SafesITe Large Memory Dual Interface Open Platform card

FIPS140-2 Level 3

Cryptographic Module Security Policy

Table of Contents

1. INTRODUCTION

This document defines the Security Policy for **SafesITe Large Memory Dual Interface Open Platform card,** also referred to as “cryptographic module”. This cryptographic module is composed mostly of a silicon chip containing a microprocessor, a crypto-processor, and an operating system burned in Read Only Memory (ROM), designed to be embedded on a plastic card to produce the **SafesITe Large Memory Dual Interface Open Platform** smart card.

The cryptographic module is submitted for validation, in accordance with FIPS140-2 Level 3 standard.

Included are a description of the security requirements for the cryptographic module and a qualitative description of how each security requirement is achieved. In particular, this security policy specifies the security rules under which the cryptographic module must operate.

Figure 1 Crypto module

2. OVERVIEW

SafesITe Large Memory Dual Interface Open Platform cryptographic module from Axalto contains a microprocessor, a crypto-processor and memory to provide a secure storage for critical information and custom programs, and processing capabilities to interact with these elements. This module is compliant with JavaCard™ specification, which enables issuers to load and run their own processes, called applets, written in Java programming language.

This product can be used to manage keys and passwords, to store and update account information, personal data, and also control debit/credit operations. Smart cards deployment covers a wide range of applications such as Internet security, Banking, mobile telecommunication, loyalty and health care. This cryptographic module brings new services, as well as increased security, portability, and convenience, to computer applications.

This cryptographic module combines the advantages of Java programming language with the ones of the cryptographic features provided by micro modules. Security comes from both software and hardware. Data security and process integrity are provided thanks to JavaCard™ features of the operating system. In addition, this cryptographic module hardware provides tamper-resistance and tamper-evidence features, that meet FIPS140-2 Level 3 physical requirements.

SafesITe Large Memory Dual Interface Open Platform cryptographic module is compliant with JavaCard™ specification (JC) Version 2.2.1 and Global Platform specification (GP) Version 2.1.1 [GP211], which define a secure infrastructure for post-issuance programmable smart cards. JavaCard™ specification defines JavaCard ™ Application Programming Interface (API) that can be used by application developers to take advantage of the various on-board cryptographic services. It also defines virtual machine interpreter and execution context that allow applications (applets) written in Java to be loaded onto this cryptographic module and placed into execution. Global Platform specification defines a life cycle for programmable smart cards to enable post-issuance features. Transitions between each stage of this life cycle involve well-defined sequences of operations.

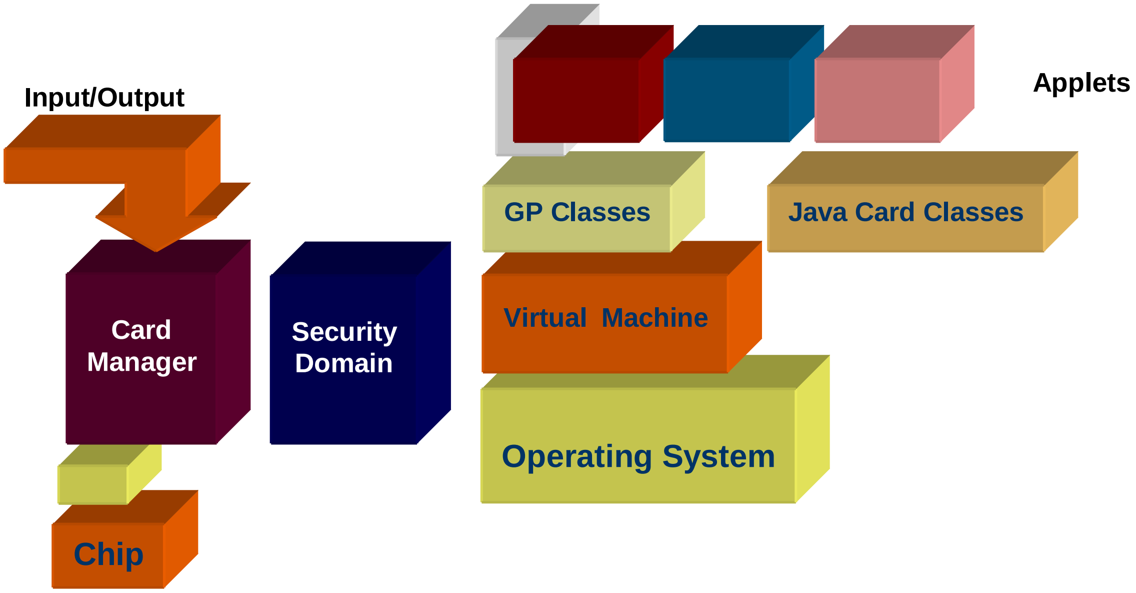

Figure 2 Internal Infrastructure

Once this cryptographic module is initialized, the Card Manager controls Input and Output. Card issuers can open secure channels to authenticate themselves and communicate securely with the card to load applets and exchange information when the card it is inserted into a Card Acceptance Device (CAD), or card reader. Each applet can provide custom commands, which can be accessed by external applications to deliver specific services.

