FIPS 140-2 Non-proprietary Security Policy

UT-125 FIPS #11 and UT-125 FIPS #21 Cryptographic Module

Hardware version 1.1 and 2.1

Firmware version 1.1

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

Table of Contents

1. Introduction

This document details the security policy for the cryptographic module UT-125 FIPS #11 version 1.1 and UT-125 FIPS #21 version 2.1 implementing firmware version 1.1, herein identified as the optional encryption unit, UT-125 FIPS #11 and UT-125 FIPS #21 for Icom Inc. radios. This non-proprietary security policy may be freely reproduced and distributed only in its entirety without revision.

1.1 Purpose

The secure operation of the UT-125 FIPS #11 and UT-125 FIPS #21 are detailed in this document to include the requirements of FIPS 140-2 and those imposed by Icom Inc. as applicable to the initialization, roles, and responsibilities of security related data and components management.

1.2 Cryptographic module Implementation

The UT-125 FIPS #11 and UT-125 FIPS #21 are multiple-chip embedded cryptographic modules as defined by FIPS 140-2. The UT-125 FIPS #11 and UT-125 FIPS #21 can be incorporated into any Icom Inc. radio which requires FIPS 140-2 level 1 cryptographic security.

1.3 Cryptographic Boundary

The UT-125 FIPS #11 and UT-125 FIPS #21 cryptographic boundary utilize the entire printed circuit board as depicted in Figure 1.

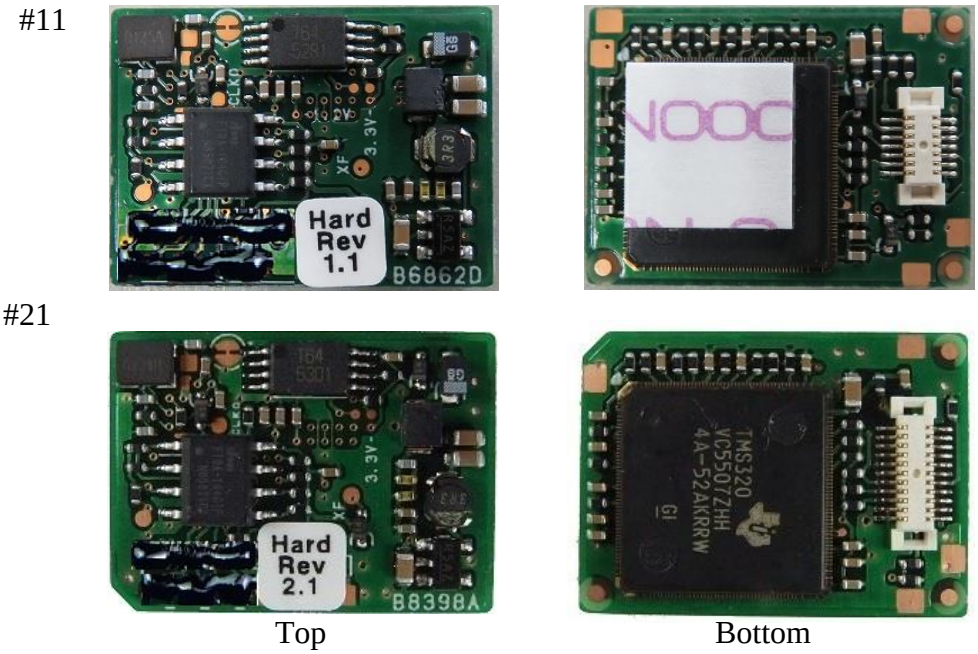


Figure 1

1.4 Logical interfaces and physical interfaces

The logical and physical interface of UT-125 FIPS #11 and UT-125 FIPS #21 cryptographic modules are detailed in Table 1.

Table 1 Ports and Interface Information on UT-125 FIPS #11 and #21

Logical Interface	Port	Physical Interface Description
Data Input	McBSP Interface	Clock input Frame sync input Data input
Data Output	McBSP Interface	Clock output Frame sync output Data output
Control Input	McBSP Interface	Frame sync input Clock input Data input Reset signal input Wake up signal input
Status Output	McBSP Interface	Data output
Power	---	External electrical power and ground

2. FIPS 140-2 Security Level

The UT-125 FIPS #11 and UT-125 FIPS #21 meet the security requirements established in FIPS 140-2 for an overall module security of Level 1 with the individual requirements and corresponding security levels detailed in Table 2.

Table 2 UT-125 FIPS #11 and UT-125 FIPS #21 Security Levels

FIPS 140-2 Security Requirement Area	Level
Cryptographic Module Specification	1
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
Electromagnetic Interference / Electromagnetic Compatibility	1
Self Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

3. Roles, Services, and Authentication

3.1 Roles

The UT-125 FIPS #11 and UT-125 FIPS #21 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 #11 and UT-125 FIPS #21. 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 #11 and UT-125 FIPS #21.

3.2 Services

The security services and functions available in the UT-125 FIPS #11 and UT-125 FIPS #21 in conjunction with the applicable operator role for each service and function can be found in Table 3 below.

Table 3 UT-125 FIPS #11 and UT-125 FIPS #21 Services and Roles

Service	Crypto Officer	User	Algorithms Used	Allowed in FIPS mode
Show Status	○	○		Yes
Self Test	○	○	AES	Yes
			HMAC	Yes
			CTR_DRBG	Yes
Power Off	○	○		Yes
Power Save	○	○		Yes
Encryption	○	○	AES OFB	Yes
			DES OFB	No
Decryption	○	○	AES OFB	Yes
			DES OFB	No
Key Load	○			Yes
Key Zeroization	○	○		Yes
Show OTAR Status	○	○		Yes
OTAR Management	○	○	CTR_DRBG	Yes
			AES MAC	Yes
			FIPS 186-2 RNG	No
			DES MAC	No
			AES ECB[1]	Yes
			DES ECB	No
Firmware Update	○		HMAC	Yes
System Management	○	○		Yes

The UT-125 FIPS #11 and UT-125 FIPS #21 support the following approved security functions:

- FIPS 197 AES 256-bit encryption and decryption with CBC, ECB, and OFB modes from SP 800-38A (Cert. # 3842)
- FIPS 198-1 HMAC with SHA-1 (Cert. # 2492)
- FIPS 180-4 SHS supporting SHA-1 (Cert. # 3165)
- SP 800-90A AES_CTR DRBG with AES-256 (Cert #1087)

[1] AES ECB is not an approved key wrapping method and is considered equivalent to plaintext in this context. This is allowed as per FIPS 140-2 IG 1.23.

The UT-125 FIPS #11 and UT-125 FIPS #21 also support the following non-approved security functions:

- AES MAC (AES Cert. #3842, vendor affirmed; P25 AES OTAR)
- DES
- DES-MAC
- RNG
- AES Key Wrapping (Key Wrapping using ECB is not an Approved method and is considered equivalent to plaintext)

3.3 Identification and Authentication

Operator identification and authentication of roles are not required or supported by the UT-125 FIPS #11 and UT-125 FIPS #21.

4. Secure Operation and Rules

This section details the security rules which should be enforced for the secure use of the UT-125 FIPS #11 and UT-125 FIPS #21 and the physical security employed.

4.1 Security Rules

The security rules presented below are a combination of those required by FIPS 140-2 for Level 1 secure use and the security rules separately implemented by Icom Inc.

FIPS 140-2 Security Rules:

The following rule is required to operate in accordance with FIPS 140-2:
Only FIPS-approved or allowed (AES MAC) cryptographic algorithms can be used. The use of RNG, DES and DES MAC is not allowed in the FIPS approved mode of operation.

4.2 Physical Security

The UT-125 FIPS #11 and UT-125 FIPS #21 are composed of production grade components which do not require any maintenance or inspection by the user to insure security.

4.3 Secure Operation Initialization

The UT-125 FIPS #11 and UT-125 FIPS #21 have algorithms that are not FIPS 140-2 approved. Therefore in order to operate the module in a secure manner, only FIPS 140-2 approved algorithms or algorithms allowed in FIPS mode (AES MAC)

must be used. In addition, a proper seed key value must be loaded into the module[2]. The use of RNG, DES and DES MAC is not allowed in the FIPS approved mode of operation.

4.4 Key Loading Instructions

The crypto-officer may load keys into the module using a key loader device that communicates to the module through a port that is exposed on the radio into which the module is installed. Each key loaded in this manner has an associated Key ID, which is used to associate the key with a given radio channel.

When operating in the FIPS mode of operation, the crypto-officer should only load AES keys in this manner. DES is not allowed in FIPS mode.

4.5 Self Tests

The UT-125 FIPS #11 and UT-125 FIPS #21 supports both power-on self-tests and continuous self-tests as shown below.

- Power-on self-tests:
  - HMAC-SHA1 Known Answer Test
  - Non-approved RNG Known Answer Test
  - AES-256 Known Answer Test (encrypt and decrypt, ECB, OFB, and CBC modes)
  - DRBG Known Answer Test
  - Firmware Integrity Test (CRC-32)

- Conditional self-tests:
  - Firmware load test (HMAC-SHA1 w/ 64-byte key)
  - 32-bit CRC check on Electronically Entered keys
  - Continuous random number generator tests (Non-approved RNG, DRBG)

4.6 Entropy for DRBG

The DRBG of UT-125 FIPS #11 and UT-125 FIPS #21 are provided with 256 bits of entropy from outside the cryptographic boundary. This entropy is received in 16 bit chunks using the Entropy Setting command until the full 256 bits of entropy is populated.

[2] Note that when the module is installed in a compatible Icom radio, this step is performed automatically by the radio processor without any operator intervention.

5. Access Control Policy

Table 4 UT-125 FIPS #11 and UT-125 FIPS #21 Cryptographic Keys and CSPs Definition

Keys and CSPs	Generation/Entry Methods	Description
Secret Key	-	256-bit AES Cryptographic Key
Traffic Encryption Key	Traffic Encryption Key is generated from key loader or OTAR KMF, and externally input plaintext or AES-256 ECB[3] encrypted key into the module.	This is a Traffic Key, and is used for encryption/decryption of voice traffic through the module's host radio.
Key Encryption Key	Key Encryption Key is generated from key loader or OTAR KMF, and externally input plaintext or AES-256 ECB[3] encrypted key into the module.	This is a Key Wrapping Key, and is used for encryption/decryption of other cryptographic Key in OTAR mode.
Warm Start Key	Warm Start Key is generated from OTAR KMF, and externally input plaintext or AES-256 ECB[3] encrypted key into the module.	Warm Start Key is used by OTAR, and initiated from OTAR KMF.
Reverse Warm Start Key	Reverse Warm Start Key is generated by the module using the approved CTR_DRBG.	Reverse Warm Start Key is used by OTAR, and initiated from OTAR.
HMAC Key	This Key is hard-coded into the module.	64-byte key used as part of module's HMAC-SHA-1 firmware-load test.
CTR_DRBG V counter	CTR_DRBG V counter is derived as part of the CTR_DRBG algorithm.	128bit V counter used by CTR_DRBG algorithm.
CTR_DRBG Key	CTR_DRBG Key is derived as part of the CTR_DRBG algorithm.	256bit Key used by CTR_DRBG algorithm.
Entropy Input	Entropy Input is externally input into the module in plaintext.	256bit Entropy input supplied from outside of cryptographic boundary, used by CTR_DRBG algorithm.
CTR_DRBG Seed	CTR_DRBG Seed is derived as part of the CTR_DRBG algorithm	384bit seed used by the CTR_DRBG algorithm.

[3]AES-256 ECB is not an approved key wrapping method and is considered equivalent to plaintext in this context. This is allowed as per FIPS 140-2 IG 1.23.

Table 5 UT-125 FIPS #11 and UT-125 FIPS #21 Services, Keys, and Access

Service	Cryptographic Keys and CSPs	Type(s) of Access
Show Status	-	-
Self-Test	-	-
Power-Off	-	-
Power Save	-	-
Encryption	Any Secret Key[4]	U
Decryption	Any Secret Key	U
Key Load	Any Secret Key	E, W
Key Zeroization	Any Secret Key	E
Show OTAR Status	-	-
OTAR Management	Any Secret Key	E, U, R, W
	CTR_DRBG V counter, CTR_DRBG Key, and CTR_DRBG Seed	E, U, R, W
	Entropy Input	U, W
Firmware Update	HMAC Key	U
System Management	HMAC Key	E

In Table 5 above the following key should be used:

E = Erase
R = Read (Encrypted Key)
U = Use
W = Write

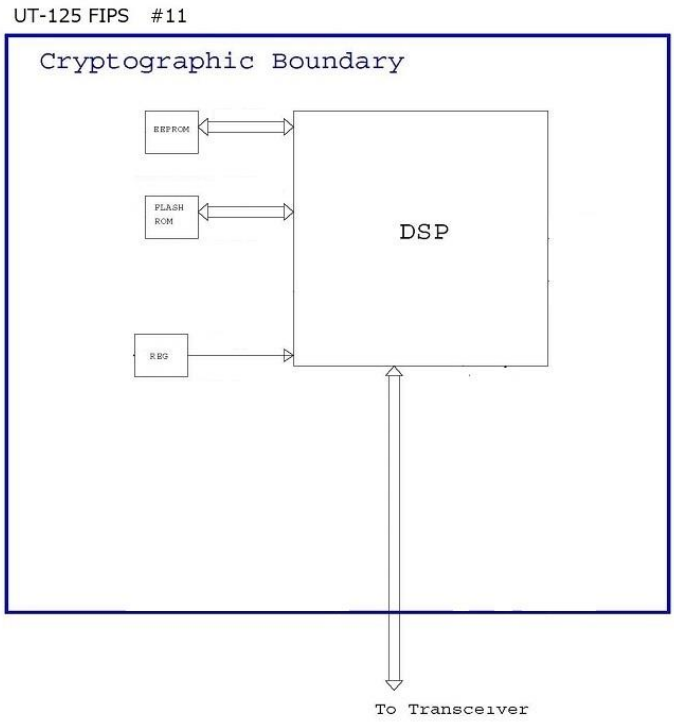
Where each of the above references the type of access the service has to the listed keys and Critical Security Parameters (CSP) on Table 5.

6. Mitigation of Other Attacks

The UT-125 FIPS #11 and UT-125 FIPS #21 have not been designed to mitigate attacks outside of those required within the FIPS 140-2 document.

[4] Any Secret Key refers to the four "sub-keys" identified in Table 5 (Traffic Encryption Key, Key Encryption Key, Warm Start Key, and Reverse Warm Start Key)

7. UT-125 FIPS #11 Block Diagram



8. UT-125 FIPS #21 Block Diagram