utimaco®

Atalla Cryptographic Subsystem (ACS)

FIPS 140-2

Non-Proprietary Security Policy

Version 1.5

December 11, 2019

Table of Contents

1 Introduction

The Atalla Cryptographic Subsystem, hereafter referred as ACS (HW P/N C9B60-2101A, C9B60-2101B, C9B60-2108A or C9B60-2108B, Loader Version 1.20, 1.21, 1.22 or 1.23, PSMCU Version 0.95, 0.96, 0.97 or 1.0, CMS-OCT Version 0.95 or 1.0, CMS-NTX Version 0.95, 0.96 or 1.0) 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 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. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

[2] FIPS 140-2 standard, the *Derived Test Requirements*, and on-line implementation guidelines.

[3] "Secure Hash Standard," FIPS Pub 180-4, Aug 2015 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[4] "Advanced Encryption Standard (AES)", FIPS PUB 197, Nov 26 2001. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[5] "Digital Signature Standard (DSS)", FIPS PUB 186-4, July 2013. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[6] "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality," Morris Dworkin, NIST Special Publication 800-38C, July 2007 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

[7] "Recommendation for Random Number Generation Using Deterministic Random Bit Generators", Elaine Barker and John Kelsey, NIST Special Publication 800-90A, June 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

[8] "Cavium OCTEON III CN73XX Hardware Reference Manual, CN73XX-HM-1.2P", Cavium, September 2016

1.2 Glossary

Term	Definition
ACS	Atalla Cryptographic Subsystem, also called Icarus Adapter
AES	Advanced Encryption Standard symmetric encryption algorithm that uses a 128-bit block and a key size of 128, 192 or 256 bits.
CBC	Cipher Block Chaining – A method of encrypting multiple blocks sequentially, by chaining the encrypted output from one block in as the IV to the next block, requiring each block to be processed in the same order in order to decrypt and get the clear data back.
CCM	Counter with CBC-MAC – A method of encrypting data and providing an integrity check, using only one key
CMS	Control and Monitoring System, comprised of three separate microcontrollers (CMS-Cerberos, CMS-OCT, and CMS-Nitrox-LPT) that monitor the security perimeter and environmental conditions and keep the Internal Master File Keys.
CPU	Central Processing Unit, also called Processor
CRC	Cyclic Redundancy Check – Used as a simple method of verifying code integrity.
CSP	Critical Security Parameter – This is a term used to indicate any cryptographic key or data that is used in a cryptographic algorithm.
DES	Data Encryption Standard symmetric encryption algorithm that uses a 64-bit block and a key size of 56 bits, plus parity
DMA	Direct Memory Access – Dedicated hardware that transfers data directly to or from memory across the PCIe BUS.
DRAM	Dynamic Random Access Memory, also referred to as DDR or just RAM – data is not retained when power is not present.
DRBG	Deterministic Random Bit Generator, NIST Special Publication 800-90A
ECB	Electronic Code Book – A method of encrypting each block of data independently of any others. Only that one encrypted block and the key are needed to decrypt the data.
EC or ECC	Elliptic Curve Cryptography algorithm – An asymmetric cryptographic algorithm used to define a point on a curve (public key) and an intersection point (private key)
ECDSA	Elliptic Curve Digital Signature algorithm – EC algorithm used to create digital signatures
Flash	Programmable read-only (nonvolatile) memory – Used to store all code and data that is retained when powered off.
IV	Initialization Vector – Used as input to a symmetric cryptographic operation
MD	Message Digest – The resulting output from a hash algorithm operation
NDRNG	Non-deterministic random number generator, used as the entropy source for the DRBG.
NVRAM	Nonvolatile RAM: General purpose memory maintained as nonvolatile
Personality	Secure software application running inside the secure boundary
PSMCU	Physical Security Monitoring Control Unit, refers collectively to all 3 of the microcontrollers that comprise the CMS, or specifically to the CMS-Cerberos microcontroller, which is the only interface via serial port from the Cavium Octeon processor.
RAM	Random Access Memory: General purpose volatile memory

