ypsid

FIPS 140-2 Non-Proprietary Security Policy

Level 3 validation

Version 0.5

November 2010

DOCUMENT CONTROL

	COMPANY	NAME	POSITION	DATE	SIGNATURE
Established by:	Sagem Orga	P. Gislard	SE		
Approved by:	Sagem Orga	R.Picon	RPM		
Safety Assurance:	Sagem Orga				
Purchasing Dpt:	Sagem Orga				
Quality Assurance:	Sagem Orga	E.Piollet	QAE		
Authorized by:	Sagem Orga	Y.Courquin	HRD		

EVOLUTIONS OF THE DOCUMENT

VERSION	DATE	NATURE OF MODIFICATION
01	FEBRUARY 2008	Document creation
02	AUGUST 2009	Hardware identification update. Firmware identification update. Zeroization mechanism update. ATR's Historical byte H13 update.
03	JANUARY 2010	§ 1.2: Adding diagram of the module § 9.1: Specifying the type of test that is performed to satisfy the EEPROM FW during Power up Integrity Test
04	OCTOBER 2010	Responses to CMVP comments.
05	NOVEMBER 2010	Responses to CMVP comments.

TABLE OF CONTENTS

GLOSSARY

AID	:	Application IDentifier
APDU	:	Application Protocol Data Unit
API	:	Application Protocol Interface
ATR	:	Answer To Reset
CBC	:	Cipher Block Chaining
CCID	:	Circuit Card Interface Devices
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
HID	:	Human Interface Devices
ISD	:	Issuer Security Domain
ISO	:	International Organization for Standardization
MAC	:	Message Authentication Code
MOC	:	Match On Card
PKCS	:	Public Key Cryptographic Standards
RAM	:	Random Access Memory
P-RNG	:	Pseudo Random Number Generation
ROM	:	Read Only Memory
RSA	:	Rivest Shamir Adleman
SEMA	:	Simple Electromagnetic Analysis
SHA	:	Secure Hash Algorithm
SPA	:	Simple Power Analysis
SSD	:	Supplementary Security Domain
TDES	:	Triple DES

REFERENCE DOCUMENTS

[FIPS 140-2]	:	National Institute of Standards and Technology, Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules, May 25, 2001
[ISO 7816-2]	:	Identification Cards – Integrated Circuit(s) Cards with Contacts Part 2: Dimensions and location of the contacts
[ISO 7816-3]	:	Identification Cards – Integrated Circuit(s) Cards with Contacts Part 3: Electronic signals and transmission protocols
[ISO 7816-4]	:	Identification Cards – Integrated Circuit(s) Cards with Contacts Part 4: Inter-industry commands for interchange
[USB]	:	Universal Serial Bus Specification Revision 2.0 April 27, 2000
[CCID]	:	Universal Serial Bus - Device Class: Smart Card CCID - Specification for Integrated Circuit(s) Cards Interface Devices - Revision 1.1 - April 22nd, 2005
[ICCD]	:	Universal Serial Bus - Device Class: Smart Card ICCD - Specification for USB Integrated Circuit(s) Card Devices - Revision 1.0 - April 22nd 2005
[HID]	:	Universal Serial Bus - Device Class Definition for Human Interface Devices (HID) - Firmware Specification - 6/27/01 - Version 1.11
[JCS]	:	Java Card ™ 2.2.1 Card Specification, Sun Microsystems
[GP]	:	Global Platform Card Specification - Version 2.1.1 - May 2003 – Global Platform – Configuration 3
[FIPS 180-2]	:	National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-2 with Change Notice 1, February 25, 2004
[ANSI X9.31]	:	American Bankers Association, Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998, Washington, D.C., 1998
[PKCS#1 v2.1]	:	RSA Laboratories, PKCS#1 v2.1: RSA Cryptography Standard, June 14, 2002
[ANSI X9.52]	:	American Bankers Association, Triple Data Encryption Algorithm Modes of Operation, ANSI X9.52 – 1998
[ISO 9797]	:	Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm
[ISO/IEC 3309]	:	Information technology -- Telecommunications and information exchange between systems -- High-level data link control (HDLC) procedures -- Frame structure
[CO GUIDE]	:	Sagem Sécurité, ypsid Crypto Officer guidance, SSE-0000067309

