Atalla HSM AT1000

PCI HSM 3.0 Security Policy

August 5, 2019

Table of Contents

1 Introduction

The Utimaco Atalla Hardware Security Module (HSM) **AT1000** is a **NextGen payments HSM** designed to protect customer sensitive data, perform cardholder authentication, and manage the cryptographic keys used in ecommerce retail payment transactions in a **controlled or uncontrolled environment**.

Atalla AT1000 provides superior hardware security to deliver maximum privacy, integrity and performance for host applications. It supports cryptographic operations to perform PIN translation and verification, card verification, card production and personalization, electronic funds interchange (EFTPOS, ATM), cash-card reloading, EMV transaction processing, and key generation and injection.

This document specifies the AT1000 security policy as per PCI HSM Version 3.0, including the services offered by the Atalla Cryptographic Subsystem (ACS), the roles supported, and all keys and CSPs employed by the ACS.

The AT1000 is based on the FIPS 140-2 level 3 validated Atalla Cryptographic Subsystem (ACS) (Certificate #3059).

1.1 Product Identification

Atalla AT1000 can be identified as follows:

Name	Identification
Model	AT1000
Hardware P/N	HW-AT-HSM-V1
Firmware Version	8.22

1.2 Glossary

Term	Definition
ACS	Atalla Cryptographic Subsystem
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

Term	Definition
	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
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

Term	Definition
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 AT1000 provides a complete security solution consisting of the FIPS-validated Atalla Cryptographic Subsystem (ACS), financial firmware image and the customized HPE Proliant DL360 Gen9 server. Specifically, it consists of a secure hardware platform, a firmware secure Loader, the PSMCU firmware, the Personality software, and the customized server. The purpose of the Loader is to load Approved application programs, called "Personalities," in a secure manner. The PSMCU firmware continually monitors the physical security of the ACS. The Personality allows the execution of the financial image commands. The server restricts access to the HSM via the front interfaces by adopting a front bezel installed with two-pick resistant locks and locking top cover. No security-relevant code runs in the server. The AT1000 requires the PCI HSM Personality to be loaded in order to operate in PCI HSM mode.

The major components of the AT1000 are:

- Atalla Cryptographic Subsystem (ACS) consisting of the Loader, PSMCU, and Personality, and providing tamper detection, tamper resistance, and automatic zeroization of Critical Security Parameters
- 1U server based on the HPE Proliant DL360 Gen9 and includes dual hard disk drives, dual power load balancing supplies, dual locking front bezel, and redundant cooling
- USB port located behind the bezel for transferring configuration files
- USB flash memory device for storing the image files, configuration information, and system logs
- Front panel display with keypad – provides status information; the keypad is protected behind the dual locking bezel and can be used to assign NIC network settings and transfer configuration files from USB
- Four Ethernet Network Interface Connectors (NICs)

The AT1000 system image and default configuration file must be copied to the USB flash memory device and inserted into the USB port located behind the bezel.

The AT1000 is initialized, configured, and managed using the Secure Configuration Assistant-3 (SCA-3). A smartcard needs to be inserted into the SCA-3 to authenticate to the HSM. The SCA-3 and its smartcards are not part of this validation effort.

The AT1000 is a security co-processor for host applications. The Figure below shows the connectivity to the AT1000 in a typical host system environment.
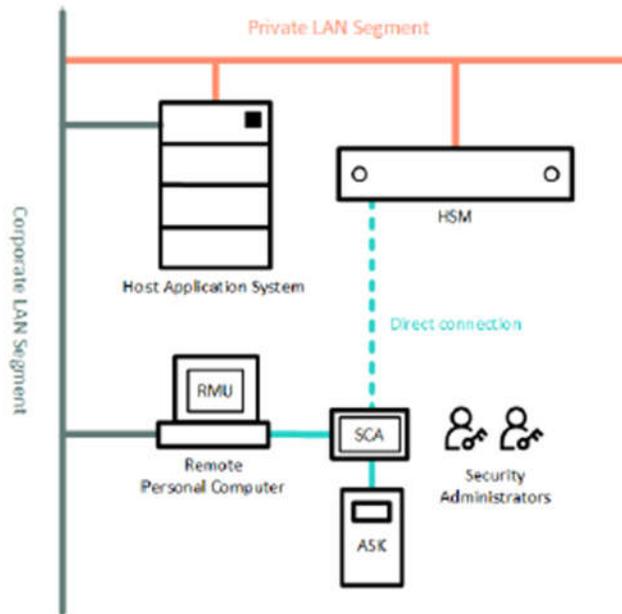
Figure 1 Typical Host System Environment

