Hewlett-Packard – Atalla Security Products

Atalla Cryptographic Subsystem (ACS) Security Policy

Version 1.0
28 October 2010

Table of Contents

0. Revision History

0.10	TAH	Created
0.20	IF	Incorporated comments
0.21	TAH	Resolved several of the TBDs
0.22	TAH	Corrected power consumption values
0.23	IF	Added cert #s and photos
0.24	IF	Incorporated comments
0.9	IF	Added Mitigation of Other Attacks Policy
1.0	IF	Expanded Rule 4

1. Introduction

The HP Atalla Cryptographic Subsystem, hereafter referred to as ACS (HW P/N 610113-001 Rev A and 610113-001 Rev B, Loader Firmware Version 0.64, and PSMCU Firmware Version 0.96) is a secure cryptographic co-processor designed for use in a variety of high security applications. This document specifies the ACS security rules, including the services offered by the cryptographic module, the roles supported, and all keys and CSPs employed by the module.

The ACS module is designed to comply with FIPS 140-2 Level 3 Security requirements.

1.1. Related Documents

[1] "Security Requirements for Cryptographic Modules," FIPS PUB 140-2, Information Technology Laboratory, National Institute of Standards and Technology. May 25, 2001.
[2] FIPS 140-2 standard, the *Derived Test Requirements*, and on-line implementation guidelines
[3] "Secure Hash Standard," FIPS Pub 180-2, 8/1/2002. http://csrc.ncsl.nist.gov/publications/fips/fips180-2/fips180-2.pdf
[4] "Advanced Encryption Standard (AES)", FIPS PUB 197, Nov 26 2001. http://csrc.nist.gov/publications/fips/fips197/fips197.pdf
[5] "Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)," ANS X9.31-1998, September 9, 1998 (see section A.2.4.).
[6] "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality," Morris Dworkin, NIST Special Publication 800-38C, May 2004.
[7] "GZIP File Format Specification," RFC1952, version 4.3, May 1996. http://www.faqs.org/rfcs

1.2. Glossary

This section contains terms used within this document.

ACS	Atalla Cryptographic Subsystem
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CPU	Central Processing Unit

CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DMA	Direct Memory Access
DRAM	Dynamic Random Access Memory
ECB	Electronic Code Book
Flash	Programmable read-only (nonvolatile) memory
HW	Hardware
IV	Initialization Vector
MD	Message Digest
MPU	Micro processing unit
NVRAM	Nonvolatile RAM: General purpose memory maintained as nonvolatile
Personality	Secure software application running inside the secure boundary
PSMCU	Physical Security Monitoring Central Unit
RAM	Random Access Memory: General purpose volatile memory
RNG	Random Number Generator
RSA	Rivest Shamir Adelman algorithm
SHA	Secure Hash Algorithm
TDES	Triple Data Encryption Standard

2. General Description

2.1. Product Overview

The HP ACS is a multi-chip embedded cryptographic module. It consists of a secure hardware platform, a firmware secure loader, and PSMCU firmware. The purpose of the cryptographic module is to load Approved (RSA-signed) application programs, called "personalities," in a secure manner. The PSMCU firmware continually monitors the physical security of the cryptographic module. The module is in a FIPS Approved mode of operation until a personality is loaded and started, at which point the module is no longer a FIPS validated module. Verification that the module is in FIPS Approved mode can be observed by running either the "getstatus" or "version" commands (see sections 5.1 and 5.2, respectively).

This security policy addresses only the hardware and the firmware secure loader; the personality is not included in the current FIPS validation. This approach creates a common secure platform with the ability to load trusted code (the personality). Once control passes from the loader to a personality, the module is no longer a FIPS validated module. Note that no personality, no matter what its FIPS 140-2 validation level, will have access to the module's secret keys and CSPs.

The cryptographic boundary of the ACS for the FIPS 140-2 Level 3 validation is the outer perimeter of the secure metal enclosure that encompasses all critical security components.