Term	Definition
RNG	Random Number Generator – An algorithm to provide random numbers
RSA	Rivest Shamir Adelman algorithm – An asymmetric cryptographic algorithm used to define a public-private key-pair that can be used to create digital signatures.
SHA	Secure Hash Algorithm that uses 256, 384, or 512 bit sizes
TDES	Triple Data Encryption Standard that uses three separate DES symmetric algorithm operations with different keys to increase the overall strength of the algorithm that can use 2 DES keys (112-bits) or 3 DES keys (168-bits)

Table 1 Terms and Definitions

2 General Description

2.1 Product Overview

The ACS is a multi-chip embedded cryptographic module. It consists of a secure hardware platform, a firmware secure loader, and three separate microcontrollers, collectively called the Physical Security Monitoring Control Unit (or PSMCU) The purpose of the cryptographic module is to load Approved (RSA and ECDSA 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 enters a non-compliant mode. Verification that the module is in FIPS Approved mode can be observed by running the "getstatus" and "version" commands (see sections 5.1 and 5.1.2, respectively).

This security policy addresses only the hardware and the firmware secure loader; the personality is not included in the current FIPS validation. But, the PCI-HSM version of the personality, as well as the Loader are included in the PCI-HSM 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 enters a non-compliant mode. Note that the PSMCU is always running and 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, as shown in Appendix A of this document.

The hardware features of the ACS include:

- Tamper penetration detection grid
- Tamper detection and response hardware
- AES cryptographic hardware – Used by the loader for encryption algorithm
- TDES cryptographic hardware – Latent functionality unused by the Loader and in default disabled state.
- MD-5 hardware – Latent Non-FIPS functionality unused and in default disabled state.
- SHA-1 cryptographic hardware – Latent functionality unused and in default disabled state.
- SHA-256 cryptographic hardware - Latent functionality unused and in default disabled state.
- SHA-512 cryptographic hardware – Used by loader for hash algorithm
- Hardware-based random number generator – Used as entropy source for SP 800-90A DRBG.
- Large number math acceleration in hardware – Used by both RSA and ECC algorithms.
- 16 CPU cores – Only one core is used by the Loader, all others are held in reset.

Note: All cryptographic support uses a combination of hardware algorithm and software to process the operations. In addition to the hardware cryptographic algorithms used by the module, Tamper Detection and Response hardware also monitors the penetration grid and environmental conditions.

2.2 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.

In addition to physical penetration monitoring, the ACS detects environmental attacks[1]:

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.

If the module has been tampered with and a “tamper event” is generated, please contact Atalla Technical Support.

2.2.1 Platform Memory

There are three types of memory within the ACS:

1. Dynamic Random Access Memory (DRAM). DDR3 SDRAM is used to hold the Loader and its data during operation.
2. Flash Memory. Non-volatile flash memory is used to hold the loader and personality images in encrypted form. No sensitive CSPs are stored in flash as cleartext once the PSMCU enters Secure State.

[1] The EFP/EFT functionality is not reviewed or tested by the CMVP.

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.

2.3 Ports and Interfaces

2.3.1 External Ports

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

- LED (Qty. 64) – used to provide continuous status of the module. The LEDs are physically mounted on the printed circuit board. There are 4 groups of 16 LEDs that are directly controlled by 4 different hardware components. The first is the PSMCU, which secures the top level cryptographic keys and provides the interface to the Octeon CPU core. The second and third are the CMS microcontrollers which control and monitor the various power supplies and environmental conditions. Finally the Octeon CPU core running the Loader has the final 16 LEDs, of which 6 are externally visible along the back edge connector that can be seen from the rear of the unit. There are also two other LEDs visible on the rear edge connector, one from the PSMCU and one for the network link and activity for the RJ45 Ethernet port. The RJ45 Ethernet port is disabled and not used by the Loader and the RJ45 Activity LED is turned off. A diagram of the physical placement of the LEDs is shown in the figure below and a description of the LEDs is given in in the table below.

