Harris Corporation

Harris AES Software Load Module

Software Version: 1.0

FIPS 140–2 Non–Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1

Prepared for:

Harris Corporation
1680 University Avenue
Rochester, NY 14610
United States of America

Phone: +1 (585) 244–5830
Email: RFComm@harris.com
http://www.harris.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
United States of America

Phone: +1 (703) 267–6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non–proprietary Cryptographic Module Security Policy for the Harris AES Software Load Module (HALM) from Harris Corporation. This Security Policy describes how the Harris AES Software Load Module meets the security requirements of FIPS 140–2 and how to run the module in a secure FIPS 140–2 mode. This policy was prepared as part of the Level 1 FIPS 140–2 validation of the module.

FIPS 140–2 (Federal Information Processing Standards Publication 140–2 – *Security Requirements for Cryptographic Modules*) details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140–2 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website, which is maintained by National Institute of Standards and Technology (NIST) and the Communication Security Establishment Canada (CSEC): http://csrc.nist.gov/groups/STM/cmvp.

The Harris AES Software Load Module is referred to in this document as the HALM, the cryptographic module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140–2 cryptographic module security policy. More information is available on the module from the following sources:

- The Harris corporate website (http://www.harris.com) contains information on the full line of products from Harris.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm) contains contact information for individuals to answer technical or sales–related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140–2 Submission Package. In addition to this document, the Submission Package contains:

- Executive summary
- Vendor Evidence document
- Finite State Model
- Other supporting documentation as additional references

This Security Policy and the other validation submission documents were produced by Corsec Security Inc., under contract with Harris. With the exception of this Non–Proprietary Security Policy, the FIPS 140–2 Validation Documentation is proprietary to Harris and is releasable only under appropriate non–disclosure agreements. For access to these documents, please contact Harris.

2 HALM Overview

2.1 Overview

Harris is a leading supplier of systems and equipment for public safety, federal, utility, commercial, and transportation markets. Their products range from the most advanced IP[1] voice and data networks, to industry-leading multiband/multimode radios, and even public safety-grade broadband video and data solutions. Their comprehensive line of software–defined radio products and systems support the critical missions of countless public and private agencies, federal and state agencies, and government, defense, and peacekeeping organizations throughout the world. This Security Policy documents the security features of the Harris AES Software Load Module (HALM) incorporated into the Harris 5300 (Mobile 800Mhz only), 5400 (Portable only), 5500 (Portable only), 7200, 7300, Unity, XG-75 UHF-L, XG-75 VHF XG-75 (800 MHz) and other terminal products, which are single and multi–band multi–mode radios that deliver end–to–end encrypted digital voice and data communications, and are Project 25 Phase 2 upgradable[2]. The HALM is identified as part SK-015086-001 R03A06.

Figure 1 – HALM Portable Terminals (Right to left: 5400, 7200, 7300, and Unity)

Figure 2 – HALM Mobile Terminals (Right to left: 5300, 7200, 7300, and Unity)

[1] IP – Internet Protocol
[2] Once the Telecommunications Industry Association (TIA) standard is finalized

The terminal products discussed in this Security Policy support FIPS-Approved secure voice and data communication using Advanced Encryption Standard (AES) algorithm encryption/decryption as specified in FIPS 197. The terminal products also ensure data integrity using a Message Authentication Code (MAC) algorithm as specified in Special Publication 800–38B. The FIPS 140-2 cryptographic module providing the cryptographic services to the terminals is a single software component called the Harris AES Software Load Module. The HALM provides cryptographic services directly to a Digital Signal Processor (DSP) application on Harris terminals.

The Harris AES Software Load Module is validated at the following FIPS 140–2 Section levels:

Table 1 – Security Level Per FIPS 140–2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[3]	1
9	Self–tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The Harris AES Software Load Module is a Level 1 software module with a multi–chip standalone physical embodiment. The physical cryptographic boundary of the HALM is the outer chassis of the terminal in which it is stored and executed. The logical cryptographic boundary of the Harris AES Software Load Module is defined by a single executable (HALM_module_R03A06.ess) running on a DSP/BIOS[4] 5.33.03 software kernel within the Harris terminals. The kernel is a modifiable operational environment since the DSP is also processing instructions supporting the non-security aspects of the terminal. See Figure 3 for a depiction.

The module is entirely encapsulated by the logical cryptographic boundary shown in the figure below. The logical cryptographic boundary of the module is shown with a teal–colored dotted line.

[3] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[4] BIOS – Basic Input Output System

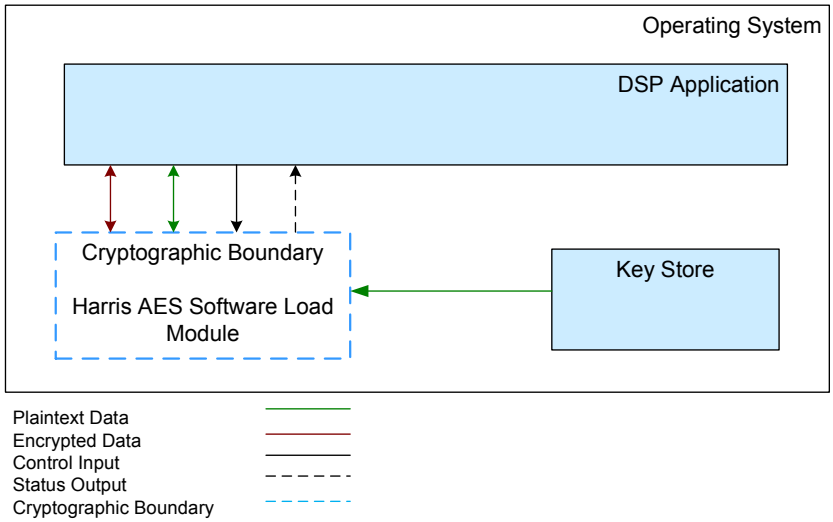

Figure 3 – Logical Cryptographic Boundary

The Harris terminal hardware that uses the HALM is designed around a Texas Instruments (TI) TMS320C55x device. Each terminal supports a Liquid Crystal Display (LCD), Light Emitting Diode (LED), keypad, speaker, microphone, Universal Device Connector (UDC), and a number of buttons, knobs and switches (as defined in Table 2 and Table 3). Enclosure of the terminal is considered to be the physical cryptographic boundary of the module as shown with a teal–colored dotted line in Figure 4 below.

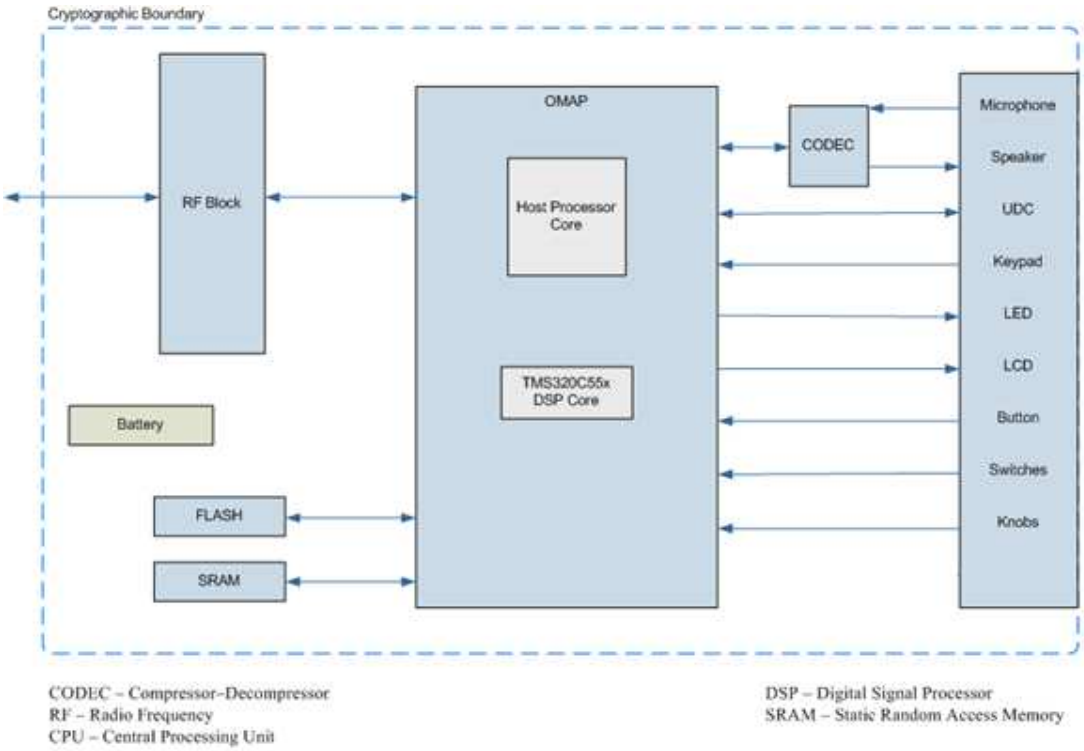

Figure 4 – Physical Cryptographic Boundary

2.3 Module Interfaces

The HALM implements distinct module interfaces in its software design. Physically, the module ports and interfaces are considered to be those of the Harris terminals on which the software executes. However, the software communicates through an Application Programming Interface (API), which allows a DSP application to access the executable. Both the APIs and the physical ports in interfaces can be categorized into the following logical interfaces defined by FIPS 140–2:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

These logical interfaces (as defined by FIPS 140–2) map to the module's physical interfaces, as described in Table 2 and Table 3.

Table 2 – FIPS 140–2 Logical Interfaces (Portable terminal)

FIPS 140–2 Logical Interface	Terminal Physical Port/Interface	Harris AES Software Load Module Interface

FIPS 140–2 Logical Interface	Terminal Physical Port/Interface	Harris AES Software Load Module Interface
Data Input Interface	• Antenna • Microphone • UDC	Arguments for an API call to be used or processed by the module
Data Output Interface	• Speaker • Antenna • LCD • LED • UDC	Arguments for an API call that specify where the result of the API call is stored
Control Input Interface	• Keypad • Knobs: Voice Group Selection Knob, Power On–Off/Volume Knob • Buttons: Emergency Button, PTT[5] Button, Option 1 Button, Option 2 Button • A/B Switch • UDC	API call and accompanying arguments used to control the operation of the module
Status Output Interface	• Speaker • Antenna • UDC • LCD • LED	Return values for API calls
Power Interface	Not applicable[6]	Not applicable

Table 3 – FIPS 140–2 Logical Interfaces (Mobile terminal)

FIPS 140–2 Logical Interface	Terminal Physical Port/Interface	Harris AES Software Load Module Interface
Data Input Interface	• Antenna Port • GPS Port • Serial Port (DB9) • CAN[7] Ports (qty 2) • I/O Port (44pin D–sub)	Arguments for an API call to be used or processed by the module

[5] PTT – Push–to–talk

[6] The battery is within the physical cryptographic boundary, which means that it is not considered as providing power input.

[7] CAN – Controller Area Network

FIPS 140–2 Logical Interface	Terminal Physical Port/Interface	Harris AES Software Load Module Interface
Data Output Interface	• Antenna Port • Serial Port (DB9) • CAN Ports (qty 2) • I/O Port (44pin D–sub)	Arguments for an API call that specify where the result of the API call is stored
Control Input Interface	• Antenna Port • Serial Port (DB9) • CAN Ports (qty 2) • I/O Port (44pin D–sub)	API call and accompanying arguments used to control the operation of the module
Status Output Interface	• Antenna Port • GPS Port • Serial Port (DB9) • CAN Ports (qty 2) • I/O Port (44pin D–sub)	Return values for API calls
Power Interface	DC Power Input	Not Applicable

2.4 Roles and Services

There are two roles in the module (as required by FIPS 140–2) that operators may assume: a Crypto–Officer role and a User role. The terminal operator implicitly assumes one of these roles when selecting each command documented in this section.

2.4.1 Crypto–Officer Role

The Crypto–Officer (CO) role is responsible for initializing the module, self–test execution, and status monitoring. Descriptions of the services available to the CO are provided in the table below. Please note that the keys and CSPs listed in the table indicate the type of access required:

- R - Read access: The Critical Security Parameter (CSP) may be read.
- W - Write access: The CSP may be established, generated, modified, or zeroized.
- X - Execute access: The CSP may be used within an Approved security function.

Table 4 – Mapping of Crypto–Officer Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
HALM_INITIALIZE	Performs self–tests on demand	API call	Status output	None
HALM_UNWRAP_KEY	Unwraps a key	API call, key, data	Status output, key	AES key – X

Service	Description	Input	Output	CSP and Type of Access
HALM_MAC_GENERATION	Generates a Message Authentication Code (MAC)	API call	Status output	AES key – X

2.4.2 User Role

The User role has the ability to perform the module's cipher operation, and data or voice conversion services. Descriptions of the services available to the role are provided in the table below. Type of access is defined in section 2.4.1 of this document.

Table 5 – Mapping of User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
HALM_GEN_KEYSTREAM	Generates keystream data	API call	Status output	AES key – X
HALM_GEN_PRIVATE_MI	Generates a Message Indicator (MI) from the Initialization Vector (IV) value specified in the data input buffer	API call	Status output	AES key – X
HALM_P25_XOR	Performs logical exclusive or operation	API call, Plaintext or Ciphertext	Status output, Plaintext or Ciphertext	None
HALM_LOAD_KEY	Load key into the module	API call, key	Status output	AES key – R
HALM_WRAP_KEY	Wraps a key	API call, key	Status output, wrapped key	AES key – X
HALM_SEND_STATUS	The status of the last functions called from the HALM_API is returned	API call	Status output	None
HALM_AES_OFB	AES OFB Encrypt	API call, key	Status output, encrypted data	AES key – X
HALM_AES_ECB	AES ECB Encrypt	API call, key	Status output, encrypted data	AES key – X
HALM_AES_ECB_DECRYPT	AES ECB Decrypt	API call, key	Status output, decrypted data	AES key – X
HALM_AES_CBC	AES CBC Encrypt	API call, key	Status output, encrypted data	AES key – X
HALM_AES_CMAC	AES CMAC	API call, key	Status output, MAC	AES key – X

2.5 Physical Security

The physical security requirements do not apply since the HALM is a software module, which does not implement any physical security mechanisms.

2.6 Operational Environment

The software module was tested and found to be compliant with FIPS 140–2 requirements on the DSP/BIOS 5.33.03 software kernel. The operating system is designed for single user mode and no further action is required to modify the environment for FIPS 140–2 compliance (see section 3 for guidance).

All cryptographic keys and CSPs are under the control of the OS[8], which protects the CSPs against unauthorized disclosure, modification, and substitution. The module only allows access to CSPs through its well–defined APIs. The module performs a Software Integrity Test using the AES Cipher–based MAC (CMAC) algorithm.

2.7 Cryptographic Key Management

The module implements the following FIPS–Approved algorithms:

Table 6 – FIPS–Approved Algorithm Implementations

Algorithm	Certificate Number
AES 256–bit ECB[9], CBC[10], OFB[11]	1482
AES CMAC	1482

[8] OS – Operating System
[9] ECB – Electronic Code Book
[10] CBC – Cipher Block Chaining
[11] OFB – Output Feedback

The module supports the following critical security parameters:

Table 7 – List of Cryptographic Keys and CSPs

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
AES key	ECB, CBC and OFB modes use 256–bit key	Enters the module in plaintext	Never exits the module	Plaintext in volatile memory and flash memory	Power cycle zeroizes volatile memory; zero key procedure documented in terminal's Operator's Manual zeroizes external flash memory.	Used as input into the cipher operation

2.8 Self–Tests

The Harris AES Software Load Module performs the following self–tests at power–up:

Table 8 – List of Power–Up Self–Tests

Power–Up Test	Description
AES Known Answer Test (KAT)	The AES KAT takes known key, and plaintext value, which is encrypted and compared to the expected ciphertext value. If the values differ, the test fails. The AES KAT then reverses this process by taking the ciphertext value and key, performing decryption, and comparing the result to the known plaintext value. If the values differ, the test fails. If they are the same, the test passes.
Software Integrity Test	The module checks the integrity of the binary (using a CMAC checksum value) at the power–up. If the MAC verifies (i.e., the newly–computed MAC is the same as the stored MAC value), the test passes. Otherwise, it fails.

The module enters the locked error state if it fails either power-up test. An operator may either restart the terminal, by power cycling the unit or return the terminal to a service depot. The module does not implement any Conditional Self–Test.

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any additional attacks in an approved FIPS mode of operation.

3 Secure Operation

The Harris AES Software Load Module meets Level 1 requirements for FIPS 140–2. The sections below describe how to place and keep the module in a FIPS–approved mode of operation.

3.1 Secure Management

The Harris AES Software Load Module is provided to the Crypto–Officer preloaded in the Harris terminals and is not distributed as a separate executable. The CO does not have to perform any action in order to install or configure the module in the terminals. The HALM is installed and always operates in a FIPS–Approved mode of operation.

3.1.1 Initialization

FIPS 140–2 mandates that a software cryptographic module at Security Level 1 shall be restricted to a single operator mode of operation. However, the operational environment of the module, the DSP/BIOS software kernel, is always in single operator mode by design. Hence, no additional step is required to fulfill the requirement.

3.1.2 Management

The Crypto–Officer should monitor the module's status regularly. If any irregular activity is noticed or the module is consistently reporting errors, then Harris customer support should be contacted.

3.1.3 Zeroization

The module does not store any keys or CSPs within its logical boundary. All ephemeral keys used by the module are zeroized upon reboot or session termination. Outside the module, external flash memory stores operational keys. These keys are loaded at the point of origin, and may be zeroized by the operator of the radio using the Key Zero procedure documented in the terminal's Operator's Manual. After the external flash memory keys are zeroized, the radio must be returned to the point of origin for repair.

3.2 User Guidance

Users can access only the module's cryptographic functionalities that are available to them. Although the User does not have any ability to modify the configuration of the module, they should report to the Crypto–Officer if any irregular activity is noticed.

4 Acronyms

This section describes the acronyms.

Table 9 – Acronyms

Acronym	Definition
ADC	Analog to Digital Converter
AES	Advanced Encryption Standard
API	Application Programming Interface
BIOS	Basic Input/Output System
CBC	Cipher Block Chaining
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Crypto–Officer
CODEC	Compressor-Decompressor
CPLD	Complex Programmable Logic Device
CRC	Cyclical Redundancy Check
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DAC	Digital to Analog Converter
DSP	Digital Signal Processor
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HALM	Harris AES Software Load Module
IP	Internet Protocol
IV	Initialization Vector
KAT	Known Answer Test
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MAC	Message Authentication Code
MI	Message Indicator
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OMAP	Open Multimedia Application Platform
OS	Operating System

Acronym	Definition
PTT	Push-to-talk
RAM	Random Access Memory
RX	Receive
SRAM	Static Random Access Memory
TI	Texas Instruments
TX	Transmit
UDC	Universal Device Connector

Prepared by:
Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030
United States of America

Phone: +1 (703) 267–6050
Email: info@corsec.com
http://www.corsec.com