1 INTRODUCTION

1.1 SCOPE

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

1.2 PRODUCT DESCRIPTION

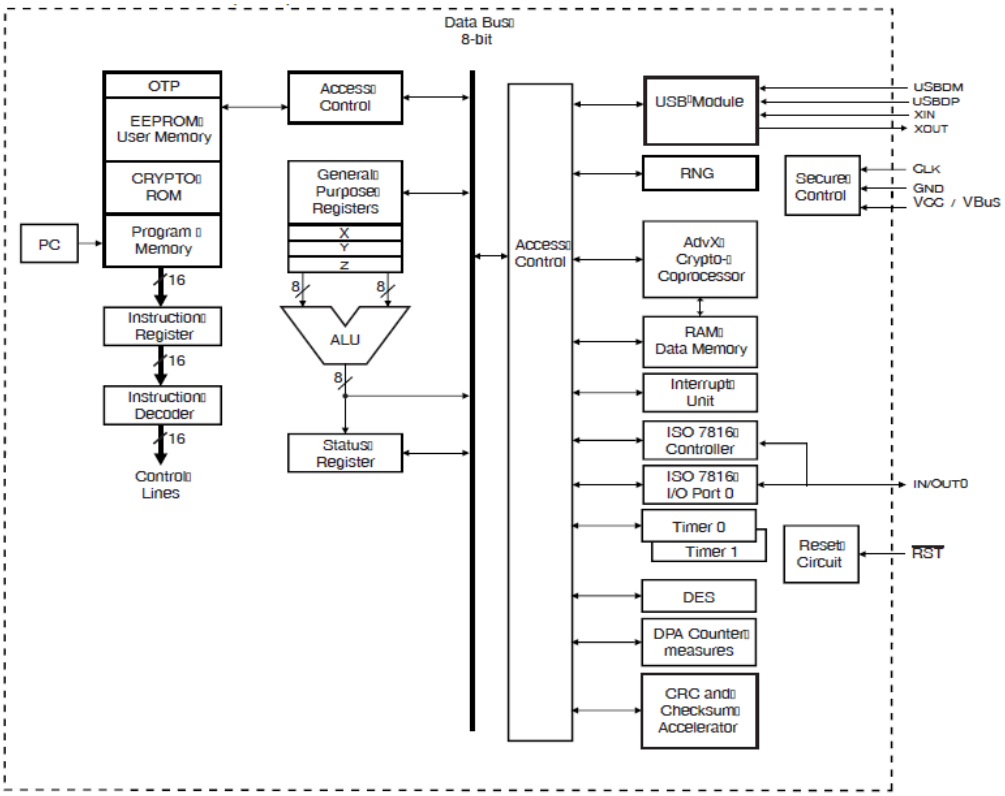

Figure 1: ypsid cryptographic module diagram

Note: On Figure 1, the dotted line represents the cryptographic boundary of the module.

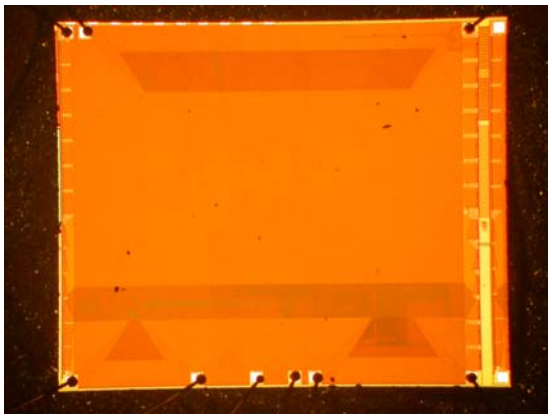

Figure 2: ypsid cryptographic module

The ypsid module is an ISO and USB interface smart card platform with a javacard operating system compliant with Sun Java Card ™ 2.2.1 **[JCS]** and Global Platform 2.1.1 **[GP]** specifications. The ypsid hardware is based on the ATMEL AT90SC 256 72 RCT-USB chip.

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

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

1.3 PRODUCT IDENTIFICATION

The identification number of the ypsid module is given below:

Module	***Identification number***	
	Hardware	***Firmware***
ypsid	AT90SC25672RCT-USB	**01029069** - FFFFFFF

The identification number of the ypsid module can be retrieved at any time.

1.4 SECURITY LEVEL

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

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

Tab 1: ypsid area specific levels

1.5 ALGORITHMS

The algorithms used in the FIPS Approved mode of operation of the ypsid module are listed in Tab 2. All of them offer FIPS Approved functionalities.

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

Tab 2: ypsid FIPS Approved algorithms

The ypsid module employs a non-deterministic hardware random number generator of the ATMEL AT90SC 256 72 RCT-USB chip to seed the FIPS Approved **[ANSI X9.31]** P-RNG function. A CRC16 (based on the ISO/IEC 3309 standard) is used for Firmware integrity by a CRC16 calculation. Triple-DES (key wrapping; key establishment methodology provides 80 bits of encryption strength).

1.6 FIPS MODE OF OPERATION

The ypsid cryptographic module only supports a FIPS Approved mode of operation.

This FIPS Approved mode of operation of the ypsid module is indicated by a specific value of a dedicated byte in the ATR: the historical byte H13 must have the following value:

B7	*B6*	*B5*	*B4*	*B3*	*B2*	*B1*	*B0*
x	1	1	x	x	x	x	x

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

- at power up by looking at the value of the ATR,
- at any time by asking the module to output the value of the ATR.

Instructions for determining the secure delivery of the module may be found in the **[CO GUIDE]**.

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 chip AT90SC 256 72 RCT-USB revision D with reference AT58829D.

The ypsid firmware is composed of an operating system complying with the **[JCS]** and **[GP]** standards.

The ypsid cryptographic module is designed to be encased in a hard opaque resin that can be embedded into a plastic card, a USB key or any other support structure. However, neither the resin nor the support structure resides within the cryptographic boundary.

2.2 CRYPTOGRAPHIC MODULE BOUNDARY

The cryptographic module boundary is realized as the external surface of the ATMEL AT90SC 256 72 RCT-USB single-chip microprocessor and does not include any embodiment elements (resin, micro-bonds, smart card contact plate, fixation glue). The boundary contains all of the relevant module components (processors performing cryptography, etc.) consistent with **[FIPS 140-2]**. There are no component exclusions from the boundary.

2.3 DESCRIPTION

The ypsid cryptographic module is composed of the ATMEL AT90SC 256 72 RCT-USB single-chip microprocessor, which includes:

- 256 KB of ROM
- 72 KB of E²PROM
- 8 KB of RAM

The ypsid cryptographic module operates using the ISO interface or the USB interface. The module automatically detects which interface is being used and answers to the terminal using the same interface.

In any case, the module does not operate using both interfaces at the same time. The ypsid module remains in FIPS mode of operation regardless of the communication interface (ISO or USB).

The module has no internal power supply (battery, capacitor, etc.). All power to the module, provided by the host (smart card reader, USB key reader), enters the power input interface through the voltage bond pad. The defined voltage range for normal conditions of use is: 1.62 V to 5.5 V.

3 CRYPTOGRAPHIC MODULE PORTS AND INTERFACES

3.1 PHYSICAL PORTS

The physical ports of the ypsid cryptographic module consist of both the ISO and the USB physical interfaces of the chip. Both physical interfaces fulfill all the Level 3 requirements for ports and interfaces (**[FIPS 140-2],** area 2).

