Icom Inc.

UT-125 FIPS #41,#51 and #61

FIPS 140-3 Non-Proprietary Security Policy

1-1-32 Kamiminami
Hirano-ku, Osaka 547-0003
Japan

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 5
2.1 Description 5
2.2 Tested and Vendor Affirmed Module Version and Identification 7
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 8
2.6 Security Function Implementations 10
2.7 Algorithm Specific Information 11
2.8 RBG and Entropy 11
2.9 Key Generation 11
2.10 Key Establishment 11
2.11 Industry Protocols 11
3 Cryptographic Module Interfaces 11
3.1 Ports and Interfaces 11
4 Roles, Services, and Authentication 12
4.1 Authentication Methods 12
4.2 Roles 12
4.3 Approved Services 12
4.4 Non-Approved Services 19
4.5 External Software/Firmware Loaded 19
5 Software/Firmware Security 19
5.1 Integrity Techniques 19
5.2 Initiate on Demand 19
6 Operational Environment 19
6.1 Operational Environment Type and Requirements 19
6.2 Configuration Settings and Restrictions 20
7 Physical Security 20
7.1 Mechanisms and Actions Required 20
8 Non-Invasive Security 20
9 Sensitive Security Parameters Management 20
9.1 Storage Areas 20
9.2 SSP Input-Output Methods 20

9.3 SSP Zeroization Methods 21
9.4 SSPs 21
10 Self-Tests 24
10.1 Pre-Operational Self-Tests 24
10.2 Conditional Self-Tests 24
10.3 Periodic Self-Test Information 25
10.4 Error States 26
10.5 Operator Initiation of Self-Tests 26
11 Life-Cycle Assurance 27
11.1 Installation, Initialization, and Startup Procedures 27
11.2 Administrator Guidance 27
11.3 Non-Administrator Guidance 27
11.4 Design and Rules 27
11.5 Maintenance Requirements 27
11.6 End of Life 27
12 Mitigation of Other Attacks 27

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Hardware 8
Table 3: Modes List and Description 8
Table 4: Approved Algorithms 9
Table 5: Vendor-Affirmed Algorithms 9
Table 6: Non-Approved, Not Allowed Algorithms 10
Table 7: Security Function Implementations 11
Table 8: Ports and Interfaces 12
Table 9: Roles 12
Table 10: Approved Services 18
Table 11: Non-Approved Services 19
Table 12: Mechanisms and Actions Required 20
Table 13: Storage Areas 20
Table 14: SSP Input-Output Methods 21
Table 15: SSP Zeroization Methods 21
Table 16: SSP Table 1 22
Table 17: SSP Table 2 24
Table 18: Pre-Operational Self-Tests 24
Table 19: Conditional Self-Tests 25
Table 20: Pre-Operational Periodic Information 25
Table 21: Conditional Periodic Information 26
Table 22: Error States 26

List of Figures

Figure 1 - Block Diagram 6
Figure 2 – Representative Images 7

1 General

1.1 Overview

This document details the security policy for the cryptographic module UT-125 FIPS #41 Hardware revision 2.2 and Hardware revision 2.3, UT-125 FIPS #51 Hardware revision 2.4 and Hardware revision 2.5, UT-125 FIPS #61 Hardware revision 2.6 and Hardware revision 2.7 implementing firmware version 1.4, herein identified as the optional encryption unit, UT-125 FIPS #41,#51 and #61 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

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
	Overall Level	1

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The UT-125 FIPS #41, #51 and #61 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.

