FTDN-030004

FEITIAN Technologies Company, LTD

ePass2003 Token and ePass2003Auto Token FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version: 1.0.11

Date: June 7, 2018

CHANGE RECORD

Revision	Date	Author	Description of Change
1.0.0	July 14, 2014	Xumeng Pang	Initial Draft
1.0.1	August 19, 2014	Xumeng Pang	According to the feedback problems to modify the document
1.0.2	December 24, 2014	Xumeng Pang	According to the feedback problems in mail to modify the document
1.0.3	July 1, 2015	Xumeng Pang	According to the feedback problems in mail on June 30, to modify the document
1.0.4	July 24, 2015	Xumeng Pang	Delete the description of mode conversion
1.0.5	March 3, 2016	Xumeng Pang	Add CMAC and KDF description
1.0.6	April 20, 2017	Xumeng Pang	Multiple updates based on open items
1.0.7	May 22, 2017	Xumeng Pang	Affirm some information
1.0.8	September 7, 2017	Xumeng Pang	Finalized for submission to CMVP
1.0.9	February 21, 2018	Xumeng Pang	Modify based on CMVP feedback
1.0.10	June 4, 2018	Xumeng Pang	Modify based on CMVP feedback
1.0.11	June 7, 2018	Xumeng Pang	Modify based on CMVP feedback

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Feitian Technologies Co., Ltd. (“Feitian”) ePass2003 Token and ePass2003Auto Token cryptographic modules, hereafter denoted the Module. The Module is a USB token containing Feitian’s own FEITIAN-FIPS-COS which is embedded in an Infineon M7893 Integrated Circuit (IC) chip and has been developed to support Feitian’sePass2003 USB token. The overall security level of the Module is 3.

The Module is designed to provide strong authentication and identification and to support network login, secure online transactions, digital signatures, and sensitive data protection. The Module is a hardware module with a multi-chip standalone embodiment. The FIPS 140-2 security levels for the Module are as follows:

Table 1 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic 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

The Module implementation is compliant with:

- ISO 7816
- ISO 14443

1.1 Cryptographic Boundary

The logical and physical cryptographic boundaries of the Module are defined by the hard, semi-transparent, polycarbonate casing of the USB token. The Module is comprised of an Infineon M7893 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 16-bit M7893 CPU (Core Processing Unit). The flash component is optional in this module. The ePass2003 Token and ePass2003Auto Token variations are physically identical, except that the ePass2003Auto Token is populated with a flash chip. The flash chip’s only purpose is to autorun the Module when connected to power. The flash chip is therefore excluded from FIPS 140-2 requirements. All other logical functions

take place through the USB connector or the contactless port, covered in Table 2. Please refer to Figure 1 below for a depiction of the physical and logical cryptographic boundary of the Module.

