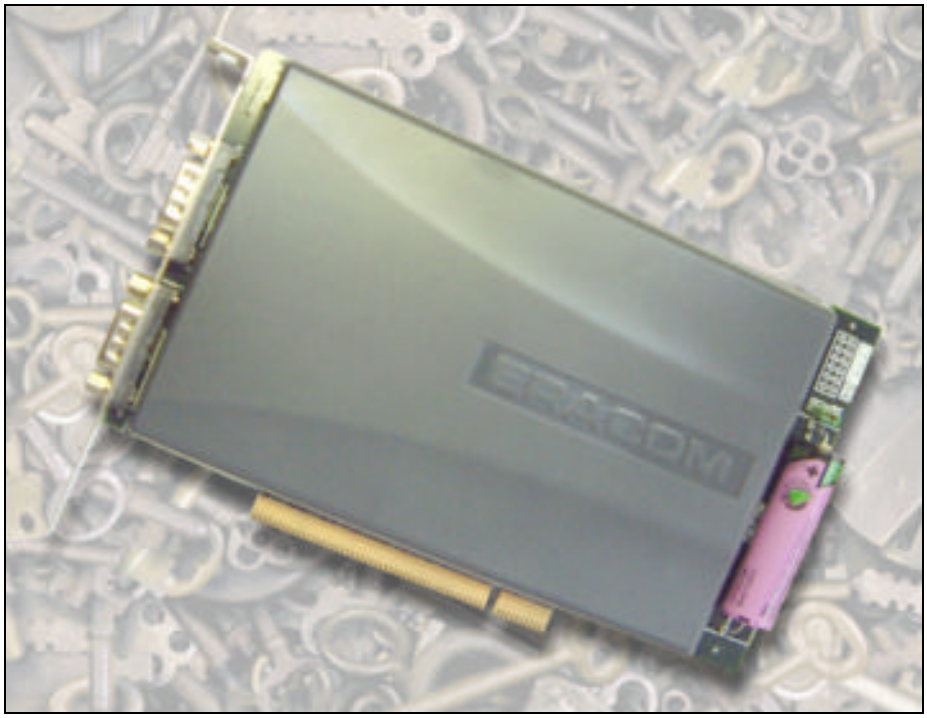
ERACOM™
A CONCORD·ERACOM COMPANY

CSA8000 Cryptographic Adapter

Hardware Revision: G; Firmware Version 1.1



FIPS 140-1 Non-Proprietary Cryptographic Module Security Policy

Level 3 Validation

July 2001

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the CSA8000 Adapter. This security policy describes how the CSA8000 Adapter meets the security requirements of FIPS 140-1 and how to operate the CSA8000 Adapter in a secure FIPS 140-1 mode. This policy was prepared as part of the Level 3 FIPS 140-1 certification of the CSA8000 Adapter.

FIPS 140-1 (Federal Information Processing Standards Publication 140-1 -- *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-1 standard and validation program is available on the NIST web site at http://csrc.nist.gov/cryptval/.

1.2 References

This document deals only with operations and capabilities of the CSA8000 Adapter in the technical terms of a FIPS 140-1 cryptographic module security policy. More information is available on the CSA8000 Adapter and other Eracom products from the following sources:

- The Eracom website contains information on the full line of security products at http://www.eracom.com.au
- For answers to technical or sales related questions please refer to the contacts listed on the Eracom website at http://www.eracom.com.au

1.3 Terminology

In this document the Eracom CSA8000 Adapter card is referred to as the adapter, the Protect 2PKI, or the module.

1.4 Document Organization

The Security Policy document is part of the complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Module Software Listing
- Other supporting documentation as additional references

This document provides an overview of the CSA8000 Adapter and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the CSA8000 Adapter.

Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

This Security Policy and other Certification Submission Documentation were produced by Corsec Security, Inc. under contract to Eracom. With the exception of this Non-Proprietary Security Policy, the FIPS 140-1 Certification Submission Documentation is Proprietary to Eracom and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Eracom.

2 The CSA8000 Cryptographic Adapter

The Eracom CSA8000 Adapter is an intelligent PCI adapter card that provides a wide range of cryptographic functions with dedicated DES/3DES and RSA hardware accelerators. This cryptographic server takes the form of a one-half length PCI adapter card and supports Smart Card key storage tokens. The module, running Cprov firmware, implements the PKCS#11 cryptographic API as defined by RSA. While certain PKCS#11 features are not supported, the module provides a comprehensive compliance to the PKCS#11 standard as well as vendor-specific extensions. The CSA8000 Adapter, which meets FIPS 140-1 level three requirements for a multi-chip embedded module, allows system integrators to incorporate proven hardware-based security with tamper protection into their PKI products. The following section describes the overall features and functionality of the adapter.

2.1 Cryptographic Module

The CSA8000 Adapter enables integrators to add high-powered PKI cryptographic functions to any server with the appropriate 33MegHz, 32Bit PCI slot. The cryptographic boundary for this product encapsulates the majority of the adapter card, the end of the adapter card where the battery is mounted is outside the cryptographic boundary. The opaque, polycarbonate cover surrounds the card to provide tamper-protection and to establish the cryptographic boundary. This boundary includes the Data Ciphering Processor (DCP), embedded processor, SDRAM memory chips, and the Real Time Clock (RTC).

The module provides key management (e.g., generation, storage, deletion, and backup), an extensive suite of cryptographic mechanisms, and process management including separation between operators. The CSA8000 Adapter also features non-volatile tamper protected memory for key storage, a hardware random number generator, a Real Time Clock, and a fast 32-bit RISC microprocessor for cryptographic processing and management.

The adapter comes preloaded with a FIPS-approved firmware and can be upgraded to new, enhanced firmware. New firmware are digitally signed by Eracom and verified by the adapter to insure a secure upgrade.

2.2 Module Interfaces

The secure CSA8000 Adapter card, which is protected by a tamper resistant polycarbonate cover, has four primary physical interfaces. The adapter features a standard PCI bus interfacing to the motherboard of the server or host machine and two asynchronous RS232 serial connectors on the end plate for connecting Smart Card readers to the module. The fourth primary interface is a power interface to the backup battery for power off memory retention.

In addition to these primary interfaces, there is a group of connector pins on the adapter circuit board outside the security perimeters. They include an external tamper source input pin (a pin input that accepts external tamper signals), tamper status output pin, four external peripheral status inputs pins, four external peripheral status output pins, a low battery output status indication pin, and an electrical ground pin. The four status output pins are not currently used by the Cprov firmware and carry no information; they will be used in future versions of this product. The four external peripheral status inputs pins have no effect on the operation of the CSA8000 Adapter; however, applications connecting to the adapter through the PCI bus may query the condition of these signals.

The CSA8000 Adapter provides a tightly secured cryptographic element. All requests for services sent to the crypto device over the PCI bus or the serial ports are captured by the adapter's processor, which controls the level of access to the on-board cryptographic services and the keys. The adapter's processor also responds to PKCS #11 functions commands, ensuring that during FIPS operation only authenticated users receive cryptographic services.

