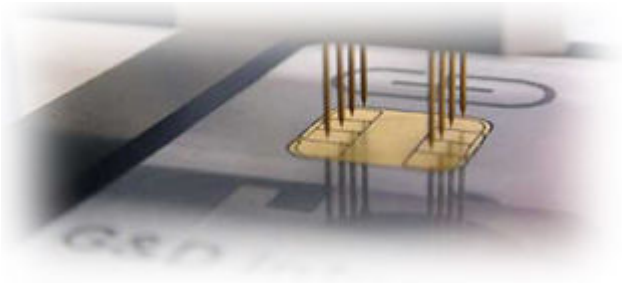
Giesecke & Devrient



Giesecke & Devrient

Sm@rtCafé Expert FIPS 64

FIPS 140-2 Non-Proprietary Security Policy

Level 3 Validation

Version 1.2
November 2004

Table of Contents

1. INTRODUCTION

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for Giesecke & Devrient (G&D) Sm@rtCafé Expert FIPS 64. This security policy describes how Sm@rtCafé Expert FIPS 64 meets the security requirements of FIPS 140-2 **[FIPS140-2]** and how to run Sm@rtCafé Expert FIPS 64 in a secure FIPS 140-2 approved mode. This policy was prepared as part of the Level 3 FIPS 140-2 validation of Sm@rtCafé Expert FIPS 64.

Throughout this document, the Sm@rtCafé Expert FIPS 64 is referred to as the chip, the Sm@rtCafé Expert FIPS 64, and the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at www.nist.gov/cmvp.

1.2 References

This document deals only with operations and capabilities of Sm@rtCafé Expert FIPS 64 in the technical terms of a FIPS 140-2 cryptographic module security policy and has been written in parts describing Open Platform functionality. More information is available on Sm@rtCafé Expert FIPS 64 from the following sources:

- Overview information of Giesecke & Devrient products and services can be found at: www.gdai.com
- For answers to technical or sales related questions, please refer to the contacts listed on the Giesecke & Devrient website at www.gdai.com

[GPCS]	Global Platform Card Specification, v2.0.1' - April 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.
[JCS]	Java Card ™ 2.2 Card Specification, June 2002, Sun Microsystems
[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, 2002
[DES]	National Institute of Standards and Technology, Data Encryption Standard, Federal Information Processing Standards Publication 46-3, October 25, 1999.

Table 1 References

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine Model
- Sm@rtCafé Expert FIPS 64 Reference Manuals
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation was produced by Giesecke & Devrient. With the exception of this non-proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is proprietary to Giesecke & Devrient and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Giesecke & Devrient.

2. SM@RTCAFÉ EXPERT FIPS 64 CRYPTOGRAPHIC MODULE SPECIFICATION

2.1 Overview

Sm@rtCafé Expert FIPS 64 (Hardware version: HD65246C1A05NB; Firmware versions: CH463JC_INABFOP003901_V101 and CH463JC_INABFOP003901_V102) 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 140-2 validated applets may be downloaded on the chip. If an applet, which is not FIPS 140-2 validated, is loaded on this module, the module loses its FIPS 140-2 validation.

State transitions between states of the life cycle involve well-defined sequences of operations. Cards that have been issued are necessarily in a "SECURED" state. This means that the G&D Security Domain has been loaded onto the card plus a set of keys and a PIN through which the Cryptographic Officer can be authenticated.

Sm@rtCafé Expert FIPS 64 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 only
- DES and Triple-DES Encryption/Decryption **[DES]**
- AES Encryption/Decryption

- DSA signature generation and verification

2.2 Physical Security with Well-Defined Interfaces

Sm@rtCafé Expert FIPS 64 is defined as a single-chip module for FIPS 140-2 purposes. The physical form of the module is a single chip coated in epoxy, with an attached faceplate. It is intended to meet overall FIPS 140-2 Level 3 requirements (see Table 2 below).

Section	Section Title	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services, and Authentication	3
4	Finite State Model	3
5	Physical Security	3
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	Electromagnetic Interference/Electromagnetic Compatibility	3
9	Self-tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	3

Table 2 – Intended Level Per FIPS 140-2 Section

The module is composed of 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%.

