Document Number: 429743-001 Rev E

Atalla Cryptographic Engine
Security Policy

Revision Date: 31 January 2003

Table of Contents

1. Version History

First public version, 25 June 2002

- Included part numbers for ACE hardware and Loader software in section 3; changed 3DES to TDES, 02 August 2002.
- Clarified use of Atalla Cryptographic Engine (ACE) terminology, 13 August 2002.
- Clarified unauthenticated services, included latest picture, 5 September 2002.
- Miscellaneous clarifications including part number designations, 2 December 2002.
- Miscellaneous clarifications including service matrix, 31 January 2003.

2. References

FIPS 140-1 Security Requirements for Security Modules

FIPS 140-2 Required Vendor Documentation

ANSI X9.31 Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry

3. Introduction

The security level of a system can be evaluated by understanding the policies and procedures of the organization administrating the system. This evaluation must also include an analysis of the hardware and software components used in the system.

The Atalla Cryptographic Engine (ACE) PCI Platform is a single component in a system. ACE contains hardware and software elements. ACE hardware that processes sensitive data or contains software code is contained within a secure, tamper protected envelope.

Software elements of ACE (which are part of larger software family name Humboldt) include Loader Software and application (personality) software. The Loader Software is used every time ACE is reset. The Loader Software controls the loading of a specific personality. Once a personality has been loaded into ACE the Loader Software can start the personality. While executing, the personality can elect to use Loader Software functions.

ACE is a multiple-chip embedded cryptographic module.

3.1 Purpose

The ACE has been designed to load software applications called Personalities. Personalities will be evaluated separately, and are not included in the current definition of the cryptographic boundary. The ACE provides a very limited set of services, as its main purpose is to load trusted software. The integrity of the loaded software is verified during the Personality load process, and relies on strong cryptography.

A FIPS approved personality is an application that has been separately validated to FIPS 140-2. It is important to note that it is not sufficient to simply load a “trusted” Personality onto the ACE; each Personality must be separately evaluated based on a specific, controlled, set of interfaces with the ACE module.

> A non-FIPS approved personality is one that has not been validated to FIPS 140-2. It is important to note that loading this type of software onto the ACE invalidates the ACE FIPS 140-2 cert.

Once a specific Personality is loaded, it is not possible to switch between FIPS and non-FIPS modes without reloading a new Personality image.

The purpose of this document is to describe the rules that shall be enforced by the ACE hardware (429728-006 Rev H) and Loader Software (523044-004 Rev D.) These components together comprise the ACE product (524103-004 Rev F.) The rules that are enforced by individual personalities are not described in this document but these personality rules should be consistent with those described here.

This document, along with hardware and software design documents, can be used to evaluate the security level of a system using the ACE PCI platform.

It is expected that the evaluation process can take place in two stages. First, ACE and the Loader Software are evaluated. Second, an individual personality is evaluated with the knowledge that the personality will have been loaded and verified by the Loader Software.

3.2 System Overview

ACE is a co-processor for a host system. Communication between the host and ACE is over a PCI bus.

The PCI bus is the ONLY external interface to the co-processor.

Instructions (commands) are sent from the host to ACE; results (responses) are returned to the host from ACE. The PCI bus and host are outside the ACE secure envelope and therefore any sensitive data that appears on the PCI bus or within host memory (after ACE has been initialized) shall be cryptographically protected.

ACE contains a combination of random access memories. This includes non-volatile battery backed up memory, volatile memory, and non-volatile flash memory. All of the memory elements are in the secure envelope. The battery backed up memory is in a single integrated circuit that includes the ACE microprocessor and cryptographic engines.

The physical integrity of the secure envelope is automatically maintained. This secure envelope is the contiguous cryptographic boundary. It is defined as the outer metal enclosure that is secured to the Motherboard printed wiring assembly (PWA.) Inside this secure boundary resides all security relevant hardware and firmware directly related to cryptographic processes.

Rule 1:

All functions requiring the use of sensitive data shall be performed within the secure envelope of ACE.

ACE maintains the secure envelope boundary. This maintenance function includes the ability to detect tampering.

This rule is enforced by the ACE physical design. All critical circuits and components are within the secure envelope. The envelope is continuously monitored to detect tampering. See EVENTS section of this document.

Rule 2:

ACE shall actively zeroize sensitive data upon tamper detection.

Zeroization, when controlled by software, is the process of writing zeroes, ones, and then zeroes to memory elements. This effectively erases the previous content. 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 . See EVENTS section of this document.

There is no special operator action to ensure that the protection mechanisms are still in place. The process of zeroizing the CSPs also zeroizes the main program content. This will cause ACE to become non-operational. An operator will observe this when there is no response to any commands.

3.3 Ownership

Atalla Security Products are typically “owned” by an institution such as a bank or computer service provider. This ownership applies to the cryptographic keys required by host applications that are protected by the product.

Other cryptographic keys are only used for protecting the secure envelope and are "owned" by Atalla.

Instructions (commands) for ACE that contain sensitive data, require this data be cryptographically protected. The user who provides instructions must be a Crypto Officer (or a host program or user acting for a Crypto Officer) who has possession of the cryptographically protected data. The generation of this data is assumed to have been done in a secure manner, for example within an ACE secure envelope or equivalent at a prior time or at a secure manufacturing facility.

Specific personalities may have a single or multiple users. The security policy for the personality will define the personality user characteristics.

Factory Crypto Officers initialize the Loader Software at a secure manufacturing facility. Their roles are not defined in this policy.

ACE with Loader Software supports two roles: USER and CRYPTO OFFICER.

Identity based authentication is required for the CRYPTO OFFICER role.

Identity based authentication is required for the USER role.

A new personality image is created by a factory Crypto Officer at the Atalla factory and delivered to ACE by the local authenticated CRYPTO OFFICER using the Personality Load service. The Crypto Officer and User roles have the same set of services, and authenticate to the roles in the same manner. There is only one authorized operator per module.

3.4 Security Level

The ACE with Loader Software is targeted for evaluation at FIPS 140-2 level 3.

Security Requirement	**Level**
Cryptographic Module Specification	3
Cryptographic Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3+EFP/EFT
Self-Tests	4
Design Assurance	3
Mitigation Of Other Attacks	N/A

Operation environment is not applicable because only trusted code is loaded.

3.5 Interfaces

3.5.1 Data Input

The data input interface is the data portion of the 120 pin PCI bus.

3.5.2 Data Output

The data output interface is the data portion of the 120 pin PCI bus.

3.5.3 Control Input

The control input interface is the data portion of the 120 pin PCI bus.

Typically the control input and data input are combined into a command and transmitted as a single message. The response message is status and optional data output.

3.5.4 Status Output

The status output interface is the data portion of the 120 pin PCI bus. There are also LEDs on ACE that have status output for use during manufacturing test.

3.5.5 Power

There are two power interfaces. The first is the power portion of the 120 pin PCI bus. It is the main source of power and is used when the module is operational. The second is the module battery. It is the power source used to maintain the non-volatile memory.

4. Principles

Rule 3:

ACE program memory and RNG starting key shall be initially loaded at an authorized manufacturing site.

This rule is important because there is only a single input/output port on the ACE hardware. The very first use of the port must be at a location where the port is not observable by adversaries. Once the initial program (Loader Software) and RNG starting key are in place then additional loading outside the factory environment is possible.

This rule is enforced by manufacturing procedures.

Rule 4:

Personality software and cryptographic keys, when loaded while ACE is outside of an authorized manufacturing site, shall themselves be cryptographically protected.

The actual key names and their uses are described in the CSP Key Table.

Rule 5.

Clear cryptographic keys in the secure envelope shall NEVER be exported out of the secure envelope.

Rules 4 and 5 are enforced by the software.

5. Sensitive Data

Cryptographic keys are the ACE’s Critical Security Parameters (CSPs). The CSP key table is included in the "Roles and Services" section of this document.

The loader program's image is factory installed and is not modifiable outside the factory environment. The image is treated like a CSP in that it will be zeroized upon tamper detection.

CSPs that are maintained in the "clear" are stored in the battery backed up non-volatile memory.

The personality program's encrypted image is stored in FLASH memory. When power is supplied to the system the FFK is used to decrypt the personality. The clear image is available in system RAM for use while power is maintained.

If a tamper occurs while system power is either on or off, the FFK and other clear CSPs in non-volatile memory are zeroized.

Once the clear CSPs are zeroized the ACE cannot be successfully used because all CSPs are unavailable. The ACE circuit card must be returned to the factory for repeating the initialization process.

FLASH, system RAM, and the special non-volatile memory integrated circuit are all located within the secure envelope.

6. Self Tests

6.1 Power Up Self Tests

6.1.1 Cryptographic Algorithm Known Answer Tests

These functions are tested at power-up by verifying correct results with known answer problems taken from the algorithms’ specifications when possible. They are also tested with known answer problems on demand by the Status and Self-Test service instruction. Note that MD5, RIPEMD and RSA are not FIPS approved algorithms.

triple DES (ECB, CBC, single key, two key, and three key option)

triple DES MAC (single key, two key, and three key option)

SHA-1

MD5

RIPEMD

RSA decryption

6.1.2 Firmware Integrity Tests

Loader firmware integrity, a 32 bit CRC verification that the loader code in non-volatile memory is unchanged. This test is performed at power-up and all other system reset conditions.

Personality image integrity, a 3keyTDES MAC verification that the personality code that is decrypted from flash to RAM is unchanged. This test is performed at power-up and all other system reset conditions.

6.1.3 Statistical Random Number Generator Test

The RNG (random number generator) is tested at power-up and on demand in full compliance of the FIPS 140-2 requirements.

The RNG is implemented using the FIPS approved method described in ANSI X9.31. The initial seeds were externally generated by a RNG using the same method. The continuous operation of the RNG uses an internal hardware random number generator to provide modified seed values. 64 bit pseudo random numbers are produced for each use and 32 bits are discarded leaving the remaining 32 bits. Each bit is equally likely to be a zero or a one. Multiple numbers are produced when more than 32 bits are required.

6.1.4 Non-Volatile Memory Test

There is a non-destructive test of the non-volatile memory. This test is performed at power-up and all other system reset conditions.

6.2 Critical Function Automatic Tests

6.2.1 Flex Grid

There is a continuous test performed to monitor the secure state of the components used for all functions. This test, The ***Flex Grid Data Clock Test***, verifies that the tamper detect processor is operating correctly and has not detected a penetration attempt.

6.2.2 Non-Volatile Memory Test

The previously described non-volatile firmware integrity and memory tests are also critical function tests.

6.2.3 Hardware Controlled Tests

The section EVENTS in this document summarizes the effects of these tests.

6.3 Conditional Self Tests

There are certain additional self-tests that are automatically performed. These tests, and the conditions for their execution, are:

Personality image integrity, a 3keyTDES MAC verification that the personality code that is decrypted from RAM during a personality load is unchanged. This test is performed during the last phase of the personality load sequence.

Continuous RNG test, a verification the random number generator is not stuck and the last number generated does not match the previous number. This test is performed for every request for a random number.

7. Service instructions

Service instructions (commands) to the ACE with Loader Software shall fall into the following categories.

7.1 Status

Limited status information shall always be available. A 32 bit status register can be read on the PCI data bus.

Additional instructions requesting ACE to send specific status information are available; e.g. get serial number. Instructions for setting "constant" values that are performed one time in the factory are not considered in this security policy; e.g. set serial number.

The operator may determine whether the module is running in FIPS or non-FIPS mode with the “version” command.

7.2 Self Test

Instructions requesting ACE to perform self-test operations are available. There are individual instructions for testing specific functions, e.g. DES and SHA-1. These tests are identical to the power-up self-tests.

7.3 Personality Load

Personality load instructions, when successful, shall result in updating the ACE FLASH.

The Personality Load service is a sequence of three commands:

(Identify) Set CRYPTO OFFICER or USER identity

(Authenticate) Prepare for image update

(Load) Write new image (keys and/or personality)

The separate data inputs for the three commands are prepared at the Atalla factory. The customer can choose how to physically control the three inputs.

The first data is a clear text name of the CRYPTO OFFICER or USER.

The second data is a RSA protected digital envelope protecting the TDES key used to encrypt the new image and also encrypt the clear text name of the CRYTO OFFICER or USER.

The third data is the encrypted image, encrypted with the TDES key sent in the second message.

If the module is able to verify the MAC applied to the RSA envelope, and verify the identity string contained within the envelope, identity based authentication is achieved.

Concurrent use by different Users or Crypto Officers is not supported. An error message will be returned from either the authenticate or load command if the three commands were not from a matched set. An error message will also be returned if there is a power interruption between commands in the sequence.

7.4 Mode Selection

The following two commands determine the loader mode of operation:

Enable FIPS

Disable FIPS

These commands are used to switch between the Internal Download Keys (IDKs) used for downloading the personality. When in FIPS mode, only a FIPS personality may be downloaded, and likewise in Non-FIPS mode. Whenever a switch between modes is made, the current personality, user keys, and all other sensitive information is destroyed. The serial number is left intact. Identification of the mode is provided in the "version" command. Each command is MAC'ed; the MAC key is stored in the code and not provided in this text for security purposes. The MAC key is a TDES key.

Both modes of operation maintain the secure envelope.

The only difference between the non-FIPS and FIPS modes is the value of the private IDK which is used to decrypt the IDFK that in turn is used to decrypt the personality image file. This difference allows for control over which type of personality is allowed to be loaded on the card, namely Non-FIPS approved or FIPS approved.

The loader only uses the approved critical functions. All functions are available to personalities. The FIPS enabled personalities are responsible for indicating to users when non approved algorithms are enabled and used.

7.5 Echo

The echo instruction allows the host to verify the communication path over the PCI bus.

7.6 Start Personality

The start personality instruction, once used, disables the current Personality Load instructions. All future personality loading and personality updates must be controlled by a new Personality Load sequence. Protection is provided so that the start personality instruction cannot cause security leakage when no personality is loaded.

The start personality service is only offered once a personality has been loaded, and is outside of the scope of the current validation.

7.7 Zeroize

The zeroize service is not a command. It is 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.

8. Roles and services

8.1 Crypto Officer Role

A CRYPTO OFFICER can perform the following services:

Request status and self test

Echo data

Start Personality

Personality Load

Select Mode (FIPS or NONFIPS)

Zeroize

Access to ACE Personality Load shall require the presentation of authenticated data to the ACE. The authenticated data is the RSA protected digital envelope containing the IDFK. The Crypto Officer is authenticated through a TDES MAC process. This method is considered cryptographically "strong" with key strength greater than 100 bits. The keys are available only at the Atalla factory. The probability of a single random test value match the actual key is:

P (single random attempt matching key) =

$1 / 2^{100} <= 10^{-36}$

The bus can transfer 132Mbytes per second. Random attack messages (average length 66 bytes) could be tried at 2M attacks per second. The probability of just getting the key correct would be:

P (maximum attempts in one second) =

$$2 \text{ (half maximum needed) } x\ 2 \ x\ 10^{6} / 2^{100} <= \ 4 \ x\ 10^{-30}$$

P (maximum attempts in one minute) =

$$60 \ x\ P \text{ (one second) } <=2.4 \ x\ 10^{-28}$$

Note that matching the Crypto Officer identity alone is not sufficient to do a Personality Load; the key must also be correct. The low probability of getting the key correct with a single guess is less than the acceptable limit of 1 out of 1,000,000 (1 out of 10^{36} is less probable than 1 out of 10^{6} .) The low probability of getting the key correct with the maximum guesses in one minute is less than the acceptable limit of 1 out of a 100,000 (1 out of 4.1 x 10^{27} is less probable than 1 out of 10^{5} .)

8.2 User Role

A User can perform all the services of a Crypto Officer. The Personality Load and Select Mode services require that the user have the properly authenticated identification and data.

8.3 Unauthenticated Services

The following services do not involve the use of CSPs and can be performed for requestors other than the Crypto Officer or User:

Status and Self Test

Start Personality

Echo

Zeroize

8.4 CSP Key Table

Key Name	**Key Use**	**Key Source**
Symmetric Keys:		
Flash File Key (FFK)	3keyTDES Encrypts code image to flash memory, decrypts code image from flash memory	Randomly generated by the loader each time a personality is downloaded
Image Download File Key (IDFK)	3keyTDES Decrypts the personality file external to the cryptographic device.	Randomly generated at the factory and delivered as a cryptogram, encrypted by IDK public (counterpart to Image Download Private key.) Destroyed after image update completed.
Image Download MAC Key (IDMK)	3keyTDES MAC Verifies personality program image integrity when downloading	Constant in code and the image loader.
FIPS Enable MAC Key (FEMK)	3keyTDES MAC Verifies "enablefips" and "disablefips" commands.	Constant in code and the image loader.
Revenue Key (RK)	3keyTDES MAC Controls personality access to revenue commands	Constant in the loader code. Only used once a personality has been loaded, which is outside the scope of the current validation.
RNGstartingKey (RNG)	3keyTDES One time initialization seed for RNG	Constant in the loader code.
Super Key (SK)	2key or 3keyTDES Used to encrypt/decrypt personality specific keys.	Initial SK is a constant in the personality code. Not used until a personality is loaded which is outside the scope of the current validation.
Asymmetric Keys:		
Image Download Private Key (IDKpvt) (IDK_FIPS) (IDK_NONFIPS)	RSA Decrypts envelope containing the Crypto Officer or User Identity and the symmetric key that encrypted the personality image (IDFK) for download to the card.	Constants in the loader code. One of the two keys is selected depending upon the current mode.

8.5 Role and CSP versus Service Matrix

Role/CSP	Service					
	Status and Self Test	Start Personality	Echo	Personality Load	Select Mode	Zeroize
Cryto Officer	X	X	X	X	X	X
User	X	X	X	X	X	X
FFK		X		X		X
IDFK				X		X
IDMK		X		X		X
FEMK					X	X
RK						X
RNG	X					X
SK						X
IDKpvt				X		X

9. Administration

The real administration of ACE takes place during the manufacturing process where the physical security boundary (secure envelope) is installed. This boundary surrounds the initial software components. Additional software components can only enter the boundary if they, the software components, are correctly authenticated and encrypted.

The enforcement of the secure envelope is continuous from the time ACE leaves the manufacturing facility. There is no method available to Crypto Officers or Users or anyone else for relaxing the monitoring of the integrity of this envelope. Once an event is detected that indicates the integrity of this envelope is in question CSPs within the envelope are destroyed and ACE is no longer in a useable state. ACE must be returned to the factory at this point. There is no method for security officers or field maintenance personnel to restore ACE to a useable state.

9.1 Crypto Officer and User Responsibility

The Crypto Officer has no administrative responsibility for maintaining the secure envelope. He does have responsibility for executing a host program that will provide the commands to perform a Personality load operation.

However, the generation of the data for the load operation is performed at a separate secure location.

For additional security a Crypto Officer or User can view the tamper evident seals on the unit to observe if attempts at tampering have occurred. If tampering is evident the unit should be removed from service.

10. Power Off States

The module is idle when there is no power applied via the 120 pin connector. The following states are the power off states of the ACE during this idle condition. When power is applied there are additional operational states.

Unknown. This is the state before factory initialization.

Software Loader. This is the state after factory initialization before a personality has been activated. The secure envelope is active.

Personality. This is the state after a personality has been loaded and the personality has been started at least one time. The secure envelope is active.

Alarm. This is the state after the secure envelope has been active and a tamper attempt has been detected.

11. 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.

ACE supports Environment Failure Protection (EFP).

When events have occurred the unit becomes non-operational either by going into the permanent ALARM state or the temporary RESET state.

The detected events are:

Physical penetration. The secure boundary has been penetrated or otherwise broken. For this document this is a single occurrence of one of multiple ACE events; 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 the normal operating voltage established for this circuitry.

Power out of limits. The host system voltage is outside of the normal operating range.

Thermal out of limits. The ACE temperature is outside of the normal operating range.

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

	Zeroize NVRAM	Reset	ALARM
Physical penetration	X		X
Battery low	X		X
Power out of limits		X	
Thermal out of limits		X	

ACE does not have physical protection methods for x-ray or gamma ray radiation. However single bit failures in any memory elements should not result in exposure of CSPs. There are no software logic paths that can be selected because of single (or multiple) bit failures that will result in export CSPs in clear text format.

12. Specific Attacks

ACE is not designed to mitigate specific attacks, e.g. Differential Timing Analysis (DTA), Differential Power Analysis (DPA), or Differential Fault Analysis (DFA.)

It is recommended that ACE reside in a system where physical access to the card and bus is restricted. This would make DTA and DPA attacks difficult.

13. Glossary

ACE	Atalla Cryptographic Engine.
CSP	Critical Security Parameter, previously referred to as SRDI, Security Related Data Item.

14. ACE Picture