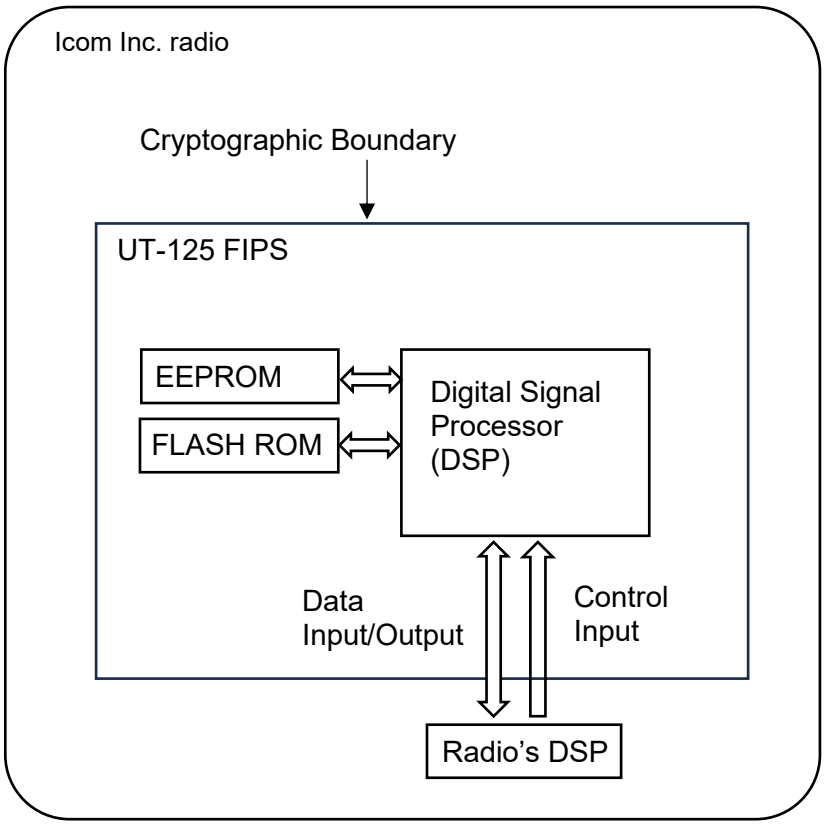
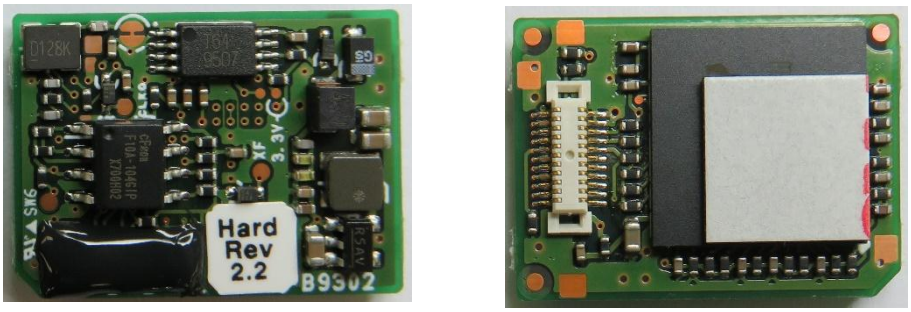


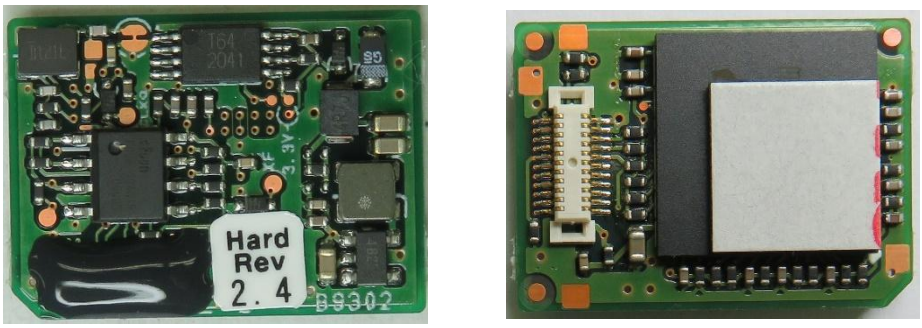
Figure 1 - Block Diagram

Figure 2 contains representative images of the cryptographic module. Other than the labels, Rev 2.2 and 2.3 of the UT-125 #41 are externally identical. Likewise, Rev 2.4 and 2.5 of UT-125 #51, Rev 2.6 and Rev 2.7 of UT-125 #61 are also externally identical.

