FIPS 140-2 Security Policy

Digital Unit

UT-120 #10 and #11 Cryptographic Module

ICOM AMERICA, INC.
2380 116th AVE NE
Bellevue, WA 98004

Document Version 1.6
November 28, 2007

Table of Contents

1. Introduction

This document details the security policy for the Digital Unit UT-120 #10 and #11 hardware version 1.1 implementing firmware Rev 3.0 version 2.8, herein identified as the UT-120 #10 and UT-120 #11, employed in ICOM AMERICA, INC. radios. This security policy may be freely reproduced and distributed only in its entirety without revision.

1.1 Purpose

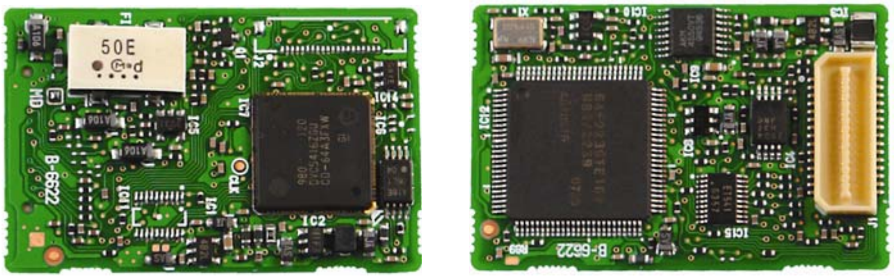
The secure operation of the UT-120 #10 or UT-120 #11 is detailed in this document to include the requirements of FIPS 140-2 and those imposed by ICOM AMERICA, INC. as applicable to the initialization, roles, and responsibilities of security related data and components management.

1.2 Digital Unit Implementation

The UT-120 #10 (or UT-120 #11) is a multiple-chip embedded cryptographic module as defined by FIPS 140-2. The UT-120 #10 (or UT-120 #11) can be incorporated into any ICOM AMERICA, INC. radio which requires FIPS 140-2 level 1 cryptographic security.

1.3 Cryptographic Boundary

The UT-120 #10 (or UT-120 #11) 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-120 #10 and #11 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-120 #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-120 #10 and #11 supports the roles of Crypto Officer and User. Only one role can exist at any one time as they are mutually exclusive.

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-120 #10 and #11. 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-120 #10 and #11.

Maintenance

Assumption of the Maintenance role is implied after the operator accesses the module using the MD pin on the module's PCB and performs the procedural zeroization of the firmware and EEPROM contents.

3.2 Services

The security services and functions available in the UT-120 #10 and #11 along with the applicable operator role for each service and function can be found in Table 2 below.

Table 2 UT-120 #10 and #11 Services and Roles

Service	**Crypto Officer**	**User**	**Maintenance**
Reset	○	○	
Power Off	○	○	○
Firmware Update	○		
Display Crypto Status		○	
Transmit Crypto On/Off		○	
Receive Crypto On/Off		○	
Change Key Setting (CKR)		○	
Read Key Setting (CKR)	○	○	
Self Test		○	
Read Crypto Key	○		○
Write Crypto Key	○		○
Zeroize Key Contents	○	○	○
AES On/Off	○	○	
DES On/Off	○	○	
APCO25 On/Off	○	○	
Switch Between Transmit and Receive		○	

The UT-120 #10 and #11 supports the following approved security functions:

- AES (Cert. # 422)
- HMAC (Cert. # 197)
- SHA-1 (Cert. # 493)

The UT-120 #10 and #11 also supports the following non-approved security functions:

- DES
- ANSI X9.31 PRNG

The AES On/Off service allows the operator to transition the module into a bypass state. In this state, with AES off, the operator would be transmitting data in the clear with no encryption. The module can be transitioned back to the encrypted mode of operation by turning AES on again.

The UT-120 #10 and #11 performs a conditional bypass test for both the transition into and the transition out of the bypass state.

3.3 Identification and Authentication

Operator identification and authentication of roles are not required or supported by the UT-120 #10 and #11.