This cryptographic module, validated to FIPS 140-2, is the Java Card platform, without any applet.

Applets that are loaded after validation must also be validated to FIPS140-2 in order to make the validation for the overall product applicable.

If an applet, which is not FIPS validated, is loaded on this module, the module loses its FIPS validation.

3. SECURITY LEVEL

SafesITe Large Memory Dual Interface Open Platform cryptographic module is designed and implemented to meet the Level 3 requirements of FIPS140-2. The cryptographic module enforces FIPS mode of operation at all times.

The individual security requirements, specified for FIPS 140-2, meet the level specifications indicated in the following table.

Security Requirements Section	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	3

4. CRYPTOGRAPHIC MODULE SPECIFICATION

SafesITe Large Memory Dual Interface Open Platform cryptographic module supports a command set aimed at allowing the mutual authentication of identities using strong cryptography with “card acceptance devices” in ISO mode (and PCs or other terminals that they might be connected to). Specifically, the Triple-DES algorithm is used within authentication commands between the cryptographic module and the “card acceptance device” environment to authenticate identities. Establishment of identities using these commands is then used to fulfill “access conditions” which limit the ability of the external world to access information and/or commands on this cryptographic module.

This validation effort will be aimed at the Systems software, virtual machine, and Card Manager application without any applets. If applets are added to this cryptographic module, then these additional applets will need to go through a separate validation and will need to be FIPS 140-2 validated. Consequently, this cryptographic module together with the approved applets will still be FIPS140-2 validated.

This cryptographic module adheres to the various ISO/IEC specifications for Integrated Circuit Chip (ICC) based identification cards. The “cryptographic boundary” for this cryptographic module vis-à-vis the FIPS 140-2 validation is the “module edge”. The module is comprised of the chip (ICC), the hard opaque epoxy, the contact faceplate, and the micro-electronic connectors between the chip and contact pad. The antenna is outside the module.

4.1 MODULE IDENTIFICATION

SafesITe Large Memory Dual Interface Open Platform cryptographic module is a single chip implementation of a cryptographic module. This cryptographic module chip is comprised of the following elements:

- Hardware, an ICC with version number A1002878
- System software is installed in Read Only Memory (ROM) as part of the chip manufacturing process (known as Hard mask) and in Electrically Erasable, Programmable Read Only Memory (EEPROM) for system options and additional customized software (known as soft mask). Two version numbers identifies software: one for the Hard Mask (HM) and one for the Soft Mask (SM). Note that in the smart card world, Hard Mask refers to software stored in ROM; in other guises, this might be referred to as “firmware”.
  These hard mask and soft mask identification numbers are returned in the response to the MaskTrack command.
- Applets that are to be loaded on this cryptographic module (not part of the present validation),
- Critical Security Parameters stored in EEPROM as part of this cryptographic module personalization operation.

This SP applies to four configurations referred to as P1, P2, P3 and P4.

In P1 all algorithms defined in §5.2.6 are enabled in contact and Contactless mode. Contactless mode is Type A
In P2 all algorithms defined in §5.2.6 are enabled in contact and Contactless mode. Contactless mode is Type B
In P3 AES, RSA, and SHA 1 crypto algorithms are disabled in Contactless mode. Contactless mode is Type A
In P4 AES, RSA, and SHA 1 crypto algorithms are disabled in Contactless mode. Contactless mode is Type B

These four configurations can be identified by hardmask, softmask and personalization numbers returned by the Mask Track command. The four configurations have the same Hardmask and softmask numbers: HM 4v1, SM 1v1 respectively, since they belong to the same product. Each configuration has a different Personalization number from 1 to 4 (for P1 to P4).

4.2 Module Interfaces

SafesITe Large Memory Dual Interface Open Platform cryptographic module has two modes of operations: Contact mode and Contactless mode. Mode is determined at power-up, depending on the interface (contact or contact-less) that powered the module. It cannot be changed until the module is reset.

4.2.1 Contact Mode

Electrical and physical interface of this cryptographic module is comprised of the 5-electrical contacts from the surface of the module to the chip. These contacts conform to the following specifications.

4.2.1.1 Physical Interface description

This cryptographic module supports eight contacts that lead to pins on the chip. Only five of these are connected. Location of the contacts complies with [ISO7816-2].

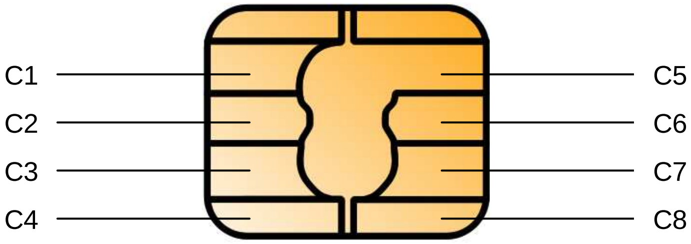

Figure 3 Design of Contact Interface

Contact dimensions are compliant to [ISO 7816-1].

Electrical features of the card are described in [ISO 7816-3].

Communication between the reader and this cryptographic module is based on a standardized, serial, half-duplex character transmission, ISO 7816 protocol, T=0 and T=1 as described in [ISO 7816-3].

