FIPS 140-3 Non-proprietary Security Policy

UT-125 FIPS #31 and #41 Cryptographic Module
Hardware versions 1.2, 1.3, 2.2 and 2.3
Firmware version 1.6

Document Revision 2.7

Icom Inc.
1-1-32, Kamiminami, Hirano-ku
Osaka 547-0003 Japan

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document details the security policy for the cryptographic module UT-125 FIPS #31 Hardware revision 1.2 and Hardware revision 1.3, UT-125 FIPS #41 Hardware revision 2.2 and Hardware revision 2.3 implementing firmware version 1.6, herein identified as the optional encryption unit, UT-125 FIPS #31 and #41 for Icom Inc. radios. This non-proprietary security policy may be freely reproduced and distributed only in its entirety without revision.

1.2 Security Levels

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	1
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:
The UT-125 FIPS #31 and #41 are multi-chip embedded cryptographic modules as defined by FIPS 140-3.
The cryptographic module can be incorporated into any Icom Inc. radio which requires FIPS 140-3 level 1 cryptographic security.

Module Type: Hardware

Module Embodiment: Multi-chip Embedded

Cryptographic Boundary:
The cryptographic boundary consists of the entire printed circuit board, as depicted in Figures 1 and 2.

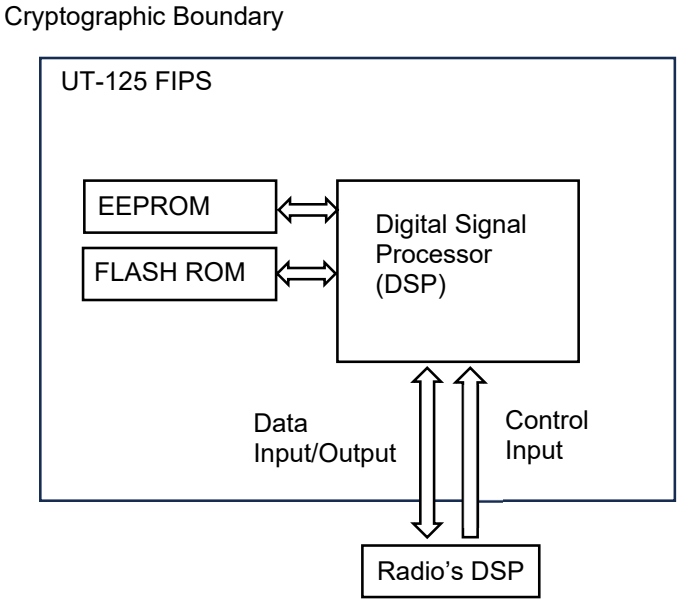
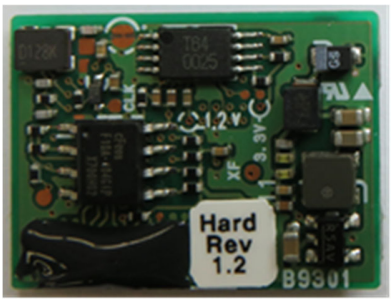
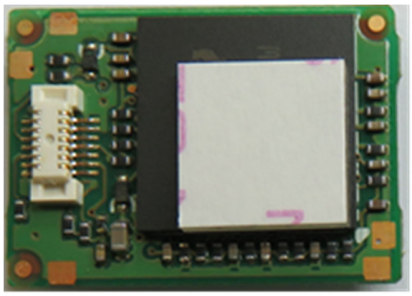


Figure 1 – Block Diagram

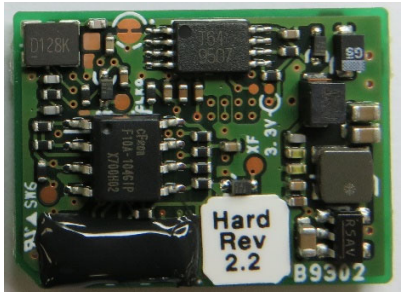
Figure 2 contains representative images of the cryptographic module. Other than the labels, Rev 1.2 and 1.3 of the UT-125 #31 are externally identical. Likewise, Rev 2.2 and 2.3 of UT-125 #41 are also externally identical.