3.1.1 ISO physical interface

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

Physical ports	***Description***
VCC	Power supply (Voltage)
RST	Reset signal
CLK	Clock signal
GND	Ground
IN/OUT 0	Input/Output

Tab 3: Description of the ISO physical ports

3.1.2 USB physical interface

For the USB interface, the physical ports of the ypsid cryptographic module consist of the USB endpoints of the chip.

Tab 4 lists the physical ports of the module for the USB interface.

USB physical ports	***Description***
VCC	Power supply (Voltage)
GND	Ground
IN/OUT 0	Input/Output
USB D+	Input/Output
USB D-	Input/Output
USB-Xin	Clock signal
USB-Xout	Clock signal

Tab 4: Description of the USB physical ports

The ports used by the USB interface are physically different from the ports used by the ISO interface, except for those that are explicitly shared between both interfaces:

- The voltage physical ports (VCC and GND) are common to the ISO and the USB interfaces.
- The IN/OUT 0 physical port may also be used by the USB interface.

3.2 LOGICAL PORTS

The logical ports of the ypsid cryptographic module consist of both the ISO and the USB logical interfaces. Both interfaces fulfill all the Level 3 requirements for ports and interfaces (**[FIPS 140-2],** area 2).

3.2.1 ISO logical interface

The ypsid module adheres to the **[ISO 7816-3]** specifications regarding the ISO 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 bond pads 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 5.

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

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

3.2.2 USB logical interface

Communications are based on the USB transmission protocol, ICCD class, as defined in **[USB]**, **[CCID]** and **[ICCD]**. The ICCD class of the USB protocol allows interacting as with a card reader interface: the host sees the module as a smart card inserted in a card reader.

The cryptographic module and the host communicate by exchanging APDU commands and APDU responses, defined in **[ISO 7816-4]** specifications.

Tab 6 describes the logical ports of the cryptographic module for the USB interface and their mapping to the physical ports.

Logical interfaces	***Physical interface***
Power	VCC
	GND
Data Input	USB D+ USB D-
Data Output	USB D+ USB D-
Control Input	USB D+ USB D-
	USB-Xin
	IN/OUT 0
Status Output	USB D+ USB D-
	USB-Xout
	IN/OUT 0

Tab 6: Functional specification of the USB interface

The ypsid module also implements the USB protocol, HID class, as defined in **[USB]** and **[HID]**. This class is not used by the ypsid platform itself, but is available for the future applets aimed to be loaded on the ypsid platform. Please see Appendix A.

4 ACCESS CONTROL POLICY

4.1 ROLES

Tab 7 presents the two roles supported by the ypsid module.

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

Tab 7: Role description

4.2 AUTHENTICATION

4.2.1 Role authentication mechanisms

The ypsid module supports identity-based authentication according to Level 3 requirements for the roles, services and authentication area of **[FIPS 140-2]**. Tab 8 presents the authentication mechanisms associated to the corresponding roles.

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

Tab 8: Roles and required authentication

The mutual authentication is performed with the authentication data through the INIT service. Therefore an operator proves the knowledge of his authentication data by successfully completing the INIT service.

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

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

The ability to change from one role to another is strictly enforced by the ypsid 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 ypsid module at the same time.

4.2.2 Role authentication strength

Tab 9 presents the strength of the role authentication mechanisms.

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

Tab 9: Strength of the FIPS Approved role authentication mechanisms

4.3 SERVICES

4.3.1 Services description

Tab 10 describes the services of the ypsid module and the security functions used at the invocation of each service.

