SHARP JCOP31ID FIPS
Security Policy
Public Version

Document *Version 1.40*

Sharp Corporation
Large-Scale IC Group

Date: 15 February 2007

Revision History

Date	Description
31 August 2005	Initial document
8 November 2005	Update and edits
9 November 2005	Update and edits
14 November 2005	Update and edits
19 November 2005	Update and edits GWS
22 November 2005	Update and edits RDS
7 December 2005	Update and edits RDS
27 December 2005	Update and edits SO
05 January 2006	Merge of IBM Edits and Sharp JAPAN Edits
11 January 2006	Update edits for Sharp items
12 January 2006	Update edits for Physical Security
22 February 2006	Edits for Security Boundary
27 February 2006	Merge of IBM Edits
03 March 2006	Merge of SMA edits
10 May 2006	Merge of IBM Edits and Sharp Edits
11 May 2006	Merge of IBM Edits
9 June 2006	Merge of IBM Edits and Sharp Edits
10 October 2006	Update edits for Sharp item
12 January 2007	Update edits
15 February 2007	Update edits (ECSVDP)

TABLE OF CONTENTS

1. MODULE OVERVIEW **5**

2. SECURITY LEVEL **6**

SECURITY POLICY OVERVIEW 6

3. SUPPORTED CRYPTOGRAPHY **7**

FIPS CRYPTOGRAPHY 7
NON-FIPS CRYPTOGRAPHY 7

4. PORTS AND INTERFACES **7**

5. ROLES AND SERVICES **9**

IDENTIFICATION AND AUTHENTICATION POLICY 10
Logical Channels *11*
Secure Channel Support *11*
SERVICES 11

6. APPROVED MODE OF OPERATION **14**

7. ACCESS CONTROL POLICY **15**

ROLES AND SERVICES 15
DEFINITION OF MODULE KEYS 15
Module Key Encryption Key (Master Key) *16*
Global PIN *16*
DEFINITION OF CSP MODES OF ACCESS 16

8. OPERATIONAL ENVIRONMENT **17**

9. EMI/EMC **17**

10. SECURITY RULES **17**

CRYPTOGRAPHIC OFFICER IDENTIFICATION & AUTHENTICATION 18
APPLET LOADING SECURITY RULES 18

11. KEY MANAGEMENT SECURITY POLICY **18**

11.1 CRYPTOGRAPHIC KEY GENERATION 18
11.2 CRYPTOGRAPHIC KEY ENTRY 18
11.3 CRYPTOGRAPHIC KEY STORAGE 18
11.4 KEY DESTRUCTION 19

12. SELF TESTS **19**

POWER UP SELF-TESTS: 19
SOFTWARE / FIRMWARE TEST 19
CONDITIONAL SELF TESTS 20
SELF-TEST FAILURES 20

13. PHYSICAL SECURITY POLICY **20**

13.1 PROTECTION AGAINST PHYSICAL TAMPERING 20
13.2 HARDWARE SECURITY FUNCTIONS - ENVIRONMENTAL STRESS 21
13.3 MALFUNCTION DETECTION 21
13.4 LOGICAL TAMPER PROTECTION 22

OPERATOR REQUIRED ACTIONS 22

14. OPERATOR GUIDANCE 23

CRYPTO-OFFICER GUIDANCE 23

USER GUIDANCE....23

15. MITIGATION OF OTHER ATTACKS.... 24

16. REFERENCES.... 25

17. DEFINITIONS AND ACRONYMS 26

1. Module Overview

The SHARP JCOP31ID FIPS is defined as a single-chip embedded cryptographic module. The base module is a single-chip 16-bit Sharp processor (HW Part #: SM4128(V3)A7; HAL Version 1.1.06) and a specifically modified version of the IBM JCOP31IDv2.2OS Release Level 0400 for this application to meet the FIPS 140-2 requirements. As defined the final module provides an operational environment with up to 528 kBytes of Cryptographic Officer/Issuer available Flash memory. The defined user space allows for multiple validated applets to be concurrently loaded and used, as well as supported re-issuance capability.

The primary purpose for this device is to provide data security for Personnel Identification. The defined module is specifically designed to prohibit non-evident tampering by both physical and electronic means and will only load FIPS-validated software applications (applets)

This document is a description of the security for the module and a description of how these requirements are achieved. This Security Policy specifies the rules under which the Cryptographic Module must operate.

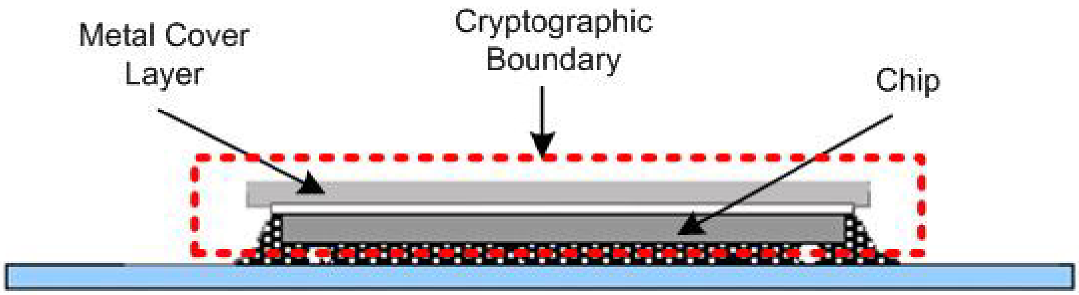


Figure 1 – Image of the Cryptographic Module

The diagram above illustrates the encapsulated IC as mounted. The interface is defined at the boundary of the IC, which is the cryptographic boundary.

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1 - Module Security Level Specification

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

Security Policy Overview

The cryptographic module is a single chip Integrated Circuit with its embedded firmware, which is inclusive of the JCOP environment. The module supports a dual communications interface employing the JCOP JavaCard Platform, on which FIPS 140-2 Level 2 validated applets may be loaded and instantiated.

