J-IDMark 64 Open

FIPS 140-2 Non-Proprietary Security Policy

Level 3 validation

Version 2

April 2008

Sagem Orga
SAFRAN Group

TABLE OF CONTENTS

GLOSSARY

AES	:	Advanced Encryption Standard
AID	:	Application IDentifier
ALU	:	Arithmetic Logic Unit
APDU	:	Application Protocol Data Unit
API	:	Application Protocol Interface
ATR	:	Answer To Reset
CBC	:	Cipher Block Chaining
CEMA	:	Correlation Electromagnetic Analysis
CO	:	Crypto Officer
CPA	:	Correlation Power Analysis
CSP	:	Critical Security Parameter
DEMA	:	Differential Electromagnetic Analysis
DES	:	Data Encryption Standard
DFA	:	Differential Fault Analysis
DPA	:	Differential Power Analysis
ECB	:	Electronic Code Book
E^2PROM	:	Electrically Erasable and Programmable Read Only Memory
EFP	:	Environmental Failure Protection
EMI	:	Electromagnetic Interference
EMC	:	Electromagnetic Compatibility
FIPS	:	Federal Information Processing Standards
GP	:	Global Platform
ISD	:	Issuer Security Domain
ISO	:	International Organization for Standardization
MAC	:	Message Authentication Code
MOC	:	Match On Card
PKCS	:	Public Key Cryptographic Standards
RAM	:	Random Access Memory
P-RNG	:	Pseudo Random Number Generation
ROM	:	Read Only Memory
RSA	:	Rivest Shamir Adleman
SEMA	:	Simple Electromagnetic Analysis
SHA	:	Secure Hash Algorithm
SPA	:	Simple Power Analysis
SSD	:	Supplementary Security Domain
TDES	:	Triple DES

REFERENCE DOCUMENTS

[FIPS 140-2]	:	National Institute of Standards and Technology, Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules, May 25, 2001
[ISO 7816-2]	:	Identification Cards – Integrated Circuit(s) Cards with Contacts Part 2: Dimensions and location of the contacts
[ISO 7816-3]	:	Identification Cards – Integrated Circuit(s) Cards with Contacts Part 3: Electronic signals and transmission protocols
[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: 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
[JCS]	:	Java Card ™ 2.2.1 Card Specification, Sun Microsystems
[GP]	:	Global Platform Card Specification - Version 2.1.1 - May 2003 – Global Platform – Configuration 3
[FIPS 180-2]	:	National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-2 with Change Notice 1, February 25, 2004
[ANSI 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
[PKCS#1 v2.1]	:	RSA Laboratories, PKCS#1 v2.1: RSA Cryptography Standard, June 14, 2002
[ANSI X9.52]	:	American Bankers Association, Triple Data Encryption Algorithm Modes of Operation, ANSI X9.52 – 1998
[ISO 9797]	:	Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm
[AES]	:	National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001. National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001.

1 INTRODUCTION

1.1 SCOPE

This document is the non-proprietary security policy for the *J-IDMark 64 Open* cryptographic module. This security policy represents the completed *J-IDMark 64 Open* product satisfying all of the requirements for **[FIPS 140-2]** Level 3 (Level 4 for physical security).

1.2 PRODUCT DESCRIPTION

The *J-IDMark 64 Open* module is a dual interface smart card platform with a javacard operating system compliant with Sun Java Card ™ 2.2.1 **[JCS]** and Global Platform 2.1.1 **[GP]** specifications. The *J-IDMark 64 Open* hardware is based on the ATMEL AT90SC 128 72 RCFT chip.

Java technology is the leading multiple application operating system for smart cards. It offers developers a convenient platform on which to develop and implement smart card applets. The *J-IDMark 64 Open* module has been designed to offer a modular and open solution based on reliable and standardized technologies. To that end, the *J-IDMark 64 Open* module contains an implementation of the Sun Java Card ™ 2.2.1 **[JCS]** specifications. It allows implementing multiple applications associated with a high security level to execute the applications by providing context independence between each of them. The *J-IDMark 64 Open* module is also compliant with the Global Platform 2.1.1 **[GP]** specifications where it secures the application management and manages the card life cycle.

The *J-IDMark 64 Open* module design takes full benefit of the ROM space available on the card micro controller by hard masking the operating system. Therefore, the full space of the 64-KB E²PROM is available for loading and instantiating applets.

The *J-IDMark 64 Open* module also implements the following functionalities that will be available for the future applets aimed to be loaded on the platform:

- On board key generation (up to a 2048-bit modulus RSA).
- Depending on the module configuration: Match On Card mechanism, developed by Sagem Défense Sécurité, for fingerprint verification.
- File system.

1.3 PRODUCT IDENTIFICATION

The *J-IDMark 64 Open* cryptographic module is available in four different versions, all of them meeting the **[FIPS 140-2]** Level 3 requirements:

- three versions, each supporting a specific Match On Card mechanism for the use of future applets,
- one version without any Match On Card mechanism.