Services	*Description*	*Security functions*
SELECT	Selection of the ISD, a SSD or an applet instance.	
GET_DATA	Retrieving general information (including ATR value) from the ISD or from an SSD.	
INIT	CO or User authentication and opening of a secured channel.	TDES, TDES MAC
GET_STATUS	Retrieving the life cycle data of Executable Load Files, Executable Modules, ISD, SSDs or applications, according to a given match/search criteria.	
SET_STATUS	Modification of the life cycle state of the module (ISD state) and locking or unlocking of SSDs and applets.	
INST_INST	Creation of an applet instance or a SSD, with its AID and its capability to be selected by default.	
INST_EXTR	Association of an ISD applet instance to a given SSD.	
LOAD	Loading of applet firmware	
STORE_DATA	Storage of a set of information in the ISD or in a SSD.	TDES
PUT_DES_KEY	Modification of a TDES key (ISD CO key set, ISD Key Encryption key, SSD User key set or SSD Key Encryption key).	TDES
PUT_RSA_KEY	Set a RSA public key (SSD DAP key).	TDES
DELETE	Deletion of an applet instance or of code or of an Executable Load File.	
SELF_TESTS	Execution of power up self-tests.	TDES, SHA-1, SHA-256, RSA, P-RNG
TERMINATE	Zeroization of the whole E²PROM.	

Tab 10: ypsid services overview

4.3.2 Services Access Control

The crypto module uses identity-based control to access the services of the ypsid module. Tab 11 presents the authorized roles for each service.

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

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

Tab 11: Service access control

4.4 CSPS

4.4.1 CSPs description

Tab 12 presents the CSPs of the ypsid module.

CSPs	***Description***
ISD CO key set (ISD_K_{ENC}, ISD_K_{MAC})	Two static double TDES keys, that are used to derive the ISD CO Session key set as part of the CO authentication. There is one ISD CO key set per module.
ISD Key Encryption key (ISD_K_{KEK})	A static double TDES key used to cipher CSPs entering the module. There is one ISD Key Encryption key per module.
ISD CO Session key set (ISD_SK_{ENC}, ISD_SK_{MAC})	Two double TDES keys, derived from the ISD CO key set using the SCP.01 protocol, used to authenticate the CO.
SSD User key set (SSD_K_{ENC}, SSD_K_{MAC})	Two double TDES keys used to derive a SSD User Session key set as part of a User authentication. There is one SSD User key set per SSD.
SSD Key Encryption key (SSD_K_{KEK})	A static double TDES key used to cipher CSPs entering the module. There is one SSD Key Encryption key per SSD.
SSD User Session key set (SSD_SK_{ENC}, SSD_SK_{MAC})	Two double TDES keys, derived from a SSD User key set using the SCP.01 protocol, used to authenticate a User.
E^2PROM Protection key	A double TDES key used to cipher the E^2PROM key storage location.
P-RNG Seed key	A double key generated by the non-deterministic hardware random number generator and used to seed the Approved **[ANSI X9.31]** P-RNG function.
P-RNG Seed	64 bits generated by the non-deterministic hardware random number generator and used to seed the Approved **[ANSI X9.31]** P-RNG function.

Tab 12: **ypsid CSPs overview**

Additionally, the ypsid module may contain RSA public key: the SSD DAP Public keys (SSD_K_{DAP}). SSD DAP keys are RSA public keys dedicated to a specific SSD and used to verify the signature of the loaded firmware. There is at most one SSD DAP key per SSD.

4.4.2 CSPs Access control

Tab 13 presents the services access rights to CSPs and keys stored in the ypsid module.

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

Tab 13: CSPs & keys access rights within services

5 PHYSICAL SECURITY

5.1 [FIPS 140-2] LEVEL 4 REQUIREMENTS

The ypsid 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 256 72 RCT-USB), 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 module 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 ypsid 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 ypsid cryptographic module.

This module performs the firmware load test on all new code, and as such the ypsid 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 ypsid cryptographic module.

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

7 CRYPTOGRAPHIC KEY MANAGEMENT

7.1 KEY OVERVIEW

Tab 14 gives an overview of all the cryptographic keys used in the ypsid module.

