Feitian Technologies Co., Ltd.

FEITIAN-FIPS-COS

HW Version 1.0.0; FW Version 1.0.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 1.4

Prepared for:

Feitian Technologies Co., Ltd.
Floor 17th, Tower B, Huizhi Mansion
No.9 Xueqing Road
Haidian District, Beijing 100085
China

Phone: +(86)010-62304466
Email: world.sales@ftsafe.com
http://www.FTSafe.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033
United States of America

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the FEITIAN-FIPS-COS from Feitian Technologies Co., Ltd. This Security Policy describes how the FEITIAN-FIPS-COS meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website, which is maintained by National Institute of Standards and Technology (NIST) and Communication Security Establishment Canada (CSEC): http://csrc.nist.gov/groups/STM/index.html.

The FEITIAN-FIPS-COS is also referred to in this document as cryptographic module or module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Feitian website (http://www.FTSafe.com/) contains information on the full line of products from Feitian.
- The CMVP website (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

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

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Feitian. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Feitian and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Feitian.

2 FEITIAN-FIPS-COS

2.1 Overview

Feitian is the leading innovator of smart card and Chip Operating System (COS) based security technologies and applications. Their product offerings include devices that provide software protection, strong authentication, and smart card operating systems. Evidence of Feitian's continued leadership and innovation is demonstrated within this Security Policy, which specifies their first FIPS 140-2 validated cryptographic module. This new module, referred to as the FEITIAN-FIPS-COS, is both an integrated circuit and an operating system, and has been developed to support their ePass series USB[1] tokens. FEITIAN-FIPS-COS is designed to provide strong authentication and identification and to support network logon, secure online transactions, digital signatures, and sensitive data protection. The FEITIAN-FIPS-COS provides all cryptographic functionality for Feitian's ePass line of products. FEITIAN-FIPS-COS supports dual-factor authentication with an ISO[2]7816-12 USB interface for the PC host connection acting as a smart card reader.

Figure 1 – FEITIAN-FIPS-COS Cryptographic Module

The FEITIAN-FIPS-COS has been validated to the FIPS 140-2 Security Levels listed in Table 1:

Table 1 – Security Level Per FIPS 140-2 Section

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

[1] USB – Universal Serial Bus
[2] ISO – International Organization for Standardization
[3] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

2.2 Module Specification

The FEITIAN-FIPS-COS is a hardware type module with a single-chip embodiment that meets overall level 2 FIPS 140-2 requirements. The module consists of two major components, a 16-bit Integrated Circuit (IC) and a COS. The cryptographic boundary of the FEITIAN-FIPS-COS is the outer IC packaging, which encompasses all module components. Please see Figure 1 for a depiction of the module.

The FEITIAN-FIPS-COS supports both a FIPS-Approved and non-FIPS-Approved mode of operation. In the FIPS-Approved mode of operation, only the FIPS-Approved or Allowed algorithms are available for use. In a non-FIPS-Approved mode, the non-Approved algorithms are also available for use. Please see Section 3.1 for instructions specifying how to configure FIPS mode.

2.3 Module Ports and Interfaces

The physical ports provided by the module are shown in Figure 2. The red dotted line indicates the cryptographic boundary.

It should be noted that although the module provides 20 physical pins, the only pins that are enabled are the eight pins specified in Table 2. All other pins are disabled, as they are not supported by the FEITIAN-FIPS-COS operating system. Therefore, any signals input over them are not interpreted by the hardware or firmware.

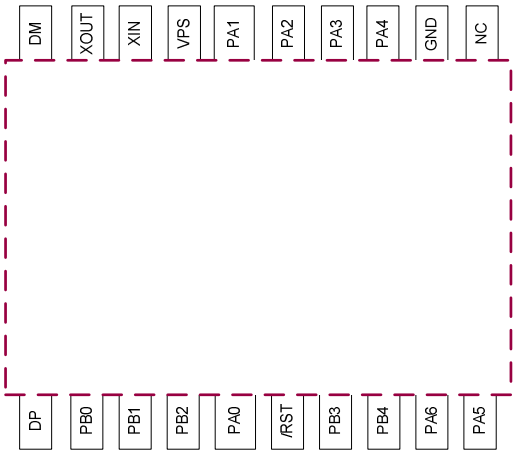

Figure 2 – Physical Ports

The logical interfaces as defined by FIPS 140-2 are accessible through the module's enabled physical ports. The mapping between the physical ports and logical interfaces is provided in Table 2 below:

Table 2 – FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	FEITIAN-FIPS-COS ISO 7816 Port	Pin and module interface
Data Input	I/O	• DP - USB data + differential input • DM - USB data + differential input • XIN - Crystal oscillator input

FIPS 140-2 Logical Interface	FEITIAN-FIPS-COS ISO 7816 Port	Pin and module interface
Data Output	I/O	• DP - USB data + differential input • DM - USB data + differential input • XOUT - crystal oscillator output
Control Input	I/O, Reset	• DP - USB data + differential input • DM - USB data + differential input • /RST - Reset
Status Output	I/O	• DP - USB data + differential input • DM - USB data + differential input • PA4 - Output to external LED
Power	VCC, Ground	• VPS - Power • GND - Ground

2.4 Roles and Services

The module supports the two roles required by FIPS 140-2: Crypto-Officer and User. The Crypto-Officer 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. Once authenticated, the operator is authorized to assume both the Crypto-Officer and User roles. Please see Table 3 for details regarding the authentication mechanism. Role selection is implicit and is based upon the service accessed. Table 6 and Table 7 below specify the full list of services per supported role.

Table 3 – Operator Authentication Mechanism

Authentication Mechanism	Authentication Data	Authentication Mechanism
Role-based	128-bit AES[4] Key Pair	Each 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 will allow fewer than 600 authentication attempts in a one minute period. Therefore, the random success rate for multiple retries is 600/2^128, which is less than 1/100,000.

All services provided by FEITIAN-FIPS-COS are implemented in accordance with ISO/IEC[5] 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 [1]. Table 4 and Table 5 show the ADPU command and response structure, respectively.

[4] AES – Advanced Encryption Standard
[5] IEC – International Electrotechnical Commission

Table 4 – APDU command structure

Header		L_c Field	Data Field	L_e Field
CLA	INS	1 byte	Input Data (1 or 3 bytes)	1 byte

- 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
- L_c – Length in bytes of the data field
- Data Field – Data input with command for processing
- L_e – Maximum number of bytes expected in the response

Table 5 – APDU command response structure

Data Field	Trailer
Response data	Status bytes

- Data Field – Data output, if applicable
- Trailer – Status bytes (e.g. 9000, 64XX)

2.4.1 Crypto-Officer Role

This section provides a list of all services accessible to a Crypto-Officer. The list includes a full description of each service, and in addition, it describes the type of access that each service has to a CSP[6].

NOTE:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Table 6 – Mapping of Crypto-Officer Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	INS[7]	Description	Input	Output	CSP and Type of Access
Read Binary	B0	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, 6284, 6A80, 6A81, 6A82, 6A86, 6A87)	No CSPs are accessed via this service.
Update Binary	D6	Allows write access to a binary file.	• Offset address of the binary file to read • Length of the data to be read	• Status (e.g. 9000, 6283, 6284, 6A80, 6A81, 6A82, 6A86, 6A87)	No CSPs are accessed via this service.

[6] CSP – Critical Security Parameter
[7] INS – the value in hex of the instruction byte of the command message

Service	INS[7]	Description	Input	Output	CSP and Type of Access
Read Record	B2	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, 6284, 6A80, 6A81, 6A82, 6A86, 6A87)	No CSPs are accessed via this service.
Update Record	DC	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, 6284, 6A80, 6A81, 6A82, 6A86, 6A87)	No CSPs are accessed via this service.
Append Record	E2	Allows a record to be appended	• 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, 6284, 6A80, 6A81, 6A82, 6A86, 6A87)	No CSPs are accessed via this service.

