J-IDMark 64 PIV

FIPS 140-2 Non-Proprietary Security Policy

Level 2 validation

Version 2

April 2008

Sagem Orga
SAFRAN Group

TABLE OF CONTENTS

GLOSSARY

AES	:	Advanced Encryption Standard
ALU	:	Arithmetic Logic Unit
APDU	:	Application Protocol Data Unit
API	:	Application Protocol Interface
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
PIV	:	Personal Identity Verification
PKCS	:	Public Key Cryptographic Standards
P-RNG	:	Pseudo Random Number Generation
RAM	:	Random Access Memory
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 201]	:	FIPS PUB 201 – Federal Information Processing Standards Publication – Personal Identity Verification (PIV) of Federal Employees and Contractors – February 25, 2005
[SP 800-73]	:	NIST Special Publication 800-73-1 - Interfaces for Personal Identity Verification – Information Security – February 2006
[FIPS 180-2]	:	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 PIV* cryptographic module. This security policy represents the completed *J-IDMark 64 PIV* product satisfying all of the requirements for **[FIPS 140-2]** level 2 (level 4 for physical security).

1.2 PRODUCT DESCRIPTION

The *J-IDMark 64 PIV* module is a dual interface smart card with a javacard operating system, compliant with Sun Java Card ™ 2.2.1 **[JCS]** and Global Platform 2.1.1 **[GP]** specifications, supporting the PIV v01 application, compliant with **[FIPS 201]** and **[SP 800-73]**.

The *J-IDMark 64 PIV* module is thus a reliable and standardized solution for PIV Cards, which allow the use of identity credentials to manage physical and logical access to Federal government locations and systems.

The *J-IDMark 64 PIV* hardware is based on the ATMEL AT90SC 128 72 RCFT chip. The *J-IDMark 64 PIV* 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-Kbyte E²PROM is available for loading and instantiating the PIV v01 application.

1.3 MODULE IDENTIFICATION

Four configurations of the *J-IDMark 64 PIV* are available, which are the combination of the following options:

- With or without the AES algorithm included in the list of the *J-IDMark 64 PIV* FIPS Approved algorithms.
- With or without cryptographic services available when using the contactless interface to communicate with the module.

Once the cryptographic module is issued, it is not possible to change the module configuration. All configurations of the module meet all the **[FIPS 140-2]** level 2 requirements.

The identification numbers of the *J-IDMark 64 PIV* reflect the configuration of the module and are given in Tab 1.

Configuration		***Identification number***			
		ROM	***Cfg Option***	***E²PROM firmware***	***Applet Id***
1	With FIPS Approved AES With contactless cryptographic services	01016221	3232	FFFFFFFF	A000000243001501010001060 1
2	Without FIPS Approved AES With contactless cryptographic services	01016221	0202	FFFFFFFF	A000000243001501010001060 1
3	With FIPS Approved AES Without contactless cryptographic services	01016221	3200	FFFFFFFF	A000000243001501010001060 1
4	Without FIPS Approved AES Without contactless cryptographic services	01016221	0200	FFFFFFFF	A000000243001501010001060 1

Tab 1: Module Identification

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 PIV* module can be retrieved at any time.

1.4 SECURITY LEVEL

The *J-IDMark 64 PIV* product is designed to meet the overall requirements applicable to the level 2 of the **[FIPS 140-2]** specifications. Moreover, the *J-IDMark 64 PIV* is compliant with the level 4 requirements for physical security (**[FIPS 140-2]**, Area 5) and with the level 3 requirements for roles, services and authentication (**[FIPS 140-2]**, Area 3), EMI/EMC (**[FIPS 140-2]**, Area 8) and design assurance (**[FIPS 140-2]**, Area 10). The area-specific security levels are described in Tab 2.

Security Requirements Section	***Level***
Cryptographic Module Specification	**2**
Cryptographic Module Ports and Interfaces	**2**
Roles, Services and Authentication	**3**
Finite State Model	**2**
Physical Security	**4**
Operational Environment	**N/A**
Cryptographic Key Management	**2**
EMI/EMC	**3**
Self-Tests	**2**
Design Assurance	**3**
Mitigation of other Attacks	**2**

Tab 2: *J-IDMark 64 PIV* area specific levels

1.5 FIPS APPROVED ALGORITHMS

The algorithms used in the FIPS Approved mode of operation of the *J-IDMark 64 PIV* module are listed in Tab 3.

Algorithms	***Standard***	***Description***
SHA-1	**[FIPS 180-2]**	Hash (for signature)
RSA	**[PKCS#1 v2.1]**	RSA signature
		RSA key generation
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 3: *J-IDMark 64 PIV* algorithms

* Depending on the card configuration, the AES algorithm may or may not be included in the list of the FIPS Approved algorithms.

The *J-IDMark 64 PIV* 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 PIV* cryptographic module only supports a FIPS Approved mode of operation and remains in this Approved mode of operation as long as the security operating rules of the module, described in §11, are respected.

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 PIV* software is composed of an operating system complying with the **[JCS]** and **[GP]** standards and the PIV v01 application loaded in E²PROM, compliant with **[FIPS 201]** and **[SP 800-73]**.

The *J-IDMark 64 PIV* cryptographic module is designed to be encased in a hard opaque resin that can be embedded into a plastic card. An antenna shall also be connected to the *J-IDMark 64 PIV* module for the purpose of contactless communications. 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 PIV* cryptographic module is composed of the ATMEL AT90SC 128 72 RCFT single chip microprocessor, which includes:

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

The *J-IDMark 64 PIV* cryptographic module operates under contact or contactless communication mode (but not under both modes at the same time). The *J-IDMark 64 PIV* 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 PIV* cryptographic module.

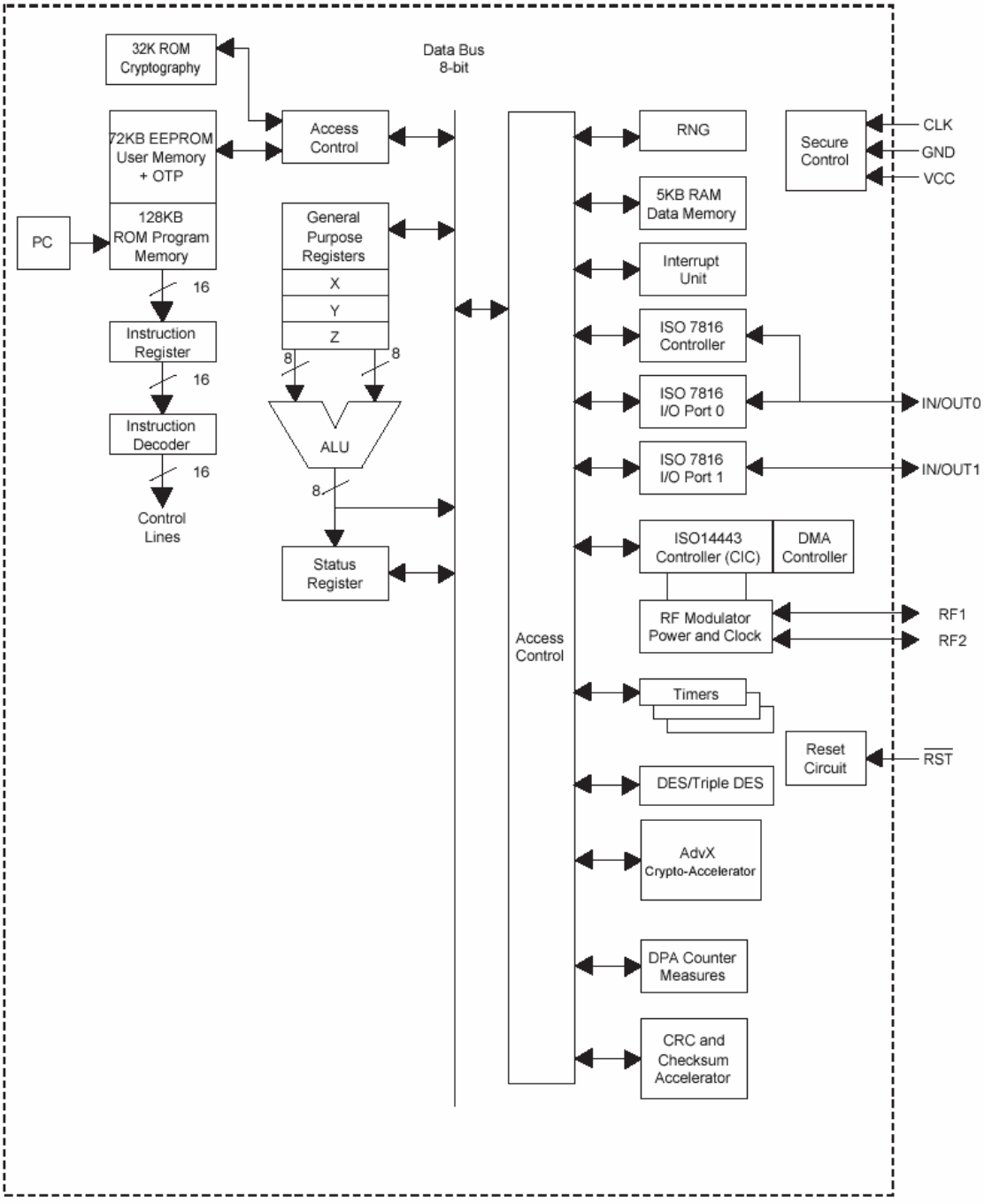

Figure 1: *J-IDMark 64 PIV* block diagram*

* ATMEL information

3 CRYPTOGRAPHIC MODULE PORTS AND INTERFACES

3.1 PHYSICAL PORTS

The physical ports of the *J-IDMark 64 PIV* 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 PIV* module consist of the bond pad locations of the chip and conform to the **[ISO 7816-2]** specifications. Tab 4 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 4: 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 PIV* are shown in Figure 2 and Tab 5:

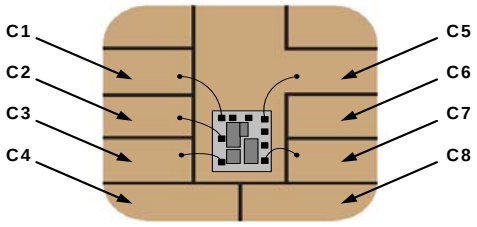

Figure 2: Contact plate description

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	

Tab 5: 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 PIV* cryptographic module consist of two electrical connections and conform to the **[ISO 14443-2]** specifications. Tab 6 lists the physical ports of the module for the contactless interface.

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

Tab 6: 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.

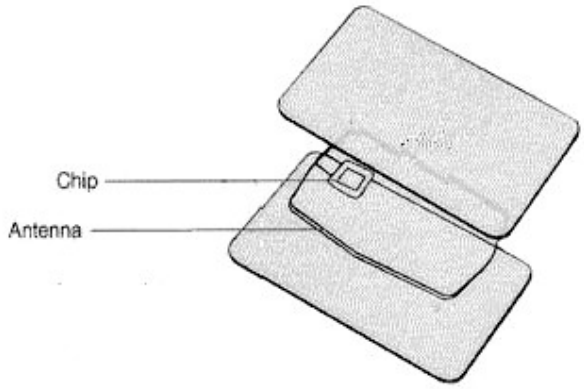

Figure 3: Chip with antenna

3.2 LOGICAL PORTS

3.2.1 Contact mode logical interface

The *J-IDMark 64 PIV* 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 7.

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 7: **Physical to logical interface mapping**

3.2.2 Contactless mode logical interface

The *J-IDMark 64 PIV* 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 8 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 8: Functional specification of the contactless interface

4 ACCESS CONTROL POLICY

4.1 ROLES

Tab 9 presents the roles supported by the *J-IDMark 64 PIV* module.

Roles	***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. The CO also performs personalization operations of the PIV v01 application.
SSD User	A SSD User has access to a given SSD. He is in charge of the management of this SSD.
PIV Admin	The PIV Admin can perform management operations on the PIV v01 application.
Cardholder	The cardholder is the owner of the card.

Tab 9: Role description

4.2 AUTHENTICATION

Tab 10 presents the authentication mechanisms associated to the corresponding roles.

Roles	***Type of Authentication***	***Authentication data***
CO	Mutual authentication	ISD CO key set
SSD User	Mutual authentication	SSD User key set
PIV Admin	External or Mutual authentication	Administration key ‘9B’
	Eventually: password verification	PIV Application PUK ‘81’[*]
Cardholder	Password verification	PIV Application PIN ‘80’ Eventually: PIV Application PUK ‘81’[*]

Tab 10: Roles and required authentication

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

- The CO is uniquely identified by the identification number of the ISD and the identification number of his ISD CO key set.
- A SSD User is uniquely identified by the identification number of the selected SSD and the identification number of his SSD User key set.
- The PIV Admin is uniquely identified by the identification number of the PIV v01 application and by the identification number of his Administration key ‘9B’ (or by the identification number of the PIV Application PUK ‘81’ if the PIV Admin is the owner).
- The Cardholder is uniquely identified by the identification number of the PIV v01 application and by the identification number of his PIV Application PIN ‘80’ (or by the identification number of the PIV Application PUK ‘81’ if the Cardholder is the owner).

[*] The owner of the PIV Application PUK may be wether the PIV Admin or the Cardholder, but not in any case both together.

The ability to change from one role to another is strictly enforced by the *J-IDMark 64 PIV* 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 PIV* module at the same time.

4.3 AUTHENTICATION STRENGTH

All the authentication mechanisms fulfill **[FIPS 140-2]** strength requirements. Tab 11 presents the strength of the authentication mechanisms.

Authentication mechanism	***Probability that a random authentication attempt succeeds***	***Probability that multiple random authentication attempts within a one minute period succeed***
External authentication	Less than $1/10^6$	Less than $1/10^5$
Mutual authentication	Less than $1/10^6$	Less than $1/10^5$
Password verification	Less than $1/10^6$	Less than $1/10^5$

Tab 11: Strength of the FIPS Approved role authentication mechanisms

4.4 SERVICES

4.4.1 Services description

Tab 12 and Tab 13 describe the services of the *J-IDMark 64 PIV* module and the security functions used at the invocation of each service.

Platform services	***Description***	***Security functions***
SELECT	Selection of the ISD, a SSD or an applet instance	
GET_DATA	Retrieving general information from the ISD or from a SSD	
INIT	Opening a secured channel and authentication of the CO or the SSD User.	P-RNG, TDES, TDES MAC
GET_STATUS	Retrieving the life cycle data of Executable Load File, Executable Module, ISD, SSDs or application, according to a given match/search criteria	
SET_STATUS	Modification of the life cycle state of the card (ISD state) and locking or unlocking SSDs and applets	
INST_INST	Creation of an applet or SSD instance from an executable load file, with its AID and its capability to be selected by default	
INST_EXTR	Association of an ISD applet instance to a given SSD	
LOAD	Load of a “load file” (dedicated to be applets)	
STORE_DATA	Storage of a set of information in ISD or in an SSD instance	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
DELETE	Deletion of an applet instance or code or Executable Load file	

Platform services	*Description*	*Security functions*
SELF_TESTS	Execution of power-up self-tests	P-RNG, TDES, AES*, SHA-1, RSA
TERMINATE	Zeroization of the whole E²PROM	

Tab 12: *J-IDMark 64 PIV* platform services overview

PIV Application services	*Description*	*Security functions*
PIV_GET_DATA	This service allows retrieving the data content of a single data object (containers values to retrieve the X.509 certificate of a key, or fingerprint templates etc…)	
PIV_GEN_AUTH	For External and Mutual authentication schemes, this service allows to the PIV Admin to get authenticated to the card thanks to the'9B' key and to access to PIV personalization services. For Internal authentication scheme, this service allows authenticating the card to the back end system if using a freely available key or to sign data if using a key protected with a PIN (for instance key '9A').	TDES/RSA
PIV_VERIFY	This command allows the card to authenticate the Cardholder by verifying he has the knowledge of the PIV Application PIN. Once authenticated, the cardholder has the possibility to upload the content of some containers or to sign data.	
PIV_CHANGE_REFERENCE_DATA	This service allows the Cardholder to get authenticated to the card and to change the value of his PIN. This service also allows the PUK owner to modify the value of the PUK.	
PIV_RESET_RETRY_COUNTER	This service allows to present a PUK value in order to unblock the PIN, to reset the PIN reset retry counter and eventually to modify its value.	
INIT	This service allows opening a secured channel (SCP) with the selected PIV instance (with the CO ISD key set), in order to authenticate the CO. Once authenticated, the CO can access to PIV personalization services.	P-RNG, TDES, TDES MAC
PIV_PUT_DATA_PERSO	This service allows the CO to create containers, to create key objects, to initialize key values, to create PIV Application PIN and to initialize it.	
PIV_PUT_DATA_ADMIN	This service allows the CO or the PIV Admin to inject the content of a container to the card.	
PIV_GEN_ASYM_KEY	This command allows the CO or the PIV Admin to generate and store in the card an asymmetric RSA key pair, i.e. a public key and a private key, and to output from the card the value of the public key.	P-RNG, RSA

Tab 13: *J-IDMark 64 PIV* PIV Application services overview

* Depending on the card configuration, the AES self-test may or may not be performed at power-up.

4.4.2 Services Access Control

The crypto module uses identity-based control to access the services of the *J-IDMark 64 PIV* module. Tab 14 and Tab 15 present 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.

Platform services	***CO***	***SSD User***	***PIV Admin***	***Cardholder***	***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			
DELETE	X				
SELF_TESTS	X	X	X	X	X
TERMINATE	X				

Tab 14: *J-IDMark 64 PIV* platform service access control

PIV Application services	***CO***	***SSD User***	***PIV Admin***	***Cardholder***	***No role***
SELECT	X		X	X	X
PIV_GET_DATA	X		X	X	X
PIV_GEN_AUTH			X	X	X
INIT			X	X	X
PIV_PUT_DATA_PERSO	X				
PIV_PUT_DATA_ADMIN	X		X		
PIV_GEN_ASYM_KEY	X		X		
PIV_VERIFY			X	X	X
PIV_CHANGE_REF_DATA			X	X	X
PIV_RESET_COUNTER			X	X	X

Tab 15: *J-IDMark 64 PIV* PIV Application service access control

4.5 CSPS DESCRIPTION

Tab 16 and Tab 17 present the cryptographic keys and other CSPs of the *J-IDMark 64 PIV* module.

Platform 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 to derive a SSD User Session key set as part of a SSD User authentication. There is one SSD 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 SSD User.
E²PROM Protection key	A double TDES key used to cipher the E²PROM 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 16: *J-IDMark 64 PIV* platform cryptographic keys and CSPs overview

PIV Application CSPs	*Description*
PIV Application PIN ‘80’	Password of alphanumeric characters used to prove the identity of the cardholder to the card. The PIV Application PIN has a reset retry counter and thus get blocked after a certain number of failed authentication attempts. The PIV Application PIN can be unblocked by presenting the PIV Application PUK to the card.
PIV Application PUK ‘81’	Password of alphanumeric password used to unblock and update the PIV Application PIN. The PIV Application PUK has a reset retry counter and thus get blocked after a certain number of failed authentication attempts. It is not possible to unblock the PIV Application PUK once it is blocked. The owner of the PIV Application PUK may be the PIV Admin or the Cardholder, but not both together.
PIV Authentication Key ‘9A’	Asymmetric private key, used for card authentication to prove the identity of the cardholder to an external entity using the PIV Application Personal Identification Number (PIN). Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation). Defined in [FIPS 201] Section 4.3 and [SP 800-73] Section 1.8.2 (pg 5).
Administration Key ‘9B’	Symmetric key, used for personalization and post-issuance activities. Defined in [FIPS 201] Section 4.3 (called *card management key* in [FIPS 201]).
Digital Signature Key ‘9C’	Asymmetric private key, that supports with its certificate the use of digital signatures for the purpose of document signing. The Public Key Infrastructure (PKI) cryptographic function is protected with a “PIN Always” access rule (this requires explicit cardholder participation every time the key is used for digital signature generation). Defined in [FIPS 201] Section 4.3 and [SP 800-73] Section 1.9.3 (pg 7).
Key Management Key ‘9D’	Asymmetric private key, that supports with its certificate the use of encryption for the purpose of confidentiality. This key is protected with a “PIN” access rule. This requires cardholder activation, but enables multiple compute operations without additional cardholder consent (e.g., the PIN need not be supplied for each operation). Defined in [FIPS 201] Section 4.3 and [SP 800-73] Section 1.9.4 (pg 7).
Card Authentication Key ‘9E’	Symmetric secret key or asymmetric private key, that supports, with its certificate if the key is an asymmetric key, PIV Card Authentication for device to device authentication purposes or for physical access. Cardholder consent is not required to use this key (e.g., the PIN need not be supplied). Defined in [FIPS 201] Section 4.3 and [SP 800-73] Section 1.9.5 (pg 7).
Additional keys ‘8A’, ‘8B’, ‘8C’, ‘8D’, ‘8E’ and ‘8F’	Symmetric secret keys or asymmetric private keys. Those keys provide additional authentication services with non PIV application or signature services if access to those keys is protected by PIV Application PIN verification.

Tab 17: ***J-IDMark 64 PIV*** **PIV Application cryptographic keys and CSPs overview**

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

4.6 CSPS ACCESS CONTROL

Tab 18 and Tab 19 present service access rights to cryptographic keys and CSPs stored in the *J-IDMark 64 PIV* module.

Platform CSPs	***Platform 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	SSD User
	PUT_DES_KEY	Modification	SSD User
	STORE_DATA	Modification	SSD User
	TERMINATE	Zeroization	CO
SSD Key Encryption key(s) (SSD_K_{KEK})	PUT_DES_KEY	Modification	SSD User
	STORE_DATA	Modification/Ciphering	SSD User
	TERMINATE	Zeroization	CO
SSD User Session key set (SSD_SK_{ENC}, SSD_SK_{MAC})	INIT	Derivation/Execution	SSD User
E²PROM Protection key set	PUT_DES_KEY	Execution	CO/SSD User
	PUT_RSA_KEY	Execution	SSD User
	TERMINATE	Zeroization	CO

Tab 18: *J-IDMark 64 PIV* platform CSPs access rights within services

PIV Application CSPs	*Services*	*Operations*	*Role*
PIV Application PIN ‘80’	PIV_CHANGE_REF_DATA	Verification/Modification	Cardholder
	PIV_PUT_DATA_PERSO	Loading	CO
	PIV_RESET_COUNTER	Unblocking/Modification	PUK owner
	PIV_VERIFY	Verification	Cardholder
	TERMINATE	Zeroization	CO
PIV Application PUK ‘81’	PIV_CHANGE_REF_DATA	Verification/Modification	PUK owner
	PIV_PUT_DATA_PERSO	Loading	CO
	PIV_RESET_COUNTER	Verification	PUK owner
	TERMINATE	Zeroization	CO
PIV Authentication Key ‘9A’	PIV_GEN_AUTH	Authentication (Internal)	Cardholder
	PIV_PUT_DATA_PERSO	Loading/Modification	CO
	PIV_GEN_ASYM_KEY	Generation	CO/PIV Admin
	TERMINATE	Zeroization	CO
Administration Key ‘9B’	PIV_GEN_AUTH	Authentication (External/Mutual)	PIV Admin
	PIV_PUT_DATA_PERSO	Loading/Modification	CO
	TERMINATE	Zeroization	CO
Digital Signature Key ‘9C’	PIV_GEN_AUTH	Signature (Internal authentication)	Cardholder
	PIV_PUT_DATA_PERSO	Loading/Modification	CO
	PIV_GEN_ASYM_KEY	Generation	CO/PIV Admin
	TERMINATE	Zeroization	CO
Key Management Key ‘9D’	PIV_GEN_AUTH	Authentication (Internal)	Cardholder
	PIV_PUT_DATA_PERSO	Loading/Modification	CO
	PIV_GEN_ASYM_KEY	Generation	CO/PIV Admin
	TERMINATE	Zeroization	CO
Card Authentication Key ‘9E’	PIV_GEN_AUTH	Authentication (Internal)	No role
	PIV_PUT_DATA_PERSO	Loading/Modification	CO
	PIV_GEN_ASYM_KEY	Generation	CO/PIV Admin
	TERMINATE	Zeroization	CO
Additional keys ‘8A’, ‘8B’, ‘8C’, ‘8D’, ‘8E’ and ‘8F’	PIV_GEN_AUTH	Authentication (Internal)	Cardholder/No role
	PIV_GEN_AUTH	Signature (Internal authentication)	Cardholder
	PIV_PUT_DATA_PERSO	Loading/Modification	CO
	PIV_GEN_ASYM_KEY	Generation	CO/PIV Admin
	TERMINATE	Zeroization	CO

Tab 19: *J-IDMark 64 PIV* PIV Application CSPs access rights within services

5 PHYSICAL SECURITY

5.1 [FIPS 140-2] LEVEL 4 REQUIREMENTS

The *J-IDMark 64 PIV* 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 PIV* 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 PIV* module. This module performs the software/firmware load test on all new code, and as such the *J-IDMark 64 PIV* 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 PIV* cryptographic module.

It is noted that the loading of validated Applets on the *J-IDMark 64 PIV* will result in a different FIPS module referenced by a separate FIPS 140 certificate.

7 CRYPTOGRAPHIC KEY MANAGEMENT

7.1 KEY OVERVIEW

Tab 20 gives an overview of all the cryptographic keys used in the *J-IDMark 64 PIV* module.

Platform 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
P-RNG Seed key	Seed key: 112	P-RNG
PIV Application Cryptographic keys	***Key size (bits)***	***Approved algorithms***
PIV Authentication Key ‘9A’	From 1024 to 2048	RSA
Administration Key ‘9B’	TDES key: 128 or 192	TDES
	AES key: 128	AES
Digital Signature Key ‘9C’	From 1024 to 2048	RSA
Key Management Key ‘9D’	From 1024 to 2048	RSA
Card Authentication Key ‘9E’	RSA CRT key: From 1024 to 2048	RSA
	TDES key: 128 or 192	TDES
	AES key: 128	AES
Additional keys ‘8A’, ‘8B’, ‘8C’, ‘8D’, ‘8E’ and ‘8F’	RSA CRT key: From 1024 to 2048	RSA
	TDES key: 128 or 192	TDES
	AES key: 128	AES

Tab 20: Cryptographic key overview

7.2 KEY GENERATION

A FIPS Approved RSA CRT key pair generation function is available on the *J-IDMark 64 PIV* (up to a 2048-bit modulus RSA). 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.

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.
- Optionally, 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 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 PIV* 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 PIV* 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 signature & SHA-1 known answer test.

9.2 CONDITIONAL SELF-TESTS

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

- RSA key pair wise consistency check after each RSA key pair generation.
- Hardware random number generation continuous test.
- **[ANSI X9.31]** Pseudo random number generation continuous test.
- TDES MAC verification after applet loading.
- 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 of those self-test fails, the cryptographic module outputs a specific status, enters an error state and remains mute until the card is reset.

Moreover, if the self-test failing is the E²PROM software/firmware integrity check, then the *J-IDMark 64 PIV* module will output a status specific to this failure, enter a terminate state and not boot any more after repowering.

[*] Depending on the card configuration, the AES self-test may or may not be performed at power-up.

10 MITIGATION OF OTHER ATTACKS

The *J-IDMark 64 PIV* module implements countermeasures to protect against the attacks listed in Tab 21:

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 21: 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 PIV* 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 PIV* cryptographic module.

11.1 SECURE OPERATION SECURITY RULES

- Operators of the *J-IDMark 64 PIV* shall have the capability at any time to retrieve the identification number of the module.
- The identification number of the *J-IDMark 64 PIV* module shall indicate its configuration.
- Operators of the *J-IDMark 64 PIV* shall check the configuration of the module before using it. Especially, the CO shall retrieve the identification number of the module and verify its configuration before personalizing the PIV v01 application.
- All the applets loaded on the *J-IDMark 64 PIV* module shall be **[FIPS 140-2]** compliant; otherwise the module shall lose its validation.
- The *J-IDMark 64 PIV* shall execute a TDES MAC verification of the code of the applets loaded on the module.
- Operators of the *J-IDMark 64 PIV* 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 PIV* module shall not allow data output during self-tests, zeroization and error states.

11.2 AUTHENTICATION SECURITY RULES

- CO, SSD User, PIV Admin shall not share or disclose secret authentication data to unauthorized operators.
- The cardholder shall keep the knowledge of his PIV Application PIN secret.
- The owner of the PIV Application PUK shall keep the knowledge of his PIV Application PUK secret.
- PIV Application PIN and PUK shall have a reset retry counter and shall get blocked after a specified number of failed authentication attempts is reached.
- 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.

11.3 CSPS MANAGEMENT SECURITY RULES

- The module shall contain a zeroization service for all CSPs stored in E²PROM.
- The *J-IDMark 64 PIV* module shall rely on CSP encryption keys for the protection of all CSPs entering or leaving the cryptographic boundary.
- The CO shall only load AES cryptographic keys if the AES algorithm is self-tested at power-up, otherwise the *J-IDMark 64 PIV* is no longer working in a FIPS Approved mode of operation.
- The PIV Application PUK shall not be unblockable.
- Only the owner of the PIV Application PUK shall have the capability to unblock the PIV Application PIN.

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 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 PIV* module.

11.5 SELF-TESTS SECURITY RULES

- The *J-IDMark 64 PIV* 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.
- The CO and the PIV Admin shall have the capability to check which self-tests are performed at power-up by retrieving the identification number of the module.
- 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 PIV* 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.