# Harris Unified Audio Card

## FIPS 140-2 Non-Proprietary Security Policy

### Level 1 Validation

Document Version 1.2

July 18, 2018

# Table of Contents



## Glossary

| Term/Acronym | Description |
|---|---|
| AES | Advanced Encryption Standard |
| DES | Data Encryption Standard |
| GWB | GateWay Base |
| HMAC | Hash-based Messaged Authentication Code |
| KEK | Key Encryption Key |
| KMU | Key Manager Interface |
| MAC | Message Authentication Code |
| OTAR | Over-the-air-rekeying |
| RNG | Random Number Generator |
| SHS | Secure Hash Standard |

| Term/Acronym | Description |
|---|---|
| TEK | Traffic Encryption Key |
| UAC | Unified Audio Card |
| UAS | Unified Administration System |
| UKEK | Unique Key Encryption Key |
| VIDA | Voice Interoperability Data Access |

# 1. Introduction

The Harris Unified Audio Card (UAC) is a multi-channel analog audio gateway used to interface analog radio communication equipment such as conventional base stations to radio systems and other devices on a Voice Interoperability Data Access (VIDA) network.

Uses of this module include interfacing radio systems and other devices on an IP-based VIDA network with any other communication equipment that is able to be interfaced to a full duplex 4-wire analog interface. The modules and UAC channels are capable of handling calls from the VIDA network and co-located external equipment. As well, the module can provide 256 bit AES encryption for voice calls passing through it.

# 2. Overview

The Harris UAC is classified as a multi chip embedded module, being a single card housing several processor chips. The UAC card is comprised of a processor and several DSP units. The card contains several ports, including 4-wire balanced-line audio interfaces, Ethernet port, and USB port. The UAC's cryptographic boundary is comprised of the physical perimeter of the card. No items are excluded from this boundary. This module was validated at level 1.