4.2.1.2 Logical Interface Description

Once electrical (physical) contact and data link layer contact is established between the module and the reader, the module functions as a “slave” processor to implement and respond to card reader commands. This cryptographic module adheres to a well-defined set of state transitions. Within each state, a specific set of commands is accessible.
Details of these commands are listed hereafter. This module also provides an additional set of internal services through the Java Card ™ APIs.

The logical interfaces are connected to the physical interfaces as follows:

Logical interface	Physical interface
Data input	C7
Data output	C7
Status output	C7
Control input	C2, C3, and C7
Power input	C1 and C5

C4, C6 and C8 are not connected.

4.2.2 Contactless Mode

4.2.2.1 Physical Interface description

In Contactless mode, the cryptographic module uses only two electrical connections, L1 and L2. These are specific contacts, connected to the antenna.

In this mode Radio frequency power and signal interface are defined in [ISO 14443-2], Type A - P1 & P3 - or Type B - P2 & P4-.

Communication between the Proximity Coupling Device (PCD) and this cryptographic module is based on a standardized, half-duplex character transmission, ISO 14443 protocol, T= CL, defined in [ISO 14443-4].

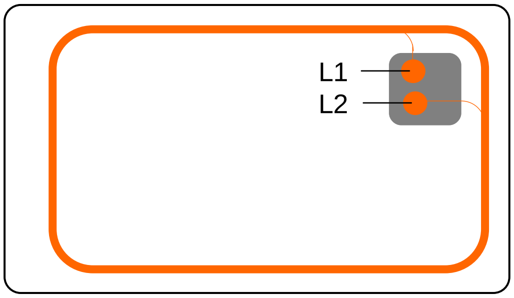

Figure 4 Design of Contactless interface

Contactless interface is using the 13,56MHz frequency to communicate. The card may embed additional Contactless devices using different frequencies to communicate. These additional devices are out of the scope of this Security Policy.

4.2.2.2 Logical Interface Description

Once communication is established between the module and the PCD, the module functions as a “slave” processor to implement and respond to the PCD commands.

The APDU commands are the same in Contact and Contactless mode.

All logical interfaces are connected to L1 and L2 that receive and transmit data, controls, status and power to and from the antenna.

5. ROLES & SERVICES

5.1 ROLES

SafesITe Large Memory Dual Interface Open Platform cryptographic module defines two distinct roles that are supported by the internal cryptographic system: the Cryptographic Officer and the User.

- ***Cryptographic Officer***: This role is the internal security controller. Cryptographic Officer (CO) establishes his identity on the module by demonstrating to the Card Manager application that he possesses the knowledge of a Triple-DES key set stored within the Card Manager. By successfully executing the INIT UPDATE and EXT AUTH commands, the Cryptographic Officer establishes a secure channel to the Card Manager. The establishment of this channel includes mutual authentication of identities between the Cryptographic Officer and the Card Manager. Once secure channel is established, the Card Manager grants authorization (on the module) to information and services. The Card Manager corresponds to Card Issuer Security Domain.

- ***User/Applet Provider***: Applet Provider is the applet developer that uses Java API, provided by the module. Cryptographic services provided by the cryptographic module are delivered through the use of appropriate APIs. An applet has its own Security Domain (Applet Provider Security Domain). The User role is an entity with knowledge of the Security Domain Triple-DES key set and authenticates in the same manner as the CO.

Identity based Authentication

- ***Identification.*** The operator identifies himself by selecting the application appropriate for his role and the key set inside the application. The application of Cryptographic Officer is the Card manager. The application of Applet Provider is the Security Domain. Selection of the application is done by a SELECT command. Selection of key set is done in the INITIALIZE UPDATE, the first command of the two commands to open a Secure Channel.

- ***Authentication.*** The operator authenticates himself using a mutual authentication comprising two commands INITIALIZE UPDATE and EXTERNAL AUTHENTICATION. During this mutual authentication, the operator has to encrypt a message sent by the card, proving knowledge of the Triple-DES key set, which was referenced during the identification.

Notes:

1. The Cardholder is the end user of this cryptographic module (when applets are loaded), who is in charge of insuring the ownership of his cryptographic module.
2. Applets that will be loaded onto thiscryptographic module may define other distinct roles that will be part of the applet's validation.

Card Manager is the controlling application on this cryptographic module. It is invoked following every cryptographic module reset and initialization operations.

5.2 SERVICES

5.2.1 Crypto Officer Administrative Services

A set of commands is provided to Crypto Officer for Security Domain administration and applet loading onto SafesITe Large Memory Dual Interface Open Platform cryptographic module. This set of commands can be used only by Crypto Officer or by Applet Providers (Users) owning a Security Domain instance with Delegated Management (DM) privilege.

This set includes the following commands:

- ***INSTALL (CO):*** install an application or a Security Domain. It requires invocation of different internal functions. INSTALL command is used to instruct Card Manager (or Security Domain with Delegated Management privilege) as to which installation step it shall perform during an application installation process.

- ***LOAD (CO):*** this command is used to load byte-codes of the Load File (package) defined in the previously issued INSTALL command.