In the above Figure, the host system uses a command-response format to communicate with the HSM:

<CMDID#FIELD1#FIELD2…#FIELDN#^CONTEXT Tag#>

A command begins with a start-of-command bracket ("<") and ends with the end-of-command bracket (">"). The pound sign ("#") is used to delimit fields within the command. The context tag is optional. If present in the command, the context tag is returned as part of the response. The caret character ("^") is an ASCII 0x5E.

The HSM will process the command and return a response. If an error is encountered, an error response will be returned. The response format is:

<RESPID#FIELD1#FIELD2…#FIELDN#^CONTEXT Tag#> [CRLF]

By default, a carriage return (CR) and line feed (LF) are appended to the response.

The commands are designed for use in financial environments, such as Automated Teller Machine (ATM), Electronic Fund Transfer (EFT), and Point of Sale (POS) networks.

2.2 Physical Security

Depending on the states of the PSMCU, two major events are generated within the secured area:

1. A "reset event" is one that forces the AT1000 to become temporarily inoperable. This is a non-catastrophic event. When the conditions that cause the "reset event" are removed the unit will operate normally.
2. A "tamper event" is one that forces the AT1000 to become permanently disabled. This is a catastrophic event. In the disabled state, all critical security parameters are erased and the AT1000 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 supports Environment Failure Protection (EFP) and 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.

The tamper detection and active zeroization mechanisms described above are provided by the ACS. It cannot be removed without having access to the top cover retention screw located behind the front bezel. The bezel is protected by two pick-resistant locks.

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 supported events and resulting states are summarized below.

- 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 functioning (in suspend mode) and requires the "resume" command from the authorized personnel, which will reset the flag.

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

Table 2 Events and States mapping

2.2.1 AT1000 Memory

There are six types of memory within the AT1000:

1. Dynamic Random Access Memory (DRAM). DDR4 SDRAM is used to hold the Loader and Personality and their 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.
3. Security Control Unit. The security control unit has non-volatile memory for storing cleartext CSPs. This memory is the first target of zeroization if a "tamper event" occurs.
4. Non-volatile RAM (SRAM). This battery-backed-up static RAM is not used by the Loader. The Personality uses this memory to store the encrypted MFK/PMFK keys and encrypted configuration data. No sensitive CSPs are stored as cleartext in the memory.
5. Volatile RAM (SRAM). This static RAM is not used by the Loader. The Personality uses this memory to store the cleartext MFK/PMFK keys during operation. It is immediately zeroized if a "tamper event" occurs or power is removed.
6. Flash memory. The USB flash memory device is inserted behind the bezel of the server and used to store the image files, configuration file, and system logs.

2.3 Ports and Interfaces

2.3.1 External Ports

The front panel of the AT1000 is protected by a customized bezel that is protected by two pick-resistant locks.
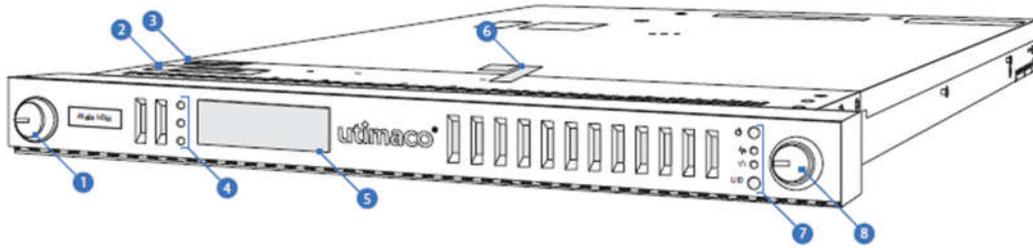
Figure 2 HSM Front View

The components on the front bezel of the HSM are defined below.
- Security locks (items 1 and 8) – the two locks are keyed differently from each other and from other HSMs
- Model and serial number label (item 2)
- Spare label (item 3) – contains part number of the HSM required for ordering a replacement
- Security LEDs (item 4) – will be green when HSM is powered on and operating normally, and red when the HSM detects a tamper condition
- Front panel display (item 5) – provides information about the HSM and a configuration menu used to configure certain HSM settings; the keypad is only available when the front bezel is open and is required in order to navigate the system information displays.
- Tamper evident label (item 6) – purpose of the label is to provide evidence that the top cover has been removed
- System Status LEDs (item 7) – four system LEDs located on the right side of the front bezel
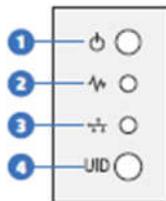
Figure 3 System Status LEDs

Item	Description	Status
1	Power On/Standby button/System power LED	The power button can only be pressed when the front bezel door is open. Amber = Standby. System shutdown, but power still applied. Green = System on. Flashing green = Performing the power on sequence. Off = No AC power. Power cord not attached or power supply failure.
2	System Health LED	Green = Normal. Flashing amber = System degraded, or only one power supply is providing power. Flashing red = System critical. It is not in an operational state.
3	Network Interface Connector LED	Green = Link to network Flashing green = Network activity Off = No network activity

Item	Description	Status
4	Unit ID button/LED	Press the button to activate or deactivate the UID LED. An indicator light is located in the rear of the HSM. Blue = Activated Off = Deactivated

Table 3 System Status LED

The following additional components are available when the bezel door is open:
- Hard disk drives – no security relevant data items are stored on these drives.
- Front panel keypad – used to navigate the system information displays.
- ACS serial number
- Top cover retention screw
- Power button
- USB 3.0 port – to transfer configuration files

The diagram below shows the interfaces on the rear panel of the server.
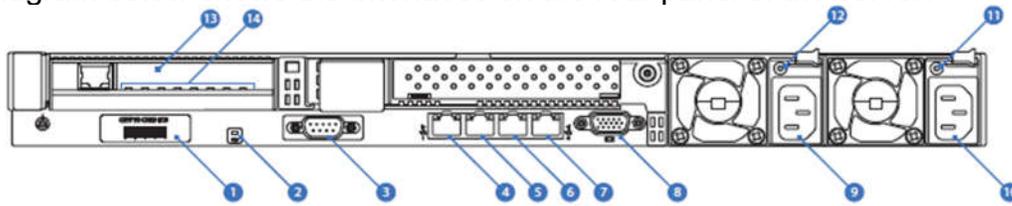
Figure 4 HSM Back View

The components on the back of the HSM are defined below.

- ACS Serial Number label (item 1)
- UID LED (item 2)
- Serial port (item 3) – for attaching the SCA-3; required to load cryptographic keys into the HSM and configure its security policy
- Network Interface Connectors (items 4, 5, 6, and 7) – four Network Interface Connectors (NICs). Each NIC has a link and activity LED, which are described below.

LED	Description	Status
LNK	Green – shows link integrity	Steady – good connection between the HSM and network Off – no connection between the HSM and network
ACT	Green – indicates port traffic for either speed.	Flashing – network traffic present Off – No traffic

Table 4 Link and Activity LED descriptions

- VGA port (item 8) – not supported interface
- Power supplies (items 9 and 10) – two hot swappable power supplies are provided. Each power has and LED. The LED provides status with a solid green indicating the normal state. When the LED is off, one or more of the following conditions exists:

- o AC power unavailable or disconnected
- o Power supply failed
- o Power supply in standby mode
- o Power supply exceeded current limit
- ACS Status LEDs (item 11) – these eight LEDs provide information on the ACS.