Below is an image of the UAC

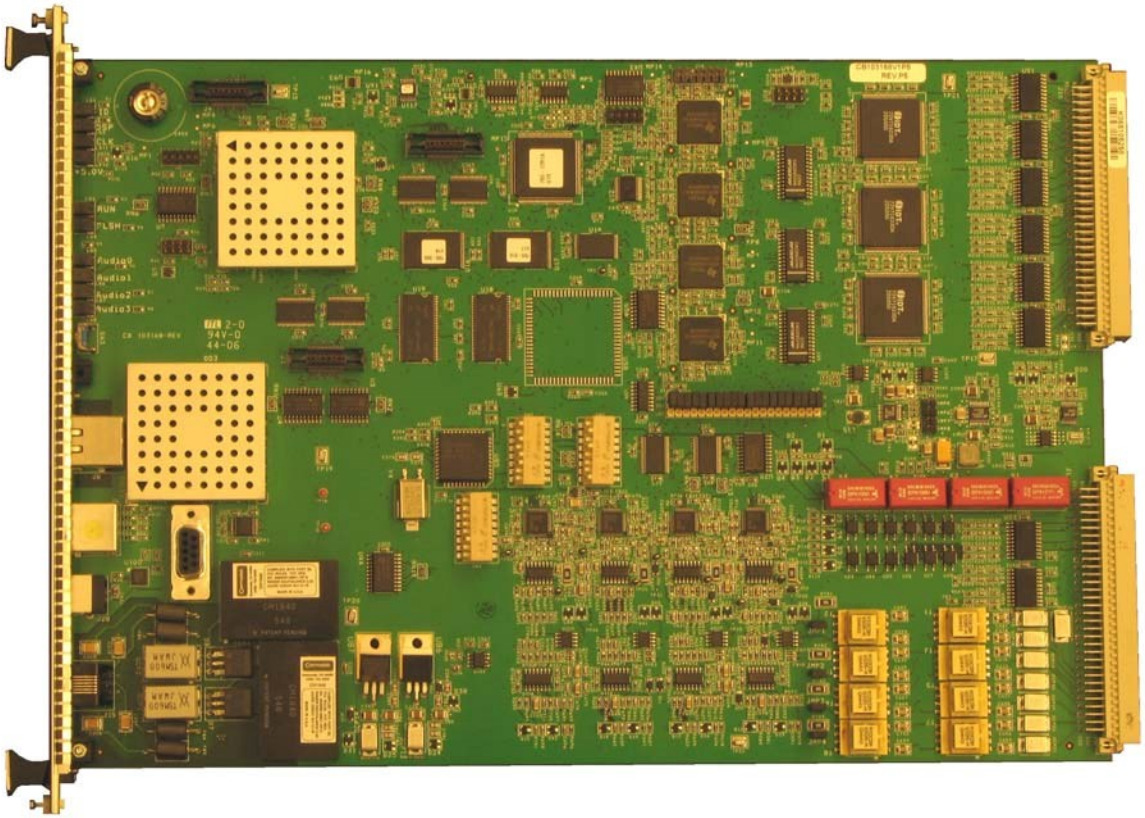

**Figure 1 UAC Image**

- Hardware Versions
  - EA-103168-002 Rev. –
  - EA-103168-002 Rev. A
  - EA-103168-002 Rev. B

- EA-103168-002 Rev. C

or

- EA-103168-002 Rev. D

- Firmware versions
  - MPC-860: SK-007765-007 v R03A08
    and
  - DSP: SK-007765-013 v R03A05

or

  - MPC-860: SK-007765-007 v R04G01
    and
  - DSP: SK-007765-013 v R04E03

## 2.1 Ports and Interfaces

The UAC provides several physical ports that are provided for interfacing with the module. These physical interfaces can each be mapped to at least one of the logical interfaces (data output, status output, data input and control input). Additionally, the module includes physical ports for providing power to the module.

The following table provides a listing of the modules physical ports and the mapping of those ports to the logical interfaces:

**Table 1 Ports and Interfaces**

| Physical Ports | Logical Interfaces |
|---|---|
| Independent Ports | |
| Ethernet Port | Data input, Data output, Control Input, Status Output |
| USB Port | Data input, Data output, Control Input, Status Output |
| RS-232 | Data input, Data output, Control Input, Status Output |
| LEDS | Status Output |
| DIP Switches and Jumpers | Control Input |
| JTAG | Data input, Data output, Control Input, Status Output |
| Legacy Key Loader | N/A; not active |
| RJ-11 | N/A; hardware removed |
| 96 Pin DIN Connectors | |
| 4-wire Balanced line audio interfaces | Data input and output |
| Auxiliary Input | Data input, Status input |
| Auxiliary Output | Data output, Control output |
| Pins C1, C31 on J10 and pins A1 and A31 in Jll | Power Interface |

## 2.2 Modes of Operation

The UAC has two modes of operation: FIPS Approved mode and non-FIPS Approved mode. Section 4 describes services and cryptographic algorithms available in FIPS-Approved mode. In non-FIPS Approved mode, the module

runs without these FIPS policy rules applied. Section 6.2 FIPS Approved Mode describes how to invoke FIPS Approved mode.

The module supports alternating bypass. This mode is always active within the module once the checks have passed during set up, so no status indicator is provided.

To transition into bypass, first the module will ensure the packets containing talk group data has a valid message ID and data length. Next, keys passed from the KMF to the talk groups are checked using a checksum to ensure they are correct. If both of these checks are successful, the module will operate in bypass mode.

## 2.3 Module Validation Level

The module meets an overall FIPS 140-2 compliance of security level 1.

**Table 2 UAC Security Levels**

| Security Requirements Section | Level |
|---|---|
| Cryptographic Module Specification | 1 |
| Cryptographic Module Ports and Interfaces | 1 |
| Roles, Services, and Authentication | 1 |
| Finite State Model | 1 |
| Physical Security | 1 |
| Cryptographic Key Management | 1 |
| Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) | 1 |
| Self-Tests | 1 |
| Design Assurance | 1 |
| Mitigation of Other Attacks | 1 |
| Operational Environment | N/A |

# 3. Roles

In FIPS Approved mode, the UAC supports 4 roles: Crypto Officer, User, JTAG Access, and Unauthorized. These roles are implicitly assumed by the actions taken by the operator.

1. Crypto Officer Role: The crypto officer role is accessed for this device when the operator is connected to the module via the command line interface, or the Key Manager and KMF. This role has full access to all commands available to the module, with the exception of key commands over Telnet. Hence, the Crypto Officer role has complete access to the system.
2. User Role: The user role of this module allows the operator access to all normal functionality of the module during access of the VNIC interface and other devices, as well as the booting stage and flash load mode of the module.
3. JTAG Access: This role is assumed when the operated accesses the JTAG ports to perform debugging using Logic Analyzers, JTAG/IEEE 1149.1 boundary-scan equipment, and in-circuit emulation pods. Per FIPS 140-1 IG 3.6, the operator MUST zeroize the module before and after each access of these ports.
4. Unauthorized: This role is assumes when an operator observes the module externally. The only action available to unauthorized operators is observation of the LEDs on the face of the module.

While up to 2 operators may access the crypto officer role over the command line interface (one via Telnet, and one over USB/Serial), only one operator may access the module using the Key Manager and KMF at any time.

# 4. Services

The services available to an operator depend on the operator's role. Unauthorized operators may view externally visible status LED when in proximity of the module but not interfacing with the module using radios or the command line interface or KMF. For all other services, an operator must access the device as described in section 5.2 Authentication.

The following subsections describe services available to operators based on role. Table 3 summarizes the available FIPS-Approved cryptographic functions. Table 4 lists all Non-Approved algorithms within the module. These are broken down into the images that run on the particular processors.

**Table 3 FIPS Approved Cryptographic Functions**

| Label | Algorithm Certificate |
|---|---|
| **DSP Firmware** | |
| AES | #1653 - (**CBC** ( e/d; 128 , 256 ); **OFB** ( e/d; 256 ) |
| **MPC860 Firmware** | |
| AES | #1652 - **ECB** ( e/d; 256 ); **CBC** ( e/d; 256 ); **OFB** ( e/d; 256 ) |
| SHS | #1450 – (**SHA-1** (BYTE-only); **SHA-256** (BYTE-only)) |
| HMAC[1] | #970 – (**HMAC-SHA1 (Key Sizes Ranges Tested:** KS<BS ); **HMAC-SHA256 ( Key Size Ranges Tested:** KS<BS ) |

**Table 4 FIPS Non-Approved Cryptographic Functions**

| Algorithm Type | Notes |
|---|---|
| **DSP Firmware** | |
| RNG | Used for generation of IVs |
| **MPC860 Firmware** | |
| AES MAC[2] | AES Cert. #1653 |
| DES | Not used by the module |
| DES MAC | Not used by the module |
| RNG | Used for generation of IVs |

Because FIPS 140-2 restricts the usage of non-FIPS approved algorithms while operating in a FIPS compliant manner, the operator should follow the rules in section 6.2 to initialize the UAC to ensure FIPS compliance.

## 4.1 User Role Services

**Table 5 User Role Services**

| Service | Description |
|---|---|
| System Booting | This service consists of powering on and off the module and all actions contained within such as firmware loading. |

[1] Only HMAC-SHA1 with a key size of 256 bits is used by this module. Key sizes less than 112 are not used by this module.

[2] Allowed in FIPS mode as part of P25 over-the-air-rekeying (OTAR).

| | |
|---|---|
| Flash Load | This service consists of actions taken by the operator during the flash load state where firmware images are loaded into the module. |
| Normal Operation | This service consists of accessing the module via a VNIC or conventional radio device during the module's operation. |

## 4.2 Crypto Officer Role Services

**Table 6 Crypto Officer Services**

| Service | Description |
|---|---|
| Monitoring Module | This service includes all commands used to enable, disable and view monitoring data. |
| Configuring Module | This service includes all commands used to set or configure settings of the module This include configuration to set up alternating bypass. |
| Key Management | This service includes all commands relating to keys, including setting, receiving, writing and clearing. This also includes the Key Manager and KMF interface. When connected via Telnet, key entry will not be allowed by the module. |
| Memory Commands | This service is comprised of the commands relating to the flash memory of the console including reading from and writing to RAM. Commands related to reading and writing to specific memory addresses will not work on memory addresses containing key data. |
| Diagnostic Tests | This service is comprised of the features available in the factory test state, including testing FLASH memory or reading current DIP switch settings. |
| Miscellaneous | These include other commands such as exit to end a command line session, help, history, and other unrelated commands. |

## 4.3 JTAG Access Role Services

While JTAG is offered as a maintenance role, there is not a defined set of services for it as it allows full access to the module and its data to perform debugging using Logic Analyzers, JTAG/IEEE 1149.1 boundary-scan equipment, and in-circuit emulation pods. Per FIPS 140-1 IG 3.6, the operator MUST zeroize the module before and after each access of these ports by using the 'clear keys' command.

## 4.4 Unauthorized Services

**Table 7 - Unauthorized Services**

| Service | Description |
|---|---|
| View status LEDs | This service involved physically observing the status LEDs on the side of the module. |

# 5. Policies

## 5.1 Security Rules

While in FIPS mode, the following restrictions are enforced by the module:

- Only the approved firmware versions listed above are able to be loaded into the module. FIPS signatures will be checked during code downloads, and if they do not match, the code will not be allowed to load into the module and the operator will be notified.
- Show Status will include FIPS relevant information
- A new LED pattern will be displayed to indicated FIPS error conditions
- Code in FLASH will be validated on a reset to ensure it contains appropriate signatures

Additionally, the operator must follow the below rule when operating the module in FIPS mode:

- If the JTAG ports are to be used, the operator must zeroize the module before and after each access of these ports.

## 5.2 Authentication

No authentication is provided by this module. Roles are assumed implicitly by access to the module and actions performed. The user role is accessed by accessing the module using radios, and the crypto officer by accessing the command line interface or KMF.

## 5.3 Access Control and SRDIs

While operating in FIPS mode, the UAC contains the following security relevant data items:

Note: Entering Keys and SRDIs through the command line interface using the commands shown below can only be done through the local USB/Serial port because the key material is transmitted in the clear. Connections using the telnet interface are blocked from using commands that affect the Keys and SRDIs. A full list of the commands available through the command line interface can be found in the UAC Software Release Notes (MS-010749-001).

**Table 8 Keys and SRDIs**

| ID | Algorithm | Size | Description | Origin | Storage | Zeroization Method |
|---|---|---|---|---|---|---|
| General Keys/CSPs | | | | | | |
| Firmware Load Key | HMAC key | 32 bytes | Used in a HMACSHA256 to check the downloaded firmware | Hardcoded in the firmware images listed in table GWB with AES encryption | Flash memory | N/A |

| P25 Keys | | | | | | |
|---|---|---|---|---|---|---|
| UKEK | Encryption key | 256-bit AES keys | Used in support of p25 OTAR transfers for AES keys. Is unique to the radio. | Entered by the crypto officer using the “Set UKEK” command from the command line interface. | Flash memory, RAM during operation | “Clear keys” command, entering maintenance mode, disabling permanent key storage and rebooting the board, or via P25 OTAR messages |
| KEK | Encryption key | 256-bit AES keys | Used to encrypt and decrypt TEKs. | Received over the air for a radio or via IP network for UAC, or using “Set Key” from the command line interface. | Flash memory, RAM during operation | “Clear keys” command, entering maintenance mode, disabling permanent key storage and rebooting the board, or via P25 OTAR messages |
| TEK | Encryption key | 256-bit AES keys | Used to encrypt and decrypt voice and data traffic. | Received over the air for a radio or via IP network for UAC or using “Set Key” from the command line interface. | Flash memory, RAM during operation | “Clear keys” command, entering maintenance mode, disabling permanent key storage and rebooting the board, or via P25 OTAR messages |

Table 8 summarizes the access operators in each role have to security relevant data items. The table entries have the following meanings:

- r – operator can read the value of the item,
- w – operator can write a new value for the item,
- x – operator can use the value of the item (for example encrypt with an encryption key), and
- d – operators can delete the value of the item (zeroize).

**Table 9 Access Control Policy**

| | Keys and CSPs | Firmware Load Key | UKEK | TEKs | KEKs |
|---|---|---|---|---|---|
| Role/Service | | | | | |
| User role | | | | | |
| System Booting | | x | | | |
| Flash Load | | x | | | |
| Normal Operation | | | | | |
| Crypto-officer Role | | | | | |
| Monitoring Module | | | | | |
| Configuring Module | | | | | |
| Key Management | | | r.w,d | r,w,d | r,w,d |
| Memory Command | | | | | |
| Miscellaneous | | | | | |

### 5.4 Physical Security

This module does not provide any physical security mechanisms.

# 6. Crypto Officer Guidance

## 6.1 Show Status

The 'show status' command will display prevalent information to the user, including the status of all self tests. Below is an example of the output.

```
Encryption Status:
   MPC860 encryption supported     : yes
   MPC860 FIPS mode                : off
   DSP 1 encryption supported      : yes
   DSP 2 encryption supported      : yes
   DSP 3 encryption supported      : yes
   DSP 4 encryption supported      : yes
   MPC860 encryption power-up test : pass
   MPC860 encryption state         : normal
```

```
DSP 1 encryption start-up test  : pass
DSP 2 encryption start-up test  : pass
DSP 3 encryption start-up test  : pass
DSP 4 encryption start-up test  : pass
MPC860 CRNG test                : pass
DSP 1 CRNG test                 : pass
DSP 2 CRNG test                 : pass
DSP 3 CRNG test                 : pass
DSP 4 CRNG test                 : pass
DSP 1 Bypass test               : pass
DSP 2 Bypass test               : pass
DSP 3 Bypass test               : pass
DSP 4 Bypass test               : pass
```

## 6.2 FIPS Approved Mode

The operator should follow the following rules to initialize the UAC to ensure FIPS compliance.

The approved version of the module's firmware is the following

**GWB with AES Encryption**

| Media Kit Number | Description | Version |
|---|---|---|
| SK-007765-020 | Boot/Loader and Factory Test AES | R03A02 |
| SK-007765-007 | MPC860 GWB w/ Encryption | R03A08 or R04G01 |
| SK-007765-013 | DSP Application - GWB w/ Encryption | R03A05 or R04E03 |
| SK-007765-001 | Low-Level Boot | R01D01 |
| SK-007765-003 | DSP Factory Test | R01D02 |

Note: When using MPC860 media kit SK-007765-007 v R03A08 you must use DSP media kit SK-007765-013 v R03A05 and when using MPC860 media kit SK-007765-007 v R04G01 you must use DSP mediak kit SK-007765-013 v R04E03.

Once installed, the operator must set the DIP switches to the following configuration to initialize the module in FIPS mode.

| Switch Bank | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | x | x | x | x |
| 4 | 0 | x | x | x | x | x | x | x |

While in FIPS mode, the following restrictions are enforced by the module:

- Only approved versions of the firmware listed above are able to be loaded into the module. FIPS signatures will be checked during code downloads, and if they do not match, the code will not be allowed to load into the module.
- Show Status will include FIPS relevant information
- A new LED pattern will be displayed to indicated FIPS error conditions
- Code in FLASH will be validated on a reset to ensure it contains appropriate signatures

Operators must also be mindful of the following while operating in FIPS mode:

- If the JTAG ports are used for any reason, the operator must zeroize the keys both before and after accessing these ports.

In FIPS Approved mode, The UAC provides FIPS-Approved cryptographic algorithms as described in the FIPS Approved Algorithm table in section 4.

# 7. Self Tests

## 7.1 Power Up Self Tests

This module contains the following Power Up Self Tests

**DSP Firmware**

- AES encrypt/decrypt KAT
- Software Integrity Test

**MPC860 Firmware**

- AES encrypt/decrypt KAT
- SHS KAT
- Non-Approved RNG KAT
- HMAC KAT
- Software Integrity Test

Additionally, there are self tests for the non-approved AES-MAC, DES and DES MAC algorithms.

## 7.2 Conditional Self tests

The module contains the following conational self tests

**DSP Firmware**

- Bypass Test
- Continuous Random Number Generation Test for non-approved RNG

**MPC860 Firmware**

- Continuous Random Number Generation Test for non-approved RNG
- Firmware Load Test

# 8. References

| Title | Document Number |
|---|---|
| Engineering Release Notes | |
| FIPS Vendor Evidence Responses | |
| FIPS Block Diagrams | |
| Installation and Configuration Manual | MM-009620-001 |
| Maintenance Manual | MM-009621-001 |
| UAC Maintenance Manual | MM-20123 |
| UAC Software Release Notes | MS-010749-001 |