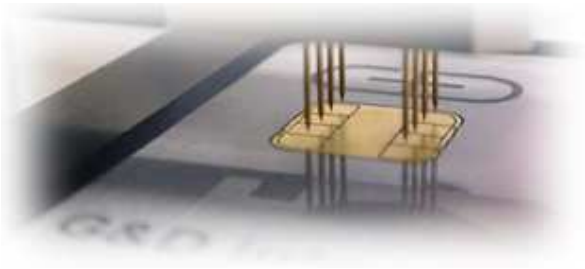
ActivCard Giesecke & Devrient



Sm@rtCafé Expert FIPS 64 with ActivCard Applet v2

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation

Version 0.4
August 2005

Table of Contents

1. INTRODUCTION

This document defines the Security Policy for the Sm@rtCafé Expert FIPS 64 with ActivCard Applet v2 applet suite cryptographic module, submitted for validation, in accordance with FIPS140-2 Level 2 requirements. Included are a 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

2.1 GIESECKE & DEVRIENT SM@RTCAFÉ EXPERT FIPS 64 CRYPTOGRAPHIC MODULE

Sm@rtCafé Expert FIPS 64 was developed by G&D and constitutes a complete operating system for smart cards. Providing a complete set of International Organization for Standardization (ISO), Europay, MasterCard and Visa (EMV) and proprietary enhanced commands, the Sm@rtCafé Expert FIPS 64 incorporates standards-based functionality along with its own optimized command set.

Sm@rtCafé Expert FIPS 64 contains an implementation of the Global Platform (GP) Version 2.0.1' specification [GPCS], which defines a secure infrastructure for post-issuance programmable smart cards. The GP specification defines a life cycle for GP compliant cards.

Sm@rtCafé Expert FIPS 64 offers Java Card technology [JCS] and Global Platform 2.0.1' [GPCS] services to applets on the chip such as ActivCard applets.
Other FIPS validated applets (tested against FIPS) may be downloaded to the chip.

State transitions between states of the life cycle involve well defines sequences of operations. Cards that have been issued to a Cardholder are necessarily in a "SECURE" state. This means that a defined set of applications have been loaded onto the card plus a set of keys and a PIN through which the identities of the Cryptographic Officer and the Cardholder can be authenticated.

The module consists of the Giesecke & Devrient Sm@rtCafé Expert FIPS 64 Java card module and the ActivCard Applet v2 which meets overall FIPS 140-2 Level 2 security requirements,. Together, the card and applets provide authentication, encryption, and digital signature cryptographic services. The hardware version number for the module is HD65246C1A05NB while the firmware version numbers are CH463JC_INABFOP003901_V101 and CH463JC_INABFOP003901_V102

2.2 ACTIVCARD APPLET V2

ActivCard Applet v2 provides significant enhancements over the ActivCard v1 Applet in service, security, and flexibility. The ActivCard Applet v2 framework is backward compatible with earlier versions of ActivCard Applets and offers a more open, stable, and flexible platform for developers to build and deploy smart card applications. ActivCard Applet v2 also complies with GSC-IS 2.1 standard.

ActivCard Applets are a modular suite of Java applets that run on a Java card. Version 2 of this suite is distinctive from Version 1 in the following ways:

- It decouples on-card application services from security management such as authentication and secure messaging, providing a more flexible, secure, and open platform for applet developers.
- It provides a flexible architecture to allow future authentication and biometric services to be added to the module without modifying existing applications.

The two applets included in the cryptographic module are:

- **Access Control Applet (ACA)** – this applet is responsible for Access Control Rules (ACR) definition, access control rules enforcement and secure-messaging processing for all card services. Three off-card entity authentication methods – OP secure messaging, PIN, and ActivCard External Authentication are included by default in the ACA applet.
- **PKI/Generic Container (PKI/GC) Applet** – The PKI/GC Applet can be used to provide secure storage for both PKI credentials, and other data, required for implementation of card services including single sign-on applications, identity, and benefits information. This applet is responsible for RSA-based cryptographic operations using the RSA private key stored in the PKI buffer. Up to 8 buffers can be configured for each applet instance.

3. SECURITY LEVEL

The Sm@rtCafé Expert FIPS 64 with ActivCard Applet v2 is designed and implemented to meet the Level 2 requirements of FIPS140-2. The cryptographic module enforces FIPS mode of operation at all times. 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	3
Operational environment	N/A
Cryptographic key management	2
EMI/EMC	3
Self tests	2
Design assurance	2
Mitigation of other attacks	2

Table 1 Individual FIPS 140-2 Security levels

4. CRYPTOGRAPHIC MODULE SPECIFICATION

The Sm@rtCafé Expert FIPS 64 with ActivCard Applet v2 supports role-based authentication of the Card Holder, Application Operators, and Cryptographic Officers, using PIN or TDES keys. All services provided by the cryptographic module are protected by a role based access control policy following the result of the authentication.

This validation effort is aimed at the systems software, virtual machines, Card Manager applications, and ActivCard applets. If additional applets are loaded into this cryptographic module, then these additional applets require a separate validation, and must be FIPS 140-2 validated. The module checks all validated applets, and does not load any applets that do not have the correct MAC.

Sm@rtCafé Expert FIPS 64 with ActivCard Applet v2 is based on the RENESAS AE46C1 smart card controller.
Some highlighted features of Sm@rtCafé Expert FIPS 64 are:

- SHA-1Hash algorithm
- Compliant to ISO 7816 Parts 1-7 [ISO]
- RSA up to 2048 bit for:
  - Digital signature generation and verification
  - Key generation

  - Encryption/Decryption for key transport
- DES and Triple-DES Encryption/Decryption
- DES MAC and TDES MAC generation and verification
- AES Encryption/Decryption
- DSA signature generation and verification

Sm@rtCafé Expert FIPS 64 with ActivCard Applet v2 is only capable of operating in response to commands sent from the reader in what is called a command-response pair. The reader sends an Application Protocol Data Unit (APDU) to the module and module responds with an APDU.

