the show-status function, the operator (Crypto Officer and User) is capable of understanding which of the self-tests have failed.

Table 8 – Power-Up Self-tests

Test Target	Description
Firmware Integrity	16 bit CRC performed over all code.
AES	Separate encryption and decryption KATs with the following Mode/ Key Size • ECB / 256 • OFB / 256
CMAC	AES CMAC KAT using a 256 bit key
SHA	SHA-256 KAT

Table 9 – Conditional Self-tests

Test Target	Description
Firmware Load	AES CMAC verification performed when firmware is loaded.
LSFR RNG	Continuous Random Number Generator Test performed per AS09.42 when a random value is requested from the LSFR (for use as an OFB IV).

5 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

6 Mitigation of Other Attacks Policy

The module has been designed to mitigate specific attacks as follows outside the scope of FIPS 140-2, with no specific limitations on attack mitigation.

Table 10 - Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism
Active Tamper	The module will detect removal from the radio while power is provided, and zeroize all EDKs and KMMIs.
Static Tamper	The module will detect removal from the radio while power is off and zeroize all EDKs and KMMIs upon next boot.

7 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. Physical security policy: all of the components within the module are production grade.
2. The SCM inhibits cryptographic operations in error states, and inhibits data output during self-tests, zeroization, and error states.
3. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
4. Keys are entered by authorized operators in plaintext form using a compatible key variable loader (manual distribution, electronic entry) or in encrypted form via OTAR automated methods.
5. The SCM does not output any CSPs.
6. For the Approved mode of operation, the operator shall use AES for Secure Communications. DES shall not be used in an Approved mode of operation.
7. An SCM is paired with a specific radio: upon detection of an invalid radio identifier, the SCM zeroizes AES keys and AES-OTAR keys as described in Table 11.
8. SCM tamper event key zeroization behavior depends on the Infinite attribute flag: when the flag is set, a tamper event zeroizes all AES keys and AES-OTAR keys; when not set, a tamper event zeroizes keys stored in RAM.

8 References and Definitions

Table 11 – References

Abbreviation	Full Specification Name
[FIPS140-2]	National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, 25 May, 2001
[FIPS 140 DTR]	National Institute of Standards and Technology, *Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules.* Draft, March 24, 2004
[FIPS PUB 197,]	National Institute of Standards and Technology, *Advanced Encryption Standard (AES)*, November 26, 2001
[FIPS PUB 46-3]	National Institute of Standards and Technology, *FIPS PUB 46-3, Data Encryption Standard (DES)*, October 25, 1999

Table 12 – Acronyms and Definitions

Acronym	Definition
AES	**A**dvanced **E**ncryption **S**tandard
DES	**D**ata **E**ncryption **S**tandard
ESN	**E**lectric **S**erial **N**umber
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.
SPI	**S**erial **P**eripheral **I**nterface