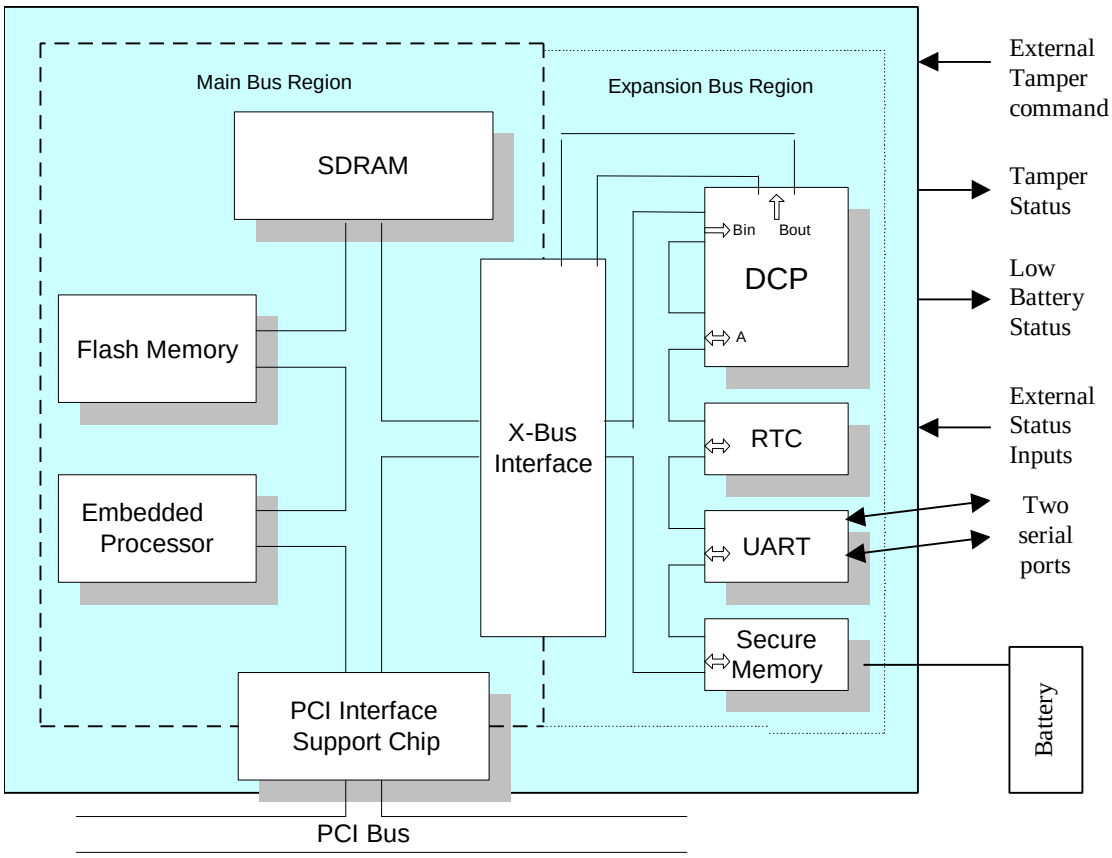


Figure 1 – Basic Block Diagram

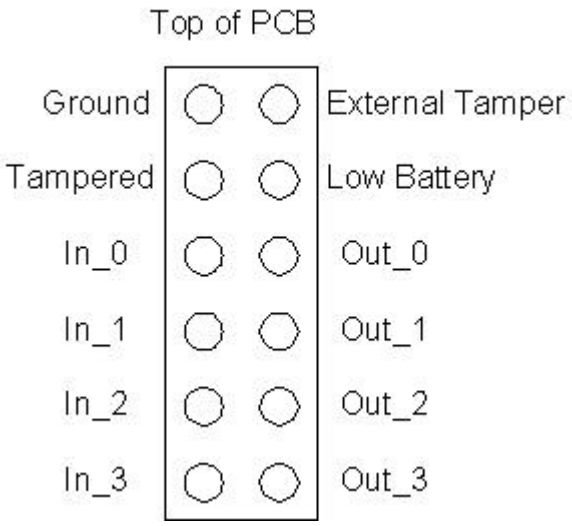


Figure 2 – External Pin Layout

The module's physical interfaces are separated into the logical interfaces, from FIPS Pub 140-1, as described in the following table:

FIPS 140-1 Logical Interfaces	Adapter Physical Interfaces
Data Input Interface	PCI Bus, Serial ports
Data Output Interface	PCI Bus, Serial ports
Control Input Interface	PCI Bus, External tamper pin
Status Output Interface	PCI Bus, Serial Ports, Low battery pin, Tampered pin
Power Interface	PCI Bus

Table 1 – FIPS 140-1 Logical Interfaces

The PCI bus is the only physical communications port used by applications connecting to the card. All applications share this physical port; however, user separation is maintained by including a MAC with the session key.

2.3 Trusted Channels

The CSA8000 Adapter implements a Trusted Channel called the Secure Message System which enables operators to securely communicate over the PCI bus interface. Trusted Channels use session keys for message encryption/decryption and message signing and verification. A Trusted Channel (TC) is created on-demand by the operator but may be terminated by either the adapter or the operator.

The adapter can manage multiple simultaneous Trusted Channels, and each TC will have its own set of randomly generated session keys. The adapter uses a class of triple length DES keys called Host Interface Master Keys (HIMK). An operator must possess one of the HIMKs stored in the adapter to establish a Trusted Channel. HIMKs are secret values

shared by the adapter and operators, which are used (along with random data) to derive TC session keys. The adapter stores HIMKs in the Admin Token.

After initial installation, the adapter will possess a single default HIMK. Administrators may create new HIMKs and destroy existing HIMKs (including the default). The adapter can contain multiple HIMKs, each one loaded via split key procedures to protect the key during entry.

Trusted Channel session keys consist of a triple length DES key used for encryption and a twenty byte long secret value used for HMAC-SHA-1 authentication. Encryption and decryption is performed using the triple length DES key in Output Feedback (OFB) mode. Authentication is performed by generation of an HMAC-SHA-1 value on the previously sent message's authentication and the new message content. This forms a "rolling authentication" such that the authentication value for each message is the result of the signing key and all previous message contents.

2.4 Roles and Services

The CSA8000 Adapter supports identity-based authentication of its operators and supports multiple simultaneous operators each with their own individual set of services. Individual operators can request multiple sessions simultaneously. Each request for services during a session contains a MAC using a negotiated session key, thus maintaining the separation of the authorized roles and services performed by each operator. Operators are authenticated to the adapter by presenting a PIN.

Roles are based on the PKCS#11 concept of Tokens. Each Token is a collection of Cryptographic Objects. All Tokens have two operators: a Security Officer (SO) and a User. The CSA8000 Adapter supports three types of Tokens, one Administration Token, multiple Cprov Tokens and one or more physical Smart Card Tokens. The SO and User of the Administration Token have special privileges which are detailed in the following sections.

There are four roles in the module that operators may assume: Admin Security Officer, Admin, Token Security Officer, or Token User. The Admin Security Officer and the Admin have access to the Crypto Officer functionality. Any other token users (i.e. non-Administration token Security Officer or users) have access to User functionality. Table 2 below lists the services available to each user. The operator explicitly selects a role when logging in by selecting a PKCS#11 Token and nominating either User or SO Role. The adapter provides bounded services to an operator based on the role to which the operator authenticated. There is only one operator assigned to each role. The purpose for each role and the services provided to each are detailed in the following sections.

Note - The services available to the roles depend on the Security Settings – the following descriptions only apply when the adapter is configured for FIPS compliance – see Section 3 of this document for details.

Role	Admin SO	Admin	Token SO	Token User
Service				
Specify Key Export Attribute on a Public Key	✓		✓	
Specify Trusted Attribute on a Public Certificate	✓		✓	
Set Initial Administrator PIN Following a Tamper	✓			
Get Token Info/Slot Info/Public Info	✓	✓	✓	✓
Change Own Password	✓	✓	✓	✓
Change RTC		✓		
Read Hardware Event Log	✓	✓		
Purge Full Hardware Event Log		✓		
Set Transport Mode		✓		
Specify Adapter Security Policy		✓		
Create CPROV Slots/Tokens		✓		
Initialise CPROV Token Labels and SO PIN		✓		
Specify CPROV Token Min PIN Length		✓		
Initialise Smart Cards/Labels/SO PIN's		✓		
Specify Smart Card Min PIN Length				
Destroy CPROV Slots/Tokens		✓		
Erase Adapter Secure Memory/PIN's/Keys		✓		
Perform Firmware Upgrade		✓		
Manage Host Interface Master Keys (Create/Delete)	✓	✓		
Public Key Cryptographic Services On an Admin Token	✓	✓		
Create Public Admin Token Objects	✓	✓		
Destroy Public Admin Token Objects	✓	✓		
Generate Public Admin Token Objects	✓	✓		
Derive Public Admin Token Objects	✓	✓		
Private Key Cryptographic Services On Admin Token		✓		
Create Private Admin Token Objects		✓		
Destroy Private Admin Token Objects		✓		
Generate Private Admin Token Objects		✓		
Derive Private Admin Token Objects		✓		
Initialize Normal Token User PIN			✓	
Reset (re-initialise) Normal Token			✓	
Public Key Cryptographic Services on a Normal Token			✓	✓
Create Public Objects on a Normal Token			✓	✓