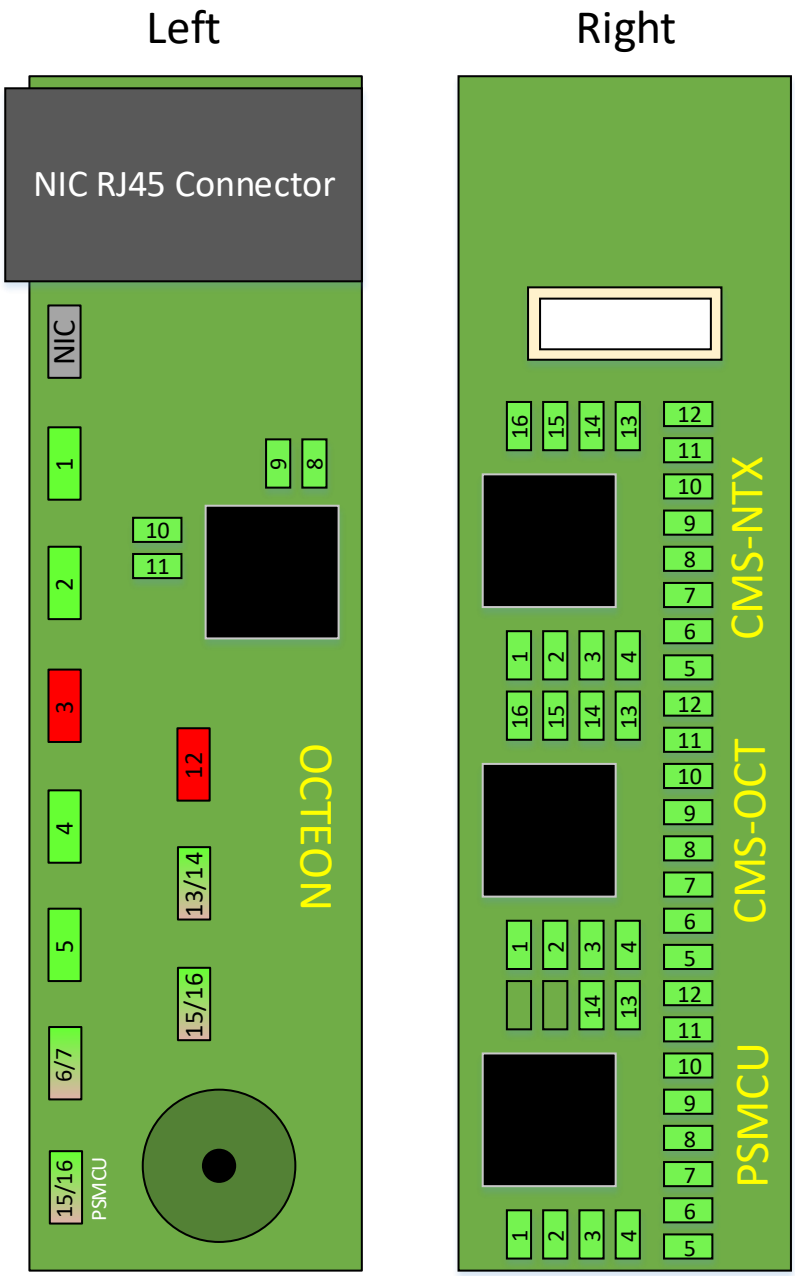

Figure 1 Status LED Layout

Group	LED #	Description	Normal State
NIC	NIC	Not currently used	Off
Octeon	1	LED_SYSTEM_READY – Icarus Banking Personality is running (Pulsing Green)	Off
	2	LED_LOADER_READY – Icarus Loader is running (Pulsing Green)	Off
	3	LED_SYSTEM_ERROR – Self-test, catastrophic or DRBG error has occurred	Off
	4	LED_BANKING_OK – Indicates the system can process banking commands	On
	5	LED_IMAGE_UPDATE – Image update in progress (Pulsing Green)	Off