Service	INS[7]	Description	Input	Output	CSP and Type of Access
External Authenticate	82	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.	• Initiate a secure session: • Authentication data of external entity (32 bytes) plus the MAC[8] (8 bytes) **Or** • Authenticate only: • Algorithm type (AES, DES[9], RSA[10]) • 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.	Initiate a secure session: • INIT_KEYenc : R, X • INIT_KEYmac: R, X • Kenc: R, X • Kmac: R, X • KSenc: W • Ksmac :W **Or** Authenticate Only: • Symmetric key: R, X • RSA Private Key: R, X
Internal Authenticate	88	Authenticates 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, DES, RSA) • Key ID (Key Index) • Length of data in the field • Random data (data field)	• Authentication data • Status (e.g. 9000, 6300, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	• Symmetric key: R, X • RSA Private Key: R, X

[8] MAC – Message Authentication Code
[9] DES – Data Encryption Standard
[10] RSA – Rivest, Adleman, and Shamir

Service	INS[7]	Description	Input	Output	CSP and Type of Access
Verify	20	Provides PIN verification. NOTE: In order for this service to be utilized, the external entity must have privileged access to the referenced PIN.	• Reference to the PIN • PID[11] • Data to be verified	• Status (e.g. 9000, 6300, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	• PIN: R, X
Change Reference Data	24	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, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	• PIN: R, W, X
Enable Verification Requirement	28	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, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	No CSPs are accessed via this service.
Disable Verification Requirement	26	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, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	No CSPs are accessed via this service.

[11] PID – Personal Identification number inDex

Service	INS[7]	Description	Input	Output	CSP and Type of Access
Reset Retry Counter	2C	Resets the retry counter of the PIN to its initial value. NOTE: Utilization of this service requires permission to modify PIN.	• Reset parameter (resets recount maximum number and remaining count to default) • Restore parameter (restores recount to initial default value) • Reference to PIN • PID	• Status (e.g. 9000, 6300, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	No CSPs are accessed via this service.
Generate Asymmetric Key Pair	46	Generates an Asymmetric key pair	• Key parameter information • Algorithm ID • Modulus Length • Private Key File Identifier (FID)	• Status (e.g. 9000, 6300, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	• RSA Private Key: W • RSA Public Key: W • DRBG[12] Seed and Seed Key: R,W, X
Encrypt	2A	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, 6300, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	• Symmetric key: R, X • RSA Public Key: R, X

[12] DRBG – Deterministic Random Bit Generator

Service	INS[7]	Description	Input	Output	CSP and Type of Access
Decrypt	2A	Performs a decrypt operation NOTE: The MSE service must have previously been utilized to choose the algorithm and key for the security operation.	• Ciphertext	• Plaintext	• Symmetric key: R, X • RSA Private Key: R, X
Verify Digital Signature	2A	Verifies a digital signature using RSA PKCS[13]#1	• Data Object of the signed data plus the digital signature	• Status of the verification	• RSA Public Key: R, X
Compute Digital Signature	2A	Computes a digital signature using RSA PKCS#1.	• Input data for generating the digital signature	• Digital Signature	• RSA Private Key: R, X
Verify Cryptographic Checksum	2A	Performs AES or Triple-DES checksum verification.	• Plaintext data object plus the cryptographic checksum data	• Status (e.g. 9000, 6300)	• Symmetric Key: R, X
Compute Cryptographic Checksum	2A	Computes an AES or Triple-DES checksum. The length of the checksum is 8 bytes.	• The data used to compute the cryptographic checksum	• Cryptographic checksum	• Symmetric Key: R, X

[13] Public-Key Cryptography Standards

Service	INS[7]	Description	Input	Output	CSP and Type of Access
Create File	E0	Creates a file	• File control parameters (data field) • Patch data parameter • Length of data field	• Status (e.g. 9000)	• INIT_KEYenc : R, X • INIT_KEYmac: R, X • Ksenc : W, X • Ksmac : W, X
Delete File	E4	Deletes a file and all files which exist within that file	• File ID	• Status (e.g. 9000)	No CSPs are accessed via this service.
Terminate Card	FE	Terminates all applications on the card	• None	• None	No CSPs are accessed via this service.
Install Secret	E3	This service is used to enter AES keys, DES keys, and PINs. The keys 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, 6A8, 6A82, 6B00, 6CXX)	• Kenc : W • Kmac : W • Internal Auth key: W • External Auth key: W • Symmetric Key: W • PIN: W

Service	INS[7]	Description	Input	Output	CSP and Type of Access
Update Key	E5	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, 6A8, 6A82, 6B00, 6CXX)	• Symmetric Key: W • INIT_KEYenc : W • INIT_KEYmac: W • Kenc : W • Kmac : W • Internal Auth key: W • External Auth key: W
Get File List	34	Allows the reading of the FID list of child files of the current file.	• None	• FID list or "Nonexistent" • Status (eg. 9000, 6700, 6982, 6986, 6A8, 6A82, 6B00, 6CXX)	No CSPs are accessed via this service.

Service	INS[7]	Description	Input	Output	CSP and Type of Access
Read Public Key	B4	Allows the output of a public key	• FID of the public key • Public Key component read parameter (Read all component, read E component, or read N component)	• Public Key data or "Nonexistent" • Status (eg. 9000, 6700, 6982, 6986, 6A8, 6A82, 6B00, 6CXX)	No CSPs are accessed via this service.
Import RSA Key	E7	Allows the input of an RSA key.	• Encrypted key data • FID of the RSA Key	• Status (eg. 9000, 6700, 6982, 6986, 6A8, 6A82, 6B00, 6CXX)	• RSA key pair: W

2.4.2 User Role

This section provides a list of all services accessible to a User. The list includes a full description of each service and, in addition, it describes the type of access that each service has to CSPs.

NOTE:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or allowed security function or authentication mechanism.

Table 7 – Mapping of User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	INS	Description	Input	Output	CSP and Type of Access
Read Binary	B0	Allows read access to a binary file.	• Offset address of the binary file to read • Length of the data to be read	• File data or "Nonexistent" • Status (e.g. 9000, 6283, 6284, 6A80, 6A81, 6A82, 6A86, 6A87)	No CSPs are accessed via this service.
Read Record	B2	Allows read access to a record.	• 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, 6284, 6A80, 6A81, 6A82, 6A86, 6A87)	No CSPs are accessed via this service.

Service	INS	Description	Input	Output	CSP and Type of Access
External Authenticate	82	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.	• Initiate a secure session: • Authentication data of external entity (32 bytes) plus the MAC (8 bytes) **Or** • Authenticate only: • Algorithm type (AES, 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.	Initiate a secure session: • INIT_KEYenc : R, X • INIT_KEYmac: R, X • Kenc: R, X • Kmac: R, X • KSenc: W • Ksmac :W **Or** Authenticate Only: • Symmetric key: R, X • RSA Private Key: R, X
Internal Authenticate	88	Authenticates 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, DES, RSA) • Key ID (Key Index) • Length of data in the field • Random data (data field)	• Authentication data • Status (e.g. 9000, 6300, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	• Symmetric key: R, X • RSA Private Key: R, X

Service	INS	Description	Input	Output	CSP and Type of Access
Verify	20	Provides PIN verification. NOTE: In order for this service to be utilized the external entity must have privileged access to the referenced PIN.	• Reference to the PIN • PID • Data to be verified	• Status (e.g. 9000, 6300, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	• PIN: R, X
Change Reference Data	24	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 password • PID	• Status (e.g. 9000, 6300, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	• PIN: R, W, X
Reset Retry Counter	2C	Resets the retry counter of the PIN to its initial value. NOTE: Utilization of this service requires permission to modify PIN.	• Reset parameter (resets recount maximum number and remaining count to default) • Restore parameter (restores recount to initial default value) • Reference to PIN • PID	• Status (e.g. 9000, 6300, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	No CSPs are accessed via this service.

Service	INS	Description	Input	Output	CSP and Type of Access
Generate Asymmetric Key Pair	46	Generates an asymmetric key pair	• Key parameter information • Algorithm ID • Modulus Length • Private Key File Identifier (FID)	• Status (e.g. 9000, 6300, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	• RSA Private Key: W • RSA Public Key: W • DRBG Seed and Seed Key: R,W, X
Encrypt	2A	Perform an encrypt operation using an Approved security function.	• Plaintext data	• Ciphertext data • Status (e.g. 9000, 6300, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	• Symmetric key: R, X • RSA Public Key: R, X
Decrypt	2A	Performs a decrypt operation	• Ciphertext	• Plaintext	• Symmetric key: R, X • RSA Private Key: R, X
Verify Digital Signature	2A	Verifies a digital signature using RSA PCKS#1	• Data Object of the signed data plus the digital signature	• Status of the verification	• RSA Public Key: R, X

Service	INS	Description	Input	Output	CSP and Type of Access
Compute Digital Signature	2A	Computes a digital signature using RSA PCKS#1.	• Input data for generating the digital signature	• Digital Signature	• RSA Private Key: R, X
Verify Cryptographic Checksum	2A	Performs and AES or Triple-DES checksum verification.	• Plaintext data object plus the cryptographic checksum data	• Status (e.g. 9000, 6300)	• Symmetric Key: R, X
Compute Cryptographic Checksum	2A	Performs an AES or Triple-DES checksum. The length of the checksum is 8 bytes.	• The data used to compute the cryptographic checksum	• Cryptographic checksum	• Symmetric Key: R, X
Get File List	34	This command is used to read the FID list of child files of the current file.	• None	• FID list or "Nonexistent" • Status (eg. 9000, 6700, 6982, 6986, 6A8, 6A82, 6B00, 6CXX)	No CSPs are accessed via this service.
Read Public Key	B4	Allows the output of a public key	• FID of the public key • Public Key component read parameter (Read all component, read E component, or read N component)	• Public Key data or "Nonexistent" • Status (eg. 9000, 6700, 6982, 6986, 6A8, 6A82, 6B00, 6CXX)	No CSPs are accessed via this service.

Service	INS	Description	Input	Output	CSP and Type of Access
Import RSA Key	E7	Allows the input of an RSA key.	• Encrypted key data • FID of the RSA Key	• Status (eg. 9000, 6700, 6982, 6986, 6A8, 6A82, 6B00, 6CXX)	• RSA key pair: W

2.4.3 Unauthenticated Services

This section provides a list of all services accessible to an unauthenticated operator. The list includes a full description of each service and, in addition, it describes the type of access that each service has to CSPs.

NOTE:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or allowed security function or authentication mechanism.

Table 8 – Mapping of Unauthenticated Services to Inputs, Outputs, CSPs, and Type of Access

Service	INS	Description	Input	Output	CSP and Type of Access
Put Data	DA	Allows data to be received and stored by the cryptographic module. In the Put Data service, only the OEM information is allowed to be set.	• Data object tag ('81' which indicates OEM info, followed by up to 32 bits of OEM info. • Length of object data	• Status (e.g. 9000, 6283, 6284, 6A80, 6A81, 6A82, 6A86, 6A87)	No CSPs are accessed via this service.

Service	INS	Description	Input	Output	CSP and Type of Access
Get Data	CA	This service allows data to be retrieved. Data refers to global data, which belongs to the cryptographic module, such as the serial number, OEM information, chip information which includes algorithm support, RAM size.	• Data object tag (e.g., '80' which indicates card serial number)	• Content of object • Status (e.g. 9000, 6283, 6284, 6A80, 6A81, 6A82, 6A86, 6A87)	No CSPs are accessed via this service.
Get Challenge	84	Requests a random value that will be used as a challenge within the External Authenticate service.	• None	• Random value • Status (e.g. 9000, 6283, 6284, 6A80, 6A81, 6A82, 6A86, 6A87)	• DRBG Seed: R, W, X • DRBG Seed Key: R; W, X
Manage Security Environment (MSE)	22	Prepares the cryptographic module for the subsequent commands, SET, STORE, RESTORE, SEID, and ERASE.	• CRDO • Algorithm Reference • Key Reference • File Reference • Length of CRDOs	• Status (e.g. 9000, 6300, 62CX, 6581, 6700, 6982, 6984, 6A81, 6A2, 6A86, 6A88)	No CSPs are accessed via this service.
Select	A4	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, 6283, 6284, 6A80, 6A81, 6A82, 6A86, 6A87)	No CSPs are accessed via this service.

Service	INS	Description	Input	Output	CSP and Type of Access
Manage Channel	70	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 (01-03).	• Status (e.g. 9000, 6283, 6284, 6A80, 6A81, 6A82, 6A86, 6A87)	No CSPs are accessed via this service.
Hash	2A	Performs a hash using SHA-1 or SHA-256.	• Input data	• Hash result or None	No CSPs are accessed via this service.

2.5 Physical Security

The FEITIAN-FIPS-COS is a production grade, single-chip cryptographic module as defined by FIPS 140-2 and is designed to meet Level 3 physical security requirements.