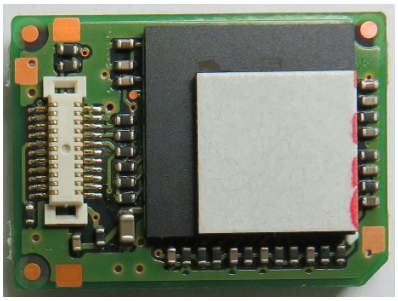
#31





#41





Top

Bottom

Figure 2 – Representative Images

2.2 Tested Module Version and Identification

Tested Module Identification – Hardware:

Model	Hardware	Firmware Version	Distinguishing Features
UT-125 #31	Rev1.2	Rev.1.6	Seal, Display on the radio display.
UT-125 #31	Rev1.3	Rev.1.6	Seal, Display on the radio display.
UT-125 #41	Rev2.2	Rev.1.6	Seal, Display on the radio display.
UT-125 #41	Rev2.3	Rev.1.6	Seal, Display on the radio display.

Table 2: Cryptographic Module Tested Configuration

2.3 Excluded Components

The cryptographic module does not have any Excluded components.

2.4 Modes of Operation

Modes List and Description:
This UT-125 FIPS cryptographic module supports both approved mode and non-approved mode as explained below.

Mode Change Instructions and Status:
The cryptographic module supports both approved, and non-approved modes depending on the McBSP interface commands being invoked. Approved algorithms output the signal of GPIO port when running. The signal of GPIO9 indicates the module is using an approved security function.

Degraded Mode Description:
The cryptographic module does not support degraded operation.

2.5 Algorithms

Approved Algorithms:
The module's CAVP certificates includes algorithms/options that are not utilized by the module in the approved mode. Only the algorithms/options listed in the table below are utilized by the module in the approved mode.

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A1399	AES-OFB (SP 800-38A)	AES-OFB	256 bits	Voice Encryption / Decryption
A1399	HMAC-SHA-1 (FIPS 198-1)	HMAC-SHA-1	MAC: 160 bits Key Length: 512 bits	Firmware Integrity, Firmware Load Test

A1399	SHA-1 (FIPS 180-4)	SHA-1	N/A	Hash function for HMAC

Table 3: Approved Algorithms

Vendor-Affirmed Algorithms:
This cryptographic module does not have a Vendor-Affirmed Algorithms algorithm.

Non-Approved, Allowed Algorithms:
This module does not implement any Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed.

Non-Approved, Allowed Algorithms with No Security Claimed:
This module does not implement any Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed.

Non-Approved, Not Allowed Algorithms:

Algorithm/Function	Use/Function
AES-CBC-MAC	Message Authentication
AES-ECB	Data Encryption / Decryption
CTR_DRBG	Pseudo-Random Number Generator
DES-ECB	Crypto Key Encryption / Decryption
DES-OFB	Voice Encryption / Decryption
PRNG	Pseudo-Random Number Generator

Table 4: Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

UT-125 FIPS Physical I/O Ports	Logical interface	Data that passes over port/interface
#31:1 DGND #41:1 GND	Power	Ground
2 CCLKO	Data Output	McBSP clock output
#31: 3 DGND #41: 3 GND	Power	Ground
4 CFSO	Data Output	McBSP frame sync output
5 CFSI	Data Input or Control Input	McBSP frame sync input
6 CDO	Data Output or Status Output	McBSP data output
7 CCLKI	Data Input or Control Input	McBSP clock input

8 DRESET	Control Input	Reset signal
9 CDI	Data Input or Control Input	McBSP data input
10 CACT	Control Input	Wake up signal
11 DVDD_3.3V	#31: Power #41: Power	#31: External electrical power (+3.3V power line) #41: GND
12 DGND	Power	#31: Ground #41: External electrical power (+3.3V power line)
13 -	#31: N/A #41: Power	#31: Non-connection #41: External electrical power (+3.3V power line)
14 DGND	#31: Power #41: N/A	#31: Ground #41: Non-connection

Table 5: Ports and Interfaces

3.2 Trusted Channel Specification

This module does not support a trusted channel.