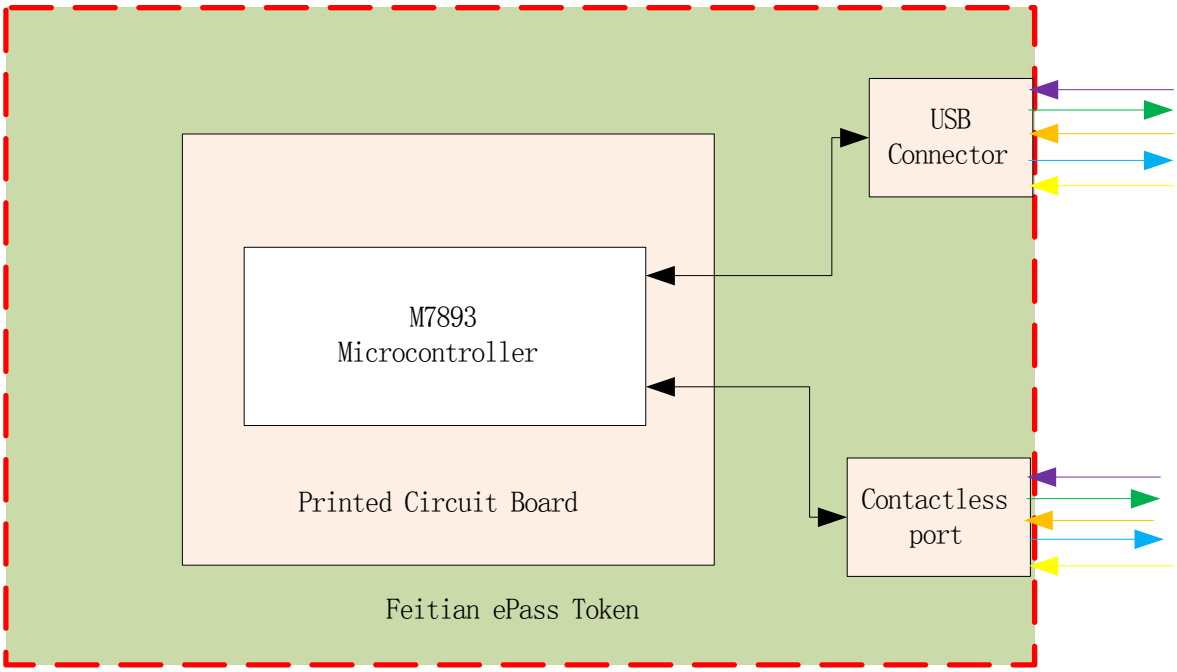

Figure 1 – Physical and Logical Cryptographic Boundary

Figure 2 – ePass2003 Token/ePass2003Auto Token (with and without plastic cap)

Table 2 – Ports and Interfaces

Port	Description	Logical Interface Type
USB Connector	The USB connector contains 4 pins: Data+ (D+), Data- (D-), VCC, and Ground (GND). These 4 pins carry out the logical interfaces as defined by FIPS 140-2	Power | Control in | Data in | Data out | Status out
Contactless Port	The contactless port contains two Advanced Contactless Bridge (ACLB). The data exchange via the ACLB interface.	Power | Control in | Data in | Data out | Status out

1.2 Version and Mode of Operation

Refer to the Module version information in Table 3.

Table 3 – Module Information

Module	HW P/N and Version	FW Version
ePass2003 Token	V2.0	4.0.01
ePass2003Auto Token	V2.0	4.0.01

The Module is configured into the Approved Mode by default in manufacturing. During module initialization, the operator has the opportunity to change the default ECDSA curve in the Module to a different Approved or non-Approved but Allowed curve; an operator shall not change the curve to a non-Approved curve. To verify that the Module is in the Approved mode of operation, an operator can send Get Data and the command shown below. The Module responds with the following information:

Table 4 – Indication Command of Approved Mode

Command and associated elements	Expected Response
GET DATA with P2=86	8001XX8102XX XX8201008302000084 01 XX90 00

Return five data objects in TLV structure:

•The first data object indicates COS mode, TAG value is '80', length byte is '01', the value indicates the mode,0x01 stands for FIPS Approved Mode.

•The second data object indicates whether the algorithm key supports import and export, TAG value is '81', length byte is '02', the value of each two bits of bit0----bit13 correspond to 3DES, AES, RSA Pub, RSA Pri, ECC Pub and ECC Pri, and it also indicates whether these keys can be imported and exported.

•The third data object is reserved, TAG value is '82', length byte is '01'.

•The fourth data object is reserved, TAG value is '83', length byte is '02'.

•The fifth data object indicates ciphertext communication in initialization phase, TAG value is '84', length is '01', the value '01' indicates ciphertext communication.

•9000h APDU status word, indicates the command has performed successfully.

2 Cryptographic Functionality

2.1 Cryptographic Functions

The Module implements the FIPS-Approved Cryptographic Functions shown in Table 5:

Table 5 –FIPS-Approved Cryptographic Functions

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC Key sizes: 128, 192, 256 bits	3327
CKG	[SP 800-133] Functions: - Section 6.1 Asymmetric signature key generation using unmodified DRBG output - Section 7.1 Direct symmetric key generation using unmodified DRBG output	Vendor-affirmed
CMAC	[SP 800-38B] Functions: Generation, Verification Key sizes: AES with 128, 192, 256 bits	3920 (AES)
DRBG[1]	[SP 800-90A] Functions: CTR DRBG Option: Triple-DES-168 (3-key) Security Strength: 112 bits	1564
ECDSA	[FIPS 186-4] Functions: Key Pair Generation, Signature Generation, Signature Verification Curve/Key size:P-256 w/ SHA-256	656
KBKDF	[SP 800-108] Functions: CMAC-based KDF using AES Mode: Counter Key sizes:128,192,256 bits	89
KTS	[SP 800-38F] Functions: AES encryption w/ CMAC Key size: 128	3327 (AES) 3920 (AES)

[1]SP 800-133 compliant. The resulting symmetric keys and seeds used for FIPS 186-4 asymmetric key generation are the unmodified output from DRBG Cert. #1564.

Algorithm	Description	Cert #
RSA	[FIPS 186-4, ANSI X9.31-1998, 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	1708
RSA CRT	[FIPS 186-4, ANSI X9.31-1998, 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	2470
SHA	[FIPS 180-4] Functions: Digital Signature Generation except SHA-1, Digital Signature Verification except SHA-1, non-Digital Signature Applications SHA sizes: SHA-1, SHA-256, SHA-384, SHA-512	3229
Triple-DES[1]	[SP 800-20] Functions: Encryption, Decryption Modes: TECB, TCBC Key size:168 independent bits (3-key)	1899
Triple-DES MAC	[FIPS 113] Functions: Generation, Verification Key size: 168 independent bits (3-key)	Vendor Affirmed, based on Cert. #1899

[1] A Triple-DES key shall not be used for more than 2^{16} 64-bit block computations, per IG A.13

Table 6 lists the non-Approved Cryptographic Functions implemented in the Module which are allowed in a FIPS-Approved mode of operation.

Table 6 – FIPS-Allowed Cryptographic Functions

Algorithm	Description
ECDSA	[IG A.2] Functions: Key Pair Generation, Signature Generation, Signature Verification Curve/Key size: Any non-Approved but Allowed ECC-256 curve on the prime field w/ SHA-256; provides 128 bits of security strength
NDRNG	[IG 1.13] Hardware Non-Deterministic RNG; minimum of 8bits per access. The NDRNG output is used to seed the FIPS Approved DRBG.

Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module including all CSP lifecycle states is described in the services detailed in Section 3.3.

Table 7 – Cryptographic keys, Cryptographic Key Components, and CSPs

CSP	Description / Usage
Managing Key	Triple-DES 168-bit key used to encrypt all keys and CSPs stored in non-volatile memory
Symmetric Key	AES 128/192/256-bit key; Triple-DES168-bit Key. These keys are used to encrypt/decrypt data or within a symmetric MAC algorithm (AES CMAC or Triple-DES MAC) to generate authentication data.
Internal Auth Key	AES 128/192/256-bit key; Triple-DES168-bit Key. These keys are used to authenticate the Module to an external entity.
External Auth Key	AES 128/192/256-bit key; Triple-DES168-bit Key. These keys are used to modify the security state of the currently selected DF.
INIT_KEYenc	AES 128-bit key used to derive KSenc which is then used to encrypt/decrypt data over a secure session between an authorized external entity and the Module.
INIT_KEYmac	AES 128-bit key used to derive KSmac which is then used to authenticate an operator or data over a secure session between an authorized external entity and the Module.
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.
Kmac	AES 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.
KSenc	AES 128-bit key used to encrypt/decrypt data over a secure session.
KSmac	AES 128-bit key used to authenticate data over a secure session.
Personal Identification Number (PIN)	6-16 byte secret This PIN is used to modify the security state of the currently selected DF.
RSA Private Key	2048-bit RSA or RSA CRT private key used to sign data.
ECC Private Key	256-bit ECDSA private key used to sign data.
DRBG Entropy Input	256-bit input collected from the NDRNG, used to derive the DRBG seed. Provides approximately 241 bits of entropy.
DRBG Value	64-bit internal CTR DRBG state value used for the SP 800-90A CTR_DRBG
DRBG Key Value	168-bit internal CTR DRBG state key used for the SP 800-90A CTR_DRBG

2.2 Public Keys

All public keys used by the Module are described in this section. All usage of these public keys by the Module is described in the services detailed in Section 3.3.

Table 8 – Public Keys

Public Key	Description / Usage
RSA Public Key	2048-bit RSA or RSA CRT public key used to verify data.
ECC Public Key	256-bit ECDSA public key used to verify data.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The Module supports the two roles required by FIPS 140-2: Cryptographic-Officer (CO) and User. 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 implicitly selected to either the CO or User role, depending on the role associated with an operator's key. All authentication mechanisms listed in Table 9 below are available to both the User and CO roles.

3.2 Authentication Methods

Please see Table 9 for details regarding the authentication mechanism.

Table 9 – Operator 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 a false acceptance occur is no greater than 1/2^128, which is less than 1/1,000,000. The Module is capable of processing 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 a false acceptance occur is no greater than 1/2^64, which is less than 1/1,000,000. The Module is capable of processing 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 Signature Verification	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 is capable of processing 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.

Authentication Type	Authentication Data	Justification
Identity-based	PIN Verification	The Module supports PIN verification. The Module enforces a PIN length of 6 to 16 bytes and does not check 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 is capable of processing a maximum of 1000 authentication attempts in a one minute period. Therefore, the random success rate for multiple retries in one minute is 1000/2^48, which is less than 1/100,000. NOTE: PIN verification is only available if the CO calls the Install Key service to install the PIN during Module initialization.

3.3 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 10 and Table 11 show a typical APDU command structure and command response structure used by the Module, respectively.

Table 10 – APDU Command Structure

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

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

Table 11 – APDU Command Response Structure

Data Field	Trailer
Response data	Status bytes

All services implemented by the Module under FIPS-Approved Mode are listed in Table 12 and Table 13 below. Each service description also describes all usage of CSPs by the service, where X indicates that the service is available to the entity, blank indicates the service is not available to that entity.

NOTE1:

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 12 and Table 13. If Secure Messaging (SM) is needed when operating the 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.

Table 12 – Authenticated Services

Service	Description	CO	U
Read Binary	Allows read access to a binary file. A binary file is a file whose content is a sequential string of bits. CSP/Key usage: No CSPs or keys are accessed via this service.	X	X
Update Binary	Allows write access to a binary file. CSP/Key usage: No CSPs or keys are accessed via this service.	X	
Read Record	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. CSP/Key usage:No CSPs or keys are accessed via this service.	X	X
Update Record	Allows write access to a record. CSP/Key usage: No CSPs or keys are accessed via this service.	X	
Append Record	Allows a record to be appended CSP/Key usage: No CSPs or keys are accessed via this service.	X	

Service	Description	CO	U
External Authenticate	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. CSP/Key usage: 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	X	X
Internal Authenticate	Authenticates the cryptographic module to an external entity NOTE: Access to an Internal Auth Key or RSA Private Key is associated by identity; an external entity authenticated to identity A cannot access keys associated with identity B. CSP/Key usage: Authenticate Only: • Internal Auth Key: R, X • RSA Private Key: R, X	X	X
Verify	Provides PIN verification. NOTE: PIN access is associated by identity; an external entity authenticated to identity A cannot access a PIN associated with identity B. This service may be used in place of External Authenticate to authenticate to the Module. CSP usage: • PIN: R, X	X	X
Change Reference Data	Modify the PIN NOTE: Permission to change a PIN is associated by identity; an external entity authenticated to identity A cannot access a PIN associated with identity B. CSP usage: • PIN: R, W, X	X	X

Service	Description	CO	U
Enable Verification Requirement	Modifies a PIN's state from invalid to valid. NOTE: Permission to change a PIN's state is associated by identity; an external entity authenticated to identity A cannot access a PIN's state associated with identity B. CSP usage: No CSPs are accessed via this service.	X	
Disable Verification Requirement	Modifies a PIN's state from valid to invalid. NOTE: Permission to change a PIN's state is associated by identity; an external entity authenticated to identity A cannot access a PIN's state associated with identity B. CSP usage: No CSPs are accessed via this service.	X	
Reset Retry Counter	Resets the retry counter of the PIN to its initial value. NOTE: Permission to change a PIN's retry counter is associated by identity; an external entity authenticated to identity A cannot access a PIN's retry counter associated with identity B. CSP usage: No CSPs are accessed via this service.	X	
Generate Asymmetric Key Pair	Generates an RSA or ECC key pair CSP/Key usage: • RSA Private Key: G, W • RSA Public Key: G, W • ECC Private Key: G, W • ECC Public Key: G, W • DRBG Entropy Input*: G, X • DRBG Value*: G, R,W, X • DRBG Key Value*: G, R, W, X *Note that DRBG Entropy Input access, and generation of DRBG Value and DRBG Key Value only occurs if the DRBG is being reseeded.	X	X
Encrypt	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. CSP/Key usage: • Symmetric Key: R, X	X	X
Decrypt	Performs a decrypt operation NOTE: The MSE service must have previously been utilized to choose the algorithm and key for the security operation. CSP/Key usage: • Symmetric Key: R, X	X	X

Service	Description	CO	U
Verify Digital Signature	Verifies a digital signature using RSA PKCS#1 or ECC. CSP/Key usage: • RSA Public Key: R, X • ECC Public Key: R, X NOTE: no security is claimed from verifying an ECC signature.	X	X
Compute Digital Signature	Computes a digital signature using RSA PKCS#1 or ECC. Note that CSP/Key usage: • RSA Private Key: R, X • ECC Private Key: R, X NOTE: no security is claimed from computing an ECC signature.	X	X
Verify MAC	Performs AES or Triple-DES MAC verification. CSP/Key usage: • Symmetric Key: R, X	X	X
Compute MAC	Computes an AES or Triple-DES MAC. The length of the checksum is 8 bytes. CSP/Key usage: • Symmetric Key: R, X	X	X
Create File	Creates a file. CSP/Key usage: No CSPs or keys are accessed via this service.	X	
Delete File	Deletes a file and all files which exist within that file. CSP/Key usage: No CSPs or keys are accessed via this service.	X	
Terminate Card	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. CSP/Key usage: • Managing Key: W	X	

Service	Description	CO	U
Install Secret	This service is only available during Module initialization to set the initial value and AC permission bytes for AES keys and Triple-DES keys, and PINs. The CSPs which may be entered are as follows: • Kenc • Kmac • Internal Auth Key • External Auth Key • Symmetric Key • PIN CSP/Key usage: • Kenc: W • Kmac: W • Internal Auth Key: W • External Auth Key: W • Symmetric Key: W • PIN: W • KSenc: R, X • KSmac: R, X	X	
Update Key	Allows the updating of the INIT_KEYs or secret file keys. This service may be used to zeroize the keys listed below by overwriting them with arbitrary data. CSP/Key usage: • INIT_KEYenc: W • INIT_KEYmac: W • Kenc: W • Kmac: W • Internal AuthKey: W • External AuthKey: W • Symmetric Key: W • Ksenc: R, X • Ksmac: R, X	X	
Get File List	Allows the reading of the FID list of child files of the current file. CSP/Key usage: No CSPs or keys are accessed via this service.	X	X
Read Public Key	Allows the output of a public key. CSP/Key usage: • RSA Public Key: R • ECC Public Key: R	X	X

Service	Description	CO	U
Import RSA Key	Allows the input of an RSA key. CSP/Key usage: • RSA Private Key: W • RSA Public Key: W • KSenc: R, X • KSmac: R, X	X	X
Import ECC Key	Allows the input of an ECCkey CSP/Key usage: • ECC Private Key: W • ECC Public Key: W • KSenc: R, X • KSmac: R, X	X	X

Table 13 – Unauthenticated Services

Service	Description
Put Data	Allows data to be received and stored by the Module. In the Put Data service, only the OEM information is allowed to be set. CSP/Key usage: No CSPs or keys are accessed via this service.
Get Data	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 1.2 of this Security Policy. CSP/Key usage: No CSPs or keys are accessed via this service.
Get Challenge	Requests a random value that will be used as a challenge within the External Authenticate service. CSP/Key usage: • DRBG Value: X • DRBG Key Value: X

Service	Description
Manage Security Environment (MSE)	Prepares the Module for the subsequent services. CSP/Key usage: • RSA Public Key: R • RSA Private Key: R • ECC Public Key: R • ECC Private Key: R • Symmetric Key: R • External Auth Key: R • Internal Auth Key: R NOTE: Read access in this case only refers to loading keys into the Module's internal RAM. No CSPs are created, disclosed or modified as a result of this service.
Select	Allows the selection of a specified file. CSP/Key usage: No CSPs or keys are accessed via this service.
Manage Channel	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. CSP/Key usage: No CSPs or keys are accessed via this service.
Hash	Performs a hash using SHA-1, SHA-256, SHA-384, or SHA-512. CSP/Key usage: No CSPs or keys are accessed via this service.
Change ECC Parameters	Allows the change of the default value of the P-256 elliptic curve parameter; this service is only available as part of module initialization into the Approved mode. It is the operator's responsibility to 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. CSP/Key usage: No CSPs or keys are accessed via this service.
Self-Test	Power cycle the Module in order to perform power up self-tests on demand CSP/Key usage: • DRBG Value: X • DRBG Key Value: X

All services listed above are all available on the USB and contactless interfaces.

4 Self-tests

4.1 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 14 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 and output a status word of "6F00".