Therefore identification numbers of the *J-IDMark 64 Open* module are:

- 01016221 - 01016221 for the first version with a PKREF/PKDIN MOC mechanism.
- 01016221 - 02016247 for the second version with an ANSI/ISO MOC mechanism.
- 01016221 - 03016251 for the third version with an ANSI/ISO MOC mechanism.
- 01016221 - FFFFFFF for the fourth version without any MOC mechanism.

The overall hardware part number identifier is AT58803, which is available in versions J, L and M. The identification number of the *J-IDMark 64 Open* module can be retrieved at any time.

1.4 SECURITY LEVEL

The *J-IDMark 64 Open* product is designed to meet the overall requirements applicable to the Level 3 of the **[FIPS 140-2]** specifications. Moreover, the *J-IDMark 64 Open* is compliant with the Level 4 requirements for physical security (**[FIPS 140-2]**, Area 5). The area-specific security levels are described in Tab 1.

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	4
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of other Attacks	3

Tab 1: *J-IDMark 64 Open* area specific levels

1.5 FIPS APPROVED ALGORITHMS

The algorithms used in the FIPS Approved mode of operation of the *J-IDMark 64 Open* module are listed in Tab 2. All of them offer FIPS Approved functionalities.

Algorithms	***Standard***	***Description***
SHA-1	**[FIPS 180-2]**	Hash (for signature)
SHA-256	**[FIPS 180-2]**	Hash (for signature)
RSA	**[PKCS#1 v2.1]**	RSA Key generation
		RSA Signature
		RSA Signature verification
TDES	**[ANSI X9.52]**	Data encryption / decryption in ECB mode
		Data encryption / decryption in CBC mode
TDES MAC	**[ISO 9797]**	Data integrity – MAC calculation / verification
AES	**[AES]**	Data encryption / decryption in ECB mode
		Data encryption / decryption in CBC mode
P-RNG	**[ANSI X9.31]**, Appendix A.2.4	Random number generation

Tab 2: *J-IDMark 64 Open* algorithms

The *J-IDMark 64 Open* module additionally employs the non-deterministic hardware random number generator of the ATMEL AT90SC 128 72 RCFT chip to seed the FIPS Approved **[ANSI X9.31]** P-RNG function.

1.6 FIPS MODE OF OPERATION

The *J-IDMark 64 Open* cryptographic module only supports a FIPS Approved mode of operation.

This FIPS Approved mode of operation of the *J-IDMark 64 Open* module is indicated by a specific value of a dedicated byte in the ATR.

Therefore it is possible to check that the module is indeed working in a FIPS Approved mode of operation:

- at power-up in contact mode by looking at the value of the ATR,
- at any time (in both contact and contactless mode) by asking the module to output the value of the ATR.

2 CRYPTOGRAPHIC MODULE SPECIFICATION

2.1 OVERVIEW

In the scope of this document, the cryptographic module is embodied by a single chip Integrated Circuit with its embedded firmware. The base chip is the ATMEL dual interface chip with reference AT90SC 128 72 RCFT.

The *J-IDMark 64 Open* firmware is composed of an operating system complying with the **[JCS]** and **[GP]** standards.

The *J-IDMark 64 Open* cryptographic module is designed to be encased in a hard opaque resin that can be embedded into a plastic card or any other support structure. An antenna shall also be connected to the *J-IDMark 64 Open* module for the purpose of contactless communication. However, neither the resin nor the antenna reside within the cryptographic boundary.

2.2 CRYPTOGRAPHIC MODULE BOUNDARY

The cryptographic module boundary is realized as the external surface of the ATMEL AT90SC 128 72 RCFT single chip microprocessor and does not include the resin, the micro-bonds, the smart card contact plate, the fixation glue nor the antenna. The boundary contains all of the relevant module components (processors performing cryptography, etc.) consistent with **[FIPS 140-2]**. There are no component exclusions from the boundary.

2.3 DESCRIPTION

The *J-IDMark 64 Open* cryptographic module is composed of the ATMEL AT90SC 128 72 RCFT single chip microprocessor, which includes:

- 128 KB of ROM
- 72 KB of E²PROM
- 5 KB of RAM

The *J-IDMark 64 Open* cryptographic module operates under contact or contactless communication mode (but not under both modes at the same time). The *J-IDMark 64 Open* module remains in FIPS mode of operation regardless of the communication mode (contact or contactless) being used to interface external devices.

The module has no internal power supply (battery, capacitor, etc.). All power to the module (provided by smart card reader) enters the power input interface through the voltage bond pad or the contactless electrical connections. The defined voltage range for normal conditions of use is: 2.7 V to 5.5 V.

Figure 1 shows the architecture of the *J-IDMark 64 Open* cryptographic module.