The smart card controller provides a number of security features, including

- High frequency detector
- High voltage detector
- Low frequency detector
- High temperature detector
- Low temperature detector

The chip is embedded in epoxy, which completely encapsulates the whole Integrated Circuit (IC). Only micro-wires connecting to the faceplate penetrate the epoxy,

connecting to the faceplate interface of the module. Attempts to tamper with the module result in damage to the epoxy, the plastic card, or the metal faceplate (scratches, chips, dents, etc.).

From the time of its manufacture, the card is in possession of the Cryptographic Officer until it is ultimately issued to the User. From that point, the card is in the physical possession of the User.

To attack the cryptographic information contained in the module, that is to attempt to compromise this information, requires physical access to the card. To eavesdrop on normal activities of the module, while it is still in possession of either the Cryptographic Officer or of the User, will be demonstrated to be difficult or impossible due to the protocols and security mechanisms protecting access to the module's information and services. To eavesdrop on the module through extraordinary means requires physical possession of the card. In this event, the absence of the card is detected by either the Cryptographic Officer or the User and the capabilities of the card within a larger systems context can be disabled.

If the module is attacked through physical means, the attack will be evident due to the disturbance of the packaging of the card and module. The ICC is embedded within an epoxy coating that is extremely difficult to penetrate without leaving evidence of the attack. Further, the packaging itself is resistant to penetration.

The RENESAS AE46C1 smart card controller provides strong enclosure by coating module components in an epoxy. Physical removal of the epoxy will cause serious damage to the ICC such that all CSPs are destroyed.

The module has been tested for and meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for home use as defined in Subpart A of FCC Part 15.

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 3.

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 3 - FIPS 140-2 Logical Interfaces

Additionally, the eight contacts of the faceplate can be mapped to the logical interfaces as depicted in Table 4.

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 4 - Contact to Function Mapping

As described in ISO 7816-2, when the module is first inserted into the reader (also referred to as the terminal), a RST signal is transmitted to contact C2. Power is applied via contact C1; C7 is set to reception mode; and the external clock is established via contact C3. The I/O interface (C7) has reception and transmission modes. The smart card reader sends commands to the module and the module transmits responses using contact C7.

Sm@rtCafé Expert FIPS 64 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 is considered as a single chip implementation of a cryptographic module.

The cryptographic boundary for Sm@rtCafé Expert FIPS 64 is the single chip micro-controller, coated in epoxy, with an attached faceplate. The chip is providing the physical boundary.

2.3 Finite State Machine Model

The card's system software undergoes a set of well-defined state transitions, as keys are stored on the card to establish Security Domains. Applets also progress through a set of well-defined state transitions as they are loaded, installed, and prepared for execution.

The Finite State Model for the Sm@rtCafé Expert FIPS 64 is published as a separate document.

2.4 Software Security

The firmware for the Sm@rtCafé Expert FIPS 64 is protected from modification due to the fact that it is stored in ROM. This systems software is written primarily using a high-level programming language and the machine language specific to the underlying chip that allows for performance increase or to enhance security of the module.

It is loaded onto the module during manufacturing and does not allow for modification. An Error Detection Code (EDC) is calculated over the firmware during this installation and is checked at each power up. Attempts to modify the firmware require direct access to the IC and are prevented by the physical security described in section 2.2 above.

The card systems software includes an on-card Java Card Virtual Machine. Applets are isolated from each other due to the fact that each runs in a "Java sandbox". The Java Card language does not contain any constructs that allow cross-sandbox communication directly; any such communication must go by way of systems software mechanisms, which allow for implementation of strict security measures.

Each applet is loaded on the card within a Secure Channel which is protected by a TDES MAC. Sm@rtCafé Expert FIPS 64 also provides a Data Authentication Pattern for each loaded applet. This insures that the chip issuer has digitally signed each applet that is to be loaded on the chip, allowing prior security verification of each applet and avoiding the loading of any unauthorized applet during the manufacturing process.

During the manufacturing process, only trusted (tested against FIPS 140-2) applets are loaded onto the chip. These include the Card Manager applet and the G&D Security Domain.