The APDU sent by the reader consists of a header and a body. The header contains a class byte differentiating between ISO defined command and private commands, an instruction byte containing the command code, and parameters relating to the command. The body contains any data that is needed for the command and, if necessary, the length of the expected data.

The response APDU transmitted by the module consists of a body and a trailer. The body contains any data that is returned in response to the command and the trailer contains the status message.

In the scope of this document, the Sm@rtCafé Expert FIPS 64 with ActivCard Applet v2 is considered as a single chip implementation of a cryptographic module.
The cryptographic boundary for Sm@rtCafé Expert FIPS 64 with ActivCard Applet v2 is the chip itself, excluding the card plastic. The chip is providing the physical boundary. Internally, the above- mentioned software pieces are included.

The ActivCard Applet v2 is composed of the following elements:
- ACA applet package version v 2.3.0.2 and 2.3.0.5
- PKI/GC applet package version 2.3.0.2 and 2.3.1.2
- ASC library package version 2.3.0.2 and 2.3.0.3

The applet and library package byte code is loaded in the cryptographic module memory. Note that the ASC library package consists of static utility classes only accessed by the applet and cannot be accessed directly by off-card entity.

The applets offer services to external 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 (SD) for the security configuration. This SD can either be the Card Manager or a separate security domain. The Card Manager is itself a security domain with additional services, and applets. The Card Manager controls the global cryptographic module status.

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 Secure Channel (SC) between the host and either the security domain or the security domain applets. The SC is generally used for administrative operations such as entering the application keys in the applet 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.

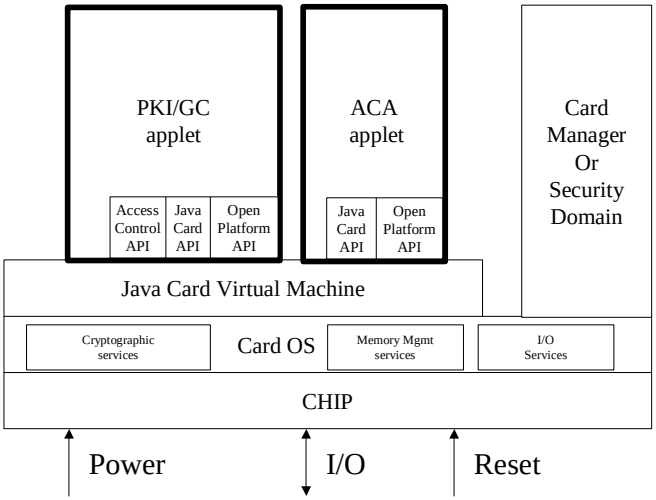


Figure 1: Functional block diagram

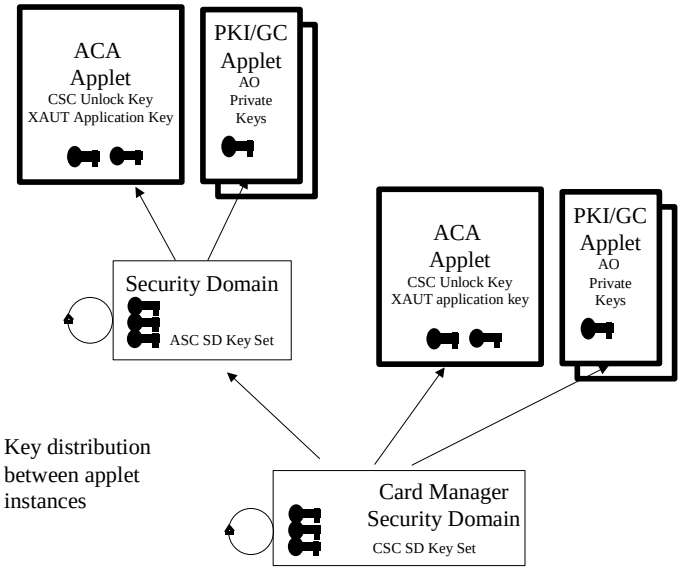


Figure 2: Key Distribution – Role separation

The Card Security Controller (CSC) role, which owns keys sets of the Card Manager, also plays an Applet Security Controller role for all applet instances depending on the Card Manager security domain.

4.1 MODULE INTERFACES

The electrical and physical interface of the Sm@rtCafé Expert FIPS 64 with ActivCard v2 applet suite, as a cryptographic module, is comprised of the 8-electrical contacts from the face of the cryptographic module to the chip. These contacts conform to the following specifications: “ISO 7816-1 Physical characteristics” and ”ISO 7816-2 Dimensions and contact location”.

4.1.1 Physical Interface description

There is only one physical interface to the module, the faceplate, which contains eight contacts, pinned as defined in ISO 7816-2. All FIPS 140-2 logical interfaces map to this single faceplate as detailed in Table 2.

FIPS 140-2 Logical Interface	Physical Interface
Data Input Interface	Faceplate
Data Output Interface	Faceplate
Control Input Interface	Faceplate
Status Output Interface	Faceplate
Power Interface	Faceplate

Table 2 - FIPS 140-2 Logical Interfaces

4.1.2 Electrical and Logical Interface specifications

Additionally, the eight contacts of the faceplate can be mapped to the logical interfaces as depicted in Table 3.

Contact	Function	FIPS 140-2 Logical Interface
C1	Power supply	Power Interface
C2	Reset	Control Input Interface
C3	Clock	Control Input Interface
C4	Not connected	N/A
C5	Ground	Power Interface
C6	Not connected	N/A
C7	Input/Output for serial data	Data Input Interface, Data Output Interface, Control Input Interface, Status Output Interface
C8	Not connected	N/A

Table 3 - Contact to Function Mapping

The module is composed of a plastic card and a single chip micro-controller, coated in epoxy, with an attached faceplate. The chip contains the processor, Read Only Memory (ROM - 368 kilobytes), Random Access Memory (RAM - 6 kilobytes), Electrically Erasable Programmable ROM (EEPROM - 64 + 4 kilobytes), co-processors, input/output (I/O), and timers. The power interface accepts voltages in the range of +5V +/-10% and +3V +/-10%.

5. ROLES & SERVICES

5.1.1 Roles

The ActivCard Applet v2 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 role, and Card Holder role.

5.1.1.1 User Roles:

- **Card Holder Role** - The Card Holder role is responsible for insuring the ownership of his cryptographic module, and for not communicating his PIN to other parties. An applet authenticates the Card Holder by verifying his PIN.
- **Application Operator 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 possession of the Application External Authenticate (XAUT) TDES 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 an OP secure channel TDES key set stored within the Card Manager. By successfully executing the OP secure channel mutual authentication protocol, the CSC role establishes a secure channel to the Card Manager and execute services allowed to the CSC role in a secure manner.
- **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 an OP secure channel TDES key set stored within the security domain. The ASC role also has the privilege of resetting the PIN try counter. This is performed either by authenticating himself using the OP secure channel key set, or an Unblock PIN XAUT TDES key. Note that the protection of the reset PIN retry counter service by XAUT external authentication is optional, as the reset PIN retry counter service is always accessible with the security domain OP key set.

5.1.2 Role Authentication

The ActivCard Applet v2 cryptographic module supports role authentication.

5.1.2.1 User Role Authentication

- The Card Holder role is authenticated with a PIN
  - **PIN**: this Card Holder role must send a Verify CHV APDU to any ActivCard applet or ACA applet to access services protected with PIN access control rules. The APDU corresponding to the applet service protected by the PIN, can access the service before the cryptographic module is removed or a reset order is sent to the cryptographic module.
- The Application Operator role is authenticated by the possession of a TDES key.
  - **Application External Authentication (XAUT) key**: The Application Operator role must prove the possession of a particular TDES key to access the PKI/GC buffer read, or update service protected with the External Authentication protocol using this particular key. An 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 to the module for verification. The APDU corresponding to the particular applet service must be sent before the cryptographic module is removed or a reset order is sent to the cryptographic module.

5.1.2.2 Cryptographic Officer Role Authentication

- The Cryptographic Officer role is authenticated by a TDES key or a TDES key set.
  - **Secure Channel 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.
  - **Unblock PIN External Authentication (XAUT) key**: The Cryptographic Officer (ASC) role must prove the possession of a particular TDES key to access the ACA Applet RESET RETRY COUNTER service protected by External Authentication with this particular key (K_{XAUT}). The host application controlled by the Cryptographic Officer role encrypts an 8-byte card challenge with K_{XAUT}, and submits a RESET RETRY COUNTER APDU that includes the resulting cryptogram for verification to the cryptographic module.

5.1.3 Services

5.1.3.1 Crypto Officer Role Administrative Services

5.1.3.1.1 Card Platform Administrative Services Available to the CSC role

The following card platform services are used for the administration of the security domains, and to load applets onto the cryptographic module. This command set includes the following commands:

- ***INSTALL:*** this APDU 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:*** this APDU is used to load the byte-codes of the Load File (package) defined in the previously issued INSTALL command.
- ***DELETE:*** this APDU is used by the CSC role to delete a Load File (package) or an applet (applet instance).
- ***DELETE ALL****:* This APDU is used to delete all packages and applet instances installed from those packages that have been loaded after completion of the card via LOAD commands.
- ***PUT KEY:*** this APDU is used to add or replace security domain key sets.
- ***SET STATUS:*** this APDU is used to modify the life cycle state of the cryptographic module or the life cycle state of an application.
- ***INITIALIZE UPDATE***: this APDU is used to initiate an OP Secure Channel with the Card Manager or a security domain. Cryptographic module and host session data are exchanged, and session keys are derived by the cryptographic module and host upon completion of this APDU. However, the Secure Channel is considered open upon completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command.
- ***EXTERNAL AUTHENTICATE***: this APDU is used by the cryptographic 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. A previous and successful execution of the INITIALIZE UPDATE command is required prior to processing this command.
- ***PUT DATA***: this APDU is used to store or replace one tagged data object provided in the command data field.
- ***GET STATUS***: this APDU command is used to retrieve the Card Manager, load file (package), and application life cycle data specific to the OP specification.
- ***GLOBAL PIN CHANGE/UNBLOCK:*** This APDU command is used to change the value of the Global PIN and to set the number of retries allowed or to unblock the current Global PIN. PIN value is encrypted with the KEK. The Global PIN is different from the Card Holder PIN used by the ActivCard applets. The Global PIN is not used by the module.

During the secured channel opening, the command access condition is specified ('CLEAR', 'MAC', 'MAC+ENC') and an access control decision is performed on the received command.

5.1.3.1.2 Applet Administrative Services available to the ASC role

The following applet administrative services are used for configuring applet specific properties and keys.

ACA Administrative Services

The following services are provided by the ACA applets.

- ***INITIALIZE UPDATE.*** This APDU 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 APDU 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.
- ***SET STATUS***: This APDU is sent when the applet instance life cycle needs to be changed. The applet instance life cycle can be: SELECTABLE, BLOCKED, and PERSONALIZED.
- ***SET APPLICATION UID***: This APDU is sent when the UID associated with the applet instance needs to be changed.
- ***REGISTER APPLET:*** This APDU registers applet instances to the ACA instance so that the access control and secure message service can be provided.
- ***REGISTER ACR:*** This APDU manages the mapping between ACRID and actual APDU instruction.
- ***RESET RETRY COUNTER:*** All PIN-protected services of all applet instances that are registered to the particular ACA instance are not accessible to the Card Holder when successive PIN verifications for that ID instance fail. These applets are then in a "PIN blocked" state.
    - If this APDU is protected in secure channel using Cryptographic Officer OP SC key set, it is used to set a new PIN value and recover Card Holder access.
    - If this APDU is protected by AC External Authenticate protocol using the Unblock External Authentication (XAUT) key, it also can be used to set a new PIN value and recover Card Holder access.
- ***PUT KEY***: This APDU is used to enter the XAUT key used to unblock the PIN, and must be used with a secure channel. The APDU format is compliant with OP specifications.
- ***GET CHALLENGE***: This APDU is used in combination with AC external authenticate to perform an external authentication of the Application Operator in order to unblock the PIN.
- ***AC EXTERNAL AUTHENTICATE***: This APDU is used in combination with a Get Challenge to authenticate the Application Operator using the AC external authenticate protocol.
- ***UPDATE PROPERTIES***. This APDU sets 1) a flag that indicates that the card holder must change his PIN before any PIN protected service can be accessed; 2) return either CAC v1 status word, or GSC-IS v 2.1 status word, when the Card Holder enters the wrong PIN.

PKI/GC Applet Administrative Services

The PKI/GC Applet provides RSA-based cryptographic services. Each PKI/GC applet instance can store up to eight objects, either an RSA key pair / certificate object or T-V buffer object

.

The following services are provided by a PKI/GC applet instance:

- ***GENERATE KEY PAIR:*** This APDU is used to generate an RSA Key Pair in the cryptographic module. The Private Key is associated with a PKI Applet instance.
- ***PUT KEY***: This APDU is used to import/unwrap the private key (Chinese Remainder Theorem) components. The APDU format follows OP specification. A unique private key exists for each RSA key pair object.
- ***SET PROPERTIES:*** This APDU is used to set the object ID of the different PKI/GC objects in the PKI/GC applet instance. Note that the access control rule is enforced at object level rather than the instance level.

- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.

5.1.3.2 Usage services

5.1.3.2.1 Card Platform and Applet Services Available to No Role (unauthenticated)

- ***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).
- ***GET DATA:*** the GET DATA command is used to retrieve a single data object. This command is available outside of a Secure Channel (no security condition). However, if issued within a Secure Channel, it must follow the same security level as defined in EXTERNAL AUTH.
- **MANAGE CHANNEL**: This command is used to open or close a logical channel
- **GET FREE SPACE**: GET FREE SPACE is used to display the largest free memory block for package loading or the complete available free EEPROM or the complete available Clear-On-Reset (COR) /Clear-On-Deselect (COD) space
-
- ***GET PROPERTIES***: This APDU is used to obtain information about applet instance configuration.
- ***GET ACR:*** This APDU is used to retrieve the ACR definition for the services.
- ***GET CERTIFICATE***. This APDU is used to obtain the certificate corresponding to RSA private key stored in the corresponding object.
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.

A user can initiate module self-tests by issuing a card reset and issuing an APDU command. The ATR value can be retrieved by issuing a card reset.

5.1.3.2.2 Applet Usage Services Available to Application Operator

The following services are available to the Application Operator role:

- ***GET CHALLENGE***. This APDU is used in combination with GC External Authenticate to perform an external authentication.
- ***AC EXTERNAL AUTHENTICATE***. This APDU communicates the cryptogram obtained by TDES encryption of a card challenge with the TDES key associated with the service – here read or update buffer – protected by XAUT.
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.

5.1.3.2.3 Applet Usage Services Available to Card Holder

Common Usage Services

The following services (APDUs) are common to all instances of applets:

- ***VERIFY CHV***: This APDU checks the PIN presented by the Card Holder against the current PIN associated with the ACA applet instance.

ACA Applet Usage Services

The ACA applet provides Card Holder Verification (CHV) services, access control enforcement, and secure messaging.

- ***CHANGE REFERENCE DATA:*** This APDU is used to change the Card Holder PIN if the Card Holder is correctly authenticated.

PKI/GC Applet Usage Services

The PKI/GC Applet provides RSA-based cryptographic services and secure storage. One RSA private key exists for each PKI buffer. The corresponding certificate is located in this PKI buffer.

The following APDUs / services are provided by a PKI/GC applet instance:

- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.
- ***PRIVATE SIGN / DECRYPT***. This APDU uses the RSA private key in the PKI buffer to sign data.

5.1.3.3 Relationship Between Roles & Services: Card Platform

Roles/Services	CSC role (Card Manager)	CSC Role (G&D Security Domain)	No Role (Unauthenticated)
INSTALL	X	X	
LOAD	X	X	
DELETE	X	X	
DELETE ALL	X		
EXTERNAL AUTHENTICATE	X	X	
GET DATA			X
GET STATUS	X		
GET FREE SPACE			X
INITIALIZE UPDATE	X	X	
GLOBAL PIN CHANGE/UNBLOCK	X		
PUT DATA	X	X	
PUT KEY	X	X	
SELECT			X
SET STATUS	X		
MANAGE CHANNEL			X

Table 4 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 (ACR) that also indicates the allowed role for that service, as detailed in the previous section.
The ACR may be configurable or fixed depending on the applet service. The ACA applet is responsible for the configuration, management, and enforcement of the ACRs for each service provided by the applet instances.

The applet services are invoked by external APDU commands sent to the cryptographic module. The ACRs are applied on the APDU commands by the ACA Applet. All services are specified in the respective Applet Specification documents.

5.1.3.4.2 Roles vs. Services: ACA Applet

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC/ASC) / SECURE CHANNEL	Application Operator or ASC / XAUT	Card Holder / PIN
ACA Applet				
INSTALL		**X**		
CHANGE REFERENCE DATA				**X**
GET PROPERTIES	**X**			
GET ACR	**X**			
INITIALIZE UPDATE	**X**			
EXTERNAL AUTHENTICATE		**X**		
VERIFY CHV	**X**			
PUT KEY		**X**		
GET CHALLENGE	**X**			
AC EXTERNAL AUTHENTICATE			**X**	
SET STATUS		**X**		
UPDATE PROPERTIES		**X**		
RESET RETRY COUNTER		**X**	**X**	
REGISTER APPLET		**X**		
REGISTER ACR		**X**		

Table 5 Roles & possible ACR configurations for ACA applet services

5.1.3.4.3 Roles vs. Services: PKI/GC Applet

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC/ASC) / SECURE CHANNEL	Card Holder / PIN	Application Operator / XAUT	Application Operator or Crypto Officer XAUT or SECURE CHANNEL
PKI/GC Applet					
INSTALL		**X**			
GET PROPERTIES	**X**				
INITIALIZE UPDATE	**X**				
EXTERNAL AUTHENTICATE		**X**			
UPDATE CERTIFICATE / STATIC BUFFER	**X**	**X**	**X**	**X**	**X**
READ CERTIFICATE / STATIC BUFFER	**X**	**X**	**X**	**X**	**X**
GET CHALLENGE	**X**				
GENERATE KEY PAIR		**X**	**X**		
PRIVATE SIGN / DECRYPT			**X**		
GET CERTIFICATE	**X**				
PUT KEY		**X**			
AC EXTERNAL AUTHENTICATE				**X**	**X**
VERIFY CHV	**X**				
SET STATUS		**X**			
SET PROPERTIES		**X**			

Table 6 Roles & possible ACR configuration for PKI/GC applet services

5.1.3.5 Module Cryptographic Functions

The purpose of the ActivCard Applet v2 is to provide a FIPS approved platform for applets that may in turn provide cryptographic services to end-user applications. The keys represent the roles involved in controlling the cryptographic module. A variety of FIPS 140-2 validated algorithms provided by the JavaCard API are used in the ActivCard Applet v2 to provide cryptographic services. These include:

- TDES, (2 keys EDE TDES)
- SHA-1,
- RSA PKCS1 (512, 768, 1024 and 2048 bit keys)

The TDES (CBC mode) algorithm is used both for authenticating the Crypto Officers (EXTERNAL AUTH command) and for encrypting data flow from the external application to the cryptographic module environment. The reverse direction is not encrypted (i.e. the status words returned in response to an APDU are not encrypted)..

The Sm@rtCafé Expert FIPS 64 module implements strong, standards-based cryptography. It includes the following FIPS-approved algorithms:

- DES (ECB and CBC modes) (Cert. #249): to be used for legacy applications only
- Triple-DES (2key TDES) (ECB and CBC modes) (Cert. #239)
- DES MAC (ECB and CBC modes) (Cert. #249, vendor affirmed)
- Triple-DES MAC (2key TDES) (ECB and CBC modes) (Cert. #239, vendor affirmed)
- AES (128, 192, 256-bit key sizes) (ECB and CBC modes) (Cert. #132)
- SHA-1 (Cert. #216)
- DSA (Cert. #102)

- RSA Sign/Verify (Cert. #7, 1024, 1536 and 2048-bit mod sizes, PKCS #1)[1]

Pseudo Random Number Generation:
- PRNG based on ANSI X9.31 Appendix A.2.4

Non FIPS-approved algorithms
- RSA encryption/decryption[2]

5.1.3.6 RNG

The Sm@rtCafé Expert FIPS 64 with ActivCard Applet v2 applet suite cryptographic module offers the services of a FIPS approved PRNG using ANSI X9.31 standard.

5.1.3.7 Self Tests

The Sm@rtCafé Expert FIPS 64 with ActivCard Applet v2 applet suite runs startup and conditional self-tests to verify that it is functioning properly. These startup self-tests are performed before the module processes the first command it receives after a Reset. Conditional self-tests are executed whenever specific conditions are met.

5.1.3.7.1 Power-Up Self Tests

The self-tests include:
Software Integrity Tests: *The module checks the integrity of its firmware:*
- **ROM:** 32 bit Checksum
- **Firmware in EEPROM:** 24 bit EDC with Reed Solomon algorithm
- **Java Code in EEPROM:** 32 bit EDC with Reed Solomon algorithm

Cryptographic Algorithm KATs: *Known Answer Tests (KATs) are run at power-up for the following algorithms:*
- **DES KAT**
- **Triple-DES KAT**
- **AES KAT**
- **DSA KAT**
- **RSA KAT**
- **RSA CRT KAT**
- **ANSI 9.17 Software RNG KAT**

5.1.3.7.2 Conditional Tests

Conditional RSA Pairwise Consistency Check: *After generating an RSA key pair, the module performs a sign/verify with that key pair to ensure that the key pair is correct. Then the module performs an encryption/decryption with that key pair to ensure that the key pair is correct.*
Conditional DSA Pairwise Consistency Check: *After generating an DSA key pair, the module performs a sign/verify with that key pair to ensure that the key pair is correct.*
If any of these self-test fails, the module will halt all operations until it is reset.
If module fails a power on self-test, the module sends the self-test failure indicator and enters the error state. No further communication is possible with the module until it is removed from the terminal and re-inserted or terminal resets the module.
Continuous RNG test: On every output generated by ANSI X9.31 and hardware RNG the module performs a comparison with previously generated random block. The 8 first bytes generated by the ANSI X9.31 PRNG and the hardware RNG are only used for doing this continuous comparison and never used for any service like cryptographic calculations. If generated numbers are equal to previous generated numbers, this selftest fails.

[1] For card with firmware version CH463JC_INABFOP003901_V102 RSA Sign/Verify operations using 2048-bit key size is considered non-Approved since a corresponding self-test is not performed
[2] RSA Encrypt/Decrypt can be used for key transport in an Approved mode of operation

If any of these self-tests fail, the module will halt all operations until it is reset.
If module fails a self-test, the module sends the self-test failure indicator and enters the error state. No further communication is possible with the module until it is removed from the terminal and re-inserted or terminal resets the module.
Software/Firmware Load Test: A TDES CBC MAC on the applet Load File is verified whenever an applet is loaded onto the cryptographic module since applet loading always takes place within a Secure Channel. If Security Domain Applet with mandated DAP privilege is installed and K_{DAP} is set in this Security Domain, every Package loaded onto the Card has to provide a DAP value (TDES MAC or RSA Signature), which is verified using the K_{DAP}.
If TDES MAC or DAP verification fails, package load is terminated. For more details see OP 2.0.1' **Error! Reference source not found.**.

5.1.4 Critical Security Parameters

1. Initialization TDES key, K_{Init}: used only for the first Card Manager key-set loading.
2. Crypto Officer (Card Manager) Security Domain TDES keys (K_{ENC}, K_{MAC} and K_{KEK}) for CO authentication as per OP specifications.
3. Secure Channel Session TDES keys (K_{SMAC} and K_{SENC} derived from Crypto Officer keys set(s)) as per the Global Platform 2.0.1' [GPCS].
4. G&D Security Domain TDES keys (SDK_{ENC}, SDK_{MAC} and SDK_{KEK}) used for User authentication as per the OP specifications.
5. Secure Channel Session TDES keys (SDK_{SMAC} and SDK_{SENC} derived from G&D Security Domain keys set(s)) as per the Global Platform 2.0.1' [GPCS].
6. "OP DAP" TDES key K_{DAP}. This 112-bit key is used during DAP verification that enables the applet provider to check, independently of the Issuer, that his applet has been correctly loaded.
7. External Authentication Keys K_{Auth} are TDES keys that enable the authentication of Application Operators (PKI/GC read or PKI/GC Update) or Cryptographic Officers (Reset Retry Counter).
8. RSA private keys K_{RSA} are managed (generated, unwrapped) from the PKI/GC applet using the Java card cryptographic services. These keys are used to sign data.

9. Personal Identification Numbers (PIN): PINs and PIN attributes are managed from the ACA Applet, which relies on Java Card PIN management service.
10. Authentication Method (or ACR): These data elements define the Authentication Method that is permanently set for the service. Several services offer a configurable Authentication Method. For such services, the authentication method should be set according to the tables in section 5.1.3.4.
11. Delegated Management TDES key $K_{Receipt}$ for Receipt generation to prove successful execution of Delegated Management command
12. TDES PRNG key: This 112-bit key is used by the ANSI X9.31 PRNG implementation

The keys 2&4 are also referred to as the OP TDES keyset.
A Security Domain (Card Manager and G&D Security Domain) key set is structured as to contain three types of TDES keys:

- K_{ENC} – A 112-bit key used for Crypto Officer and User authentication and to derive session keys for encrypted mode of the secure channel,
- K_{MAC}, – A 112-bit key used for Crypto Officer and User authentication and to derive session key for MAC mode of the secure channel,
- K_{KEK} – A 112-bit key used to encrypt keys, to be imported into the platform using the Put Key command.

5.2 ACCESS TO CSPS VS SERVICES

The following matrix identifies how different services access CSPs for each applet.

5.2.1 Card Manager & G&D Security Domain applet

Card Manager &G&D Security Domain applet Columns: Services (roles) Rows: Access to CSPs	**Card Holder**	**Application Operator**	**Crypto Officer (CSC)**	INSTALL	LOAD	DELETE	DELETE ALL	PUT KEY	SET STATUS	INITIALIZE UPDATE:	EXTERNAL AUTHENTICATE	PUT DATA	GET STATUS	GLOBAL PIN CHANGE/UNBLOCK
OP TDES keyset														
Enter/Delete Key			X			X	X	X						
Generate/Verify Cryptogram			X							X	X			
Decrypt APDU Payload			X											X
Decrypt PIN/key using KEK								X						X
Secure Channel session keys														
Verify MAC			X	X	X	X	X	X	X		X	X	X	X
Decrypt APDU Payload			X	X	X	X	X	X	X		X	X	X	X
"OP DAP" TDES key K_{DAP}														
DAP Verification			X		X									
Enter/Delete Key						X		X						
TDES key $K_{Receipt}$														
Enter/Delete Key						X		X						
Receipt Generation					X									
TDES PRNG Key														
Generation of random data										X				

5.2.2 ACA Applet

ACA applet Columns: Services (roles) Rows: Access to CSPs	**Card Holder**	**Application Operator**	**Cryptographic Officer**	**INSTALL/INSTANTIATE (CSC)**	**CHANGE REFERENCE DATA**	**GET PROPERTIES (NO ROLE)**	**GET ACR (NO ROLE)**	**INITIALIZE UPDATE (NO ROLE)**	**EXTERNAL AUTHENTICATE (ASC)**	**VERIFY CHV (C.H)**	**PUT KEY (ASC)**	**GET CHALLENGE (NO ROLE)**	**AC EXTERNAL AUTHENTICATE (ASC)**	**SET STATUS (CSC)**	**UPDATE PROPERTIES (ASC)**	**RESET RETRY COUNTER (ASC)**	**REGISTER APPLET (ASC)**	**REGISTER ACR (ASC)**
ACR																		
Install			X	X														
Register ACR			X															X
PIN																		
Reset Retry Counter			X													X		
Change Reference Data	X				X													
Verify CHV	X									X								
XAUT Key																		
Enter/Delete Key			X								X							
Verify Cryptogram		X											X					
OP key set																		
Enter/Delete Key			X								X							
Verify Cryptogram			X						X		X					X		
Decrypt APDU Payload			X								X					X		
Applet Instance Status																		
Set Status			X											X				
Register Applet			X														X	
Update Property			X												X			
TDES PRNG Key																		
Random Number Generation			X					X				X						

5.2.3 PKI/GC Applet

PKI/GC applet services Columns: Services (roles) Rows: Access to CSPs	***Card Holder***	***Application Operator***	***Cryptographic Officer***	**INSTALL/INSTATIATE (CSC)**	**GET PROPERTIES (any)**	**INITIALIZE UPDATE (any)**	**EXTERNAL AUTHENTICATE (ASC) UPDATE CERT / STATIC BUFFER (A. O)**	**READ CERT / STATIC BUFFER (A.O)**	**GET CHALLENGE (No Role) AC EXTERNAL AUTHENTICATE (A.O)**	**GENERATE KEY (ASC or CH)**	**GET CERTIFICATE (any)**	**PRIVATE SIGN / DECRYPT (C.H)**	**SET STATUS (ASC)**	**SET PROPERTIES (ASC)**	**VERIFY CHV (C.H)**	**PUT KEY (ASC)**
PIN																
Verify CHV	X														X	
RSA Key Pair																
Generate Key	X		X							X						
Enter CRT Components			X													X
Delete Private Key			X													X
Sign Data	X											X				
OP key set																
Verify Cryptogram			X				X									
Decrypt Data			X				X									X
Applet Instance Status																
Install			X	X												
Set Status			X										X			
Set Properties			X											X		
TDES PRNG Key																
Random Number Generation	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 usage of the module as follows:
- Module service access control rules must be configured per tables 1, 2, and 3 in section 5.1.3.
- Follow all security rules outlined in section 6.1.2.
- The card with firmware version CH463JC_INABFOP003901_V102 should not be used to perform 2048-bit RSA Sign/Verify using the PRIVATE SIGN / DECRYPT APDU in an Approved mode
- RSA Decrypt using the PRIVATE SIGN / DECRYPT APDU should be used only for performing key transport in an Approved mode

6.1.2 Authentication Security Rules

The module implements specific methods for identifying and authenticating the different roles. The implementation consists of binding a role-based ACR 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.
- Applets shall provide role-based authentication:
    - The Card Holder is authenticated by the knowledge of a unique PIN.
    - The Crypto Officer is authenticated via OP secure channel mutual authentication protocol using the card manager/security domain key set that composed of 3 TDES double length keys. Two keys are used to authenticate and MAC the command payload. A third key is used to encrypt keys transported within the APDU command (Initialize Update & External Authenticate commands). For Crypto Officer is also authenticated via AC external authenticate protocol using the Unblock PIN XAUT TDES key.
    - The Application Operator role is authenticated via AC external authenticate protocol using the application XAUT TDES key.
- Cryptographic services are restricted to authenticated roles.
- The role authentication methods (ACRs) for each applet service are set by the Crypto Officer during applet instantiation and can only be modified by the Crypto Officer.
- When authentication of the role cannot be performed because the related key or PIN 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.
- Applet instance configuration may require the combined authentication of different roles to access a particular service. For instance the Application Operator, or the Cryptographic Officer, must both authenticate to access the Update Certificate / Static Buffer service.

6.1.3 Applet Life Cycle Security Rules

The ActivCard Applet v2 only permits loading of FIPS approved applets. Applets can only be loaded through an OP 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 Card Acceptance Device are controlled by a valid role; Card Holder, Application Operator or Cryptographic Officer / crypto-officer.
- Management of applet life cycles (load, install, delete, personalize keys), shall follow the Open Platform standard [VOPS].
- Applet and key APDU command management (i.e. Load, install, delete, put key) are protected by secure channel MAC (TDES-CBC). Their origin is authenticated, and their integrity verified. In particular this protects the applet byte code against tampering when downloaded at post-issuance.

- The download of validated applet packages, and the installation of applet instances, may occur either at pre-issuance, issuance or post-issuance.
- There may be as many instances of each applet as there are cryptographic module resources available.

6.1.4 Access Control Security Rules

- Keys must be loaded through an OP secure channel. Consequently, keys are always loaded in the encrypted form.
  - The password or PIN that is used by the applet to authenticate the Card Holder must not be divulged to other parties than the Card Holder.
  - The ACA applet must be configured by the cryptographic officer so that:
    - After 1 <= N <= 10 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

6.1.5 Physical Security Rules

The physical security of the Sm@rtCafé Expert FIPS 64 with ActivCard applet v2 suite is designed to meet FIPS 140-2 level 3 requirements. A hard opaque epoxy is used to encapsulate the module to meet level 3 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 Applet Loading Security Rules

Only applets validated according to FIPS 140-2 shall be loaded onto the Sm@rtCafé Expert FIPS 64 cryptographic module.

Applets can only be loaded through a secure channel thus requiring a TDES MAC verification over each Load block.

In the Sm@rtCafé Expert FIPS 64 module, the applet is always loaded by the Issuer (Cryptographic Officer) or authorized by Issuer in case of Delegated Management.

6.1.6.1 "OP Delegated Management"

If Delegated Management shall be used, the Crypto Officer has to set Delegate Management Keys for Token verification (K_{Token}) and Receipt generation ($K_{Receipt}$), install the G&D Security Domain with Delegated Management privilege and set Secure Channel keys of this Security Domain.

User of G&D Security Domain can load packages or install applications on the card, only if he/she establishes a secure channel and presents the card with a Token during the OP Install for Load command. The Token is a RSA signature generated by the Card Issuer using the Card Issuer private key to ensure that the Card Issuer has authorized the load process and the Load File or the install process. If the token verification is successful, the card processes the Load command and answers with a receipt, i.e. a TDES MAC generated by the Card, acknowledging that the operation was successfully performed. For details see OP 2.0.1' [GPCS]

6.1.6.2 "OP DAP"

If the G&D Security Domain is instantiated with a DAP verification privilege, an applet may be loaded with an optional DAP. If the G&D Security Domain is instantiated with mandated DAP verification privilege, a DAP is required.

The mechanism designated as "DAP" in OP 2.0.1' [GPCS] enables the applet provider to check, independently of the Issuer (Cryptographic Officer), that his applet has been correctly loaded. This check is done by a MAC verification on the applet. This MAC is an algorithm using DES MAC for the first n-1 Load blocks and a TDES MAC for the last Load block. All the DES and TDES operations use TDES DAP

key (K_{DAP}), loaded in the G&D Security Domain. This process is described in detail in the Reference Manual Sm@rtCafé Expert FIPS 64.

6.1.7 Key Management Security Policy

6.1.7.1 Cryptographic key generation

-TDES Session key generation as per **Open Platform (OP) specification [GPCS]** using FIPS140-2 approved ANSI X9.31 PRNG to generate random data required for Secure Channel Opening.

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

6.1.7.2 Cryptographic key entry

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

6.1.7.3 Cryptographic key storage

The Keys are structured to contain the following parameters:

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

6.1.7.4 *Cryptographic key zeroization*

The cryptographic module zeroizes cryptographic keys by reloading a zero-valued key set for Crypto Officer OP secure channel key set, or Application Operator XAUT key, or closing of secure channel for session keys**.** The cardholder PIN is zeorized by setting it to zero value. The RSA private key is zeorized by reloading a zero-valued key.

Key Management Details can be found in a specific proprietary document.

The Sm@rtCafé Expert FIPS 64 module replaces initialization Key Kinit of Card Manager with first new keyset loaded into Card Manager.

Security Domain (Card Manager and G&D Security Domain) Keysets (including K_{ENC}, K_{MAC} and K_{KEK}) loaded onto the card can be deleted using the Delete APDU or replaced by reloading another key set for Crypto Officer and User using the Put Key command.

The Sm@rtCafé Expert FIPS 64 module destroys cryptographic session keys K_{SMAC} and K_{SENC} of Security Domain (Card Manager and G&D Security Domain) when closing of a secure channel.
The key for “OP DAP” K_{DAP} can only be updated.

The Application Operator XAUT key can be zeroized by using the PutKey command.
To delete K_{DAP}, the Security Domain containing the key must be deleted. This operation deletes all the keys contained in the Security Domain.

The keys loaded for Delegated Management K_{Token} and $K_{Receipt}$ can be zeroized by overwriting the values using the Put Key command or by using the Delete command.

The CardHolder PIN can be zeroized by overwriting with a new value using the Change Reference Data command. The RSA private keys can be zeroized by using the PutKey command to replace the key

All keys including PRNG TDES key for FIPS140-2 approved ANSI X9.31 PRNG can be zeroized by setting the card state to TERMINATED.

6.1.8 Mitigation of attacks Security Policy

The cryptographic module implements countermeasures for three attacks commonly used against smart cards: simple power analysis (SPA), differential power analysis (DPA), and timing analysis. These attacks work by monitoring the power consumption (SPA, DPA) or timing of operations during cryptographic processing in order to gain information about sensitive content, such as secret keys.

The module's IC has a co-processor for performing DES and Triple-DES operations. This co-processor was specifically designed by Renesas Semiconductor to counter SPA, DPA, and timing analysis attacks. G&D has conducted testing of the module's DES and Triple-DES processing for resistance to these attacks and found that no information was leaked during this processing via these attacks.

The module's RSA implementation has been hardened against SPA, DPA, fault and timing analysis using a variety of techniques. For timing analysis, the timing of the RSA implementation does not correlate to the inputs to the implementation. To counter SPA, conditional jumps based on the exponent and squares were avoided. Randomization of the base and exponent is employed to counter DPA. G&D has conducted testing of the module's RSA processing for resistance to these attacks and found that no information was leaked during this processing via these attacks.

7. SECURITY POLICY CHECK LIST TABLES

7.1 ROLES & REQUIRED AUTHENTICATION

Role	Type of authentication	Authentication data
Card Security Controller	OP secure channel mutual authentication protocol	OP secure channel TDES key set of three
Applet Security Controller	OP secure channel mutual authentication protocol or TDES	OP secure channel TDES key set of three or Unblock PIN XAUT TDES key
Application Operator	AC External Authenticate protocol	Application XAUT TDES key
Card Holder	Verify CHV service	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 role services are listed in Section 5.1.3.1.1
Applet Security Controller	The Applet Security Controller role services are listed in Section 5.1.3.1.2
Application Operator	The Application Operator role services are listed in Section 5.1.3.2.2
Card Holder	The Card Holder role services are listed in Section 5.1.3.2.3

7.4 ACCESS RIGHTS WITHIN SERVICES

Service	CSP	Types of Access (i.e. Read, Write, Execute)
Crypto Officer (CSC/ASC) Service	OP secure channel TDES key set of three or Unblock PIN XAUT TDES key	Execute (encrypt, decrypt), write (put key)
Application Operator Service	Application XAUT TDES key	Execute (encrypt, decrypt)
Card Holder Service	PIN	Execute (Verify CHV), write (Change Reference Data)

7.5 MITIGATION OF OTHER ATTACKS

Other Attacks	Mitigation Mechanism	Specific Limitations
Simple Power Analysis	Counter Measures against SPA	N/A
Differential Power Analysis	Counter Measures against DPA	N/A

8. REFERENCES

[JVM] Java Card ™ 2.2 Virtual Machine Specification v1.1 - June 1999, Sun Microsystems

[JCAPI] Java Card ™ 2.2 Application Programming Interface, Sun Microsystems

[JCDG] Java Card ™applet developer's guide

[JCRE] Java Card ™ 2.2 Runtime Environment (JCRE) Specification, Sun Microsystems

[JCS] Java Card ™ 2.2 Card Specification, June 2002, Sun Microsystems

[VOPS] 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

[GPCS] Global Platform Card Specification, v2.0.1' - April 2000

[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.

[DSS] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 27, 2000.

[ISO] ISO/IEC 7816-3 : Second edition 1997-09-18, Identification cards - Integrated circuit(s) cards with contacts - Part 3 : Electronic signals and transmission protocols, ISO/IEC FCD 7816-4: 2003 (Draft) Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange, Working draft dated 2003-01-17, ISO SC17 Document 17N2268T, ISO/IEC 7816-5 : 1994, Identification cards - Integrated circuit(s) cards with contacts - Part 5 : Numbering system and registration procedure for application identifiers, ISO/IEC FCD 7816-6 : 2003 (Draft), Identification cards - Integrated circuit(s) cards with contacts - Part 6 : Interindustry data elements for interchange – FCD dated 2003-01-17, ISO SC17 Document 17N2270T, ISO/IEC FCD 7816-8: 2003 (Draft), Integrated circuit(s) cards with contacts, Part 8: Interindustry commands for a cryptographic toolbox. FCD dated 2003-01-17, ISO SC17 Document 17N2272T, ISO/IEC FCD 7816-9: 2003 (Draft), Integrated circuit(s) cards with contacts, Part 9: Interindustry commands for card and file management. FCD dated 2003- 01-17, SC17 Document 17N2274T.

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
GSC-IS	Government Smart Card Interoperability Standard
JCRE	Java Card ™ Runtime Environment
PKI	Public Key Infrastructure
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