4. Secure Operation and Rules

This section details the security rules which should be enforced for the secure use of the UT-120 #10 (or UT-120 #11) 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 AMERICA, INC.

FIPS 140-2 Security Rules

The following rules are required to operate in accordance with FIPS 140-2:

1. Enable a FIPS authorized mode.
2. The FIPS approved cryptographic algorithms are required (specifically AES).
3. Have at least one button programmed to enact the “Zeroize” function.

ICOM Security Rules

1. Loaded keys shall be generated by a FIPS 140-2 approved device.
2. The UT-120 #10 and #11 has a limited operational environment implemented in hardware and is not-user modifiable. Firmware updates are only available from ICOM AMERICA, INC. and are verified to be from ICOM AMERICA, INC. using the HMAC-SHA1 algorithm.
3. Any non-validated firmware subsequently loaded will invalidate the original validation.

Maintenance Role and Interface

The Maintenance role can only be used once, since the procedure for entering the maintenance role effectively performs the zeroization of all CSPs including the HMAC integrity load key. In order to recover from this state, the UT-120 #10 and #11 must be returned to the manufacturer.

The following steps are performed to enter the maintenance role:

1. Attach the module to a general purpose computer using the ‘MD’ pin on the module’s printed circuit board.
2. Zeroize the contents of the EEPROM and firmware

4.2 Physical Security

The UT-120 #10 and #11 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-120 #10 (or UT-120 #11) has modes of operation which are not FIPS 140-2 approved. Therefore, the following set of configuration procedures and parameters should be followed to use the UT-120 #10 in a FIPS 140-2 compliant manner:

1. With the CS-F70 cloning software installed on your PC connect the radio and PC together using an OPC-1122 cloning cable.
2. Turn on the encryption for the channels with which you will operate in a FIPS 140-2 approved mode by selecting the column labeled “Encryption” on the software user interface.
3. Select the CKR (Common Key Reference) number corresponding to the FIPS approved algorithm CKR on the key loading device.
4. Select the buttons you wish to assign the functions of encryption and zeroize to. These functions are both FIPS 140-2 approved modes of operation.
5. Disconnect the OPC-1122 cable from the radio.
6. Turn the radio on.
7. Select the channel programmed with the FIPS 140-2 approved algorithms from steps 2 and 3 above.
8. Press the button to which the encryption function was assigned.
9. The radio is now configured to operate in a FIPS 140-2 compliant manner.

The approved modes of operation available on the UT-120 #10 and #11 are AES-256 bit for encryption and decryption and zeroize for clearing the AES key. All other modes available are not FIPS 140-2 approved and therefore are not authorized when the UT-120 #10 (or UT-120 #11) is to be employed in a manner compliant with FIPS 140-2.

5. Access Control Policy

Table 3 UT-120 #10 and #11 Services, Keys, and Access

	Cryptographic Keys, CSPs & Type of Access					
Service	TEK[1]	Reset	Firm Update	AES ON	Seed	Key Load
Reset		W				
Firmware Update			W			
Crypto Status for Display						
Transmit Cryptographic On/Off	S			W		S
Receive Cryptographic On/Off	S			W		S
Changing Key Setting (CKR)	S					S
Reading Key Setting (CKR)	N			R		
Self Test	S			W	S	S
Reading Cryptographic Key	N					
Writing cryptographic Key	W					S
Zeroize Key Contents	D					S
Power Off						
Switch Between Transmit and Receive	S				S	S
Declaring Use Right of Encryption	S			W		S
APCO25 On/Off	S			W		S

In Table 3 above the following key should be used:

D	Delete
N	None
R	Read
S	Select
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 3.

[1] Traffic Encryption Key – The AES (approved) or DES (non-approved) key value used to perform encryption and decryption.

6. Mitigation of Other Attacks

The UT-120 #10 and #11 has not been designed to mitigate attacks outside of those required within the FIPS 140-2 document.