Atalla Cryptographic Subsystem (ACS)

Hardware Version: C9B60-2108A, C9B60-2108B and C9B60-2108C

Firmware Version: Loader Version 1.24; PSMCU Version 1.0.1, or 1.0.3; CMS-OCT Version 0.95,1.0.0, or 1.0.3; CMS-NTX Version 1.0.0; Loader Stage 1 Version 1.10; Loader Stage 2 Version 1.20; Boot Version 1.23

FIPS 140-3
Non-Proprietary Security Policy

Document Version 1.75

February 5, 2025

Contents

Introduction

The Atalla Cryptographic Subsystem (ACS), hereafter referred as ACS, 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 140-3 Level 3 Security requirements.

Related Documents

[1] "Security Requirements for Cryptographic Modules," FIPS PUB 140-3, Information Technology Laboratory, National Institute of Standards and Technology. March 22, 2019. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

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

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

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

[5] "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

[6] "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

[7] "Recommendation for Block Cipher Modes of Operation: Methods and Techniques."Dworkin, Morris, NIST Special Publication 800-38A, December 2001. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

[8] "Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping." Dworkin, Morris, NIST Special Publication 800-38F, December 2012. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf

[9] "Recommendation for Cryptographic Key Generation." Elaine Barker, Allen Roginsky, and Richard Davis, NIST Special Publication 800-133 Revision 2, June 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf

[10] "Recommendation for Random Bit Generator (RBG) Constructions." Elaine Barker, John Kelsey, Kerry McKay, Allen Roginsky, and Meltem Sönmez Turan, NIST SP 800-90C 3pd, September 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90C.3pd.pdf

[11] "Recommendation for the Entropy Sources Used for Random Bit Generation." Meltem Sönmez Turan (NIST), Elaine Barker (NIST), John Kelsey (NIST), Kerry McKay (NIST), Mary Baish (NSA), Michael Boyle (NSA), NIST Special Bulletin 800-90B, January 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf

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
CKG	Cryptographic Key Generation
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 800-90Arev1
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.

Term	Definition
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
ENT	SP800-90B entropy source
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
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.
PSP	Public Security Parameter
RAM	Random Access Memory: General purpose volatile memory
RBG	Random Bit Generator: A device or algorithm that outputs a random sequence that is effectively indistinguishable from statistically independent and unbiased bits.
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
SSP	Sensitive Security Parameter
Triple-DES	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

Product Overview

1. General

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

1.1 Security Level

ISO/IEC 24759 Section 6 [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	3
2	Cryptographic Module Specification	3
3	Cryptographic Module Interfaces	3
4	Roles, Services, and Authentication	3
5	Software/Firmware Security	3
6	Operational Environment	N/A
7	Physical Security	3
8	Non-invasive Security	N/A
9	Sensitive Security Parameter Management	3
10	Self-Tests	3
11	Life-Cycle Assurance	3
12	Mitigation of Other Attacks	N/A

Table 2 Security Level

2. Cryptographic Module Specification

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 module is in an Approved mode of operation until a personality is loaded and started, at which point the module enters a non-compliant state. Verification that the module is in Approved mode can be observed by running the “getstatus” and “version” commands.

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 state. Note that the PSMCU is always running and no personality, no matter what its FIPS 140-3 validation level, will have access to the module’s secret keys and CSPs.

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

Model	Hardware (Part Number & Version)	Firmware Version	Distinguishing Features
ACS	C9B60-2108A	Loader: 1.24 PSMCU: 1.0.1 CMS-OCT: 1.0.0 CMS-NTX: 1.0.0 Loader Stage 1: 1.10 Loader Stage 2: 1.20 Boot: 1.23	N/A
ACS	C9B60-2108B	Loader: 1.24 PSMCU: 1.0.1 CMS-OCT: 1.0.0 CMS-NTX: N/A Loader Stage 1: 1.10 Loader Stage 2: 1.20 Boot: 1.23	N/A
ACS	C9B60-2108C	Loader: 1.24 PSMCU: 1.0.1, 1.0.3 CMS-OCT: 1.0.0, 1.0.3 CMS-NTX: N/A Loader Stage 1: 1.10 Loader Stage 2: 1.20 Boot: 1.23	N/A

Table 3 Cryptographic Module Tested Configuration

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
- Triple-DES cryptographic hardware – Latent functionality unused and in default disabled state.
- MD-5 hardware – Latent 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 800-90Arev1 DRBG, SP800-90B Entropy Source, and SP800-90C RBG draft constructions.
- 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.

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s)/Key Strength(s)	Use/Function
A2606	AES-CCM [SP 800-38C]	AES-CCM	256-bit	Encrypt, Decrypt
A2606	Conditioning Component Block Cipher Derivation Function [SP 800-90B]	Conditioning Component Block Cipher Derivation Function SP800-90B	256-bit	Vetted conditioner for ENT (P)
A2606	Counter DRBG [SP 800-90Arev1]	Counter DRBG	AES 256-bit with derivation function and no prediction resistance	Symmetric Key Generation
A2606	ECDSA SigVer [FIPS 186-4]	ECDSA SigVer	NIST P-521 with SHA2-512	Authentication, Signature Verification, and Integrity Testing
A2606	RSA SigVer [FIPS 186-4]	RSA SigVer	PKCS#1.5 with 2048-bit and 4096-bit modulus and SHA2-512	Authentication, Signature Verification, and Integrity testing
AES 4600	AES-CBC [SP 800-38A]	AES-CBC	256-bit	Encrypt, Decrypt
AES-CCM A2606	KTS [SP 800-38F]	SP800-38C and SP800-38F. KTS (key unwrapping) per IG D.G.	256-bit keys providing 256 bits of encryption strength	Establish keys
N/A	ENT (P) [SP 800-90B]	ENT (P)	SP800-90B Entropy Source	Entropy source for Counter DRBG
SHS 3776	SHA2-512 [FIPS 180-4]	SHA2-512	SHA2-512	Hashing
Vendor Affirmed	CKG [SP 800-133rev2]	Section 6.1	Cryptographic Key Generation; SP 800-133rev2 and IG. D.H.	Symmetric Key Generation

Table 4 Approved Algorithms

Note: The module does not implement any non-approved algorithms allowed in the approved mode of operation, non-approved algorithms allowed in the approved mode of operation with no security claimed or non-approved algorithms not allowed in the approved mode of operation.

2.1 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*** below, represents the cryptographic boundary.

Note: There is no visibly discernable difference between hardware versions other than the part number.

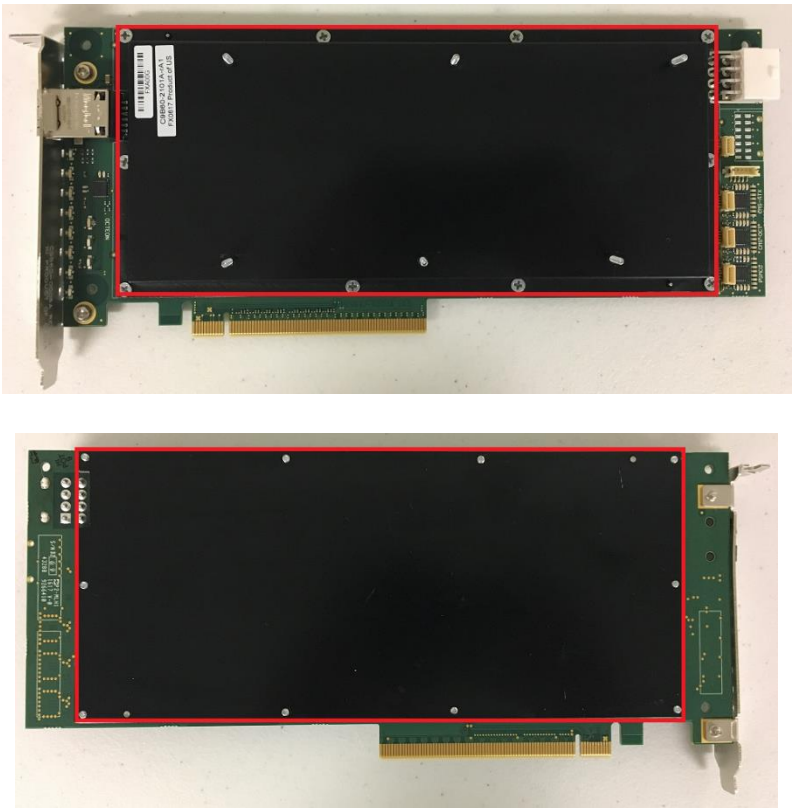

Figure 1: Front and back side of the Atalla Cryptographic Subsystem

3. Cryptographic Module Interfaces

3.1 External Ports

There are four physical 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.

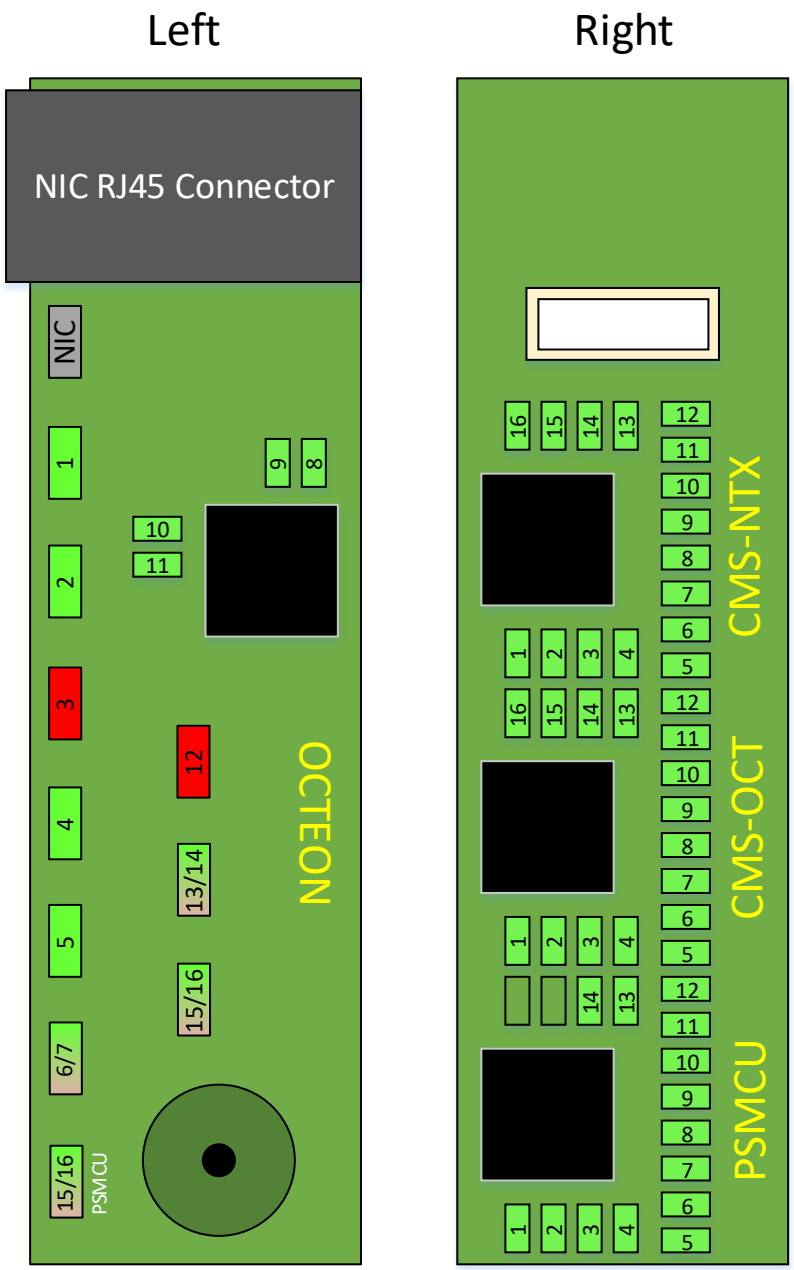

Figure 2 Status LED Layout

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 5 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 Port	Logical Interface	Data that passes over port/interface
LEDs 0-63	Status Output	Secondary status output and informational data
Serial Interface	Data Input, Control Input, Status Output	Alternate interface for communication channel
PCIe	Data Input, Control Input, Status Output	Primary Interface for communication

Table 6 Ports & Interfaces

Note: No SSPs 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.

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 it is 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

4. Roles, Services and Authentication

4.1 Roles

4.1.1 Unauthenticated Role

An unauthenticated role has access to services as specified in Table 9. These services fall under Exception “e” (show status, show version, and self-tests) or Additional Comment 5 (zeroization) from FIPS 140-3 IG 4.1.A.

4.1.2 Crypto Officer Role

A Crypto Officer is responsible for the overall security of the module. Only an operator in the Crypto Officer role can load a personality into the ACS.

4.1.3 User Role

A User can perform a limited number of the services available on the module as indicated in the following section.

4.2 Service Inputs and Outputs

Role	Service	Input	Output
Crypto Officer	Firmware Load	prepdnld and writeimage	“ok” upon success “fail” upon failure
Unauthenticated	Status Information	GetStatus	Status information
Unauthenticated	Version	Version	Version numbers of loader, boot, psmcu, cms-oct, cms-ntx (if applicable)
Unauthenticated	Help	Help	List of available commands

Unauthenticated	Get Time	Gettime	Time in yymmddhhmmss and “ok” upon success
Unauthenticated	Get Serial Number	Getsn	Serial number and “ok” upon success
Unauthenticated	Echo Test	Echo along with testing text	Testing text is returned upon success
Unauthenticated	RSA Signature Test	Test_sig_rsa	“ok” upon success, “fail” upon test failure
Unauthenticated	ECDSA Signature Test	Test_sig_ecdsa	“ok” upon success, “fail” upon test failure
Unauthenticated	SHA Test	Test_sha	“ok” upon success, “fail” upon test failure
Unauthenticated	AES Test	Test_aes	“ok” upon success, “fail” upon test failure
Unauthenticated	RBG Test	Test_rng	“ok” upon success, “fail” upon test failure
Unauthenticated	DRBG Test	Test_drbg	“ok” upon success, “fail” upon test failure
Unauthenticated	Entropy Test	Test_entropy	“ok” upon success, “fail” upon test failure
Unauthenticated	CCM Test	Test_ccm	“ok” upon success, “fail” upon test failure
Unauthenticated	CRC Test	Test_crc	“ok” upon success, “fail” upon test failure
Crypto Officer	Personality Load	prepdnld and writeimage	“ok” upon success, “fail” upon failure
Unauthenticated	Zeroize	N/A	ALARM or TAMPER state
User	Start Personality “go”	“go”, “go-pci”, “go-fips”	“ok” when personality is valid and ready to start

Table 7 Roles, Service Commands, Input and Output

4.3 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.

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.

4.3.1 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) (not SSP's), 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 4096-bit RSA key and a P-521 ECDSA private key shall be used for the authentication process.

4.3.2 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.

Role	Authentication Method	Authentication Strength
Crypto Officer	Single-Factor Cryptographic Device Authenticators	256 bits; (RSA) Authentication is performed using RSA 4096 /w SHA-512 signatures (provides 152 bits of strength). The probability that a random attempt will succeed, or a false acceptance will occur, is approximately 1 in 2^152, which is less than 1 in 1,000,000. The command authentication takes approximately 1 second to complete. Therefore a maximum of 60 authentication attempts can be made per minute. Based on this maximum rate, the probability that a random attempt will succeed in a one-minute period is approximately 60 in 2^152, which is less than 1 in 100,000. (ECDSA) Authentication is performed using ECDSA P-521 /w SHA-512 signatures (provides 256 bits of strength). The probability that a random attempt will succeed, or a false acceptance will occur, is approximately 1 in 2^256, which is less than 1 in 1,000,000. The command authentication takes approximately 1 second to complete. Therefore a maximum of 60 authentication attempts can be made per minute. Based on this maximum rate, the probability that a random attempt will succeed in a one-minute period is approximately 60 in 2^256, which is less than 1 in 100,000.
User	Single-Factor Cryptographic Device Authenticators	112 bits; Authentication is performed using RSA 2048 /w SHA-512 signatures (provides 112 bits of strength). The probability that a random attempt will succeed, or a false acceptance will occur, is

		approximately 1 in 2^112, which is less than 1 in 1,000,000. The command authentication takes approximately 1 second to complete. Therefore a maximum of 60 authentication attempts can be made per minute. Based on this maximum rate, the probability that a random attempt will succeed in a one-minute period is approximately 60 in 2^112, which is less than 1 in 100,000.

Table 8 Roles and Authentication

4.4 Approved Services

The following table specifies the module's approved services. For Access rights to Keys and/or SSPs the following legend applies:

G = Generate: The module generates or derives the SSP.
R = Read: The SSP is read from the module (e.g. the SSP is output).
W = Write: The SSP is updated, imported, or written to the module.
E = Execute: The module uses the SSP in performing a cryptographic operation.
Z = Zeroise: The module zeroises the SSP.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
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	AES-CCM, AES-CBC, RSA SigVer, ECDSA SigVer, KTS	IMFK, PSK, PECSK, FFK	Crypto Officer	E, E, E, GWE	The successful completion of a service is an implicit indicator for the use of an approved service

	the scope of this validation must be validated through the FIPS 140-3 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-3 validation. This service is authenticated as described below					
Status Information	Limited status information shall always be available. This command is used to read and display the status of the module. The status includes tamper information, personality application load status, mode of operation (Approved vs. non-compliant state), etc. Approved vs. non-compliant state of operation is indicated by the combination of status, software version information, and hardware serial number given in the output of the	N/A	N/A	Unauthenticated	N/A	The successful completion of a service is an implicit indicator for the use of an approved service

	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. Note, this corresponds to the “Show Status” mandatory service.					
Version	The version command is used to retrieve the loader name, product type, software version,	N/A	N/A	Unauthenticated	N/A	The successful completion of a service is an implicit

	and build date and time. Note, this corresponds to the "Show module's versioning information" mandatory service.					indicator for the use of an approved service
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.	N/A	N/A	Unauthenticated	N/A	The successful completion of a service is an implicit indicator for the use of an approved service
Get Time	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).	N/A	N/A	Unauthenticated	N/A	The successful completion of a service is an implicit indicator for the use of an approved service
Get Serial Number	This command reads the value of	N/A	N/A	Unauthenticated	N/A	The successful

	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.					completion of a service is an implicit indicator for the use of an approved service
Echo Test	The echo command is used to test the I/O connection to the Loader.	N/A	N/A	Unauthenticated	N/A	The successful completion of a service is an implicit indicator for the use of an approved service
RSA Signature Test	This command performs a known-answer test of the RSA 4096-bit modulus signature computation algorithm using test vectors published on NIST CAVP website.	RSA SigVer	N/A	Unauthenticated	N/A	The successful completion of a service is an implicit indicator for the use of an approved service
ECDSA Signature Test	This command performs a known-answer test of the ECDSA P-521 curve signature computation algorithm using test vectors	ECDSA SigVer	N/A	Unauthenticated	N/A	The successful completion of a service is an implicit indicator for the use of an

	published on NIST CAVP website.					approved service
SHA Test	This command does a test of the SHA-512 cryptographic engine using the test vectors contained in [2].	SHA2-512	N/A	Unauthenticated	N/A	The successful completion of a service is an implicit indicator for the use of an approved service
AES Test	This command does a test of the AES cryptographic engine using the test vectors contained in [3].	AES-CBC	N/A	Unauthenticated	N/A	The successful completion of a service is an implicit indicator for the use of an approved service
RBG Test	This command does a known-answer test of the SP800-90C RBG draft construction.	N/A	N/A	Unauthenticated	N/A	The successful completion of a service is an implicit indicator for the use of an approved service
DRBG Test	This command does a known-answer test of the SP800-90Arev1 DRBG using known answer test values contained in [6].	Counter DRBG	N/A	Unauthenticated	N/A	The successful completion of a service is an implicit indicator for the use

						of an approved service
Entropy Test	This command does a self-test of the SP800-90B Entropy Source generating 4096 entropy samples with continuous health-tests enabled.	ENT (P)	N/A	Unauthenticated	N/A	The successful completion of a service is an implicit indicator for the use of an approved service
CCM Test	This command does a test of the CCM mode of operation of the AES algorithm using test vectors published on NIST CAVP website.	AES-CCM	N/A	Unauthenticated	N/A	The successful completion of a service is an implicit indicator for the use of an approved service
CRC Test	This command does a test of the CRC-32 cyclical redundancy check algorithm using known answer test.	N/A	N/A	Unauthenticated	N/A	The successful completion of a service is an implicit indicator for the use of an approved service
Personality Load	Personality Load service is to download personalities. Personality load instructions, when successful, result in updating the	AES-CCM, AES-CBC, RSA SigVer, ECDSA SigVer, CKG,	IMFK, PSK, PECSK, PDEK, IDFK, FFK, DRBG Seed, DRBG Key, DRBG V, Entropy input string	Crypto Officer	E, E, E, E, EZ, GWE, GWE, GWE, GWE, GWE	The successful completion of a service is an implicit indicator for the use

	flash memory. This service is authenticated as described below.	Counter DRBG, KTS				of an approved service
Zeroize	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. Note, this corresponds to the “Perform	N/A	ALL	Unauthenticated	Z	The successful completion of a service is an implicit indicator for the use of an approved service

	zeroization" mandatory service.					
Start Personality "go"	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	AES-CCM, AES-CBC, RSA SigVer, KTS	IMFK, GSK, PSK, PECSK, FFK	User	E, E, E, E, E	The successful completion of a service is an implicit indicator for the use of an approved service

	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 be 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.					

Table 9 Approved Services

Note: The services that correspond to the “Perform self-tests” mandatory service include RSA Signature Test, ECDSA Signature Test, SHA Test, AES Test, RBG Test, DRBG Test, Entropy Test, CCM Test, and CRC Test. The self-tests can also be invoked on-demand by power cycling the module.

Note: All services that specify an approved security function correspond to the “Perform approved security functions” mandatory service.

The module does not support any Non-Approved services.

5. Software/Firmware Security

The integrity of the module's executable firmware is verified using CRC-32 (EDC), a 64-bit EDC, and approved integrity techniques for the following firmware components:

- CRC-32 - Loader Stage 1, Loader Stage 2, and Boot
- 64-bit EDC – PSMCU, CMS-OCT, CMS-NTX
- RSA SigVer (FIPS 186-4) (Cert. #A2606) using 4096-bit modulus with PKCS #1.5 padding and SHA2-512, ECDSA SigVer (FIPS 186-4) (Cert. #A2606) using P-521 and SHA2-512 – Loader

The firmware integrity tests can be invoked on-demand by power-cycling the module. The required CASTs are executed for the RSA and ECDSA approved integrity techniques prior to the execution of the firmware integrity test. Please refer to Section 2.10 of this document for more information.

6. Operational Environment

Not Applicable. The module has a limited operational environment and is validated with Physical Security Level 3.

7. Physical Security

The embodiment of the ACS is of a multi-chip embedded module.

The Physical Security and Security Control Unit (PSMCU) within the ACS continually monitors the physical security of the module for attempts to physically penetrate the cryptographic boundary.

Depending on states of (PSMCU) two major events are generated within the secured boundary of the module.

1. A "reset event" is one that forces the module 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 module to become permanently disabled. This is a catastrophic event. In the disabled state all critical security parameters are erased and the module can only provide status information to users. Any physical penetration results in a "tamper event". This event causes active zeroization of all cleartext CSPs.

The following table specifies the required actions required by the operator to ensure the physical security of the ACS is maintained.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details

Tamper Response	This is constantly maintained by the module	Tamper response will automatically occur if a tamper event is detected. No actions necessary.
Zeroization	This is constantly maintained by the module	Zeroization will occur after any tamper event. A user can choose to invoke this service by physical removal of the batteries.
Alarm	These automatically occur following a tamper attempt, or failure of critical function or self-tests	Alarm state will be entered automatically, and the unit will become non-operational

Table 10 Physical Security Inspection Guidelines

In addition to physical penetration monitoring, the module supports Environment Failure Protection (EFP)[1] for the following parameters.

	Temperature or Voltage Measurement	Specify EFP or EFT	Specify if this condition results in a shutdown or zeroization
Low Temperature (reset)	+5℃	EFP	Shutdown
Low Temperature (tamper)	-20℃	EFP	Zeroization
High Temperature (reset)	+63℃	EFP	Shutdown
High Temperature (tamper)	+100℃	EFP	Zeroization
Low Voltage (on host power)	12V= <9.6V 3V= <2.5V	EFP	Shutdown
High Voltage-(on host power)	12V= >14.4V 3V= >4.13V	EFP	Shutdown
Low Voltage (NOT on host power)	Battery voltage = <8V	EFP	Zeroization

Table 11 EFP/EFT

The following table specifies the temperature range that the hardness of the module's enclosure was tested at.

	Hardness tested temperature measurement
Low Temperature	-20 ℃
High Temperature	+100 ℃

[1] For FIPS 140-3 validation the EFP/EFT functionality was tested in order to meet the Security Level 3 requirements.

Table 12 Hardness Testing Temperature Ranges

7.1 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.

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 module temperature is outside of the normal operating range while operating on external power.
- Thermal out of limits 2 – the module temperature is outside operational limits of components while operating on battery power only.
- Card removal detection event – the ACS is removed from the host. This event is not catastrophic but rather warning event. The module is up and running but not functioning (in suspend mode) and requires the “resume” command from the authorized personnel, which will reset the flag.

8. Non-invasive Security

This section is not applicable due to no requirements currently being defined in SP 800-140F.

9. Sensitive Security Parameters Management

The following table specifies the SSPs utilized by the module. The module supports the zeroization of all SSPs.

Key/SSP Name /Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & related keys
IMFK (CSP)	256 bits	AES-CCM Cert #A2606	CKG (Vendor Affirmed)	N/A	N/A	PSMCU, plaintext	Zeroized actively by tamper event, and passively by battery failure	Encrypting and decrypting all other CSPs
PDEK (CSP)	256 bits	AES-CCM Cert. #A2606; KTS (AES-CCM Cert. #A2606)	Factory pre-loading of a key	N/A	N/A	Flash ROM, encrypted	Zeroized when the IMFK is zeroized	Performs encryption and decryption of the CCM envelope
IDFK (CSP)	256 bits	AES-CBC Cert #AES 4600	External	Input encrypted and authenticated by the PDEK using AES-CCM	KTS (AES-CCM Cert. #A2606)	SDRAM, plaintext	Zeroized after image download is complete or	Used in CBC mode to decrypt the downloaded personality application

							interrupted	
FFK (CSP)	256 bits	AES-CBC Cert #AES 4600	CKG (Vendor Affirmed)	N/A	N/A	Flash ROM, encrypted	Zeroized when the IMFK is zeroized	Used in CBC mode to decrypt the personality
Entropy Input String (CSP)	501 bits	Counter DRBG Cert. #A2606; CKG (Vendor Affirmed	ENT (P)	N/A	N/A	Volatile Memory, plaintext	Zeroized with any loss of power	Entropy
DRBG Seed (CSP)	1002 bits	Counter DRBG Cert. #A2606; CKG (Vendor Affirmed)	ENT (P)	N/A	N/A	Volatile Memory, plaintext	Zeroized with any loss of power	Entropy Input, 512-bit; Nonce, 256-bit; Personalization String, 256-bit
DRBG Key (CSP)	256 bits	Counter DRBG Cert. #A2606; CKG (Vendor Affirmed)	Generated per SP 800-90Arev1	N/A	N/A	Volatile Memory, plaintext	Zeroized actively by tamper event, passively by battery failure, or by any power failure	DRBG Internal State
DRBG V (CSP)	128 bits	Counter DRBG Cert. #A2606;	Generated per SP 800-90Arev1	N/A	N/A	Volatile Memory, plaintext	Zeroized actively by tamper event,	DRBG Internal State

		CKG (Vendor Affirmed)					passively by battery failure, or by any power failure	
GSK (PSP)	112 bits	RSA SigVer Cert. #A2606	Factory pre-loading of a key	N/A	KTS (AES-CCM Cert. #A2606) as part of Loader image.	Stored Encrypted by the IMFK	Zeroized when the IMFK is zeroized	Signature verification public key for Go Command
PSK (PSP)	152 bits	RSA SigVer Cert. #A2606	Factory pre-loading of a key	N/A	N/A	Stored Encrypted by the IMFK	Zeroized when the IMFK is zeroized	Used for image validation for the personality application. Note, this is not an SSP.
PECSK (PSP)	256 bits	ECDSA SigVer Cert. #A2606	Factory pre-loading of a key	N/A	N/A	Stored Encrypted under the IMFK	Zeroized when the IMFK is zeroized	Used for image validation for the personality application. Note, this is not an SSP.

Table 13 SSPs

The following table specifies the module's only entropy source, which is internal to the module's cryptographic boundary.

Entropy Sources	Minimum Number of Bits of Entropy	Details
SP800-90B Entropy Source	1002-bits	The DRBG requests 512-bits of entropy input, 256-bits of nonce data, and a 256-bit personalization string from the entropy source. The entropy source provides 7.834 bits of entropy per byte of output from the vetted Conditioning Component Block Cipher Derivation Function SP 800-90B (A2606). Therefore the DRBG is seeded with at least 1002 bits of entropy before generating keys.

Table 14 Non-Deterministic Random Number Generation Specification

10.Self-Tests

The following self-tests are performed automatically by the module without requiring operator intervention.

1. **Pre-operational self-tests**
    a. Pre-operational software/firmware integrity test:
        i. Firmware Integrity Test: The integrity of the Loader is verified at startup by checking a 4096-bit RSA signature and ECDSA P-521 signature.Stage 1, Stage 2, and Boot are verified by CRC-32. PSMCU, CMS-OCT, and CMS-NTX are verified by a 64-bit EDC. All must be verified successfully to continue
    b. Pre-operational critical functions test:
        i. Memory: Done during DDR RAM initialization
        ii. 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.

2. **Conditional self-tests**
    a. Conditional cryptographic algorithm test
        i. SHA2-512 hash - Known answer test
        ii. AES-ECB 256-bit Encrypt – Known answer test (ECB is only used for self-tests)
        iii. AES-ECB 256-bit Decrypt – Known answer test (ECB is only used for self-tests)
        iv. AES-CBC 256-bit Encrypt – Known answer test
        v. AES-CBC 256-bit Decrypt – Known answer test
        vi. RSA SigVer (FIPS 186-4) 4096-bit modulus with SHA2-512 - Known answer test
        vii. ECDSA SigVer (FIPS 186-4) P-521 with SHA2-512 - Known answer test
        viii. SP800-90Arev1 Counter DRBG (instantiate/generate/reseed) – Known answer test
        ix. SP800-90B ENT (P) Self-Test- 4096 entropy samples generated with continuous health-tests (APT and RCT) enabled.
        x. AES -CCM 256-bit Encrypt – Known Answer Test
        xi. AES -CCM 256-bit Decrypt – Known Answer Test
        xii. Continuous SP800-90B ENT (P) Health Tests (APT and RCT).
        xiii. Continuous SP800-90Arev1 DRBG periodic self-tests (Instantiate/Generate/Reseed).

    b. Conditional software/firmware load test:
        i. 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.

c. Conditional critical functions test:
    i. “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. When an error state occurs, cryptographic operations (like “go”, personality load, etc.) are disabled until the error state has been rectified.

Since the module is only powered-on for short periods of time (30-60 seconds to start a personality, 3-4 minutes to update flash) self-tests are periodically performed by nature of the design (i.e. power-on self-tests, conditional self-tests, and signature tests on every start of the card). The only time the loader remains active for more than a couple minutes is if the ACS card has tampered or entered test state, in which case it is prevented from doing any cryptographic or security-related operations, permanently, so there is no need for periodic self-tests, in this case.

In addition to the automatic self-tests, the module supports cryptographic algorithm self-test services (<algorithm> Test). These services allow the user to request on-demand invocation of any specific test. Additionally, the user can invoke all of the self-tests on demand by power-cycling the module.

11. Life-cycle Assurance

The module is always in an Approved mode of operation until a personality is loaded and started, at which point the module enters a non-compliant state. The ACS loads and generates its initial keys randomly in manufacturing in the factory, during the process of entering into secure state. Once secure state has been entered, the physical security monitoring of external penetration, and voltage/thermal operating conditions are continuously maintained by the PSMCU, which is battery and system powered. The monitoring is maintained for the entire ACS life cycle. During normal operational use of the cryptographic operations, any failed startup test or self-test will enter a state that does not allow any cryptographic operations to be completed without cycling the power to the ACS. If an event is detected that results in the ACS security boundary being compromised, all keys are erased immediately and the ACS enters Tampered State, which renders the device cryptographic operations unusable, ending the ACS life cycle. There is no means to recover from this state, without irreversible damage.

HSM lifecycle is documented and located within the HSM security directory and available upon request.

12. Mitigation of Other Attacks

The module does not implement any additional attack mitigation techniques.