The hardware features of the ACS include:

- Tamper detection and response hardware

- AES hardware – Latent functionality unused and in default disabled state.
- TDES hardware – Latent functionality unused and in default disabled state.
- SHA-1 hardware – Latent functionality unused and in default disabled state.
- MD5 hardware – Latent Non-FIPS functionality unused and in default disabled state.
- Hardware-based random number generator – Latent functionality and is non-FIPS Approved
- Modular exponentiation hardware – Latent functionality and is non-FIPS Approved

Note: No components of the hardware cryptographic engine are used by the loader. All cryptographic support used by the module is provided by software. The only hardware used by the module is for Tamper Detection and Response hardware. The cryptographic hardware engine is reserved for use by personality applications, which are beyond the scope of this validation.

2.1.1. Physical Security

Depending on states of Physical Security and Security Control Unit, two major events are generated within the secured area:

1. A "reset event" is one that forces the platform to become temporarily inoperable. This is a non-catastrophic event. When the conditions that cause the "reset event" are removed the unit will operate.
2. A "tamper event" is one that forces the platform to become permanently disabled. This is a catastrophic event. In the disabled state all critical security parameters are erased and the platform can only provide status information to users.

Any physical penetration results in a “tamper event”. This event causes active zeroization of all cleartext CSPs.

Two (2) tamper labels, applied to the edges of the module’s covers during manufacturing, provide physical tamper evidence. The tamper labels are located near the fan and wrap around the front and back. The tamper labels should be inspected periodically to verify that fresh labels have not been applied to a tampered module.

2.1.2. Platform Memory

There are four types of memory within the ACS:

1. Dynamic Random Access Memory (DRAM). DRAM is used to hold the Loader and its data during operation.
2. Flash Memory. Non-volatile flash memory is used to hold the Loader. No sensitive CSPs are stored in flash as cleartext.
3. Security Control Unit. The security control unit has non-volatile memory for storing cleartext CSPs. This memory is the first target of zeroization if a “tamper event” occurs.
4. Non-volatile RAM. This battery-backed-up static RAM is not used by the Loader.

2.2. Ports and Interfaces

2.2.1. External Ports

There are five data paths into and out of the ACS.

- LED (Qty. 2) (Status Output) – used to provide continuous status of the module. The LEDs are not physically mounted on the printed circuit board. Instead, a connector is provided in order to route the electrical signals for the LEDs to the front panel of the chassis enclosure which ultimately houses the ACS. The LED signal voltage swings through 3.3V DC, active low, and the LED current is limited to 5 mA.
- RJ45 Ethernet (Qty. 2), compatible with 10/100/1000 Base T IEEE 802.3. – used as the primary communication I/O channel. Only UDP protocol is supported.
- USB 1.1/2.0 (Qty. 2) interface with a nonstandard connector – latent interface not initialized and left in its default disabled state. No software support of any kind is provided for this interface.
- Serial Interface. This port is standard RS-232, it is an alternative communication I/O channel
- IIC Interface. This interface is a dedicated HP interface used solely for inputting the "go" command.
- PCI/PCI-X. This interface is used to provide power to the ACS; it is left in its default disabled state.

The following table shows the relationships among the physical and logical ports:

			Physical Ports					
		RJ45 Ethernet Port 0	RJ45 Ethernet Port 1	LED 0	LED 1	Serial Interface	IIC	PCI-PCI-X
Logical Ports	Data Input	√	√			√		
	Data Output†	√	√			√		
	Control Input	√	√			√	√	
	Status Output	√	√	√	√	√		
	Power							√

†Note: No CSPs of any type are output from the module under any condition. The data which is output is of informational nature, such as version numbers, command return codes and error messages, etc.

2.2.2. Power

Primary main system power is derived from the 3.3V pins on the PCI/PCI-X connector. In addition, the 5V and 12V pins on the PCI/PCI-X connector also supply additional power for the following purposes:

- 5V: Power for the USB connections (which are not energized in this application) and power for the battery circuit when host power is available.
- 12V: Fan power.