	6/7	LED_SECURE/TAMPER – Indicates Secure state (Solid Green), Tamper state (Flashing Red) or Test state (slow blinking Green)	Solid Green
	8	LED_ACCESS_TYPE – Indicates HSM Enrolled in an Association (Solid Green)	Off
	9	LED_CATASTROPHIC – Fatal error during Personality normal operation	Off
	10	LED_DRBG_ERROR – Failure during continuous DRBG self-test	Off
	11	LED_SELF_TEST_ERROR – Loader or Personality diagnostic self-test error	Off
	12	Not used	Off
	13/14	BATTERY_LIFE (Good = Green, Replace = Red/Green, Critical = Red, Expired = Flashing Red)	Solid Green
	15/16	CPU_BUSY (0% = Solid Green, 100% = Flashing Red)	Solid Green
PSMCU	15/16 Left Edge	PSMCU General/Loader Status – Indicates in Loader and not Enrolled (Off), in Loader and Personality is Enrolled (Flashing Green), in Personality (Solid Green), or PSMCU fault (Flashing Red)	Off or Solid Green
	1	T1 – State of Top Serpentine Trace 1	On
	2	T2 – State of Top Serpentine Trace 2	On
	3	TP – State of Top Penetration Layer	On
	4	B1 – State of Bottom Serpentine Trace 1	On
	5	B2 – State of Bottom Serpentine Trace 2	On
	6	BP – State of Bottom Penetration Layer	On
	7	FA – State of Picket Fence Trace A	On
	8	FB – State of Picket Fence Trace B	On
	9	FC – State of Picket Fence Trace C	On
	10	FD – State of Picket Fence Trace D	On
	11	FE – State of Picket Fence Trace E	On
	12	Board Removal – Solid Green if good, Flashing Green if not	On
	13	Vbat – State of the Vbat supply	On
	14	THERMAL_STATUS_LED	On
CMS-OCT	1	DDR0_2V5_STATUS – State of 2.5V supply for DDR bank 0	On
	2	DDR0_1V2_STATUS – State of 1.2V supply for DDR bank 0	On
	3	DDR0_0V6_STATUS – State of 0.6V supply for DDR bank 0	On
	4	Unused	Off
	5	HOST_12V_STATUS – State of the host 12V supply	On
	6	HOST_3V3_STATUS – State of the host 3.3V supply	On
	7	VDD_1V5_STATUS – State of the Octeon 1.5V supply used for PCIe	On
	8	VDD_1V5lp_STATUS – State of the Octeon 1.5V aux supply	On
	9	CORE_5V0_STATUS – State of the 5.0V supply used in the CORE regulator	On
	10	CORE_0V9_STATUS – State of the Octeon core 0.9V supply	On
	11	PLL_DC_OK_STATUS – State of the PLL_DC_OK line to the Octeon	On
	12	CHIP_RESET_STATUS – State of the CHIP_RESET line to the Octeon	On
	13	TEMPERATURE_STATUS – State of the Octeon temperature reading	Off
	14	DDR1_0V6_STATUS – State of 0.6V supply for DDR bank 1	On
	15	DDR1_1V2_STATUS – State of 1.2V supply for DDR bank 1	On
	16	DDR1_2V5_STATUS – State of 2.5V supply for DDR bank 1	On
CMS-NTX	1	NTX_CLOCK_STATUS	On
	2	NTX_E_LOCK_STATUS	On for first minute after HOST power on, off after unless Nitrox Is activated by the Octeon during normal operation of the system
	3	NTX_S_LOCK_STATUS	
	4	NTX_Z_LOCK_STATUS	
	5	NTX_5V0_STATUS	
	6	NTX_0V9_STATUS	
	7	NTX_1V8_STATUS	
	8	NTX_1V8_VPH_STATUS	
	9	NTX_1V8_VPTX_STATUS	
	10	NTX_RESET_L	
	11	NTX_DC_OK	
	12	NTX_ZERO	Off
	13	Unused	Off
	14	Unused	Off
	15	NTX_HOST_3V3_GOOD_LED	On
	16	NTX_HOST_12V_GOOD_LED	On

Table 2 Status LED Meanings

- RJ45 Ethernet (Qty. 1), compatible with 10/100 Base T IEEE 802.3. – Not used by the loader and not in the scope of this document.
- Serial port. This is standard RS-232.
- PCIe. This interface is the primary interface used to send commands and data to, and receive status from, the ACS. In addition, this is the primary power connection to the ACS.

