ePass2003 Cryptographic Module

Part No: ePass2003-A2 & ePass2003-X18
Firmware Version No: V1.0.11

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 3
Document Version: V1.0
Date: April 16, 2020

FEITIAN Technologies Co., Ltd.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Purpose

This non-proprietary Security Policy for the ePass2003 cryptographic module by Feitian Technologies Co., Ltd. ("Feitian") describes how the module meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode.

This document was prepared as part of the Level 3 FIPS 140-2 validation of the module. The following table lists the module's FIPS 140-2 security level for each section.

Section	Section Title	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services, and Authentication	3
4	Finite State Model	3
5	Physical Security	3
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	EMI/EMC	3
9	Self-Tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

Table 1 - FIPS 140-2 Section Security Levels

1.2 Background

Federal Information Processing Standards Publication (FIPS PUB) 140-2 – *Security Requirements for Cryptographic Modules* details the requirements for cryptographic modules. More information on the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS), Cryptographic Module Validation Program (CMVP), the FIPS 140-2 validation process, and a list of validated cryptographic modules can be found on the CMVP website:

http://csrc.nist.gov/groups/STM/cmvp/index.html

More information about Feitian Technologies Co., Ltd ePass2003 token can be found on the Feitian website:

https://ftsafe.com/

1.3 Document Organization

This non-proprietary Security Policy is part of the ePass2003 cryptographic module FIPS 140-2 submission package. Other documentation in the submission package includes:

- Product documentation
- Vendor evidence documents
- Finite state model
- Additional supporting documents

2 Module Overview

This document defines the Security Policy for the ePass2003 cryptographic module, hereafter denoted as the Module. The Module is a USB token containing Feitian's own FT-FIPS-COS which is embedded in a Hongsi HS32 Integrated Circuit (IC) chip and has been developed to support Feitian's ePass2003 USB token. The Module is designed to provide strong authentication and identification and to support network login, secure online transactions, digital signatures, and sensitive data protection.

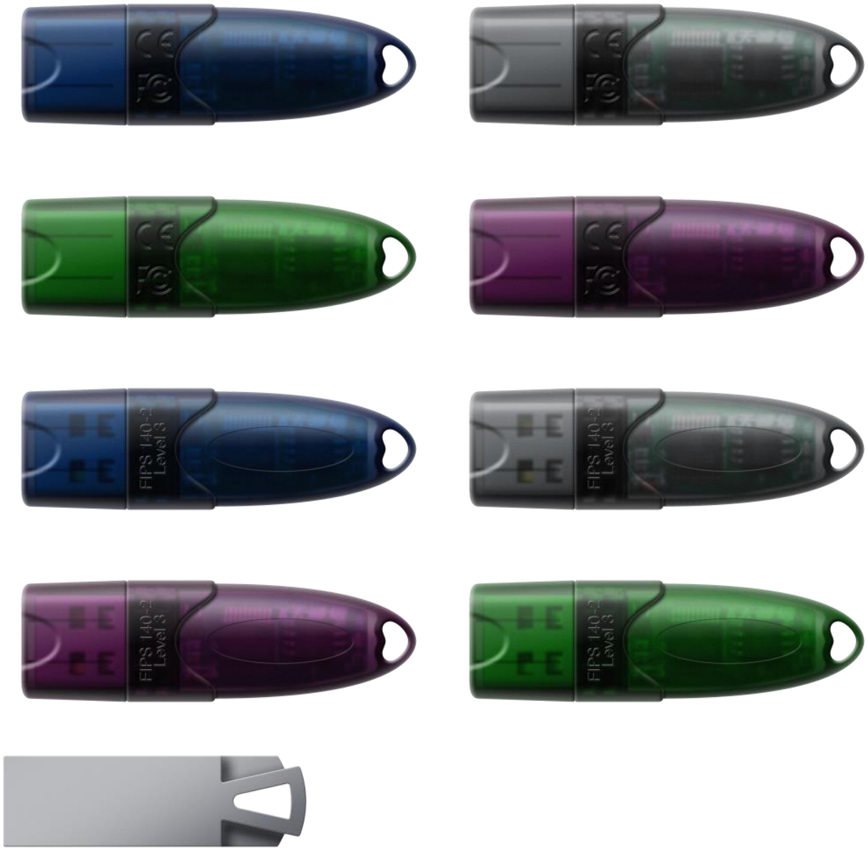

Figure 1 – Feitian ePass Token
ePass2003-A2 (top eight) & ePass2003-X18 (bottom left)

[

2.1 Cryptographic Module Specification

The Module is a hardware module with a multi-chip standalone embodiment. The logical and physical cryptographic boundaries of the Module are defined by the hard, semi-transparent, polycarbonate or metal casing of the USB token. The Module is comprised of a Hongsi HS32 microcontroller sitting atop a Printed Circuit Board (PCB). The PCB carries the signals and instructions of the microcontroller to the other components contained within the Module. All cryptographic functions and firmware are stored within the microcontroller package and executed by a 32-bit CPU (Core Processing Unit).