After completion of the manufacturing process (including pre-personalization) when the chip has reached its normal Operating Life Cycle State (Card Manager Secured State), only trusted FIPS 140-2 validated applets shall be loaded or installed onto the module. Furthermore, at the time of loading, these applets must be identified as part of the cryptographic module. If a non-validated applet is loaded on the card, the FIPS 140-2 validation of the card no longer holds

2.4.1 Command Structure

Sm@rtCafé Expert FIPS 64 provides a well-defined, static set of commands. A smart card reader sends these commands to the module and then responses are transmitted from the module to the reader. Only these commands are available to an operator, and only the faceplate interface may be used to access the module's functionality.

The details of these commands are defined in the Sm@rtCafé Expert FIPS 64 Technical Specification Document that is included as a proprietary and private extension to this Sm@rtCafé Expert FIPS 64 Policy document.

This card also provides an additional set of on-card services through the Java Card APIs. The API classes and their associated methods are also defined in Sm@rtCafé Expert FIPS 64 Technical Specifications. These services are only available internally, to an applet loaded on the card. They cannot be accessed from outside the module

3. ROLES & SERVICES

3.1 Roles

The Sm@rtCafé Expert FIPS 64 cryptographic module supports two roles: the Cryptographic Officer (CO) and the User.

- ***The Cryptographic Officer:*** is the on-card security controller and establishes his identity on the Sm@rtCafé Expert FIPS 64 module in TDES verification of a key set stored with the Card Manager application. Through mutual authentication between the Cryptographic Officer and the Card Manager a secure channel will be established so that access to security-critical information and services can be granted. The Card Manager applet is the Card Issuer Security Domain.

- ***The User/Applet provider*****:** The module supports a User role that has possession of the G&D Security Domain keyset and can request services provided by the G&D Security Domain instantiated on the card. The CO is responsible for instantiating the G&D Security Domain and thereby defining User roles. Upto 127 G&D Security Domain instances can be created if memory resources permit.

3.1.1 Identity based Authentication

- ***Identification.*** The module supports a single identity: the Card Manager Security Officer who can assume both the CO and User role. The operator identifies himself by selecting his application and the key set inside the application. The application of the Cryptographic Officer is the Card manager. The application of the User/Applet provider is the G&D Security Domain. The selection of the application is done by a SELECT command.

  The selection of the key set is done in the INITIALIZE UPDATE, the first command of the two commands that open the Secure Channel.

- ***Authentication.*** The operator authenticates himself using a mutual authentication scheme comprising two commands INITIALIZE UPDATE and EXTERNAL AUTHENTICATE. During this mutual authentication, the operator has to encrypt and TDES MAC a challenge sent by the card, proving knowledge of the TDES key set which was referenced during the identification.

  Dedicated services are provided by the Sm@rtCafé Expert FIPS 64 module to manage the CardHolder PIN (GlobalPIN). Please note that the module provides functionality to change/unblock Global PIN. However, the module does not use the Global PIN to provide authentication to its users. Any applets loaded on the card may use this PIN for authenticating Card Holders as end-users of the Sm@rtCafé Expert FIPS 64.

3.2 Services

3.2.1 Crypto Officer Administrative Services

The Crypto Officer uses a command set for the administration of the G&D Security Domains and to load applets onto the Sm@rtCafé Expert FIPS 64 module. This command set includes the following commands

- **DELETE ALL**: 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.
- **GET STATUS**: if the Card Manager is the current application, this command is used to retrieve Card Manager information according to a given search criteria.
- **PIN CHANGE** / **UNBLOCK:** this command replaces or unblocks the Global PIN (Card Holder PIN).
- **SET STATUS**: this command is used to modify the life cycle state of the Sm@rtCafé Expert FIPS 64 module or the life cycle state of an application.

Applets loaded onto the Sm@rtCafé Expert FIPS 64 module post-issuance must be FIPS 140-2 validated.

Applets are loaded through a Secure Channel established by the Crypto Officer with the Card Manager during the Identification/authentication process. The applet is divided in a series of blocks that fit in a LOAD command. The loading is managed in a series of LOAD commands, each one transmitting a block, encrypted and followed by a TDES MAC with the Secure Channel session keys established during the identification process. The correct transmission of each block of the applet and therefore of the whole applet is ensured by the TDES MAC.

Optionally a mechanism called “OP DAP” enables the applet provider to check that his applet has been correctly loaded independently of the Issuer. The DAP verification consists of a series of DES MAC verification, ended by a TDES MAC verification. All the DES and TDES MAC operations use the”OP DAP” TDES key, loaded in the G&D Security Domain.

