ActivCard

MARTSOFT

Eagle 64K Flash Module v1

FIPS140-2 Level 2

Cryptographic Module Security Policy

Version 1.6

Table of Contents

1. INTRODUCTION

This document defines the Security Policy for the “Eagle 64K Flash Module V1”, submitted for validation, in accordance with FIPS140-2 Level 2 standard. Included are the description of the security requirements for the module and a qualitative description of how each security requirement is achieved. In particular, this security policy specifies the security rules under which the cryptographic module must operate.

2. OVERVIEW

Eagle 64K Flash Module V1 is based on Atmel Secure IC, MartSoft Global Platform Java Card OS and ActivCard Applet Suite. The module provides processing capability and memory for storing instructions and data.

When the module is placed in plastic smart card housing, it is ideal for secure identification, digital signature, storing and updating account information, personal data, and even monetary value, with increased security, portability and convenience to computer applications.

The Eagle 64K Flash Module V1 combines the advantages of the Java programming language and cryptographic services. The module security comes from both software and hardware. Data integrity and security are provided through cryptographic services, Java features, and the Operating System Software. In addition, the cryptographic module hardware provides a tamper-resistance and tamper-evidence features, that meets FIPS 140-2 Level 2 physical security requirements.

2.1 ATMEL SECURE IC AT90SC6464C

The AT90SC6464C is a low-power, high-performance secure microcontroller with Flash program memory, EEPROM data memory and a crypto-processor, based on the AVR RISC architecture. By executing powerful instructions in a single clock cycle, the AT90SC6464C achieves throughputs close to 1 MIPS per MHz. Its Harvrd architecture includes 32 general-purpose registers directly connected to the ALU, allowing two independent registers to be accessed in one single instruction executed in one clock cycle.

The AT90SC6464C uses a new AVR core (#3) that allows the linear addressing of up to 8 M bytes of code and up to 16 M bytes of data as well as a number new functional and security features. It includes 128K bytes of Atmel's high density, nonvolatile memory. The on-chip downloadable Flash allows the program memory to be reprogrammed in-system. This technology combined with the versatile AVR CPU on a monolithic chip provides a highly flexible and cost-effective solution to many smart card applications.

The crypto engine featured in the AT90SCC series is a 16-bit processor dedicated to perform fast encryption or authentication functions. Additional security features include power and frequency protection logic, logical scrambling on program data and addresses, Power Analysis countermeasures and memory access controlled by a supervisor mode, to mention a few.

2.2 MARTSOFT GLOBALPLATFORM JAVA CARD OS

MartSoft GlobalPlatform Java Card OS (MSGP) is developed on top of Atmel AT90SC6464C. MSGP loads and runs applets written in the Java Card programming language, and offers cryptographic functions to be used by Java Card applets.

MSGP v.09F7 is a Global Platform Java Card OS with SKI, PKI, and multiple security domains, which

provides a secure environment for multiple applications developed by multiple application providers. MSGP v.09F7 is fully compliant with Java Card 2.1.1 [JCAPI] and Open Platform Card Specification v2.0.1 [VOPS]. Each of the on-card cryptographic algorithms including random number generator, Triple-DES, SHA-1, and RSA has been individually validated for compliance with FIPS requirements [FIPS140-2A, FIPS140-2C].

Eagle Flash 64K Module V1 is considered operating in FIPS-approved mode if only the FIPS-validated applets are instantiated according to the security policy described in this document. Under this condition, the module always operates in FIPS-approved mode. The module checks all validated applets and will not load any applets that do not have the correct MAC. The Global Platform specification well defines card and applet life cycle states and state transitions. Once applets are loaded and the cryptographic module is initialized, off-card applications communicate with the applets on the Eagle 64K Flash Module V1 through a secure channel as defined in [VOPS], which is a secure communication pathway that can be established between off-card applications and on-card applications and the Card Manager.

2.3 ACTIVCARD APPLETS

ActivCard applet suite consists of the following applets:

- ID applet
- PKI applet
- GC applet

The ID applet offers Card Holder Verification (CHV) services to external applications.
The PKI Applet offers RSA based cryptographic services to external applications.
The GC Applet offers secure storage services to external applications.

There may be as many instances of each applet as there are available cryptographic module resources. There are dependencies between applet instances PKI ➔ GC ➔ ID. This means that a PKI instance requires a GC instance and an ID instance to operate. On the other hand, an ID instance can be present alone on the cryptographic module.

Those applets are included within the cryptographic boundary of the module, and they provide cryptographic services for the host applications. They are therefore subject to validation.

The document further refers to any of these three applets by ‘the applet’(s).

3. SECURITY LEVEL

The Eagle 64K Flash Module V1 is designed and implemented to meet the Level 2 requirements of FIPS140-2. The cryptographic module enforces FIPS mode of operation at all time. The individual security requirements specified for FIPS 140-2 meet the level specifications indicated in the following table.

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2

Self Tests	2
Design Assurance	2
Mitigation of other attacks	2

4. CRYPTOGRAPHIC MODULE SPECIFICATION

The Eagle 64K Flash Module V1 supports role based authentication of card holder, application operators and cryptographic officers using PIN or TDES keys. All services provided by the cryptographic module are protected by role based access control policy following the result of the authentication.

This validation effort will be aimed at the systems software, virtual machine, Card Manager application, and ActivCard applets. If additional applets are added to this card, then these additional applets will need to go through a separate validation and will need to be FIPS 140-2 validated. If non-validated applets are loaded onto the module at post-issuance, the module is considered operating in non-FIPS mode.

The Eagle 64K Flash Module V1 adheres to the various ISO/IEC specifications for Integrated Circuit Chip (ICC) based identification cards. The “cryptographic boundary” for the Eagle 64K Flash Module V1 vis-à-vis the FIPS 140-2 validation is the “module edge”. The module is comprised of the chip (ICC), the contact faceplate, and the micro-electronic connectors between the chip and contact pad.

The Eagle 64K Flash Module V1 is a single chip implementation of a cryptographic module. The Eagle 64K Flash Module V1 chip is comprised of the following elements:

- ATMEL AT90SC6464C, 8/16 bit RISC micro controller. System software is installed in OTP Flash Memory as part of the chip manufacturing process (known as hard mask) and in Electrically Erasable, Programmable Read Only Memory (EEPROM) for system options and additional customized software (known as soft mask). The software is then designated: Hard Mask Global Platform and Java OS version 09F7, Soft Mask Global Platform and Java OS version 09F7. Note that in the smart card world, Hard Mask refers to software stored in ROM or Flash; in other guises, this might be referred to as “firmware”. These hard mask and soft mask identification numbers are returned in the Answer To Reset (ATR) character string following the issuing of a RESET signal to the cryptographic module.

- Critical Security Parameters stored in EEPROM as part of the card personalization operation.

- The ActivCard applets are composed of the following elements:
  - ID applet package version 1.0.0.14
  - PKI applet package version 1.0.0.14
  - GC applet package version 1.0.0.20

The applet package byte code is loaded in the card memory.

The applets offer services to off-card applications, and rely on key management, secure memory management and cryptographic services provided by the cryptographic module.

The services are activated with “APDU commands” sent to the cryptographic module.

Applets depend on a unique Security Domain for the security configuration. This Security Domain can either be the Card Manager or a separate security domain instance.

The Card Manager is itself a Security Domain with additional services to load, install applets and controls the global card status.

The funictional block diagram of the module firmware is shown in Figure 1.

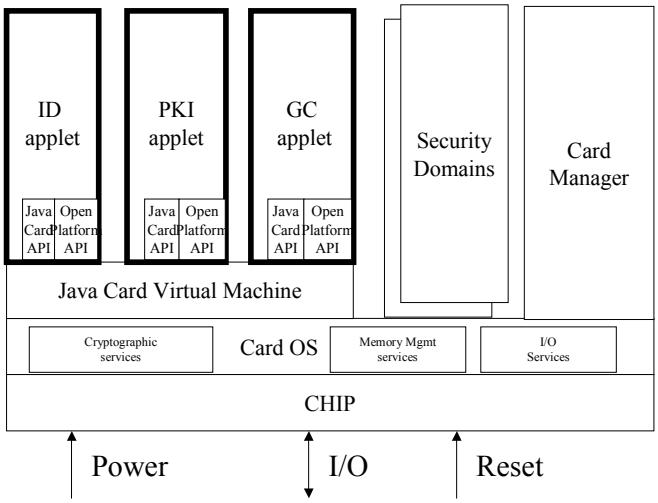


Figure 1: Functional block diagram

Every security domain holds one or more security domain key sets composed of TDES keys. The ownership of a key set allows for establishing a Global Platform Secure Channel (SC) between the host and the security domain. The SC is generally used for administrative operations such as entering the application keys in the applets instances belonging to the security domain, or entering new key sets in the security domain itself. Note that a security domain key set can be used to enter a replacement key set in the same security domain – the replacement involves the deletion of the original key set. This is how an Applet Security Controller role (ASC), which solely owns the replacement key set, can take control of the personalization of all applet instances belonging to a security domain.

Cryptographic keys ownership and their distribution to security domains and the applet instances are illustrated in Figure 2.

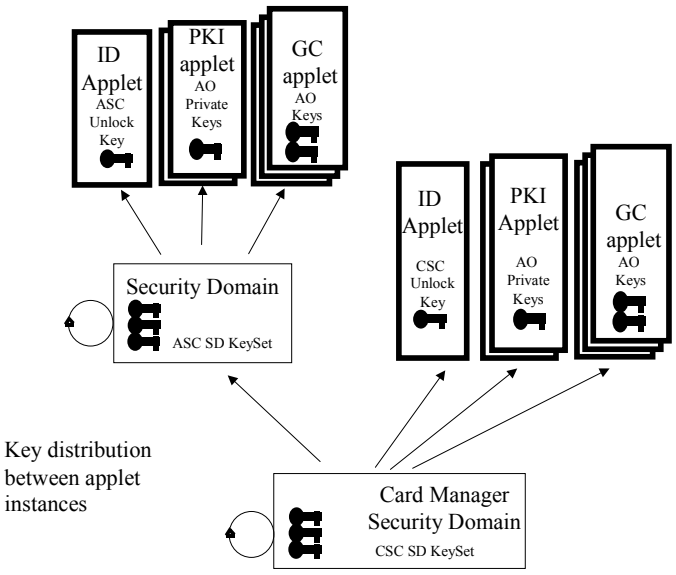


Figure 2: Key Distribution – Role separation

4.1 MODULE INTERFACES

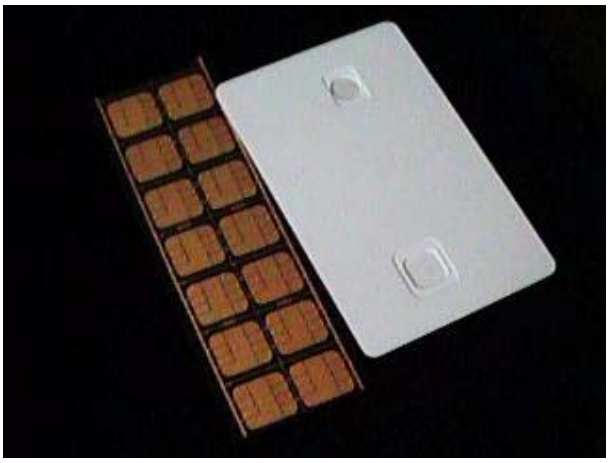
The electrical and physical interface of the Eagle 64K Flash Module V1 is comprised of the 8-electrical contacts from the face of the cryptographic module to the chip. These contacts conform to the following specifications.

4.1.1 Physical Interface description

The Eagle 64K Flash Module V1 supports eight contacts that lead to pins on the chip. Only five of these are used. The location of the contacts complies with ISO/IEC 7816-2 standard. Minimum contact surface area is 1.7mm * 2.0 mm. Contact dimensions are standard credit card compliant as per ISO/IEC 7816-1 standard:

Dimension	Value
Length	85.5mm
Width	54.0mm
Thickness	0.80mm

The Eagle 64K Flash Module V1 and the card before the module is embedded are shown next.



4.1.2 Electrical specifications

4.1.2.1 Specific electrical functions of the contacts:

Contact	Function
C1	Vcc supply voltage 3 to 5V +/- 0.5V
C2	RST (Reset)
C3	CLK (Clock)
C4	Reserved for Future Use (RFU)*
C5	GND (Ground)
C6	Not used*
C7	I/O bi-directional line
C8	Reserved for Future Use (RFU)*

* The contacts whose functions are “Not used” or “RFU”, are not connected to the module.

4.1.2.2 ICC supply current:

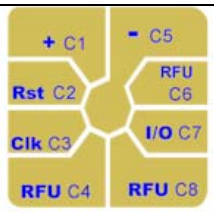
Maximum value: 10 mA at 5MHz (3mA type), short time peak value according to ISO 7816-3.

The communication between the card reader and the Eagle 64K Flash Module is based on a standardized, half-duplex character transmission, ISO 7816 protocol.

Both protocols T=0 and T=1 are supported.

4.1.3 Logical Interface Description

The logical interface and their physical location are shown below.

	Data Input: C7 Data Output: C7 Status Output: C7 Control Input: C2, C3, and C7 Power Input: C1 and C5

Once electrical (physical) contact and data link layer contact is established between the cryptographic module and the card reader, the cryptographic module functions as a “slave” processor to implement and respond to the card reader commands. The cryptographic module adheres to a well-defined set of state transitions. Within each state, a specific set of commands is accessible.

The details of these commands are listed hereafter.

5. ROLES & SERVICES

5.1.1 Roles

The Eagle 64K Flash Module V1 defines four distinct roles that are supported by the on-module cryptographic system: Card Security Controller (CSC) role, Applet Security Controller (ASC) role, Application Operator (AO) role, and Card Holder (CH) role.

5.1.1.1 User Roles:

- **Card Holder (CH) Role** - The Card Holder role is responsible for insuring the ownership of his cryptographic module and for not communicating his PIN to other entities. An applet authenticates the Card Holder by verifying his PIN.
- **Application Operator (AO) Role** – The Application Operator role represents an external application requesting the services offered by the applets. An applet authenticates the Application Operator role by verifying the possession of an Application External Authentication (XAUT) key.

5.1.1.2 Cryptographic Officers roles:

- **Card Security Controller (CSC) Role:** This role is responsible for managing the security configuration of the card manager and security domains. The CSC role authenticates to the cryptographic module by demonstrating to the card manager application that he possesses the knowledge of a TDES key set stored within the card manager. By successfully executing the Global Platform Secure Channel mutual authentication protocol [VOPS], the CSC role establishes a secure channel to the card manager. Once authenticated, off card applications are authorized to access information and services that are provided by the card manager and security domain.
- **Applet Security Controller (ASC) Role:** This role is responsible for managing the security configuration of the applets. The ASC role authenticates to the cryptographic module by demonstrating to the Applet security domain that he possesses the knowledge of a TDES key set stored within the security domain. The ASC role can also unblock a previously blocked PIN service by proving the possession of the Unblock PIN External Authentication (XAUT) key. Note that the protection of the PIN unblock service by Unblock PIN External Authentication (XAUT) key is optional, as the PIN unblock service is always accessible with the ID applet security domain key set.

5.1.2 Role Authentication

The Eagle 64K Flash Module V1 supports role-based authentication.

5.1.2.1 User Role Authentication

- The card holder role is authenticated with PIN or PIN Always
  - **PIN**: The Card Holder role must send a Verify CHV command to any ActivCard applet to access any applet service protected with PIN. The APDU command corresponding to the applet service protected by PIN can access the service before the cryptographic module is removed or a reset signal is sent to the cryptographic module.

- **PIN Always**: The Card Holder role must send a Verify CHV command to any ActivCard applet to access any applet service protected with PIN Always. The APDU corresponding to the applet service must be sent immediately after the PIN has been verified.

- The Application Operator role is authenticated by the possession of the following key.
  - **Application External Authentication (XAUT) key**: The Application Operator role must prove the possession of a particular TDES key by executing the AC External Authentication protocol to access the GC Applet read or update service with this particular key: A 8-byte challenge is first obtained from the applet. The Application controlled by the operator encrypts the challenge with a 112-bit TDES key, and submits the resulting cryptogram for verification. The APDU corresponding to the particular applet service must be sent before the cryptographic module is removed or a reset order is send to the cryptographic module.

5.1.2.2 Cryptographic Officer Role Authentication

- The Cryptographic Officer role is authenticated by using a TDES key or a TDES key set.
  - **Crypto Officer Security Domain key set:** The Cryptographic Officer (CSC or ASC) role must prove the possession of a key set composed of 3 TDES keys. Two keys (K_{MAC}, K_{ENC}) are used to derive session keys according to Global Platform specification described in [VOPS]. The session keys ensure the confidentiality of the command payload, allow the mutual authentication of the parties and protect the APDU command integrity. A third key (K_{KEK}) is used to encrypt keys transported within the APDU command. The mutual authentication protocol is a two-pass protocol. In the first pass (Initialize Update), a host challenge is generated and sent to the security domain application. The security domain application responds with a card challenge and a cryptogram generated over the host and card challenge. In the second pass (External Authenticate), the host verifies the card cryptogram and sends to the security domain application a host cryptogram generated over the card and host challenge. The card finally verifies the host cryptogram and concludes the mutual authentication successfully.
  - **Unblock PIN External Authentication (XAUT) key**: The Cryptographic Officer (ASC) role must prove the possession of this TDES key (K_{XAUT}) by executing the AC External Authentication protocol to access the ID Applet PIN Unblock service. The host application controlled by the Cryptographic Officer role encrypts an 8 byte Card challenge with K_{XAUT}, and submits a PIN Unblock APDU including the resulting cryptogram for verification to the cryptographic module. The AC External Authentication protocol is a two-pass one-way authentication protocol. In the first pass (Get Challenge), the host gets the card challenge, generates the host cryptogram over the card challenge, and returns the host cryptogram in the second pass (AC External Authenticate). The card responds the successful status if the cryptogram is verified by the card application.

5.1.3 Services

5.1.3.1 Crypto Officer Role Administrative Services

5.1.3.1.1 Card Platform Administrative Services

One command set is supported by the CSC, and is used only by the CSC to allow for the administration of the Security Domains and to load applets onto the cryptographic module. This command set includes the following commands:

- **INSTALL (CSC):** This command is used to instruct a Security Domain or the Card Manager as to which installation/instantiation step it shall perform during an Applet installation process.
- **LOAD (CSC):** This command is used to load the byte-codes of the Load File (package) defined in the previously issued INSTALL command.
- **DELETE (CSC):** This command is used by the CSC role to delete a Load File (package) or an applet instance.
- **PUT KEY (CSC & ASC):** This command is used to add or replace Security Domain key sets.

5.1.3.1.2 Applet Administrative Services

All services below are accessible by ASC role.

Common Administrative Services

The following services are provided by all instances of ID, GC and PKI applets.

- **INITIALIZE UPDATE.** This command corresponds to the OP secure channel specification. It is used to mutually authenticate with the Cryptographic Officer and derive the session keys.
- **EXTERNAL AUTHENTICATE**. This command corresponds to the OP secure channel specification. It is used to mutually authenticate with the Cryptographic Officer and derive the session keys for the secure channel.

ID Applet Administrative Services

The ID applet provides Card Holder Verification (CHV) services. Here are the different commands / services that are provided by an ID applet instance:

- **UNBLOCK PIN**. This command is a parameterized **CHANGE PIN/UNBLOCK** command. All PIN-protected services of all applet instances that are attached to a particular ID instance are not accessible to the Card Holder when successive PIN verifications for that ID instance fail. These applets are then in “PIN blocked” state. This command is used to set a new PIN value and recover Card Holder access when used within a secure channel of the ASC or through the AC External Authentication using Unblock PIN External Authentication (XAUT) key.
- **CHANGE PIN.** This command is a parameterized **CHANGE PIN/UNBLOCK** command. If the PIN applet is not blocked, and the command is used outside a secure channel, this command is used to set a new PIN value if the current PIN can be presented by the card holder.
- **PUT KEY**. This command is used to enter the Unblock PIN External Authentication (XAUT) key, and must be used within a secure channel. The APDU format is compliant with Global Platform specification [VOPS].
- **GET CHALLENGE**. This command is used in combination with AC External Authenticate to perform an external authentication of the Application Operator in order to unblock the PIN.
- **UNBLOCK PIN AC EXTERNAL AUTHENTICATE**. This command is used in combination with a Get Challenge; this command is used to unblock the PIN by presenting a cryptogram produced by TDES encryption of the challenge with the Unblock PIN External Authentication (XAUT) key (see put key). It also provides the ID applet instance with the new PIN value.
- **CHANGE PIN AFTER FIRST USE**. This command indicates that the Card Holder must change his PIN before any PIN protected service can be accessed.

PKI Applet Administrative Services

The PKI Applet provides RSA-based cryptographic services. There is one RSA private key for each PKI applet instance. The corresponding certificate is located in the attached GC instance.
Here are the different commands / services that are provided by a PKI applet instance:

- **GENERATE KEY PAIR**. This command is used to generate a RSA Key Pair in the cryptographic module. The Private Key is associated to a PKI applet instance.
- **PUT KEY**. This command is used to import/unwrap the private key (Chinese Remainder Theorem) components. The command format follows OP specification. There is a unique private key for each PKI applet instance.

GC Applet Administrative Services

The Generic Container Applet provides secure storage services. Each GC applet instance corresponds to one storage area consisting of two buffers: one buffer contains the TAGs and Lengths of stored data elements, and the other buffer contains the values of each data element.
Here are the different commands / Services that are provided by a GC applet instance:

- **PUT KEY**. This command imports/unwraps the TDES Application External Authentication (XAUT) keys. The APDU format follows the Global Platform specification [VOPS]. There are three XAUT keys for each GC Applet instance: read Tag+Length Buffer key, read Value Buffer key, and update any buffer key.

5.1.3.2 User services

5.1.3.2.1 Card Platform Services

The card platform services are:

- **GET DATA**: This command is used to retrieve a single data object.
- **GET STATUS**: This command is used to retrieve Card Manager information according to a given search criteria if the Card Manager is the current application.
- **GET RESPONSE**: This command is restricted to T = 0 ISO protocol for an incoming command which have data to send back. That data is received with the GET RESPONSE command sent immediately after the command it is related to.
- **PUT DATA**: This command is used to store or replace one tagged data object provided in the command data field.
- **SELECT**: This command is used for selecting an application (Card Manager, Security Domain or Applet). The Card Manager may be selected either for the loading of a Load File or for installing a previously loaded application (or Security Domain).

5.1.3.2.2 Applet User Services

Common User Services

The following commands/services are common to all instances of GC, ID and PKI applets:

- **SELECT**: This command causes the selection of the applet. The select() method of the applet instance is called.
- **GET PROPERTIES**. This command is used to obtain information about applet instance configuration.
- **VERIFY CHV**. This command checks the PIN presented by the Card Holder against the current PIN associated with the ID applet instance.

ID Applet User Services

The ID applet provides Card Holder Verification (CHV) services. All ID applet user services are described in the Common User Services section above.

PKI Applet User Services

The PKI Applet provides RSA-based cryptographic services. There is one RSA private key for each PKI applet instance. The corresponding certificate is located in the attached GC instance.
Here are the different commands / Services that are provided by a PKI applet instance:

- **GET CERTIFICATE**. This command is used to obtain the certificate corresponding to the PKI applet instance private key. The certificate is located in the GC instance that is attached to the PKI applet instance.
- **SIGN**. This command uses the RSA private key in the applet instance to sign data.

GC Applet User Services

The GC Applet provides secure storage services. Each GC applet instance corresponds to one storage area consisting of two buffers: one buffer contains the TAGs and Lengths of stored data elements, and the other buffer contains the values of each data element.
Here are the different commands / Services that are provided by a PKI applet instance:

- **UPDATE BUFFER**. This command is used to write or modify data elements in storage area. There is no CSP stored in these buffers.
- **READ BUFFER**. This command is used to read data elements from storage area. There is no CSP stored in these buffers.
- **GET CHALLENGE**. This command is used in combination with AC External Authenticate to perform an external authentication.
- **AC EXTERNAL AUTHENTICATE**. This command communicates the cryptogram obtained by TDES encryption of a card challenge with the TDES key associated to the service – read or update buffer – by executing the AC External Authentication protocol.

5.1.3.3 Relationship between Roles & Services: Card Platform

Roles/Services	CSC role (Card Manager Security Domain)	No role (Unauthenticated)
INSTALL	X	
LOAD	X	
DELETE	X	
EXTERNAL AUTHENTICATE	X	
GET DATA	X	X
GET STATUS	X	X
GET RESPONSE	X	X
INITIALISE UPDATE		X
PUT DATA	X	
PUT KEY	X	
SELECT		X
SET STATUS	X	

Table 1: Role and possible ACR configuration for Card Manager

5.1.3.4 Relationship between Roles & Services: Applets

5.1.3.4.1 Access Control Rules

Each applet service is associated with a role-based Access Control Rule that also indicates the allowed role for that service, as detailed in the previous section.
The Access Control Rule may be configurable or fixed depending on the Applet service. Each applet instance may be configured independently. Once set, the ACR cannot be deleted or modified for the applet instance lifetime.
The applet services are invoked by external APDU commands sent to the cryptographic module. The ACRs are applied on the APDU commands.
All services are specified in the respective Applet Specification documents.

5.1.3.4.2 Roles vs. Services: ID Applet

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC/ASC) / SECURE CHANNEL or XAUT (unblock PIN only)	Application Operator / XAUT	Card Holder / PIN
ID Applet				
INSTALL		X		
CHANGE PIN				X
UNBLOCK		X		
GET PROPERTIES	X			
INITIALIZE UPDATE	X			
EXTERNAL AUTHENTICATE		X		
VERIFY CHV				X
PUT KEY		X		
GET CHALLENGE	X			
AC EXTERNAL AUTHENTICATE		X		
CHANGE PIN AFTER FIRST USE				X

Table 2. Roles & possible ACR configuration for ID applet services

5.1.3.4.3 Roles vs. Services: GC Applet

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC/ASC) / SECURE CHANNEL	Card Holder / PIN	Card Holder / PIN ALWAYS	Application Operator / XAUT	A.O. or C.H. / XAUT or PIN	A.O. and C.H /. XAUT then PIN
GC Applet							
INSTALL		X					
GET PROPERTIES	X						
INITIALIZE UPDATE	X						
EXTERNAL AUTHENTICATE		X					
UPDATE BUFFER	X	X	X	X	X	X	X
READ BUFFER	X	X	X	X	X	X	X
GET CHALLENGE	X						
PUT KEY		X					
AC EXTERNAL AUTHENTICATE					X	X	X
VERIFY CHV			X	X			

Table 3. Roles & possible ACR configuration for GC applet services

5.1.3.4.4 Roles vs. Services: PKI Applet

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC/ASC) / SECURE CHANNEL	Card Holder / PIN	Card holder / PIN ALWAYS
PKI Applet				
INSTALL		X		
GET PROPERTIES	X			
INITIALIZE UPDATE	X			
EXTERNAL AUTHENTICATE		X		
GENERATE KEY PAIR		X	X	
GET CERTIFICATE	X		X	X
SIGN			X	X
VERIFY CHV			X	X
PUT KEY		X		

Table 4. Roles & possible ACR configuration for PKI applet services

5.1.3.5 Module Cryptographic Functions

The purpose of the Eagle 64K Flash Module V1 is to provide cryptographic services to end-user applications. The keys represent the roles involved in controlling the cryptographic module. A variety of algorithms are used in the Eagle 64K Flash Module V1 to provide cryptographic services; these include:

- TDES (2 keys TDES)
- TDES MAC (2 keys TDES)
- SHA-1
- RSA PKCS1 (512, 768, 1024 bit keys)

The TDES (CBC mode) algorithm is used both for authenticating the Crypto Officer (EXTERNAL AUTH command) and is used for encrypting data flow from the external application to the cryptographic module environment. The responses are not encrypted; i.e. the status words returned in response to an APDU are not encrypted. TDES, RSA and SHA-1 algorithms are provided as services through Java APIs to applets that may be loaded onto the cryptographic module.

5.1.3.6 RNG

The Eagle 64K Flash Module V1 offers the services of a FIPS approved DRNG using ANSI X9.31 standard.

5.1.3.7 Self Tests

5.1.3.7.1 Power Up Self Tests

The Eagle 64K Flash Module V1 performs the required set of self-tests at power-up time. When the Eagle 64K Flash Module V1 is inserted into a smart card reader, once power is applied to the card (contact) interface, a “Reset” signal is sent from the reader to the card. The card then performs a series of GO/NO-GO tests before it responds (as specified by ISO/IEC 7816) with an Answer To Reset (ATR) packet of information. These tests include:

- Integrity test
  - Card OS (Flash-emulated ROM and EEPROM) integrity check

- Applet Package (EEPROM) integrity check
- Algorithm (known answer) tests
  - TDES (ECB/CBC mode encrypt/decrypt),
  - RSA PKCS1 (sign/verify)
  - SHA-1
  - X9.31 DRNG

If any of these tests fail, the card will go mute until the next power up.

5.1.3.7.2 Conditional Tests

RSA Key generation:

- A pair wise consistency check is performed during key generation including CRT and non-CRT.

Random Number Generator:

- NDRNG: a 8-byte continuous test is performed during each use of the Hardware non-deterministic RNG. The NDRNG is used to generate seed values to feed the DRNG.

- DRNG: a 8-byte continuous testing is performed during each use of the FIPS140-2 approved deterministic RNG.

Software/Firmware load test

- A TDES CBC MAC is verified each time an applet is loaded onto the card.

If any of these tests fail, the card will return a security condition error then go mute until the next power up.

5.1.4 Critical Security Parameters

5.1.4.1 Cryptographic Keys :

The Eagle 64K Flash Module V1 includes the following keys:

- **Initialization Key** K_{init} (TDES, double length), used only for the first Card Manager key-set loading,
- **Crypto Officer Security Domain key set**. A Security Domain key set is structured in such a way as to contain three types of TDES keys:
  - $K_{enc,auth}$ used to derive session keys for Crypto Officer authentication and encrypted mode of the secure channel,
  - K_{mac}, used to derive session key for MAC mode of the secure channel,
  - K_{kek} used to encrypt keys, to be imported into the platform.
- **TDES Session keys** (keys derived from Crypto Officer keys set $K_{enc,auth}$ and K_{mac})
- **Application External Authentication (XAUT) Keys**: These are TDES keys that enable the authentication of Application Operators (Read Buffer /Update Buffer)
- **Unblock PIN External Authentication (XAUT) Key:** These are TDES keys that enable Applet Security Controller to perform the PIN Unblock operation.
- **RSA private keys**: These keys are managed (generated, unwrapped) from the PKI applet using the java card cryptographic services. These keys are used to sign data.

5.1.4.2 List of Applets CSPs

The following Critical Security Parameters (CSPs) are managed from the applets:

- **Personal Identification Numbers or passwords (PIN)**: PINs and PIN attributes are managed from the ID applet, which relies on the Java Card PIN management service.

5.1.5 RSA Public Key

RSA public keys are managed in the Eagle 64K Flash Module V1 as follows:

- When RSA key pair is generated on the module, the RSA public key is exported as response to the RSA key generation command, and is not stored on the module.
- When RSA key pair is not generated on the module, only the private key is imported into the module. The corresponding RSA public key is not imported.

5.2 ACCESS TO CSPS VS SERVICES

The following Matrix shows for each applet how services access CSPs.

5.2.1 ID Applet

ID applet Columns: Services(roles) Rows: Access to CSPs	**Card Holder**	**Cryptographic Officer**	INSTALL-instantiate (CSC)	CHANGE PIN (CH)	UNBLOCK PIN (ASC)	GET PROPERTIES(No role)	INITIALIZE UPDATE(No role)	EXTERNAL AUTHENTICATE(ASC)	VERIFY CHV(CH)	PUT KEY(ASC)	GET CHALLENGE(No role)	AC EXTERNAL AUTHENTICATE(ASC)
PIN												
Change PIN	X			X								
Unblock PIN		X			X							
Verify CHV	X								X			
Unblock PIN External Authentication (XAUT) Key												
Delete key		X								X		
Enter key		X								X		
Verify cryptogram		X			X							X
Card Manager Key set												
Verify Cryptogram		X			X			X		X		
Decrypt data		X	X		X			X		X		

5.2.2 PKI Applet

PKI applet services Columns: Services (roles) Rows: Access to CSPs	***Card Holder***	***Cryptographic Officer***	INSTALL instantiate (CSC)	GET PROPERTIES (No role)	INITIALIZE UPDATE(No role)	EXTERNAL AUTHENTICATE(ASC)	GENERATE KEY PAIR (ASCor CH)	GET CERTIFICATE(No role)	SIGN(C.H)	VERIFY CHV(C.H)	PUT KEY(ASC)
PIN or Password											
Verify CHV	X									X	
RSA Key Pair											
Generate Key Pair	X	X					X				
Enter CRT components		X									X
Delete private key		X									X
Sign data	X								X		
Card Manager Key set											
Verify Cryptogram		X				X					X
Decrypt Data		X	X			X					X

5.2.3 GC Applet

GC applet services Columns: Services (roles) Rows: Access to CSPs	**Card Holder**	**Cryptographic Officer**	**Application Operator**	INSTALL (Instantiate) (CSC)	GET PROPERTIES (No role)	INITIALIZE UPDATE (No role)	EXTERNAL AUTHENTICATE (ASC)	UPDATE BUFFER (ASC or AO or CH)	READ BUFFER (ASC or AO or CH)	GET CHALLENGE (No role)	PUT KEY (ASC)	AC EXTERNAL AUTHENT(A0)	VERIFY CHV (CH)
PIN or Password													
Verify CHV	X												X
Application External Authentication (XAUT) Keys													
Delete key		X									X		
Enter key		X									X		
Verify cryptogram			X									X	
Card Manager Key set													
Verify Cryptogram		X					X						
Decrypt Data		X		X				X	X		X		

6. SECURITY RULES

6.1.1 Approved Mode of Operation

To maintain the module in an approved mode of operation, the operator must restrict the usage of the module as follows:

- Module service access control rules must be configured per tables 1, 2, 3, and 4 in section 5.1.3.
- follow all security rules below.

6.1.2 Role Based Authentication Security Rules

The module implements specific methods for authenticating the different roles. The implementation consists of the binding of a role-based Access Control Rule to each service.

- The module shall provide the following distinct operator roles: The Card Holder role, Application Operator role, Applet Security Controller role and Card Security Controller role.
- The applets shall provide role-based authentication:
  - The card holder role is authenticated by the possession of a PIN.
  - The Card Security Controller role and Applet Security Controller roles are authenticated by proving the possession of a key set composed of 3 TDES keys. Two keys are used to authenticate the command payload. A third key is used to encrypt keys transported within the APDU command (Initialize Update & External Authenticate commands).

    - When performing PIN Unblock services the Applet Security Controller role is authenticated by proving the possession of the Unblock PIN External Authentication (XAUT) TDES key.
- Cryptographic services are restricted to authenticated roles.
- The Role authentication methods or Access Control Rule (ACRs) for each applet service are set by the Cryptographic officer during Applet instantiation and cannot be modified during the lifetime of the ID applet instance.
- When authentication of the role cannot be performed because the related key or password or key attributes are missing, the corresponding service must be disabled.
- The results of authentication must be set in transient memory and therefore cleared when the module is powered down.
- The applet instance configuration may require the combined authentication of different roles to access a particular service. For instance the application operator and then the card holder must both authenticate themselves to access the Update Buffer service.
- The Card Holder can access services requiring Application Operator authentication after the Application Operator has been authenticated successfully.
- The Application Operator can access services requiring Card Holder authentication by PIN after the Card Holder has been authenticated successfully. This rule is not applicable for services requiring Card Holder authentication with PIN ALWAYS.

6.1.3 Applet Life Cycle Security Rules

The Eagle 64K Flash Module V1 allows only loading of FIPS approved applets. Applets can only be loaded through the Global Platform secure channel; i.e. they pass from the external application to the cryptographic module in an encrypted and MACed form.

- The Card Holder must take the necessary measures to insure that the terminal and/or the Card Acceptance Device are controlled by a valid role: Card Holder, application operator or Cryptographic Officer / crypto-officer.
- The management of the life cycle of the applets – load, install, delete, personalize keys, shall follow the Open Platform standard as described in [VOPS].
- Applets management and key management APDU commands (such as download, install, delete, put key) are protected by Global Platform secure channel MAC (TDES-CBC). They have their origin authenticated and their integrity verified. In particular this protects the applet byte code against tampering when downloaded at post issuance.
- The download of validated applets packages and the installation of applet instances may either occur at pre-issuance, issuance or post-issuance.
- There may be as many instances of each applet as there are available cryptographic module resources.

6.1.4 Access Control Security Rules

- Keys must be loaded through a secure channel. Consequently, keys are always loaded in the encrypted form.
- The PIN that is used by the applet to authenticate the Card Holder must not be divulged to other parties than the Card Holder.
- The ID applet must be configured by the cryptographic officer so that:
    - After 1 <= N <= 255 consecutive unsuccessful PIN code validation attempts, the Card Holder services must be disabled. (eg. The PIN is blocked)
    - The PIN length L verifies the following rules:
        - 6 <= L <= 255 for PIN composed with random numeric (0-9) or alpha-numeric (0-9, a - z, A – Z) characters

- If separation of roles between the Card Holder and Cryptographic officer is required for a particular service, such as the RSA Signature service the PIN always ACR must be selected.
- Access control rules for services are either set permanently or configured through applet instance installation parameters. For configurable services, the access control rule should be set according to the tables in section 5.1.3.4.

6.1.5 Physical Security Rules

The physical security of the Eagle 64K Flash Module V1 is designed to meet FIPS 140-2 level 2 requirements. A hard opaque epoxy is used to encapsulate the module to meet level 2 requirements. From the time of its manufacture, the cryptographic module is in possession of the Cryptographic Officer until it is ultimately issued to the end user.

6.1.6 Key Management Security Policy

6.1.6.1 Cryptographic key generation

-The random nonce used for the Global Platform secure channel TDES session key derivation is generated using FIPS140-2 approved ANSI X9.31 DRNG for Global Platform secure channel establishment.

- RSA key pair generation using FIPS140-2 approved ANSI X9.31 DRNG.

6.1.6.2 Cryptographic key entry

Keys shall always be input in encrypted format, using the Put Key command within a secure channel. During this process, the keys are double encrypted (using the Session Key and the K_{kek} Key).

6.1.6.3 Cryptographic key storage

The Keys are structured to contain the following parameters:

- Key id, which is the Id of the key,
- Algo Id, which determines which algorithm to be used,
- Integrity Mechanisms.

6.1.6.4 *Cryptographic key zerorization*

The cryptographic module destroys cryptographic keys by reloading a zero value key-set for security domains key set, application external authentication (XAUT) keys, unblock PIN external authentication (XAUT) key, or by closing of secure channel for session keys**.**
Key management details can be found in a specific proprietary document.

6.1.6.5 Card Holder PIN zerorization

The Card Holder PIN is zerorized by setting a zero PIN value.

6.1.7 Mitigation of attacks Security Policy

Eagle 64K Flash Module V1 has been designed to mitigate the following attacks:

- Simple Power Analysis,
- Differential Power Analysis.

7. SECURITY POLICY CHECK LIST TABLES

7.1 ROLES & REQUIRED AUTHENTICATION

Role	Type of authentication	Authentication data
Card Security Controller	Global Platform mutual authentication secure channel protocol	Card Manager Global Platform TDES key set
Applet Security Controller	Global Platform mutual authentication secure channel protocol, or AC External Authenticate challenge response protocol	Security Domain Global Platform TDES key set, or Unblock PIN External Authenticate (XAUT) key
Application Operator	AC External Authenticate challenge response protocol	Application External Authentication (XAUT) keys
Card Holder	Verify CHV	PIN

7.2 STRENGTH OF AUTHENTICATION MECHANISMS

Authentication Mechanism	Strength of Mechanism
TDES authentication	> 1 : 1,000,000
PIN	> 1 : 1,000,000

7.3 SERVICES AUTHORIZED FOR ROLES

Role	Authorized Services
Card Security Controller	The Card Security Controller services are listed in Section 5.1.3.1.1
Applet Security Controller	The Applet Security Controller services are listed in Section 5.1.3.1.2
Application Operator	The Application Operator Services are listed in Section 5.1.3.2.1
Card Holder	The card holder services are listed in Section 5.1.3.2.2

7.4 ACCESS RIGHTS WITHIN SERVICES

Service	CSP	Types of Access (eg. Read, Write, Execute)
Crypto Officer (CSC/ASC) Service	TDES Crypto Officer Keys	Execute (encrypt, decrypt), write (put key)
Application Operator Service	TDES Application Operator Keys	Execute (encrypt, decrypt)
Card Holder Service	PIN	Execute (Verify CHV), write (Change PIN)

7.5 MITIGATION OF OTHER ATTACKS

Other Attacks	Mitigation Mechanism	Specific Limitations
Simple Power Analysis	Dummy instruction and multi-path methods	N/A
Differential Power Analysis	Dummy instruction and multi-path methods	N/A
Voltage and frequency based attack	Voltage monitor sensor and frequency monitor sensors are enabled. If the voltage or frequency violates the designated range, the chip will be reset. These are active counter measures.	N/A

8. REFERENCES

[JVM] Java Card ™ 2.1 Virtual Machine Specification v1.1 - june 1999, Sun Microsystems
[JCAPI] Java Card ™ 2.1 Application Programming Interface, Sun Microsystems
[JCDG] Java Card ™applet developer's guide
[JCRE] Java Card ™ 2.1 Runtime Environment (JCRE) Specification, Sun Microsystems
[VOPS] Global Platform - Open Platform Card Specification, v2.0.1' – April 2000
[VOPI] Visa Open Platform Card Implementation Specification - march 1999, Visa International
[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.
[FIPS140-2] National Institute of Standards and Technology, FIPS 140-2 standard.
[FIPS140-2A] National Institute of Standards and Technology, FIPS 140-2 Annex A: Approved Security Functions.
[FIPS140-2B] National Institute of Standards and Technology, FIPS 140-2 Annex B: Approved Protection Profiles,
[FIPS140-2C] National Institute of Standards and Technology, FIPS 140-2 Annex C: Approved Random Number Generators

[FIPS140-2D] National Institute of Standards and Technology, FIPS 140-2 Annex D: Approved Key Establishment Techniques
[DES] National Institute of Standards and Technology, Data Encryption Standard, Federal Information Processing Standards Publication 46-3, October 25, 1999.
[DES Modes] National Institute of Standards and Technology, DES Modes of Operation, Federal Information Processing Standards Publication 81, December 2, 1980.

9. ACRONYMS

Acronyms	Definitions
ACR	Access Control Rule
AO	Application Operator
AP	Application Provider
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASC	Applet Security Controller
ATR	Answer To Reset
CBC	Cipher Block Chaining
CO	Cryptographic Officer
CH	Card Holder
CSP	Critical Security Parameter
CSC	Card Security Controller
DES	Data Encryption Standard
ECB	Electronic Code Book
EEPROM	Electrically Erasable and Programmable Read Only Memory
GC	Generic Container
JCRE	Java Card ™ Runtime Environment
MAC	Message Authentication Code
OP	Open Platform
PIN	Personal Identification Number
RAM	Random Access Memory
ROM	Read only Memory
SD	Security Domain
SC	Secure Channel
TDES	Triple DES (112-bit length keys)
XAUT	External Authentication