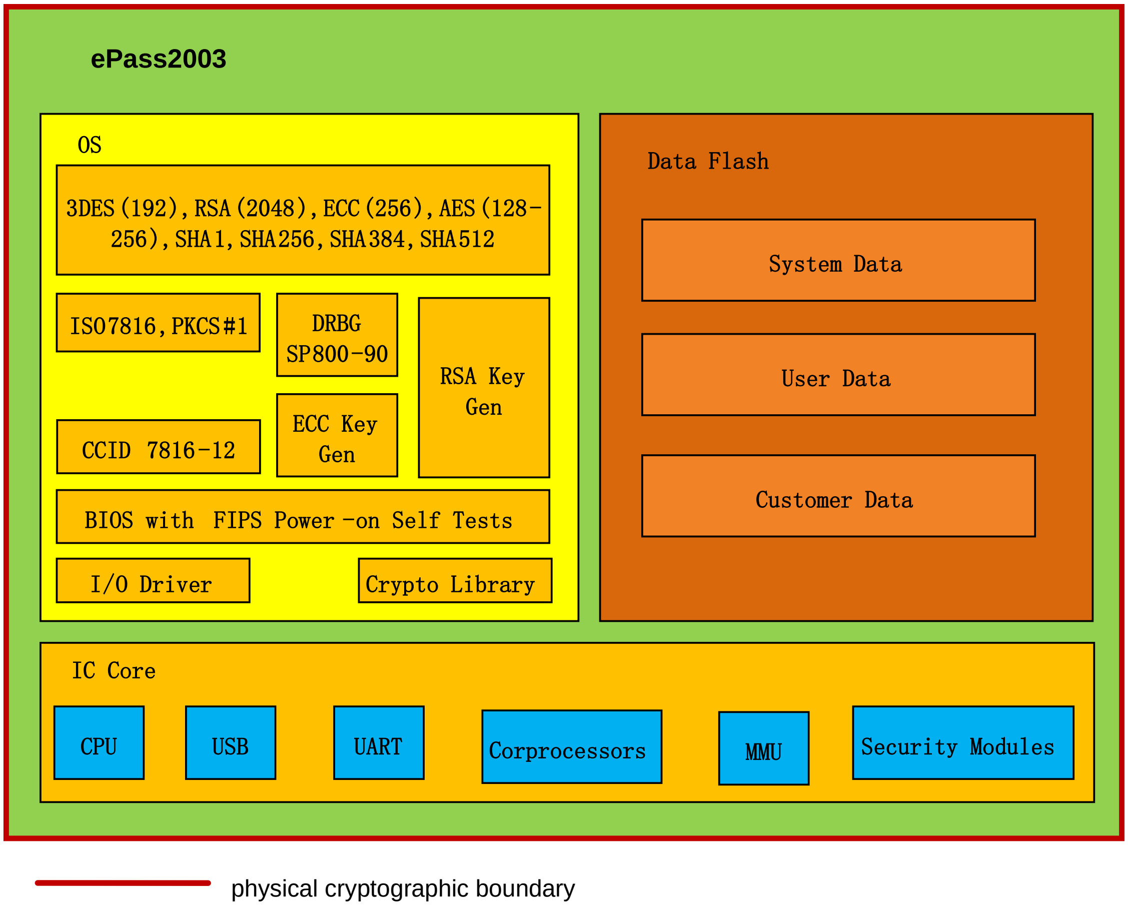

Figure 2 - Physical Block Diagram

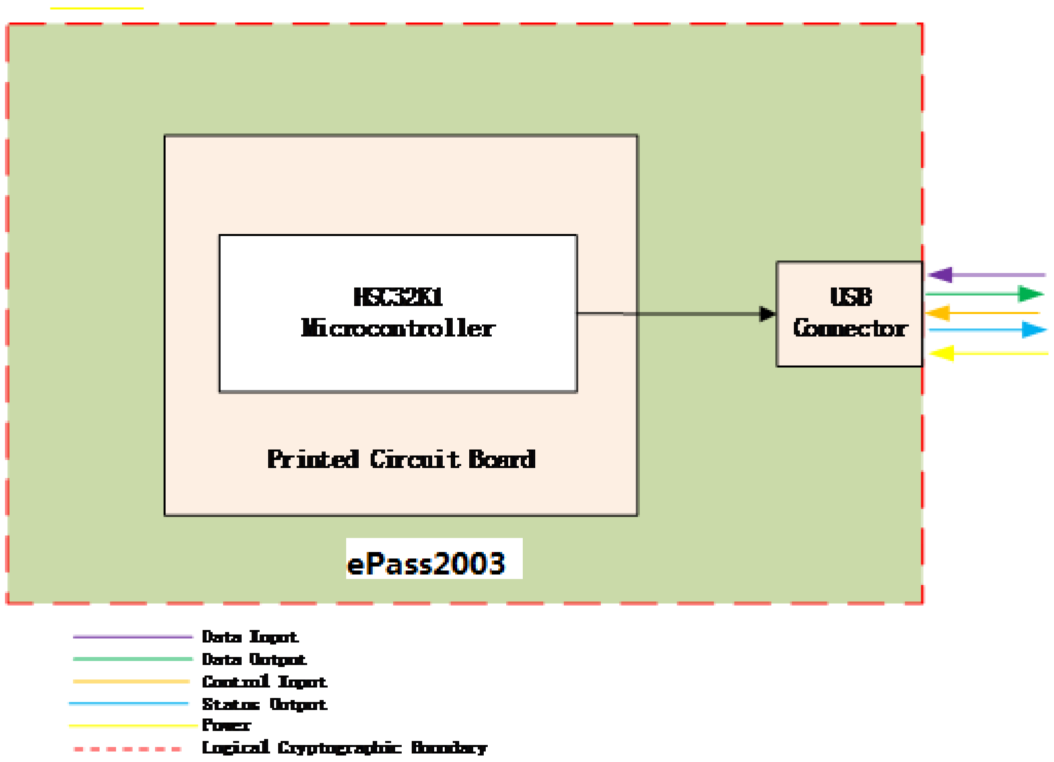

Figure 3 - Logical Boundary

2.2 Cryptographic Module Ports and Interfaces

The Module's ports and interfaces that are supported when operating in FIPS mode are as follows:

- USB port
- LED

Table 2 shows how the Module's physical interfaces map to the logical interfaces defined in FIPS 140-2.