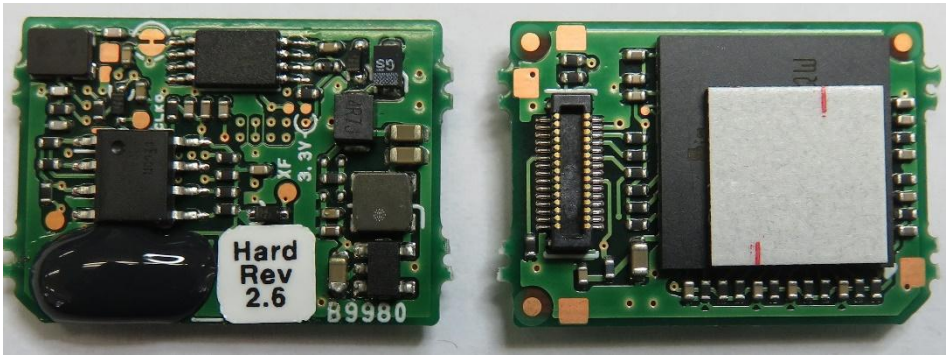
#41



#51



#61



Top Bottom

Figure 2 – Representative Images

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
UT-125 #41	Rev2.2 and Rev2.3	Rev. 1.7	TMS320VC5507ZAY	Label, Display on the radio display.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
UT-125 #51	Rev2.4 and Rev2.5	Rev. 1.7	TMS320VC5507ZAY	Label, Display on the radio display.
UT-125 #61	Rev2.6 and Rev2.7	Rev. 1.7	TMS320VC5507ZAY	Label, Display on the radio display.

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

The cryptographic module does not have any Excluded components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	Approved Algorithm running	Approved	High-Level Status Indicator via GPIO9 Port
Non-approved Mode	When Approved Algorithm is not running	Non-Approved	Low-Level Status Indicator via GPIO9 Port

Table 3: Modes List and Description

Mode Change Instructions and Status:

The cryptographic module supports both approved and non-approved modes depending on the McBSP interface commands being invoked. The GPIO9 port indicates whether the module is using an Approved security function by providing a High-Level Status Output for services using approved security functions and a Low-Level Status Output for all other services.

Degraded Mode Description:

The cryptographic module does not support degraded operation.

2.5 Algorithms

Approved Algorithms:

The module's CAVP certificates include 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.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6944	Direction - Encrypt Key Length - 256	SP 800-38A
AES-CMAC	A6944	Direction - Generation, Verification Key Length - 256	SP 800-38B

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A6944	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-KW	A6944	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38F
AES-OFB	A6944	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
Counter DRBG	A6944	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
HMAC-SHA-1	A5246	Key Length - Key Length: 512	FIPS 198-1
HMAC-SHA2-256	A6944	Key Length - Key Length: 256	FIPS 198-1
KDF SP800-108	A6944	KDF Mode - Counter Supported Lengths - Supported Lengths: 256	SP 800-108 Rev. 1
SHA-1	A5246	Message Length - Message Length: 256-65536 Increment 8	FIPS 180-4
SHA2-256	A6944	Message Length - Message Length: 256-65536 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG Section 4	Key Type:Symmetric	N/A	SP800-133r2, Section 4 Example 1

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

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:

N/A for this module.

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:

Name	Use and Function
AES-CBC-MAC	MAC for OTAR

Name	Use and Function
DES ECB	Crypto Key Encryption / Decryption
DES OFB	Voice Encryption / Decryption
PRNG	Pseudo-Random Number Generator

Table 6: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Crypto Channel	BC-UnAuth	AES Ciphers		AES-OFB: (A6944) AES-CBC: (A6944) AES-ECB: (A6944)
Crypto Channel KTS	KTS-Unwrap KTS-Wrap	Key Wrapping	Standard:SP 800-38F IG D.G:Approved Key Wrapping Method 2 Caveat:Key establishment methodology provides 256-bits of security strength	AES-KW: (A6944) AES-ECB: (A6944)
Firmware Data Integrity	MAC	Data Integrity		HMAC-SHA-1: (A5246) SHA-1: (A5246)
Key Derivation	KBKDF	Key Derivation for MAC		KDF SP800-108: (A6944) HMAC-SHA2-256: (A6944) SHA2-256: (A6944)
Key Generation	CKG	CKG for Reverse Warm Start Key		Counter DRBG: (A6944) AES-ECB: (A6944) CKG Section 4: () Key Type: Symmetric
Message Authentication	MAC	MAC for OTAR		AES-CMAC: (A6944) AES-CBC: (A6944)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

N/A for this module.

2.8 RBG and Entropy

The module's DRBG is seeded with a factory pre-loaded entropy input string per FIPS 140-3 IG 9.3.A, Scenario 2(a). Therefore, the following caveat applies to this module:

No assurance of the minimum strength of generated SSPs (e.g., keys)

When the module is manufactured, a 256-bit entropy input string believed to contain 256-bits of entropy is written to the Flash ROM.

At the first boot, this entropy input string is used to seed the DRBG. The state of the DRBG instance is maintained even when the module's power is turned off.

2.9 Key Generation

The Reverse Warm Start Key is generated by CKG compliant with SP800-133rev2 Section 4, 6.1. The output U of the approved DRBG is used directly as the symmetric key, with no XOR or post-processing. The DRBG is also fed with 256 bits of entropy from an external source, so the DRBG output also has at least 256 bits of security strength.

The generated symmetric key is used only as the Reverse Warm Start Key in Section 9.4. Please refer to section 9.4 SSPs.

Keys/SSPs generated/used in the approved mode shall not be used in the non-approved mode and vice-versa.

2.10 Key Establishment

N/A for this module.

2.11 Industry Protocols

N/A for this module.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
GND	Power	Ground
CSCKO	Data Output	McBSP clock output
CFSO	Data Output	McBSP frame sync output

Physical Port	Logical Interface(s)	Data That Passes
CFSI	Data Input Control Input	McBSP frame sync input
CSDO	Data Output Status Output	McBSP data output
CSCKI	Data Input Control Input	McBSP clock input
OPRST	Control Input	Reset signal
CSDI	Data Input Control Input	McBSP data input
OPACT	Control Input	Wake up signal
DVDD_3.3V	Power	External electrical power (+3.3V power line)

Table 8: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

This module does not support the operator authentication.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None
User	Role	User	None

Table 9: Roles

4.3 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.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Decryption	Decoding from ciphertext to plaintext	Port Output (GPIO 9)	McBSP command:Control Input or Data Input	McBSP command:Status Output or Data Output	Crypto Channel	Crypto Officer - Reverse Warm

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			(Request Command)	(Response Command)		Start Key: E - TEK(Traffic Encryption Key): E - Warm Start Key: E User - Reverse Warm Start Key: E - TEK(Traffic Encryption Key): E - Warm Start Key: E
Encryption	Encoding from plaintext to ciphertext.	Port Output (GPIO 9)	McBSP command:Control Input or Data Input (Request Command)	McBSP command:Status Output or Data Output (Response Command)	Crypto Channel	Crypto Officer - Reverse Warm Start Key: E - TEK(Traffic Encryption Key): E - Warm Start Key: E User - Reverse Warm Start Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TEK(Traffic Encryption Key): E - Warm Start Key: E
Firmware Update	Updating the firmware in the crypto module.	Port Output (GPIO 9)	McBSP command:Control Input (Request Command)	McBSP command:Status Output (Response Command, Indicate Command)	Firmware Data Integrity	Crypto Officer - CTR_DRBG Key : Z - CTR_DRBG Seed : Z - CTR_DRBG V counter : Z - HMAC Key: E - SP 800-90B ENT (P) Entropy String : Z
Key Load	Loading crypto key using Key Fill Device Interface Protocol.	N/A	McBSP command:Control Input or Data Input (Request Command)	McBSP command:Status Output (Response Command, Indicate Command)	None	Crypto Officer - KEK (Key Encryption Key): W - TEK(Traffic Encryption Key): W
Key Managem	Changing/ Adding/ Generating/	Port Output	McBSP command:Control Input	McBSP command:Status Output	Crypto Channel Key	Crypto Officer - KEK