- ***DELETE (CO):*** this command is used by Crypto Officer (or the owner of a Security Domain with Delegated Management privilege) to delete a Loaded File (package), an Application (applet instance) or a Security Domain.

Applets loaded onto this cryptographic module must be FIPS 140-2 validated.

Prior to Applet loading, Crypto Officer establishes a Secure Channel with the Card Manager during the Identification/authentication process. Applet is divided in a series of blocks that fit in a LOAD command. Loading is made of a series of LOAD commands, each one transmitting a block, encrypted and followed by a Triple-DES CBC MAC, computed with the Triple-DES key set selected by Crypto Officer during the identification process. The Triple-DES CBC MAC ensures the correct transmission of each block of the applet, therefore ensuring the correct transmission of the whole applet.

Additionally (and optionally) a mechanism called “GP DAP” enables the applet provider to check, independently of the Issuer, that his applet has been correctly loaded. The applet provider can perform this check by one of the two following means:

- The “GP DAP RSA” is a mechanism that verifies an RSA signature on the CAP file using a 1024-bit DAP public key present on the card. It verifies the integrity of the applet on behalf of the applet provider and it also authenticates applet provider as the originator of the applet.

5.2.2 Crypto Officer & User services

Commands that are available for both Crypto Officer & Users are the following commands:

- **SELECT**: this command is used to select an application (Card Manager, Security Domain or Applet). Card Manager may be selected either to load of a Load File, to install an application loaded previously or to activate a Security Domain. This command is available outside a Secure Channel.

- **INITIALIZE UPDATE**: this command is used to initiate a Secure Channel with Card Manager or a Security Domain. Cryptographic module and host session data are exchanged, and session keys are generated in this cryptographic module upon completion of this command. However, the Secure Channel is not considered open until completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow INITIALIZE UPDATE command.

- **EXTERNAL AUTHENTICATE**: this command is used by this cryptographic module to authenticate host, to establish Secure Channel, and to determine the level of security required for all subsequent commands within Secure Channel. A previous and successful execution of INITIALIZE UPDATE command is required prior to processing this command.

- **PUT DES KEY**: this command is used to add or replace Card Manager & Security Domain key sets, except the RSA DAP public key.

- **PUT RSA KEY**: this command is used to add or replace a key set containing only the RSA DAP or DM 1024-bit public key.

- **SET STATUS**: this command is used to modify the life cycle state of this cryptographic module or the life cycle state of an application.

- **GET STATUS**: this command is used to retrieve information regarding the Card Manager or Applications according to a given search criteria. For example: The life cycle state can be retrieved using this command.

- **STORE DATA**: this command is used to store or replace one tagged data object provided in the command data field.

- **GET DATA**: this command is used to retrieve a single data object. it is available outside Secure Channel (no security condition). However, if issued within a Secure Channel, it must follow the same security level as defined in EXTERNAL AUTH. No CSP are accessible with this command.

- **MANAGE CHANNEL:** This command is used to open or close a logical channel from an already opened logical channel or from the basic logical channel

- **MASK TRACK**: This command allows reading of up to 10 traceability data bytes. It is used to determine that the module is under FIPS approved mode of operation and also to determine the configuration. This command is available outside a Secure Channel.

- **GET SIZE**: This command is provided to retrieve the EEPROM memory size available for new applet loading and/or object instantiation.

- **CHANGE ATR**: This command allows modifying the ATR.

- **READ SERIAL NUMBER**: This command is provided to retrieve chip Serial Number, which identifies the chip and therefore the cryptographic module as unique. This command is available outside a Secure Channel.

All commands except (Select, Initialize Update, External Authentication, Get Data, Read Serial Number, and Mask Track) need a secured channel to be executed. During the secured channel opening, the command access condition is specified (’MAC’, ’MAC+ENC’) and all commands received within the Secure Channel must meet the access condition, failing which the command is rejected & Secure Channel is terminated.

5.2.3 Relationship between Roles & Services

Roles / Services	Crypto -Officer (Card Manager Security Domain)	User/Applet Providers (Applet Security Domain)	Unauthenticated (Any role)
SELECT	X	X	X
INITIALIZE UPDATE			X
EXTERNAL AUTHENTICATE	X	X	
PUT DES KEY	X	X	
PUT RSA KEY(2)	X	X	
INSTALL	X	X(1)	
LOAD	X	X(1)	
DELETE	X	X(1)	
SET STATUS	X	X	
GET STATUS	X	X	
STORE DATA	X	X	
GET DATA	X	X	X
MASK TRACK	X	X	X
GET SIZE	X	X	
CHANGE ATR	X	X	
READ SERIAL NUMBER	X	X	X
MANAGE CHANNEL	X	X	X

Table 1: Roles vs. Services

Note (1) INSTALL, LOAD & DELETE commands are available to Security Domains having the Delegated Management privilege.