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

		Physical Ports			
		Ethernet Port	LEDs 0-63	Serial Interface	PCIe
Logical Ports	Data Input			√	√
	Data Output†			√	√
	Control Input			√	√
	Status Output		√	√	√

Table 3 Logical to Physical Port Mappings

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.

2.3.2 Power

Primary main system power is derived from the 3.3V pins on the PCIe connector. The supplies derived from the 3.3V pins are

- Nitrox 1.8V (PLL, VPH & VPTX)
- External printer interface (LPT)
- CMS main power
- Octeon PCIe 1.5V supply
- Octeon DDR4 memory supplies (2.5V, 1.2V and 0.6V)

In addition to the power from the PCIe connector there is an additional power connector on the right side of the board. This connector provides 12V that is used solely to provide the CORE (0.9V) power for the Octeon through a step down regulator.

Also on the PCIe connector there is a 3.3Vaux supply pin that provides standby power to the two CMS chips as well as the PSMCU. This power is present whenever the HOST has power available regardless of whether is it turned on or not.

Finally there is a battery supply input that provides power to the PSMCU to maintain perimeter penetration detection and security keys when neither the 3.3V or 3.3Vaux power from the HOST is available.

The power requirements are:

- 3.3V: 10 W
- 3.3Vaux: 250 mW
- Vbat: 100 mW
- 12V: 80 W (maximum)
- Total Power: 91 W

2.4 Supported Algorithms

The Loader includes these FIPS-Approved algorithms:

- FIPS 180-4 SHA-512 (Cert. # 3776)
- FIPS 197 AES (encrypt, decrypt, ECB and CBC modes, 256-bit keys only) (Cert. # 4600)
- SP 800-38C CCM encrypt and MAC, decrypt and MAC (AES, 256-bit keys only) (Cert. # 4601)
- SP 800-90A DRBG (AES-256 CTR with derivation function) (Cert. # 1542)
- FIPS 186-4 RSA (signature verification); 2048 and 4096-bit keys (Cert. # 2518)
- FIPS 186-4 ECDSA (signature verification); NIST P-521 curve (Cert. # 1128)
- SP 800-133 CKG (vendor affirmed)

The module includes these non-approved, but allowed algorithms:

- NDRNG hardware entropy source used to seed the SP 800-90A DRBG. A minimum of 1024 bits of entropy is gathered before generating keys.
- CRC-32 used as 32-bit EDCs for Boot and Loader code.

2.5 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	Not Applicable

Table 4 Security Level

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 test of Boot and Loader code.
2. Firmware Integrity Test: The integrity of the Loader is verified at startup by checking a 4096-bit RSA signature and ECDSA P-521 signature, both of which must be verified successfully to continue.
3. The cryptographic functions are all tested at startup using known answer tests
    a. SHA-512 hash
    b. AES-256 (encrypt, decrypt, ECB and CBC modes)
    c. RSA-4096 signature verification
    d. ECDSA P-521 signature verification
    e. SP 800-90A DRBG
    f. CCM mode of AES algorithm (encrypt and decrypt)

4. Critical Functions Tests:
    a. Memory test – done during DDR RAM initialization
    b. Key Integrity Check: All Loader keys are stored encrypted using CCM. The key CCM MAC is used to verify integrity before these keys are used. All PSMCU CSPs are stored within the PSMCU in cleartext form use leftmost 16-bytes of SHA-512 hash as the check digits. The check digits are used to verify integrity before these keys are used.