Destroy Public Objects on a Normal Token			✓	✓
Generate Public Objects on a Normal Token			✓	✓
Derive Public Objects on a Normal Token			✓	✓
Private Key Cryptographic Services on a Normal Token				✓
Create Private Objects on a Normal Token				✓
Destroy Private Objects on a Normal Token				✓
Generate Private Objects on a Normal Token				✓
Derive Private Objects on a Normal Token				✓
Public key cryptographic services on smart card token				
Create Public Objects on a Smart Card Token			✓	✓
Destroy Public Objects on a Smart Card Token			✓	✓
Generate Public Objects on a Smart Card Token				
Derive Public Objects on a Smart Card Token				
Private Key Cryptographic Services on a Smart Card Token				
Create Private Objects on a Smart Card Token				✓
Destroy Private Objects on a Smart Card Token				✓
Generate Private Objects on a Smart Card Token				
Derive Private Objects on a Smart Card Token				
	Admin SO	**Admin**	**Token SO**	**Token User**

Table 2 - Roles and Services Table

Check marks represent services that each role has available and grayed areas are services that do not make sense for that specific role.

2.4.1 Administrator Security Officer

The primary role of the Administrator Security Officer (ASO) is to introduce the Administrator to the system. The ASO is able to set the initial Administrator PIN value but is not able to change the administration PIN after it is initialized. There is a factory default login ID and password, which allows access to the Administrator Security Officer role. The FIPS operational policy requires the ASO to change the default ID and Password. The ASO can perform the following actions:

- *Set the initial Administrator PIN value during initial configuration and following a tamper*
- *Create, destroy, public objects on their own token.*
- *Specify a key EXPORT attribute on a public key*
- *Specify TRUSTED attribute on a public certificate*
- *Exercise status querying services.*

- *May change his/her own PIN*
- *May revoke Authentication*
- *Manage Host Interface Master Keys*

2.4.2 Administrator

The Administrator is responsible for the overall security management of the adapter and controls Slots (PKCS#11 defines a slot as a logical reader that potentially contains a token) and Token Security Officers. The following actions are available to the Administrator:

- *Has exclusive Read/Write access to the Admin Slot*
- *Set or Change RTC value*
- *Read the Hardware Event Log*
- *Purge a full Hardware Event Log*
- *Configure the Transport Mode feature.*
- *Specify the Security Policy of the adapter.*
- *Create new Cprov Slots/Tokens and specify their Labels SO PINs and min PIN Length*
- *Initialize smart cards and specify their Labels SO PINs and min PIN Length*
- *Destroy Individual Cprov Slots/Tokens.*
- *Erase all adapter Secure Memory including all PINS and User Keys*
- *Perform Firmware Upgrade Operation*
- *Manage Host Interface Master Keys*
- *Create, destroy, import, export, generate, derive public or private objects on their Admin token.*
- *Exercise cryptographic services with Private Keys on the Admin Token*
- *Exercise cryptographic services with Public Keys on the Admin Token*
- *Exercise status querying services*
- *May change his/her own PIN*
- *May revoke Authentication*

2.4.3 Token SO

The Token SO is responsible for granting and revoking ownership of its token. If the Token does not have a User PIN, the Token SO should initialize it by assigning the Label and User PIN. He may also revoke the Token User's privileges (and possibly reassign the token to another operator) but only by destroying all the key material of the original operator first.

- *Set the User PIN on a Token with no User PIN.*
- *Reset (re-initialize) the Token (destroys all sensitive and non sensitive data) and sets new Label and SO PIN*
- *Create, destroy, public objects on their own token.*
- *Specify a key EXPORT attribute on a public key*
- *Specify TRUSTED attribute on a public certificate*
- *Exercise status querying services.*

- *May change his/her own PIN*
- *May revoke Authentication*

2.4.4 Token User

Token users may manage and use private and public keys on their own tokens.

- *Exercise cryptographic services with Public Keys on their own Token*
- *Exercise cryptographic services with Private Keys on their own Token*
- *Create, destroy, import, export, generate, derive private or public objects on their own token.*
- *Exercise status querying services.*
- *May change his/her own PIN*
- *May revoke Authentication*

2.4.5 Unauthenticated Operators

Certain services are available to operators who have not (yet) authenticated to the adapter:

- Exercise status querying services.
- Authenticate to a Token

2.4.6 Access Control

The adapter services and key management are based on the PKCS #11 API, the availability of services is based on Tokens and access to a storage object within that Token. For every object there are attributes that define the access the SO and User can have to the object as well as the commands they can perform on the object. There are three types of storage objects supported by the adapter:

- **System Objects**: objects on the Administration Token available only to the adapters Administrator.
- **Private Objects**: objects available only to the Token User.
- **Public Objects**: objects available to all operators of the adapter. Users must be Authenticated to the Token to perform cryptographic operations with these objects.

Trusted Channels are used as part of the Adapter Access Control. Operators must establish a TC (see section [2.3] above) before they can authenticate to a Token by presenting their PINs with C_Login. After a successful authentication, the application side of the Trusted Channel must perform message signing on all requests for cryptographic services. The adapter correspondingly will verify the signatures on all requests that involve cryptographic services and refuse the requests if the signature fails to verify.

2.5 Physical Security

The adapter is covered in a polycarbonate cover to protect the cryptographic components from probing. The adapter provides tamper detection via a pressure micro-switches and light sensors mounted on the card beneath the cover. The pressure switches are mounted

on both the top and bottom of the card, protecting the critical security parameters if either side of the cover is removed. If the tamper detection devices are triggered, the memory containing all critical security parameters (keys and pins) is zeroized. Zeroization occurs in two ways depending on the power status of the module. When the module is powered the device will overwrite all critical security parameters. When the module is in a power off state, the backup battery power is removed from the RAM. Additionally, the CSA8000 Adapter provides settings that enable zeroization if the module is removed from the host PCI slot and provides an interface lead where an external tamper source may be fitted.

The adapter meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for home use (ClassB) and is labeled in accordance with FCC requirements.

2.6 Secure Cryptography

The CSA8000 Adapter functions as a high-speed server of cryptographic services. The module securely administers both cryptographic keys and other critical security parameters such as PINs. The module has the capacity to generate keys, import and export keys protected under a key encryption key, store keys, delete keys and backup keys to smart cards. Table 3 provides a listing of the keys types in the module.

Key Table	
HIMK	Host Interface Master – Shared secret to protect initial handshake between the application and the module.
HIK	Host Interface Key – a unique key is negotiated for each session; also called session key
User Private Keys	As a tool users can create both symmetric and asymmetric keys, to be used to perform any of the encryption mechanisms provided by the module
Public Keys	Both symmetric and asymmetric keys available to any user of the module.

Table 3 – Key Types

The module supports the following cryptographic mechanisms; however, not all of the mechanisms are available in a FIPS compliant mode (see Section 3 below for FIPS mode configuration). An authenticated operator must have access to an object and permissions to use a key in order to make use of these algorithms.