3.3 Control Interface Not Inhibited

This module does not have control output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

This module does not support operator authentication.

4.2 Roles

The UT-125 FIPS #31 and #41 support the roles of Crypto Officer and User.

Crypto Officer:
Assumption of the Crypto Officer role is implied when any of the services specific to a Crypto Officer are executed.

The Crypto Officer role is responsible for the keys and firmware of the UT-125 FIPS #31 and #41. The management of keys, such as loading, reading and writing, is the domain of the Crypto Officer. The main tool for key management utilized by the Crypto Officer is an approved key loading device.

The Crypto Officer role will also manage firmware updating and checking procedures.

User:
Assumption of the User role is implied when any of the services specific to a User are executed.

The User role is primarily consists of the services which conduct the encryption and decryption of communication, invoke self-tests, and indicate the status of the UT-125 FIPS #31 and #41.

Role	Service	Input	Output

User/Crypto Officer	Decryption	McBSP command:Control Input or Data Input (Request Command)	McBSP command:Status Output or Data Output (Response Command)
User/Crypto Officer	Encryption	McBSP command:Control Input or Data Input (Request Command)	McBSP command:Status Output or Data Output (Response Command)
Crypto Officer	Firmware Update	McBSP command:Control Input (Request Command)	McBSP command:Status Output (Response Command, Indicate Command)
User/Crypto Officer	Key Load	McBSP command:Control Input or Data Input (Request Command)	McBSP command:Status Output (Response Command, Indicate Command)
User/Crypto Officer	Key Zeroisation	McBSP command:Control Input (Request Command)	McBSP command:Status Output (Response Command)
User/Crypto Officer	Power-Off	McBSP command:Control Input (Request Command)	McBSP command:Status Output (Response Command, Indicate Command)
User/Crypto Officer	Self-Tests	Reset signal (Physical port): Control Input	McBSP command: Status Output
User/Crypto Officer	Show Key Status	McBSP command:Control Input (Request Command)	McBSP command:Status Output (Response Command)
User/Crypto Officer	Show Status	McBSP command:Control Input (Request Command)	McBSP command:Status Output (Response Command)
User/Crypto Officer	Show Version	McBSP command:Control Input (Request Command)	McBSP command:Status Output (Response Command)
Crypto Officer	System Management	McBSP command:Control Input (Request Command)	McBSP command:Status Output (Response Command)
User/Crypto Officer	Key Management	McBSP command:Control Input or Data Input (Request Command)	McBSP command:Status Output or Data Output (Response Command)

Table 6: Roles, Service Commands, Input and Output

4.3 Approved Services

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Decryption	Decoding from ciphertext to plaintext	AES-OFB	TEK	O/U	E	Port Output (GPIO9)
Encryption	Encoding from plaintext to ciphertext	AES-OFB	TEK	O/U	E	Port Output (GPIO9)
Firmware Update	Updating the firmware in the crypto module	HMAC-SHA-1	HMAC Key	O	E, W	Port Output (GPIO9)
Key Load	Loading crypto key using Key Fill Device Interface Protocol	N/A	TEK	O/U	W	N/A
Key Zeroisation	Zeroising crypto key using Key Fill Device Interface Protocol	N/A	TEK	O/U	Z	N/A
Power-Off	Turning the power off on the module	N/A	N/A	O/U	N/A	N/A
Self-Tests	Self-testing the operation of the crypto functions	AES-OFB HMAC-SHA-1	N/A	O/U	N/A	N/A