Conditional Self-Tests

1. Continuous NDRNG test.
2. Continuous DRBG test.
3. DRBG (Instantiate/Generate/Reseed) health tests.
4. Firmware load test: This is a series of tests used to validate the integrity of the Loader firmware or personality when loaded into the module. These tests include CCM for secure and authenticated key transport, Signature test (RSA 4096-bit modulus and ECDSA P-521 curve both with SHA-512), AES-256 file decryption, and CRC-32 for simple integrity check.
5. Critical Functions Tests:
    a. “go” command personality start validation: The “go” command is authenticated using a 2048-bit signature. Following this, the personality integrity is validated with CRC-32, then decrypted using AES-256, then validated again by verifying its signatures (RSA 4096-bit modulus and ECDSA P-521 curve both with SHA-512), 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

This section lists the security rules, under which the module shall operate, including the security rules derived from the requirements of the FIPS 140-2 standard.

Rule 1:
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 2:
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 3:
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.

Rule 4:
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 5:
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 6:
The ACS does not support maintenance and bypass modes.

Rule 7:
Failure of self-tests result in the module entering an error state.

Rule 8:
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 Show Status

5.1.1 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, mode of operation (Approved vs. non-Approved), etc. Approved vs. non-Approved operation is indicated by the combination of status, software version information, and hardware serial number given in the output of the command. The status output is broken into three parts: basic status, which customers can use for simple problem diagnosis; extended status, which is used by 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 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.

5.1.2 Version

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

5.1.3 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.

5.1.4 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).

5.1.5 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.

5.1.6 Echo

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

5.2 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-512. These tests are identical to the power-up self-tests.

5.2.1 Test_aes

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

5.2.2 Test_ccm

This command does a test of the CCM mode of operation of the AES algorithm using test vectors published on NIST CAVP website.

5.2.3 Test_crc

This command does a test of the CRC-32 cyclical redundancy check algorithm using known answer test.

5.2.4 Test_rng

This command does a known-answer test of the DRBG using known answer test values contained in [7].

5.2.5 Test_sha

This command does a test of the SHA-512 cryptographic engine using the test vectors contained in [3].

5.2.6 Test_sig_rsa

This command performs a known-answer test of the RSA 4096-bit modulus signature computation algorithm using test vectors published on NIST CAVP website.

5.2.7 Test_sig_ecdsa

This command performs a known-answer test of the ECDSA P-521 curve signature computation algorithm using test vectors published on NIST CAVP website.

5.3 Personality Load

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

5.4 Go (Start Personality)

The start personality service passes control from the loader to the personality in one of 3 different types (A PCI-HSM validated personality mode, a FIPS validated personality mode, and a mode for personalities that have not been PCI-HSM or FIPS validated). This service must be authenticated by an operator in the User role by verifying a signature of the “go” command for the specified personality type (i.e. go, go-pci, or go-fips), which must also match the type of the personality stored in flash. If the PSMCU active “type” value has not been selected (i.e. type = “General”), any of the 3 personality types can be loaded. If the PSMCU active “type” value has already been selected (i.e. type != “General”) by a previous personality load, then only that same type of personality can be loaded, without resetting the PSMCU “type” value. Once the PSMCU “type” value has been selected and the personality has been enrolled in an association, it will require the personality to be reset to factory state and then the server power-cycled or rebooted. If the personality is loaded and not enrolled into an association yet, it will automatically reset the “type” to “General” on the next power cycle or reboot.

5.5 Zeroize[2]

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.

5.6 Firmware Load

Firmware Load service is to update the Loader firmware. Two commands are required to perform this service: prepdnld and writeimage. The former prepares the module to receive an image download and the latter is used to load the firmware to the module. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation. This service is authenticated as described in section 6.

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 four operator identities – one capable of assuming the Crypto Officer (CO) and the other three capable of assuming the User role for one of the three different personality modes. (See the next section for a discussion of roles.)

