FIPS 140-2 Security Policy

UT-125 FIPS #10 Cryptographic Module
Hardware version 1.0
Firmware version 1.0

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

Document Version 1.4

Table of Contents

1. Introduction

This document details the security policy for the cryptographic module UT-125 FIPS #10 version 1.0 implementing firmware version 1.0, herein identified as the optional encryption unit, UT-125 FIPS #10 for Icom Inc. radios. This non-proprietary security policy may be freely reproduced and distributed only in its entirety without revision.

1.1 Purpose

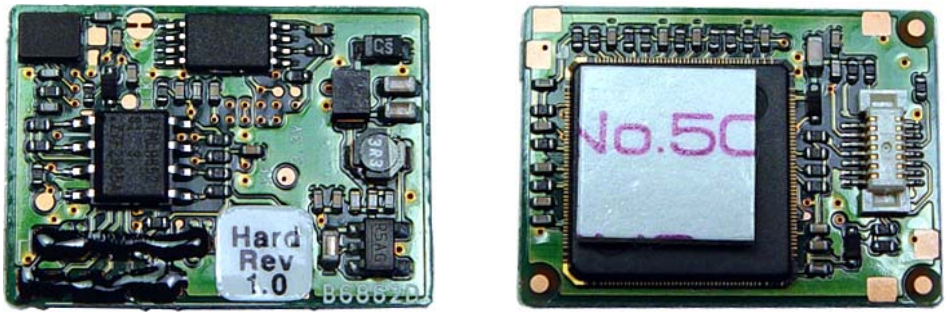
The secure operation of the UT-125 FIPS #10 is detailed in this document to include the requirements of FIPS 140-2 and those imposed by Icom Inc. as applicable to the initialization, roles, and responsibilities of security related data and components management.

1.2 Cryptographic module Implementation

The UT-125 FIPS #10 is a multiple-chip embedded cryptographic module as defined by FIPS 140-2. The UT-125 FIPS #10 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 #10 cryptographic boundary is the entire printed circuit board as depicted in Figure 1.



Top Bottom

Figure 1

2. FIPS 140-2 Security Level

The UT-125 FIPS #10 meets the security requirements established in FIPS 140-2 for an overall module security of Level 1 with the individual requirements and corresponding security level detailed in Table 1.

Table 1 UT-125 FIPS #10 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 #10 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 #10. 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 involved in the services which conduct the encryption and decryption of communication, invoke self tests, and indicate the status of the UT-125 FIPS #10.

3.2 Services

The security services and functions available in the UT-125 FIPS #10 along with the applicable operator role for each service and function can be found in Table 2 below.

Table 2 UT-125 FIPS #10 Services and Roles

Service	Crypto Officer	User
Show Status	○	○
Self Test	○	○
Power Off	○	○
Power Save	○	○
Encryption	○	○
Decryption	○	○
Key Load	○	
Show OTAR Status	○	○
OTAR Management	○	○
Firmware Update	○	
System Management	○	○

The UT-125 FIPS #10 supports the following approved security functions:

- AES (Cert. # 1303)
- HMAC (Cert. # 758)
- SHS (Cert. # 1193)
- RNG Cert # 726)

The UT-125 FIPS #10 also supports the following non-approved security functions:

- AES MAC (AES Cert. #1303, vendor affirmed; P25 AES OTAR)
- DES
- DES-MAC

3.3 Identification and Authentication

Operator identification and authentication of roles are not required or supported by the UT-125 FIPS #10.

4. Secure Operation and Rules

This section details the security rules which should be enforced for the secure use of the UT-125 FIPS #10 and the physical security employed.

4.1 Security Rules

The security rules presented below are 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 DES and DES MAC is not allowed in the FIPS approved mode of operation.

4.2 Physical Security

The UT-125 FIPS #10 is 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 #10 has 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[1]. The use of 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.

5. Access Control Policy

[1] 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.

Table 3 UT-125 FIPS #10 Cryptographic Keys and CSPs Definition

Keys and CSPs	Description
Secret Key	256-bit AES or 56-bit DES Cryptographic Key
Traffic Encryption Key	Key used for encryption/decryption of voice traffic through the module's host radio.
Key Encryption Key	Key used for encryption/decryption of Cryptographic Key.
Warm Start Key	Temporal Key used for OTAR "Warm Start" Block
Reverse Warm Start Key	Temporal Key used for OTAR "Reverse Warm Start" Block
RNG Seed	20-byte seed value used as part of the module's FIPS 186-2 RNG.
RNG Key	20-byte seed key used as part of the module's FIPS 186-2 RNG.
HMAC Key	64-byte key used as part of module's HMAC-SHA-1 firmware-load test.

Table 4 UT-125 FIPS #10 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[2]	U
Decryption	Any Secret Key	U
RNG	RNG Key	W, U
	RNG Seed	U
Key Load	Any Secret Key	E, W
Show OTAR Status	-	-
OTAR Management	Any Secret Key	E, U, R, W
Firmware Update	HMAC Key	U
System Management	HMAC Key	E
	RNG Key	E

In Table 4 above the following key should be used:

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

[2] Any Secret Key refers to the four "sub-keys" identified in Table 3 (Traffic Encryption Key, Key Encryption Key, Warm Start Key, and Reverse Warm Start Key)

Where each of the above references the type of access the service has to the listed keys and Critical Security Parameters (CSP) on Table 4.

6. Mitigation of Other Attacks

The UT-125 FIPS #10 has not been designed to mitigate attacks outside of those required within the FIPS 140-2 document.