Note (2) The Put RSA Key command is only used to import the RSA Public Key used for DAP or Delegated Management

5.2.4 Services available for Applets

SafesITe Large Memory Dual Interface Open Platform Cryptographic Module implements a secure environment for execution of User-developed applications, known as JavaCard Applets. Applets that are developed and downloaded onto the module shall use the cryptographic module JavaCard APIs. These APIs are only available to applets. So they are not accessible before an applet is loaded, and are presented here as information to the User who would develop applets with the goal of obtaining a separate validation encompassing both this Cryptographic Module and their applets.

These APIs are listed in the CO/User guidance document. Among them, the ones that contain cryptographic services are the following:

- Key Generation:
  - RSA key pair generation: this API generates a pair of RSA keys.
- Key Wrapping:

  - RSA algorithm API supports key wrapping/unwrapping for the key establishment. Key wrapping uses an RSA public key. Key unwrapping uses an RSA private key.
- Message Digest:
  - SHA-1: this API performs a SHA-1 Message Digest,
- Random Numbers Generation:
  - Secure Random Generation: this API generates a random data, using ANSI X9.31 FIPS140-2 approved method (Deterministic RNG).
- Signature and Verification:
  - RSA SHA-1 PKCS1 mode. Signature uses an RSA private key. Verification uses an RSA public key.
- Origin authentication and Data integrity verification:
  - Triple-DES: these APIs offer Triple-DES MAC in CBC mode with various padding (no padding, ISO9797 M1 and M2),
  - AES: these APIs offer AES in CBC mode with various padding (no padding, ISO9797 M1 and M2),
  - RSA SHA-1 PKCS1 mode. Verification uses an RSA public key.
- Bulk Encryption/Decryption:
  - DES (non-compliant)/Triple-DES: these APIs offer DES (non-compliant)/Triple-DES CBC or ECB mode using various padding (no padding, ISO9797 M1 and M2),
  - AES: these APIs offer AES CBC or ECB mode using various padding (no padding, ISO9797 M1 and M2),
- PIN

  PIN APIs are available for applets to authenticate the cardholder.

These algorithms shall be used only in a FIPS approved mode of operation. This will be checked during applet's validation. We recall that only FIPS 140-2 validated applets shall be loaded on the cryptographic module.

GP specification defines also various APIs that may be used by applets and provide the same services as the Card Manager Commands (such as secure channel opening). In particular, the Global PIN may be implemented by applets through the use of a dedicated API.

5.2.5 Relationship between Roles and APIs services

All the above-mentioned applet services can be accessed by applets owned by Card issuer or owned by another Provider. This means that these services can be related to keys stored in Card Manager (Crypto Provider), a Security Domain, or in an Applet Security Domain.

5.2.6 Card Cryptographic Functions

The purpose of SafesITe Large Memory Dual Interface Open Platform cryptographic module is to provide a FIPS approved platform for applets that may in turn provide cryptographic services to end-user applications.
Keys represent the identity of the roles involved in controlling this cryptographic module.
Triple-DES, AES, RSA and SHA-1 algorithms are provided as services to applets that may be loaded onto this cryptographic module. These algorithms are presented via the Java Card API and shall be used only in a FIPS approved mode of operation. Validation of the use of these cryptographic services in a Java Card applet is subject to a separate validation involving applets. This cryptographic module validation does not include any applets.

This cryptographic module cryptographic functions are as follows:

- DES [non-compliant]:
  - DES is used together with Triple-DES to compute a retail MAC, which is used as an EDC for the "GP DES DAP" and for the DM Receipt. Data over which retail MAC is calculated is considered protected by an Error Detection Code (EDC).

  - DES functions are also provided as services to applets, through JavaCard APIs. Applets must not use DES in an Approved mode.

- **Triple-DES, (Triple-DES 2-Key or Triple-DES 3-Key) [Cert.** #479**]:**
  - Triple-DES 2-Key (CBC mode) algorithm is used
    - As a Triple-DES MAC to authenticate Crypto Officer (EXTERNAL AUTH command) by verifying the host cryptogram.
    - As a Triple-DES MAC to authenticate the originator and to verify integrity of messages.
    - To encrypt APDU data flow from the off module to the on-module environment. The status field is not encrypted; i.e. the status words returned in response to an APDU are not encrypted

  - Triple-DES 2-Key (ECB mode) algorithm is used
    - To generate the Triple-DES session keys in the Secure Channel protocol.
    - To decrypt keys input using the Put DES KEY APDU.

  - Triple-DES 2-Key is also used together with DES as an EDC (cf. DES).
  - Triple-DES 2-Key and Triple-DES 3-Key functions are also provided as services to applets, through JavaCard APIs.

- **AES [Cert.#** 463**]:**
  - AES functions are only provided as services to applets through JavaCard APIs.
  - In P3 & P4 configurations, AES functions are disabled in Contactless mode

- **SHA-1 [Cert.#** 531**]:**
  - SHA-1 message digest is used in the RSA signature.
  - It is used in DAP and DM.
  - It is also provided as a service through JavaCard APIs to applets.
  - In P3 & P4 configurations, SHA-1 is disabled in Contactless mode

- **RSA (1024, 1536, 2048 bit keys) [Cert.** #183**]:**
  - RSA is used for the “OP RSA DAP” mechanism to verify a firmware package loaded on the card.
  - RSA is used for the DM to verify the token signature input along with a DM command APDU.
  - RSA functions are also provided as services to applets, through JavaCard APIs. The applet shall use RSA only for “key wrapping” or “signature” operations. This will be checked during the applet’s FIPS validation.
  - In P3 & P4 configurations, RSA functions are disabled in Contactless mode

- **DRNG ANSI X9.31 [Cert.** #248**]:**
  - The DRNG function that uses Triple-DES 2-Key is used to generate a nonce during the INITIALIZE UPDATE command.
  - It is provided as a service through JavaCard APIs to applets.
  - It is also used in the RSA key generation to generate primes. RSA key generation is provided as a service to applets through JavaCard APIs.