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

Tab 14: Cryptographic key overview

7.2 KEY GENERATION

No cryptographic key is generated on board.

7.3 ENTRY/OUTPUT

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

Cryptographic keys are never output from the cryptographic module.

7.4 STORAGE

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

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

7.5 ZEROIZATION

There is a zeroization mechanism to actively overwrite all static cryptographic keys and other CSPs stored in the E²PROM, which is implemented via the Destroyed service. This is achieved by erasing the whole E²PROM (erasing the whole E²PROM will also terminate the module).

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

8 EMI/EMC

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

9 SELF-TESTS

The ypsid cryptographic module performs a set of self-tests to ensure that it is working properly, as required by **[FIPS 140-2]**.

9.1 POWER UP SELF-TESTS

The ypsid module performs the following self-tests at power up:

- E²PROM firmware integrity check CRC16 test.
- **[ANSI X9.31]** Pseudo random number generation known answer test.
- TDES 2 key CBC ciphering/deciphering known answer test.
- RSA CRT signature & SHA-1 known answer test.
- RSA signature verification known answer test.
- SHA-256 known answer test.

9.2 CONDITIONAL SELF-TESTS

The ypsid module performs the following conditional self-tests:

- Hardware random number generation continuous test.
- **[ANSI X9.31]** pseudo random number generation continuous test.
- TDES MAC Firmware Load Test (Note: new applet code is applicable only to future validated cryptographic modules based on this product).
- CRC integrity check for CSPs.

9.3 SELF-TESTS ON DEMAND

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

9.4 SELF-TESTS FAILURE

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

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

10 MITIGATION OF OTHER ATTACKS

The ypsid module implements countermeasures to protect against the attacks listed in Tab 15:

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 15: Mitigation of other attacks

Note: As an expanded security feature of **[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 ypsid module unusable. Therefore, if an attacker tries to remove the shield of the module, he will not be able to access any sensitive information.

11 SECURITY RULES

The following represents the security rules established for and supported by the ypsid cryptographic module.

11.1 SECURE OPERATION SECURITY RULES

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

11.2 AUTHENTICATION SECURITY RULES

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

11.3 KEY MANAGEMENT SECURITY RULES

- The module shall contain a zeroization service for all CSPs stored in E²PROM.
- The ypsid module shall rely on CSP encryption keys for the protection of all CSPs entering the cryptographic boundary.
- The P-RNG seed key shall not have the same value as the P-RNG seed.

11.4 PHYSICAL SECURITY RULES

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

11.5 SELF-TESTS SECURITY RULES

- The ypsid module shall perform power up self-tests automatically, without operator intervention.
- The operator of the module shall be able to perform power up self-tests at any time, on demand.
- When a self-test fails, the module shall output a specific status and enter an error state.
- Moreover, if the self-test failing is the E²PROM firmware integrity check, then the ypsid 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.

APPENDIX A: FUTURE MODULE FUNCTIONALITY

The ypsid module also implements the following functionalities that will be available for the future applets aimed to be loaded on the platform:

- On board key generation (up to a 2048-bit modulus RSA).
- File system.
- MOC mechanism for fingerprint verification.

AUTHENTICATIONS:

Fingerprint verification

A MOC mechanism is available for the use of the future validated applets which will be loaded. It is not actually used by the ypsid itself to authenticate a role.

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

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

PIN verification

Future validated applets loaded on the ypsid platform may use the Global PIN for file access control or applet role authentication. It is not used by the ypsid platform itself to authenticate a role.

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

KEY GENERATION:

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

CONDITIONAL SELF TESTS:

RSA key pair wise consistency check after each RSA key pair generation. No cryptographic key is actually generated on board by the ypsid platform itself. But a FIPS Approved RSA CRT key pair generation function is available to the future applets loaded on the ypsid platform. Therefore the corresponding self-test is also available for the use of the future applets.