The power requirements are:

- 3.3V: 8.2 W
- 5V: 15 mW
- 12V: 1.2 W
- Total Power 9.4 watts

Other voltage requirements on the platform are derived from the main power except for the 3V battery backup power source. This battery source is used to maintain the real time clock and to operate the security control unit. The power requirement from the battery is approximately 2.7 milliwats.

2.3. Supported Algorithms

The Loader includes these FIPS-Approved algorithms, implemented in firmware:

- SHA-256 (Cert. #1194)
- AES (encrypt, decrypt, ECB and CBC modes; 256-bit keys only) (Cert. #1305)
- AES CCM (decrypt; 256-bit keys) (Cert. #1311)
- Deterministic random number generation based on ANSI X9.31 [5]. (Cert. #728) The RNG is seeded in the factory by an approved HW random number generator.
- RSA (signature verification); 1024 and 4096-bit keys (Cert. #625)

2.4. Security Level

Security Requirement	Level
Cryptographic Module Specification	3
Cryptographic Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Machine	3
Physical Security	3
Operating Environment	Not Applicable
Cryptographic Key Management	3
EMI/EMC	3
Self-tests	3
Design Assurance	3
Mitigation of Other Attacks	3

3. Self-Tests

There are a number of integrity tests performed automatically by the module.

Power-Up Self-Tests

1. System Integrity Test: CRC-32 [7] test of Boot and Loader code.
2. Firmware Integrity Test: The integrity of the Loader is verified at startup by checking a 1024-bit RSA signature.
3. The cryptographic functions are all tested at startup using known answer tests
    a. SHA-256
    b. AES-256 (encrypt, decrypt, ECB and CBC modes)
    c. RSA-4096 signature verification
    d. X9.31 RNG known answer test
    e. CCM mode of AES algorithm (decrypt only)

4. Critical Functions Tests:
    a. DRAM test
    b. Key Integrity Check: All keys are stored with integrity check digits, and those check digits are verified whenever the key is retrieved by the loader for use. All clear text key values are destroyed immediately after use.

Conditional Self-Tests

1. Continuous RNG test per ANSI X9.31 [5]. The initial seed is provided in manufacturing.
2. Firmware load test: This is a series of tests used to validate the integrity of the personality when it is loaded into the module. These tests include CCM for secure and authenticated key transport, Signature test (RSA 4096-bit modulus with SHA-256), AES-256 file decryption, and CRC-32.
3. Critical Functions Tests:
    a. Key Integrity Check: All keys are stored with integrity check digits, and those check digits are verified whenever the key is retrieved by the loader for use. All clear text key values are destroyed immediately after use.
    b. “go” command personality start validation: The “go” command is authenticated using a 1024-bit signature. Following this, the personality is validated with CRC-32, then decrypted using AES-256, then validated again using SHA-256 prior to passing control to it.

Failure of any of the above tests results in an error state. Recovery from the error state requires power cycling.

In addition to the automatic integrity tests, the module supports a cryptographic self-tests service. This service allows the user to request any specific test.

4. Rules

Rule 1:
HP Atalla maintains no databases of device secrets and has no “backdoor access” to customer’s secrets.

Rule 2:
All functions requiring the use of sensitive data shall be performed within security area. This rule is enforced by the Platform physical design. All the critical circuits and components are within the secure area, which is continuously monitored to detect tampering.

Rule 3:
All sensitive data shall be zeroized upon tamper detection. Zeroization, when controlled by hardware, is a process that effectively erases the previous content. This rule is enforced by the tamper detect circuits, switches, and the software.

Rule 4:
Personality software and cryptographic keys, when loaded outside of manufacturing site shall be cryptographically protected. The actual key names and their uses are described in section 8 of this document. Personalities are signed by HP. The corresponding signature keys (i.e., the GSK private key and the PSK private key) remain solely under the control of HP and the knowledge of those keys are not distributed or divulged outside the manufacturer's control

Rule 5:
Clear cryptographic keys in the security area shall never be exported. In fact, no cryptographic keys of any kind are ever exported from the unit.

Rule 6:
Before performing any non-status or -self-test service the user must present the correct authorization. Where several stages are required to assemble the authorization, all the steps must be performed on the same connection.

Rule 7:
The ACS does not support maintenance and bypass modes.

Rule 8:
Failure of self-tests result in the module entering an error state.

Rule 9:
Power-up self-tests initiated after power up or power cycle do not require input or operator intervention.

5. Services

The following services provide user authentication and/or cryptographic functionality as well as diagnostics capabilities. The available services depend on defined roles.

5.1. Getstatus

Limited status information shall always be available. This command is used to read and display the status of the Platform, such as tamper information, personality application load status, and mode of operation (Approved versus non-Approved). To fully determine whether the module is operating in a

FIPS-approved mode of operation, the mode of operation status must return Approved and the version information given in the output of the command must correspond to the version specified in this Security Policy. The status output is broken into four parts: basic status, which customers can use for simple problem diagnosis; network status, for diagnosing network issues; extended status, which is used by HP Atalla for problem analysis; and event status, which is a date-and-time stamped record of all events which have taken place with the ACS, also for use by HP Atalla for problem analysis. There is an optional parameter for basic getstatus service to display the other status information. None of the status information can compromise the security of the module in any way.

5.2. Version

The version command is used to retrieve the loader name, product type, software version, and build date and time.

5.3. Help

The help command simply returns a list of the available commands. Help is context sensitive; i.e., it shows only the commands valid at the current time, so the responses are different in normal, error, and tamper states. It does not provide any syntax help.

5.4. Gettime

This command is used to read the contents of the real time clock. The date and time are a 12-character formatted ASCII string with the format: YYMMDDHHMMSS (year-month-day-hour-minute-second).

5.5. Getsn

This command reads the value of the serial number field stored in the EEROM. If the serial number has not been set, an error is returned. The serial number is at most a 15-character ASCII string.

5.6. Setnet

This command is used to set the user-manageable network parameters for the unit. These parameters include the IP address, netmask, and gateway for each Ethernet port. The parameters are stored in the serial EEPROM. Other network parameters are set either automatically as part of the UDP protocol with the host server or by the factory prior to deployment.

5.7. Setport

This command is used to configure the serial port. The port can be configured for all supported data rates and with or without character echo. The valid data rates include 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 bits per second.

5.8. Echo

The echo command is used to test the I/O connection to the Loader.

5.9. Self-Tests

Instructions requesting the Platform to perform self-test operations are available. There are individual instructions for testing specific functions, e.g. AES and SHA-256. These tests are identical to the power-up self-tests.

5.9.1. Test_aes

This command does a test of the AES cryptographic engine using the test vectors contained in [4]

5.9.2. Test_ccm

This command does a test of the CCM mode of operation of the AES algorithm.

5.9.3. Test_rng

This command does a known-answer test of the RNG using a fixed key, beginning context, and result.

5.9.4. Test_sha

This command does a test of the SHA-256 cryptographic engine using the test vectors contained in [3].

5.9.5. Test_signature

This command performs a known-answer test of the signature computation algorithm.

5.10. Personality Load

Personality load instructions, when successful, result in updating the flash memory. This service is authenticated as described in section 6.

5.11. Go (Start Personality)

The start personality service passes control from the loader to the personality. This service must be authenticated by an operator in the User role. Once the personality has been started, the module is no longer a FIPS validated module.

5.12. Zeroize[1]

The zeroize service is not a command. It occurs automatically following any tamper event. A user can choose to invoke this service by the physical removal of the batteries. This results in the battery low event, which zeroizes non-volatile RAM, and forces the unit into the ALARM state. The time required for the PSMCU to perform the zeroization is less than 500 microseconds from the time of detection. The first half of this time, less than 250 microseconds, is used for the primary CSP erasure, while the second half is used for extended CSP erasure.

6. Authentication

The ACS supports identity based authentication of operators. The operator's identity is represented by public key stored on behalf of the respective operator. Signing with the corresponding private key authenticates the operator. Note that the module is only able to store two operator identities – one capable of assuming the Crypto Officer (CO) and the other capable of assuming the User role. (See the next section for a discussion of roles.)

The Crypto Officer role is far more security relevant than the User role, so authentication for a Crypto Officer requires a significantly longer key.

6.1. Crypto Officer

A Crypto Officer is required to be properly authenticated and its authentication mechanism is controlled by the PSK (private key), which is used to sign personality images. A CO uses his knowledge of the PSK (private key) to create signed personality images for download to the unit. A 4096-bit RSA key shall be used for authentication process.

[1] Refer to Rule 3 for detailed information on zeroization

6.2. User Authentication

A User is required to be properly authenticated and his authentication mechanism is controlled by the GSK (private key), which is used to sign the 'go' command. A User uses his knowledge of the GSK (private key) to sign the 'go' command which allows the Loader to exit and start the personality. The User's authentication key is a 1024-bit RSA key.

6.3. Authentication Strength

User authentication is determined by the GSK, a 1024-bit digital signature verification key. This key has an equivalent strength of 80 bits. For this example:

$2^{80} = 1.2\ E24$

This exceeds the 1:1,000,000 ratio requirements for false acceptance of authentication.

The 'go' command authentication takes approximately 1 second to complete, allowing 60 attempts per minute. Therefore, the probability of a false acceptance in one minute is approximately:

$60 / 2^{80} = 60 / 1.2\ E24 = 5.0\ E-21$

This exceeds the FIPS threshold of 1:100,000 per minute for false acceptance of authentication with repeated attempts.

A Crypto Officer authentication is determined by the PSK, a 4096-bit digital signature verification key. This key has an equivalent strength of greater than 128 bits. Since the 80 bits strength described above so exceeds the requirements, the >128 bits value here will also exceed the requirements by at least a factor of 2^{48}.

7. Roles

7.1. Crypto Officer Role

A Crypto Officer is responsible for the overall security of the Platform. In particular, only an operator in the Crypto Officer role can load a personality into the ACS.

7.2. User Role

A User can perform a limited number of the services available on the Platform.

7.3. Roles vs. Services Matrix

Acronyms: A – available, √ – unauthenticated command.

Commands / Services	Roles		
	CO	User	None
Status			
GetStatus			√
Version			√
Help			√
Gettime			√
Getsn			√
Setnet			√
Setport			√
Echo			√
Self-test			
Test_signature			√
Test_sha			√
Test_aes			√
Test_rng			√
Test_ccm			√
Personality Load	A		
Go (Start Personality)		A	
Zeroize			√

8. CSPs

8.1. Platform Keys

Key Name	Key Type	Description
IMFK	AES, 256-bit	IMFK – Internal Master File Key. This key is used for encrypting and decrypting all the other CSPs. This key is created on a first boot and is destroyed actively by tamper event or passively by battery failure.
PDEK	AES, 256-bit	PDEK – Prepare Download Encryption Key. This key performs encryption and decryption of the CCM envelope. This key is loaded as part of manufacturing initialization. It is destroyed indirectly when the IMFK is destroyed
IDFK, IDFK_IV	AES, 256-bit	IDFK – Image Download File Key (and IV). This key, used in CBC mode, decrypts the downloaded personality application. This key is input to the module encrypted and authenticated by the PDEK using CCM and destroyed following completion or interruption of image download. It is not stored in volatile memory.
FFK,	AES, 256-bit	FFK – Flash File Key (and IV). This key, used in CBC mode, encrypts

FFK_IV		and decrypts the personality, which is saved in flash ROM. This key is randomly generated when a newly downloaded personality is ready for encryption and saved in flash ROM and is destroyed indirectly when the IMFK is destroyed
PRNGK	AES, 256-bit	PRNGK – Pseudo-Random Number Generator Key. This key is used to run the ANSI X9.31 Pseudo-Random number generator. This key is randomly generated as part of manufacturing initialization and is destroyed indirectly when the IMFK is destroyed

8.2. Public Keys

Key Name	Key Type	Description
GSK	RSA, 1024-bit	GSK – Go Command Signature Public Key. User authentication key. The User is enrolled as part of manufacturing initialization.
LSK	RSA, 1024-bit	LSK – Loader Signing Public Key is used for the image validation for the Loader. This process is an integrity check on the stored loader file.
PSK	RSA, 4096-bit	PSK – Personality Signing Public Key. Crypto Officer authentication key. This key is used for the image validation for the personality application. The Crypto Officer is enrolled as part of manufacturing initialization.

8.3. Access Rights within Services

Acronyms: R – Read, W – Write, N/A – Not Available.

Service	Cryptographic Keys and CSPs	Type of Access
Power-up self-tests	LSK	R
Getstatus	None	N/A
Version	None	N/A
Help	None	N/A
Gettime	None	N/A
Getsn	None	N/A
Setnet	None	N/A
Setport	None	N/A
Echo	None	N/A
Self-Test	None	N/A
Personality Load	IMFK	R
	PSK	R
	PDEK	R
	IDFK/IDFK_IV	decrypts, uses, discards

	PRNGK	R
	FFK/FFK_IV	W
Go (Start Personality)	IMFK	R
	GSK	R
	FFK/FFK_IV	R

9. Power On/Off States

The module is idle when there is no power applied via the 80-pin PCI-lite connector. The following states are the power off states of the Platform during this idle condition. When power is applied there are additional operational states:

State	Description
Initialized Loader	This is a state when the module leaves the factory. No personality is loaded.
Personality	This is a state when personality application loaded in Flash ROM and ready to run.
Download Personality	This is a state when actual personality application download is being performed.
Alarm	This is the state after the secure envelope has been active and a tamper attempt has been detected

9.1. Loader Alarm State LED Failure and Status Indication

The hardware has an LED to indicate the presence of the error conditions plus hard faults, such as RAM test failure and Loader signature test failure. The color of this LED is yellow.
The following LED states are defined:

- Underlined values are LED off
- **Bold values are LED on**

The alarm states indicated by the loader are shown in the following table:

Condition	LED operation (pattern in ms)	Appearance
Normal operation	Continuous	Off solid
Hard failure	**Continuous**	On solid
Tamper or other zeroization	**200** 200	Fast blink
Self-test failure	**200** 200	Fast blink
Busy	**200** 200 **200** 600	2 blinks

9.2. Loader Security State LED Status Indication

A second LED is used to indicate the state of the PSMCU, which is the security monitoring subsection. This LED is green.
The following LED states are defined:

- Underlined values are LED off
- **Bold values are LED on**

The states indicated by the loader are shown in the following table:

State or Alarm	LED operation (pattern in ms)	Appearance
Secure State, no alarms	**ON solid**	**ON solid**
Test State	**1000** 1000	Slow, regular blink
Secure State, Operating Temperature out of range	**200** 200 **200** 1000	2 short blinks
Secure State, Voltage out of range	**200** 200 **200** 200 **200** 1000	3 short blinks
Zeroized State	**250** 250	Fast, regular blink
Software integrity test failure	OFF solid	OFF solid

10. Mitigation of Other Attacks

The module has been designed to mitigate undetected penetration by means of a tamper penetration detection grid.

The physical security mechanisms of the module are the same as those employed by the previously validated ACS module (certificate# 1174). A complete envelope of protection is provided around the module. Any physical penetration results in a "tamper event," causing active zeroization of all cleartext CSPs.

11.Appendix A. Product Photo

Below are photographic pictures of the Atalla Cryptographic Subsystem. The red line around the outer metallic enclosure represents the cryptographic boundary.

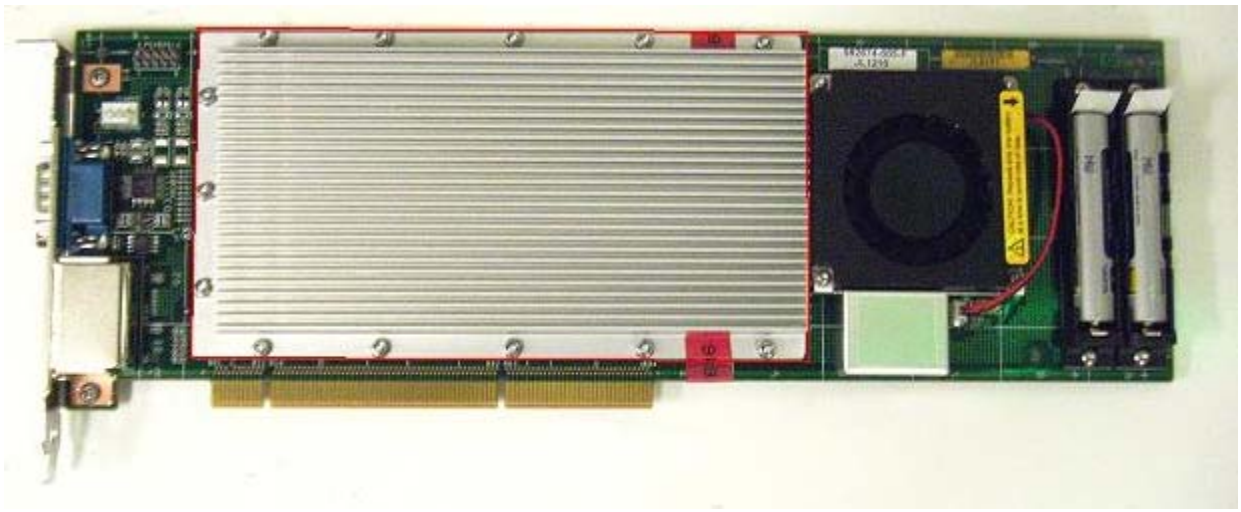

Figure 1: Front side of Atalla Cryptographic Subsystem

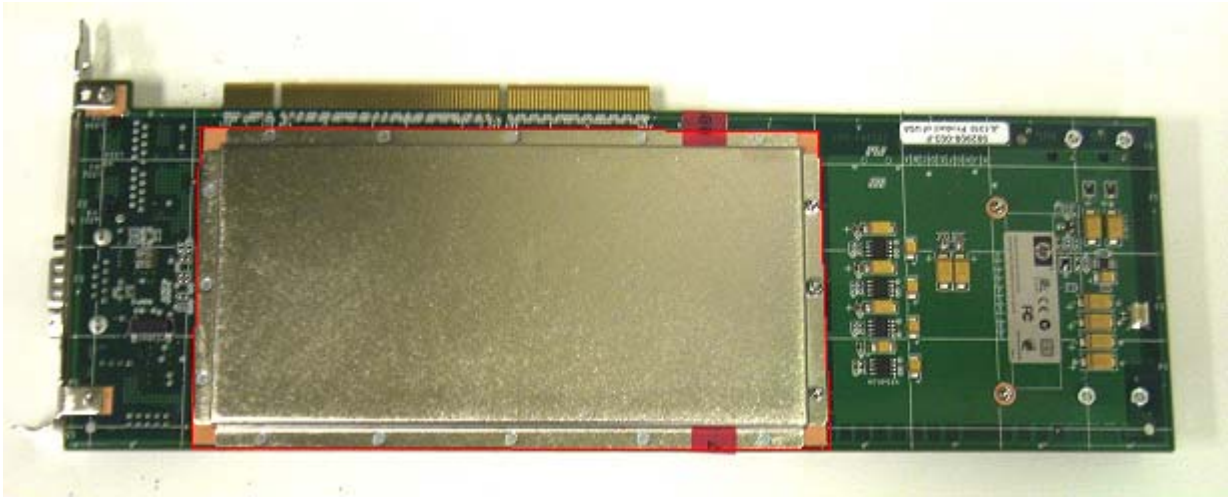

Figure 2: Back side of Atalla Cryptographic Subsystem