Table 14 – Power Up Self-tests

Test Target	Description
AES (Cert. #3327)	KATs: Encryption and Decryption Modes: ECB Key sizes: 128 bits
CMAC(AES Cert. #3920)	KATs: Generation and Verification Key sizes: AES with 256 bits
DRBG (Cert. #1564)	KATs: Triple-DES CTR (Instantiate, Generate and Reseed) Security Strength: 112 bits
ECDSA(Cert. #656)	PCT: Signature Generation and Verification Curves/Key sizes: P-256
Firmware Integrity	32-bitEDC performed over ROM, RAM and flash[2]via HW. A secondary 16-bit CRC is also performed over flash[2]via FW.
KDF, using Pseudorandom Functions(Cert. #89)	KATs: KDF Mode: Counter
RSA (Cert. #1708)	KATs: Signature Generation and Signature Verification Key sizes: 2048 bits
RSA CRT (Cert. #2470)	KATs: Signature Generation and Signature Verification Key sizes: 2048 bits
SHA (Cert. #3229)	KATs:SHA-1, SHA-256, SHA-512[3]
Triple-DES(Cert. #1899)	KATs: Encryption and Decryption Modes: TECB Key sizes: 3-key

[2] Flash in this case refers to the M7893 microcontroller's internal flash, not the excluded flash chip.

[3]A SHA-384 KAT is not required when SHA-512 is self-tested, as specified in IG 9.4.

4.2 Conditional self-tests

Table 15 – Conditional Self-tests

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

5 Physical Security Policy

The Module is a made of a completely hardened, production-grade polycarbonate. The colored polycarbonate 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 M7893 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 plastic 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 plastic 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.

Note: Module hardness testing was performed at ambient temperature. No assurance is provided for Level 3 hardness conformance at any other temperature.

6 Operational Environment

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

7 Electromagnetic interference and compatibility (EMI/EMC)

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.

8 Mitigation of Other Attacks Policy

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.

9 Guidance and Security Rules

9.1 Initial Setup

The ECC parameters installed in the module are FIPS approved by default. If the Change ECC Parameters service is used during initialization, the operator must ensure the new parameters loaded into the module are FIPS Approved or Allowed. The module is delivered with a pair of AES keys (INIT_KEYenc and INIT_KEYMAC used to derive Ksenc and Ksmac) to allow authentication and secure initialization of the module. All communication to initialize the module will require a secure session using Ksenc and Ksmac for encrypting and MACing all data input and output.

For additional information regarding module initialization, please refer to the ePass2003 Token User Manual.

9.2 Security Rules

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

1. Data output is logically disconnected during key generation and zeroization. Data output is inhibited while the module is performing self-tests or in an error state.
2. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
3. The Module does not enter or output plaintext CSPs.
4. The Module does not output intermediate key values.
5. The Module does not support a bypass mode.
6. No additional interface or service is implemented by the Module which would provide access to CSPs.
7. In the case that zeroization is required, the Crypto-Officer shall obtain possession of the Module and then maintain sole physical possession of the cryptographic module until all keys have been zeroized.
8. The Module supports concurrent operators using four separate logical channels. The logical channel ID is the parameter that allows for logical separation within the Module. It should be noted that besides user and control data separation, the authentication status per logical channel is also kept separate. References

10 References

The following standards are referred to in this Security Policy.

Table 16 – References

Abbreviation	Full Specification Name
[FIPS140-2]	Security Requirements for Cryptographic Modules, May 25, 2001
[SP800-131A]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011
[ISO 7816-4]	ISO/IEC 7816-4:2006 Identification cards – Integrated circuit cards – Part 4: Inter industry commands for interchange
[ISO 14443]	ISO/IEC 14443-1:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics ISO/IEC 14443-2:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface ISO/IEC 14443-3:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anti-collision ISO/IEC 14443-4:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation Methods and Techniques, December 2001
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication , May 2005
[FIPS 140-2 IG]	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, June 2012
[FIPS 113]	Computer Data Authentication, 30 May 1985
[FIPS 197]	Advanced Encryption Standard (AES), November 26, 2001
[FIPS 186-4]	Digital Signature Standard (DSS), July 2013
[PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard, June 14, 2002
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators, January2012
[SP 800-20]	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS):Requirements and Procedures, March 2012
[SP 800-108]	Recommendation for Key Derivation Using Pseudorandom Functions, October 2009
[SP 800-133]	NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, December 2012

11 Acronyms and Definitions

Table 17 – Acronyms and Definitions

Acronym	Definition
AC	Access Condition
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
IC	Integrated Circuit
IEC	International Electro technical Commission
ISO	International Organization for Standardization
SM	Secure Messaging
VCC	Common Collector Voltage