FIPS 140-2 Interface	Physical Interface
Data Input	USB port
Data Output	USB port
Control Input	USB port
Status Output	USB port, LED
Power	USB port

Table 2 - Module Interface Mappings

2.3 Roles &Services

2.3.1 Assumption of Roles

The Module uses identity-based authentication and has the two roles required by FIPS 140-2: Cryptographic Officer (CO) and User(U).

The CO is the role responsible for module initialization, including file system management, key management, and access control management. The User role is the everyday user of the device. An operator's role is explicitly selected to either the CO or User role, depending on the role associated with an operator's key.

2.3.2 Services

All services provided by the Module are implemented in accordance with ISO/IEC 7816-4, which defines the interface available as a command and response pair referred to as an Application Protocol Data Unit (APDU). The Module will process only one command at a time, per channel (of four available logical channels), and must process and respond before allowing another command to be processed over any given channel. Table 3 and Table 4 show a typical APDU command structure and command response structure used by the Module, respectively.

Header					Lc Field	Data Field	Le Field
CLA	INS	P1	P2	(P3)	1 or 2 bytes	Input Data	1 or 2 bytes

Table 3 – APDU Command Structure

APDU command structure descriptions:

CLA – The Class byte indicates the class of the command as follows:

- If the class of the command is inter-industry or not
- If secure messaging is required
- Logical channel 0-3

INS – The Instruction byte indicates the command to process as follows:

- Command word
- Data encoding

P1\P2 –The command parameters.

P3 –When the length of Lc or Le is two bytes, P3 exist and a value of '0'.

Lc – Length in bytes of the data field

Data Field – Data input with command for processing

Le – Maximum number of bytes expected in the response

Data Field	Trailer
Response data	Status bytes

Table 4 – APDU Command Response Structure

All services implemented by the Module under the FIPS-Approved Mode are listed in Table 5 and Table 6 below. Each service description also describes all usage of CSPs by the service.

NOTE 1:

R – Read: The CSP is read.

G – Generate: The CSP is generated or derived.

W – Write: The CSP is modified or zeroized.

X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

NOTE 2:

Authenticated and unauthenticated services are listed in Table 5 and Table 6. If Secure Messaging (SM) is needed when performing a service, Ksenc and Ksmac are used to calculate SM.

NOTE 3:

There are 4 Access Condition (AC) permission bytes associated with each key and the PIN stored in the Module. These bytes define use permission, modification permission, activation permission, and invalidation permission (activation and invalidation permission are associated with the PIN only). For some services, permissions must be set appropriately by the CO during module initialization or the service will fail to execute. The CO updates the Access Condition via the Install Secret service. If specific permissions are required, this is noted within the service descriptions of Table 5 below.

Service	Operator	Description	Input	Output	CSP
Read Binary	CO&U	Allows read access to a binary file. A binary file is a file whose content is a sequential string of bits.	• Offset address of the binary file to read • Length of the data to be read	• File data or "Nonexistent" • Status (e.g. 9000,6283,6A80, 6A81,6A82,6A86)	No CSPs are accessed via this service.
Self Tests	CO & U	Performance of the Power-On Self-Tests	• None	• Status (e.g. 9000,6283,6A80, 6A81,6A82,6A86)	No CSPs are accessed via this service.
Update Binary	CO&U	Allows write access to a binary file.	• Offset address of the binary file to write • Length of the data to be write	• Status (e.g. 9000,6283,6A80, 6A81,6A82,6A86)	No CSPs are accessed via this service.
Read Record	CO&U	Allows read access to a record. A record is a type of data storage structure as defied within ISO 7816. Records are stored in files.	• Record number • Read parameter (i.e., all records starting at specified record number, or just one record)	• Record data or "Nonexistent" • Status (e.g. 9000,6283,6A80, 6A81,6A82,6A86)	No CSPs are accessed via this service.
Update Record	CO&U	Allows write access to a record	• Record number • Length of record • Record data • Read parameter (i.e., update the record specified by the record number)	• Status (e.g. 9000,6283,6A80, 6A81,6A82,6A86)	No CSPs are accessed via this service.
Append Record	CO&U	Allows a record to be append	• Record number • Current file • Length of record • Record data • Read parameter (i.e., update the record specified by the record number)	• Status (e.g. 9000,6283,6A80, 6A81,6A82,6A86)	No CSPs are accessed via this service.