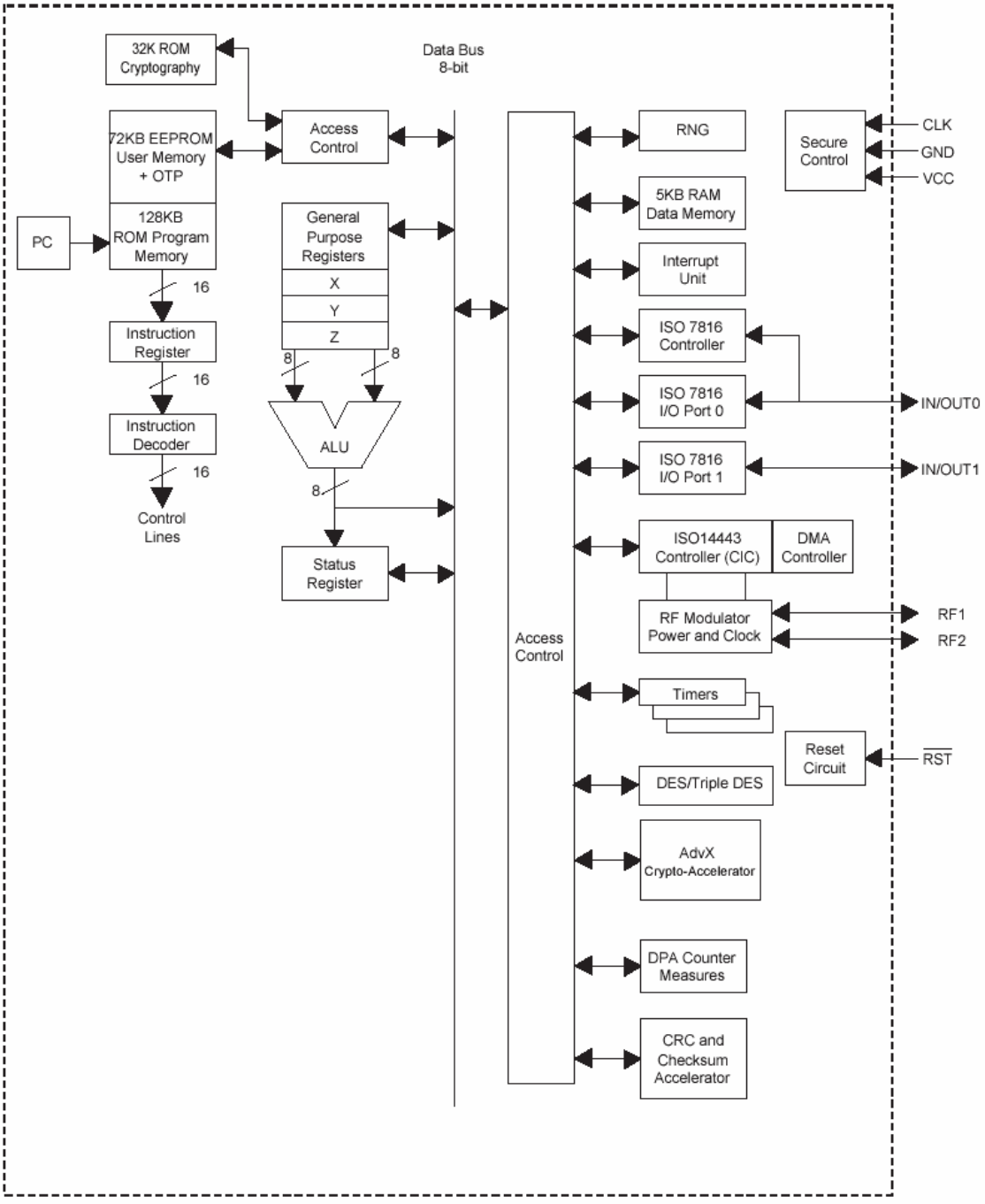

Figure 1: *J-IDMark 64 Open* block diagram*

* ATMEL information

3 CRYPTOGRAPHIC MODULE PORTS AND INTERFACES

3.1 PHYSICAL PORTS

The physical ports of the *J-IDMark 64 Open* cryptographic module consist of both the contact and contactless interfaces of the chip. The ports used in the contact mode are physically different from the ports used in contactless mode.

3.1.1 Contact mode physical interface

For the contact interface, the physical ports of the *J-IDMark 64 Open* module consist of the bond pad locations of the chip and conform to the **[ISO 7816-2]** specifications. Tab 3 lists the physical ports of the module for the contact interface.

Physical ports	***Description***
VCC	Power supply (Voltage)
RST	Reset signal
CLK	Clock signal
GND	Ground
IN/OUT 0	Data Input/Output
IN/OUT 1	Not Used

Tab 3: Description of the contact physical ports

Micro-bonds can connect the cryptographic module physical ports to a contact plate compliant with the **[ISO 7816-2]** specifications. Micro-bonds and contact plate are not included in the cryptographic boundary but are still described hereafter for illustration purposes.