5.2.7 Self-Tests

5.2.7.1 Power Up Self Tests

SafesITe Large Memory Dual Interface Open Platform cryptographic module performs the required set of self-tests before executing any cryptographic operation.
When a CAD with a contact or Contactless interface powers module up, it sends back (as specified by ISO/IEC 7816) an Answer To Reset (ATR) with static data about the module. Then it waits for the first command.

When first command arrives, the module executes the power-up Self-Tests.

Power-up Self-Tests include:

- RAM functional test & clearing at Reset,
- EEPROM Firmware integrity check with a CRC-16. This test is performed on the softmask and packages stored in EEPROM.
- Algorithm (known answer) tests for:
  - CRC-16,
  - Triple-DES - decrypt
  - AES - encrypt/decrypt,
  - SHA-1 Hashing,
  - RSA SHA PKCS1 sign and verify.
  - DRNG

If any of these tests fails, this cryptographic module responds with a self-test error status. Then, the cryptographic module goes mute. No data of any type is transmitted from the cryptographic module to the CAD while self-tests are performed and in mute state.

In P3 and P4 configurations, in Contactless mode, AES, SHA and RSA algorithms being disabled, the corresponding self-tests are not performed.

5.2.7.2 Conditional Tests

RSA Key generation:

A pair wise consistency check is performed during key generation in which a sign/verify operation is performed using the newly generated key pair to ensure their consistency. ..
Note that this operation can only be activated by applets. It is therefore out of scope of this validation.

Random Number Generator:

NDRNG: A 64 bits continuous testing is performed on the Hardware non-deterministic RNG. The NDRNG is used to generate seed & seed key values to feed the DRNG.
DRNG: A 64 bits continuous testing is performed during each use of the FIPS140-2 approved deterministic RNG based on ANSI X9.31.

Software/Firmware load test

A Triple-DES CBC MAC is verified whenever an applet is loaded onto this cryptographic module. This MAC is linked to secure messaging.
An optional DAP verification is made. The algorithm used is RSA PKCS#1 signature with a 1024-bit key. DAP is required if a Security Domain with mandated DAP privilege has been instantiated on the module.

5.3 CRITICAL SECURITY PARAMETERS (CSP):

5.3.1 Cryptographic Keys:

The SafesITe Large Memory Dual Interface Open Platform cryptographic module contains the following keys:

1. Triple-DES Card Manager key set, 2 of which are used for CO authentication and generation of session keys and stored in EEPROM. The 3rd key (K_{KEK}) in the key set is used for key encryption. Each key in the key set is a 16-byte Triple-DES key.
2. Triple-DES Card Manager Session keys. These consist of a session 16-byte encryption key (S-ENC) used for APDU data encryption/decryption using Triple-DES & a 16-byte session MAC key (S-MAC) used for APDU MAC generation & verification using Triple-DES MAC.

And in addition, the key sets of each applet Security Domain.

3. Triple-DES Applet Security Domain key set used in the same manner as Card Manager Keyset, but used for User authentication.
4. Triple-DES Applet Session keys used in the same manner as Card Manager Session keys.

Key sets #1 & #3 are loaded/replaced on the card with the Put DES Key command.
The Session keys in #2 & #4 are temporary keys stored in RAM and zeroized when the Secure Channel is terminated.

5.3.2 Other CSPs

The SafesITe Large Memory Dual Interface Open Platform cryptographic module cryptographic module includes of the following CSPs:

- Seed and Seed Keys: This cryptographic module includes a DRNG X9.31. This DRNG uses an 8-byte Seed and an 16-byte Seed Key as inputs to the DRNG. The seed & seed-key values are generated by the hardware RNG and stored only in RAM. These values are zeroized when the module is reset in contact mode or when the module is deselected in contactless mode.

6. SECURITY RULES

6.1 IDENTIFICATION & AUTHENTICATION SECURITY RULES

The module implements specific methods for identifying and authenticating the different roles. The implementation consists of the binding of Identity-based Access Control Rules to each service that requires authentication.

6.1.1 User Identification and Authentication

- **User/Applet Provider Authentication**: User/Applet Provider must prove the possession of the Applet Security Domain Key Set composed of 3 Triple-DES keys. Two keys are used to authenticate the command payload. A third key is used to encrypt keys transported within APDU command. This is the same process as the Crypto Officer authentication (Initialize Update & External Authenticate commands) but it uses the Triple-DES keys of the Applet Security Domains.