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
ent (OTAR)	Zeroising crypto key and module parameter.	(GPIO 9)	or Data Input (Request Command)	or Data Output (Response Command)	Derivation Key Generation Crypto Channel KTS	(Key Encryption Key): W,E,Z - Reverse Warm Start Key: G,E,Z - TEK(Traffic Encryption Key): W,E,Z - Warm Start Key: W,E,Z User - KEK (Key Encryption Key): W,E,Z - Reverse Warm Start Key: G,E,Z - TEK(Traffic Encryption Key): W,E,Z - Warm Start Key: W,E,Z
Key Zeroisation	Zeroising crypto key using Key Fill Device Interface Protocol.	N/A	McBSP command:Control Input (Request Command)	McBSP command:Status Output (Response Command)	None	Crypto Officer - KEK (Key Encryption Key):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - TEK(Traffic Encryption Key): Z User - KEK (Key Encryption Key): Z - TEK(Traffic Encryption Key): Z
Message Authentication	Generating/Verification of Message Authentication Code	N/A	McBSP command: Control Input or Data Input (Request Command)	McBSP command: Status Output or Data Output (Response Command)	Message Authentication	Crypto Officer - Reverse Warm Start Key: E - TEK(Traffic Encryption Key): E - Warm Start Key: E User - Reverse Warm Start Key: E - TEK(Traffic Encryption Key): E - Warm

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Start Key: E
Power-Off	Turning the power off on the module.	N/A	McBSP command:Control Input (Request Command)	McBSP command:Status Output (Response Command, Indicate Command)	None	Crypto Officer - CTR_DRBG Key : Z - CTR_DRBG V counter : Z - Reverse Warm Start Key: Z User - CTR_DRBG Key : Z - CTR_DRBG V counter : Z - Reverse Warm Start Key: Z
Self-Tests	Self-testing the operation of the crypto functions.	N/A	Reset signal (Physical port): Control Input	McBSP command: Status Output	None	Crypto Officer User
Show Key Status	Providing the crypto parameter.	N/A	McBSP command:Control Input (Request Command)	McBSP command:Status Output (Response Command)	None	Crypto Officer User
Show Status	Showing current status.	N/A	McBSP command:Control Input (Request Command)	McBSP command:Status Output (Response Command)	None	Crypto Officer User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Version	Show module's versioning information.	N/A	McBSP command:Control Input (Request Command)	McBSP command:Status Output (Response Command)	None	Crypto Officer User
System Management	Zeroising and Initializing the various setting values	N/A	McBSP command:Control Input (Request Command)	McBSP command:Status Output (Response Command)	None	Crypto Officer - KEK (Key Encryption Key): Z - Reverse Warm Start Key: Z - TEK(Traffic Encryption Key): Z - Warm Start Key: Z User - KEK (Key Encryption Key): Z - Reverse Warm Start Key: Z - TEK(Traffic Encryption Key): Z - Warm Start Key: Z

Table 10: Approved Services

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Decryption	Decoding from ciphertext to plaintext	DES OFB	Crypto Officer, User
Encryption	Encoding from plaintext to ciphertext	DES OFB	Crypto Officer, User
Key Management	Changing/Adding/Generating/Zeroising crypto key and module parameter.	AES-CBC-MAC DES ECB PRNG	Crypto Officer, User

Table 11: 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.

5 Software/Firmware Security

The module's firmware is provided as the 3059C4_17.MOT (boot and application firmware) or 3059C4_17(F).MOT (just application firmware) binary images.

5.1 Integrity Techniques

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

5.2 Initiate on Demand

The 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

Mechanism	Inspection Frequency	Inspection Guidance
Production grade components	N/A	N/A

Table 12: 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 non-invasive mitigation techniques.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
DSP RAM	Temporary storage of SSP's	Dynamic
EEPROM	Persistent storage for cryptographic keys	Static
Flash ROM	Persistent storage of firmware and pre-loaded entropy	Static

Table 13: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
KFD Protocol to DSP RAM	External KFD	DSP RAM	Plaintext	Manual	Electronic	

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
KFD Protocol to EEPROM	External KFD	EEPROM	Plaintext	Manual	Electronic	
OTAR Input to DSP RAM	External KMF	DSP RAM	Encrypted	Wireless	Electronic	Crypto Channel KTS
OTAR Input to EEPROM	External KMF	EEPROM	Encrypted	Wireless	Electronic	Crypto Channel KTS
OTAR Output	DSP RAM	External KMF	Encrypted	Wireless	Electronic	Crypto Channel KTS

Table 14: SSP Input-Output Methods

KFD stands for Key Fill Device, which functions as a Key Loader.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Firmware Update	The firmware update process overwrites the factory pre-loaded DRBG SSPs.	Overwritten SSPs are not recoverable	Invoking firmware update service
Power lost	Module power loss causes all SSPs stored in volatile memory to be effectively overwritten with zeroes.	Zeroised SSPs in volatile memory are not recoverable after being effectively overwritten with zeroes.	Disconnecting power from module host radio.
Zeriose command	McBSP Command causes all stored SSPs to be overwritten with zeroes.	Zeroised SSPs in EEPROM or DSP RAM are not recoverable after being overwritten with zeroes.	Send the McBSP command.

Table 15: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
CTR_DRBG Key	Used as part of the internal state of the DRBG	256 bits - 256 bits	DRBG CSP - CSP	Counter DRBG (A6944)		Key Generation
CTR_DRBG Seed	DRBG input of entropy input	384 bits - 256 bits	DRBG CSP - CSP	Manufacturer Pre-loaded		Key Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	string and non-random nonce.					
CTR_DRBG V counter	Used as part of the internal state of the DRBG	128 bits - 128 bits	DRBG CSP - CSP	Counter DRBG (A6944)		Key Generation
HMAC Key	Used for updating the firmware	512 bits - 256 bits	Symmetric - CSP	Manufacturer Pre-loaded		Firmware Data Integrity
KEK (Key Encryption Key)	This is a Key Wrapping Key, and is used for encryption/decryption of other cryptographic Key in OTAR mode.	256 bits - 256 bits	Symmetric - CSP			Crypto Channel Crypto Channel KTS
Reverse Warm Start Key	Reverse Warm Start Key is generated by the module and used by OTAR	256 bits - 256 bits	Symmetric - CSP	Key Generation		Crypto Channel Crypto Channel KTS Key Generation
SP 800-90B ENT (P) Entropy String	Pre-loaded entropy input for DRBG.	256 bits - 256 bits	DRBG CSP - CSP	Manufacturer Pre-loaded		Key Generation
TEK(Traffic Encryption Key)	Used for encryption/decryption of voice and data traffic through the module's host radio.	256-bits - 256-bits	Symmetric - CSP			Crypto Channel Crypto Channel KTS Key Derivation
Warm Start Key	Warm Start Key is generated by an OTAR KMF and used by OTAR	256 bits - 256 bits	Symmetric - CSP	Key Derivation		Crypto Channel Crypto Channel KTS Key Generation

Table 16: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
CTR_DRBG Key		DSP RAM:Plaintext	Until power lost	Power lost	
CTR_DRBG Seed		EEPROM:Plaintext Flash ROM:Plaintext		Zeriose command	
CTR_DRBG V counter		DSP RAM:Plaintext	Until power lost	Power lost	
HMAC Key		EEPROM:Plaintext		Zeriose command	
KEK (Key Encryption Key)	KFD Protocol to DSP RAM KFD Protocol to EEPROM OTAR Input to DSP RAM OTAR Input to EEPROM OTAR Output	EEPROM:Plaintext		Zeriose command	
Reverse Warm Start Key	OTAR Input to DSP RAM OTAR Input to EEPROM	DSP RAM:Plaintext	Until power lost or zeroise command received.	Zeriose command Power lost	
SP 800-90B ENT (P) Entropy String		EEPROM:Plaintext Flash ROM:Plaintext		Zeriose command	
TEK(Traffic Encryption Key)	KFD Protocol to DSP RAM KFD Protocol to EEPROM OTAR Input to DSP RAM OTAR Input to EEPROM OTAR Output	EEPROM:Plaintext		Zeriose command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Warm Start Key	OTAR Input to DSP RAM OTAR Input to EEPROM	DSP RAM:Plaintext	Until power lost	Zeriose command	

Table 17: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
CRC-32	32-bit CRC	KAT	SW/FW Integrity	Status Output	32 bit CRC Check of firmware integrity.

Table 18: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Decryption (A6944)	256-bits	KAT	CAST	Status Output	Decryption	Start-up
AES-CBC Encryption (A6944)	256-bits	KAT	CAST	Status Output	Encryption	Start-up
AES-CMAC Generation (A6944)	256 bit key with 64-bit MAC length	KAT	CAST	Status Output	MAC Generation	Start-up
AES-ECB Decryption (A6944)	256-bits	KAT	CAST	Status Output	Encryption	Start-up
AES-ECB Encryption (A6944)	256-bits	KAT	CAST	Status Output	Decryption	Start-up
AES-OFB Decryption (A6944)	256-bits	KAT	CAST	Status Output	Decryption	Start-up
AES-OFB Encryption (A6944)	256-bits	KAT	CAST	Status Output	Encryption	Start-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG (A6944)	AES-256 with DF	KAT	CAST	Status Output	SP 800-90Ar1 Instantiate, Generate health tests	Start-up
CRC-16	16-bit CRC	Manual Entry Test	Manual Entry	Status Output	Verify	Key load
Firmware Load Test	HMAC-SHA-1	Firmware Load Test	SW/FW Load	Status Output	Verify	Firmware update
HMAC-SHA-1 (A5246)	512 bit key with 160 bit MAC length	KAT	CAST	Status Output	Verify	Start-up
KDF SP800-108 (A6944)	Counter Mode with HMAC-SHA2-256	KAT	CAST	Status Output	Key Derivation	Start-up

Table 19: Conditional Self-Tests

KAT: Known Answer Test
FDT: Fault-Detection Tests
Integrity: Integrity Test

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
CRC-32	KAT	SW/FW Integrity	On demand	Manual

Table 20: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC Decryption (A6944)	KAT	CAST	On demand	Manual
AES-CBC Encryption (A6944)	KAT	CAST	On demand	Manual
AES-CMAC Generation (A6944)	KAT	CAST	On demand	Manual
AES-ECB Decryption (A6944)	KAT	CAST	On demand	Manual
AES-ECB Encryption (A6944)	KAT	CAST	On demand	Manual

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-OFB Decryption (A6944)	KAT	CAST	On demand	Manual
AES-OFB Encryption (A6944)	KAT	CAST	On demand	Manual
Counter DRBG (A6944)	KAT	CAST	On demand	Manual
CRC-16	Manual Entry Test	Manual Entry	On demand	Manual
Firmware Load Test	Firmware Load Test	SW/FW Load	On demand	Manual
HMAC-SHA-1 (A5246)	KAT	CAST	On demand	Manual
KDF SP800-108 (A6944)	KAT	CAST	On demand	Manual

Table 21: Conditional Periodic Information

The module does not perform periodic self-tests.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Application Self-Test Error	Power-Up Self-Test failure state in Application Program	Application Self-Test Error	McBSP command:Control Input	McBSP command:Status Output : $05
Boot Self-Test Error	Power-Up Self-Test failure state in Boot Program	Boot Self-Test Error	McBSP command:Control Input	McBSP command:Status Output : $04
EEPROM Error	EEPROM's communication error state	Boot EEPROM Error Application EEPROM Error	McBSP command:Control Input	McBSP command:Status Output : $03

Table 22: Error States

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
The operator is responsible for ensuring sufficient security strength for the keys being 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 FIPS 140-3 for Level 1 secure use and the security rules separately implemented by Icom Inc.

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.