The contact plate is composed of 8-electrical contacts and is connected to the chip via the micro-bonds, which supply the chip with data I/O communications, clock, power and control functionality between the chip and the end-users.

The specific definitions for the contacts and the relation to the physical ports of the *J-IDMark 64 Open* are shown in Figure 2 and Tab 4:

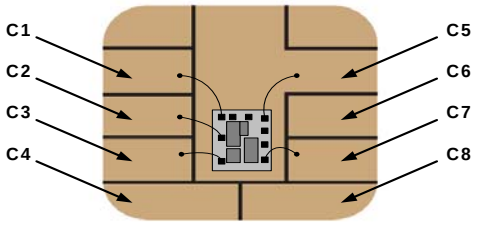

Figure 2: Contact plate description

Contact number	*Assignment*	*Module bond pad*
C1	Power supply (Voltage)	VCC
C2	Reset signal	RST
C3	Clock signal	CLK
C4	Not used	/
C5	Ground	GND
C6	Not Used	/
C7	Data Input/Output	IN/OUT 0
C8	Not used	/
/	Not used	IN/OUT 1

Tab 4: Functional specification of the contact plate

3.1.2 Contactless mode physical interface

For the contactless interface, the physical ports of the *J-IDMark 64 Open* cryptographic module consist of two electrical connections and conform to the **[ISO 14443-2]** specifications. Tab 5 lists the physical ports of the module for the contactless interface.

Port name	*Description*
RF1	Clock Power Communication link with the reader
RF2	

Tab 5: Description of the contactless physical ports

The two electrical connections RF1 and RF2 are used to close the loop of an external antenna. When the cryptographic module is close to a card reader producing an electromagnetic field, the antenna, which is an inductive coupling area, provides an energizing field that also generates a sub carrier that modulates the transmission of digital information. This antenna is not included in the cryptographic boundary but is still mentioned here for a better understanding of the cryptographic module.

Figure 3 shows a typical embedding of the cryptographic module with the antenna: the top and bottom layers of a smart card sandwich the whole chip with antenna. The antenna is typically 3 to 5 turns of very thin wire or conductive ink, connected to the chip.

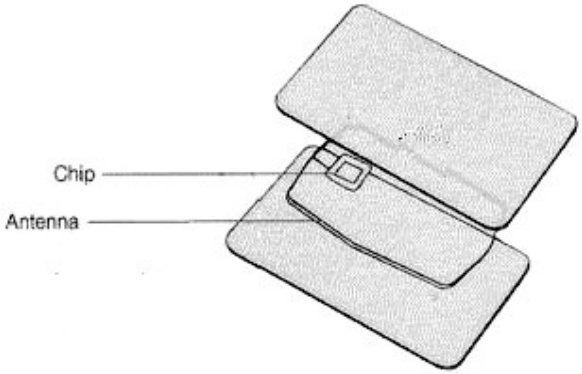

Figure 3: Chip with antenna

3.2 LOGICAL PORTS

3.2.1 Contact mode logical interface

The *J-IDMark 64 Open* adheres to the **[ISO 7816-3]** specifications regarding the contact interface, which describe the relationship between the cryptographic module and its host (e.g. smart card reader) as one of "slave" and "master," respectively.

Communications are established by the host, which sends signals to the cryptographic module through the contacts defined in § 3.1.1. Communication then continues by the cryptographic module sending an appropriate response back to the host. The communication channel is single-threaded: once the host sends a command to the cryptographic module, it waits until a response is received. No overlapping between multiple command-response pairs is allowed.

Messages between the cryptographic module and the host are conveyed using the T=0 link level protocol defined in **[ISO 7816-3]**.

The cryptographic module receives and executes a well-defined set of APDU commands sent by the host and answers with APDU responses according to the **[ISO 7816-4]** specifications. The APDU communication protocol defines the following four logical interfaces:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

All logical interfaces are mapped to appropriate physical ports according to Tab 6.

Physical interfaces	***Logical interfaces***
VCC	Power
RST	Control Input
CLK	Control Input
GND	Power
IN/OUT 0	Data Input Data Output Control Input Status Output

Tab 6: **Physical to logical interface mapping**

3.2.2 Contactless mode logical interface

The *J-IDMark 64 Open* adheres to the **[ISO 14443-3]** and **[ISO 14443-4]** specifications regarding the contactless interface. Communications are based on the **[ISO 14443-3]** T=CL half-duplex transmission protocol.

Tab 7 describes the logical ports of the cryptographic module for the contactless interface and their mapping to the physical ports.

Port name	***Logical interface***
RF1	Power Data input Data output Control input Status output
RF2	

Tab 7: Functional specification of the contactless interface

4 ACCESS CONTROL POLICY

4.1 ROLES

Tab 8 presents the two roles supported by the *J-IDMark 64 Open* module.