External Authenticate	CO&U	Authenticates an external entity to the cryptographic module. This service may also be used to both authenticate and initiate a secure session with an external entity. NOTE: Prerequisite to this service is the use of Get Challenge service. The key as referenced within the service call exists under the current file.	• Initiate a secure session: • Authentication data of external entity (32 bytes) plus the MAC (8 bytes) Or • Authenticate only: • Algorithm type (AES, Triple-DES,RSA) • Key ID (Key Index) • Length of data in the field • Authentication data (data field)	• Status (e.g. 9000) • Retry number for the referenced key incremented by one. NOTE: If successful this number is then reset to the maximum.	• Managing Key: R,X Initiate a secure session: • INIT_KEYenc: R, X • INIT_KEYmac: R, X • Kenc: R, X • Kmac: R, X • KSenc: G • KSmac: G Or Authenticate Only: • External Auth Key: R, X • RSA Public Key: R, X
Internal Authenticate	CO&U	Authenticate the cryptographic module to an external entity NOTE: In order for this service to be utilized, the external entity must have privileged access to the referenced key.	• Algorithm type (AES, Triple-DES,RSA) • Key ID (Key Index) • Length of data in the field • Random data (data field)	• Authentication data • Status (e.g. 9000,6300,62CX, 6984,6A81,6A86, 6A88)	• Managing Key: R, X • Internal Auth Key: R, X • RSA Private Key: R, X
Verify	CO&U	Provides PIN verification. NOTE: In order for this service to be utilized, the external entity must have privileged access to the referenced PIN.PIN access is associated by identity; an external entity authenticated to identity A cannot access a PIN associated with identity B.	• Reference to the PIN • PID • Data to be verified	• Status (e.g. 9000,6300,63CX, 6700,6982,6A86, 6A88)	• Managing Key: R, X • PIN: R, X
Change Reference Data	CO&U	Modify the PIN NOTE: In order for this service to be utilized the external entity must have privileged access to the referenced PIN.	• Old PIN • New PIN • Reference to the PIN • PID	• Status (e.g. 9000,6300,63CX, 6700,6982,6A86, 6A88)	• Managing Key: R, X • PIN: R, W, X
Enable Verification Requirement	CO&U	Modifies a PIN’s State from invalid to valid. NOTE: Utilization of this service requires permission to activate the PIN.	• Reference to the PIN • PID	• Status (e.g. 9000,6300,63CX, 6700,6982,6A86, 6A88)	• Managing Key: R, X • PIN: R, W
Disable Verification Requirement	CO&U	Modifies a PINs State from valid to invalid. NOTE: Utilization of this service requires permission to invalidate the PIN.	• Reference to the PIN • PID	• Status (e.g. 9000,6300,63CX, 6700,6982,6A86, 6A88)	• Managing Key: R, X • PIN: R, W

Reset Retry Counter	CO&U	Resets the retry counter of the PIN to its initial value. NOTE: Utilization of this service requires permission to modify the PIN.	• Reset parameter (resets recount maximum number and remaining count to default) • Reference to PIN • PID	• Status (e.g. 9000,6300,63CX, 6700,6982,6A86, 6A88)	• Managing Key: R, X • PIN: R, W
Generate Asymmetric Key Pair	CO&U	Generates an Asymmetric key pair	• Key parameter information • Algorithm ID • Modules length • Private key file Identifier and public key file identifier(FID)	• Status (e.g. 9000,6581,6700,6982,6984,6A80,6A86)	• Managing Key: R, X • RSA Private Key: G • RSA Public Key: G • ECDSA Private Key: G • ECDSA Public Key: G • DRBG Entropy Input: G, R, W, X • DRBG Seed Value: G, R, W, X • DRBG V Value: G, R,W, X • DRBG Key Value: G, R, W, X Note: generation of DRBG Entropy Input, Seed value, V value and Key value only occurs if the DRBG is being reseeded.
Encrypt	CO&U	Performs an encrypt operation using an Approved security function. NOTE: The MSE service must have previously been utilized to choose the algorithm and key for the security operation.	• Plaintext data	• Ciphertext data • Status (e.g. 9000,6700,6982,6984,6A80,6A86)	• Managing Key: R, X • Symmetric Key: R, X
Decrypt	CO&U	Performs a decrypt operation NOTE: The MSE service must have previously been utilized to choose the algorithm and key for the security operation.	• Ciphertext data	• Plaintext data • Status (e.g. 9000,6700,6982,6984,6A80,6A86)	• Managing Key • : R, X • Symmetric Key: R, X
Verify Digital Signature	CO&U	Verifies a digital signature using RSA PKCS#1 or ECDSA NOTE: No security is being claimed for verifying an ECDSA signature.	• Data Object of the signed data plus the digital signature	• Status of the verification	• Managing Key: R, X • RSA Public Key: R, X • ECDSA Public Key: R, X
Generate Digital Signature	CO&U	Generates a digital signature using RSA PKCS#1 or ECDSA. NOTE: No security is being claimed for generating an ECDSA signature.	• Input data for generating the digital signature	Digital Signature	• Managing Key: R, X • RSA Private Key: R, X • ECDSA Private Key: R, X

Verify Cryptographic Checksum	CO&U	Performs AES CMAC verification.	- Plaintext data object plus the cryptographic checksum data	- Status (e.g. 9000,6300)	- Managing Key: R, X - Symmetric Key: R, X
Compute Cryptographic Checksum	CO&U	Compute AES CMAC.	- The data used to compute the checksum	- Cryptographic checksum	- Managing Key: R, X - Symmetric Key: R, X
Create File	CO	Create a file.	- File control parameters (data field) - Length of the data field	- Status (e.g. 9000,6A80.6A84, 6A86)	No CSPs are accessed via this service.
Delete File	CO	Delete a File.	- File ID	- Status (e.g. 9000,6A80.6A84, 6A86)	No CSPs are accessed via this service.
Terminate Card	CO	Terminates all applications on the Module. The Managing Key is zeroized when this service is called, causing all stored keys and CSPs to be inaccessible.	- None	- None	- Managing Key: W
Install Secret	CO	This service is used to enter AES keys, Triple-DES keys, and PINs. CSPs which may be entered are as follows: - Kenc - Kmac - Internal Auth Key - External Auth Key - Symmetric Key - PIN	- Encrypted PIN or Key data - “Final” secret or “Not Final” secret flag	- Status (eg.9000,6700,6982,6986,6A82,)	- Managing Key: R, X - Kenc: W - Kmac: W - Internal Auth Key: W - External Auth Key: W - Symmetric Key: W - PIN: W - KSenc: R, X - KSmac: R, X
Update Key	CO	Allows the updating of the INIT_KEYs or secret file keys.	- INIT_KEYs - Secret Key data - New error counter plus the key value	- Status (eg.9000,6700,6982,6986,6A82,)	- Managing Key: R, X - INIT_KEYenc: W - INIT_KEYmac: W - Kenc: W - Kmac: W - Internal Auth Key: W - External Auth Key: W - Symmetric Key: W
Get File List	CO&U	Allows the reading of the FID list of child files of the current file.	- None	- FID list or “Nonexistent” - Status (eg. 9000,6700,6982)	No CSPs are accessed via this service.
Read Public Key	CO&U	Allows the output of a public key.	- FID of the public key - Public Key component read parameter	- Public Key data or “Nonexistent” - Status (eg.9000,6700,6982,6984,6A82)	- Managing Key: R, X - RSA Public Key: R - ECDSA Public Key: R

