Harris Corporation

Harris AES Load Module

Firmware Version: R06A02

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.7

Prepared for:

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

Phone: +1 585 242-3214
Email: RFComm@harris.com
http://www.harris.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 22033
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 Load Module from Harris Corporation. This Security Policy describes how the Harris AES Load Module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which 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 National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The Harris AES Load Module is referred to in this document as the HALM, the crypto 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 about the products incorporating the module is available from the following sources:

- The Harris 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/140-1/140val-all.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:

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

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Harris. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package 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 Load Module (HALM), which is incorporated into terminal products provided by Harris Corporation, such as the XL family of radios, in order to provide FIPS-Approved security functions.

The Harris AES Load Module provides support to secure voice and data communications by providing Advanced Encryption Standard (AES) algorithm encryption/decryption as specified in FIPS 197. The HALM ensures data integrity using a Cipher-based Message Authentication Code (CMAC) algorithm as specified in Special Publication 800-38B. The HALM interacts with a Digital Signal Processor (DSP) application executing on the Harris XL family of radios and other terminal products in order to provide its services to those terminals.

The Harris AES Load Module is validated at the FIPS 140-2 Section levels shown in Table 1.

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	1
6	Operational Environment	N/A
7	Cryptographic Key Management	1
8	EMI/EMC[2]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The Harris AES Load Module is a Level 1 firmware module with a multiple-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 Load Module is defined by a single executable (HALM.bin; Firmware Version: R06A02) running on Harris BIOS[3] Kernel

[1] IP – Internet Protocol
[2] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[3] BIOS – Basic Input/Output System

v1 within the Harris terminals. The Harris BIOS Kernel v1 acts as the module's operating system, and is provided by the internal Blackfin BF707 DSP. The kernel is a non-modifiable operational environment.

The HALM is stored in flash memory while the host terminal is powered off. When power is supplied to the radio, the terminal's Freescale Vybrid VF5xx GPP[4] transfers the HALM from flash memory to the SRAM[5]of the DSP. Figure 1 shows the module executing in SRAM memory. The module is entirely encapsulated by the logical cryptographic boundary, shown in Figure 1 below. The logical cryptographic boundary of the module is shown with a red-colored dotted line.

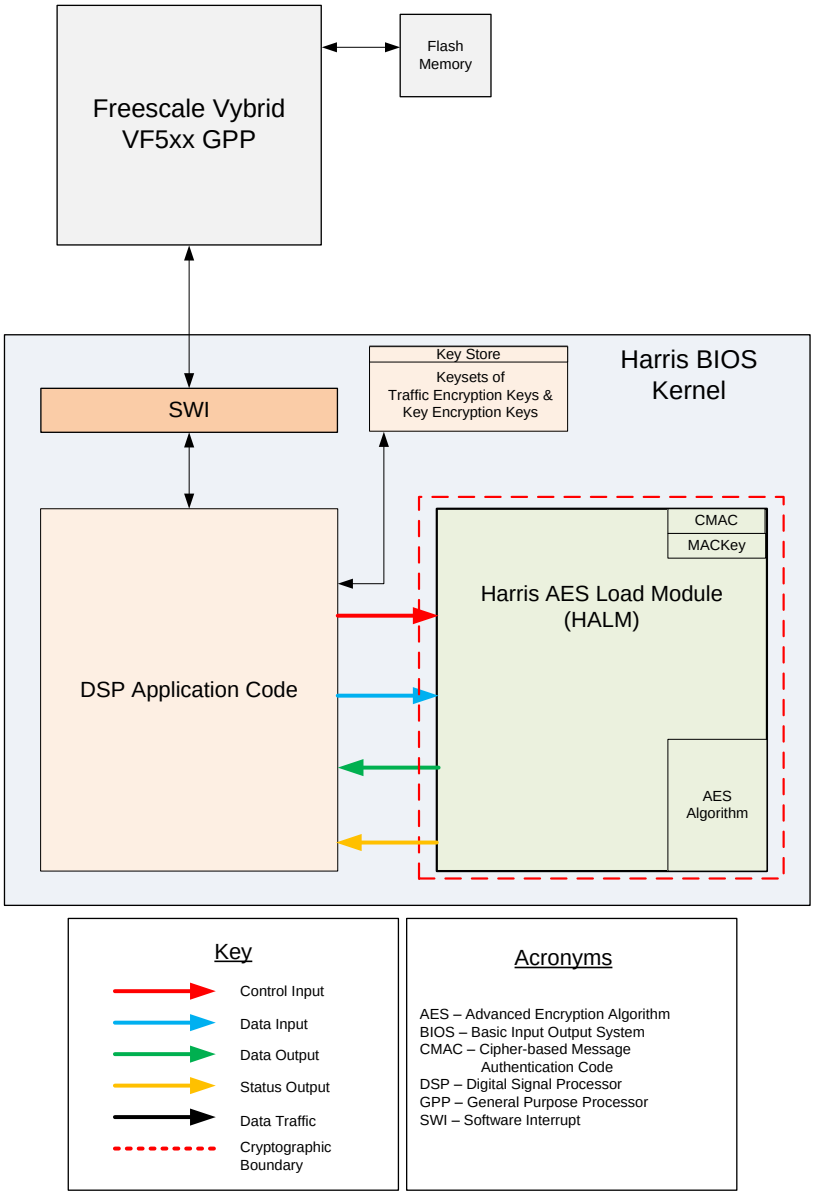

Figure 1 – Logical Cryptographic Boundary

As a firmware cryptographic module, the Harris AES Load Module has a physical cryptographic boundary in addition to its logical cryptographic boundary. The Harris terminal hardware that uses the HALM is

[4] GPP – General Purpose Processor
[5] SRAM – Static Random Access Memory

designed around the Freescale VF5xx GPP. The enclosure of the terminal is considered to be the physical cryptographic boundary of the module as shown with a red-colored dotted line in Figure 2 below.

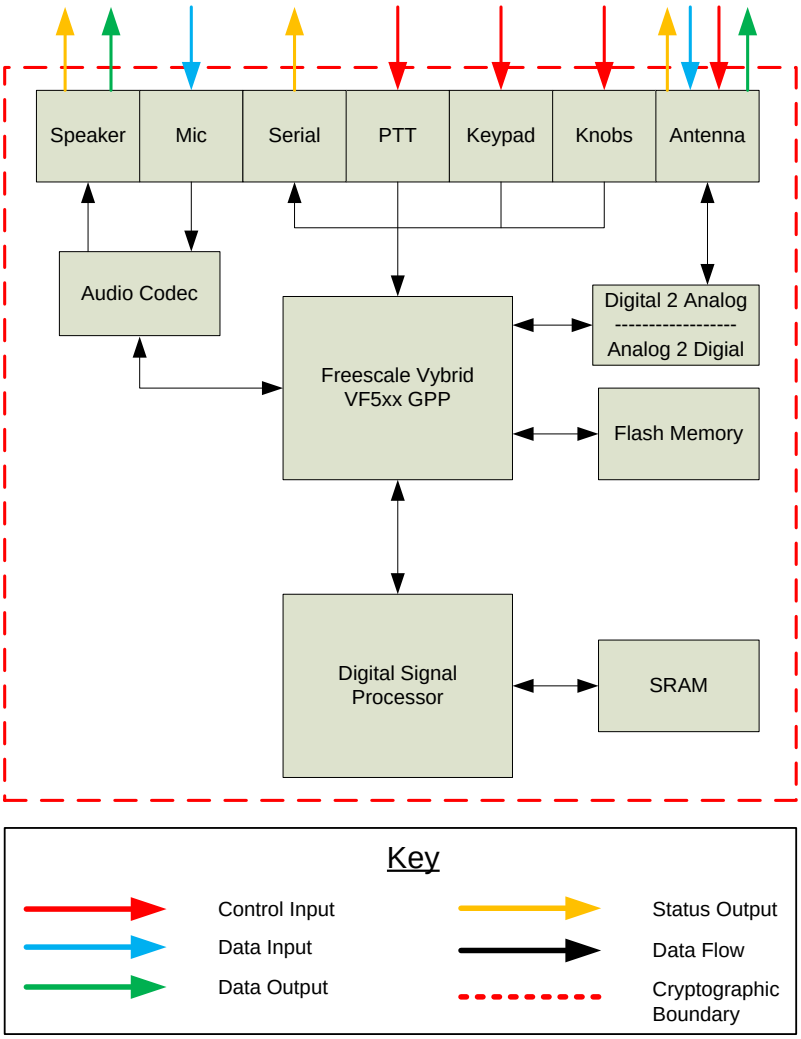

Figure 2 – Physical Cryptographic Boundary

2.3 Module Interfaces

The HALM implements a single module interface in its firmware design. This interface is the module's logical interface and is provided by a single Application Programming Interface (API). The API is accessed by an application running on the DSP. Physically, the module ports and interfaces are considered to be those of the Harris terminals on which the firmware executes. Both the API and the physical ports and 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

Table 2 maps the FIPS 140-2 Logical Interfaces to the physical interfaces of the terminal and the logical interface of the module.

Table 2 – FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Terminal Physical Port/Interface	Harris AES Load Module Interface
Data Input Interface	• Antenna • Microphone	Arguments for an API to be used or processed by the module
Data Output Interface	• Antenna • Speaker	Arguments for an API call that specify where the result of the API call is stored
Control Input Interface	• Antenna • Keypad • Knobs: Voice Group Selection Knob, Power On-Off/Volume Knob • PTT[6] Button	API call and accompanying arguments used to control the operation of the module
Status Output Interface	• Antenna Port • Serial Port (DB9) • Speaker	Return values for API calls

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 (CO) role and a User role. The operator implicitly assumes one of these roles when selecting each command documented in this section.

2.4.1 Crypto-Officer Role

The 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 Table 3 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 3 – Crypto-Officer Role's Services

Service	Description	CSP and Type of Access
HALM_INITIALIZE	Performs self-tests on demand	None
HALM_SEND_STATUS	The status of the last function called from the HALM_API is returned	None

Service	Description	CSP and Type of Access
HALM_WRAP_KEY	Wraps a key	AES Key Wrap Key – X AES Unwrapped Key – R
HALM_UNWRAP_KEY	Unwraps a key	AES Key Wrap Key – X AES Wrapped Key – R
ZEROIZE	Zeroizes keys in volatile memory via power cycle	AES-256 Cipher Key – W AES-128 Cipher Key – W AES CMAC Key – W AES Key Wrap Key – W

2.4.2 User Role

The User role has the ability to perform the module's cipher operation, and data encryption/decryption services. Descriptions of the services available to the role are provided in Table 4 below. Type of access is defined in section 2.4.1 of this document.

Table 4 – User Role's Services

Service	Description	CSP and Type of Access
HALM_GEN_KEYSTREAM	Generates key stream data	AES-256 Cipher Key – X
HALM_GEN_PRIVATE_MI	Generates a Message Indicator (MI) from the Initialization Vector (IV) value specified in the data input buffer	AES-256 Cipher Key – X
HALM_P25_XOR	Performs logical Exclusive OR (XOR) operation	None
HALM_LOAD_KEY	Load key into the module	AES-256 Cipher Key – R AES-128 Cipher Key – R
HALM_AES_OFB	AES OFB[7] Encryption operation	AES-256 Cipher Key – X
HALM_AES_OFB_PASSTHRU	AES OFB Encrypt/Decrypt	AES-256 Cipher Key – X
HALM_AES_ECB	AES ECB Encryption operation	AES-256 Cipher Key – X AES-128 Cipher Key – X
HALM_AES_ECB_DECRYPT	AES ECB Decryption operation	AES-256 Cipher Key – X AES-128 Cipher Key – X
HALM_AES_CBC	AES CBC Encryption operation	AES-256 Cipher Key – X
HALM_MAC_GENERATION	Generates a Message Authentication Code (MAC)	AES CMAC Key – X

[7] OFB – Output Feedback

Service	Description	CSP and Type of Access
HALM_AES_CMAC	AES CMAC operation	AES CMAC Key – X

2.5 Physical Security

The firmware module relies on the physical embodiment of the radios, which store the module within their enclosure. The radios meet Level 1 physical security requirements, and are made of production grade material, opaque within the visible spectrum.

2.6 Operational Environment

Per Implementation Guidance Section G.3, the operational environment requirements do not apply to the Harris AES Load Module. The cryptographic boundary of the module includes the entire Harris AES Load Module image (HALM.bin). The firmware image runs on a non-modifiable operational environment, the Harris BIOS Kernel v1. The kernel does not allow the loading of any new applications. Hence, the operational environment of the module is a non-modifiable operational environment.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 5.

Table 5 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES 128- and 256-bit encrypt/decrypt in ECB[8] mode	#3338
AES 256-bit encrypt in CBC[9] mode	#3338
AES 256-bit encrypt/decrypt in OFB mode	#3338
AES 256-bit CMAC generation/verification	#3338
AES 256-bit Key Wrap	#3338

[8] ECB – Electronic Code Book
[9] CBC – Cipher Block Chaining

The Harris AES Load Module is not responsible for the permanent storage of any cryptographic keys. Keys that enter the module are stored temporarily in volatile memory. Zeroization of keying material in volatile memory occurs at shutdown or reboot of the radio hosting the module. Keys are either passed into the module in plaintext or wrapped with an AES key. The AES-128 and AES-256 Cipher Keys, the AES CMAC Key, and the AES Key Wrap Key are passed into the module in plaintext are used for encryption, decryption, CMAC, wrapping, and unwrapping services. These keys are generated externally and are stored in a key store external to the module (See Figure 1). The AES Wrapped Key is passed into the module encrypted, or wrapped by an AES key wrap key. The key is unwrapped by the AES Key Wrap Key and then sent to the logical Data Output Interface in plaintext. This newly unwrapped key will be a new AES-128 or AES-256 Cipher Key. The AES Unwrapped Key is passed into the module in plaintext in order to be wrapped by the AES Key Wrap Key. The newly wrapped key then exits the module encrypted in order to be transmitted by the radio.

The module supports the critical security parameters listed in Table 6:

Table 6 – List of Cryptographic Keys and CSPs

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
AES-256 Cipher Key	256-bit AES Key	Generated externally; Input Electronically in Plaintext via GPC[10] INT[11] Path	Never exits the module	The key resides in plaintext in volatile memory while in use by the module; The key is not actively stored by the module	Power cycle zeroizes volatile memory	Used as input into the ECB, CBC, and OFB cipher operations
AES-128 Cipher Key	128-bit AES Key	Generated externally; Input Electronically in Plaintext via GPC INT Path	Never exits the module	The key resides in plaintext in volatile memory while in use by the module; The key is not actively stored by the module	Power cycle zeroizes volatile memory	Used as input into the ECB cipher operation

[10] GPC – General Purpose Computer
[11] INT - Internal

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
AES CMAC Key	256-bit AES Key	Generated externally; Input Electronically in Plaintext via GPC INT Path	Never exits the module	The key resides in plaintext in volatile memory while in use by the module; The key is not actively stored by the module	Power cycle zeroizes volatile memory	Used as input into the CMAC operation
AES Key Wrap Key	256-bit AES Key	Generated externally; Input Electronically in Plaintext via GPC INT Path	Never exits the module	The key resides in plaintext in volatile memory while in use by the module; The key is not actively stored by the module	Power cycle zeroizes volatile memory	Used as input into the key wrapping and unwrapping operations
AES Wrapped Key	128- or 256-bit AES Key	Generated externally; Input Electronically Encrypted	Exits the module in plaintext via GPC INT Path	The key is not stored by the module	Not applicable	The key is passed in to the module to be unwrapped by the module and passed back to the terminal
AES Unwrapped Key	128- or 256-bit AES Key	Generated externally; Input Electronically in Plaintext via GPC INT Path	Exits the module encrypted	The key is not stored by the module	Not applicable	The key is passed in to the module to be wrapped by the module and passed back to the terminal

2.8 Self-Tests

Self-tests are performed by the module at power-up after the module is loaded into SRAM memory. The module checks its integrity using a CMAC and ensures the correct performance of the AES cryptographic algorithm by performing a Known Answer Test. The Harris AES Load Module performs the self-tests listed in Table 7 at power-up.

Table 7 – List of Power-Up Self-Tests

Start-Up Test	Description
AES Known Answer Test (KAT)	The AES KAT takes a known key and encrypts a known plaintext value. The encrypted value is compared to the expected ciphertext value. If the values differ, the test is failed. 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 is failed. If they are the same, the test is passed.
Firmware Integrity Test	The module checks the integrity of the binary (using a CMAC checksum value) at the start-up. If the MAC verifies correctly (i.e., the newly-computed MAC is the same as the stored MAC value), the test passes. Otherwise, it fails.

The module is not required to perform any conditional self-tests.

The module enters an error state if it fails either power-up self-test listed above. To attempt to clear the error state, an operator may restart the terminal (thereby restarting the module and re-running the power-up self-tests). If the self-tests fail upon restart, the operator must return the terminal containing the module to Harris for repair or reinstallation.

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 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 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. In order to operate the module, the CO shall turn on the Harris terminal.

3.1.1 Initialization

The Harris AES Load Module is initialized by the DSP when the host terminal is powered on. The DSP uses the HALM's initialization routines to load the HALM into memory, allocate memory for operation, and start the module's power-up self-test. Until the module's power-up self-tests have been performed, the module is not operational. The services listed in Section 2.4 (Roles and Services) of this document are not available until the module performs and passes its power-up self-test. Operator intervention is not required in order to initialize the module.

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. The operator can determine that the module is operating in the FIPS-Approved mode of operation when the module returns the *HALM_INITIALIZE_OK* status. This status is passed to the operator after the module passes all of its power-up self-tests. The operator can also determine the status of the module by performing the "HALM_SEND_STATUS" service.

3.1.3 Zeroization

The module does not store any keys or CSPs within its logical boundary. All ephemeral keys that are used by the module are zeroized upon shutdown or reboot of the host terminal.

3.2 User Guidance

Users can only access the module's cryptographic functionalities that are available to them. The User should report to the Crypto-Officer if any irregular activity is noticed.

4 Acronyms

This section defines the acronyms used in this document.

Table 8 – Acronyms

Acronym	Definition
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
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DSP	Digital Signal Processor
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GPP	General Purpose Processor
HALM	Harris AES Load Module
INT	Internal
IP	Internet Protocol
IV	Initialization Vector
KAT	Known Answer Test
MAC	Message Authentication Code
MI	Message Indicator
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OS	Operating System
PTT	Push-to-talk
SRAM	Static Random Access Memory
XOR	Exclusive OR

Prepared by:
Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

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