The Crypto Officer role is far more security relevant than the User role from the FIPS perspective, 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) and PECSK (private key), which are used to sign personality images, and the LSK (private key) and LECSK (private key), which are used to sign the Loader firmware. A CO uses his knowledge of the PSK (private key) and PECSK (private key) to create signed personality images for download to the unit. Similarly, the CO uses his knowledge of the LSK (private key) and LECSK (private key) to create signed loader images. A

[2] Refer to Rule 2 for detailed information on zeroization

4096-bit RSA key and a P-521 ECDSA private key shall be used for the authentication process.

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 for each of the three personality types. A User uses his knowledge of the GSK (private key) to sign either the ‘go’ command, the ‘go-pci’ command, or the ‘go-fips” command which allows the Loader to exit and start a personality of the same designated type. The User’s authentication key is a 2048-bit RSA key.

6.3 Authentication Strength

User authentication is determined by the GSK, a 2048-bit digital signature verification key. This key has an equivalent strength of 112 bits. For this example:

$2^{112} = 5.19\ E33$

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

The 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:

$60 / 2^{112} = 60 / 5.19\ E33 = 1.15\ E-32$

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 or LSK, a 4096-bit digital signature verification key and a PECSK or LECSK, a NIST P-521 curve ECDSA digital signature verification key. Both signatures (i.e., PSK and PECSK or LSK and LECSK) must be verified for successful authentication, therefore the key with the greater strength will be used for strength equivalence. The 4096-bit RSA key strength is equivalent to 150 bits and the P-521 EC key has an equivalent strength as 256 bits. Both types of keys exceed the requirements; the P-521 ECDSA key will exceed the requirements by at least a factor of 2^{144}.

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			√
Echo			√
Self-test			
Test_sig_rsa			√
Test_sig_ecdsa			√
Test_sha			√
Test_aes			√
Test_rng			√
Test_ccm			√
Test_crc			√
Personality Load	A		
Go (Start Personality)		A	
Zeroize			√
Firmware Load	A		

Table 5 Roles vs. Services Matrix

8 CSPs

8.1 Platform Keys[3]

Key Name	Type and Size	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 using unmodified output from the DRBG 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, 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 using unmodified output from the DRBG when a newly downloaded personality is ready for encryption and saved in flash ROM encrypted and authenticated by the IMFK using CCM and destroyed indirectly when the IMFK is destroyed
DRBG Seed	Entropy Input, 1024-bit; Nonce, 256-bit; Personalization String, 256-bit	DRBG Seed – 1536 bits to seed the DRBG. The entropy input and nonce are generated using the NDRNG. The seed is stored in plaintext in volatile memory and destroyed by any loss of power.
DRBG Key	AES, 256-bit	DRBG Key – part of SP 800-90A DRBG Internal State. It is generated with the DRBG, stored in plaintext in volatile memory, and destroyed actively by tamper event, passively by battery failure, or by any power failure.
DRBG V	DRBG Internal State value, 128-bit	DRBG V – part of SP 800-90A DRBG Internal State. It is generated with the DRBG, stored in volatile memory, and destroyed actively by tamper event or passively by battery failure, or by any power failure.

Table 6 Platform Keys

[3] All symmetric keys that are generated by the DRBG are generated from the direct output of the Approved DRBG.

8.2 Public Keys

Key Name	Key Type	Description
GSK	RSA, 2048-bit	GSK – Go Command Signature Public Key. User authentication key. The User is enrolled as part of manufacturing initialization.
LSK	RSA, 4096-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. Also, requires LECSK signature verification.
LECSK	ECDSA, P-521	LECSK – Loader Elliptic Curve Signing Public Key is used for the image validation for the Loader. This process is an integrity check on the stored loader file. Also, requires LSK signature verification.
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. Also, requires PECSK signature verification.
PECSK	ECDSA, P-521	PECSK – Personality Elliptic Curve Signing Public Key. Crypto Officer authentication key. This key is used for the image validation for the personality application. The Crypto Office is enrolled as part of the manufacturing initialization. Also, requires PSK signature verification.

