Sagem Orga
SAFRAN Group

J-IDMARK 64

FIPS 140-2 Non-Proprietary Security Policy

Level 3 validation

Version 1.0
October 2006

TABLE OF CONTENTS

GLOSSARY

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
EEPROM	:	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
IC	:	Integrated Circuit
ISO	:	International Organization for Standardization
MAC	:	Message Authentication Code
MOC	:	Match On Card
PIN	:	Personal Identification Number
PKCS	:	Public Key Cryptographic Standards
PKI	:	Public Key Infrastructure
RAM	:	Random Access Memory
PRNG	:	Pseudo Random Number Generation
ROM	:	Read Only Memory
RSA	:	Rivest Shamir Adleman
SDO	:	Security Data Object: SDO are PINs and cryptographic keys
SE	:	Security Environment
SEMA	:	Simple Electromagnetic Analysis
SHA	:	Secure Hash Algorithm
SM	:	Secure Messaging
SPA	:	Simple Power Analysis
TDES	:	Triple DES

REFERENCE DOCUMENTS

[ISO 7816-2] : Identification Cards – Integrated Circuit(s) Cards with Contacts
Part 2: Dimensions and location of the contacts

[ISO7816-3] : Identification Cards – Integrated Circuit(s) Cards with Contacts
Part 3: Electronic signals and transmission protocols

[ISO7816-4] : Identification Cards – Integrated Circuit(s) Cards with Contacts
Part 4: Inter-industry commands for interchange

[FIPS 140-2] : National Institute of Standards and Technology, Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) , May 25, 2001

[JCS] : Java Card ™ 2.1.1 Card Specification, Sun Microsystems

[GP] : Visa Global Platform Card – Implementation Requirements – Configuration 1 – Compact Version 2.0.1, February 2002

[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

[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

1 INTRODUCTION

1.1 SCOPE

This document is the non-proprietary security policy for the J-IDMark 64 (HW P/N AT58829-C-AA, Version 01, FW Version J-IDMark 64 IDT 005) cryptographic module. This security policy represents the completed J-IDMark 64 (with Applet ID v1) satisfying all of the requirements for **[FIPS 140-2]** level 3 (level 4 for physical security).

1.2 PRODUCT DESCRIPTION

The J-IDMark 64 cryptographic module is based on the Sagem Orga implementation of the Java Card ™ Platform. It is a single chip cryptographic Java Card ™ module, which runs an Applet written in the Java programming language. The Applet, called ID v1, installed on the J-IDMark 64, has been designed in order to be **[FIPS 140-2]** level 3 validated. The J-IDMark 64 hardware (HW P/N AT58829-C-AA, Version 01, FW Version J-IDMark 64 IDT 005) is based on the Atmel AT90SC25672RCT 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 product has been designed to offer a modular and open solution based on reliable and standardized technologies. To that end, the J-IDMark 64 module contains an implementation of the Sun Java Card ™ 2.1.1 **[JCS]** specifications, in which the ID v1 application is developed in Java standard language. The J-IDMark 64 module is also compliant with the Global Platform 2.0.1 **[GP]** specifications where it secures the application management and manages the life cycle of the card and the ID v1 application. Open Platform APIs offer security services as well.

The J-IDMark 64 module design takes full benefit of the large ROM space available on the card micro controller by hard masking the operating system and the ID v1 applet. Therefore, the full space of 64-Kbyte EEPROM is available for end users.

The ID v1 Applet can be instantiated several times prior to the card issuance but not at any time thereafter. The Applet includes the following features:

- The PKI-based digital signature is able to perform highly secure cryptographic transactions (up to 2048-bit RSA) and digital certificate management. The on board key generation is possible up to a 2048-bit modulus RSA. Therefore, it is possible to perform enhanced digital signatures, key wrapping and authentication with RSA.
- The file system allows secure storage of various data and identification management rights (driving/fishing licenses, health care entitlement, car certificate, etc.) loaded on the card.
- The Match On Card feature, provided by Sagem Défense Sécurité, performs 1:1 comparison between the fingerprint template coming from a biometric sensor and the biometric reference stored in the card. The comparison is carried out by the card micro controller with biometric algorithms. This feature reinforces security, as it is impossible to write a biometric template on the card without the proper card access privileges.

1.3 SECURITY LEVEL

The J-IDMark 64 module is designed to meet the overall requirements applicable to the level 3 of the **[FIPS 140-2]** specifications. Moreover, J-IDMark 64 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: [FIPS 140-2] security requirement sections for level 3

1.4 FIPS MODE OF OPERATION

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

At power-up, a specific value of a dedicated byte in the ATR demonstrates that the module is indeed a FIPS validated module.

The FIPS Approved algorithms used in the approved mode of operation are listed in Tab 2:

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

* RSA (Key wrapping, key establishment methodology provides between 80 and 112 bits of encryption strength)

Tab 2: J-IDMark 64 algorithms

The module additionally employs a non-deterministic hardware random number generator to seed the FIPS Approved ANSI X9.31 PRNG function.

2 CRYPTOGRAPHIC MODULE SPECIFICATION

2.1 OVERVIEW

In the scope of this document, the cryptographic module is embodied by a single chip Integrated Circuit (IC) with its embedded software. The chip reference is the contact interface chip, AT90SC25672RCT, and is provided by ATMEL.

The J-IDMark 64 software is composed of the ID v1 applet that relies on a limited operational environment operating system complying with the **[JCS]** and **[GP]** standards.

The life cycle of the J-IDMark 64 can be divided into two phases:

- The personalization phase, which addresses data and CSP loading.
- The field use, which corresponds to the end usage of the card by the cardholder.

The J-IDMark 64 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. The resin, however, does not reside within the cryptographic boundary.

2.2 CRYPTOGRAPHIC MODULE BOUNDARY

The cryptographic module boundary is realized as the external surface of the ATMEL AT90SC25672RCT single chip microprocessor and does not include the resin, the micro-bonds, the smart card contact plate or the fixation glue. 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 cryptographic module is composed of the ATMEL AT90SC25672RCT single chip microprocessor, which includes:

- 256 Kbytes of ROM
- 72 Kbytes of EEPROM
- 8 Kbytes of RAM

Figure 1 shows all the components of the J-IDMark 64 cryptographic module.

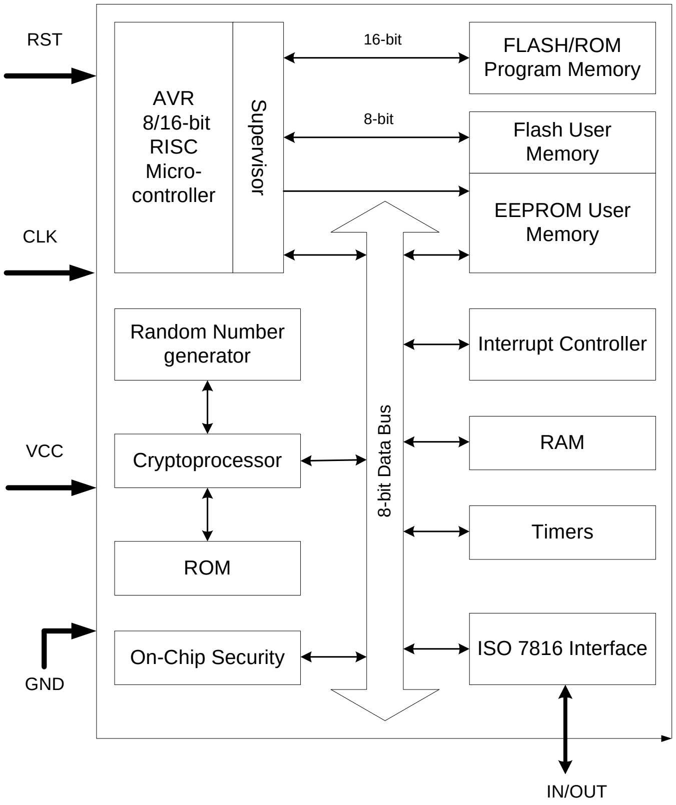

Figure 1: J-IDMark 64 block diagram

The defined voltage range for normal conditions of use is: 1.62 V to 5.5 V.

The J-IDMark 64 cryptographic module operates under contact mode.

3 CRYPTOGRAPHIC MODULE PORTS AND INTERFACES

3.1 PHYSICAL PORTS

The physical ports of the J-IDMark 64 cryptographic 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:

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

Tab 3: Description of the 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 are shown in Figure 2 and Tab 4:

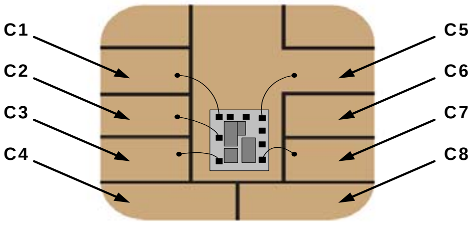

Figure 2: Contact plate description

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
C8	Not used	

Tab 4: Functional specification of the contact plate

All power to the module (provided by smart card reader) enters the power input interface through the voltage bond pad. The module has no internal power supply (battery, capacitor, etc.).

3.2 LOGICAL PORTS

The J-IDMark 64 adheres to the **[ISO7816-3]** specifications, 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. 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.

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 **[ISO7816-4]** 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 5.

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

Tab 5: **Physical to logical interface mapping**

4 ACCESS CONTROL POLICY

4.1 ROLES

Tab 6 presents the three roles supported by the J-IDMark 64 module.

Role	***Description***
Perso CO	This type of cryptographic officer is responsible for managing the setup of the cryptographic module during the personalization phase.
Admin CO	This type of cryptographic officer is in charge of managing ongoing security functions (e.g. unblocking the PIN) during the field use of the J-IDMark 64 module.
User	A user (e.g. a cardholder) who can access data and services according to his access rights during field use of the J-IDMark 64 module. The data access rights are defined during the personalization phase.

Tab 6: Role description

4.2 AUTHENTICATION

Tab 7 presents the identification mechanisms associated to the corresponding roles.

Role	***Type of Authentication***	***Authentication data***
Perso CO	Mutual authentication (symmetric scheme)	Perso key set (two 2-key TDES keys)
Admin CO	Mutual authentication (symmetric scheme)	Admin key set (two 2-key TDES keys)
User	Password	PIN (Global and/or User)
	Biometry	One or two User fingerprint(s)

Tab 7: Roles and required authentication

J-IDMark 64 supports identity-based authentication according to level 3 requirements for the roles, services and authentication section of **[FIPS 140-2]**:

- The Perso CO is uniquely identified by his Perso key set identification number.
- The Admin CO is uniquely identified by the pair: applet ID v1 instance identification number & Admin key set identification number
- Users are uniquely identified by the pair: applet ID v1 instance identification number & PINs or fingerprints identification number.

The ability to change from one role to another is strictly enforced by the J-IDMark 64 features. Moreover, it is not possible to have more than one authenticated operator on the J-IDMark 64 module at the same time: all previous authentication records are cleared when a new authentication takes place.

4.3 AUTHENTICATION MECHANISMS

Tab 8 presents the strengths of the different authentication mechanisms.

Authentication mechanism	***Description***	***Strength of mechanism***	
		Probability that a random authentication attempt succeeds	***Probability that multiple random authentication attempts within a one minute period succeed***
Mutual authentication (symmetric scheme)	Perso CO authentication	Less than $1/10^6$	Less than $1/10^5$
	Admin CO authentication		
Password	User PIN or Global PIN verification	Less than or equal to $1/10^6$	Less than or equal to $1/10^5$
Biometry	User Fingerprint matching	Less than or equal to $1/10^6$	Less than or equal to $1/10^5$

Tab 8: Strengths of the authentication mechanisms

Generic access rights for an unauthenticated operator may be controlled using the External keys.

All authentication-related records are cleared from memory when the module power is removed. Prior authentication information is no longer available.

4.4 SERVICES

4.4.1 Services description

Tab 9 describes the services of the J-IDMark 64 module and the security functions used at the invocation of each service.

Services	***Description***	***Security functions***
PERSO_CM.INIT	Beginning of the personalization process and authentication of the Perso CO	PRNG, TDES, TDES MAC
CM.SEL	Selection of an applet instance	
PERSO_CM.END	End of the personalization process	
PERSO_AP.INIT	Perso CO authentication and opening of a secure channel	PRNG, TDES, TDES MAC
PERSO_AP.DATA	Data personalization	
PERSO_AP.SDO	SDOs & SEs personalization	TDES
PERSO_AP.END	End of the applet instance personalization phase	
FMS.SEL	File object selection	
FMS.UPDATE	File object update	
FMS.READ	File object read	
FMS.READ_OBJ	Data object read	
FMS.CREATE	File object creation in applet instance	
FMS.DELETE	File object deletion	
SDO.READ	Read SDO public attribute	
SDO.GEN	Generation of an asymmetric key pair value for an asymmetric RSA key pair SDO	PRNG, RSA
MSE.REST	SE Selection	
MSE.UPDATE	Current SE modification	
MSE.READ	Read current SE	
HASH.LAST	Last block HASH	SHA-1 or SHA-256[1]
AUTH.USER.PWD_ONLY	Password based User authentication	TDES
AUTH.USER.BIO_ONLY	Biometry based User authentication	TDES
AUTH.USER.PWD	PIN verification for file access permission	TDES
AUTH.MUT.SYM	Mutual authentication (symmetric scheme) for: - Admin CO authentication - Secure messaging set up	PRNG, TDES, TDES MAC
AUTH.EXT.SYM	External key verification for file access permission	PRNG, TDES, TDES MAC
AUTH.USER.BIO	Biometric verification for file access permission	TDES
AUTH.USER.READ_BIO	Read biometric information	
AUTH.USER.UNBLOCK	PIN unblocking	TDES
AUTH.USER.CHANGE	PIN modification and biometry initialization	TDES
CARD_TERM.REC	Card signature (asymmetric scheme)	RSA
SIGN.GEN	Data signature for non repudiation	RSA
CONFID.DECIPH	Message key unwrapping	RSA
APPLET.TERMINATE	Zeroization of the whole EEPROM	
SHOW.STATUS	Verification that the module is working properly	
ON.DEMAND.SELFTESTS	Execution of power-up self tests	PRNG, TDES, TDES MAC, SHA-1, SHA-256, RSA

Tab 9: J-IDMark 64 services overview

[1] The choice between SHA-1 and SHA-256 is up to the host.

4.4.2 Services Access Control

The crypto module uses identity-based control to access the services of the J-IDMark 64 module. Tab 10 presents the access control rules and the authorized roles for each service.

The term ‘No role’ is used to identify services for which authentication is not required (note: initiating the act of authentication, by nature, does not require an authenticated state for this module).

Services	***Perso CO***	***Admin CO***	***User***	***No role***
PERSO_CM.INIT	X			
CM.SEL	X	X	X	X
PERSO_CM.END	X			
PERSO_AP.INIT	X			
PERSO_AP.DATA	X			
PERSO_AP.SDO	X			
PERSO_AP.END	X			
FMS.SEL	X	X	X	X
FMS.UPDATE	(1)	(1)	(1)	(1)
FMS.READ	(1)	(1)	(1)	(1)
FMS.READ_OBJ	X	X	X	X
FMS.CREATE	(1)	(1)	(1)	(1)
FMS.DELETE	(1)	(1)	(1)	(1)
SDO.READ	X	X	X	X
SDO.GEN			(1)	
MSE.REST		X	X	X
MSE.UPDATE		X	X	X
MSE.READ		X	X	X
HASH.LAST			X	
AUTH.USER.PWD_ONLY				(2)
AUTH.USER.BIO_ONLY				(2)
AUTH.USER.PWD			(2)	(2)
AUTH.MUT.SYM			(2)	(2)
AUTH.EXT.SYM			(2)	(2)
AUTH.USER.BIO			(2)	(2)
AUTH.USER.READ_BIO		X	X	X
AUTH.USER.UNBLOCK		X		
AUTH.USER.CHANGE			X	
CARD_TERM.REC			(1)	
SIGN.GEN			(1)	
CONFID.DECIPH			(1)	
APPLET.TERMINATE		X		
SHOW.STATUS	X	X	X	X
ON.DEMAND.SELFTESTS	X	X	X	X

Tab 10: Service access control

An X means that the service is available within the role. A reference number (1 or 2) means that there might be one of the following additional access rules to be met in order to completely perform the service:

(1): The access control rule for each accessed file or CSP must be met to successfully perform the service. Access control rules are personalizable and can be: 1) always accessible, 2) never accessible or 3) accessible based on pre-conditions.

Pre-conditions can be:

- Opened secure messaging

and/or

- An External key verification

and/or

- PIN or biometry presentation.

(2): The reset retry counter corresponding to the accessed CSP must be different from 0.

4.5 CRYPTOGRAPHIC KEYS AND CSPS

Tab 11 presents the cryptographic keys and CSPs of the J-IDMark 64 module. All secret and private keys/CSPs are zeroizable via the Zeroize Service (APPLET.TERMINATE).

Cryptographic keys and CSPs	***Description***
Perso CO key set	Two static TDES double keys used to authenticate the Perso CO.
Perso CO session key set	Two TDES keys used to set up a secure messaging during the personalization phase of the module.
Admin CO key set	Two static TDES double keys used to authenticate the Admin CO. There is one Admin CO key set per Applet ID v1 instance.
Admin CO session key set	Two TDES keys used to set up secure messaging after Admin CO authentication.
Card key set	Two static double TDES keys used to perform a mutual authentication between the card and a remote terminal. There is one Card key set per applet ID v1 instance.
Card session key set	Two TDES double keys used to set up secure messaging.
EEPROM area protection key set	Two static TDES double keys used to protect the confidentiality and integrity all PINs and cryptographic keys stored in EEPROM.
CSP encryption key	A static TDES double key used to encrypt any CSPs input in or output from the cryptographic module during the personalization phase and field use. There is one CSP encryption key per applet ID v1 instance. The value of the CSP encryption key can be modified by the Perso CO during the personalization phase.
Global PIN	A PIN represented by 8 alphanumeric characters. The Global PIN is common to all instances of the ID v1 Applet.
User PINs	PINs of minimum 4 alphanumeric characters used to authenticate a user. There is a maximum of 4 different PINs per instance of the ID v1 Applet.
Biometric data	Used to authenticate a user. There is a maximum of 4 different biometric templates per applet ID v1 instance.
External keys	Static TDES double keys used to allow access rights to objects. There is a maximum of 4 different TDES keys per applet ID v1 instance.
RSA private keys	There are up to 3 RSA private keys per applet ID v1 instance used for: - Signatures. - Key unwrapping.
PRNG Seed key	This double key is used to seed the Approved ANSI X9.31 PRNG function. It is generated by the non-deterministic hardware random number generator.

Tab 11: **Cryptographic keys and CSPs overview**

The only public keys are the RSA public key counterparts to the RSA private keys.

4.6 CSPS ACCESS CONTROL

Tab 12 presents the service access rights for each CSP.

CSPs	***Services***	***Operations***
Perso CO key set	PERSO_CM. INIT	Authentication
	PERSO_AP.INIT	Authentication
Admin CO key set	PERSO_AP.SDO	Creation
	AUTH.MUT.SYM	Authentication
	SDO.READ	Read public attribute
	APPLET.TERMINATE	Zeroization
Card key set	PERSO_AP.SDO	Creation
	AUTH.MUT.SYM	Authentication
	SDO. READ	Read public attribute
	APPLET.TERMINATE	Zeroization
CSP encryption key	PERSO_AP.END	Modification
	PERSO_AP.SDO	Decryption
	SDO.READ	Read public attribute
	APPLET.TERMINATE	Zeroization
PINs (global & user)	PERSO_AP.SDO	Creation
	AUTH.USER.PWD_ONLY	Verification
	AUTH.USER.PWD	Verification
	AUTH.USER.CHANGE	Modification
	AUTH.USER.UNBLOCK	Unblock
	SDO. READ	Read public attribute
	APPLET.TERMINATE	Zeroization
Biometric data	PERSO_AP.SDO	Creation
	AUTH.USER.READ.BIO	Reading
	AUTH.USER.BIO_ONLY	Verification
	AUTH.USER.BIO	Verification
	AUTH.USER.CHANGE	Initialization
	AUTH.USER.UNBLOCK	Unblock
	SDO. READ	Read public attribute
	APPLET.TERMINATE	Zeroization
External keys	PERSO_AP.SDO	Creation
	AUTH.EXT.SYM	Verification
	SDO. READ	Read public attribute
	APPLET.TERMINATE	Zeroization
RSA private keys	PERSO_AP.SDO	Creation
	SDO.GEN	Generation
	SDO. READ	Read public attribute
	SIGN.GEN	Data Signature
	CARD_TERM.REC	Signature
	CONFID.DECIPH	Unwrapping
	APPLET.TERMINATE	Zeroization
EEPROM Area Protection key set	No specific service (done automatically)	Encryption/Decryption
		Integrity
	APPLET.TERMINATE	Zeroization

Tab 12: CSPs access rights within services

5 PHYSICAL SECURITY

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

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

The module implementation is a production grade, commercially available single chip device (ATMEL AT90SC25672RCT), which contains the following security features:

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

The physical enclosure of the chip is a metallic layer, which covers sensitive circuitry, provides advanced protection against physical attacks and fulfills the physical tampering and probing requirements.

6 OPERATIONAL ENVIRONMENT

The J-IDMark 64 cryptographic module may be defined as possessing a non-modifiable operational environment. It does not support the modification of the operational environment (firmware, OS, etc.). Additionally, no software or firmware can be downloaded or altered post-issuance. The Operational Environment requirements of **[FIPS 140-2]** Area 6, therefore, do not apply to the J-IDMark 64 cryptographic module.

7 CRYPTOGRAPHIC KEY MANAGEMENT

7.1 KEY OVERVIEW

Cryptographic keys	***Key size***	***Approved algorithms***
Perso CO key set	Encryption key: 112 bits	TDES
	Mac key: 112 bits	TDES MAC
Perso CO session key set	Encryption key: 112 bits	TDES
	Mac key: 112 bits	TDES MAC
Admin CO key set	Encryption key: 112 bits	TDES
	Mac Key: 112 bits	TDES MAC
Admin CO session key set	Encryption key: 112 bits	TDES
	Mac Key: 112 bits	TDES MAC
Card key set	Encryption key: 112 bits	TDES
	Mac key: 112 bits	TDES MAC
Card session key set	Encryption key: 112 bits	TDES
	Mac key: 112 bits	TDES MAC
EEPROM area protection key set	Encryption key: 112 bits	TDES
	Mac key: 112 bits	TDES MAC
CSP encryption key	112 bits	TDES
External keys	112 bits	TDES TDES MAC
RSA private keys	1024 to 2048 bits	PRNG RSA
RSA public keys	1024 to 2048 bits	PRNG

Tab 13: Cryptographic key overview

7.2 KEY GENERATION

Among cryptographic keys, only the RSA key pairs can be generated on board after issuance, using the FIPS approved PRNG function.

7.3 ENTRY/OUTPUT

All static cryptographic keys used in the field, except RSA key pairs, are input encrypted with a dedicated CSP encryption key during the personalization of the cryptographic module. If not generated on board, RSA keys can also be input during personalization along with the others cryptographic keys.

Cryptographic keys are never input or output in plaintext form from the cryptographic module.

7.4 STORAGE

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

- An API which does not allow those operations.
- A dedicated key set which encrypts the EEPROM area where cryptographic keys are stored.

7.5 ZEROIZATION

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

In addition, session keys 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 cryptographic module performs a set of self-tests to ensure that it is working properly. When a self-test fails, the cryptographic module enters an error state and remains mute until the card is reset.

9.1 POWER-UP SELF-TESTS

The J-IDMark 64 performs the following power-up self-tests:

- EEPROM software/firmware integrity check.
- TDES-MAC known answer test.
- TDES ciphering/deciphering known answer test.
- RSA signature & SHA-1 known answer test.
- SHA-256 known answer test
- ANSI X9.31 Pseudo random number generation test.

9.2 CONDITIONAL SELF-TESTS

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

- RSA key pair wise consistency check after each RSA key pair generation.
- Hardware random number generation continuous test.
- Pseudo random number generation continuous test.

9.3 SELF-TESTS ON DEMAND

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

10 MITIGATION OF OTHER ATTACKS

The J-IDMark 64 implements countermeasures to protect against the attacks listed in Tab 14:

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 14: Mitigation of other attacks

11 SECURITY RULES

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

11.1 SECURE OPERATION SECURITY RULES

- The J-IDMark 64 module does not allow itself to return to the personalization lifecycle state once personalization has been performed: personalization can therefore only be performed once.
- Perso CO an Admin CO should verify at power-up of the card the value of the byte in the ATR, which indicates that the card is **[FIPS 140-2]** level 3 compliant.
- If the J-IDMark 64 module is **[FIPS 140-2]** level 3 compliant, then all the instances of the ID v1 Applet are **[FIPS 140-2]** level 3 compliant.
- Each instance of the ID v1 supports two operating modes, which correspond to different command access control policies: normal and reinforced. If the instance works under the reinforced mode, then a mutual authentication between the cryptographic module and the host (card reader or terminal…) is required to perform services such as user authentication and signatures. The mode of operation of each instance is set during the personalization phase and cannot be changed afterwards. Both of these modes of operation are FIPS Approved.
- The operator shall check that the module is working properly by requesting the serial number data of the module. If the command answers, 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 module does not allow data output during self-tests, key generation, zeroization and error states.

11.2 AUTHENTICATION SECURITY RULES

- The User shall keep the knowledge of his PIN(s) secret. Perso-CO and Admin CO shall also not share or disclose their secret key set.
- No authentication record is 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 able to perform authentication-required services on the J-IDMark 64 module at a time.
- For each instance of the ID v1 Applet, only one user can be authenticated using the biometric mechanism, as all the biometric templates must correspond to the same physical person.

11.3 PIN MANAGEMENT SECURITY RULES

- Only the Admin CO is allowed to unblock a PIN once the card is in the field.
- The Global PIN can be used to authenticate a user and to restrain access to some files. There is only one Global PIN for the J-IDMark 64 module, so the Perso CO shall be aware, when allocating the use of this PIN, that this CSP is common to all the instances of the ID v1 applet.
- The module shall employ a count mechanism to limit the maximum number of multiple PIN authentication attempts to ten.

11.4 KEY MANAGEMENT SECURITY RULES

- The module shall contain a zeroization service for all cryptographic keys and CSPs.
- Cryptographic keys that have a retry counter shall not be unblockable.
- The J-IDMark 64 module shall rely on the CSP encryption key for the protection of all CSPs entering or leaving the cryptographic boundary.

11.5 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 and during initialization.

11.6 SELF-TESTS SECURITY RULES

- The J-IDMark 64 module shall perform startup 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 enter an error state.
- No data shall be output during self-tests.