6.1.2 Cryptographic Officer Identification &Authentication

- **Crypto Officer Authentication**: Cryptographic Officer must prove the possession of this cryptographic module Manager Key Set composed of 3 Triple-DES keys. Two keys are used to authenticate the command payload. A third key is used to encrypt keys transported within the APDU command (Initialize Update & External Authenticate commands).

6.1.3 Attempt Counter

- **Attempt Counter**: An attempt counter is associated with each key set of a Security Domain or the Card Manager.
- **Initialization**: This counter is set to 3 at the creation of the key set and at each successful authentication using this key set.
- **Decrementation**: This counter is decremented by 1 at each unsuccessful authentication using this key set. When the counter reaches 0, the key set is blocked, which means that it cannot be used any more for authentication.

6.2 FIPS MODE OF OPERATION

The cryptographic module enforces FIPS mode of operation at all times.
This hardmask & softmask version, FIPS mode and configuration of the card can be determined by the MASK TRACK APDU with the following expected output in the data field:

Byte Offset	Value	Meaning
‘00’	47h	Founder code
‘01’	ECh	Component Code
‘02’	04h	Hardmask Code
‘03’	01h	Hardmask Version
‘04’	01h	Softmask Code
‘05’	01h	Softmask Version
‘06’	00h	Applet Code
‘07’	00h	Applet Version
‘08’	06h	EEPROM image version / Chip Revision number

‘09’	01h	RSA,AES & SHA-1 enabled; Type A
	02h	RSA,AES & SHA-1 enabled; Type B
	03h	RSA,AES & SHA-1 disabled; Type A
	04h	RSA,AES & SHA-1 disabled; Type B

6.3 APPLET LOADING SECURITY RULES

6.3.1 Integrity and Confidentiality of the loading

Only applets validated to FIPS 140-1 or 140-2 shall be loaded onto this cryptographic module.
Applets can only be loaded through a secure channel; i.e. they pass from the off module to the on-module environment in MACed form.
This is the only mandatory rule. It guaranties the integrity of applet during its loading. The applet data must also be encrypted if Secure Channel mode Is MAC+ENC.

6.4 ACCESS CONTROL SECURITY RULES

- Secret Keys are always loaded in encrypted form.

6.5 PHYSICAL SECURITY RULES

Physical security of this cryptographic module is designed to meet FIPS 140-2 level 3 requirements. A hard opaque epoxy is used to encapsulate the module to meet level 3 requirements. From the time of its manufacture, this cryptographic module is under control of Cryptographic Officer until it is ultimately issued to the end user.

6.6 KEY MANAGEMENT SECURITY POLICY

6.6.1 Cryptographic key generation

- Triple-DES Session keys for Secure Channel Opening, conforming to Open Platform Card Specification v2.1.1 using FIPS140-2 approved ANSI X9.31 DRNG to generate challenge data.
- RSA key pair generation using FIPS140-2 approved ANSI X9.31 DRNG. Keys are generated in CRT format.

6.6.2 Cryptographic key entry/output

Secret Keys shall always be input in encrypted format, using the Put DES Key command. In this command, keys are encrypted using the K_{kek} Key and the Triple-DES ECB algorithm. This command is passed within a secure channel that may be MAC+ENC. In this case the keys transferred are encrypted once again, using the S-ENC session key.

6.6.3 Cryptographic key storage

Keys are structured to contain the following parameters:

- Key id, which is the Id of the key,
- Algo Id, which determines which algorithm to be used,
- Integrity Mechanisms (CRC-16).

6.6.4 Cryptographic key zeroization

SafesITe Large Memory Dual Interface Open Platform cryptographic module zeroizes cryptographic keys by reloading another key-set for Crypto Officer keys, Security Domains Applets Keys, or closing of secure channel for session keys**.** Seed & seed-key are zeroized from RAM by resetting the card.
Key Management Details can be found in the CO / User Guidance document.

6.7 MITIGATION OF ATTACKS SECURITY POLICY

The SafesITe Large Memory Dual Interface Open Platform cryptographic module has been designed to mitigate the following attacks:

- Timing attacks,
- Simple Power Analysis,
- Differential Power Analysis.
- Differential Fault Analysis

7. SECURITY POLICY CHECK LIST TABLES

7.1 ROLES & REQUIRED AUTHENTICATION

Role	Type of authentication	Authentication data
Crypto Officer	Triple-DES authentication	Triple-DES keys (Card Manager keyset) & 8-byte cryptogram
User/Applet Provider	Triple-DES authentication	Triple-DES keys (Applet Security Domain keyset) & 8-byte cryptogram

7.2 STRENGTH OF AUTHENTICATION MECHANISMS

Authentication Mechanism	Strength of Mechanism
Triple-DES authentication	Probability that a random attempt succeeds is much less than 1 in 1,000,000
Triple-DES authentication	With an attempt counter of 3, probability that a random attempt in 1 minute succeeds is much less than 1 in 100,000

7.3 SERVICES AUTHORIZED FOR ROLES

Role	Authorized Services
Crypto Officer	CO Administrative Services as listed in Section 5.2.1 CO & User Services as listed in Section 5.2.2
User/Applet Provider	CO & User Services as listed in Section 5.2.2. APIs as listed in Section 5.2.4.