Item	Description	Status
0	Not Used.	Off Solid.
1	HSM Initialization State	Off Solid – Normal during the first 5 seconds after the HSM is powered on, or when the HSM is in the ready state (LED2 is in Heartbeat mode). On Solid – If this LED is on solid and not changing in brightness intensity, there is a problem with the HSM. Power cycle the HSM, if this error condition persists, the HSM must be replaced. Heartbeat – LED changes brightness intensity from bright to dim repeatedly, only during the HSM initialization state.
2	HSM Ready State	Off Solid – normal during the first 10 seconds after the HSM is powered on, or when the HSM is in the initialization state (LED1 is in Heartbeat mode). On Solid – if this LED is on solid and not changing in brightness intensity, there is a problem with the HSM. Power cycle the HSM, if this error condition persists, the HSM must be replaced. Heartbeat – LED changes brightness intensity from bright to dim repeatedly. This indicates a normal state.
3	System Error	Off Solid – this is the normal state. Flashing Red – the ACS encountered a fatal error. Power the HSM.
4	Command Ready	Off Solid – normal during the first 10 seconds after the HSM is powered on, or when the HSM is in the initialization state (LED1 is in Heartbeat mode). Once initialization is complete, it will be on solid. On Solid – the ACS is ready to accept commands. This is the normal state.
5	Image Update	Off Solid – this is the normal state. Heartbeat – LED changes brightness intensity from bright to dim repeatedly. This indicates a software image update is in progress. Flashing Green – the image update process has failed.
6	ACS Secure State	Off Solid – normal during the first 10 seconds after the HSM is powered on, or when the HSM is in the initialization state (LED1 is in Heartbeat mode). Once initialization is complete, it will either be on solid or flashing. On Solid – the ACS is in secure state. This is the normal state. Flashing Green – the ACS is in test mode. The HSM must be replaced. Flashing Red – the ACS has tampered. The HSM must be replaced.

Item	Description	Status
7	Security Controller	Solid Green – the HSM is enrolled in a security association. Slowly Blinking Green – the HSM is not enrolled in a security association.

Table 5 ACS Status LEDs

- ACS (item 12) – all cryptographic command processing is performed within its security boundary.

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

		Physical Ports					
		Ethernet Port	Serial Port	USB Port	LEDs	Front Panel Display	Front Panel Keypad
Logical Ports	Data Input	√	√	√			
	Data Output	√	√	√			
	Control Input	√	√	√			√
	Status Output	√	√	√	√	√	

Table 6 Logical to Physical Port Mappings

Refer to the AT1000 Installation and Operations Guide for additional information on all the interfaces available on the AT1000.

2.3.2 Power

The HSM has two hot swappable power supplies. For full power and load sharing, each of the two power supplies should be connected to a separate power source. The power supply specifications are shown below.

Specification	Value
Input requirements	
Rated input voltage	100 to 127 VAC 200 to 240 VAC
Rated input frequency	50 Hz to 60 Hz
Rated input current	4.8 A at 100 VAC 2.4 A at 200 VAC
Maximum rated input power	480 W at 100 VAC 480 W at 200 VAC
BTUs per hour	1638 at 100 VAC

	1638 at 200 VAC

Table 7 Power Supply Specifications

For the ACS, the 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

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 8 Power On/Off States

2.4 Supported Algorithms

The Loader includes these FIPS-Approved algorithms, implemented in firmware:
- 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 Personality includes the following approved and tested algorithms:
- AES (encrypt, decrypt; CBC mode; 128-, 192-, 256-bit keys)
- AES CMAC (generate; 128-, 192-, 256-bit keys)
- 3DES (encrypt, decrypt; ECB, CBC, 8-bit CFB, 64-bit CFB, and OFB)
- RSA (sign, verify, encrypt, decrypt; 2048-4096-bit key)
- NIST SP 800-90 CTR_DRBG
- SHA-256
- HMAC SHA-256

3 Self-Tests

There are several self-tests performed by the AT1000.

3.1 Power-Up Self-Tests

Loader
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.

Personality
1. Personality Integrity Test (includes Kernel): The integrity of the Personality is verified by the Loader during Personality Load and when issuing the Go command. In addition, during initialization two CRC-32 tests are performed to verify the Personality; these tests are also performed once-a-day and on-demand.
2. Known Answer Tests
    a. AES – CBC mode (encrypt, decrypt)
    b. AES – CMAC (generate only)
    c. 3DES – ECB, CBC, 8-bit CFB, 64-bit CFB, and OFB modes (encrypt, decrypt)
    d. RSA (encrypt and decrypt)
    e. RSA (signature generation and verification)
    f. SHA-256
    g. SP 800-90 DRBG
    h. HMAC SHA-256

3.2 Conditional Self-Tests

Loader
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-pci" command personality start validation: The "go-pci" 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.

Personality
1. Continuous RNG Test:
   a. Hardware RNG
   b. DRBG
2. RSA Pairwise Consistency Test

3.3 Periodic Self-Tests

The AT1000 performs self-tests once a day. The DIAGTEST_TIME parameter in the config.prm file needs to be set to a six digit value (HHMMSS). This value specifies the time when the once a day self-tests are performed.

3.4 On-Demand Self-Tests

The AT1000 allows self-tests to be performed on operator demand. These self-tests are identical to the power-up self-tests.

Loader
The following commands can be used to perform the on-demand self-tests:
1. Test_aes – tests the AES cryptographic engine
2. Test_ccm – tests the CCM mode of operation of the AES algorithm
3. Test_rng – tests the RNG using a fixed key, beginning context, and result
4. Test_sha – tests the SHA-256 cryptographic engine
5. Test_sig_rsa – tests the RSA 4096-bit modulus signature computation algorithm
6. Test_sig_ecdsa – tests the ECDSA P-512 curve signature computation algorithm

Note that these self-tests can only be performed when the Loader is running (i.e., prior to loading the Personality).

Personality
The Personality allows on-demand self-tests to be performed using the Diagtest command <9A#DIAGTEST#Algorithm#RSA Option#>

The "Algorithm" field identifies the type of test that will be performed:

0 – All on-demand self-tests
1 – 3DES KAT
2 – DRBG KAT
3 – RSA KAT
6 – SHA-2 KAT
7 – Personality and Kernel Integrity Test
8 – AES KAT
9 – HMAC SHA-256 KAT

The HSM also allows on-demand self-tests to be initiated by the SCA. The SCA Crypto Test instructs the HSM to perform all self-tests.

3.5 Self-Test Failures

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

Personality
Failure of any power-up, periodic, and on-demand self-tests results in an error state. In this state, all commands, except for the status commands 9A, 1101, 1110, 1120, and 1223, will return the error <00#080012#0717#>. Recovery from the error state requires power cycling.

Failure of the RSA pairwise consistency test results in a soft error. Only the affected command will be affected by the error. The AT1000 will create another RSA key pair if the test fails.

Failure of the continuous RNG test results in a soft error. The calling command and other commands that use the random number generator function will return error <00#080012#0716#>. Commands that do not use the random number generator are not affected by the error. Recovery from the error requires power cycling.

4 Rules

This section lists the security rules, under which the module shall operate.

Rule 1:
All functions requiring the use of sensitive data shall be performed within security area. This rule is enforced by the AT1000 physical design. All the critical circuits and components are within the secure area, which is continuously monitored to detect tampering.

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.

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 AT1000 does not support maintenance and bypass modes.

Rule 7:
Failure of self-tests result in the AT1000 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 Loader Services

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.

5.1.7 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 and are listed in the On-Demand Self-Test section.

5.1.8 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 5.2.

5.1.9 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.

5.1.10 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.

5.1.11 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. This service is authenticated as described in section 5.2.

5.2 Personality Services

These services can be split into three categories: HSM management/configuration, shareholder services, and banking commands. The first two categories are performed using the Atalla Secure Configuration Assistant (SCA) under dual-control. The banking commands are designed for use in financial environments and use the command-and-response format as described in Section 2.1.

5.2.1 HSM Management

Services include initializing and managing the HSM. These include the creation of a security association, management of key components, HSM Command and Option configuration, audit log management, and updating the firmware. Refer to the SCA User Guide for the complete list of available services.

5.2.2 Shareholder services

Services include the creation of and initialization from shareholder smartcards. Refer to the SCA User Guide for the complete list of Shareholder services.

5.2.3 Banking Commands

The AT1000 supports a number of commands that are available to the Personality User. Standard commands and options are available by default and, if required, can be disabled using the SCA. Premium Value commands and options are disabled by default and need to be purchased prior to enabling them. Utility commands are enabled by default and cannot be disabled. These are status commands and are not security-relevant. Refer to the HSM Atalla Key Block Banking Command Reference Manual for the complete list of available banking commands.

6 Roles

6.1 Loader Crypto Officer

The Loader Crypto Officer (LCO) is responsible of the overall security of the Loader Platform. In particular, only an operator in the Loader Crypto-Officer role can load a Personality into the AT1000.

The Loader Crypto-Officer is required to be properly authenticated. The authentication mechanism is controlled by the PSK (private key) and PECSK (private key), which are used to sign Personality images. The LCO uses the PSK and PECSK to create signed

Personality images for download to the unit, 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, and the LSK and LECSK to create signed Loader images.

The LCO authenticates using the PSK and PECSK.

6.2 Loader User

The Loader User can perform a limited number of the services available on the AT1000.

The Loader User is required to be properly authenticated. The authentication mechanism is controlled by the GSK (private key), which is used to sign the 'go-pci' command. The Loader User uses the GSK (private key) to sign the 'go-pci' command which allows the Loader to exit and start the Personality.

The Loader User authenticates using the GSK.

6.3   Personality Security Administrator

The Personality Security Administrator configures and manages the HSM. Configuration changes are only allowed under dual control.

The Personality Security Administrator is authenticated by the 256-bit AES Smartcard Identity key.

6.4 Personality Shareholder

Limited services are available to the Personality Shareholder. The main purpose of this role is to bring up a clone of a second HSM under dual control.

The Personality Shareholder is authenticated by the 2048-bit Smartcard Identity key. This key has a certificate signed by the Atalla Root Authentication Key.

6.5 Personality User

The Personality User can perform the banking commands and options specified in the HSM Atalla Key Block Banking Command Reference Manual. The type of commands and options that are available depends on the Security Policy defined by the Security Administrator.

6.6 Roles vs. Services Matrix

Acronyms: A – available, √ – unauthenticated command.

Commands / Services   **Roles**

Commands / Services	CO	User	None	Personality Security Administrator	Personality Shareholder	Personality User
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				
Loader Zeroize			√			
Firmware Load	A					
HSM Management				A		
Shareholder Services					A	
Banking Commands						A

Table 9 Roles vs. Services Matrix

7 CSPs

7.1 Platform Keys

Key Name	Type and Size	Description
Loader Keys		
IMFK	AES, 256-bit	Encrypts all Loader keys
PIMFK	AES, 256-bit	Encrypts MFK/PMFK, Device Identity Public Keys
HSMAK	AES, 256-bit	Encrypts all Personality keys stored in Flash
PDEK	AES, 256-bit	Decrypts CCM envelope of image download
IDFK, IDFK_IV	AES, 256-bit	Decrypts download image
FFK, FFK_IV	AES, 256-bit	Decrypts Personality stored in flash
DRBG Seed	Entropy Input, 1024-bit; Nonce, 256-bit; Personalization String, 256-bit	DRBG Seed

DRBG Key	AES, 256-bit	DRBG Key
DRBG V	DRBG Internal State value, 128-bit	DRBG V – part of SP 800-90A DRBG Internal State
GSK	RSA, 2048-bit	Loader user authentication key; verifies "go-pci" command signature
LSK	RSA, 4096-bit	Verifies Loader download signature
LECSK	ECDSA, P-521	Verifies Loader download signature
PSK	RSA, 4096-bit	Loader Crypto-Officer authentication key; verifies image download signature
PECSK	ECDSA, P-521	Loader Crypto-Officer authentication key; verifies image download signature
Personality Keys		
Atalla Root Authentication Public Key	RSA, 2048-bit	Signing device identity certificate
Device Identity Public Key	RSA, 2048-bit	Used to establish a secure session between the HSM and the smartcard
Device Identity Private Key	RSA, 2048-bit	Used to establish a secure session between the HSM and the smartcard
Smartcard Identity Public Keys	RSA, 2048-bit	Authenticates the Personality Shareholder
AES Smartcard Identity Keys	AES, 256-bit	Authenticates the Security Administrators
Association Keys	AES, 256-bit	Derive authentication key to authenticate Security Administrators
Secure Channel Session Key (encrypt)	AES, 256-bit	Protects the communication between the smartcard and HSM
Secure Channel Session Key (MAC)	AES CMAC, 256-bit	Protects the communication between the smartcard and HSM
AES Master File Keys (AMK)	AES, 256-bit	Encrypts user keys for local storage
Pending AES Master File Keys (PAMK)	AES, 256-bit	Encrypts user keys for local storage (used in AMK key update process)
Master File Keys (MFK)	3DES, 112-, 168-bit	Encrypts user keys for local storage
Pending Master File Keys (PMFK)	3DES, 112-, 168-bit	Encrypts user keys for local storage (used in MFK key update process)
User Key Encryption Key (KEK)	AES, 128-, 192-, 256-bit, or 3DES, 112-, 168-bit	Encrypts Working keys
User Keys	AES, 128-, 192-, 256-bit, or 3DES, 112-, 168-bit	Used to encrypt PIN blocks and other types of data, calculate MACs, derive keys, etc.
DRBG Key	AES, 256-bit	Key used by Personality to run NIST SP 800-90A DRBG
DRBG Seed	Entropy Input, 1024-bit; Nonce, 256-bit;	DRBG Seed

