Security Policy

for

FORTEZZA Crypto Card

Version 1.1a

January 16, 1997

Prepared by

National
Semiconductor™

iPower Business Unit
2900 Semiconductor Drive
P.O. Box 58090, M/S 16-225, Santa Clara, CA 95052-8090
Telephone (408) 721-5000

This page intentionally blank

Release Notes

22 Jan 96	Version 1.0	Submitted from contractor.
02 Feb 96	Version 1.1	Reformatted to iPower document including some reordering of sections and subsections; corrected minor typos; reordered command descriptions, SRDI list, Modes of Access list and Table 3 by alphabetic sort; corrected Security Rules 9 and 12c per reviewer's comments.
16 Jan 97	Version 1.1a	Removed "Private Information" statement on page i; removed "Company Private Information" notation from page footers; replaced individual's name with "reviewer's" in preceding paragraph.

Table of Contents

1. Scope of Document

This document describes the Security Policy for the FORTEZZA Crypto Card. The Security Policy specifies the security rules under which the FORTEZZA card operates. This document covers the security related services of the card and is not intended to address non-security related FORTEZZA card services or functions.

The FORTEZZA Crypto Card is a cryptographic module which implements, the Digital Signature Algorithm (FIPS 186), Secure Hash Algorithm (FIPS 180-1), NSA's Key Exchange Algorithm (KEA) and the SKIPJACK/LEAF (FIPS 185) encryption algorithm. The card complies with PCMCIA specification Standard Release 2.1. The card provides 41 individual commands which can be used to support cryptographic based authentication and encryption applications.

2. Security Level

The cryptographic module is designed to meet the overall security requirements of FIPS 140-1 security level-2. Table 1 lists the security levels corresponding to each of the eleven security requirement sections of FIPS 140-1. The module does not contain an operating system, hence the requirements of that section do not apply.

Table 1, Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module	2
Module Interfaces	2
Roles and Services	2
Finite State Machine	2
Physical Security	2
Software	2
Operating System Security	N/A
Key Management	2
Cryptographic Algorithms	2
EMI/EMC	2
Self Tests	2

3. Roles and Services

The FORTEZZA cryptographic module supports two distinct operator roles. These operator roles are:

1. User Role

2. Cryptographic Officer (Site Security Officer) Role

The cryptographic module enforces the separation of operator roles using role based operator authentication. An operator must select a role and then log-on using the appropriate access code (PIN Phrase) for that role. At the end of each session the operator must log-out. The defined roles supported by the module are:

1. The Site Security Officer (SSO) Role

   This role is equivalent to the Crypto Officer Role defined in FIPS 140-1. An authorized operator acting in the SSO role has access to all possible services provided by the module (both User and SSO services). However, this role provides additional services not available to an operator acting in the User Role. These additional services relate to card initialization functions, setting of PIN phrases (i.e. SSO, User and Zeroize), archiving private keys and setting the real time clock.

2. The User Role

   This role is equivalent to the User Role defined in FIPS 140-1. An authorized operator acting in the User role has access to all services provided by the module except those restricted to the SSO role only. See Table 3 for a definition of those services available for each role.

   Certain non-cryptographic card services (commands) may be called without the card being initialized. The services that may be performed prior to SSO or User log-on are marked with a (2) in Table 2.

3.1 List of Commands

The commands (services) executed by the FORTEZZA Crypto Card are listed in Table 2.

Table 2, Operator Services Command Set

Change PIN (1)
Check PIN (2)
Decrypt
Delete Certificate
Delete Key
Encrypt
Extract X (1)
Firmware Update (1)
Generate IV
Generate MEK
Generate Ra
Generate Random No. (2)
Generate TEK
Generate X
Get Certificate
Get Hash
Get Personality List-
Get Status (2)
Get Time (2)
Hash
Initialize Hash
Install X
Load Certificate
Load DSA Parameters
Load Initialization Value (1)
Load IV
Load X
Relay
Restore
Save
Set Key
Set Mode
Set Personality
Set Time (1)
Sign
Timestamp
Unwrap Key
Verify Signature
Verify Timestamp
Wrap Key
Zeroize (2)

Notes: (1) Commands available only to the SSO
(2) Commands may be called without the card being initialized

3.2 Command Descriptions

Most of the commands are self explanatory, by their labels. Commands that merit more explanation are described below. Refer to the FORTEZZA Crypto Card Interface Control Document for a description of each command.

Check PIN is a command used to implement an SSO or User log-on to a card.

Change PIN is the command used by an SSO to change an old or default PIN to a new PIN.

Extract X is used to remove a TEK wrapped X from the card for distribution or local storage purposes.

Install X is the reverse of Extract X.

Load DSA Parameters installs a FORTEZZA certificate's DSA p's, q's, and g's for a signer not within the local User's domain. Note: an application will normally obtain the KEA and DSA p's, q's and g's from a reference file to build a FORTEZZA certificate.

Load Initialization Values is used to enable an SSO to install a card's random seed and plaintext User's local storage key (Ks).

Relay transfers a TEK wrapped X from one workstation to another that is *not* the end destination of X.

Restore restarts an interrupted process (see Save, below.) One (1) encryption/ decryption process plus one (1) hash process may be saved and restored at a time.

Save optionally may be used to interrupt encryption, decryption, and hashing.

Set Key is used by an application to select a Key Register, the contents of which will be used in following commands. **Set Key** is used like Set Personality.

Set Personality selects a Certificate Register, the contents of which will be used in following commands.

Set Time is used by an SSO to advance or stop the card's clock (date and time). For security reasons, there is no way to reverse the card's clock.

4. Security Rules

The security rules enforced by the FORTEZZA Crypto Card are enumerated below.

1. There is only one SSO and one User per card.
2. After 10 unsuccessful SSO log-on attempts, the SSO's PIN and all keying material are zeroized. After zeroization, the PIN is set to a known ZEROIZED PIN value.
3. After 10 unsuccessful User log-on attempts, the User's PIN value is zeroized, requiring the user to return the card to the SSO.
4. Only an SSO may update card firmware, load initialization parameters, set the date/time of the real time clock, set the SSO and User PINs, change PINs, and Extract an X-value
5. The only valid Cryptologic Commands that may be performed on a card prior to SSO or User log-on are Get Status, Get Time, Generate Random Number, Check Pin, and Zeroize.
6. Either a logged on User or SSO may load, generate, or install X-values. Only the SSO may load X-values and/or a certificate in Certificate Index 0.
7. Only the original SSO (the SSO who possesses the SSO PIN) may extract an x-value. The original SSO can only extract x-values that the original SSO created/loaded.

8. The cryptographic module implements the FIPS PUB 185 Escrowed Encryption Standard (ESS) for encryption and decryption of message traffic. This standard specifies use of a symetric-key algorithm (SKIPJACK) and a Law Enforcement Access Field (LEAF). The module supports the following SKIPJACK modes; Electronic Codebook (ECB), 64 bit Output Feedback (OFB), Cipher Block Chaining (CBC) and 8/16/32/64 bit Cipher Feedback (CFB).

9. The cryptographic module implements an NSA designed asymmetric encryption algorithm called the Key Encryption Algorithm (KEA). KEA is used to generate a Token Encryption Key (TEK) which is used to wrap Message Encryption Keys (MEK) and Private keys (X).

10. The cryptographic module implements the FIPS PUB 180-1 Secure Hash Standard Secure Hash Algorithm (SHA-1).

11. The cryptographic module implements the FIPS PUB 186 Digital Signature Standard Digital Signature Algorithm (DSA).

12. Upon the application of power, or upon receipt of a Reset command, the cryptographic module performs the power-up self-tests described below:

    a) Cryptographic algorithm test: Known answer tests are performed, on all cryptographic algorithms implemented in hardware, including SKIPJACK encrypt and Secure Hash Algorithm.

    b) Software/firmware Test: ROM and non-volatile on-chip and off-chip memory tests are performed using a FIPS approved authentication technique.

    c) Random Number Generator Test: Functional testing of ring oscillators and LFSR is performed.

    d) Critical functions test: Test of on-chip Real Time Clock.

    e) RAM Test: Functional test of RAM memory.

13. Conditional Tests.

    a) Pairwise consistency tests: Test not performed.

    b) Software/firmware load test: A load test is performed.

    c) Continuous random number generator test: A random number generator test is performed once upon every functional access of the random number generator (once regardless of the length of the random number needed.).

14. The following initialization of the FORTEZZA card must be accomplished by the SSO before the card will support User cryptographic services.

    a) Install the card’s Ks value.

    b) Change the SSO default PIN phrase.

    c) Load a certificate into certificate index 0.

d) Set the User PIN phrase.

15. Before the card can be used for cryptographic services, the User must successfully log on and select a personality (certificate). Prior to selecting a personality, card services that do not require a user's private key may be selected.

16. When the card is in a Zeroized State, as the result of a Zeroize command or of 10 unsuccessful log on attempts, the SSO must use the Zeroize PIN phrase to log on. All card parameters must then be reinitialized.

5. Security Relevant Data Items

The Security Relevant Data Items (SRDIs) are defined below.

Certificate: An internal data structure containing public X.509 certificate plus private KEA and DSA information about a User. The structure of the FORTEZZA version of the X.509 certificate is defined in the FORTEZZA Application Implementors Guide, Document # PD4002103-1.01.

Cipher mode: Selected cipher mode (ECB, CBC, OFB, or CFB).

Data: Plain text or Cipher text data.

g parameter: One of the parameters used with the KEA and DSA.

Hash: Value produced by "digesting of a message" using the NIST Secure Hash Algorithm (SHA-1).

Manufacturer Default PIN: The SSO PIN phrase that must be entered to log-on to the card when it is first received from the manufacturer.

Message Encryption Key (MEK): Key generated by the card's random number generator, used for encrypting/decrypting message data.

Message Initialization Vector (IV): This is a 64 bit random number used to initialize the SKIPJACK encryption algorithm. The algorithm is initialized with a unique IV for each message encrypted.

p parameter: A prime number used in the KEA and DSA.

q parameter: A prime divisor used in the KEA and DSA.

r value: One of two parameters used in DSS to define a digital signature (s is the other).

Ra: A random number generated by the message originator in a KEA key exchange.

Rb: A random number received from the message recipient in a direct-connection key exchange.

Real Time Clock (RTC): Date and time maintained by the on-board real-time clock. Only the SSO can set (advance or stop) the RTC.

s value: One of two parameters used in DSS to define a digital signature (r is the other).

SSO Role PIN: The PIN phrase that must be input to enter the SSO role.

Status: Current module state, mode & personality status.

Token Encryption Key (TEK): Generated by the KEA. Used to wrap key.

User Role PIN: The PIN phrase that must be input to enter the User role.

User Storage Key Variable (Ks): Stored in Register 0 after a successful user Check PIN phrase.

User's Private Key (X): This is the private part of the Public/Private key pair used in the Key Encryption Algorithm (KEA) and the DSA.

User's Public Key (Y): This is the public part of the Public/Private key pair used in the Key Encryption Algorithm and the DSA.

Zeroize Default PIN: The SSO PIN phrase that must be entered to log-on to the card once it has been zeroized.

6. Modes of Access

Terms used in the Modes of Access column of Table 3 are described below:

Clear (index#): Clear SRDI at register index # n.

Generate: The SRDI is generated by the card.

Initialize: Hash function command.

Initiate/Continue: Hash function commands

Input: Data input to the card via the Data In Block.

Input (index#): Input SRDI into register index # n.

Output: Data output from the card via the Data Out Block.

Output (index#): Output of SRDI from register index # n.

Select: Selection of parameters or mode.

Select (index#): Selection of a key or certificate from index # n.

Store: The SDRI is stored in the Crypto Card

Unwrap: Decrypt one key with a different key.

Wrap: Encrypt one key with a different key.

Zeroize: A process that clears User and SSO PIN phrases, and other memory on the card, as required.

The host application program and the FORTEZZA Crypto Card communicate by means of a shared memory interface consisting of a Command Block, a Data-In Block and a Data-Out Block. The application places a Command Block at the start address of the card's shared memory. The Command Block is made up of six fields: Command, Pointer to Next Command Block, Pointer to Data-In, Pointer to Data-Out, Response, and Channel Specifier. The Data-In Block is used to provide input data to commands executed on the card. The Data-Out Block is used to provide output data to the application program. Keys are stored in Key Registers which the host selects based upon their Key Register Index Identifier. The card contains storage for 10 keys identified by Key Register Index 0 through 9. The card contains storage for certificates including one SSO certificate and multiple User certificates. These are stored according to a certificate index.

7. User & SSO Services vs SRDIs vs Modes of Access

The relationships between User and SSO Services, SRDIs and Modes of Access to SRDIs are shown in Table 3.

Table 3, Services vs SRDIs vs Modes of Access

Service	SRDI	Modes of Access	SSO Role	User Role
Change PIN Phrase	PIN (current) PIN (new) SSO/User type Ks	Input Input Input Unwrap, wrap	X	
Check PIN Phrase	PIN Ks p, q & g parameters	Input Unwrap, move to reg 0 Select	X	X
Decrypt	Data - cipher text Data - plain text	Input Output	X	X
Delete Certificate	Certificate	Clear (index#)	X	X
Delete Key	MEK	Clear (index#)	X	X
Encrypt	Data - plain text Data - cipher text	Input Output	X	X
Extract X	Selected X-value	Output (TEK wrapped X value)	X	
Firmware Update	Fortezza F/W	Replace	X	
Generate IV	IV data	Generate, output	X	X
Generate MEK	MEK	Generate, store	X	X
Generate Ra (Ra is used in generation of TEK)	Ra	Generate, output	X	X
Generate Random No.	Random number	Generate, output	X	X
Generate TEK (TEK used in Encrypt, Decrypt, Wrap)	Ra or Rb Yb or Ya TEK p, q and g	Input Input Generate, store Select	X	X
Generate X	X-value Y-value p,q, & g parameters certificate	Generate, wrap, store Generate, output,store Input Select(index#)	X	X
Get Certificate	Certificate	Output (index#)	X	X
Get Hash	Hash (value)	Output (hash value)	X	X

Service	SRDI	Modes of Access	SSO Role	User Role
Get Personality List	Certificates	Output (all certificate names in memory)	X	X
Get Status	Status (state, mode, personality)	Output (status)	X	X
Get Time	RTC	Output (date/time)	X	X
Hash	Hash (function)	Initiate/continue	X	X
Initialize Hash	Hash (function)	Initialize (per SHA-1)	X	X
Install X (used to restore an archived X-value	X-value Yb p,q, & g parameters	Input Input Input	X	X
Load Certificate	Certificate	Input (index#)	X	X
Load DSA Parameters	p, q & g parameters	Input (index #)	X	X
Load Initialization Value	Random seed value Ks (user key)	Input Input, wrap	X	
Load IV	IV data	Input	X	X
Load X	X p,q, & g parameters Y generated value	Input (index#) Input (index#) Output	X	X
Relay	X-value Ra Ya (extractor) Yb (installer) TEK	Input, unwrap, wrap Input, generate new Input Input Generate (for unwrap, Gen. new (for wrap)	X	X
Restore	Crypto state (hash, encrypt, or decrypt)	Input (hash-value, or encrypt /decrypt state)	X	X
Save	Crypto state (hash, encrypt, or decrypt)	Output, Store (hash-value, or encrypt or decrypt state)	X	X
Set Key	MEK	Select (index#)	X	X
Set Mode	Cipher mode (ECB /CBC/OFB/CFB)	Select (cipher mode)	X	X
Set Personality	Certificate	Select (index#)	X	X
Set Time	RTC	Input (date/time)	X	

Service	SRDI	Modes of Access	SSO Role	User Role
Sign	Hash (value) p, q & g r value s value	Input Select Output Output	X	X
Timestamp	Hash value p, q, & g r value s value RTC (signed)	Input Select Compute, output Compute output Output	X	X
Unwrap Key	TEK MEK	Select(index#) Select(index#),unwrap	X	X
Verify Signature	Hash value p, q & g r value s value Y value (originator)	Input Select Input Input Input	X	X
Verify Timestamp	p, q, & g Hash Value r value s value RTC (signed)	Select Input Input Input Input	X	X
Wrap Key	TEK MEK	Select (index#) Select (index#),wrap	X	X
Zeroize	Card data & internal buffers	Zeroize	X	X