7.4 ACCESS RIGHTS WITHIN SERVICES

CSP	Service	Role	Types of Access
Card Manager Keyset	PUT DES KEY command	Crypto Officer	Write
Card Manager Keyset PRNG Seed & Seed key	INITIALIZE UPDATE	Crypto Officer	Execute Execute
Card Manager Keyset Card Manager Session keys	EXTERNAL AUTH	Crypto Officer	Execute Execute
Card Manager K_{KEK} Card Manager Keyset	PUT DES KEY command	Crypto Officer	Execute Write
Triple-DES CO Session Keys	INITIALIZE UPDATE	Crypto Officer	Create
Triple-DES CO Session Key: S_{enc}	Message encryption	Crypto Officer	Execute
Triple-DES CO Session Key: S_{mac}	Message integrity	Crypto Officer	Execute
Card Manager Keyset	PUT DES KEY command	Crypto Officer	Write
Security Domain Keyset PRNG Seed & Seed key	INITIALIZE UPDATE	User	Execute Execute
Security Domain Keyset Security Domain Session keys	EXTERNAL AUTH	User	Execute Execute
Security Domain K_{KEK} Security Domain Keyset	PUT DES KEY command	User	Execute Write
Triple-DES User Session Keys	INITIALIZE UPDATE	Crypto Officer	Create
Triple-DES User Session Key: S_{enc}	Message encryption	Crypto Officer	Execute
Triple-DES User Session Key: S_{mac}	Message integrity	Crypto Officer	Execute
Seed	DRNG computation	Crypto Officer/User	Execute
Seed Key	DRNG computation	Crypto Officer/User	Execute

7.5 MITIGATION OF OTHER ATTACKS

Other Attacks	Mitigation Mechanism	Specific Limitations
Timing attacks	Counter Measures against Timing attacks	N/A
Simple Power Analysis	Counter Measures against SPA	N/A
Differential Power Analysis	Counter Measures against DPA	N/A
Differential Fault Analysis	Counter Measures against DFA	N/A

8. REFERENCES

Reference	Title
[FIPS140-2]	National Institute of Standards and Technology, FIPS 140-2 standard.
[FIPS140-2A]	National Institute of Standards and Technology, FIPS 140-2 Annex A: Approved Security Functions.
[FIPS140-2B]	National Institute of Standards and Technology, FIPS 140-2 Annex B: Approved Protection Profiles.
[FIPS140-2C]	National Institute of Standards and Technology, FIPS 140-2 Annex C: Approved Random Number Generators.
[FIPS140-2D]	National Institute of Standards and Technology, FIPS 140-2 Annex D: Approved Key Establishment Techniques
[JCVM221]	Java Card ™ 2.2.1 Virtual Machine Specification, Sun Microsystems
[JCAPI221]	Java Card ™ 2.2.1 Application Programming Interface, Sun Microsystems
[JCRE221]	Java Card ™ 2.2.1 Runtime Environment (JCRE) Specification, Sun Microsystems
[GP211]	Global Platform Card Specification v 2.1.1 - march 2003
[ISO 7816-1]	ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 1: Physical Characteristics
[ISO 7816-2]	ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 2: Dimension and Location of the contacts
[ISO 7816-3]	ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 3: Electronic signals and transmission protocol
[ISO 7816-4]	Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands for interchange
[ISO 14443-2]	Contactless integrated circuit(s) cards – Proximity cards — Part 2: Part 2: Radio frequency power and signal interface
[ISO 14443-3]	Contactless integrated circuit(s) cards – Proximity cards — Part 3: Initialization and anti-collision
[ISO 14443-4]	Contactless integrated circuit(s) cards – Proximity cards — Part 4: Transmission protocol
[X9.31]	American Bankers Association, Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998, Washington, D.C., 1998.
[FIPS 197]	FIPS-197: Advanced Encryption Standard (AES)
[FIPS 46-3]	FIPS-46-3: Data Encryption Standard (DES)
[SP 800-38 A]	NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of operation
[FIPS 180-2]	FIPS-46-3: Secure Hash Standard (SHA)
[RSA PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard
[ISO 9796-2]	ISO/IEC 9796-2

9. ACRONYMS

Acronyms	Definitions
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Application Provider
API	Application Programming Interface
ATR	Answer To Reset
CAD	Card Acceptance Device
CBC	Cipher Block Chaining
CO	Crypto Officer
CRC	Cycling Redundancy Check
CSP	Critical Security Parameter
DAP	Data Authentication Pattern
DES	Data Encryption Standard
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
DM	Delegated Management
DRNG	Deterministic Random Number Generator
ECB	Electronic Code Book
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
ICC	Integrated Circuit Card
ISO	International Organization for Standardization
JC	Java Card ™
JCRE	Java Card ™ Runtime Environment
MAC	Message Authentication Code
NDRNG	Non Deterministic Random Number Generator
GP	Global Platform
PC	Personal Computer
PCD	Proximity Coupling Device
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
RAM	Random Access Memory
RFU	Reserved for Future USE
RNG	Random Number Generator
ROM	Read only Memory
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis