Smart Guardian FIPS Cryptographic Module

Security Policy

Document *Version 1.1*

Gemalto, Inc.

Revision Date 11/16/09

TABLE OF CONTENTS

1. Module Overview

The Smart Guardian FIPS (HW P/Ns HWP117762 Version A, HWP117763 Version A, HWP118770 Version A, HWP118771 Version A; FW Version 1411) is a portable device which provides a robust security for data protection. The Smart Guardian FIPS is a multi-chip embedded cryptographic module, as defined by FIPS 140-2, and consists of Lexar FC4410-VF-AB or AC controller, Gemalto .NET Smart Card v2+ for SEG Lite FIPS (T1008016) based on Infineon SLE88 CFX4000P Secure IC Chip, Flash Memory (s), and some non-security related discrete components. The entire cryptographic boundary is encapsulated in a hard, opaque epoxy to provide Level 3 physical security. Lexar FC4410 USB Controller employs validated Federal Information Processing Standard (FIPS 140-2) 256-bit AES engine for on-the-fly encryption and decryption of data stored on the flash memories and SHA 256 for computing digests. Gemalto Smart Card provides key management, authentication and signature validation.

Figure 1 –Smart Guardian FIPS

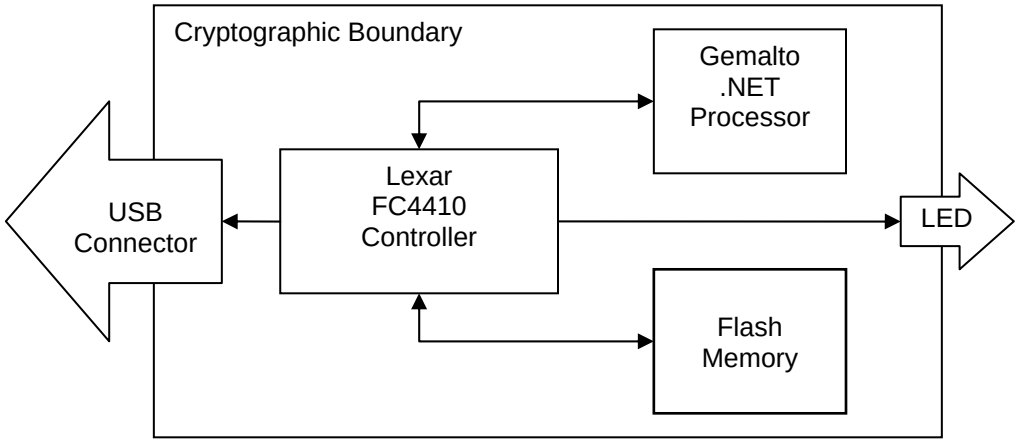

Figure 2 – Diagram for Smart Guardian FIPS

2. Security Level

The cryptographic module meets the overall requirements applicable to a Level 3 multi-chip standalone FIPS 140-2 Cryptographic Module.

Table 1 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module 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
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

The cryptographic module supports FIPS Approved algorithms as follows:

Security Functions	Cert #.	Description
AES	990, 877	CBC/ECB Encryption and Decryption
TDES	719	CBC/ECB Encryption and Decryption
RNG	503	ASNI X9.31 RNG
SHA-1	869	Hashing algorithm
SHA-256	957, 869	Hashing algorithm
HMAC-SHA-1	491	Keyed hashing algorithm
RSA(1024 and 2048)	424	Sign\Verify (PKCS #1.5) with SHA-1

The module supports the following non-Approved algorithms allowed for use in the Approved mode of operation.

- AES Key Wrap (The key establishment methodology provides 192 bits of encryption strength)
- RSA encrypt/decrypt (The key establishment methodology provides 80 or 112 bits of encryption strength)
- TRNG (NDRNG) used to provide seeding for the Approved RNG

The module as configured employs the following algorithms for security functions:

- AES 256 bit encryption/decryption
- AES 192 bit for Key Wrapping
- SHA-1
- RSA 1024 (PKCS #1.5) signature verification
- ANSI X9.31 RNG and NDRNG
- Triple-DES

Non-Approved mode of operation

The module does not support a non-Approved mode of operation.

4. Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

Ports	Interface
USB - Type A	Data Input, Data Output, Status Output, Control Input, Power
LED	Status Output

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module shall support three operator roles User, Card Administrator (Crypto-Officer), and Storage Administrator. The cryptographic module shall enforce the authentication of roles using identity-based operator authentication. Each of the Card Administrator and Storage Administrator roles has its own administrator key and key encryption key. The administrator roles use a challenge/response-based authentication mechanism.

Table 2 – Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Card Administrator (Crypto-Officer)	Identity-based	Card Admin Key: The module stores the unique key in the secure memory of the smart card.
Storage Administrator	Identity-based	Storage Admin Key: The module stores the unique key in the secure memory of the smart card.
User	Identity-based	Unique PIN: The module stores the PIN in the secure memory of the smart card.

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Administrators Challenge/Response. The Admin Key is 24 bytes long. The challenge and response are each 8 bytes long.	With 8 bytes challenge and response, respectively, the probability that a random attempt will succeed or a false acceptance will occur is $1/2^{64}$ = $1/(1.84x10^{19})$, which is less than 1/1,000,000. The admin authentication takes about 0.125s. The maximum number of tries in one minute is 60/0.125 = 480. The probability of successfully authenticating to the module through random attempts within one minute is $480/2^{64}$ =

	$2.61x10^{-17}$, which is less than 1/100,000.
User PIN: Character set: alphanumeric letters – total of 94 different letters • 26 characters – upper/lower cases – total of 52 • 10 digits • Special characters – total of 32 (`, ~, !, @, #, $, %, ^, &, *, (,), -, _, =, +, [, {,], }, \, |, ;, :, ‘, “, ,, <, ., >, /, ?) Minimum length: 4 Maximum length: 256	The probability that a random attempt will succeed or a false acceptance will occur is $1/94^n$, where n the number of characters in the PIN. When n=4, the minimum PIN length, $1/94^4$ = 1/78,074,896, which is less than 1/1,000,000. The user authentication takes more than 2.5s. The maximum number of tries in one minute is 60/2.5 = 24. For n = 4, the probability of successfully authenticating to the module through random attempts within one minute is less than $24/94^4 = 0.0307 \times 10^{-5}$, which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Non- Authenticated	Card Admin.	Storage Admin.	User	Service	Description
X	X	X	X	Set Language	Select the desired language on first time token use as well as subsequent uses.
X	X	X	X	Data Read Plaintext	Allows the User to read data from unencrypted partition
X	X	X	X	Data Write Plaintext	Allows the User to write data to unencrypted partition
X	X	X	X	Lock	Prevent access to the encrypted partition by locking that partition zeroizing keys on the data storage controller.
X	X	X	X	User Login	Login as a user.
X	X	X	X	Lock Read Only Partition	Closes data storage read only partition to limit access to partition.
X	X	X	X	Authenticate Administrator	Authenticate Administrator using challenge response protocol
X	X	X	X	Get Status	Access module status available to unauthenticated users
X	X	X	X	Self-Tests	The token is self-tested every time the token is powered up.
X	X	X	X	Generate Connection Hash	Generate a connection digest
X	X	X	X	Token Proof	Prove to external entities that a message is from a valid token.
X	X	X	X	Card Admin Login	Authenticate Card Admin
X	X	X	X	Storage Admin Login	Authenticate Storage Admin
	X	X	X	Logout	Logout of role
	X	X	X	Get Operator Status	Access status available to authenticated operators
	X			Manage Content	Manage smartcard content
	X			De-Provision	Reset the token to its original state before provision.
	X			Provision	Part of the initial token setup that includes setting Card Admin key, Storage admin key; initializing secure

Non- Authenticated	Card Admin.	Storage Admin.	User	Service	Description
					storage on-card application; generating AES key for data encryption; setting public and private partition state.
	X			SC Assembly Update	Update smart card assembly.
	X			Un-Block PIN	Un-block user PIN.
	X			Update KEK	Change Card Admin or User KEK
	X			Update Card Admin Key	Change Card Admin key.
	X			Smart Card Zeroize	Zerorize plaintext CSPs stored on Smart Card component.
		X		Verify Client Signature	Verifies Signature during client application update using a RSA Public key hardcoded into the Secure Storage assembly.
		X		Drive Resize	Change the sizes of public and private partition. All data on the drives is lost as a result of resize operation.
		X		Unlock Read Only Partition	Open data storage read only partition to support content update.
		X		Update Storage Admin KEK	Change Storage Admin KEK
		X		Update Storage Administrator Key	Change Storage administrator key. The GetChallenge must be called before making this call.
		X		Controller Firmware Update	Update firmware for mass storage component.
			X	Change PIN	Allows authenticated user to modify PIN value used for authentication.
			X	Data Read Encrypted	Allows the User to read data from encrypted partition
			X	Data Write Encrypted	Allows the User to write data to encrypted partition
			X	Unlock Encrypted	Enable access to the encrypted partition by unlocking that partition. This requires the user to provide the user PIN.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

The module supports the following CSPs:

- AES Data Storage Key: 256 bit AES key used to protect data in flash
- Card Admin Key: 192-bit Triple-DES key used to authenticate card administrator
- Storage Admin Key: 192-bit Triple-DES key used to authenticate storage administrator
- User PIN: Authenticates User
- Seed and Seed Key: Initializes the RNG
- Card Admin KEK: 192-bit AES key used to wrap the new Admin key, new Admin KEK, User PIN (Unblock), and User KEK during update.
- Storage Admin KEK: 192-bit AES key used to wrap the new storage admin key.
- User KEK: 192-bit AES key used to update PIN

Public Keys:

- Gemalto Assembly Update Public Key: Verify Firmware loading.
- FC4410 Controller Firmware RSA public Key: Verify a Firmware loading.

Definition of CSPs Modes of Access

Table 6 defines services that access CSPs. The modes of access shown in the table are defined as follows:

- **U**se: This operation reads and uses data items for the performance of a service
- **G**enerate: This operation generates a key
- **D**estroy: This operation actively overwrites data items
- **I**mport: This operation accepts the input of data items through the Data Input port
- **O**utput: This operation exports data items through the Data Output port
- **W**rite: Stores information to storage media

Table 5 – Roles & Services with CSP Access Rights

User	Card Admin	Storage Admin	Non-Authenticated	Services	AES Data Storage Key	Card Admin Key	Card Admin KEK	Storage Admin Key	Storage Admin KEK	User PIN	User KEK	Seed and Seed Key
X				Change PIN						IW	U	
X				Data Read Encrypted	U							
X				Data Write Encrypted	U							
	X			Change Card Admin Key		IW	U					
	X			Zeroize Smart Card	D	D	D	D	D	D	D	D
	X			De-Provision	D	D	D	D	D	D	D	D
	X			Provision	G	W	W	W	W		W	
	X			Un-Block PIN		U	U			IW		
		X		Change Storage Admin Key				IW	U			
		X		Drive Resize	G			U				
			X	User Login						U		U
			X	Card Admin Login			U					U
			X	Storage Admin Login			U					U

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable. The module implements a limited operational environment. The module's validation to FIPS 140-2 is not valid if any application is loaded.

8. Security Rules

The cryptographic module's design corresponds to the following security rules.

