IDeal Citiz v2.0 Open

FIPS 140-2 Security Policy

Non-Proprietary

July 2015, 16th

TABLE OF CONTENTS

GLOSSARY

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^{2}PROM	:	Electrically Erasable and Programmable Read Only Memory
EFP	:	Environmental Failure Protection
EMI	:	Electromagnetic Interference
EMC	:	Electromagnetic Compatibility
FiDi	:	Clock Frequency Rate / Data Bit Rate ratio as per ISO7816-3
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
DRBG	:	Deterministic Random Bit Generator
ROM	:	Read Only Memory
RSA	:	Rivest Shamir Adleman
SEMA	:	Simple Electromagnetic Analysis
SHA	:	Secure Hash Algorithm
SPA	:	Simple Power Analysis
SSD	:	Supplementary Security Domain

1 REFERENCE DOCUMENTS

[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

[ANSI X9.52] : American Bankers Association, Triple Data Encryption Algorithm Modes of Operation, ANSI X9.52 – 1998

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

[FIPS 46-3] Data Encryption Standard (DES) and Modes of Operation

[FIPS 180-4] : National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4 with Change Notice 1, February 25, 2004

[FIPS 186-4] Digital Signature Standard (DSS), july 19, 2013

[FIPS 197] Advanced Encryption Standards (AES), November 2001

[GP] : GlobalPlatform Card Specification - Version 2.1.1 – March 2003

[GP_AMD_D] : GlobalPlatform Card Technology Secure Channel Protocol 03 Card Specification v2.2 – Amendment D – Version 1.1, sept 2009, *ref GPC_SPE_014*

[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 9797] : Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm

[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 ™ 3.0.2 Classic Edition Card Specification, Sun Microsystems

[NIST SP800-38B] : Recommendation for Block Cipher Modes of Operation: the MAC mode for authentication, may 2005

[NIST SP800-90A] : Recommendation for Random Number Generation Using Deterministic Random Bit Generators: ref: NIST-SP800-90A, jan 2012

[NIST SP800-56A] : Recommendation for Pair-Wise Key Establishment Schemes Using discret Algorithm cryptography, march 2007

[NIST SP800-108] Recommendation for Key Derivation Using Pseudorandom Functions, Oct 2009

[PKCS#1 v2.1] : RSA Laboratories, PKCS#1 v2.1: RSA Cryptography Standard, June 14, 2002

EMVco EMV Integrated Circuit Card Specification for Payment Systems Book1, 2, 3 and 4 V4.2 June 2008

2 INTRODUCTION

2.1 SCOPE

This document presents the security policy of the *IDeal Citiz v2.0 Open* cryptographic module for overall FIPS 140-2 level 3 validation.

The “Infraestructura Chaves Públicas Brasiliera - ICP-Brasil, Public Key Infrastructure” is based on FIPS 140-2, this document also aswers to the validation of the PKI of the Instituto Nacianoal de Tecnologia da Informação (ITI) of Brazil without any additional information.

2.2 PRODUCT DESCRIPTION

The *IDeal Citiz v2.0 Open* cryptographic module is a contact/contactless JavaCard multi-applications product in a single Integrated Circuit Chip specifically designed for the security of data.

Customers, as government and enterprise, may download applications in card for identification, health or banking markets.

Java technology is the leading multiple applications operating system for smart cards. It offers developers a convenient platform on which to develop and implement smart card applets. The *IDeal Citiz v2.0 Open* module has been designed to offer a modular and open solution based on reliable and standardized technologies. To that end, the *IDeal Citiz v2.0 Open* module contains an implementation of the Sun Java Card ™ 3.0.2 Classic Edition **[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 *IDeal Citiz v2.0 Open* module is also compliant with the GlobalPlatform Card Specification - Version 2.1.1 **[GP]** with SCP03 as defined in the Amendment D **[GP_AMD_D]**, where it secures the application management and manages the card life cycle.

2.3 SECURITY LEVELS

The *IDeal Citiz v2.0 Open* module respects the following Security Levels of the Security Requirements:

Security Requirements	Security Levels
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	3
Operation Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-tests	3
Design Assurance	3
Mitigation of the Other Attacks	3

Tab 1: Security Level of Security Requirements

2.4 PRODUCT IDENTIFICATION

The *IDeal Citiz v2.0 Open* cryptographic module can be identified by using the GET DATA command and retrieving the CPLC (the ID is ‘9F 7F’) information.

This table indicates Firmware Version 2.0.

Offset	L	Meaning	Format	type	Value	Description
0	2	IC Fabricator	BCD	Static	‘81 00’	INFINEON IC
2	2	IC Type	BCD	Static	-	see Tab 3
4	2	Operating System Identifier	BCD	Static	‘49 21’	Operating System Identifier: Morpho ID
6	2	Operating System Release Date	‘YDDD’	Static	’41 39’	-
8	2	Operating System Release Level XXh Major / YYh Minor	BCD	Static	-	Firmware Version ‘10 00’ represents Firmware Version 2.0
10	2	IC Fabrication Date	‘YDDD’	Dynamic	-	Filled in at IC manufacturing
12	4	IC Serial Number	-	Dynamic	-	Filled in at IC manufacturing
16	2	IC Batch Number	-	Dynamic	-	Filled in at IC manufacturing
18	2	IC Module Fabricator ID	BCD	Static	-	Filled in at module manufacturing
20	2	IC Module Packaging Date	‘YDDD’	Dynamic	-	Filled in at module manufacturing
22	2	IC Card Body Manufacturer	BCD	Static	-	Filled in at embedding
24	2	IC Module Embedding Date	‘YDDD’	Dynamic	-	Filled in at embedding
26	2	Pre-personalization Agent ID	BCD	Static	-	Filled in at pre-personalization
28	2	Pre-personalization Date	‘YDDD’	Dynamic	-	Filled in at pre-personalization
30	4	Pre-personalization Equipment ID	-	Static	-	Filled in at pre-personalization
34	2	IC Personalizer ID	-	Static	-	Filled in at personalization
34	2	IC Personalization Date	‘YDDD’	Dynamic	-	Filled in at personalization
38	4	IC Personalization equipment ID	-	Static	-	Filled in at at personalization

Tab 2: Product Identification

The *IDeal Citiz v2.0 Open* cryptographic module is composed of the INFINEON M7892 single chip microprocessor, which is configured as per the following table:

M7892 Chip Configuration	IC Type	Contact	Contactless	Flash Memory Size	MiFare option
SLE 78 CFX 3000 P	’78 14’	Yes	No	300 KB	No
SLE 78 CLFX 3000 P	’78 02’	Yes	Yes	300 KB	No
SLE 78 CLFX 3000 PM	’78 06’	Yes	Yes	300 KB	Yes
SLE 78 CFX 4000 P	’78 13’	Yes	No	400 KB	No
SLE 78 CLFX 4000 P	’78 01’	Yes	Yes	400 KB	No
SLE 78 CLFX 4000 PM	’78 05’	Yes	Yes	400 KB	Yes

Tab 3: Cryptographic Module Configurations

2.5 OPERATION MODES

The *IDeal Citiz v2.0 Open* cryptographic module supports basically one operation mode which is FIPS compliant.

The approved mode of operation is entered at power-up, and it can be checked in any roles by selecting the ISD and sending the GET DATA command with the CPLC identifier “9F 7F” as defined in section **[2.4]**.

The *IDeal Citiz v2.0 Open* cryptographic module optionaly supports MiFare, which is a non-FIPS operation mode.

This operation mode is negotiated at power-up at the lowest comunication level with card-reader supporting MiFare only. It is composed of reserved memory area for its data and a Library running on its own.

No data is shared between MiFare and the other part of the software.

MiFare:

- Is fundamentally a memory storage device, where the memory is divided into segments and blocks with simple security mechanisms for access control.
- Employes a proprietary protocol compliant to parts (but not all) of ISO/IEC 14443-3 Type A (contactless), with an NXP proprietary security protocol for authentication and ciphering.
- Is a library optionaly embedded in the contactless version of the *IDeal Citiz v2.0 Open* cryptographic module. The chip reference ends by PM.

3 CRYPTOGRAPHIC MODULE SPECIFICATION

3.1 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 INFINEON dual interface chip with reference M7892.

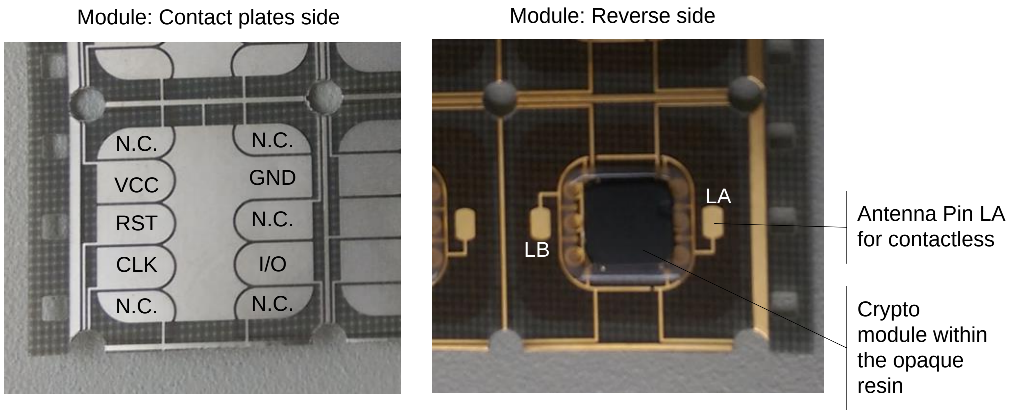
The *IDeal Citiz v2.0 Open* cryptographic module is designed to be encased in a hard opaque resin on contact or contactless module that can be embedded into a plastic card or any other support structure.

The *IDeal Citiz v2.0 Open* firmware is composed of an operating system complying with the **[JCS]** and **[GP]** standards. The firmware and the hardware are specifically designed for handling sensitive data; i.e. input and output within secured channel and processing under protections.

There are no component exclusions from the hardware and software boundary.

3.2 HARDWARE BOUNDARY

The cryptographic module boundary is realized as the external surface of the INFINEON M7892 single chip microprocessor and does not include the resin, the micro-bonds, the smart card contact plate in contact, the antenna for contactless, the fixation glue. The boundary contains all of the relevant module components (processors performing cryptography, etc.) consistent with **[FIPS 140-2]**.


Module: Contact plates side

Module: Reverse side

N.C.
VCC
RST
CLK
N.C.
N.C.
GND
N.C.
I/O
N.C.
LA
LB
Antenna Pin LA for contactless
Crypto module within the opaque resin

Figure 1: Contact/Contactless Module in reel

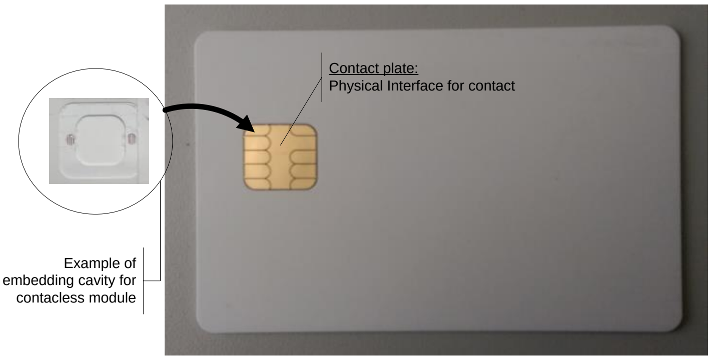

Contact plate:
Physical Interface for contact
Example of embedding cavity for contaceless module

Figure 2: Example of plastic card embedment

Module dimension is defined as per ISO7816-2:2007

Interface	Description
VCC	Contact: Power and Pad Supply Vcc
RST	Contact: Reset
CLK	Contact: Clock
GND	Contact: Common ground reference
IO	Contact: In/Out Data interface
L_A	Contactless: Coil Connection L_A
L_B	Contactless: Coil Connection L_B

Tab 4: Contact/contactless physical ports

The *IDeal Citiz v2.0 Open* cryptographic module operates under contact mode or contactless mode.

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:

- Contact, the voltage bond pads VCC/GND. The defined voltage ranges for normal conditions of use are the one specified by [ISO 7816-3] class A (2.7V to 3.3V) and class B (4.5V to 5.5V).
- Contactless, the voltage bond pad L_A/L_B. The defined voltage range for normal conditions of use is 2.70V to 3.30V, with a carrier frequency in the range of 13.40 to 13.70 MHz.

3.3 SOFTWARE BOUNDARY

The cryptographic module is composed of the hardware; i.e. the INFINEON M7892 chip, and the software which includes:

- The **Issuer Security Domain, ISD,** as defined in **[GP]** standard, is the application responsible for the security of the card. It enforces the third party application installations through the GP 2.1.1. Card Content Manager, e.g. loading and instantiation. In addition the ISD can instantiate SSD’s.
- **Supplementary Security Domain’s, SSD,** may be instantiated in card with the authorization of the ISD. SSD’s are responsible of the installation of their applications.
  The Cryptographic Module provides the application developers the capability of administrate directly their applications, once the ISD authorization is provided.
- An **Operating System** providing the loaded applications with the chip resources and services defined by:
  - GlobalPlatform Card Specification 2.1.1
  - SUN Java Card ™ 3.0.2 Classic Edition

Applets are not included in the scope of software in this validation. The loading of an applet(s) will negate the existing validation. Validation of a module containing an applet(s) requires a new 3SUB or 5SUB validation report and resubmission to the CMVP.

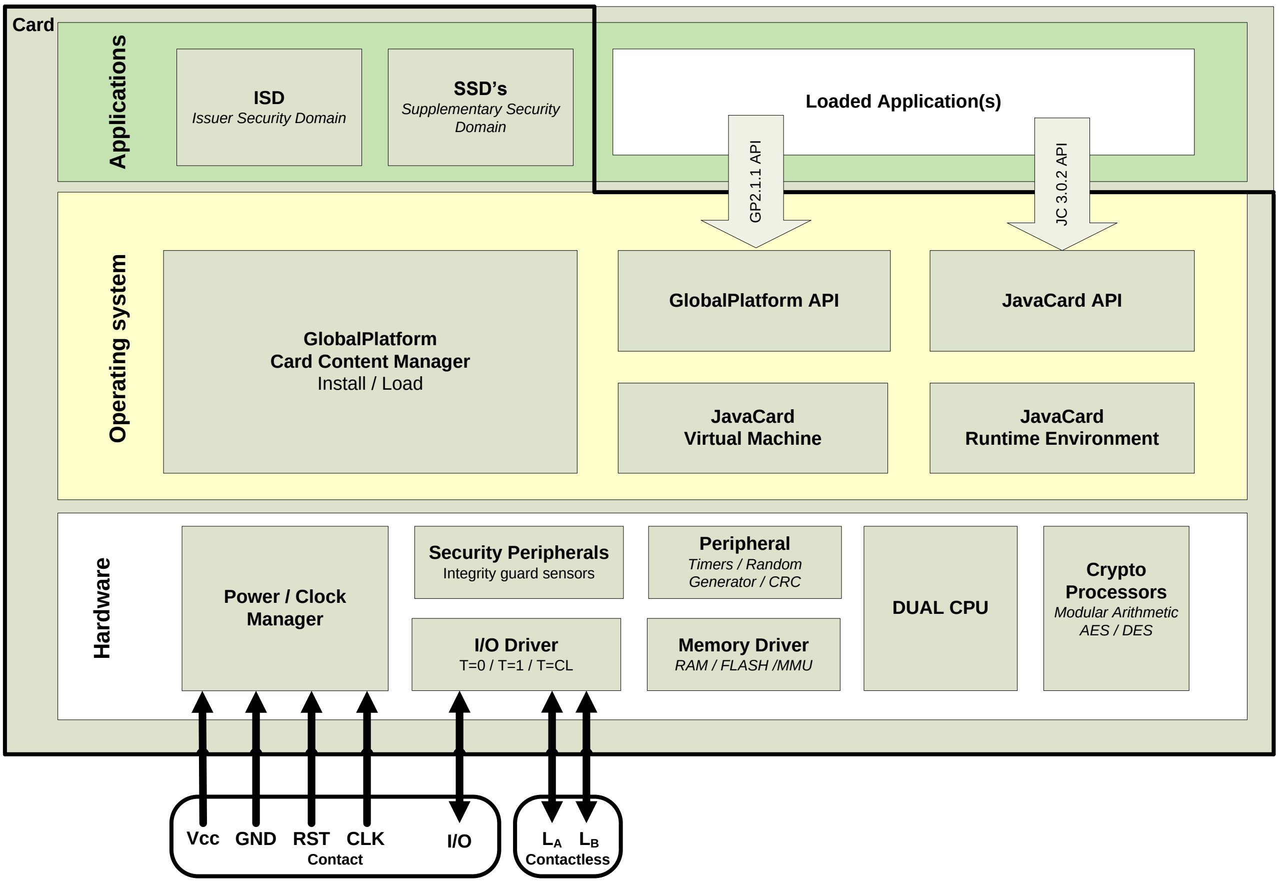


Figure 3: Cryptographic Module Block Diagram

The Cryptographic Module addresses contact, contactless and contact/contactless markets. And so the software can be tuned for each of these markets; for instance the contactless software layer can be removed of the cryptographic module if not used.

Software and hardware is stored within the on-chip memory of the processor, which is included within the module boundary

Note that the protocol of communication of Cryptographic Module is configured once and definitely at factory for Identity (ISO 7816) or Banking (EMVco) markets.

All the communications with the Crypto-Officer and users go through the contact interface of the contactless interface.

The MiFare option is out of the software boundary.

3.4 FIPS APPROVED ALGORITHMS

The following algorithms are used by the platform and meet all FIPS 140-2 requirements.

Algorithms	Standard	Description	CAVP Cert #
Symmetric Algorithms			
Triple-DES	**[ANSI X9.52]** **[FIPS 46-3]** **[NIST SP800-67]**	*Triple-DES [2Keys, 3Keys]* . Data encryption / decryption in ECB mode . Data encryption / decryption in CBC mode	1689
AES	**[FIPS 197]**	*AES [128, 192, 256]* . Data encryption / decryption in CBC mode	2818
Asymmetric Algorithms			
RSA	**[FIPS** 186-4] **[PKCS#1 v2.1]**	*RSA StraightForward* . Signature verification *[1024 to 3072 bit keys]*	1472
HASH			
SHA	**[FIPS 180-4]**	SHA-1	2362
MAC			
CMAC	**[NIST SP800-38B]**	CMAC AES128-192-256	2818
Key Derivation Functions			
KBKDF	**[NIST SP800-108]**	For SCP03, secure messaging defined by **[GP_AMD_D]** KDF in counter mode, AES128-192-256	62

Tab 5: *IDeal Citiz v2.0 Open* FIPS Approved Algorithms by the platform

Algorithms usable by applets

The following algorithms are implemented in the platform and can be called by loaded applets.

The FIPS 140-2 validation did not include an applet, therefore these algorithms were not considered during the validation. Applets which use these functions will have to implement compliant key management and self-tests and undergo a re-validation (either 3SUB or 5SUB) for the complete module to be FIPS 140-2 validated.

Algorithms	Standard	Description	CAVP Cert #
Symmetric Algorithms			
Triple-DES	**[ANSI X9.52]** **[FIPS 46-3]** **[NIST SP800-67]**	*Triple-DES [2Keys, 3Keys]* . Data encryption / decryption in ECB mode . Data encryption / decryption in CBC mode . Triple-DES-MAC generates 8 byte MAC using Triple-DES CBC as defined by JavaCard. *This algorithm is Vendor affirmed* Note : Single DES is not approved for FIPS 140-2. The use of 2 key Triple-DES for encryption is currently 'restricted', until Dec 2015 when it will be 'disallowed'.	1689
AES	**[FIPS 197]**	*AES [128, 192, 256]* . Data encryption / decryption in ECB mode . Data encryption / decryption in CBC mode	2818
Asymmetric Algorithms			
RSA	**[FIPS** 186-4] **[PKCS#1 v2.1]**	*RSA CRT* . Signature generation *[768 to 3072 bit keys]* . Signature verification *[768 to 3072 bit keys]* Note: The key length must be greater or equal to 1024 bits to be compliant with FIPS 140-2.	1472
		RSA StraightForward . Signature generation *[512 to 2112 bit keys]* . Signature verification *[512 to 3072 bit keys]* Note: The key length must be greater or equal to 1024 bits to be compliant with FIPS 140-2.	1472
ECDSA	**[FIPS** 186-4]	Signature Generation *Curves: P-224, P-256, P-384, P-521*	494
		Signature Verification *Curves: P-224, P-256, P-384, P-521*	494
HASH			
SHA	**[FIPS 180-4]**	SHA-1[(3)], SHA-224, SHA-256, SHA-384, SHA-512 Note: The use of SHA1 for Digital Signature Generation will cause the module not to be compliant with FIPS 140-2 (as described in NIST SP800-131A)	2362
MAC			
CMAC	**[NIST SP800-38B]**	CMAC AES128-192-256	2818
HMAC	**[FIPS PUB 198A]**	Keyed-Hash Message Authentication Code	1765
Key Derivation Key			
KDF	**[NIST SP800-108]**	For SCP03, secure messaging defined by **[GP_AMD_D]** KDF in counter mode, AES128-192-256	62
DRBG			
DRBG	**[NIST SP800-90A]**	Deterministic Random Number Generation, AES-128	482

Tab 6: *IDeal Citiz v2.0 Open* FIPS Approved Algorithms for Applets

3.5 FIPS ALLOWED BUT NOT-APPROVED ALGORITHMS

Algorithms	**Standard**	**Description**	**Used by Platform**	**Available to Applets**
AES Key Wrapping	**[GP_AMD_D]**	Sensitive Data Decryption for SCP03 (ISD_K_{DEK} or SSD_K_{DEK}, based on approved AES-CBC) Key establishment methodology provides 128 to 256 bits of encryption strength.	Y	Y
Triple-DES Key Wrapping	**[GP]**	Sensitive Data Decryption for SCP02 (ISD_K_{DEK} or SSD_K_{DEK}, based on approved Triple-DES-CBC or Triple-DES-EBC) key establishment methodology provides 112 bits of encryption strength	Y	Y
T-RNG	AIS31 guidelines	Follow the class PTG.2, and the statical tests as per NIST SP800-22	Y	Y

Tab 7: *IDeal Citiz v2.0 Open* FIPS Allowed but Not-Approved Algorithms

4 CRYPTOGRAPHIC MODULE PORTS AND INTERFACES

4.1 PHYSICAL PORTS

The physical ports of the *IDeal Citiz v2.0 Open* cryptographic module consist of the contact and contactless interfaces of the chip.

The hardware of the chip detects the type of connection; i.e. in contact with a physical connection to VCC pin and in contactless with the detection of a radio frequency field. The chip is connected until power off.

4.1.1 Contact mode physical interface

On contact interface, two protocols are supported: T=0 and T=1 as defined in the **ISO7816** and **EMVco** standards.

The data rate is negotiated at the power-up; i.e. the cryptographic module sends the ATR wherein the greater possible baudrate is set (FiDi Max value) , then the terminal determines and sets the suitable baudrate in the range [FiDi=’11’ and FiDi Max].

The FiDi max value is set in the ATR during personalization in the ranges defined within the next two tab.

4.1.1.1 PROTOCOL T=0

The available speeds are the following one:

FiDi	Supported for	Baudrate (f = 3,57 MHz)
'11'	ISO & EMV	9 600
‘12’	ISO & EMV	19 200
‘13’	ISO & EMV	38 400
'14'	ISO & EMV	76 800
'18'	ISO & EMV	115 200

Tab 8: Supported contact speeds for T=0

The extended lengths are not supported.

4.1.1.2 PROTOCOL T=1

The available speeds are the following one:

FiDi	Supported for	Baudrate (f = 3,57 MHz)
'11'	ISO & EMV	9 600
‘12’	ISO & EMV	19 200
‘13’	ISO & EMV	38 400
'14'	ISO & EMV	76 800
'18'	ISO & EMV	115 200

Tab 9: Supported contact speeds for T=1

The extended lengths are supported. The size limit is 1168 bytes.

4.1.2 Contactless Physical Interface

The contactless interface supports the **ISO14443** standards.

The available speeds are:

Supported for	Speed
ISO & EMV	106 kbit/s
ISO	212 kbit/s
ISO	424 kbit/s
ISO	848 kbit/s

Tab 10: Supported contactless speeds

The negotiation of the communication speed is performed at each boot and is based on the greater common speed.

4.2 LOGICAL INTERFACE

The logical ports of The *IDeal Citiz v2.0 Open* defined according to *Figure 3*; the applications receive and send APDU's in contact or contactless ports, and the loaded applets are based on GlobalPlatform and JavaCard API's.

4.2.1 Contact Logical Interface

The *IDeal Citiz v2.0 Open* adheres to the **[ISO 7816-3]** specifications regarding the contact interface, which describe the relationship between the cryptographic module and its host (i.e. smart card reader) as one of "slave" and "master," respectively.

Interface	ISO7816 standard
CLK	Control IN
RST	Control IN
IO	Control IN, Data IN, Data OUT, Status OUT
VCC	Power
GND	Power

Tab 11: Contact Physical to Logical Interface mapping

4.2.2 Contactless Logical Interface

The *IDeal Citiz v2.0 Open* adheres to the **[ISO 14443]** specifications regarding the contactless interface, which describe the relationship between the cryptographic module and its host (i.e. smart card reader) as one of "slave" and "master," respectively.

Interface	ISO 14443 standard
L_A	Control IN, Data IN, Data OUT, Status OUT
L_B	Control IN, Data IN, Data OUT, Status OUT

Tab 12: Contactless Physical to Logical Interface mapping

4.3 SOFTWARE INTERFACES

Loaded applications support Java Card ™ 3.0.2 Classic Edition API and GlobalPlatform Card Specification - Version 2.1.1 API.

5 ROLES, SERVICES, AND AUTHENTICATION

5.1 ROLES

Tab 13 presents the roles, as defined by FIPS, supported by the *IDeal Citiz v2.0 Open* module.

Role	Description
CO Role	The Crypto Officer, so called CO, has access to the ISD. It is in charge of card security management, applet code loading, applet instantiation, SSD creation and SSD personalization. It can associate any created applet instance to a SSD or let this instance be linked to the ISD. The CO must authenticate to the Cryptographic Module with the Secure Channel Protocol defined by GlobalPlatform with DES or AES keys. This authentication is mandatory before any use of the ISD services.
User Roles	A User has access to a given SSD. It is in charge of the installation of its applications; i.e check the load file integrity before loading, personalization of its applications, provide its applications with secure channels, as defined by GlobalPlatform. User must authenticate to the Cryptographic Module with the Secure Channel Protocol defined by GlobalPlatform with DES or AES keys. This authentication is mandatory before any use of the SSD services.
No Roles	This role can access to unsecured services only, as far as it has no knowledge of any secrets.
Maintenance Role	Not supported

Tab 13: Roles Description

Basically the module does not support concurrent Crypto Officer Role, User Role and no-Role at the same time.

5.2 AUTHENTICATION

5.2.1 Secure Channel Protocols

The communication with an operator is based on the secure channel protocols #02 or #03 defined by GlobalPlatform. These protocols, namely SCP02 or SCP03, enforce:

- the operator authentication
- the integrity and the authentication of the data
- the confidentiality of the communication

The authentication is based on the processing of two APDU commands, i.e. INITIAL UPDATE and EXTERNAL AUTHENTICATE as defined by GlobalPlatform.

The probability that a random attempt succeeds at authentication depends on the block size, i.e. 64bit is Triple-DES and 128bit in AES.The probability is respectively 1 / 2^{64} and 1 / 2^{128}, that meets FIPS requirements (1/ 10^{6}).

5.2.2 Role authentication

The *IDeal Citiz v2.0 Open* module supports identity-based authentication. Tab 14 presents the authentication mechanisms associated to the corresponding roles.

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

Tab 14: 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 its 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 ISD (or SSD) counts the authentication attempts and the module no more answers once a defined threshold is reached. This feature is defined as “velocity checking” by GlobalPlatform in a range of [0 - 255].

The ability to change from one role to another is strictly enforced by the *IDeal Citiz v2.0 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 *IDeal Citiz v2.0 Open* module at the same time.

5.2.3 Authentication Strength

5.2.3.1 ROLE AUTHENTICATION MECHANISMS STRENGTH

The following table shows the key length of each secure channel and the corresponding key strength as defined by [NIST SP800-131A]:

Protocol	Key length	Key Strength
SCP02	Triple-DES 2 Keys	112bit
SCP03	AES 128	128bit
	AES 192	192bit
	AES 256	256bit

Tab 15: Strength of the Secure Channel Protocols

Tab 16 presents the strength of the authentication mechanisms, which is a summary of section 5.2.1 where the probabilities are detailed.

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	Mutual authentication (symmetric scheme)	Less than $1/10^6$	Less than $1/10^5$

Tab 16: Strength of the role authentication mechanisms

5.2.3.2 OTHER AUTHENTICATION MECHANISMS STRENGTH

Fingerprint verification

Depending on the *IDeal Citiz v2.0 Open* module version, a MOC mechanism may be available for the use of the future validated applets which will be loaded. It is not used by the *IDeal Citiz v2.0 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 strength of this authentication mechanism is configured during the module configuration (for example 10^{-4}). The application can use combination between fingerprints for higher strength.

PIN verification

Future validated applets loaded on the *IDeal Citiz v2.0 Open* may use the Global PIN for file access control or applet role authentication. It is not used by the *IDeal Citiz v2.0 Open* itself to authenticate a role.

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

5.3 SERVICES

5.3.1 Crypto-Officer Services

The crypto-officer and the ISD must authenticate each other before any processing. Only public data is accessible in plain-text.

Services	Description	Security functions
MANAGE_CHANNEL	CO opens or closes supplementary logical channels; i.e. LC#1, LC#2, or LC#3	None
SELECT	CO selects an application	None
GET_DATA	CO retrieves general public data (including ATR value) from the ISD or SSD.	None
INIT	CO authenticates and opens of a secured channel, with INITIAL UPDATE and EXTERNAL AUTHENTICATE APDU commands	SCP02 or SCP03 establishment
GET_STATUS	CO retrieves the life cycle data of Executable Load Files, Executable Modules, ISD, SSDs or applications, according to a given match/search criteria.	SCP02 or SCP03
SET_STATUS	CO modifies the life cycle state of the card (ISD state) and locks or unlocks SSDs and applets.	SCP02 or SCP03
INST_INST	CO creates an applet instance or a SSD instance, with INSTALL [for Install] APDU command	SCP02 or SCP03 Token Verification [(a)]
INST_EXTR	CO associates an ISD applet instance to a given SSD, with INSTALL [for Extradition]	SCP02 or SCP03 Token Verification [(a)]
LOAD	CO loads Executable Load Files with INSTALL [for Load] and LOAD APDU Commands. If required, SSD checks the load file signature (DAP Verification).	SCP02 or SCP03 Token Verification [(a)] DAP Verification [(b)]
STORE_DATA	CO stores a set of information in the ISD.	SCP02 or SCP03 Token Verification [(a)]
PUT_DES_KEY	CO modifies Triple-DES keys: ISD CO key set, ISD Key Encryption key, ISD Receipt Generation Key	SCP02 or SCP03
PUT_AES_KEY	CO modifies AES keys: ISD User key set or ISD Key Encryption key	SCP02 or SCP03
PUT_RSA_KEY	CO set or modifies the Public RSA key; Token Verification ISD. This key is public and so is not encrypted with ISD_K$_{DEK}$.	SCP02 or SCP03
DELETE	CO deletes an SSD/applet instance or an Executable Load File.	SCP02 or SCP03 Token Verification [(a)]

Tab 17: *IDeal Citiz v2.0 Open* Crypto-Officer services overview

Note [(a)]: The ISD performs Token Verification; i.e. the ISD authorizes the processing of the INSTALL commands. Token Verification is performed only if requested in the INSTALL commands.

Note [(b)]: SSD performs DAP Verification; i.e. SSD checks the signature of the Executable Loaded Files and so authorizes or not the loading process. The DAP Verification is optional if the Executable Load File belongs to the ISD (Crypto-Officer), and is mandatory if the Executable Load File belongs to an SSD (User).

5.3.2 User Services

The user and its SSD must authenticate each other before any processing. Only public data is accessible in plain-text.

Services	Description	Security functions
MANAGE_CHANNEL	User opens or closes supplementary logical channels; i.e. LC#1, LC#2, or LC#3	None
SELECT	User selects an application	None
GET_DATA	User retrieves general public data (including ATR value) from the ISD or SSD.	None
INIT	User authenticates and opens of a secured channel, with INITIAL UPDATE and EXTERNAL AUTHENTICATE APDU commands	SCP02 or SCP03 establishment
GET_STATUS	User retrieves the life cycle data of Executable Load Files, Executable Modules, ISD, SSDs or applications, according to a given match/search criteria.	SCP02 or SCP03
SET_STATUS	User modifies the life cycle state of the card (ISD state) and locks or unlocks SSDs and applets.	SCP02 or SCP03
INST_INST	User creates an applet instance, with INSTALL [for Install] APDU command	SCP02 or SCP03 Token Verification[c]
INST_EXTR	User associates an SSD applet instance to another SSD, with INSTALL [for Extradition]	SCP02 or SCP03 Token Verification[c]
LOAD	User loads Executable Load Files with INSTALL [for Load] and LOAD APDU Commands. If required, SSD checks the load file signature (DAP Verification).	SCP02 or SCP03 Token Verification[c] DAP Verification[d]
STORE_DATA	User stores a set of information in the SSD.	SCP02 or SCP03 Token Verification[c]
PUT_DES_KEY	User modifies TDES keys: SSD key set, SSD Key Encryption key, SSD DAP Verification Key [e]	SCP02 or SCP03
PUT_AES_KEY	User modifies AES keys: SSD User key set or SSD Key Encryption key	SCP02 or SCP03
PUT_RSA_KEY	User modifies public RSA key: DAP Verification Key [e]	SCP02 or SCP03
DELETE	User deletes an SSD/applet instance or an Executable Load File.	SCP02 or SCP03 Token Verification[c]

Tab 18: *IDeal Citiz v2.0 Open* User services overview

Note [c]: The ISD performs Token Verification; i.e. the ISD authorizes the processing of the INSTALL commands. Token Verification is Mandatory.

Note [d]: SSD performs DAP Verification; i.e. SSD checks the signature of the Executable Loaded Files and so authorizes or not the loading process. The DAP Verification is optional and depends if the verification is requested within the INSTALL [for load] command.

Note [e]: The DAP Verification Key is a public RSA Key or a DES Key.

5.3.3 No Role Services

An off-card device, namely terminal, that is neither a crypto officer nor a user, can perform the following services of the cryptographic module.

Services	Description	Security functions
MANAGE_CHANNEL	Terminal opens or closes supplementary logical channels; i.e. LC#1, LC#2, or LC#3	None
SELECT	Terminal selects of an application	None
GET_DATA	Terminal retrieves general public data (including ATR value) from the ISD or SSD.	None

Tab 19: *IDeal Citiz v2.0 Open* no role services overview

5.3.4 Services and Roles Mapping

The crypto module uses identity-based control to access the services of the *IDeal Citiz v2.0 Open* module. Tab 20 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
MANAGE_CHANNEL	X	X	X
SELECT	X	X	X
GET_DATA	X	X	X
INIT	X	X	
GET_STATUS	X		
SET_STATUS	X		
INST_INST	X	X	
INST_EXTR	X	X	
LOAD	X	X	
STORE_DATA	X	X	
PUT_DES_KEY	X	X	
PUT_AES_KEY	X	X	
PUT_RSA_KEY	X	X	
DELETE	X	X	

Tab 20: Services and Roles mapping

5.4 CRITICAL SECURITY PARAMETERS

5.4.1 Description

Tab 21 presents the cryptographic keys and other CSPs of the *IDeal Citiz v2.0 Open* module.

CSPs	**Description**
ISD key set (ISD_K_{ENC}, ISD_K_{MAC}, ISD_K_{DEK})	This key set is 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 Session key set (ISD_SK_{ENC}, ISD_SK_{MAC}, ISD_SK_{DEK})	This key set is derived from the ISD CO key set using the SCP02 (Triple-DES) or SCP03 (AES) protocols, used to authenticate the CO.
ISD Token Verification (ISD_K_{Token})	This key authorizes the processing of the INSTALL commands.
ISD Receive Generation (ISD_$K_{Receipt}$)	This key generates receipts send-out to CO that confirms that INSTALL commands have been performed.
SSD User key set (SSD_K_{ENC}, SSD_K_{MAC}, SSD_K_{DEK})	This key set is 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 Session key set (SSD_SK_{ENC}, SSD_SK_{MAC}, SSD_SK_{DEK})	This key set is derived from a SSD User key set set using the SCP02 (Triple-DES) or SCP03 (AES) protocols, used to authenticate a User.
SSD DAP key (SSD_K_{DAP})	Verification of the signature of Executable Loaded File. There is at most one SSD DAP key per SSD.

Tab 21: **Cryptographic keys and CSPs overview**

5.4.2 Access Control

The two following tables present service access rights to cryptographic keys and CSPs stored in the *IDeal Citiz v2.0 Open* module for ISD and SSD; i.e. respectively for Cryto-Officer and User modes.

Services	ISD_K$_{ENC}$, ISD_K$_{MAC,}$ ISD_K$_{DEK}$	ISD_SK$_{DEK}$	ISD_SK$_{ENC}$, ISD_SK$_{MAC}$	ISD_K$_{Token}$	ISD_K$_{Receipt}$
MANAGE_CHANNEL	-	-	-	-	-
SELECT	-	Delete	Delete	-	-
GET_DATA	-	-	-	-	-
INIT	Execute	Create	Create	-	-
GET_STATUS	-	-	Execute	-	-
SET_STATUS	-	-	Execute	-	-
INST_INST	-	-	Execute	Execute	Execute
INST_EXTR	-	-	Execute	Execute	Execute
LOAD	-	-	Execute	Execute	Execute
STORE_DATA	-	-	Execute	-	-
PUT_DES_KEY	Update	Execute	Execute	-	Update
PUT_AES_KEY	Update	Execute	Execute	-	-
PUT_RSA_KEY	-	-	-	Update	-
DELETE	-	-	Execute	Execute	Execute
TERMINATE	-	-	Execute	-	-

Tab 22: Services and ISD Keys mapping

Services	SSD_K$_{ENC}$, SSD_K$_{MAC}$, SSD_K$_{DEK}$	SSD_SK$_{DEK}$	SSD_SK$_{ENC}$, SSD_SK$_{MAC}$	SSD_K$_{DAP}$
MANAGE_CHANNEL	-	-	-	-
SELECT	-	Delete	Delete	-
GET_DATA	-	-	-	-
INIT	Execute	Create	Create	-
GET_STATUS	-	-	-	-
SET_STATUS	-	-	-	-
INST_INST	-	-	Execute	-
INST_EXTR	-	-	Execute	-
LOAD	-	-	Execute	Execute
STORE_DATA	-	-	Execute	-
PUT_DES_KEY	Update	Execute	Execute	Update
PUT_AES_KEY	Update	Execute	Execute	-
PUT_RSA_KEY	-	-	Execute	Update
DELETE	-	-	Execute	-

Tab 23: Services and SSD Key mapping

6 PHYSICAL SECURITY

6.1 ELECTROMAGNETIC INTERFACE AND COMPATIBILITY –EMI/EMC-

The *IDeal Citiz v2.0 Open* module conforms to the EMI/EMC requirements specified by part 47 Code of the Federal Regulations, part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

6.2 HARDWARE SECURITY

The *IDeal Citiz v2.0 Open* module is designed to provide hardware security:

- Opacity
- Tamper resistance and tamper evidence
- Physical penetration
- Resistance to chemical attack

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.

Note: Module hardness testing was performed at ambient temperature; no assurance is provided for level 3 hardness conformance at any other temperature.

6.3 SECURITY MECHANISMS

The module implementation is a production grade, commercially available single chip device (INFINEON M7892), which contains the following hardware security features:

- Dual CPU mechanism, for fault detection
- Full CPU, Memory, Bus an Cache encryption
- Error Detection Codes (EDC) in all memories
- Error code for cache protection (Post Failure Detection, PFD)
- Address and data scrambling of memories
- Active I^2 shield

6.4 MODULE ENCAPSULATION

The physical encapsulation of the chip is a metallic and opaque 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 *IDeal Citiz v2.0 Open* module will notice the attempt just by looking at the module.

7 MITIGATION OF OTHER ATTACKS

The cryptographic module mitigates the following attacks:

Attacks	Countermeasures	Limitations
SPA/SEMA	Countermeasures against Simple Power Analysis / Simple ElectroMagnetic Analysis attacks	N/A
Timing	Countermeasures against Timing attacks	N/A
DPA/DEMA	Countermeasures against Differential Power Analysis / Differential ElectroMagnetic Analysis attacks	N/A
CPA/CEMA	Countermeasures against Correlation Power Analysis / Correlation ElectroMagnetic Analysis attacks	N/A
DFA	Countermeasures against Differential Fault Analysis attacks	N/A

Tab 24: Mitigation of Other Attacks

The software implements countermeasures based on the hardware capabilities of the chip, see section 6.3 for the list of security mechanisms. In addition the software enhances the mitigations with:

- additional confidentiality and integrity on the sensitive data,
- correctness and completeness of the execution of the code.

8 CRYPTOGRAPHIC KEY MANAGEMENT

8.1 KEY OVERVIEW

Tab 25 gives an overview of all the cryptographic keys used in the *IDeal Citiz v2.0 Open* module.

Cryptographic keys	Key name	Algorithms	Key size (bits)
ISD Key Set	Encryption key: ISD_K_{ENC}	Triple-DES	112
		AES	128, 192, 256
	Mac key: ISD_K_{MAC}	Triple-DES MAC	112
		CMAC	128, 192, 256
	ISD_K_{DEK}	Triple-DES	112
		AES	128, 192, 256
ISD Session Key Set	Encryption key: ISD_SK_{ENC}	Triple-DES	112
		AES	128, 192, 256
	Mac key: ISD_SK_{MAC}	Triple-DES MAC	112
		CMAC	128, 192, 256
ISD Token Verification Key	ISD_K_{Token}	RSA	1024 RSA Public Key
ISD Receipt Generation	$ISD\_K_{Receipt}$	DES	112
SSD Key Set	Encryption key: SSD_K_{ENC}	Triple-DES	112
		AES	128, 192, 256
	Mac Key: SSD_K_{MAC}	Triple-DES MAC	112
		CMAC	128, 192, 256
	SSD_K_{DEK}	Triple-DES	112
		AES	128, 192, 256
SSD Session Key Set	Encryption key: SSD_SK_{ENC}	Triple-DES	112
		AES	128, 192, 256
	Mac Key: SSD_SK_{MAC}	Triple-DES MAC	112
		CMAC	128, 192, 256
SSD DAP Verification Key	SSD_K_{DAP}	RSA	1024 RSA Public Key

Tab 25: Cryptographic key overview

8.2 KEY ESTABLISHMENT TECHNIQUES

8.2.1 ISD Key Establishment Techniques

ISD Key Set:

This key set is first entered in the Cryptographic Module in factory before the first run of the ISD. The description of the secured method uses for this loading is out of the scope of this document.

The Crypto Officer can update this key set with the PUT_DES_KEY or PUT_AES_KEY services, see section 5.3.1.

ISD Session Key Set:

These three keys are derivated from ISD_K_{ENC}, ISD_K_{MAC}, and ISD_K_{DEK} according to **[GP]** section E.4.1 "DES Session Keys", and [GP_AMD_D] section 6.2.1 "AES Session Keys".

They are created at SCP establishment and destroyed at the end of the current session.

ISD Token Verification Key:

The Crypto Office has to set this key with the PUT_RSA_KEY in case of Delegated Management requirement.

ISD Receipt Generation Key:

The Crypto Office optionally sets this key with the PUT_DES_KEY in case of Delegated Management requirement.

8.2.2 SSD Key Establishment Techniques

SSD Key Set:

The user provides this key set to the SSD under the ISD protection; i.e. the SCP.

The user updates this key with the PUT_DES_KEY or PUT_AES_KEY services see section 5.3.2.

SSD Session Key Set:

These three keys are derivated from SSD_K_{ENC}, SSD_K_{MAC}, and SSD_K_{DEK} according to **[GP]** section E.4.1 "DES Session Keys", and [GP_AMD_D] section 6.2.1 "AES Session Keys".

SSD DAP Verification Key:

The user updates this key with the PUT_RSA_KEY see section 5.3.2.

8.3 KEY GENERATION

The key generations are proposed to applets only; i.e. the platform applications as ISD and SSD do not perform any key generations.

RSA CRT, RSA, ECDH and Elliptic Curve cryptographic keys are generated on board, based on DRBG.

An RSA CRT key pair generation function, compliant with **[PKCS#1 v2.1]**, is available to the future applets loaded on the *IDeal Citiz v2.0 Open*. Entry/Output

The 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); i.e under trusted path.

Cryptographic keys are output from the cryptographic module only if a trusted path has been establishment before; i.e. CSP encryption.

9 SELF-TESTS

The *IDeal Citiz v2.0 Open* cryptographic module performs a set of self-tests to ensure that it works properly.

9.1 POWER-UP SELF-TESTS

The *IDeal Citiz v2.0 Open* module performs the following self-tests (KAT method) at power-up:

- DRBG
- Triple-DES ciphering/deciphering known answer test
- AES ciphering/deciphering known answer test

The *IDeal Citiz v2.0 Open* module is able to process APDU commands only once the Self-Tests are passed.
The Known Answer Test method consists on comparing the result of computation according to referenced data; i.e. known input, known output and known key. All these data are dedicated to self-test only and stored in Flash. The keys are handled as any keys in the module, see section **[**8**]**.

The T-RNG is tested; the KAT method cannot be applied because T-RNG does not support any input data, so the test consists in checking the probability.

9.2 CONDITIONAL SELF-TESTS

The platform performs the following conditional self-tests before the first use.

- RSA StraightForward: signature
- SHA1

Applets do not have to self-test the following algorithms since it is automatically done by the platform when they call the JavaCard API for the first time. These self-tests are not used by the platform without an applet, and were not included within the scope of the platform validation, except for the RSA StraightForward and SHA1:

- RSA with CRT: ciphering, signature, and key generation
- RSA StraightForward: ciphering, signature, and key generation
- ECDSA: signature, and key generation
- SHA 1, SHA 224, SHA 256, SHA 384, and SHA 512

Note: SHA 1 is automatically tested in the RSA signature verification tests.

The module does not self-test the following algorithms:

- HMAC
- CMAC

Note: FIPS 140-2 compliant applications using CMAC and/or HMAC shall implement their own CMAC KAT and/or HMAC KAT, and shall call them before first algorithm use.

9.3 SELF-TESTS ON DEMAND

The suites 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 enters in an error state and remains mute until the card is reset.

9.5 SOFTWARE TESTS

9.5.1 Integrity Tests

The integrity of each sensitive data, i.e. keys and CPS, is tested at usage.

9.5.2 Key Pair-Wise Tests

RSA Key generation

Consistency test is performed on RSA Key generation.

Elliptic Curve Key Generation

Consistency test is performed on Elliptic Curve Key generation.

9.5.3 Random Generator

The T-RNG is continuously tested.

The DRBG is continuously tested.

9.5.4 Loaded Application test

JavaCard applications are loaded in module according to the security defined by GlobalPlatform; i.e. the operator has to be authenticated as Crypto-Officer or User, the installation services are authorized by the ISD; the loaded application signature is verified according to the DAP specification (RSA).

10 SECURITY RULES

The following represents the security rules established for and supported by the *IDeal Citiz v2.0 Open* cryptographic module.

10.1 PRIVILEGES SECURITY RULES

- Each application and Security Domain in card has a set of privileges defined by GP.

10.2 SECURE OPERATION SECURITY RULES

- The *IDeal Citiz v2.0 Open* module cannot return back to the personalization lifecycle state once personalization has been performed: personalization can therefore only be performed once.
- Operators have the capability at any time to retrieve the identification number of the *IDeal Citiz v2.0 Open* module.
- All the applets loaded on the *IDeal Citiz v2.0 Open* module shall be **FIPS** compliant; otherwise the module shall lose its validation.
- The installation phases, executed by ISD and SSD, are all performed under secure messaging with authentication, confidentiality and integrity.
- In delegated management the *IDeal Citiz v2.0 Open* module shall both verify the authorization of the execution of the install commands with the ISD token verification, and Load File signature with the SSD DAP verification.
- CO and Users 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 *IDeal Citiz v2.0 Open* module does not output data during self-tests and error states.
- The module is set in mute state on attack detection. The mutecard counter is incremented and the module is set in an infinite loop. The module restarts only after a hardware reset.
- The module is set in terminate state; i.e. no-more usable because all secrets are erased, e.g. keys, if:
  - A configured number of mutecards is reached. It is set at pre-personalization.
  - The terminal sends a Terminate command to the module.

10.3 AUTHENTICATION SECURITY RULES

- CO and Users do not share or disclose their secret authentication data to unauthorized operators.
- After reception of the *IDeal Citiz v2.0 Open* module, the User updates his authentication data.
- The *IDeal Citiz v2.0 Open* module does not record any authentications after power down.
- The strength of each authentication mechanism is better than $1/10^6$ for a one-time guess and $1/10^5$ for multiple attempts in a 1-minute period.
- The *IDeal Citiz v2.0 Open* module authenticates one operator at a time.

10.4 KEY MANAGEMENT SECURITY RULES

- The module has a zeroization service for all CSPs stored in Flash. The zeroization is triggered when the module is set to terminated state.
- The *IDeal Citiz v2.0 Open* module relies on CSP encryption service for the protection of all CSPs entering or leaving the cryptographic boundary.

10.5 PHYSICAL SECURITY RULES

- The *IDeal Citiz v2.0 Open* module shall be inspected periodically for evidence of tampering. Nevertheless, inspections are barely impossible for the end-user since the module is either included within a plastic card for contactless or in between contact plates and resin and plastic card.
- The *IDeal Citiz v2.0 Open* module remains mute until it is reset in case UV light or temperatures go outside acceptable bounds.
- A FLASH, RAM, ROM integrity check failure lead to mute the *IDeal Citiz v2.0 Open* module.
- The *IDeal Citiz v2.0 Open* module is physically protected by opaque resin and plastic card.

10.6 SELF-TESTS SECURITY RULES

- The *IDeal Citiz v2.0 Open* module performs power-up self-tests automatically, without operator intervention.
- The operator is able to perform power-up self-tests at any time, on demand.
- The *IDeal Citiz v2.0 Open* module enters an error state when a self-test fails.
- No data is output before power-up self-tests are completed.
- No data is output when conditional self-tests are performed.

10.7 DELIVERY PROCESS

The delivery process shall be agreed by each party; i.e. Manufacturer, crypto-officer, and optionally personalization center. Each of the following steps is performed with authentication, confidentiality and integrity, typically, it is composed of:

- Manufacturer (Morpho): The software and the personalizer’s keyset are pre-loaded in the module. Plastic card embodiment is done. Optionally, applets are loaded too.
- Personalization center: The crypto-officer (or personalizer) can load and personalize the applets.
- Delivery to end-users is under the responsibility of the crypto –officer.