3.2.2 Crypto Officer & User services

The following commands are available for both the Crypto Officer and the User:

• ***INSTALL (CO):*** the INSTALL command instructs a Security Domain or the Card Manager which installation step it shall perform during an application installation process.

• ***LOAD (CO):*** the LOAD command loads the byte-codes of the Load File (package) defined in the previously issued INSTALL command.

• ***DELETE :*** the DELETE command deletes a Load File (package) or an Application (applet instance).

• **EXTERNAL AUTHENTICATE**: this command is used by the Sm@rtCafé Expert FIPS 64 module to authenticate the host, 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 command is used to store or replace one tagged data object provided in the command data field.

• **PUT KEY**: this command is used to add, replace or modify a single key or key sets.

3.2.3 Unauthenticated services:

- **MANAGE CHANNEL**: This command is used to open or close a logical channel
- **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 AUTHENTICATE.
- **SELECT**: this command is used for selecting an application (Card Manager or G&D Security Domain).
- **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.
- **INITIALIZE UPDATE**: this command is used to initiate a Secure Channel with the Card Manager or a Security Domain. Sm@rtCafé Expert FIPS 64 module and host session data are exchanged, and session keys are generated by the Sm@rtCafé Expert FIPS 64 module upon completion of this command. However, the Secure Channel is not considered open until completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command.

A user can initiate module self-tests by issuing a card reset and issuing an APDU command. The module provides a Get ATR service to retrieve the module ATR value on power-up

All commands (except Manage Channel, Select, Initialize update, Get Free Space and Get Data) need a secured channel to be executed by either a CO or User. During the secure channel opening, the command access condition is specified ('CLEAR','MAC','MAC+ENC') and an access control is done on received commands.

3.2.4 Relationship between Roles & Services

Roles/Services	Crypto –Officer (Card Manager Security Domain)	User/Applet Providers (G&D Security Domain)	Unauthenticated (Any role)
INSTALL	X	X	
LOAD	X	X	
DELETE	X	X	
DELETE ALL	X		
EXTERNAL AUTHENTICATE	X	X	
GET DATA			X
GET FREE SPACE			X
GET STATUS	X		
INITIALIZE UPDATE			X
PIN CHANGE/UNBLOCK	X		
PUT DATA	X	X	
PUT KEY	X	X	
SELECT			X
MANAGE CHANNEL			X
SET STATUS	X		

Table 5 Relationship between Roles & Services

3.2.5 Applets Services

Applets that are developed and downloaded onto the Sm@rtCafé Expert FIPS 64 module shall use the Sm@rtCafé Expert FIPS 64 Java Card APIs. These APIs are listed in a detailed separate proprietary document and are only accessible by on-card applets. The APIs containing cryptographic services are:

- Key Generation/Exchange:

  - RSA key pair generation: this API generates a pair of RSA keys.

  - Key exchange: the RSA algorithm API supports key wrapping/unwrapping.

  - DSA key pair generation: this API generates a pair of DSA keys as per FIPS 186-2.

- Message Digest:

  - SHA-1: this API performs a SHA -1 Message Digest.

- Random Numbers Generation:

  - Secure Random Generation: this API generates a random data, using output from the ANSI X9.31 FIPS140-2 approved method (Deterministic RNG) xored

with random data generated by Hardware Random Generator (Non-Deterministic RNG) provided by the chip.

- Signature and Verification:

  - RSA using SHA-1. Origin authentication and Data integrity verification:

  - DSA using SHA-1.- Origin authentication and Data integrity verification:

  - DES/TDES MAC: these APIs offer DES or TDES MAC in CBC and ECB modes with various padding (no padding, PKCS5, ISO9797 M1 and M2).

- Encryption/Decryption:

  - DES/TDES/AES: these APIs offer DES/TDES/AES encryption and decryption services using CBC or ECB mode using various padding (no padding, PKCS5, ISO9797 M1 and M2).

  - RSA: [1]these APIs offer RSA up to keylength of 2048-bit using various padding (no padding, PKCS1, ISO14888 and ISO9796).

The above stated algorithms shall be used only in a FIPS approved mode of operation and their use will be tested during the applet's FIPS 140-2 validation.

The OP specification defines various OP APIs that may be used by the applets and that provide the same services as the Card Manager Commands (such as secure channel opening). In particular, the Global PIN verification may be implemented by the applets through the use of a dedicated API

3.2.6 Card Cryptographic Functions

The cryptographic module provides a FIPS approved platform for applets that provide cryptographic services to end -user applications.

FIPS 140-2 validated algorithms in the Sm@rtCafé Expert FIPS 64 cryptographic module provide cryptographic services; these include:

• **DES**:

  • DES is used together with TDES as a MAC. It enables the Applet Provider to verify the correct loading of the applet during DAP verification. The algorithm is a series of DES terminated by a TDES as described in OP 2.0.1' **[GPCS]**.

  • DES and DES MAC functions are also provided as services to applets, through JavaCard APIs. They shall be used only for legacy systems.

[1] RSA Encrypt/Decrypt should only be used for key transport (key wrapping/unwrapping) in an Approved mode

- **TDES (2 key TDES)**:
  - The TDES (CBC mode) algorithm is used
    - for authenticating the Crypto Officer (EXTERNAL AUTH command)
    - for encrypting data flow from the host to the card. The reverse direction is not encrypted; i.e. the data and the status words returned in response to an APDU are not encrypted.
    - As a TDES MAC to authenticate the originator and to verify the integrity of the message
  - TDES MAC is also used together for DAP verification
  - TDES and TDES MAC functions are also provided as services to applets, through JavaCard APIs.
- **AES (128, 192 and 256-bit key-sizes)**:
  - AES functions are only provided as services to applets, through JavaCard APIs.
- **SHA-1**:
  - The SHA-1 function is only provided as a service through Java APIs to applets.
- **RSA PKCS#1 (1024-2048 bit keys)**:
  - RSA Signature Verification services are used during DAP verification.
  - RSA Sign/Verify functions are only provided as services to applets, through JavaCard APIs. The applet shall use RSA only for key wrapping/unwrapping or signature generation/verification.
- **DSA (512, 768 and 1024 bit key sizes)**
  - DSA Sign/Verify is only provided as as services to applets, through JavaCard APIs

3.2.7 RNG

The cryptographic module offers a Secure RNG implementation in which the output from a FIPS approved PRNG compliant with ANSI X9.31 standard (Appendix A.2.4) xored with random data generated by Hardware Random Generator of the chip.

3.3 Critical Security Parameters (CSP):

3.3.1 Cryptographic Keys

The Sm@rtCafé Expert FIPS 64 cryptographic module includes the following keys:

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))

4. G&D Security Domain TDES keys (SDK_{ENC}, SDK_{MAC} and SDK_{KEK}) used for User authentication as per the OP specficiations

5. Secure Channel Session TDES keys (SDK_{SMAC} and SDK_{SENC} derived from G&D Security Domain keys set(s))

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. Delegated Management RSA key K_{Token} for Token verification to check if Delegated Management command is authorized by Crypto Officer.

8. Delegated Management TDES key $K_{Receipt}$ for Receipt generation to prove successful execution of Delegated Management command.

The keys 1 & 2 are put into the Crypto Officer Security Domain key sets, using the Put Key command.

The keys 3 & 5 are temporary keys stored in RAM.

The keys 4,6, 7 & 8 are put in the G&D Security Domains, using the Put Key command.

A Security Domain (Card Manager and G&D Security Domain) key set is structured as to contain three types of TDES keys:

• $K_{enc,auth}$ – 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.

3.3.2 Other CSPs

The Sm@rtCafé Expert FIPS 64 cryptographic module includes another type of CSP:

• A Global Personal Identification Number (PIN),

The Global PIN is a 6-12 character (numeric) string that may be used (through a dedicated OP API) to authenticate the Cardholder to the Sm@rtCafé Expert FIPS 64 module. A cardholder can prove knowledge of a shared secret (the PIN) by successfully entering a PIN sequence and thereby authenticate himself to the Sm@rtCafé Expert FIPS 64 module. Please note that the module provides functionality to change/unblock Global PIN. However, the module does not use the Global PIN to provide authentication to the Crypto Officer and User roles. Any applets loaded on the card post-issuance may use this PIN for authenticating Card Holders by using a dedicated on-card API.

- TDES PRNG key: This 112-bit key is used by the ANSI X9.31 PRNG implementation

4. SECURITY RULES

4.1 Identification & Authentication Security Rules

Sm@rtCafé Expert FIPS 64 implements Identity-based Access Control Rules for identifying and authenticating the Crypto Officer and the User/Applet Provider role.

• **User/Applet Provider Authentication:** The User/Applet Provider must prove possession of the G&D Security Domain keyset composed of 3 TDES keys (SDK_{ENC}, SDK_{MAC} and SDK_{KEK}). SDK_{ENC}, SDK_{MAC} are used to derive the session keys used to encrypt, authenticate and check the integrity of the command data. SDK_{KEK} is used to encrypt keys transported within the APDU command. This is the same process as the Crypto Officer authentication (Initialize Update & External Authenticate commands) but it uses the TDES keys of the G&D Security Domain.

4.1.1 Cryptographic Officer Identification &Authentication

• **Crypto Officer Authentication:** The Cryptographic Officer must prove possession of the Card Manager Key Set composed of 3 TDES keys (K_{ENC}, K_{MAC} and K_{KEK}). K_{ENC}, K_{MAC} are used to derive the session keys used to encrypt, authenticate and check the integrity of the command data. K_{KEK} is used to encrypt keys transported within the APDU command. This is the same process as the User authentication (Initialize Update & External Authenticate commands) and follows the OP 2.0.1' specfications **[GPCS]**.

4.2 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.

4.2.1 "OP Delegated Management"

If Delegated Management is used, the Crypto Officer has to set Delegate Management Keys for Token verification (K_{Token}) and Reciept 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 reciept, i.e. a TDES MAC generated by the Card, acknowledging that the operation was successfully performed. For details see OP 2.0.1' **[GPCS]**.

4.2.2 "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.

4.3 Access Control Security Rules

• Keys must be loaded through a secure channel and encrypted with the K_{kek}. Therefore the keys are always loaded in encrypted form.

• Global PIN is set through a secure channel and encrypted with the K_{kek}. Therefore is always transferred in encrypted form.

4.4 Physical Security Rules

The physical security of the Sm@rtCafé Expert FIPS 64 cryptographic module 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. Once it is manufactured, the Sm@rtCafé Expert FIPS 64 module belongs to the Cryptographic Officer until it is ultimately issued to the end user.

4.5 Key Management Security Policy

4.5.1 Cryptographic key generation

-TDES Session key derivation for Secure Channel, conforming to Open Platform Card Specification v2.0.1' **[GPCS]**. The random data required for opening a Secure Channel is generated using the FIPS140-2 approved ANSI X9.31 PRNG **[X9.31]** xored with random data generated by Hardware Random Generator of the chip.

- RSA and DSA key pair generation using FIPS140-2 approved ANSI X9.31 PRNG **[X9.31]** xored with random data generated by Hardware Random Generator of chip.

4.5.2 Cryptographic key entry/output

If Keys are imported they shall always be encrypted with the KEK and transferred by using the Put Key command within a secure channel.

During this process, the keys are double encrypted (using the Session Key K_{enc} and the KEK) if the Secure Channel security level is set to MAC+ENC.

4.5.3 Cryptographic key storage

The Keys contain the following parameters:

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

4.5.4 Cryptographic key destruction

The Sm@rtCafé Expert FIPS 64 module replaces initialitzation Key K_{init} 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. 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 them with new values using the Put Key command or using the Delete command.

The Global PIN can be zeroized by overwriting with a new value.

Key Management Details can be found in section 6.

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

4.6 Approved mode

The cryptographic module enforces FIPS mode of operation at all times. However, the module provides certain non-Approved functions as internal services to applets loaded on the card via the JavaCard API. These services are not accessbile to an external

user. It is the responsibility of the applet to not use these functions in an Approved mode. This will also be checked during the applet's FIPS 140-2 validation. Please note that only FIPS 140-2 valdidated applets can be loaded on the card.

The non-Approved functions provided by the card are:

- RSA Encrypt/Decrypt
- RSA 1984-bit and 2048-bit Sign/Verify
  (for firmware version CH463JC_INABFOP003901_V102 only)

The ATR value returned by the module during power-up serves as an Approved mode indicator. The ATR returned by Sm@rtCafé Expert FIPS 64,version CH463JC_INABFOP003901_V101 is:

ATR = 3B FD 18 00 FF 80 B1 FE 45 1F 07 80 73 00 21 13 57 4A 54 48 61 31 4A 00 52

The ATR returned by Sm@rtCafé Expert FIPS 64, version CH463JC_INABFOP003901_V102 is:

ATR: 3B FD 18 00 FF 80 B1 FE 45 1F 07 80 73 00 21 13 57 4A 54 48 61 31 47 00 5F

The only difference between the two versions is that for the card with firmware version CH463JC_INABFOP003901_V102 an RSA power-up KAT is not performed on the software implementation and thus RSA Sign/verify cannot be performed using 1984-bit and 2048-bit keys in the Approved mode. For the card with firmware version CH463JC_INABFOP003901_V101, a power-up self-test is performed and thus the card can be used for RSA Sign/Verify operations using 1984-bit and 2048-bit keys in the Approved mode.

In both versions RSA Encrypt/Decrypt can only be used for performing key transport (key wrapping/unwrapping) in the Approved mode.

5. SECURITY POLICY CHECK LIST TABLES

5.1 ROLES & REQUIRED AUTHENTICATION

Role	Type of authentication	Authentication data
Crypto Officer	TDES authentication	TDES keys (Crypto Officer Security Domain)
User/Applet Provider	TDES authentication	TDES keys (G&D Security Domain)

Table 6 Roles and required authentication

5.2 STRENGTH OF AUTHENTICATION MECHANISMS

Authentication Mechanism	Strength of Mechanism
TDES authentication	Probability that a random attempt succeeds is less than 1 in 1,000,000

Table 7 Strength of authentication mechanisms

5.3 SERVICES AUTHORIZED FOR ROLES

Role	Authorized Services
Crypto Officer	All CO Services as listed in Section 3.2.1 and 3.2.2
User/Applet Provider	Only User Services as listed in Section 3.2.2

Table 8 Services authorized for roles

5.4 ACCESS RIGHTS WITHIN SERVICES

CSP	Service	Role	Types of Access
TDES CO keys: K_{ENC}, K_{MAC}, K_{KEK}, K_{Token}, $K_{Receipt}$	PUT KEY command	Crypto Officer	Write
TDES CO Keys: K_{ENC}, K_{MAC}	INITIALIZE UPDATE & EXTERNAL AUTH	Crypto Officer	Execute
TDES CO Key: K_{KEK}	PUT KEY, PIN CHANGE/UNBLOCK commands (encryption of the loaded Key or PIN)	Crypto Officer	Execute
TDES CO Session Keys: K_{SENC}, K_{SMAC}	INITIALIZE UPDATE & EXTERNAL AUTH	Crypto Officer	Create
TDES CO Session Key: K_{SENC}	Message encryption	Crypto Officer	Execute
TDES CO Session Key: K_{SMAC}	Message integrity	Crypto Officer	Execute
TDES User Keys: SDK_{ENC}, SDK_{MAC}, SDK_{KEK}, K_{DAP}	PUT KEY command	User	Write
TDES User Keys: SDK_{ENC}, SDK_{MAC}	INITIALIZE UPDATE & EXTERNAL AUTH	User	Execute
TDES User Key: K_{SDKEK}	PUT KEY command (encryption of the loaded Key)	User	Execute
TDES User Session Keys: SDK_{SENC}, SDK_{SMAC}	INITIALIZE UPDATE & EXTERNAL AUTH	User	Create
TDES User Session Key: SDK_{SENC}	Message encryption	User	Execute
TDES User Session Key: SDK_{SMAC}	Message integrity	User	Execute
"OP DAP" TDES Key: K_{DAP}	PUT KEY command	Crypto Officer	Write
"OP DAP" TDES Key: K_{DAP}	LOAD command (MAC verification by G&D Security Domain)	Crypto Officer and User	Execute
Delegated Management TDES key $K_{Receipt}$	PUT KEY command	Crypto Officer	Write
Delegated Management TDES key $K_{Receipt}$	LOAD command	Crypto Officer	Execute
Global PIN	PIN CHANGE/UNBLOCK command	Crypto Officer	Write
TDES PRNG key	INITIALIZE UPDATE command and RSA, DSA key generation	Crypto Officer and User	Execute

Table 9 Access rights within services

6. CRYPTOGRAPHIC KEY MANAGEMENT

The Sm@rtCafé Expert FIPS 64 with Applets smart card includes the following keys:

- Initialization Key, K_{init} used only for the first Card Manager key-set loading.

- Security Domain (Card Manager and G&D Security Domain) key sets each containing three TDES keys stored in EEPROM. Each key is 112-bits.

    1. K_{enc} used for Cryptographic Officer or User authentication per OP Specification

    2. K_{mac}, used for Cryptographic Officer or User authentication per OP Specification

    3. K_{kek} used as Key Wrapping Key for encrypting keys input into the module using the Put Key command

- Secure Channel session keys SMAC and SENC. These are 112-bit TDES keys stored in RAM

- "OP DAP" TDES key, a 112-bit TDES key used for DAP verification using TDES MAC.

- "OP DAP" RSA key, a 1024-bit public key used for DAP verification using RSA signature verification.

- TDES PRNG key used with FIPS140-2 approved ANSI X9.31 PRNG **[X9.31]** is generated using Hardware Random Generator of chip during initialization.

- Delegated Management 1024-bit RSA key K_{Token} for Token verification to check if Delegated Management command is authorized by Crypto Officer.

- Delegated Management 112-bit TDES key $K_{Receipt}$ for Receipt generation to prove successful execution of Delegated Management command.

All keys can be zeroized by setting the card state to TERMINATED.

6.1 Standards-Based Cryptography

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)

- 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)[2]

Pseudo Random Number Generation:

- PRNG based on ANSI X9.31 [X9.31] Appendix A.2.4

6.2 Non FIPS-approved algorithms

- RSA encryption/decryption[3]

[2] For card with firmware version CH463JC_INABFOP003901_V101 RSA Sign/Verify operations using 1984 and 2048-bit key sizes are considered non-Approved since a corresponding self-test is not performed
[3] RSA Encrypt/Decrypt can be used for key transport in an Approved mode of operation

7. SELF-TESTS

The Sm@rtCafé Expert FIPS 64 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. The self-tests include:

Software Integrity Tests: The module checks the integrity of its firmware:

- **ROM:** 16 bit Checksum
- **Firmware in EEPROM:** 24 bit MAC using a Generalized Hamming Code
- **Java Code in EEPROM:** 32 bit MAC using a Reed Solomon algorithm

Cryptographic Algorithm KATs: Known Answer Tests (KATs) are run at power-up for the following algorithms:

- **DES KAT**
- **Triple-DES KAT**
- **DES MAC KAT**
- **Triple-DES MAC KAT**
- **AES KAT**
- **DSA Sign/Verify test**
- **RSA KAT** on the hardware implementation
- **RSA KAT** on the software implementation using a 2048-bit CRT key is performed only on the module with firmware version CH463JC_INABFOP003901_V101
- **ANSI 9.17 Software RNG KAT**

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 a DSA key pair, the module performs a sign/verify with that key pair to ensure that the key pair is correct.
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 continous comparison and never used for any service like cryptographic calculations. If generated numbers are equal to previous generated numbers, this selftest fails.

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' **[GPCS]**.

8. MITIGATION OF ATTACKS

The 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.

9. ACRONYMS

ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
ATR	Answer-To-Reset
CBC	Cipher-Block Chaining
CSP	Critical Security Parameter
CO	Crypto Officer
CRT	Chinese Remainder Theorem
Dap	Data Authentication Pattern
DES	Data Encryption Standard
DPA	Differential Power Analysis
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMV	Europay Mastercard and Visa
EEPROM	Electrically Erasable Programmable ROM
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
G&D	Giesecke & Devrient
GHC	Generalized Hamming Code
I/O	Input/Output
IC	Integrated Circuit
ISO	International Organization for Standardization
JCRE	Java Card ™ Runtime Environment
KAT	Known Answer Test
MAC	Message Authentication Code
MD5	Message Digest algorithm 5
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OP	Opem Platform
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PRNG	Pseudo Random Number Generator
PUK	Personal Unblocking Key
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest Shamir and Adleman
RST	Reset
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis