Hewlett-Packard Company, Atalla Security Products

Atalla Cryptographic Subsystem (ACS) Security Policy

February 8, 2008
Document Version 1.1

.

Table Of Contents

1. INTRODUCTION

The Atalla Cryptographic Subsystem (ACS) (HW P/N 543856-001, Loader Firmware Version 1.0, PSMCU Firmware Version 7.0) 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 4 Security requirements.

1.1 Reference 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] TDES standard, ANSI X9.52, *Triple Data Encryption Algorithm Modes Of Operation*
[5] "Advanced Encryption Standard (AES)", FIPS PUB 197, Nov 26 2001. http://csrc.nist.gov/publications/fips/fips197/fips197.pdf
[6] "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.).

1.2 Glossary

This section contains terms used within this document.

ACS	Atalla Cryptographic Subsystem
AES	Advanced Encryption Standard
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CPU	Central Processing Unit
CSP	Critical Security Parameter
DMA	Direct Memory Access
Flash	Non volatile memory
IV	Initialization Vector
MPU	Micro processing unit
Personality	Secure software application running inside the secure boundary
PSMCU	Physical Security Micro Control Unit
RNG	Random Number Generator
RSA	Rivest Shamir Adelman algorithm
SHA	Secure Hash Algorithm
TDES	Triple-DES

2. GENERAL DESCRIPTION

2.1 Product Overview

The Atalla Cryptographic Subsystem, or ACS (HW P/N 543856-001, Loader Firmware Version 1.0, PSMCU Firmware Version 7.0), 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 always in a FIPS Approved mode of operation. The ACS module indicates its FIPS mode of operation by verifying the Loader Firmware and PSMCU Firmware versions using the GetStatus service. When a personality is loaded and started, the module is no longer a FIPS validated module. For the module with a running personality to be a validated FIPS module, it must successfully go through re-validation testing.

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. From this point, the module can be reset and placed into FIPS mode again through power cycle. 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 FIPS 140-2 Level 4 validated module is the outer perimeter of the secure metal enclosure on the PCI card that encompasses all critical security components.

The hardware features of the ACS include:

- Tamper detection grid
- Tamper detection and response hardware
- AES hardware – Not tested and is latent functionality
- TDES hardware – Not tested and is latent functionality
- SHA-1 hardware – Not tested and is latent functionality
- MD5 hardware – Latent functionality and is non-FIPS Approved
- 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. The loader uses only the 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 three 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.

In addition to physical penetration monitoring, the ACS detects environmental attacks:

1. Temperature measurement. A "reset event" is generated whenever the temperature drops outside the range +5 to +63 degrees Celsius. A "tamper event" is generated whenever the temperature drops outside the range of -20 to +100 degree Celsius.
2. Voltage measurement. A "reset event" is generated whenever the voltages (except battery) are present and are plus or minus 15 percent of their expected values. A "tamper event" is generated whenever the battery voltage is below 15 percent of it expected value.

Tamper labels, applied to the edges of the module’s covers during manufacturing, provide physical tamper evidence.

2.1.2 Platform Memory

There are three types of memory within the ACS:

1. Random Access Memory (RAM). RAM 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.

2.2 Ports and Interfaces

2.2.1 External Ports

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

- PCI-X bus (Power Interface) – only used as a power interface.
- DB 9 RS-232 serial (Control Input, Data Input, Data Output, Status Output), compatible with PC COM ports – is used for communication of configuration or status information.
- LED (Qty. 2) (Status Output) – used to provide status of the module.
- RJ45 Ethernet (Qty. 2), compatible with 10/100/1000 Base T IEEE 802.3. – intended to be used for direct memory access (DMA) transfer of messages. NOTE: Latent interfaces - these ports are not enabled until a personality is loaded and started.

It should be noted that although a data output interface is supported, the module only outputs data when a personality is loaded and executed, which is outside the scope of the current validation. The only information that leaves the cryptographic boundary does so through the status output interface.

2.2.2 Power

Main system power is derived from the 3.3, 5.0, and 12.0-volt pins on the PCI-X connector. The power requirement from this source is approximately 12 watts. Other voltage requirements on the platform are derived from the main power except for the 3-volt 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 200 microwatts.

2.3 Supported Algorithms

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

- SHA-256 (Cert. #473)

- AES (ECB and CBC modes, encrypt and decrypt, 256-bit keys only; CCM mode, decrypt only, 256-bit keys only) (Cert. #406)
- Deterministic random number generation based on ANSI X9.31 [9]. (Cert. #200)
- RSA (signature verification); 1024 and 4096-bit keys (Cert. #148)

2.4 Security Level

Security Requirement	Level
Cryptographic Module Specification	4
Cryptographic Ports and Interfaces	4
Roles, Services and Authentication	4
Finite State Machine	4
Physical Security	4
Operating Environment	Not Applicable
Cryptographic Key Management	4
EMI/EMC	4
Self-tests	4
Design Assurance	4
Mitigation of Other Attacks	Not Applicable

3. SELF TESTS

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

Power-Up Self Tests

1. Firmware Integrity Test: The integrity of the loader is verified at startup by checking a 1024-bit RSA signature.
2. 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 DRNG known answer test
3. Critical Functions Test: 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 cleartext key values are destroyed immediately after use.

Conditional Self Tests

1. Continuous DRNG test
2. Firmware load test

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. Refer to section 10 of this document for more information.

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. A user can zeroize the module by physically removing both external batteries. This results in the battery low event, which zeroizes non-volatile RAM, and forces the unit into the ALARM state.

Rule 4:
Personality software and cryptographic keys, when loaded outside of the manufacturing site, shall be cryptographically protected with an Approved FIPS 140-2 algorithm using the appropriate key sizes. The actual key names and their uses are described in section 6 of this document.

Rule 5:
Plaintext 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 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. The status includes tamper information, personality application load status, and module version information used to verify the Approved mode of operation. The status output is broken into two parts: basic status, which customers can use for simple problem diagnosis, and extended status, which is used by HP Atalla for problem analysis. There is an optional parameter for getstatus service to display extended status. The extended status does not display any information that may compromise the security of the module.

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 Setport

This command is used to set the data rate and optionally the echo state of the serial port. The available rates are 2400, 4800, 9600, 38400, 56000, or 115200 bits per second. The default data rate is 38400 bps.

5.7 Echo

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

5.8 Self Test

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.

5.8.1 Test_sha

This command does a test of the SHA-256 cryptographic engine using the test vectors contained in [4].

5.8.2 Test_aes

This command does a test of the AES cryptographic engine using the test vectors contained in [6]

5.8.3 Test_rng

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

5.8.4 Test_signature

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

5.9 Personality Load

Personality load instructions, when successful, result in updating the flash memory. This service is authenticated as described in section 6.1.

5.10 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 module (per this validation).

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 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 (CO) is required to be properly authenticated and authentication mechanism is controlled by the PSK, 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.

6.2 User Authentication

A User is required to be properly authenticated and his authentication mechanism is controlled by the GSK, 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 (CO) is responsible for overall security of the Platform. In particular, only an operator in crypto officer role can load a personality into the ACS.

7.2 User Role

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

7.3 Roles vs. Services Matrix

Acronyms: A – available, N/A – not available, U/A – unauthenticated command.

Commands / Services	Roles	
	CO	User
Status		
GetStatus	U/A	U/A
Version	U/A	U/A
Help	U/A	U/A
Gettime	U/A	U/A
Getsn	U/A	U/A
Setport	U/A	U/A
Echo	U/A	U/A
Selftest		
Test_signature	U/A	U/A
Test_sha	U/A	U/A
Test_aes	U/A	U/A
Test_rng	U/A	U/A
Personality Load	A	N/A
Go (Start Personality)	N/A	A

8. CSPs

8.1 The Platform Keys Table

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 keys. 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.
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 ACS encrypted by the PDEK and destroyed following completion or interruption of image download. It is not stored in non-volatile memory.
FFK, FFK_IV	AES, 256-bit	FFK – Flash File Key (and IV). This key, used in CBC mode, encrypts 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 passively, 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 passively, 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

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
Setport	None	N/A
Echo	None	N/A
Self Test	None	N/A
Personality Load	PSK	R
	PDEK	R
	IDFK/IDFK_IV	decrypts, uses, discards
	FFK/FFK_IV	W
Go (Start Personality)	GSK	R
	FFK/FFK_IV	R
	PSK	R

9. POWER OFF/ON STATES

The module is idle when there is no power applied via the 188-pin 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 Indication

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

Alarm	**Pattern** (time in ms)	Appearance
SRAM Test Failure Alarm	**On Solid**	On Solid
Signature Verify Alarm	**400** 900	1 blink
DRAM Test Failure Alarm	**400** 300 **400** 900	2 blinks
Jump to Final Loader Failure Alarm	**400** 300 **400** 300 **400** 900	3 blinks
Download Failure Alarm	**400** 300 **400** 300 **400** 300 **400** 900	4 blinks

When unrecoverable alarms occur in the final loader, the status LED is turned on solid.

10. EVENTS

Events are signals that are generated by hardware circuits that monitor the physical environment. There are no actions required by the operator to enable the monitoring of the physical environment. There is no method for the operator to disable the monitoring of the physical environment.
The Platform supports Environment Failure Protection (EFP). When events have occurred the unit becomes non-operational either by going into the permanent ALARM state or the temporary RESET state.
The detected events are:

- Physical penetration - the secure boundary has been penetrated or otherwise broken. This event shall happen also by grid, switch, and signal level detection mechanisms.
- Battery low - the battery output voltage that powers the physical detectors and maintains Critical Security Parameters falls below or increases above of the normal operating voltage established for this circuitry.
- Voltage out of limits - the host system voltage is outside of the normal operating range.
- Thermal out of limits 1 - the platform temperature is outside of the normal operating range while operating on external power.

- Thermal out of limits 2 – the platform temperature is outside operational limits of components while operating on battery power only.
- Card removal detection event – the ACS PCI card is removed from the Platform. This event is not catastrophic but rather warning event. The Platform is up and running but not functioning and requires the "resume" command from the authorized personnel, which will reset the flag.

The following table shows the actions and resulting states for each event.

	Zeroize NVRAM	**Reset**	**Physical Security Alarm**
Physical Penetration	X		X
Battery Low/High	X		X
Power out of limits		X	
Thermal out of limits 1		X	
Thermal out of limits 2	X		X
Card removal detection			

11. APPENDIX A

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

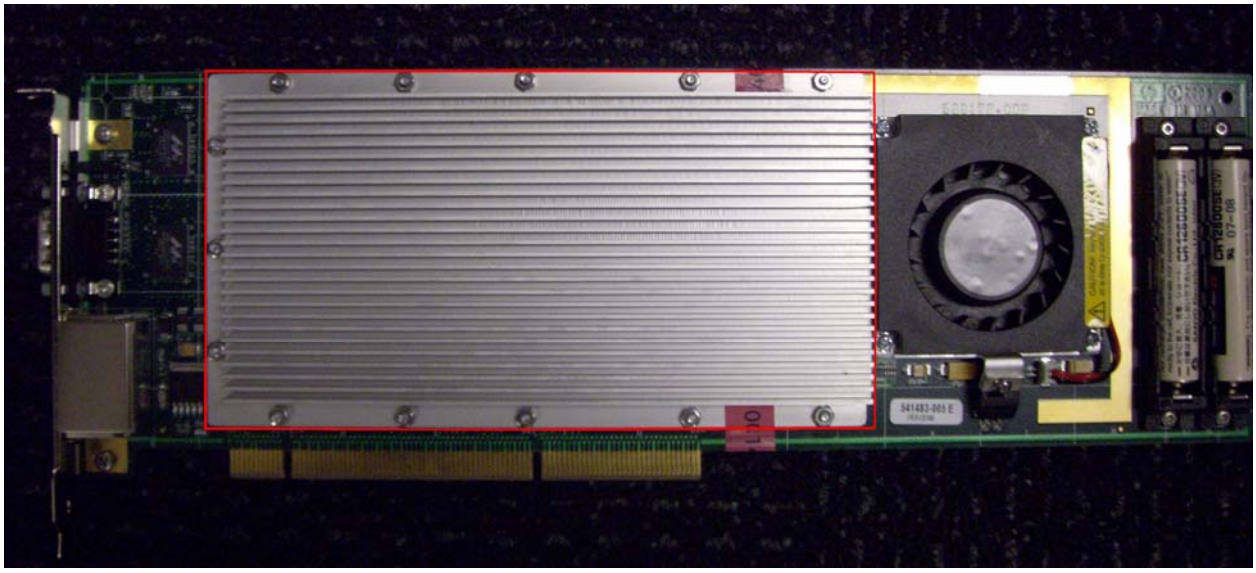

Figure 1: Front side of Atalla Cryptographic Subsystem.

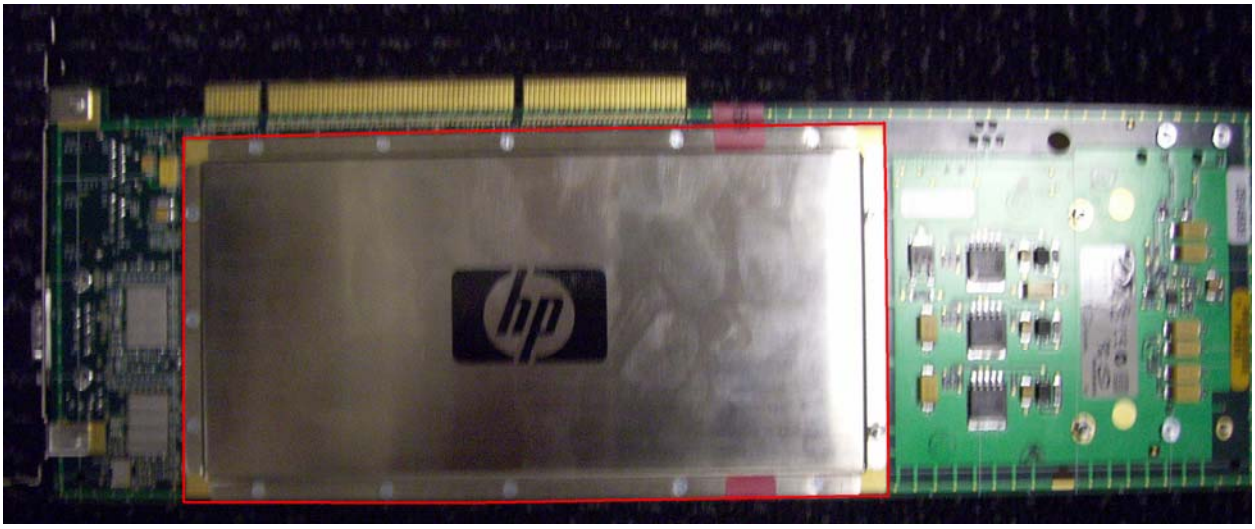

Figure 2: Back Side of Atalla Cryptographic Subsystem.