The FEITIAN-FIPS-COS is covered with a hard opaque epoxy coating that provides evidence of attempts to tamper with the module and was tested at temperatures of 0 to 80 degrees Celsius. The FEITIAN-FIPS-COS does not contain any doors, removable covers, or ventilation holes or slits. No maintenance access interface is available. No special procedures are required to maintain physical security of the module while delivering to operators.

2.6 Operational Environment

The operational environment requirements do not apply to the FEITIAN-FIPS-COS as it only supports a limited operational environment.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 9:

Table 9 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES in ECB, CBC[14] modes using 128-bit key sizes	1473
Triple-DES in ECB, CBC modes using 168-bit key sizes	991
RSA PKCS#1 v1.5 signature generation/verification – using 1024- and 2048-bit keys	720
ANSI[15] X9.31 Key Pair Generation	720
SHA-1 and SHA-256	1332
SP800-90 DRBG	58

Additionally, the module utilizes the non-FIPS-Approved algorithm implementations listed in Table 10 and Table 11:

Table 10 – FIPS-Allowed Algorithm Implementations

Algorithm
Non-Deterministic Random Number Generator (NDRNG)
RSA PKCS#1v1.5 1024, 2048 bit encrypt/decrypt to provide key establishment (Key establishment methodology provides 80-112 bits of security)

[14] CBC – Cipher-Block Chaining
[15] ANSI – American National Standards Institute

Table 11 – FIPS Non-Approved Algorithm Implementations

Algorithm
DES ECB and CBC
AES CBC-MAC [Non-Compliant]

The module supports the critical security parameters listed in Table 12.

Caveat: The module generates cryptographic keys whose strengths are modified by available entropy.

Table 12 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Use	Generation / Input	Output	Storage	Zeroization	Key To Entity
Symmetric Key	AES or Triple-DES 128-bit key	These keys are used to encrypt/decrypt data, or within a symmetric MAC algorithm to generate authentication data.	**Generation:** This key is not generated within the module. **Input:** This key may be input encrypted within a secure channel.	N/A: The module does not support the output of this key.	These keys are stored obfuscated in EEPROM[16].	Procedurally overwrite keys with arbitrary data using the Update Key service.	Storage: 4-bit key ID Input/Output: This key is associated with the Crypto-Officer role during Input via the usage of the AES MAC.
Internal Auth Key	AES 128-bit, Triple-DES 112 and 168 -bit, or DES key	These keys are used to authenticate the module to an external entity.	**Generation:** This key is not generated within the module. **Input:** This key may be input encrypted within a secure channel.	N/A: The module does not support the output of this key.	These keys are stored obfuscated in EEPROM.	Procedurally overwrite keys with arbitrary data using the Update Key service.	Storage: 4-bit key ID Input/Output: This key is associated with the Crypto-Officer role during Input via the usage of the AES MAC.

[16] EEPROM - Electronically Erasable Programmable Read-Only Memory

Key	Key Type	Use	Generation / Input	Output	Storage	Zeroization	Key To Entity
External Auth Key	AES 128-bit, Triple-DES 112 and 168 -bit, or DES key	These keys are used to modify the security state of the currently selected DF[17].	**Generation:** This key is not generated within the module. **Input:** This key may be input encrypted within a secure channel.	N/A: The module does not support the output of this key.	These keys are stored in obfuscated EEPROM within a special files used to store symmetric keys and PINs.	Procedurally overwrite keys with arbitrary data using the Update Key service.	Storage: 4-bit key ID Input/Output: This key is associated with the Crypto-Officer role during Input via the usage of the AES MAC.
$INIT\_KEY_{enc}$	AES 128-bit key	This key is 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.	**Generation:** This key is not generated within the module. It is a factory-set key which is used only in the initialized state of the module. **Input:** This key is factor-set and cannot be modified or input outside of manufacturing.	N/A: The module does not support the output of this key.	This key is stored obfuscated under the reserved file in EEPROM.	Procedurally overwrite key with arbitrary data using the Update Key service.	Storage: 4-bit key ID Input/Output: N/A

[17] DF – Dedicated File

Key	Key Type	Use	Generation / Input	Output	Storage	Zeroization	Key To Entity
$INIT\_KEY_{mac}$	AES 128-bit key	This key is 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.	**Generation:** This key is not generated within the module. It is a factory-set key which is used only in the initialized state of the module. **Input:** This key is factor-set and cannot be modified or input outside of manufacturing.	N/A: The module does not support the output of this key.	This key is stored obfuscated under the reserved file in EEPROM.	Procedurally overwrite keys with arbitrary data using the Update Key service.	Storage: 4-bit key ID Input/Output: N/A
K_{enc}	AES 128-bit, Triple-DES 112 and 168 -bit	This key is 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.	**Generation:** This key is not generated within the module. **Input:** This key may be input encrypted within a secure channel.	N/A: The module does not support the output of this key.	These keys are stored obfuscated at index 0x00 of the currently selected DF.	Procedurally overwrite keys with arbitrary data using the Update Key service.	Storage: 4-bit key ID Input/Output: N/A

Key	Key Type	Use	Generation / Input	Output	Storage	Zeroization	Key To Entity
K_{mac}	AES 128-bit, Triple-DES 112 and 168 -bit	This key is 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.	**Generation:** This key is not generated within the module. **Input:** This key may be input encrypted within a secure channel.	N/A: The module does not support the output of this key.	These keys are stored obfuscated at index 0x00 of the currently selected DF.	Procedurally overwrite keys with arbitrary data using the Update Key service.	Storage: 4 bit key ID Input/Output: N/A
KS_{enc}	AES 128-bit, Triple-DES 112 and 168 -bit	This key is used to encrypt/decrypt data over a secure session.	**Generation:** Generated from the $INIT\_KEY_{enc}$ or K_{enc} key as part of the Secure Channel Protocol v01 as specified within Global Platform v2.1. **Input:** This key cannot be input.	N/A: The module does not support the output of this key.	These keys are stored in plaintext, within module RAM.	Power cycle the module.	Storage: This key is associated with a logical channel ID (0-3) for which it is being used to secure messaging. Input/Output: N/A, this key is not output

Key	Key Type	Use	Generation / Input	Output	Storage	Zeroization	Key To Entity
KS_{mac}	AES 128-bit, Triple-DES 112 and 168 -bit	This key is used to authenticate data over a secure session.	**Generation:** Generated from the $INIT\_KEY_{mac}$ or K_{mac} key as part of the Secure Channel Protocol v01 as specified within Global Platform v2.1. **Input:** This key cannot be input.	N/A: The module does not support the output of this key.	These keys are stored in plaintext, within module RAM.	Power cycle the module.	Storage: This key is associated with a logical channel ID (0-3) for which it is being used to secure messaging. Input/Output: N/A, this key is not output
Personal Identification Number (PIN)	6-16 byte secret	This key is used to modify the security state of the currently selected DF.	**Generation:** This key is not generated within the module. **Input:** This key may be input encrypted within a secure channel.	N/A: The module does not support the output of this key.	These secrets are stored obfuscated in EEPROM.	Procedurally overwrite keys with arbitrary data using the Update Key service.	Storage: 4-bit key ID

Key	Key Type	Use	Generation / Input	Output	Storage	Zeroization	Key To Entity
RSA Private Key	1024-, 2048- and 3072-bit RSA private key	This key is used to decrypt or sign data.	**Generation:** This key is generated using the Approved SP800-90 DRBG. **Input:** This key may be input encrypted within a secure channel.	N/A: The module does not support the output of this key.	These keys are stored obfuscated in EEPROM.	Procedurally overwrite keys with arbitrary data using the Import RSA Key service.	Storage: 4-bit File ID NOTE: Only one RSA Private key may be stored in an RSA Private Key file.
RSA Public Key	1024, 2048 and 3072, bit RSA public key.	This key is used to decrypt or verify data.	**Generation:** This key is generated using the Approved SP800-90 DRBG. **Input:** This key may be input encrypted within a secure channel.	Output in plaintext using the Read Public key command.	These keys are stored obfuscated in EEPROM.	N/A: this key is a public key and therefore does not have to be zeroized.	Storage: 4-bit File ID NOTE: Only one RSA Public key may be stored in an RSA Public Key file.
DRBG Seed	256-bit random value	256-bit seed value used as input into the SP800-90 DRBG	**Generation:** This CSP is generated using the modules non-deterministic RNG.	N/A: The module does not support the output of this CSP.	Stored in plaintext in module RAM.	Power cycle the module.	Associated with an internal module variable.

Key	Key Type	Use	Generation / Input	Output	Storage	Zeroization	Key To Entity
DRBG Seed Key	192-bit Triple-DES Seed Key	192-bit seed value used as input into the SP800-90 DRBG	**Generation:** This CSP is generated using the modules non-deterministic RNG.	N/A: The module does not support the output of this CSP.	Stored in plaintext in module RAM.	Power cycle the module.	Associated with an internal module variable.

2.8 EMI/EMC

The FEITIAN-FIPS-COS conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use):

2.9 Self-Tests

The FEITIAN-FIPS-COS performs the following self-tests at power-up:

- Firmware integrity test using a 16-bit CRC[18]
- Cryptographic Known Answer Tests (KATs)
    - AES KAT
    - Triple-DES KAT
    - SHA-1 KAT
    - SHA-256 KAT
    - RSA signature generation/verification KAT
    - DRBG KAT

The module performs the following conditional self-tests:

- Continuous Random Number Generator test for both the NDRNG and the SP800-90 DRBG.
- RSA pairwise consistency test for sign/verify and encrypt/decrypt

The module supports only one error condition, referred to as the FIPS Error State. Any failure of a FIPS self-test will cause the module to enter the FIPS error state, which does not allow for any data output and/or cryptographic service usage. If an operator attempts to utilize any module services, the service will not be invoked and status output will be provided via the return value of the APDU. The status output provided in the APDU response packet will be '6F 00'. In order to transition out of the FIPS error state, the module must be power-cycled.

2.10 Mitigation of Other Attacks

The FEITIAN-FIPS-COS is not designed to mitigate any specific attacks outside of those required by FIPS 140-2, including but not limited to power consumption, timing, fault induction, or TEMPEST attacks.

[18] CRC – Cyclical Redundancy Check

3 Secure Operation

The FEITIAN-FIPS-COS meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

3.1 Initial Setup

The module is delivered with a pair of AES Keys ($INIT\_KEY_{enc}$ and $INIT\_KEY_{mac}$) to allow authentication and secure initialization 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.

It is the Crypto-Officer's responsibility to configure the module into the FIPS-Approved mode or operation. In order to do this the Crypto-Officer shall ensure the following:

- Only keys of the proper length shall be loaded into the module.
  - Symmetric Keys which are input shall be greater than or equal to 112 bits.
  - All RSA Keys input shall be greater than or equal to 1024 bits.
- The Crypto-Officer role shall ensure that all files require Secure Channel Protocol to access

For additional information regarding module initialization please refer to the FEITIAN-FIPS-COS User Manual [3].

3.1.1 Zeroization

In the case that zeroization is required, the Crypto-Officer shall maintain sole physical possession of the cryptographic module until all keys have been zeroized.

4 Acronyms and Terms

This section describes the acronyms and terms.

Table 13 – Acronyms and Terms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
API	Application Programming Interface
CA	Certification Authority
CBC	Cipher-Block Chaining
CLA	Class Byte of the APDU message header
CMVP	Cryptographic Module Validation Program
COS	Card Operating System
CRC	Cyclical Redundancy Check
CRDO	Control Reference Data Object
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
EEPROM	Electronically Erasable Programmable Read-Only Memory
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FID	File Identifier
FIPS	Federal Information Processing Standard
FW	Firmware
GND	Ground
HW	Hardware
IC	Integrated Circuit
ID	Identifier
IEC	International Electrotechnical Commission

Acronym	Definition
INS	Instruction byte of the APDU message header
ISO	International Organization for Standardization
KAT	Known Answer Test
KDF	Key Derivation Function
MAC	Message Authentication Code
MF	Master File
MSE	Manage Security Environment
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
PC	Personal Computer
PKCS	Public-Key Cryptography Standards
PID	Personal Identification Number Index
PIN	Personal Identification Number
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
Triple-DES	Triple Data Encryption Standard

5 References

This section describes the acronyms and terms.

Table 14 – References

Reference Number	Reference
1	ISO/IEC 7816-4:2005 (E) : Identification cards – Integrated circuit cards – Part 4, Second edition, 2005-01-15
2	Design Solution for the FT_FIPS_COS, 1.0.0
3	FEITIAN-FIPS-COS User Manual, V1.0

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com