Import RSA Key	CO&U	Allows the input of a RSA Key.	• Encrypted key data • FID of the RSA Key.	• Status (eg. 9000, 6700, 6982, 6A82)	• Managing Key: R, X • RSA Private Key: W • RSA Public Key: W • KSenc: R, X • KSmac: R, X
Import ECDSA Key	CO&U	Allows the input of an ECDSA key	• Encrypted key data • FID of the ECDSA Key.	• Status (eg. 9000, 6700, 6982, 6A82)	• Managing Key: R, X • ECDSA Private Key: W • ECDSA Public Key: W • KSenc: R, X • KSmac: R, X

Table 5 - Authenticated Services

Service	Operator	Description	Input	Output	CSP
Put Data	CO&U	Allows data to be received and stored by the Module. In the Put Data service, only the OEM information is allowed to be set.	• Data object tag which indicates OEM info, followed by up to 32 bytes of OEM info • Length of object data	• Status (eg. 9000, 6700, 6A80,6A86	No CSPs are accessed via this service.
Get Data	CO&U	This service allows data to be retrieved. Data refers to global data, which belongs to the Module, such as the serial number, OEM information, and chip information (which includes algorithm support and RAM size). This service is used to obtain the FIPS Mode indicator as described in Section 2.14 of this Security Policy.	• Data object tag (e.g. '80' which indicates card serial number)	• Content of object • Status (e.g. 9000,6a80,6a86)	No CSPs are accessed via this service.
Get Challenge	CO&U	Requests a random value that will be used as a challenge within the External Authenticate service.	• None	• Random Value • Status (e.g. 9000, 6A86)	• DRBG Key Value: X • DRBG V value: X
Manage Security Environment (MSE)	CO&U	Prepares the Module for the subsequent commands, Perform Security Operation.	• CRDO • Algorithm Reference • Key Reference • File Reference • Length of CRDOs	• Status (e.g. 9000,6982,6A81 ,6A82,6A86)	No CSPs are accessed via this service.
Select	CO&U	Allows the selection of a specified file.	• File identifier • Dedicated file Name • File path starting at master file • File path starting at dedicated file	• File control information • Status (e.g. 9000,6a80,6A82 ,6A86)	No CSPs are accessed via this service.

Service	Operator	Description	Input	Output	CSP
Manage Channel	CO&U	Allows the assignment, opening, and closing of a logical channel. A logical channel is a logical link between the host system and a file on the smart card.	• Number of logical channel to be assigned, opened, or closed	• Status (e.g. 9000, 6283, 6A80, 6A81,6A86)	No CSPs are accessed via this service.
Hash	CO&U	Performs a hash using SHA-1, SHA-256, SHA-384, or SHA-512.	• Input data	• Hash result or none	No CSPs are accessed via this service.
Change ECDSA Parameters	CO&U	Allows the change of the default value of the P-256 elliptic curve parameter. This service is only available during module initialization. It is the operator's responsibility to either use a NIST-Approved parameter as specified in FIPS 186-4 Appendix D or generate the parameter according to FIPS 186-4 Section 6.1.1.	• The value of the P-256 elliptic curve parameter.	• Status (e.g. 9000)	No CSPs are accessed via this service.

Table 6 - Unauthenticated Services

2.4 Authentication Mechanisms

Please see Table 7 for details regarding the authentication mechanism.

Authentication Type	Authentication Data	Justification
Identity-based	128-bit AES Key Challenge-Response	The AES key is 128 bits in length. The probability that a random attempt will succeed or that a false acceptance will occur is no greater than $1/2^{128}$, which is less than 1/1,000,000. The Module will allow a maximum of 600 authentication attempts in a one minute period. Therefore, the random success rate for multiple retries in one minute is 600/2^128, which is less than 1/100,000.
Identity-based	3-key Triple-DES Challenge-Response	Three-key Triple-DES has an encryption strength of 112 bits. Assuming a block size of 64 bits, the probability that a random attempt will succeed or that a false acceptance will occur is no greater than 1/2^64, which is less than 1/1,000,000. The Module will allow a maximum of 600 authentication attempts in a one minute period. Therefore, the random success rate for multiple retries in one minute is 600/2^64, which is less than 1/100,000.
Identity-based	RSA Digital Signature	The Module supports RSA public key authentication. Using conservative estimates and equating 2048-bit RSA w/ SHA-256 to 112-bits of strength, the probability for a random attempt to succeed is 1/2^112, which is less than 1/1,000,000. The Module will allow a maximum of 600 authentication attempts in a one minute period. Therefore, the random success rate for multiple retries in one minute is 600/2^112, which is less than 1/100,000.
Identity-based	PIN	The Module supports PIN verification. The Module enforces a PIN length of 6 to 16 bytes, without checking for a particular encoding. Therefore, the probability that a random attempt will succeed is no greater than 1/2^48, which is less than 1/1,000,000. The Module will allow a maximum of 600 authentication attempts in a one minute period. Therefore, the random success rate for multiple retries in a one minute period is 600/2^48, which is less than 1/100,000.

Table 7 – Authentication Mechanism

2.5 Physical Security

The Module is made of a completely hardened, production-grade polycarbonate or metal. The colored polycarbonate or metal enclosure obscures a clear view of the hardware components within. A hard, non-malleable metal casing surrounds the USB connector. The casing is made of hard, production-grade, black, opaque plastic.

The coloring of the Module obscures any visible writing on the PCB. The visible critical components within the Module are further covered to meet FIPS 140-2 level 3 physical security requirements. The HS32 microcontroller is covered with a black, opaque, tamper-resistant, epoxy encapsulate, thus completely covering all critical cryptographic components from plain view. The USB connector located outside of the casing of the USB token is made of a hard, black, opaque, production grade plastic and prevents access to the rest of the USB token. Any attempt at removal or penetration of the enclosure has a high probability of causing serious damage to the Module and the hardware components within the enclosure, which will reveal clear tamper evidence. Removal of the metal surrounding the USB connector will result in the physical damage of the USB connector and its associated pins, rendering the entire cryptographic module useless. If the USB connector is exposed, there is no power going to the USB token. Once power is removed from the cryptographic module, all plaintext keys and unprotected CSPs are zeroized.

2.6 Operational Environment

The operational environment requirements do not apply to the Module, as it only supports a limited operational environment.

2.7 Cryptographic Key Management

2.7.1 Algorithm Implementations

A list of FIPS-Approved algorithms implemented by the Module can be found in Table 8.

Algorithm	Modes and Key Sizes	Validation Number
AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC Key sizes: 128, 192, 256 bits	C1061
CKG	[SP 800-133]	Vendor affirmed

	Functions: Cryptographic Key Generation Symmetric cryptographic keys are generated by the direct unmodified output of the module’s NIST SP 800-90A DRBG. The DRBG output is also used as a seed for asymmetric key generation.	
AES CMAC	[SP 800-38B] Functions: Generation, Verification Key sizes: AES with 128,192,256 bits	C1061
CVL	ECDSA Signature Generation Component P-256 w/ SHA-256	C1061
DRBG	[SP 800-90A] Functions: CTR DRBG Option: Triple-DES 192-bits (3-key) Security Strength: 112	C1061
ECDSA	[FIPS 186-4] Functions: Key Pair Generation, Signature Generation, Signature Verification Curve/Key size:P-256 w/ SHA-256	C1061
KBKDF	[SP 800-108] Functions: CMAC-based KDF using AES Mode: Counter Key sizes:128,192,256 bits	C1061
KTS	Functions: AES Encryption/Decryption w/ CMAC Key size: 128	C1061
RSA	[FIPS 186-4, ANSI X9.31 (Key Generation) and PKCS #1 v2.1 (PKCS1.5)] Functions: Key Pair Generation, Signature Generation, Signature Verification Key size: 2048 w/ SHA-256, SHA-384 and SHA-512 (sig gen only)	C1061 C1062
SHS	[FIPS 180-4] Functions: Digital Signature Generation except SHA-1, Digital	C1061

	Signature Verification except SHA-1, non-Digital Signature Applications SHA sizes: SHA-1, SHA-256, SHA-384, SHA-512	
Triple-DES	[SP 800-67] Functions: Encryption, Decryption Modes: TECB, TCBC Key size:192-bits (3-key)	C1061

Table 8 - FIPS-Approved Algorithm Implementations

A list of non-Approved but Allowed algorithms implemented by the Module can be found in Table 9.

Algorithm	Modes and Key Sizes
NDRNG	[Annex C] Hardware Non-Deterministic RNG; NDRNG output is used to seed the FIPS Approved DRBG. The estimated amount of minimum entropy provided by the NDRNG is 167.16615 bits.

Table 9 - Non-Approved but Allowed Algorithm Implementations

2.7.2 Key Management Overview

Key or CSP	Usage	Storage	Generation	Input	Output	Zeroization	Access
Managing Key	192-bit AES key, used to encrypt CSPs and keys.	Flash, plaintext	This key is generated using the Approved SP800-90A DRBG.	No	No	Zeroized by Terminate Card command	CO&U
INIT_KEYenc	AES 128-bit key, used to derive a session key which is then used to encrypt/decrypt data over a secure session between an authorized external entity and the Module.	Flash, ciphertext, encrypted by managing key	This key is not generated within the Module.	This key is factory-set.	No	Can't be used any more when the Managing key is zeroized.	CO
INIT_KEYmac	AES CMAC 128-bit key, used to derive a session key which is then used to authenticate an operator or data over a secure session between an authorized external entity and the Module.	Flash, ciphertext, encrypted by managing key	This key is not generated within the Module.	This key is factory-set.	No	Can't be used any more when the Managing key is zeroized.	CO

Key or CSP	Usage	Storage	Generation	Input	Output	Zeroization	Access
Symmetric Key	AES 128/192/256-bit or Triple-DES 192-bit key , used to encryption/decryption data, or within a symmetric MAC algorithm (AES CMAC) to generate authentication data	These keys are encrypted by managing key and stored in flash in secret file used to store symmetric keys and PINs.	This key is not generated within the Module.	Install secret command	No	Can't be used any more when the Managing key is zeroized.	CO&U
Internal Auth Key	AES 128/192/256-bit, Triple-DES 192-bit or RSA 2048-bit private key, used to authenticate the Module to an external entity.	These keys are encrypted by managing key and stored in flash in secret file used to store symmetric keys and PINs.	This key is not generated within the Module.	Install secret command	No	Can't be used any more when the Managing key is zeroized.	CO&U
External Auth Key	AES 128/192/256-bit, Triple-DES 192-bit or RSA 2048-bit private key, used to modify the security state of the currently selected DF.	These keys are encrypted by managing key and stored in flash in secret file used to store symmetric keys and PINs.	This key is not generated within the Module.	Install secret command	No	Can't be used any more when the Managing key is zeroized.	CO&U
Kenc	AES 128-bit key, used to derive a session key which is then used to encrypt/decrypt data over a secure session between an authorized external entity and the Module.	These keys are encrypted by managing key and stored in flash in secret file used to store symmetric keys and PINs.	This key is not generated within the Module.	Install secret command	No	Can't be used any more when the Managing key is zeroized.	CO&U

Key or CSP	Usage	Storage	Generation	Input	Output	Zeroization	Access
Kmac	AES CMAC 128-bit key, used to derive a session key which is then used to authenticate an operator or data over a secure session between an authorized external entity and the Module.	These keys are encrypted by managing key and stored in flash in secret file used to store symmetric keys and PINs.	This key is not generated within the Module.	Install secret command	No	Can't be used any more when the Managing key is zeroized.	CO&U
Personal Identification Number (PIN)	6-16 byte secret used to modify the security state of the currently selected DF.	PINs are encrypted by managing key and stored in flash in secret file used to store symmetric keys and PINs.	PIN is not generated in the Module.	Install secret command	No	Can't be used any more when the Managing key is zeroized.	CO&U
RSA Private Key	2048-bit RSA private key is used to sign data.	They are encrypted by managing key and stored in flash in secret file used to store RSA Private key.	Generated in accordance to FIPS 186-4.	Import RSA key command or generate asymmetric key pair	No	Can't be used any more when the Managing key is zeroized.	CO&U
ECDSA Private Key	256-bit ECDSA private key used to sign data.	They are encrypted by managing key and stored in flash in secret file used to store ECDSA Private key.	Generated in accordance to FIPS 186-4.	Import ECDSA key command or generate asymmetric key pair	No	Can't be used any more when the Managing key is zeroized.	CO&U

Key or CSP	Usage	Storage	Generation	Input	Output	Zeroization	Access
KSenc	AES 128-bit key used to encrypt/decrypt data over a secure session	RAM, plaintext	Generated from The INIT_KEYenc or Kenc key as part of the Secure Channel Protocol v03 as specified within Global Platform v2.1.	No	No	Zeroized when power cycle.	CO&U
KSmac	AES CMAC 128-bit key used to authenticate data over a secure session	RAM, plaintext	Generated from the INIT_KEYmac or Kmac key as part of the Secure Channel Protocol v03 as specified within Global Platform v2.1.	No	No	Zeroized when power cycle.	CO&U
DRBG Entropy Input	256-bit input collected from the NDRNG, used to derive the DRBG seed.	RAM, plaintext	Internally generated and associated with an internal module variable.	No	No	Zeroized when power cycle.	CO&U
DRBG Seed Value	232-bit bit seed used for seeding the CTR_DRBG	RAM, plaintext	Internally generated and associated with an internal module variable.	No	No	Zeroized when power cycle.	CO&U
DRBG V Value	Internal CTR DRBG state value is used for SP 800-90A CTR_DRBG (consists of 64 bits)	RAM, plaintext	Internally generated and associated with an internal module variable.	No	No	Zeroized when power cycle.	CO&U
DRBG Key Value	Internal CTR DRBG state value is used for SP 800-90A CTR_DRBG (Consists of 192 bits)	RAM, plaintext	Internally generated and associated with an internal module variable.	No	No	Zeroized when power cycle.	CO&U

Key or CSP	Usage	Storage	Generation	Input	Output	Zeroization	Access
RSA Public Key	2048-bit RSA public key used to verify data	They are encrypted by managing key and stored in flash in secret file used to store ECDSA Private key.	Generated in accordance to FIPS 186-4.	Import RSA key command or generate asymmetric key pair.	Output in plaintext using the Read Public key command.	Can't be used any more when the Managing key is zeroized.	CO&U
ECDSA Public Key	256-bit ECDSA public key used to verify data	They are encrypted by managing key and stored in flash in secret file used to store ECDSA Private key.	Generated in accordance to FIPS 186-4.	Import ECDSA key command or generate asymmetric key pair.	Output in plaintext using the Read Public key command.	Can't be used any more when the Managing key is zeroized.	CO&U

Table 10 - Cryptographic Keys, Key Components, and CSPs

2.7.3 Key Generation& Input

Keys/CSPs generated by the Module:

- Managing Key: 192-bit AES key, which is generated by 192-bit DRBG.
- RSA Key pair: 2048-bit key pair generated in accordance to FIPS 186-4.
- ECDSA Key pair: 256-bit key pair generated in accordance to FIPS 186-4
- KSenc: Using the INIT_KEYenc or KEYenc key with KDF algorithm to get the key.
- KSmac: Using the INIT_KEYmac or KEYmac key with KDF algorithm to get the key.
- DRBG Entropy Input, DRBG Seed Value, DRBG V Value and DRBG Key Value: Using CTR DRBG block cipher DF function to derive 32 bytes from NDRNG to get the DRBG Seed, DRBG Value and DRBG key value.

Keys/CSPs entered into the module by install secret command

- Symmetric Key
- Internal Auth Key
- External Auth Key
- Kenc
- Kmac
- PIN

Keys entered into the Module by an operator:

- External Auth Key
- RSA Key Pair
- ECDSA Key Pair

Keys entered into the Module by vendor during manufacturing:

- INIT_KEYenc
- INIT_KEYmac

2.7.4 Key Output

The following keys/CSPs are never output from the Module:

- Managing Key
- INIT_KEYenc
- INIT_KEYmac
- Symmetric Key
- Internal Auth Key
- External Auth Key
- Kenc
- Kmac
- PIN
- Ksenc
- Ksmac
- RSA Private Key
- ECDSA Private Key
- DRBG Entropy Input

- DRBG Seed Value
- DRBG V Value
- DRBG Key Value

The following keys are output from the Module via some services:

- ECDSA Public Key
- RSA Public Key

2.7.5 Storage

The storage of keys/CSPs are listed in table 10.

2.7.6 Zeroization

The zeroization of keys/CSPs are described in table 10.

2.8 Electromagnetic Interference / Electromagnetic Compatibility

The Module conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

2.9 Self Tests

2.9.1 Power Up Self Tests

There are two flags used to indicate the first command of power up and whether the power up self-tests are passing. The first flag is judged, if this command is the first command of this power up, then power up self-tests are called and the value of the flag is changed. During the process, if any test fails the second flag is assigned to indicate a self-test has failed, otherwise the second flag is assigned to success. The second flag is judged after the process above, if the flag indicates the power up self-tests failed then the Module enters the error state, otherwise the Module will process the command.

On power up, the Module performs self-tests as described in Table 11 below after the first APDU command received. All tests must be completed successfully prior to any other use of cryptography by the Module. If one of the tests fails, the Module enters the error state. Self-tests can be called by an operator at any time by power cycling the Module.

Test Target	Description
AES	KATs: Encryption and Decryption Modes: ECB Key sizes:128 bits
CMAC	KATs: Generation and Verification Key sizes: AES with 256 bits
DRBG	KATs: Triple-DES CTR (Instantiate, Generate and Reseed) Security Strengths: 192-bits
ECDSA	PCT: Signature Generation and Verification Curves/Key sizes: P-256
Firmware Integrity	A 16-bit CRC is performed over FLASH via FW
KDF, using Pseudorandom Functions	KATs: KDF Mode: Counter

Test Target	Description
RSA	KATs: Signature Generation and Signature Verification Key sizes: 2048 bits
RSA CRT	RSA sig gen KAT. RSA CRT sig ver is also tested as part of RSA sig ver KAT
SHA	KATs: SHA-1,SHA-256, SHA-512
Triple-DES	KATs: Encryption and Decryption Modes: TECB Key sizes: 3-key

Table 11 – Power up self tests

2.9.2 Conditional Self Tests

The Module performs the following conditional self tests:

Test Target	Description
NDRNG	NDRNG Continuous Test performed when a random value is requested from the NDRNG.
DRBG	DRBG Health Test performed on startup. Continuous Test performed when a random value is requested from the DRBG.
ECDSA	ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation.
RSA	RSA Pairwise Consistency Test performed on every RSA key pair generation.

Table 12 – Conditional self tests

2.10 Design Assurance

SVN (Subversion) is used by Feitian Information Systems Inc as a software configuration management tool. With its client TortoiseSVN, SVN helps to control revisions of any collection of files and source code stored in a central repository; by configuring the configuration items, the project participants—developing, document writing and testing personnel—maintain all types of data placed into repository.

For additional information regarding design assurance, please refer to the “FIPS_ePass2003_CM”.

2.11 Mitigation of Other Attacks

This section is not applicable. The Module is not intended to mitigate any attacks beyond the FIPS 140-2 Level 3 requirements for this validation.

2.12 Initialization

Please refer to Section 2.13 and 2.14 for information regarding module initialization. For additional information regarding module initialization, please refer to the “FIPS_ePass2003_User Manual”.

2.13 Crypto Officer Guidance

The Module is delivered with a pair of AES Keys (INIT_KEYenc and INIT_KEYmac) to allow authentication and secure initialization of the Module. Initialization of the module into the Approved Mode of Operation is performed by the manufactuer during manufacturing of the Module. All communications to initialize the Module will require a secure session using this key pair which will encrypt and authenticate all data input. During module initialization, the operator at manufacturing shall not invoke the “Change ECDSA Parameters”, using only the P-256 elliptic curve for ECDSA (Given the potential for modification of ECDSA parameters, no security is being affirmed for the generation and verification of ECDSA signatures). The Module will only operate in FIPS mode and provides only FIPS-Approved and allowed functions.

To confirm operation in the Approved Mode of Operation, the operator can issue the “Get Data” command (‘0x00CA018600’, which returns COS related information). If the third return byte of the status output from the “Get Data” command is “0x01”, then the module is operating in the Approved Mode of Operation.

All communication of the module will require a secure session using the Ksenc and KSmac for encrypting and MACing all data input and output.

Operators shall maintain physical possession of the device until keys are zeroized successfully. In this way, the zeroization technique is performed in a time that will not allow the CSPs to be compromised.

2.14 User Guidance

To confirm operation in the Approved Mode of Operation, the operator can issue the “Get Data” command (‘0x00CA018600’, which returns COS related information). If the third return byte of the status output from the “Get Data” command is “0x01”, then the Module is operating in the Approved Mode of Operation.

As a result of the SP 800-67 rev2 transition, the Module limits the number of 64-bit block encryptions with the same Triple-DES key to 2^16. When this threshold is met, the Module no longer supports Triple-DES encryption.

Operators shall maintain physical possession of the device until keys are zeroized successfully (confirmation of successful zeroization is denoted with a return code of “9000”). In this way, the zeroization technique is performed in a time that will not allow the CSPs to be compromised.

3 Acronyms

Acronym	Definition
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
CBC	Cipher Block Chaining
COS	Chip Operating System
CPU	Core Processing Unit
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
CTR	Counter
DES	Digital Encryption Standard
DF	Dedicated File
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FID	File Identification
FIPS	Federal Information Processing Standard
HSCOS	Feitian Chip Operating System
IC	Integrated Circuit
IEC	International Electro technical Commission
ISO	International Organization for Standardization
SM	Secure Messaging
VCC	Voltage (at the) Common Collector

Table 13 - Acronym Definitions