Table 7 Public Keys

8.3 Access Rights within Services

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

Service	Cryptographic Keys and CSPs	Type of Access
Power-up self-tests	LSK	R
	LECSK	R
Getstatus	None	N/A
Version	None	N/A
Help	None	N/A
Gettime	None	N/A
Getsn	None	N/A
Echo	None	N/A
Self-Test	None	N/A
Personality Load	IMFK	R
	PSK	R
	PECSK	R
	PDEK	R
	IDFK/IDFK_IV	R, D
	FFK/FFK_IV	R, W
	DRBG Seed	R, W
	DRBG Key	R, W
	DRBG V	R,W
Go (Start Personality)	IMFK	R
	GSK	R
	PSK	R
	PECSK	R
	FFK/FFK_IV	R
Firmware Load	IMFK	R
	PSK	R
	PECSK	R
	PDEK	R
	IDFK/IDFK_IV	R, D
Zeroize	All	D

Table 8 Access Rights within Services

9 Power On/Off States

The module is idle when there is no power applied via the 80-pin PCIe 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 or if there is a failure in critical function or self-tests.

Table 9 Power On/Off States

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)[4]. 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 is removed from the Platform. This event is not catastrophic but rather warning event. The Platform is up and running but not

[4] The EFP/EFT functionality is not reviewed or tested by the CMVP.

functioning (in suspend mode) 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	Suspend	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				X

Table 10 Events and States mapping

Appendix A Product Photo

The cryptographic boundary of the module is the outer perimeter of the secure metal enclosure that encompasses all critical security components. The red line around the outer metallic enclosure, as shown in ***Figure 2*** below, represents the cryptographic boundary.

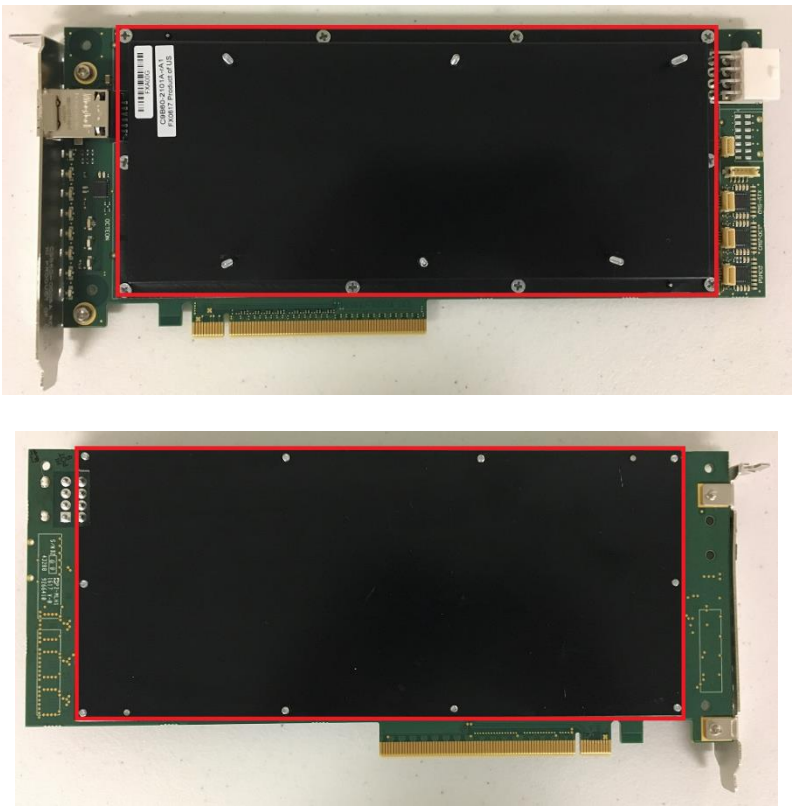

Figure 2: Front and back side of the Atalla Cryptographic Subsystem