Show Key Status	Providing the crypto parameter.	N/A	N/A	O/U	N/A	N/A
Show Status	Showing current status	N/A	N/A	O/U	N/A	N/A
Show Version	Show module's versioning information	N/A	N/A	O/U	N/A	N/A
System Management	Zeroising various setting values	N/A	TEK, HMAC Key	O	Z	N/A

Table 7: Approved Services

O = Crypto Officer
U = User
G = Generate: The module generates or derives the SSP.
R = Read: The SSP is read from the module (e.g. the SSP is output).
W = Write: The SSP is updated, imported, or written to the module.
E = Execute: The module uses the SSP in performing a cryptographic operation.
Z = Zeroise: The module zeroises the SSP.

4.4 Non-Approved Services

Service	Description	Algorithms Accessed	Role	Indicator
Decryption (non-approved)	Decoding from ciphertext to plaintext	DES-OFB	O/U	N/A
Encryption (non-approved)	Encoding from plaintext to ciphertext	DES-OFB	O/U	N/A
Key Management	Changing/Adding/Generating/Zeroising crypto key and module parameter.	AES-CBC-MAC AES-ECB CTR_DRBG DES-ECB PRNG	O/U	N/A

Table 8: Non-Approved Services

4.5 External Software/Firmware Loaded

The firmware update is performed via the Firmware Update service, which executes the firmware load test.

4.6 Bypass Actions and Status

This module does not support a bypass capability.

4.7 Cryptographic Output Actions and Status

This module does not support a self-initiated cryptographic output capability.

5 Software/Firmware Security

The module's firmware is provided as the 3059C3_16.MOT (boot and application firmware) or 3059C3_16(F).MOT (just application firmware) binary images.

5.1 Integrity Techniques

The module uses CRC-32 as EDC method for the integrity testing.

5.2 Initiate on Demand

The software/firmware integrity test is performed every time the module is started / rebooted.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:
As shown in Table 1 this cryptographic module operates at security level 1.

The module maintains control of its own SSPs retained within the module. The module's operational environment consists of firmware with access to SSPs managed wholly by the module itself. Please see Section 9 for SSP details.

6.2 Configuration Settings and Restrictions

This module is a hardware module with a limited operational environment.
Cryptographic module stores firmware to flash ROM within cryptographic boundary.
.

7 Physical Security

7.1 Mechanisms and Actions Required

This is multi-chip embedded cryptographic module.
The circuitry uses standard passivation techniques and meets Security Level 1. This plug-in module is contained within a production grade radio enclosure and uses commercially available IC chips.

8 Non-Invasive Security

The cryptographic module does not have the non-invasive mitigation techniques.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Name	Description	Persistence Type
EEPROM	For Cryptographic key	Static
DSP RAM	For Temporary SSPs	Dynamic

Table 9: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
KFD* Protocol	Key Fill Device	EEPROM or DSP RAM	Plaintext	Manual	Electronic	None

Table 10: SSP Input-Output

*Key Fill Device (Key Loader)

9.3 SSP Zeroization Methods

Method	Description	Rationale	Operator Initiation Capability
Zeroise command	McBSP Command: Control Input / Status Output	Zeroising Key in EEPROM or DSP RAM	Starting with Operator's invocation. Determining whether the procedures were successful with Status Output.
Power lost	Module power lost	Zeroising SSP in volatile memory	Operator's invocation.

Table 11: SSP Zeroization Methods

9.4 SSPs

Key / SSP Name / Type	Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroisation	Use & related keys
TEK (Traffic Encryption Key)	256-bits	AES-OFB A1399	N/A	KFD* Protocol	N/A	EEPROM (Plaintext)	Zeroise command from McBSP interface	Used for encryption/ decryption of voice traffic through the module's host radio.
HMAC Key	256-bits	HMAC-SHA-1 A1399	Manufacturer pre-loaded	N/A	N/A	EEPROM (Plaintext)	Zeroise command from McBSP interface	Used for updating the firmware.

Table 12: SSPs

*Key Fill Device (Key Loader)

9.5 Transitions

The cryptographic module is not subject to transitions.

9.6 Additional Information

Keys/SSPs used in the approved mode shall not be used in the non-approved mode and vice-versa.
The cryptographic module does not support manual key entry.

Please note that Zeroise command from McBSP interface is used for changing the key data in DSP RAM. Then, those updated key data will be written to EEPROM.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Pre-Operational self-tests:

- Pre-Operational software/firmware integrity test;
  - Firmware Integrity Test (CRC-32)

10.2 Conditional Self-Tests

Conditional self-tests:

- Cryptographic Algorithm Self-Tests
  - AES-ECB Encrypt Known Answer Test (256-bit key)*
  - AES-ECB Decrypt Known Answer Test (256-bit key)*
  - AES-CBC Encrypt Known Answer Test (256-bit key)*
  - AES-CBC Decrypt Known Answer Test (256-bit key)*
  - AES-OFB Encrypt Known Answer Test (256-bit key)
  - AES-OFB Decrypt Known Answer Test (256-bit key)
  - HMAC-SHA-1 Known Answer Test
  - *Algorithm only used for self-tests in approved mode.
- Conditional software/firmware load test;
  - Firmware load test (HMAC-SHA1 w/ 512-bit key)
- Conditional Critical Functions Test
  - 32-bit CRC check on Electronically Entered keys

10.3 Periodic Self-Test Information

The module does not perform periodic self-tests.

10.4 Error States

Number	Byte Size	Information	Logical Interface
$01	1	Show Status (see *Table 7*) $00=Program Running $01=Initial Sequence	Status Output

		$02=Firmware Update $03=EEPROM Error $04=Boot Self-Test Error $05=Application Self-Test Error	

Table 13: Error Indicators

Value	Status	Finite State Model
$00	Program Running	Idle
$01	Initial Sequence	Application Initialization, Application Self-Test, Database Load
$02	Firmware Update	Firmware Update
$03	EEPROM Error	Boot EEPROM Error, Application EEPROM Error
$04	Boot Self-Test Error	Boot Self-Test Error
$05	Application Self-Test Error	Application Self-Test Error

Table 14: Error Status

10.5 Operator Initiation of Self-Tests

The module's pre-operational self-tests and conditional CASTs can be performed on demand by power cycling the module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Install
For the cryptographic module installation, refer the radio service manual.

Secure Initialization
Proper keys must be loaded into the module.

Key Loading Instructions
Crypto-Officer may load keys into the modules using the key loader devices.
The radio hardware communicates with the module through the defined ports.
Each key loaded into the module has an associated key ID which is used to associate the key with a given radio channel.

Operation of the module
The cryptographic module contains non-approved security functions. Only services which utilize approved security functions are indicated as such by the module.

11.2 Administrator Guidance

Please refer to the McBSP command guidance.

11.3 Non-Administrator Guidance

Please refer to the McBSP command guidance.

11.4 Design and Rules

The security rules presented below are a combination of those required by FIPS140-3 for Level 1 secure use and the security rules separately implemented by Icom Inc.

FIPS 140-3 Security Rules:
Only approved algorithms can be used, and the use of RNG, DES is not allowed in the approved mode of operation.

11.5 Maintenance Requirements

The cryptographic module is composed of production grade components which do not require any maintenance or inspection by the user to ensure security.

11.6 End of Life

When distributing or discarding the cryptographic module to other operators, send the McBSP command "All Key Zeroise" ($ 77) to initialize and sanitize all cryptographic keys (SSPs).
(Since the cryptographic module does not perform Operator Authentication, it does not retain authentication data.)

12 Mitigation of Other Attacks

This module does not support other attack mitigation.