Role	***Description***
CO	The CO has access to the ISD. He is in charge of ISD management, applet code loading, applet instantiation, SSD creation and SSD personalization. He can associate any created applet instance to a SSD or let this instance be linked to the ISD.
User	A User has access to a given SSD. He is in charge of the management of this SSD.

Tab 8: Role description

4.2 AUTHENTICATION

The *J-IDMark 64 Open* module supports identity-based authentication according to Level 3 requirements for the roles, services and authentication area of **[FIPS 140-2]**. Tab 9 presents the authentication mechanisms associated to the corresponding roles.

Role	***Type of Authentication***	***Authentication data***
CO	Mutual authentication	ISD CO key set (ISD_K_{ENC}, ISD_K_{MAC})
User	Mutual authentication	SSD User key set (SSD_K_{ENC}, SSD_K_{MAC})

Tab 9: Roles and required authentication

The identity-based feature is achieved through the mutual-authenticate functionality:

- The CO is uniquely identified by the identification number of the ISD and the identification number of his ISD CO key set.
- A User is uniquely identified by the identification number of the selected SSD and the identification number of his SSD User key set.

The ability to change from one role to another is strictly enforced by the *J-IDMark 64 Open* design:

- All previous authentication records are cleared when a new authentication takes place.
- All authentication-related records are also cleared from memory when the module power is removed. Prior authentication information is no longer available.

Therefore, it is not possible to have more than one authenticated operator on the *J-IDMark 64 Open* module at the same time.

4.3 AUTHENTICATION STRENGTH

4.3.1 Role authentication mechanisms strength

Tab 10 presents the strength of the authentication mechanisms.

Authentication mechanism	***Description***	***Probability that a random authentication attempt succeeds***	***Probability that multiple random authentication attempts within a one minute period succeed***
CO authentication	Mutual authentication (symmetric scheme)	Less than $1/10^6$	Less than $1/10^5$
User authentication			

Tab 10: Strength of the FIPS Approved role authentication mechanisms

4.3.2 Other authentication mechanisms strength

Fingerprint verification

Depending on the *J-IDMark 64 Open* module version, a MOC mechanism may be available for the use of the future validated applets which will be loaded. It is not actually used by the *J-IDMark 64 Open* itself to authenticate a role.

This feature performs a 1:1 comparison between the fingerprint template coming from a biometric sensor and the biometric reference stored in the module. The module can be configured so that one or two fingerprints comparison is needed for the authentication to succeed.

The strength of this authentication mechanism (whether with one or two fingerprints) is better than $1/10^6$ for a one-time guess and $1/10^5$ for multiple attempts in a 1-minute period.

PIN verification

Future validated applets loaded on the *J-IDMark 64 Open* may use the Global PIN for file access control or applet role authentication. It is not used by the *J-IDMark 64 Open* itself to authenticate a role.

This authentication mechanism can provide a strength better than $1/10^6$ for a one-time guess and $1/10^5$ for multiple attempts in a 1-minute period.

4.4 SERVICES

4.4.1 Services description

Tab 11 describes the services of the *J-IDMark 64 Open* module and the security functions used at the invocation of each service.

Services	***Description***	***Security functions***
SELECT	Selection of the ISD, a SSD or an applet instance.	
GET_DATA	Retrieving general information (including ATR value) from the ISD or from an SSD.	
INIT	CO or User authentication and opening of a secured channel.	TDES, TDES MAC
GET_STATUS	Retrieving the life cycle data of Executable Load Files, Executable Modules, ISD, SSDs or applications, according to a given match/search criteria.	
SET_STATUS	Modification of the life cycle state of the card (ISD state) and locking or unlocking of SSDs and applets.	
INST_INST	Creation of an applet instance or a SSD, with its AID and its capability to be selected by default.	
INST_EXTR	Association of an ISD applet instance to a given SSD.	
LOAD	Loading of applet software	
STORE_DATA	Storage of a set of information in the ISD or in a SSD.	TDES
PUT_DES_KEY	Modification of a TDES key (ISD CO key set, ISD Key Encryption key, SSD User key set or SSD Key Encryption key).	TDES
PUT_RSA_KEY	Set a RSA public key (SSD DAP key).	TDES
DELETE	Deletion of an applet instance or of code or of an Executable Load File.	
SELF_TESTS	Execution of power-up self-tests.	TDES, AES, SHA-1, SHA-256, RSA, P-RNG
TERMINATE	Zeroization of the whole E^2PROM.	

Tab 11: *J-IDMark 64 Open* services overview

4.4.2 Services Access Control

The crypto module uses identity-based control to access the services of the *J-IDMark 64 Open* module. Tab 12 presents the authorized roles for each service.

The term 'No role' is used to identify services for which authentication is not required. Indeed, initiating the act of authentication, by nature, does not require an authenticated state for this module.

Services	***CO***	***User***	***No role***
SELECT	X	X	X
GET_DATA	X	X	X
INIT			X
GET_STATUS	X		
SET_STATUS	X		
INST_INST	X		
INST_EXTR	X		
LOAD	X		
STORE_DATA	X	X	
PUT_DES_KEY	X	X	
PUT_RSA_KEY		X	
DELETE	X		
SELF_TESTS	X	X	X
TERMINATE	X		

Tab 12: Service access control

4.5 CSPS DESCRIPTION

Tab 13 presents the cryptographic keys and other CSPs of the *J-IDMark 64 Open* module.

CSPs	***Description***
ISD CO key set (ISD_K_{ENC}, ISD_K_{MAC})	Two static double TDES keys, that are used to derive the ISD CO Session key set as part of the CO authentication. There is one ISD CO key set per module.
ISD Key Encryption key (ISD_K_{KEK})	A static double TDES key used to cipher CSPs entering the module. There is one ISD Key Encryption key per module.
ISD CO Session key set (ISD_SK_{ENC}, ISD_SK_{MAC})	Two double TDES keys, derived from the ISD CO key set using the SCP.01 protocol, used to authenticate the CO.
SSD User key set (SSD_K_{ENC}, SSD_K_{MAC})	Two double TDES keys used to derive a SSD User Session key set as part of a User authentication. There is one SSD User key set per SSD.
SSD Key Encryption key (SSD_K_{KEK})	A static double TDES key used to cipher CSPs entering the module. There is one SSD Key Encryption key per SSD.
SSD User Session key set (SSD_SK_{ENC}, SSD_SK_{MAC})	Two double TDES keys, derived from a SSD User key set using the SCP.01 protocol, used to authenticate a User.
SSD DAP key (SSD_K_{DAP})	A RSA public key dedicated to a SSD used to verify the signature of the loaded software. There is at most one SSD DAP key per SSD.
E^2PROM Protection key	A double TDES key used to cipher the E^2PROM key storage location.
P-RNG Seed key	A double key generated by the non-deterministic hardware random number generator and used to seed the Approved **[ANSI X9.31]** P-RNG function.

Tab 13: **Cryptographic keys and CSPs overview**

4.6 CSPS ACCESS CONTROL

Tab 14 presents services access rights to cryptographic keys and CSPs stored in the *J-IDMark 64 Open* module.

CSPs	***Services***	***Operations***	***Role***
ISD CO key set (ISD_K_{ENC}, ISD_K_{MAC})	INIT	Execution	CO
	PUT_DES_KEY	Modification	CO
	STORE_DATA	Modification	CO
	TERMINATE	Zeroization	CO
ISD Key Encryption key (ISD_K_{KEK})	PUT_DES_KEY	Modification	CO
	STORE_DATA	Modification/Ciphering	CO
	TERMINATE	Zeroization	CO
ISD CO Session key set (ISD_SK_{ENC}, ISD_SK_{MAC})	INIT	Derivation/Execution	CO
SSD User key set(s) (SSD_K_{ENC}, SSD_K_{MAC})	INIT	Execution	User
	PUT_DES_KEY	Modification	User
	STORE_DATA	Modification	User
	TERMINATE	Zeroization	CO
SSD Key Encryption key(s) (SSD_K_{KEK})	PUT_DES_KEY	Modification	User
	STORE_DATA	Modification/Ciphering	User
	TERMINATE	Zeroization	CO
SSD User Session key set (SSD_SK_{ENC}, SSD_SK_{MAC})	INIT	Derivation/Execution	User
SSD DAP key(s) (SSD_K_{DAP})	PUT_RSA_KEY	Modification	User
	STORE_DATA	Modification/Ciphering	User
	TERMINATE	Zeroization	User
E^2PROM Protection key set	PUT_DES_KEY	Execute	CO/User
	PUT_RSA_KEY	Execute	User
	TERMINATE	Zeroization	CO

Tab 14: CSPs access rights within services

5 PHYSICAL SECURITY

5.1 [FIPS 140-2] LEVEL 4 REQUIREMENTS

The *J-IDMark 64 Open* module is designed and manufactured to fulfill the requirements of **[FIPS 140-2]** Level 4 physical security:

- Opacity
- Tamper resistance and tamper evidence
- Physical penetration testing
- Chemical testing
- EFP for temperature and voltage (note: clock frequency protections are also in place).

All the hardware, firmware and data components of the module are physically protected. The module does not contain any door, ventilation hole or removable cover. No maintenance access interface, as defined in **[FIPS 140-2]**, is available.

5.2 SECURITY MECHANISMS

The module implementation is a production grade, commercially available single chip device (ATMEL AT90SC 128 72 RCFT), which contains the following hardware security features:

- Voltage monitor
- Frequency monitor
- Light protection
- Temperature monitor.

For values of voltage, clock input frequency, UV light or temperature which go outside acceptable bounds, the module prevents further operation by entering an error state and remaining mute until the card is reset. Therefore the security of the module is not compromised by unusual environmental conditions outside of the module's normal operating range.

5.3 MODULE ENCAPSULATION

The physical encapsulation of the chip is a metallic layer, which covers sensitive circuitry and thus prevents all the sensitive components from being visible. It provides advanced protection against physical attacks and fulfills the physical tampering and probing requirements. Therefore, if an attacker tries to remove metallic layer of the module, the owner of the *J-IDMark 64 Open* module will notice the attempt just by looking at the module.

6 OPERATIONAL ENVIRONMENT

Only **[FIPS 140-2]** validated applets may be downloaded on the *J-IDMark 64 Open* module.

This module performs the software/firmware load test on all new code, and as such the *J-IDMark 64 Open* cryptographic module is defined as possessing a limited operational environment.

The Operational Environment requirements of **[FIPS 140-2]** Area 6, therefore, do not apply to the *J-IDMark 64 Open* cryptographic module.

It is noted that the loading of validated applets will result in a different FIPS module (combination of platform and applet or applets) referenced by a separate FIPS 140 certificate.

7 CRYPTOGRAPHIC KEY MANAGEMENT

7.1 KEY OVERVIEW

Tab 15 gives an overview of all the cryptographic keys used in the *J-IDMark 64 Open* module.

Cryptographic keys	***Key size (bits)***	***Approved algorithms***
ISD CO key set	Encryption key: ISD_K_{ENC}: 112	TDES
	Mac key: ISD_K_{MAC}: 112	TDES MAC
ISD Key Encryption key	ISD_K_{KEK}: 112	TDES
ISD CO Session key set	Encryption key: ISD_SK_{ENC}: 112	TDES
	Mac key: ISD_SK_{MAC}: 112	TDES MAC
SSD User key set	Encryption key: SSD_K_{ENC}: 112	TDES
	Mac Key: SSD_K_{MAC}: 112	TDES MAC
SSD Key Encryption key	SSD_K_{KEK}: 112	TDES
SSD User Session key set	Encryption key: SSD_SK_{ENC}: 112	TDES
	Mac Key: SSD_SK_{MAC}: 112	TDES MAC
E²PROM Protection key	Encryption key: 112	TDES
SSD DAP key	SSD_K_{DAP}: 1024 to 2048	RSA
P-RNG Seed key	Seed key: 112	P-RNG

Tab 15: Cryptographic key overview

7.2 KEY GENERATION

No cryptographic key is generated on board.

A FIPS Approved RSA CRT key pair generation function, compliant with **[PKCS#1 v2.1]**, is available to the future applets loaded on the *J-IDMark 64 Open*. This function relies on a FIPS Approved pseudo random number generation algorithm compliant with **[ANSI X9.31]**.

7.3 ENTRY/OUTPUT

All static cryptographic keys are always input in the module ciphered with a CSP encryption key (the ISD Key Encryption key or a SSD Key Encryption key).

Cryptographic keys are never output from the cryptographic module.

7.4 STORAGE

Static cryptographic keys are stored in E²PROM and are prevented from disclosure, modification and substitution by:

- An API which does not allow those operations.
- An integrity check for each key.
- A dedicated key (the E²PROM Protection key) which encrypts the E²PROM area where cryptographic keys are stored.

7.5 ZEROIZATION

There is a zeroization mechanism to actively overwrite all static cryptographic keys and other CSPs stored in the E²PROM.

In addition, session keys (ISD CO Session key set and SSD CO Session key set) are erased at the end of each session.

8 EMI/EMC

The cryptographic module has been tested to meet the EMI/EMC FCC Part 15 Class B requirements.

9 SELF-TESTS

The *J-IDMark 64 Open* cryptographic module performs a set of self-tests to ensure that it is working properly.

9.1 POWER-UP SELF-TESTS

The *J-IDMark 64 Open* module performs the following self-tests at power-up:

- E²PROM software/firmware integrity check.
- **[ANSI X9.31]** Pseudo random number generation known answer test.
- TDES 2 key CBC ciphering/deciphering known answer test.
- AES CBC ciphering/deciphering known answer test.
- RSA CRT signature & SHA-1 known answer test.
- RSA signature verification known answer test.
- SHA-256 known answer test.

9.2 CONDITIONAL SELF-TESTS

The *J-IDMark 64 Open* performs the following conditional self-tests:

- RSA key pair wise consistency check after each RSA key pair generation. No cryptographic key is actually generated on board by the J-IDMark 64 Open platform itself. But a FIPS Approved RSA CRT key pair generation function is available to the future applets loaded on the J-IDMark 64 Open. Therefore the corresponding self-test is also available for the use of the future applets.
- Hardware random number generation continuous test.
- **[ANSI X9.31]** Pseudo random number generation continuous test.
- TDES MAC Firmware Load Test (Note: New Applet code is applicable only to future validated cryptographic modules based on this product).
- CRC integrity check for CSPs.

9.3 SELF-TESTS ON DEMAND

The suite of cryptographic power-up self-tests may be performed at any time by repowering the module.

9.4 SELF-TESTS FAILURE

If any self-test fails, the cryptographic module outputs a specific status, enters an error state and remains mute until the card is reset.

Moreover, in case the self-test failing is the E²PROM software/firmware integrity check, then the *J-IDMark 64 Open* module outputs a specific status related to this particular error and enters a terminate state. The module then will not boot any more after repowering.

10 MITIGATION OF OTHER ATTACKS

The *J-IDMark 64 Open* module implements countermeasures to protect against the attacks listed in Tab 16:

Attacks	***Countermeasures***
SPA/SEMA	Countermeasures against SPA/SEMA attacks
Timing	Countermeasures against Timing attacks
DPA/DEMA	Countermeasures against DPA/DEMA attacks
CPA/CEMA	Countermeasures against CPA/CEMA attacks
DFA	Countermeasures against DFA attacks

Tab 16: Mitigation of other attacks

Note: As an expanded security feature above **[FIPS 140-2]** single chip requirements, when the chip detects that its shield (metallic layer) is broken or damaged, it triggers a security mechanism that, by erasing the E²PROM, will definitively render the *J-IDMark 64 Open* module unusable. Therefore, if an attacker tries to remove the shield of the module, he will not be able to access to any sensitive information.

11 SECURITY RULES

The following represents the security rules established for and supported by the *J-IDMark 64 Open* cryptographic module.

11.1 SECURE OPERATION SECURITY RULES

- The *J-IDMark 64 Open* module does not allow itself to return to the personalization lifecycle state once personalization has been performed: personalization can therefore only be performed once.
- Operators of the *J-IDMark 64 Open* should verify at power-up of the card in contact mode the value of the byte in the ATR which indicates that the card is **[FIPS 140-2]** Level 3 compliant.
- Operators of the *J-IDMark 64 Open* shall have at any time the capability, both in contact and contactless mode, to check whether the module is **[FIPS 140-2]** Level 3 compliant or not.
- Operators of the *J-IDMark 64 Open* shall have the capability at any time to retrieve its identification number.
- All the applets loaded on the *J-IDMark 64 Open* module shall be **[FIPS 140-2]** compliant; otherwise the module shall lose its validation.
- The *J-IDMark 64 Open* shall execute a TDES MAC verification of the code of the applets loaded on the module. Additionally, a signature verification with a SSD DAP key may be performed.
- CO and Users shall have the capability to check that the module is working properly. This can be done by requesting the serial number data of the module. If the command answers, then the module is working correctly. If the command does not answer, then the module is either in error state, powered off or terminated. The module shall be distinctive in indicating which of these states it occupies.
- The *J-IDMark 64 Open* module shall not allow data output during self-tests, zeroization and error states.

11.2 AUTHENTICATION SECURITY RULES

- CO and Users shall not share or disclose their secret authentication data to unauthorized operators.
- After reception of the *J-IDMark 64 Open* module, the User shall update his authentication data.
- No authentication record shall be kept after power down of the module.
- The strength of each authentication mechanism shall be better than $1/10^6$ for a one-time guess and $1/10^5$ for multiple attempts in a 1-minute period.
- Only one authenticated operator shall be accepted on the *J-IDMark 64 Open* module at a time.

11.3 KEY MANAGEMENT SECURITY RULES

- The module shall contain a zeroization service for all CSPs stored in E²PROM.
- The *J-IDMark 64 Open* module shall rely on CSP encryption keys for the protection of all CSPs entering or leaving the cryptographic boundary.

11.4 PHYSICAL SECURITY RULES

- The card shall be inspected periodically for evidence of tampering.
- Access to the module shall be limited prior to initialization based on the physical security protections and the lack of available interfaces prior to and during initialization.
- For values of voltage, clock input frequency, UV light, or temperature which go outside acceptable bounds, the module shall remain mute until it is reset.
- An E²PROM integrity check failure shall lead to terminate the *J-IDMark 64 Open* module.

11.5 SELF-TESTS SECURITY RULES

- The *J-IDMark 64 Open* module shall perform power-up self-tests automatically, without operator intervention.
- The operator of the module shall be able to perform power-up self-tests at any time, on demand.
- When a self-test fails, the module shall output a specific status and enter an error state.
- Moreover, if the self-test failing is the E²PROM software/firmware integrity check, then the *J-IDMark 64 Open* module shall not be able to boot any more.
- No data shall be output before power-up self-tests are completed.
- No data shall be output when conditional self-tests are performed.