	Personalization String, 256-bit	
DRBG V	DRBG Internal State value, 128-bit	DRBG V – part of SP 800-90A DRBG Internal State

Table 10 Platform Keys

7.2 Key Management Techniques

The HSM is PCI approved to use the key management techniques listed in this Section. The following techniques are supported:

- ANS X9.24 parts 1 and 2
- Derived Unique Key Per Transaction (DUKPT)
- Master-Session
- ANS TR-31
- ANS TR-34
- EMV key derivation techniques – master key derivation and session key techniques that include tree-based derivation, common session (SU-46), and American Express
- AS 2805
- Country and/or issuer-specific session key derivation algorithms
- NIST SP 800-108

7.3 Key Storage

Internal (key tables) and external (application/host database) keys are stored encrypted and MACed in accordance with ANS x9.24 part 1. All internal keys are stored encrypted in fixed position with error detection. The root keys cannot be explicitly accessed, modified, or exported and are subject to zeroization during a tamper event. These protection mechanisms protect keys against unauthorized disclosure and substitution and ensure key separation.

The Personality Security Administrators and Shareholders are advised to securely store the smartcards required for authenticating to the AT1000.

7.4 PIN Management

The AT1000 meets the PIN requirements specified in PCI HSM requirement C1 by enabling Option 46.

Enabling Option 46 limits all standard Atalla PIN translation commands to either ISO-0 or ISO-3 PIN blocks (input and output) and prevents any change of the PAN.

Refer to the HSM Atalla Key Block Banking Command Reference Manual for additional guidance.

8 Secure Operation

The AT1000 manuals provide guidance on how to securely setup, configure, and operate the AT1000.

8.1 Initial Setup

The device should be unpacked and inspected according to the AT1000 Installation and Operations Guide. Customers are required to inspect the shipping container, compare the packing list with the purchase order, examine the content, and inspect each item (including damaged tamper labels). If damage is evident, notify Technical Support immediately. Refer to the Installation and Operations Guide for the Atalla AT1000 for installation and configuration instructions, maintenance information, safety tips, and other information.

8.2 PCI HSM Mode

The PCI HSM Personality must be loaded for the HSM to operate in PCI HSM mode. During the initial setup, the AT1000 system image file and config.prm file must be copied to the Utimaco provided USB flash memory device that ships with the AT1000. The config.prm file defines the startup, TCP/IP, and log parameters, and is accessed during the AT1000 power on sequence. These parameters must be modified.

Operating in PCI HSM mode does not start until two Security Administrators generate or load a PCI HSM Security Association – a dual control operation.

8.3 Key Loading

System initialization consists of loading cryptographic keys, such as the Master File Key (MFK), and defining the security policy. The number of MFK components are specified during the initialization steps using the SCA and Atalla smart cards. Only one key component per Security Administrator smart card will be accepted by the HSM. All key loading is performed under dual control using split keys. Refer to the Atalla Secure Configuration Assistant-3 for additional information on key loading.

8.4 Periodic Self-Tests Configuration

One of the parameters that need to be added to the STARTUP settings in config.prm is DIAGTEST_TIME to setup the required periodic self-tests. To set this parameter, DIAGTEST_TIME needs to be set to the value HHMMSS, where:

HH = hour (valid values are 00 through 23)
MM = minute (valid values are 00 through 59)
SS = second (valid values are 00 through 59)

The HSM's system clock is set to Coordinated Universal Time (UTC) and cannot be changed to a local time. The default value is 000000 (midnight UTC time).

Refer to the AT1000 Installation and Operations Guide for additional information and guidance on the config.prm file.

8.5 Version

The AT1000 model number is located in the lower right corner of the front panel. The AT1000 Hardware Part Number is displayed on the top cover right above the caution label. It is also displayed on the packaging of the server.

Once the Personality is running, the software version and PCI mode can be verified by using commands 1101 or 1110, as shown in the examples below:

Command:
<1101#>
Response:
<2101#Atalla HSM AT1000-AKB PCI-HSM Version: 8.22, Date: Apr 4 2019, Time: 21:33:03#E2EC#3#>

Command:
<1110#>
Response:
<2100#Atalla HSM AT1000-AKB PCI-HSM Version: 8.22.0.0, Date: Apr 4 2019, Time: 21:33:03#>

8.6 Log

Security administrators are advised to frequently review the logs. The AT1000 maintains four different types of logs.

For the Loader, events are logged to an EEPROM device. These events can only be viewed when the Loader is running (i.e., prior to loading the Personality). The getstatus command can be used to display the events. The Loader EEPROM log cannot be modified or deleted.

For the Personality, all AT1000 events are logged in the system log in NVRAM and copied to the USB flash memory device. They are optionally output to the serial port and/or status port. The USB flash memory device is located behind the front bezel and is protected by two pick-resistant locks. The system log cannot be erased without removing the USB drive from the unit. The command <9A#CLEAR_LOG#> closes the current system log on the USB drive, clears the system log that is stored in NVRAM, and then uses the current date and time to create a new system log on the USB flash memory device. The command will not erase the old system log files from the USB device. When removing the USB drive for archiving purposes, the USB drive shall be replaced with another USB drive to avoid potentially losing system log events. To ensure that self-test events are being logged in the system log, the FILE_LEVEL must be set to 4.

All dual-control operations are stored in the internal security audit log. The security audit log data is stored in flash memory, which is not physically accessible without tampering the device. All dual-control operations are stored in the internal security audit log. The security audit log can be viewed and managed by the SCA or viewed remotely if the AT1000 is configured appropriately. The security audit log can only be cleared using dual-control authentication.

The AT1000 maintains a fourth PCI HSM log file (signed.log) that keeps records of key management, modification of authentication data, software/firmware updates, and

enabling and disabling HSM security functions. Most of these records are also available in the security audit and system log. The signed.log file consists of entries that are individually signed. The log signing public key can be retrieved from the HSM using command 1204 and the log entries can be verified using command 1205.

Refer to the AT1000 manuals for additional information on the supported logging mechanisms.

8.7 Commands and Options

A couple of mechanisms exist to determine the list of enabled and disabled commands and options. The Personality Security Administrator can use the SCA to view the list of enabled and disabled commands by going to HSM Management and clicking on HSM Configuration Management. The HSM Command Configuration screen contains a list of disabled commands on the left and a list of enabled commands on the right. Similarly, the HSM Option Configuration screen contains a list of disabled options on the left and a list of enabled options on the right.

The Personality User can view the list of enabled commands and options by sending command <9A#CONFIG-ON#> and the list of disabled commands and options by sending <9A#CONFIG-OFF#>.

When operating in PCI mode, the following options must not be enabled: 4A, 6C, and 8CWhen operating in PCI mode, the following options should be enabled: 42, 46, 48, 49, 4B, 4C, and 4E

All other commands and options do not impact the PCI compliance.

8.8 Key Replacement

Keys should be replaced with new keys whenever compromise is suspected, or when the time deemed feasible to discover the keys through exhaustive attack elapses (as per NIST SP 800-57 Part 1).

8.9 Secure Decommissioning

To securely decommission the HSM, perform the following steps:

1. Reset the HSM to factory state by issuing commands 1227 and 1228. These commands operate as a pair and will erase the user-defined security policy and all CSPs.
2. Remove the ACS card followed by the batteries and arrange for a secure disposal service to permanently destroy the HSM.