Symmetric Ciphers	CAST 128, DES, Triple DES (Double or Triple length keys), IDEA, RC2, RC4, AES (Rijdael)
Symmetric Cipher Modes	ECB, CBC, OFB
MAC Generation	HMAC-MD5, HMAC-RMD128, HMAC-RMD160,

	HMAC-SHA1
Asymmetric Ciphers	RSA, RSA PKCS#1, DSA - Digital Signature Algorithm, Diffie-Hellman
Message Digest	SHA-1, MD2, MD5, RIPEMD-128, RIPEMD-160
Certificate Management	o Generate a X 509 Version 3 Certificate (Using RSA or DSA) o Verify signatures with a X 509 Version 3 Certificate (RSA or DSA) o Generate a PKCS#10 Certificate Request, Decode (RSA or DSA) o PKCS#7 Certificate / CRL package.(RSA or DSA)

The CSA8000 Adapter maintains an organized key architecture including several keys with specific purposes. The Host Interface Master Key (HIMK) is used as the master derivation key for session keys, which in turn can be used for transporting keys and PINs into the adapter. The module supports public and private keys. Private keys can only be seen and used by the operator that created the key. Public keys may be seen by unauthenticated users and Token SOs (but not used to perform cryptographic operations while in FIPS Operation). Token SO and Token Users have access to Token Public access keys, the adapter Proof of Origin signing key, and to any HIMKs in the Admin Token.

The CSA8000 Adapter uses a hardware random number generator in the DCP in combination with FIPS-approved RNG techniques from FIPS 186-2 to provide fast key generation. RSA or DSA Public keys generated within the adapter can be digitally signed with a signing key (stored inside the adapter from manufacturing) providing proof of the origin of the key generating device. After a key is generated and stored, it may be exported. Keys may be stored temporarily (and will be destroyed when the communications session is terminated) or stored permanently (protected by battery backed, tamper protected memory). The adapter also offers the ability to transfer split key components to/from Smart Cards and to generate these components from internally stored keys and to merge these components into internal keys. All keys within the module can be zeroized. Token Users and Token SOs can zeroize keys under their control; however, the Administrator has complete authority to zeroize all keys in the module.

2.7 Self-Tests

In order to prevent any secure data being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The CSA8000 Adapter includes an array of self-tests which are run during startup and periodically during operations. The self-tests run at power-up include cryptographic known answer test (KAT) on the FIPS-approved algorithms (DES, 3DES, SHA-1) and on all other algorithms supported by the adapter. Also performed at startup are software integrity tests using a 32-bit Error Detection Code (EDC) and SHA-1 message digest, a statistical random number generator test, and several other critical functions tests including check sums on every functional module and hardware checks to validate the RAM, Secure Memory, RTC, and Serial communications devices. Other tests are run

periodically or conditionally such as a software load test for upgrades using RSA private key signature and the continuous random number generator test. A pairwise consistency check is run when an RSA or DSA key pair is generated. Whenever the cryptographic hardware is used it is monitored for errors.

If any of these self-tests definitively fails, the adapter will transition into an error state. Within the error state, all cryptographic functions are disabled and the adapter outputs status information indicating the failure to a PCI bus mailbox register.

3 Secure Operation of the CSA8000 Adapter

The CSA8000 Adapter is a versatile security tool; there are many features that can be configured to be on or off. A number of configuration settings are recommended when operating the CSA8000 Adapter in a FIPS 140-1 compliant manner. Other conditions are required in order to maintain compliance with FIPS 140-1 requirements. When the conditions listed below are met, the CSA8000 Adapter meets all of the FIPS 140-1, Level 3.

Required for FIPS Mode

- In order to maintain the FIPS compliance only FIPS-approved, Eracom-signed upgrades shall be uploaded to the adapter.
- Crypto functionality is restricted to the FIPS-Approved Algorithms (DES, TripleDES, SHA-1, DSA, and RSA for signatures). In order to maintain FIPS mode and hence FIPS compliance, users of the module and developers writing applications to interface to the module, must use or implement API calls that use only the FIPS-Approved algorithms.
- Each operator must not share his/her PIN(s) with any other operator.
- The following Security Policy settings must be configured -
    - CKF_ENTRUST_READY must be FALSE
    - CKF_ALWAYS_SENSITIVE must be SET
    - CKF_AUTH_PROTECTION must be SET
    - CKF_MODE_LOCKED must be SET.
    - CKF_NO_PUBLIC_CRYPTO must be SET.

Recommend for FIPS Mode

- The default HIMK should be deleted after a new HIMK is setup on the adapter.
- The minimum PIN length for any new slot should be configured to be at least 4.