The red line around the IC shows the module cryptographic boundary. The defined module contains a 16-bit microprocessor, 8 Kilobytes of RAM and up to 528 Kilobytes of available non-volatile memory. The module uses Java Card™ Technology and makes available GlobalPlatform services to applets loaded and instantiated on the module. This document addresses the submission for validation of the module in accordance with FIPS 140-2 Level 2 standard. Basic security requirements are described for the module. The security rules by which the cryptographic module must operate are defined.

All of the low-level services, inclusive of memory management, I/O control, cryptographic algorithms and physical security are addressed herein. A specific implementation of the Java Card™ specification version 2.2.1 and GlobalPlatform version 2.1.1 specification are detailed. These services can be accessed by the applets instantiated from code loaded in the module's non-volatile memory using the specified version of the Java Card™ Application Programming Interface (API).

GlobalPlatform services are provided through a Card Manager. These services are conditionally available internally (accessible by applets) and external to the cryptographic boundary (accessible by external or non-chip applications). This validation is limited in scope to the Systems software, virtual machine, and Card Manager with no instantiated applets.

If any applet is instantiated, the module is no longer configured as a FIPS 140-2 approved module. Instantiation of any applet will require the module be re-validated. And instantiating an applet does not affect the operational mode. The FIPS approved module no longer exists to operate in a non-approved mode.

3. Supported Cryptography

FIPS Cryptography

In FIPS mode, the cryptographic module only supports FIPS Approved algorithms as follows:

- TDES (supports 2 and 3 key) ECB and CBC encryption / decryption
- TDES message authentication code generation and verification
- ECDSA[1]: Maximum key length 384 bits. Note: Need to use NIST recommend curves and key sizes (Curves (P-192 P-224 P-256 P-384)).
- AES[1] supports 128, 192, 256 bit key lengths, ECB, CBC
- RSA[1] key generation, encryption and decryption: supports key lengths between 1024 and 2048 bits in steps of 32 bits. Note: This operation cannot be used for bulk data encryption. It exists for the purpose of key wrapping and digital signature operations. For encryption and decryption, CRT and non-CRT keys are supported, but only CRT keys can be generated. (If used for key establishment, the methodology provides between 80 bits and 112 bits of encryption strength)
- FIPS approved DRNG: A deterministic general-purpose random number generator (DRNG) implemented according FIPS PUB 186-2 Appendix 3, using DES. The DRNG is self-checking and will stop processing if it detects that it is generating the same number repeatedly.
- Hardware NDRNG. This is used only to seed the approved DRNG and to overwrite key data when no longer required. The NDRNG is self-checking and will stop processing if it detects that it is generating the same number repeatedly.
- Hashing Algorithms: SHA-1.

1 – Not supported without an application.

Non-FIPS Cryptography

Use of non-approved algorithms places the module in a non-approved mode of operation.

The cryptographic module provides non-FIPS Approved algorithms as follows:

- DES (non-compliant)
- AES[1] Message Authentication Code generation and verification
- RSA[1] keys of 512 up to 1024 bits in steps of 32 bits. *(If used for key establishment, the methodology provides between 56 bits and 80 bits of encryption strength)*
- Elliptic Curve Secret Value Derivation Primitive (ECSVDP)[1]

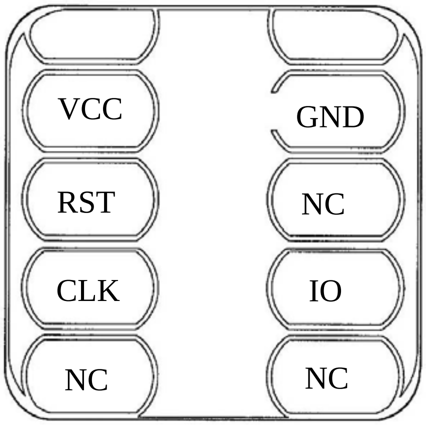
1 – Not supported without an application.

4. Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

- **Contact mode**: Communication to and from the cryptographic module is through an Input/Output interface that can be a printed circuit contact plate to provide the electrical connection required. Bond wires connect the module to the printed circuit contact plate. The Contact plate and printed circuit are outside of the module cryptographic boundaries.

Power (VCC)	Supply voltage input (2.7V to 5.5V)
Ground (GND)	Supply Ground connection
Clock (CLK)	Clock Input
Reset (RST)	Externally applied Reset Signal
Input/Output (IO)	Input or Output of Serial data



- **Transmission protocols**: For the defined module the protocols are compatible with ISO/IEC 7816-3 (half duplex character oriented transmission protocols ISO T=0 and T=1. The module supports the Protocol and Parameter Selection to select a new protocol type or change transmission baud rate. Up to 256 data bytes can be exchanged within one command. The maximum communication speed in contact mode is 145,200 bit/s with a clock of 4.5 MHz).
- **Contactless mode**: The module uses two electrical connections to the antenna, which are physically different from the electrical connections used in contact mode. The antenna is not within the cryptographic boundaries of the module. When the module and antenna are moved into close proximity of a compatible reader/writer, power is provided to the module and data is transmitted to and from the module by means of a 13.56 MHz modulation signal, per ISO 14443 Type B specifications. The module operates independently of the external clock for all application, with the reader/writer providing the necessary power source.
- **RF signal and Power interface**: Both are fully compliant with ISO/IEC 14443 part 2: Radio frequency power and signal interface for contactless integrated circuit cards. Initialization and anti-collision parameters are fully compliant with ISO/IEC 14443 Type B requirements. The contactless communication range of the module is about 2 cm. This distance is designed to assure correct operation and high resistance to eavesdropping on transactions. Communications in the contactless mode is based on a fully standardized (ISO/IEC 14443 Type B), half-duplex transmission protocol, T=CL.
- **Logical Data Interface**: Once communication is established between the reader and the platform, the platform functions as a “slave” processor to implement and respond to the reader commands. The platform adheres to a well defined set of state transitions. Within each state, a specific set of commands is accessible. The I/O ports of the platform (either physical in contact mode or virtual in the case of RF transmission) provide the following logical interfaces which employ Application Program Data Units (APDUs) as described here:

APDU commands consist of a mandatory command header (***Control Input***) of four bytes followed by a conditional command body (***Data Input***). The response APDU consists of an conditional response body (***Data Output***) followed by a mandatory response trailer (***Status Output***).

Table 2 - ISO 7816-4 Command/Data structure

Header	**Body**
CLA INS P1 P2	[Lc Field] [Data Field] [Le Field]

The number of bytes present in the data field of the command APDU is denoted by Lc.

The maximum number of bytes expected in the data field of the response APDU is denoted by Le (length of expected data). When the Le field contains only zeros, the maximum number of available data bytes is requested.

Table 3 - ISO 7816-4 Command Response/Data structure

Body	**Trailer**
[Data Field]	SW1 SW2

Given that the data fields are conditional, the following table shows the various logical interface combinations that are possible.

Table 4 - ISO 7816 Command/Data combinations

ISO Command Type	**Command Data**	**Expected Response**
1	No Data	No Data
2	No Data	Data
3	Data	No Data
4	Data	Data

5. Roles and Services

Roles

The cryptographic module supports the following roles:

- **Cryptographic-Officer**: This role is responsible for administrating the cryptographic platform and security configuration. The Cryptographic-Officer is obliged to authenticate his identity to the System Software Card Manager (SS CM) before the SS CM would permit changes to any existing configuration from outside of the cryptographic boundary. Depending on the operational security policy, the Cryptographic-Officer may further need to establish a secure channel with the GlobalPlatform SS CM Security Domain.

Authentication and secure channel communication requires the knowledge of shared secrets between the SS CM and the Cryptographic-Officer. The role of Cryptographic-Officer may be played by the Issuer of a specific form factor (e.g. a card) containing the module.

- **Applet Provider**: The Applet Provider is the external entity that makes use of the Java API available on the module. Applications loaded and instantiated on behalf of the Applet Provider make use of the SS CM. Some applications will access cryptographic services provided by the module using well documented JavaCard APIs.

One or more Applet Provider applications may require a dedicated Security Domain instance independent of the available SS CM Security Domain.

- **User**: A User is an external entity that makes use of one or more applications resident on the module. Users select applications by name.

Identification and Authentication Policy

The module supports identity-based authentication as follows:

- **Identification**. The identification of a user of a FIPS validated application on the module is achieved by selecting the application using a known Application Identifier Name (e.g., AID) and conditionally providing a key set reference associated with the application.

The use of the documented JavaCard SELECT APDU command is the manner by which a particular applet is internally selected by the SS CM and made the focus of further commands.

The role and operational responsibilities of the Cryptographic-Officer often results in the selection of the SS CM. Selection of the SS CM in this role includes life cycle management of key material. The selection of the key set by which the Cryptographic-Officer is authenticated is done by reference and uses the GlobalPlatform APDU command INITIALIZE UPDATE. This APDU command produces information in a manner that will be immediately used to mutually authenticate the Cryptographic-Officer, residing beyond the cryptographic boundary, and the module internal SS CM.

- **Authentication***.* Any external entity (e.g. the Cryptographic-Officer) attempting to achieve an authenticated state with the System Software Card Manager resident in the module is obliged to use the GlobalPlatform specified form of a mutual authentication protocol. The GlobalPlatform mutual authentication is achieved by the external entity sending two APDU commands in a specific order. The order of commands is the APDU command INITIALIZE UPDATE is sent first followed by the ISO/IEC 7816-4 APDU command EXTERNAL AUTHENTICATE. The System Software makes use of a shared secret, symmetrical key cryptographic convention for achieving this mutual authentication.

The protocol description for this mutual authentication is detailed here:

The INITIALIZE UPDATE command allows the external entity to indicate to the System Software Card Manager (SS CM) what key set (and specific key reference within the key set) is required to be used for this particular authentication sequence along with challenge data. The SS CM performs internal processing on the external entity challenge data supplied to the SS CM to create the SS CM authentication cryptogram to be returned as part of the response.

The response to the INITIALIZE UPDATE APDU command is a constructed message containing key diversification data, session protocol indication, session key version number, the SS CM authentication cryptogram and the SS CM external entity challenge data. The authentication cryptogram returned in the response is enciphered with the specific shared secret key indicated by the external entity. The encipher operation employs the Triple DES algorithm as specified in the GlobalPlatform specification.

The external entity uses the information from the INITIALIZE UPDATE response to first authenticate the SS CM (i.e. validation of the SS CM authentication cryptogram). Presuming the SS CM is authenticated to the external entity, the next step is for the external entity to compute an authentication cryptogram to be sent to the SS CM using the next APDU command in this ordered sequence; EXTERNAL AUTHENTICATE.

The external entity sends the authentication cryptogram information and any secure channel requests in the APDU command EXTERNAL AUTHENTICATE to the SS CM. The SS CM attempts to authenticate the external entity by deciphering the authentication cryptogram using the Triple DES algorithm specified in the GlobalPlatform specification. Successful completion of this last step in the protocol results in the external entity and SS CM having authenticated each other. A benefit of this protocol is any secure channel requirements are met at the same time (without the need for additional APDU commands).

This authenticated state evaluates to TRUE by the SS CM after successful completion of the mutual authentication protocol described herein. The authenticated state shall remain TRUE until such time another application is selected, or the module is physically reset, or the removal of power. The authenticated state evaluates to FALSE under all other conditions.

Failure of the EXTERNAL AUTHENTICATE command in this mutual authentication protocol (or out of sequence use of INITIALIZE UPDATE) represents a possible brute force attack on the SS CM and module. To address this threat, a numeric counter is implemented which records the number of consecutive failed authentication operations noted by the SS CM. Too many consecutive failed authentication attempts results in the SS CM placing itself in a "locked" state.

Logical Channels

Support for Logical Channels is supported as per ISO/IEC 7816-4:2005. Logical Channels allow for multiple, unique application sessions to be communicating simultaneously with several applications resident in the module.

Secure Channel Support

Full support for a Secure Channel using the TDES algorithm is provided as defined by GlobalPlatform specification 2.1.1, Clause 8 "Secure Communication".

The Secure Channel provides a means to achieve confidentiality and data integrity for communicating between an internal selectable application residing on the module and an external entity located beyond the cryptographic boundary. There are three phases to any Secure Channel; Initiation, Operation, and Termination. Secure Channel relies upon one or more Secure Channel Protocols as defined by either GlobalPlatform or the Applet Provider.

The life of a Logical Secure Channel is limited to the duration of an Application Session.

Services

An authenticated state of TRUE for the Cryptographic Officer results in special access to several services. These services are used to manage cryptographic material held within one or more Security Domains and to allow the loading of applications into the module.

INSTALL: Installing an application or Security Domain requires the invocation of several different on-card functions (e.g. the install method). The INSTALL command is used to instruct the Card Manager as to which installation step it shall perform during an application installation process. The command must be used in the context of a Secure Channel and so its level of security must match the security level defined in the EXTERNAL AUTHENTICATE command.

LOAD*:* This command is used to load the byte-codes of the Load File (package) defined in the previously issued INSTALL command. Applets are loaded inside a Secure Channel established by the Crypto Officer with the Card Manager during the identification/authentication process. The applet is divided into a series of blocks that fit in a LOAD command. The loading consists of a series of LOAD commands, each one transmitting a block, encrypted and followed by a TDES MAC with the TDES key set selected by the Crypto Officer during the identification process. The TDES MAC ensures the correct transmission of each block of the applet, therefore ensuring the correct transmission of the whole applet.

DELETE: This command is used to delete a uniquely identifiable object. The object may be an Application, a load file, or a Key-Set. The command must be used in the context of a *Secure Channel* and so its level of security must match the security level defined in the EXTERNAL AUTHENTICATE command.

PUT PUBLIC KEY: This command is used to load RSA Public keys for DAP Verification. This command is used by Security Domain that supports DAP Verification (i.e. has the DAP Verification privilege) to add a public key modulus and it related exponent. The PUT KEY command may only be issued within a Secure Channel Session and the level of security for the command is dependent on the security level defined in the EXTERNAL AUTHENTICATE command. The public key components are only loaded once and not updated and the public key for Crypto Officer is set during this module is loaded, this command can not be used by Crypto Officer.

GET STATUS: The Get Status command is used to verify that the Card Manager has enabled all the access control rules. It allows retrieving of Card Manager and Application related life cycle status information according to a given match/searching criteria. This command can also be used by the Cryptographic officer to verify that the module is still in FIPS Mode and that only FIPS approved applications are instantiated. It's the complementary command to Set Status. The command must be used in the context of a Secure Channel and so its level of security must match the security level defined in the External Authenticate command.

INITIALIZE UPDATE: This command initiates a Secure Channel used by subsequent commands. It allows platform authentication by the Crypto Officer or User, and computes session keys used for MAC computation and command encryption in issuance of subsequent commands. However, the Secure Channel is not considered open until completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command.

EXTERNAL AUTHENTICATE: This command is used by the module to authenticate the host, to establish the Secure Channel, and to determine the level of security required for all subsequent commands within the Secure Channel. The EXTERNAL AUTHENTICATE command must be preceded by the INITIALIZE UPDATE command.

STORE DATA: This command is used to personalize a data object from a Security Domain or to transfer data to an Application. The Issuer Security Domain determines if the command is intended for itself or an Application depending on a previously received command. Multiple Store Data commands transfer data to the Application by breaking the data into smaller components for transmission. In this case, Store Data command is numbered (starting at '00' and increments by one in a sequential manner). The command must be used in the context of a Secure Channel and the level of security for the command is dependent on the security level defined in the External Authenticate command.

SET STATUS: This command is used by Crypto Officer to modify the life cycle state of the card or the life cycle of designated application with Crypto Officer, or User to modify the life cycle of its own application. Set Status is the complementary command to Get Status. When the command is performed as the APDU one, it must be used by Crypto Officer in the context of a Secure Channel and so its level of security must match the security level defined in the External Authenticate command. When it is performed with Global Platform API, it can be used by User.

PUT TDES KEY: this command is used to:
1. Set the Initialization Secret Key (ISK);

2. Set the Receipt verification Secret Key (RSK);
3. Add a new key-set version containing a complete set of keys (Set of 3 double length DES keys);
4. Replace multiple keys within an existing key-set version;
5. Replace multiple keys within an existing key-set version and change its version number (Key-set replacement). If it already exists in the Issuer Security Domain, the current key-set or specific key is replaced. A key is uniquely identified by the combination of its key-set version and its key index. An application may have multiple key-set versions. Multiple keys may exist within a given key-set version. The command must be used in the context of a Secure Channel and so its level of security must match the security level defined in the EXTERNAL AUTHENTICATE command to add or replace Security Domain key sets.

SET/VERIFY PIN: This command is used to change or verify the global PIN. The global PIN handler is Cardholder Verification Method service. This command is defined as Global Platform API and can be accessed by Crypto Officer or User.

DAP VERIFICATION: DAP verification allows the Crypto-Officer to check application code integrity and authenticity with the public key of a Security Domain specified in LOAD command before the application code is loaded. .

No Role

The following services are available without authentication.

GET DATA: The GET DATA command is used to retrieve a single data object, such as the Card Identification data that can be used to determine if the module manufacturing configuration is in approved mode . This command can be used in clear mode outside of a Secure Channel. The following data objects can be retrieved using the get data command:

GetData Commands

Table 5 – GetData Retrievable Data Objects

Tag (coded in P1, P2)	Length in bytes	(coded in Le) Meaning
9F7Fh	2Dh	Card production life cycle (42 bytes)
00CFh	0Ch	User Key diversification data (10 bytes)
00E0h	Variable	Key Information Template
00C1h	05h	Sequence Counter of the default Key Version Number (Implicit Key version)
0066h	Variable	Card Recognition Data

SELECT: This command is used to select an application (Card Manager, Security Domain or Applet), and does not require prior authentication. This command also allows the identification of the Cryptographic Officer when issued with the Card Manager AID, and the identification of the User/Application Provider when issued with a Security Domain AID.

Table 6 illustrates what services are available by role.

Table 6 – Services authorized for Roles

Role / Service	Crypto Officer / Issuer	User / Applet Providers	Unauthenticated (No Role)
SELECT	X	X	X
INITIALIZE UPDATE	X	X	
EXTERNAL AUTHENTICATE	X	X	
STORE DATA	X	X	
GET DATA	X	X	X
SET STATUS	X	X	
GET STATUS	X		
PUT TDES KEY	X	X	
PUT PUBLIC KEY		X	
INSTALL	X		
LOAD	X		
DELETE	X		
SET / VERIFY PIN	X	X	
DAP VERIFICATION	X		

Table 7 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
TDES, 2 or 3 key	The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{80}$ or $1/2^{112}$ which are less than 1 in 1,000,000. The probability of successfully authenticating to the module within one minute is $10/2^{80}$ or $10/2^{112}$ which are less than 1 in 100,000.

6. Approved Mode of Operation

This security policy does not include any non-FIPS validated applet instances. As such, the cryptographic module is always in an approved mode of operation. The security services described in this document can be used to load any kind of applets into the JavaCard chip platform. However, it is the responsibility of the Cryptographic Officer/Issuer to insure that only FIPS validated instances are created. The FIPS approved mode of operation for the evaluation described in this security policy starts from the instantiation of the Card Manager and Security Domains and ends with the instantiation of any non-FIPS validated applets or the instantiation of a FIPS validated applet that has its Applet Access Control Rules (ACRs) set improperly.

The Cryptographic Officer/Issuer can determine whether the card is still in FIPS mode by authenticating to the Card Manager and issuing a Get Status command to list all the applications instances currently installed in the card. To prevent a non FIPS approved applet from being instantiated and given the AID (application identifier) of an approved applet the module assigns the applet with the AID specified in the executable load file. The Cryptographic-Officer/Issuer may then at any time check that only FIPS approved executable load files have been instantiated. The Get Data command on a selected applet instance allows the Cryptographic-Officer to verify that the ACRs have been set correctly.

7. Access Control Policy

Roles and Services

Table 8 – Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User / Applet Providers	TDES Authentication	TDES Keys (User/Applet Provider Security Domain)
Crypto Officer / Issuer	TDES Authentication	TDES Keys (Crypto-Officer Security Domain)

Definition of Module Keys

Initial Issuer Transport Key

1. **KDC**: Initial Issuer Key set: Set of three Triple DES Keys (called KDC_{ENC} KDC_{MAC} and KDC_{KEK}) of 16 bytes each. The first two, KDC_{ENC} and $KDC_{MAC,}$ are only used to generate Secure Channel session keys during the initiation of a Global Platform Secure Channel, and the last one, KDC_{KEK} is used as a key transport key within a secure channel. The process used to generate a unique KDC per cryptographic module takes place outside of the crypto module. KDC_{ENC} and KDC_{MAC} are used to generate KSC_{ENC} and KSC_{MAC} keys that are used to authenticate the secure sessions with the card Manager (Section 11.1 Cryptographic Key Generation). KDC_{KEK} is used directly to wrap the CO CDK key set and the User ADK key set when they are entered into the module for the first time.

2. **KSC**: Initial Issuer Session Transport Keyset: Set of two transient Triple DES Keys (called KSC_{ENC} KSC_{MAC}) of 16 bytes each. The transient keys are cleared on power down. KSC_{ENC} is used for Secure Channel Encryption, and KSC_{MAC} is used for Secure Channel MAC verification.

Crypto-Officer keys in the Card Manager

1. **CDK**: Crypto Officer Keyset: Set of three Triple DES Keys (called CDK_{ENC} CDK_{MAC} and CDK_{KEK}) of 16 bytes each. The first two, CDK_{ENC} and CDK_{MAC}, are only used to generate Secure Channel session keys (CSK_{ENC} and CSK_{MAC}) during the initiation of a Global Platform Secure Channel, and the last one, CDK_{KEK} is used as a key transport key within the secure channel. The process used to generate a unique CDK per cryptographic module takes place outside of the crypto module.

2. **CSK**: Crypto Officer Session Keyset: Set of two transient Triple DES Keys (called CSKENC and CSKMAC) of 16 bytes each. CSKENC is used for Secure Channel Encryption, and CSKMAC is used for Secure Channel MAC verification.

User/Applet Provider Keys in Security Domains

1. **ADK**: Applet Provider Keyset: Set of three Triple DES Keys (called ADK_{ENC} ADK_{MAC} and ADK_{KEK}) of 16 bytes each. The first two, ADK_{ENC} and ADK_{MAC}, are only used to generate Secure Channel session keys (ASK_{ENC} and ASK_{MAC}) during the initiation of a Global Platform Secure Channel, and the last one, ADK_{KEK} is used as a key transport key within the secure channel. This keyset is present in both type of Security Domain, Security Domain with Delegated Management, and Security Domain with DAP Verification. The process used to generate a unique ADK per cryptographic module takes place in the cryptographic HSM outside of the crypto module.

2. **ASK**: Applet Provider Session Keyset: Set of two transient Triple DES Keys (called ASK_{ENC} and ASK_{MAC}) of 16 bytes each. ASK_{ENC} is used for Secure Channel Authentication and optionally Encryption, and ASK_{MAC} is used for Secure Channel MAC verification.

3. **K_{DAP}**: Key DAP: Public RSA Key (1024 bits) used to verify the DAP on an application code to be loaded into the module and authorize or not its loading. This key may or may not be loaded into the module. It is an added feature and is not intended to satisfy any of the FIPS 140-2 requirements for applet loading. This key is present only in a Security Domain with DAP Verification.

Module Key Encryption Key (Master Key)

This is a two-key T-DES key generated during manufacturing at time of burning the program lock fuse. It is used by the module to encrypt all secret and private keys that are stored within the module, in Flash.

Global PIN

The global PIN is managed by the Card-Manager and can be used by applets. The PIN is stored in BCD format and includes only numerical digits, coded on a nibble (4 bits), left justified, and eventually padded on the right with 'F' nibble if necessary (i.e. the number of digits is odd). The maximum length is 8 bytes or 16 digits.

Definition of CSP Modes of Access

Table 9 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

Table 9 – CSP Access Rights within Roles & Services

Service	Role	CSP	Access
PUT TDES KEY	CO	CDK_{ENC} CDK_{MAC} and CDK_{KEK}	Write
	USER/AP	ADK_{ENC} ADK_{MAC} and ADK_{KEK}	Write
INITIALIZE UPDATE & EXTERNAL AUTH	CO	KDC_{ENC} and KDC_{MAC} CDK_{ENC} and CDK_{MAC}	Read & Execute
	USER/AP	ADK_{ENC} and ADK_{MAC}	Read & Execute
TDES Key Encryption (during key	CO	CDK_{KEK}	Write

loading)	USER/AP	ADK_{KEK}	Write
Message Integrity & Encryption	CO	KSC_{ENC} & KSC_{MAC} CSK_{ENC} & CSK_{MAC}	Read & Execute
	USER/AP	ASK_{ENC} & ASK_{MAC}	Read & Execute
Message Integrity Only	CO	KSC_{MAC} CSK_{MAC}	Read & Execute
	USER/AP	ASK_{MAC}	Read & Execute
set PIN or verify PIN with GlobalPlatform API	CO	Global PIN	Write
	USER/AP	Global PIN	Write
PUT PUBLIC KEY command	USER/AP	K_{DAP}	Write
RSA PKCS#1 Signature Verification by Applet Provider Security Domain	USER/AP	K_{DAP}	Read & Execute
Internal use only for module to encrypt all secret and private keys stored in Flash memory.	CO	Module Key Encryption Key	Read & Execute
	USER/AP	Module Key Encryption Key	Read & Execute

8. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because a TDES MAC must be used to load applets and the module supports a limited operational environment..

9. EMI/EMC

The cryptographic module meets the Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) requirements specified by United States Standards 47 CFR Part 15, Subpart B: “Unintentional Radiators, Digital Devices, Class B”.

10. Security Rules

This section documents the security rules enforced by the cryptographic module to implement the FIPS 140-2 Level 2 security requirements.

The cryptographic module shall provide two distinct operator roles. These are the User/Applet Provider role, and the Cryptographic Officer/Issuer role. The operator who wishes to authenticate into the User/Applet Provider role must first identify him/herself by providing both an application identifier and a Key ID. The authentication is then done by proving the possession of the particular keyset identified in the identification phase. This Key Set is composed of 3 TDES keys. One key is used to encrypt the command data, one key to authenticate the user, and the third key is used to encrypt keys transported within the APDU command. This is the same process as the Crypto Officer/Issuer authentication (Initialize Update & External Authenticate commands) which uses the TDES keys of the Applet Provider Security Domains.

Cryptographic Officer Identification & Authentication

The operator that wishes to authenticate into the Cryptographic Officer role must first identify him/herself by providing both information to uniquely select the Card Manager, and a Key Set ID. The authentication is then done by proving the possession of the particular keyset identified in the identification phase. This Key Set is composed of 3 TDES keys. One key is used to encrypt the command data, one key to authenticate the user, and the third key is used to encrypt keys transported within the APDU command. This is the same process as the User authentication (Initialize Update & External Authenticate commands).

Applet Loading Security Rules

Applets can only be loaded through a secure channel in that they pass from the outside the module environment into the module environment in a MACed form. An additional applet encryption is also available as an option. To activate that option, the Cryptographic Officer/Issuer would have to request the encryption option when opening the secure channel with the module. The applet code would then not only be MACed, using CSKMAC, but also encrypted using CSKENC. In the JCOP environment, the applet is always loaded by the Issuer (Cryptographic Officer/Issuer). The optional mechanism designated as “DAP” in GP 2.1.1 enables the applet provider to check, independently of the Issuer (Cryptographic Officer), that his applet has been correctly loaded. This check is done by verifying an RSA PKCS#1 signature on the Hash of the applet code being loaded. This process is described in detail in the GP 2.1.1 document.

If an applet is loaded, the module will no longer be configured as a FIPS 140-2 Approved module.

11. Key Management Security Policy

11.1 Cryptographic key generation

TDES Session key derivation for Secure Channel Opening, conforming to Open Platform Card Specification v2.1 using FIPS186-2 approved ANSI X9.31 DRNG. RSA key pair generations (up to 2048 bit key length) with strong prime numbers[1] (ANSI X9.31) using FIPS140-2 approved DRNG. RSA Chinese Remainder Keys can be generated. This cryptographic service is made available through Java APIs only.

11.2 Cryptographic key entry

Keys shall always be input in encrypted format, using the Put Key (TDES or Public) command within a secure channel. During this process, the keys are encrypted using the Key Encryption Key and optionally the encryption session key of the secure channel. Keys can never be output by the module.

11.3 Cryptographic key storage

The Keys are structured to contain the following parameters:

- Key set version
- Key Index, which is the ID of the key,

[1] For further information on “strong prime numbers”, see ANSI x9.31, Appendix C, Section C.3 Strong Primes

• Algorithm ID, which determines which algorithm to be used,
• Integrity Mechanisms.
.

11.4 Key Destruction

The module destroys cryptographic keys by reloading another key-set with the same version number for Crypto Officer Keys and User/Application Provider Keys, using the **PUT TDES KEY** or **PUT PUBLIC KEY** command.
User/Application Provider Keys can also be zeroized by deleting the Security Domain that hosts the keys, using the **DELETE** command.
Closing of the secure channel has also the effect of zeroizing the associated session keys stored in RAM memory.

The module key encryption key is zeroiable on the moment that the card life cycle is changed to TERMINATED state with **SET STATUS** command.

12. Self Tests

Self Tests listed are initiated by resetting the module.

Power up Self-Tests:

The following tests are implemented:

- AES
  -encrypt two blocks in CBC mode with known key and compare result to a known value
  -decrypt result and compare to the original input
- TDES
  -encrypt two blocks in CBC mode with known key and compare result to a known value
  -decrypt result and compare to the original input
- RSA: key length 1024 bits
  -sign 128-bytes of data using CRT private key and compare result to a known value
  -verify result using public key and compare to the original input
- ECDSA: curve P-192/key length 24 bytes
  -sign 20 bytes of data using known key and compare result to a known value
  -verify result of signature
- DRNG
  -seed DRNG with known number and compare the second number generated to a known value
- SHA-1
  -hash the string “abc” and compare result to known value

Software / Firmware Test

All software code that is in Flash will be checked with a 16-bit CRC.

The one CRC value for each software code is generated and stored in loading the software and the CRC is calculated and compared with the stored value every power-up.

If the integrity check in power-up fails, the module will be mute and no prompt will be returned.

Conditional Self Tests

Conditional Self Tests are performed each time the associated functions are utilized.

Software load test, TDES MAC.
Continuous RNG tests will be performed on all of the implemented RNGs.
160-bit DRNG
32-bit NDRNG

Self-Test Failures

The module does not output an explicit indicator on the status of self-tests. The module indicates the failure of self-tests upon entry into an error state and no further APDU's are processed. The module remains mute.

13. Physical Security Policy

13.1 Protection against Physical Tampering

Module

The module structure is a flip-chip. The chip surface faces a circuit board. The module is protected by a hard removal and penetration resistant metal cover. Tamper evidence is apparent upon attempted removal of the cover or penetration of the module.

Memory Scrambling

The data bus between the CPU and the memory is scrambled as a countermeasure against physical probing attacks, such as reading and writing on the data bus.

The Data Bus consists of 4 buses, which are the CPU BUS, MEMORY BUS1, MEMORY BUS2, COPRO BUS. The CPU BUS connects the CPU and the Memory or the Peripheral Circuit Control Register. Through this CPU BUS, the CPU reads or writes data. A bus scrambling method is implemented on the CPU BUS between the CPU and the Memory (ROM, RAM and FLASH) as a countermeasure against the physical probing attacks of reading or writing data. MEMORY BUS1 and MEMORY BUS2 are also scrambled, storing the memory data in a scrambled format.

The COPRO BUS is between the Numeric Co-Processor and Memory (RAM) is isolated from the CPU BUS. This bus is implemented by the same scrambled method which is between the CPU and Memory. The data in Memory (RAM), is handled in a scrambled format.

The data bus for the FLASH Memory (NVRAM) and the data bus for the ROM and RAM is diverged in order to lower the power consumption and to be protected against physical probing attacks.

Shielding Layer with Wire Break-Down Sensor

The circuits are covered with a shielding layer, including Wire Break-Down Sensor. These signal lines are provided beneath a shielding layer that fully buries these signal lines, as a protection against probing attacks.

The Wire Break-Down sensor detects the break-down of the detection wiring located below the shielding layer of the chip. The BREAK WIRE ERROR signal becomes active when the detector wires are damaged. In response to this signal, the chip automatically enters the system reset state.

Flat Layout

The CPU, Numeric Co-Processor and other logical blocks are made in glue logic. Glue logic is irregular and the routing of glue logic is done in an unpredictable way, distributing all functions across the layout. The functional blocks are not grouped in the traditional CPU design style.

Narrow Wiring

The 0.18µm C-MOS process is used for this chip, so that the spaces between the wires are very narrow. The narrow wiring prevents an attacker from probing the wires.

Passivation

The surface of the chip is covered with a passivation layer. The passivation prevents an attacker from probing the circuits directly.

Security Fuse for Test Mode

The test modes on the chip are blocked and become invalid irreversibly.

13.2 Hardware Security Functions - Environmental Stress

Power-Up and Power-Down Reset

Power-Up and Power-Down Reset monitors the supply power from the input, either by contact plate or from the RF field input. If the supply power is adequate for the chip to correctly operate, Power-Up and Power-Down Reset releases the RESET state, allowing chip operation. Power supply variations outside allowed parameters will force a RESET state to the chip.

Voltage Sensors

Voltage Sensors monitor the internal voltage, and an error signal becomes active when the monitored voltage exceeds the upper limit value, or drops below the lower limit value. The chip will be forced into the system-reset state automatically, preventing an operation in unstable conditions.

Over-Voltage Protector

When the VCC voltage becomes excessive, an Over-voltage Protector absorbs the power to protect the chip.

Voltage regulator

The Voltage Regulator generates the internal voltages from RF field on the antenna contacts; and supplies them to other sub-systems.

Clock Frequency Sensors

Clock frequency sensors monitor the external and internal clock frequency. An error signal becomes active when the period of the high level or the low level of clock signal falls short of the specified value. In response to this signal, the chip automatically enters the system reset state. The sensors prevent operation in an unstable condition of clock.

Temperature Sensor

The temperature sensor monitors the chip temperature. An error signal becomes active when the chip temperature exceeds the upper limit value or falls below the expected lower limit value. In response to this signal, the chip automatically enters the system reset state.

13.3 Malfunction Detection

Odd Address Access Violation

When the address for accessing word data is an odd number, the chip generates a software reset automatically.

Illegal Instruction

When an undefined code is detected fetching the instruction code, the chip automatically generates a software reset.

13.4 Logical Tamper Protection

Memory Protection

A Memory Protection Circuit ensures the security of the module by setting a limitation to the memory space which can be accessed by an instantiated program, behaving like a firewall. The Memory Protection Circuit automatically generates internal software reset when unauthorized access is detected.

DES

The operation of the DES process is divided into several states. In one form of attack the state of the DES operation is guessed from the consumption current of a circuit, and there is a method for driving the DES key. In this countermeasure, every state of the DES operation is designed for a balanced consumption current so that all operation steps appear the same, thereby greatly increasing the level of difficulty to guess state of the DES operation.

RSA / ECC

The Numeric Co-Processor executes modular exponentiation using a square-and-multiply algorithm. The processing times of modular-square and modular-multiplication are designed to be equal. Modular-square and modular-multiplication use the same multiplier so that the difference of the power consumption between the two operations does not occur, blocking any outside observation capability.

The Numeric Co-Processor executes elliptic curve cryptosystem software operations using a double-and-add algorithm. The order of doubling and adding becomes constant, and does not depend on the value of a scalar coefficient (i.e. operand k). Therefore, the power consumption at the elliptic curve cryptosystem operation does not depend on the value of a scalar coefficient, blocking outside observation.

Random Number Generator (RNG)

This random number generator is the circuit to generate a deterministic random number; consisting of the 1 bit self-running random number generator, the M sequence generator and the 32-bit shift register. The random number generated can be used as the challenge data of the encryption key or the approval data.

Operator Required Actions

Upon receipt of the card, the issuer shall inspect the card for evidence of tamper for the contact pads and any other suspicious markings on the card itself.

14. Operator Guidance

The FIPS 140-2 required nonproprietary operator guidance are covered in this Security Policy document. This section describes a relationship between the FIPS 140-2 required operator guidance and a relevant section in this Security Policy document.

Crypto-Officer Guidance

The following table shows the FIPS 140-2 required guidance for Crypto officer and a relevant section in this Security Policy document.

Table 10 – Crypto officer Guidance

Required guidance	Relevant section
Administrative functions	Table 6 – Services authorized for Roles in Section 5. Identification and Authentication Policy
Security events	Section 5. Identification and Authentication Policy
Security parameters	"Definition of CSP Modes of Access" in section 7. Access Control Policy
Physical ports	"Physical Ports" in section 4. Ports and Interfaces
Logical interfaces	"Logical Interfaces" in section 4. Ports and Interfaces
Procedures on how to administer the cryptographic module in a secure manner	Section 10. Security Rules
Assumption of user behavior on secure operation	Operator Required Actions in Section 13 Physical Security Policy

User Guidance

The following table shows the FIPS 140-2 required guidance for User and a relevant section in this Security Policy document.

Table 11 – User Guidance

Required guidance	Relevant section
Approved security functions	Table 6 – Services authorized for Roles in Section 5.

	Identification and Authentication Policy
Physical ports	"Physical Ports" in section 4. Ports and Interfaces
Logical interfaces	"Logical Interfaces" in section 4. Ports and Interfaces

15. Mitigation of Other Attacks

The module has been designed to mitigate Differential Power Analysis (DPA), which is outside of the scope of FIPS 140-2.

In addition to the above passivation material, increased protection against physical attacks include:

- Low / high supply voltage sensor
- Low / high clock frequency sensor
- Low / high temperature sensor

* Unauthorized Memory Access Protection

Table 12 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
DPA protection	DES circuitry has built-in protection	Not Applicable

16. References

1. WECOS release 5, JCOP edition for Sharp, version 1.5; Hardware Abstraction Layer specification, April 2006.
2. Java Card TM 2.2.1 Virtual Machine Specification – June 2002, Sun Microsystems
3. Java Card TM 2.2.1 Application Programming Interface – revision 1.1- October 2003, Sun Microsystems
4. Java Card TM 2.2.1 Runtime Environment Specification - October 2003, Sun Microsystems
5. Global Platform 2.1.1 Card Implementation Requirements –May 2002, Visa International
6. Security Requirements for Cryptographic Modules, FIPS 140-2 National Institute of Standards and Technology..
7. Integrated circuit(s) cards with contacts - Part 2 Dimension and Location of the contacts. ISO/IEC 7816-2 (1999)
8. Integrated circuit(s) cards with contacts - Part 3 Electronic signal and transmission protocols. ISO/IEC 7816-3 (1997), ISO/IEC 7816-3 AMD1 (2002)
9. Integrated circuit(s) cards with contacts - Part 4: Inter industry commands for interchange. ISO/IEC 7816-4 (1995), ISO/IEC 7816-4 AMD1 (1997)
10. Numbering system and registration procedure for application identifiers. ISO/IEC 7816-5 (1994), ISO/IEC 7816-5 AMD1 (1996)
11. Information technology – Security techniques – Digital signature scheme giving message recovery - Part 2: Mechanism using a hash function. ISO/IEC 9796-2 (1997)
12. Information technology – Security techniques – Message Authentication Codes – Part 1: Mechanisms using a block cipher. ISO/IEC 9797-1 (1999)
13. Contactless integrated circuit(s) cards – Proximity cards — Part 2: Part 2: Radio frequency power and signal interface, ISO/IEC 14443-2 (2001)
14. Contactless integrated circuit(s) cards – Proximity cards — Part 3: Initialization and anti-collision, ISO/IEC 14443-3 (2001)
15. Contactless integrated circuit(s) cards – Proximity cards — Part 4: Part 4: Transmission protocol, ISO/IEC 14443-4 (2001)
16. "Integrated Circuit Card Specifications for Payment Systems" – EMV 2000
    a. Part 1: Electromechanical Characteristics, Logical Interface, and Transmission Protocols (version 3.0)
    b. Part 2: Data Elements and Commands (version 3.0)
    c. Part 3: Application Selection (version 3.0)
    d. Part 4: Security Aspects (Version 3.0)

17. Definitions and Acronyms

Acronyms

AES	Advanced Encryption Standard
AID	Application Identifier
AP	Application Provider
APDU	Application Protocol Data Unit
API	Application Programming Interface
ATR	Answer To Reset (contact mode)
ATS	Answer to Select (contactless mode)
API	Application Programming Interface
CBC	Cipher Block Chaining
CRC	Cyclic Redundancy Check
DAP	Data Authentication Pattern
DES	Data Encryption Standard
DPA	Differential Power Analysis
DM	Delegated Management
DRNG	Deterministic Random Number Generator
ECB	Electronic Code Book
ECSVDP	Elliptic Curve Secret Value Derivation Primitive
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
ICAO	International Civil Aviation Organization
ISO	International Standard Organization
JC	Java Card ™
JCRE	Java Card ™ Runtime Environment
MAC	Message Authentication Code
NDRNG	Non Deterministic Random Number Generator
OP	Open Platform
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
RAM	Random Access Memory
ROM	Read only Memory
RSA	Public key cryptographic algorithm invented by Rivest, Shamir and Adleman
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
TDES	Triple DES
TLV	Tag Length Value