1. The cryptographic module shall provide services to a single operator with multiple roles. These are the User, the Card Admin and the Storage Admin roles.
2. The module shall support a mutual authentication protocol proving knowledge of a shared secret.
3. An unauthenticated operator shall not be able to modify, substitute, or disclose any cryptographic CSPs or compromise the security of the module.
4. The cryptographic module shall encrypt all user data with a validated AES algorithm.
5. The cryptographic module shall perform the following Power up Self-tests:
    - Cryptographic algorithm tests:
        - AES 256 Enc/Dec KAT
        - SHA-256 KATs
        - TDES Enc/Dec KAT
        - AES Enc/Dec KAT
        - RSA Sign/Verify KAT
        - RSA Encrypt/Decrypt KAT
        - SHA-1 KAT
        - HMAC-SHA-1 KAT
        - ANSI X9.31 RNG KAT
    - Firmware Integrity - EDC
6. The cryptographic module shall perform the following Conditional Tests:
    - ANSI X9.31 RNG and NDRNG Continuous Test
    - Field Firmware Upload Test (Controller – RSA Digital Signature Verification)
    - Firmware Load Test (Gemalto – RSA Digital Signature Verification)
    - RSA pair-wise consistency test
7. The cryptographic module shall perform the following tests
    - Memory Tests
8. The operator shall be capable of commanding the module to perform the power up self-test. The operator will power cycle the module.
9. Prior to each use, the internal RNG shall be tested using the conditional test specified in FIPS 140-2 §4.9.2.

10. Data output shall be inhibited during self-tests and error states.
11. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
12. The module shall not support concurrent operators.
13. The module shall not support the bypass of cryptographic functionality.
14. The module shall not support the manual entry of keys.
15. The module shall not support entry or output of plaintext CSPs.
16. The module shall enforce a timed access protection mechanism that supports a limited number of authentication attempts per minute. After a configurable number of consecutive unsuccessful password validation attempts have occurred, the cryptographic module shall not accept additional validation attempts until reset by an authenticated Crypto-Officer or reset to the manufacturing state.
17. The module shall provide the ability to zeroize all plaintext CSPs. This is performed by initiating the zeroize command for the smart card and locking the token.
18. RSA shall only be used with key lengths greater than or equal to 1024 bits.
19. The module shall only support an Approved Mode of Operation.
20. Additional cryptographic functionality is available upon loading of additional firmware or by firmware update. Note: Any loading of firmware will immediately invalidate the FIPS 140-2 module. There is no assurance provided unless the module is revalidated according to current FIPS PUB 140-2 requirements. The LED will provide status if firmware content has been modified.
21. LED status is available as follows.
    - FIPS Self-Test Failure: The module will output a LED flash pattern at blink rate of 1/3 of a second flash with 50/50 on/off cycle.
    - Configuration modified using firmware load: The module will output a persistent LED flash pattern at blink rate of 1/9th of a second with a 75/25 on/off cycle.

9. Physical Security Policy

Physical Security Mechanisms

The cryptographic module is a multichip standalone device. The module includes the following physical security mechanisms:

- Hard potting material encapsulation and metal enclosure of circuitry.

The only components exposed from the potting material are the USB port and the LED indicator. The module does not support a maintenance access interface.

Table 6 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Potting Material and hard metal enclosure	Once per operator use.	Inspect the token for damage to the enclosure.

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks outside of the scope of FIPS 140-2. This area is noted as not being applicable.

11. Definitions and Acronyms

Term	Meaning
AES	Advanced Encryption Standard
CSP	Critical Security Parameter
DES	Data Encryption Standard
TDES	Triple-DES: Enhanced encryption algorithm based on DES
HMAC	Hashed Message Authentication Code
KAT	Known Answer Test
PKCS#11	PKCS (Public-Key Cryptography System or Cryptoki): API proposed by RSA Labs, which presents a “virtual token” for applications, and management functions to locate and manipulate cryptographic tokens.
PKI	Public Key Infrastructure
POST	Power On Self Test
RSA	Rivest Shamir Adleman
SHA	Secure Hashing Algorithm
USB	Universal Serial Bus