# Contents

1 Introduction 5  
1.1 Purpose 5  
1.2 References 5  
1.3 Document Organization 7  

2 Cryptographic Module Specification 8  
2.1 Overview 8  
2.2 Cryptographic Algorithms 8  
2.3 Physical Security with Well-Defined Interfaces 9  
   2.3.1 Security Level 9  
   2.3.2 The NXP P5Cx081 and P5CD145 smart card controllers 10  
   2.3.3 The Physical Security 13  
   2.3.4 The Contact Interface 13  
   2.3.5 The Contactless Interface 14  
   2.3.6 The Cryptographic Boundary 14  
2.4 Finite State Model 14  
2.5 Firmware Security 14  
2.6 Command Structure 15  

3 Roles and Services 16  
3.1 Roles 16  
   3.1.1 Identity-based Authentication 16  
3.2 Services 16  
   3.2.1 Crypto Officer Administrative Services 17  
   3.2.2 Crypto Officer Services and User Services 17  
   3.2.3 Unauthenticated Services 18  
   3.2.4 Relationship between Roles and Services 18  
   3.2.5 Applet Services 19  
   3.2.6 Cryptographic Functions 20  
   3.2.7 Random Bit Generator 20  
3.3 Critical Security Parameters (CSP) 20  

4 Security Rules 23  
4.1 Identification and Authentication Security Rules 23  
4.2 Applet Loading Security Rules 23  
   4.2.1 GP Delegated Management 23  
   4.2.2 GP DAP 23  
4.3 Access Control Security Rules 24
4.4 Physical Security Rules 24
4.5 Key Management Security Policy 24
   4.5.1 Cryptographic key generation 24
   4.5.2 Cryptographic key entry/output 24
   4.5.3 Cryptographic key storage 24
   4.5.4 Cryptographic key zeroization 25
4.6 Approved mode 25

5 Security Policy Check List Tables 27
   5.1 Roles and Required Authentication 27
   5.2 Algorithm Strengths 27
   5.3 Strength of Authentication Mechanisms 27
   5.4 Services Authorized for Roles 27
   5.5 Mitigation of Other Attacks 27
   5.6 Access Rights within Services 28

6 Cryptographic Key Management 29

7 Standards-Based Cryptography 30
   7.1 FIPS approved algorithms 30
   7.2 The non-FIPS approved algorithms 30
   7.3 Other algorithms allowed in FIPS mode 30
   7.4 Self-Tests 31
      7.4.1 Power-Up Tests 31
      7.4.2 Conditional Tests 31
      7.4.3 Module behaviour upon self-test failure 32

8 Mitigation of Attacks 33

9 Acronyms 34
1 Introduction

1.1 Purpose

This is a non-proprietary Security Policy for the Giesecke & Devrient (G&D) cryptographic module Sm@rtCafé Expert 6.0. This Security Policy describes how the cryptographic module meets the security requirements applicable to Level 3 of FIPS 140-2 [FIPS 140-2] and accompanying cryptography-based standards and how to run it in FIPS-Approved mode.


1.2 References


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 14443-3: 2001, Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3:
Initialization and anticollision


[RSA PKCS#1 v2.1] RSA Laboratories, PKCS#1 v2.1: RSA Cryptography Standard, June 14, 2002.

1.3 Document Organization

This Security Policy is one document in a FIPS 140-2 submission package. In addition to this document, the submission package contains:

- The Vendor Evidence document
- The Finite State Machine Model
- The Sm@rtCafé Expert 6.0 Reference Manual, [SCE60 RefMan]
- Other supporting documentation

This Security Policy and the other validation submission documentation were 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 Cryptographic Module Specification

2.1 Overview

Sm@rtCafé Expert 6.0 is a single-chip cryptographic module. The firmware is implemented on three different NXP smart card controllers (see Section 2.3.2).

Table 1 identifies the validated product configurations.

<table>
<thead>
<tr>
<th>Product Model Name</th>
<th>FW Image Name</th>
<th>Tested Hardware Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sm@rtCafé Expert 6.0</td>
<td>Sm@rtCafé Expert 6.0</td>
<td>NXP P5CD081, dual interface: ISO 7816 contacts, ISO 14444-3 contactless</td>
</tr>
<tr>
<td>Sm@rtCafé Expert 6.0</td>
<td>Sm@rtCafé Expert 6.0</td>
<td>NXP P5CD145, dual interface: ISO 7816 contacts, ISO 14444-3 contactless</td>
</tr>
<tr>
<td>Sm@rtCafé Expert 6.0</td>
<td>Sm@rtCafé Expert 6.0</td>
<td>NXP P5CC081, ISO 7816 contact only, SSOP20 package (SMD)</td>
</tr>
</tbody>
</table>

Hardware Versions: P5CC081, P5CD081, P5CD145

Firmware Version: Sm@rtCafé Expert 6.0

Providing a complete set of International Organization for Standardization (ISO), Europay, MasterCard and Visa (EMV), and GlobalPlatform commands, the Sm@rtCafé Expert 6.0 incorporates standards- and specifications-based functionality along with a proprietary command set.

The firmware is a Classic Edition Java Card 3 Platform ([JCAPI], [JCRE], [JCVM]) that implements the GlobalPlatform (GP) Card Specification Version 2.1.1 ([GPCS2.1.1]) and the Secure Channel Protocol 03 specified in Amendment D to GlobalPlatform Card Specification Version 2.2, ([GP2.2, Amendment D]). The GP specifications define a secure infrastructure for post-issuance programmable smart cards and a life cycle for GP compliant products.

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

The module can load applets post-validation, FIPS 140-2 validated or not. If a non-validated applet is loaded, the FIPS 140-2 validation of the module is no longer valid.

2.2 Cryptographic Algorithms

The cryptographic module implements the following cryptographic algorithms:
<table>
<thead>
<tr>
<th>Name of the Algorithm</th>
<th>Approved</th>
<th>Allowed</th>
<th>Non-approved</th>
<th>Supported by the module (yes / no)*</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES with 128, 192, and 256 bits key lengths, ECB and CBC modes, Cert. #1755</td>
<td>x</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>3-key Triple-DES and 2 key Triple-DES, ECB and CBC modes, Cert. #1136</td>
<td>x</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>RSA with up to 2048 bits modulus length, Cert. #874</td>
<td>x</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>RSA CRT with up to 2048 bits modulus length, Cert. #874</td>
<td>x</td>
<td></td>
<td></td>
<td>no</td>
</tr>
<tr>
<td>ECDSA in GF(p) with P=192, P=224 and P=256 curves, Cert. #232</td>
<td>x</td>
<td></td>
<td></td>
<td>no</td>
</tr>
<tr>
<td>SHA-1, Cert #1542</td>
<td>x</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>SHA-224, SHA-256, SHA-384, and SHA-512 hash functions, Cert. #1542</td>
<td>x</td>
<td></td>
<td></td>
<td>no</td>
</tr>
<tr>
<td>CMAC</td>
<td>x</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>Triple-DES MAC</td>
<td>x</td>
<td></td>
<td></td>
<td>no</td>
</tr>
<tr>
<td>DRBG (Deterministic Random Number Generator), Cert. #116</td>
<td>x</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>ECDH Key Agreement</td>
<td>x</td>
<td></td>
<td></td>
<td>no</td>
</tr>
<tr>
<td>AES for key wrapping</td>
<td>x</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>TRNG (non-deterministic hardware RNG, used for seeding the DRBG)</td>
<td>x</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>DES</td>
<td>x</td>
<td></td>
<td></td>
<td>no</td>
</tr>
<tr>
<td>DSA</td>
<td>x</td>
<td></td>
<td></td>
<td>no</td>
</tr>
<tr>
<td>RSA Encryption and Decryption</td>
<td>x</td>
<td></td>
<td></td>
<td>no</td>
</tr>
<tr>
<td>Korean SEED</td>
<td>x</td>
<td></td>
<td></td>
<td>no</td>
</tr>
<tr>
<td>RIPEMD-160</td>
<td>x</td>
<td></td>
<td></td>
<td>no</td>
</tr>
<tr>
<td>MD5</td>
<td>x</td>
<td></td>
<td></td>
<td>no</td>
</tr>
</tbody>
</table>

* “no” means that the module, as validated, does not support this algorithm. The algorithm can be used by post-validation loaded applets.

2.3 Physical Security with Well-Defined Interfaces

2.3.1 Security Level

Sm@rtCafé Expert 6.0 is a single chip cryptographic module that meets FIPS 140-2 Level 3 requirements as indicated in Table 2.

Table 2 Module Security Level Specification

<table>
<thead>
<tr>
<th>Security Requirements Section</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic Module Specification</td>
<td>3</td>
</tr>
<tr>
<td>Module Ports and Interfaces</td>
<td>3</td>
</tr>
<tr>
<td>Finite State Model</td>
<td>3</td>
</tr>
<tr>
<td>Physical Security</td>
<td>3</td>
</tr>
<tr>
<td>Operational Environment</td>
<td>N/A</td>
</tr>
<tr>
<td>Roles, Services, and Authentication</td>
<td>3</td>
</tr>
<tr>
<td>Cryptographic Key Management</td>
<td>3</td>
</tr>
</tbody>
</table>
2.3.2 The NXP P5Cx081 and P5CD145 smart card controllers

Sm@rtCafé Expert 6.0 is available on three different NXP smart card controllers. The following table lists the main differences.

<table>
<thead>
<tr>
<th>Security Requirements Section</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMI/EMC</td>
<td>3</td>
</tr>
<tr>
<td>Self-tests</td>
<td>3</td>
</tr>
<tr>
<td>Design Assurance</td>
<td>3</td>
</tr>
<tr>
<td>Mitigation of Other Attacks</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>P5CC081</th>
<th>P5CD081</th>
<th>P5CD145</th>
</tr>
</thead>
<tbody>
<tr>
<td>EEPROM size</td>
<td>80 KB</td>
<td>80 KB</td>
<td>144 KB</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Contact interface</td>
<td>Dual Interface (contact and contactless)</td>
<td>Dual Interface (contact and contactless)</td>
</tr>
</tbody>
</table>

The functional diagram for NXP P5CD081 controller is depicted in Figure 1. The functional diagram for NXP P5CD145 controller is depicted in Figure 4. The functional diagram for NXP P5CC081 controller is depicted in Figure 5.

The controller contains the processor, Read Only Memory (264 KB), Random Access Memory (7680 B), Electrically Erasable Programmable ROM (80 KB for NXP P5Cx081, 144 KB for NXP P5CD145), co-processors, I/O, and timers. The power interface accepts voltages in the range of +5V +/-10% and +1.8V +/-10%.

The NXP controllers are secure ISO/IEC 7816 dual-interface and contact PKI smart card controllers providing the following security features:

- Low and high clock frequency sensor
- Low and high temperature sensor
- Low and high supply voltage sensor
- Single Fault Injection (SFI) attack detector
- Light sensors (including Integrated memory light sensor functionality)

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 controllers have been tested for and meet applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for home use as defined in Subpart B of FCC Part 15.

The P5CD081 and P5CD145 modules are each composed of a single chip micro-controller, coated in epoxy, with an attached faceplate (Figure 3), an ISO/IEC 14443 A contactless interface and an ISO/IEC 7816 contact interface.

For the smart card form factor, the P5CC081 module is composed of a single chip micro-controller, coated in epoxy, with an attached faceplate and an ISO/IEC 7816 contact interface. For the USB token form factor, the P5CC081 module is embedded in opaque tamper-evident SSOP20 package (Figure 2) that is placed in the USB token composite enclosure.
Figure 1: Block Diagram of the NXP P5CD081

Figure 2: Picture of the SSOP20 package

Figure 3: Picture of the module faceplate
Figure 4 Block Diagram of the NXP P5CD145

Figure 5 Block Diagram of the NXP P5CC081
2.3.3 The Physical Security

For the smart card form factor, the module’s strong enclosure is achieved by opaque tamper-evident covering of the die. Physical removal of the top metal layer will cause serious damage to the cryptographic module such that all CSPs are destroyed. 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.

For the USB token form factor, opaque enclosure with visible tamper-evidence preventing probing of the module and visual inspection is provided by the SSOP20 SMD package (Figure 2).

The module hardness testing was performed over the ambient temperature range from 0°C to +80°C. The temperature testing was performed during the hardware vendor’s IC release process and as part of the IC’s Common Criteria evaluation [CertRep NXP]. No assurance is provided for Level 3 hardness conformance at any temperature beyond the range of 0°C to +80°C.

2.3.4 The Contact Interface

There is only one physical contact interface to the module, the faceplate, which contains eight contacts, pinned as defined in ISO/IEC 7816-2. All FIPS 140-2 logical interfaces map to this single faceplate as detailed in Table 3.

### Table 3 FIPS 140-2 Logical and Physical Interfaces

<table>
<thead>
<tr>
<th>FIPS 140-2 Logical Interface</th>
<th>Physical Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Input Interface</td>
<td>Faceplate, Pin pitch Faceplate, Contactless</td>
</tr>
<tr>
<td>Data Output Interface</td>
<td>Faceplate, Pin pitch Faceplate, Contactless</td>
</tr>
<tr>
<td>Control Input Interface</td>
<td>Faceplate, Pin pitch Faceplate, Contactless</td>
</tr>
<tr>
<td>Status Output Interface</td>
<td>Faceplate, Pin pitch Faceplate, Contactless</td>
</tr>
<tr>
<td>Power Interface</td>
<td>Faceplate, Pin pitch Faceplate, Contactless</td>
</tr>
</tbody>
</table>

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

### Table 4 Contact to Function Mapping

<table>
<thead>
<tr>
<th>ISO/IEC 7816 (P5C081, P5CD145)</th>
<th>Dual interface (P5CD081, P5CD145)</th>
<th>FIPS 140-2 Logical Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Symbol</td>
<td>Symbol</td>
<td></td>
</tr>
<tr>
<td>C1 VCC</td>
<td>VDD</td>
<td>Power Interface</td>
</tr>
<tr>
<td>C2 RST</td>
<td>RST_N</td>
<td>Control Input Interface</td>
</tr>
<tr>
<td>C3 CLK</td>
<td>CLK</td>
<td>Control Input Interface</td>
</tr>
<tr>
<td>C4 AUX1</td>
<td>LA</td>
<td>Data Input Interface, Data Output Interface, Control Input Interface, Status Output Interface</td>
</tr>
<tr>
<td>C5 GND</td>
<td>VSS</td>
<td>Power Interface</td>
</tr>
<tr>
<td>C6 SPU</td>
<td>N.C.</td>
<td>N/A</td>
</tr>
<tr>
<td>C7 I/O</td>
<td>IO1</td>
<td>Data Input Interface, Data Output Interface, Control Input Interface, Status Output Interface</td>
</tr>
<tr>
<td>C8 AUX2</td>
<td>LB</td>
<td>Data Input Interface, Data Output Interface, Control Input Interface, Status Output Interface</td>
</tr>
</tbody>
</table>
As described in ISO/IEC 7816-2, when the card 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 reader sends commands to the card and the card transmits responses using contact C7.

2.3.5 The Contactless Interface

The contactless interface operates in accordance with ISO/IEC 14443 A. The T=CL protocol is supported for communication between the Proximity Coupling Device (PCD) and the cryptographic module according to Part 4 of [ISO14443]. This interface is only available on the P5CD081 and P5CD145 chip types.

2.3.6 The Cryptographic Boundary

The Sn@rtCafé Expert 6.0 is a single-chip implementation of a cryptographic module. The cryptographic boundary is the single chip micro-controller providing either a dual interface (ISO/IEC 7816 contact interface and ISO/IEC 14443 A contactless interface for hardware versions P5CD081 and P5CD145) or a contact-only interface (ISO/IEC 7816 contact interface for hardware version P5CC081).

2.4 Finite State Model

The Sn@rtCafé Expert 6.0 firmware undergoes a set of well-defined state transitions. The Finite State Model for the Sn@rtCafé Expert 6.0 is provided as a separate document.

2.5 Firmware Security

The Sn@rtCafé Expert 6.0 firmware is protected from modification as it is stored in ROM of the NXP chip. This is system software written primarily using a high-level programming language and machine language that is specific to the underlying chip that allows for performance increase and enhancement of the module’s security.

The Sn@rtCafé Expert 6.0 firmware is loaded onto the chip during manufacturing. An Error Detection Code (EDC) is calculated over the firmware during the installation process and checked each time the module is powered up. Attempts to modify the firmware require direct access to the IC and are prevented by the physical security mechanisms of the IC and the enclosure listed in Section 2.3.2.

The Sn@rtCafé Expert 6.0 firmware includes a Java Card virtual machine. Applets are isolated from each other due to the fact that each runs in a “Java sandbox” as defined in the Java Card virtual machine Specification [JCVM]. The Java Card programming language does not contain any constructs that allow cross-sandbox communication directly; any such communication must go by way of system software mechanisms, which allow for implementation of strict security measures.

Each applet is loaded on the module within a Secure Channel requiring at least MAC verification over each Load Block. CMAC as specified in NIST SP 800-38B [SP 800-38B] is used for MAC calculations. Sn@rtCafé Expert 6.0 provides the Data Authentication Pattern (DAP) acc. to [GPCS2.1.1] for secure content loading.

During the manufacturing process only trusted (i.e., validated 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 Operating Life Cycle State (Card Manager SECURED State), only FIPS 140-2 validated applets shall be loaded and installed onto the module. At the time of loading, these applets must be identified as part of the cryptographic module. The FIPS 140-2 validation testing of Sn@rtCafé Expert 6.0 targeted this specific configuration. Changes to that configuration (such as loading an applet), would constitute a new module, and the new configuration would need to undergo FIPS 140-2 testing for FIPS 140-2 compliance.
2.6 Command Structure

The Sm@rtCafé Expert 6.0 firmware provides a well-defined, static set of commands. The details of these commands are defined in the Sm@rtCafé Expert 6.0 Reference Manual [SCE60 RefMan] included as a proprietary and private extension to this Security Policy.

Sm@rtCafé Expert 6.0 is only capable of operating in response to commands that are sent from the reader. The reader sends a command Application Protocol Data Unit (APDU) to the module and module responds with a response APDU, thus exchanging command-response pairs.

An APDU sent by the reader consists of a header and an optional body. The header contains a class byte differentiating between ISO defined commands and custom commands, an instruction byte containing the command code, and command-specific parameters. The command body contains data that is needed for command execution and, if necessary, followed by the length of expected response data.

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

The module provides a set of services through the Java Card API that is specified in [JCAPI] and the GlobalPlatform API [GPCS2.1.1]. The implemented Java Card package API classes are listed in Sm@rtCafé Expert 6.0 Reference Manual [SCE60 RefMan]. These services are only available internally to applets loaded and installed on the module. They cannot be accessed from outside the module.
3 Roles and Services

The module defines two distinct roles that are supported by the on-module cryptographic system, the Crypto Officer role and the User/Applet provider role.

3.1 Roles

Sm@rtCafé Expert 6.0 supports the following roles:

The Crypto Officer (CO). This role is responsible for managing the security configuration of the Card Manager and Security Domains. The CO role authenticates to the cryptographic module by demonstrating to the Card Manager application that he possesses the knowledge of a GP Secure Channel AES key set stored within the Card Manager. By successfully executing the GP mutual authentication protocol specified in [GP2.2, Amendment D], the CO role establishes a Secure Channel to the Card Manager and executes services allowed to the CO in a secure manner.

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

After it has been manufactured, Sm@rtCafé Expert 6.0 is in possession of the Crypto Officer until it is ultimately issued to the User. From that point, Sm@rtCafé Expert 6.0 is in the physical possession of the User.

3.1.1 Identity-based Authentication

Identification. The operator identifies himself by selecting his application and the key set inside the application. The application of the Crypto Officer is the Card Manager. The application of the User/Applet provider is the G&D Security Domain.

An application is selected by issuing a SELECT command.

The selection of the key set is done by issuing the INITIALIZE UPDATE command, which is the first command of the two commands required to open a Secure Channel.

Authentication. The operator authenticates himself using a mutual authentication scheme comprising two commands INITIALIZE UPDATE and EXTERNAL AUTHENTICATE. During the mutual authentication, the operator has to encrypt a challenge sent by the module and compute a MAC over the encrypted result, proving knowledge of the AES key set which was referenced during the identification process. AES keys with the following lengths are supported: 128, 192, 256 bits. The strength of authentication is assessed in Section 5.2.

Dedicated services are provided by Sm@rtCafé Expert 6.0 to manage the Card Holder PIN (Global PIN). The module provides functionality to change/unblock the Global PIN. However, the module does not use the Global PIN to provide authentication to its users. Any applet installed on the module may use this PIN for authenticating Card Holders as end-users of Sm@rtCafé Expert 6.0. In addition or alternatively to the Global PIN mechanism, applications can implement a private PIN identification mechanism.

3.2 Services

All commands (except the commands listed for unauthenticated services in Section 3.2.3) need a Secure Channel to be executed by either the CO or the User. During the Secure Channel opening, the command access condition is specified ('NO SECURITY LEVEL', 'AUTHENTICATED', 'C_MAC', 'C_DECRYPTION') and access control is done on the received command APDUs.
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 6.0. The following commands may be sent to the Card Manager / Issuer Security Domain.

**DELETE ALL** is used to delete all packages and applet instances installed from those packages that have been loaded after completion of the module via LOAD commands.

**CHANGE / UNBLOCK PIN** replaces or unblocks the Global PIN (Card Holder PIN).

Applets loaded onto the module post-issuance must be FIPS 140-2 validated. If non-validated applets are loaded, the FIPS 140-2 validation of the module is no longer valid.

Applets are loaded through a Secure Channel established by the Crypto Officer (off-card entity) with the Card Manager (on-card entity) during the mutual 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 transmitting a block that is optionally encrypted and followed by a MAC across the header and the data field of the APDU command using the Secure Channel session keys generated during the mutual authentication process. CMAC as specified in [SP 800-38B] is used for MAC calculations. AES in CBC mode as specified in [SP 800-38A] is used for encryption / decryption.

Optionally a mechanism called “GP DAP” enables the applet provider to check that his applet has been correctly loaded independently of the Issuer. The following DAP verification modes are defined in [GPCS2.1.1]:

- Single-DES plus final Triple-DES MAC
- 2-key Triple-DES MAC (referred to as “full Triple-DES MAC”)
- 1024-bits RSA SSA-PKCS1-v1_5 signature as defined in PKCS#1 applied to a SHA-1 digest of the data being signed

The DES Load File Data Block Signature verification consists of a series of DES MAC verification, ended by Triple-DES MAC verification. All the DES and Triple-DES MAC operations use the “GP DAP” Triple-DES key, loaded in the G&D Security Domain. DAP verification using this method shall not be used in FIPS approved mode, as DES is not an approved security function per [FIPS 140-2].

The “full Triple-DES MAC” is as defined in [ISO/IEC 9797-1] as MAC Algorithm 1 with output transformation 1, without truncation, and with Triple-DES taking the place of the block cipher. The full Triple-DES MAC DAP verification consists of a series of Triple-DES MAC verifications. All Triple-DES MAC operations use the “GP DAP” Triple-DES key loaded in the G&D Security Domain. Full Triple-DES MAC DAP verification is allowed in the approved mode of operation.

The RSA Load File DAP is calculated using PKCS#1 signature with padding the SHA-1 digest is according to PKCS#1 V1.5 and encrypting it with the private RSA key with 1024 bits modulus length. DAP verification using RSA is allowed in the approved mode of operation.

3.2.2 Crypto Officer Services and User Services

The following commands are available to the Crypto Officer and to the User:

**INSTALL** instructs a Security Domain or the Card Manager which installation step it shall perform during an application installation process. It may only be executed within a Secure Channel. Its level of security depends on the security level defined in EXTERNAL AUTHENTICATE.

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

**DELETE** deletes a Load File (package) or an Application (applet instance).

**EXTERNAL AUTHENTICATE** is used by the module to authenticate the host, to establish the Secure Channel, and to determine the level of security required for all subsequent commands.
within the Secure Channel. A previous and successful execution of the INITIALIZE UPDATE command is required prior to processing this command.

**PUT Key** is used to add or replace a single key or a set of keys.

**GET STATUS** is used to retrieve the life cycle data for Applications, Load Files (packages), or the Issuer Security Domain based on the search criteria defined in the APDU parameter and data fields. This command may only be executed within a Secure Channel. Its level of security depends on the security level defined in EXTERNAL AUTHENTICATE.

**SET STATUS** is used to modify the card life cycle state (by Crypto Officer only) and the life cycle state of an application (by Crypto Officer or User). If this command is used to set the Issuer Security Domain life cycle state to TERMINATED, all keys and the Global PIN are zeroized.

**STORE DATA** is used to store or to set the value of data elements utilized and managed by the Issuer Security Domain.

### 3.2.3 Unauthenticated Services

The following commands are available without prior role authentication:

**MANAGE CHANNEL** is used to open or to close a logical channel.

**GET DATA** is used to retrieve a single data object. It 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** is used for selecting an application (Card Manager or G&D Security Domain).

**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** is used to initiate a Secure Channel with the Card Manager or a Security Domain. The session data are exchanged and session keys are generated by the module upon completion of this command. The Secure Channel is not considered open until completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command.

### 3.2.4 Relationship between Roles and Services

**Table 5 Services Authorized for Roles**

<table>
<thead>
<tr>
<th>Roles/Services</th>
<th>Crypto Officer (Issuer Security Domain)</th>
<th>User/Applet Provider (G&amp;D Security Domain)</th>
<th>Unauthenticated (Any role)</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALL</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>LOAD</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>DELETE</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>DELETE ALL</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXTERNAL AUTHENTICATE</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>GET DATA</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>GET FREE SPACE</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GET STATUS</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>INITIALIZE UPDATE</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHANGE/UNBLOCK PIN</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STORE DATA</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>PUT KEY</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SELECT</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MANAGE CHANNEL</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3.2.5 Applet Services

User-developed Java Card applets that are downloaded onto the module shall use the Java Card API that is accessible by on-card applets only. The following cryptographic services are provided to the applets through the API:

Key Generation and Key Exchange:
- Generation of pairs of ECDSA keys.
- Generation of pairs of RSA keys.
- Generation of pairs of RSA keys with the private key in its Chinese Remainder Theorem form, RSA CRT.
- The ECDH key agreement scheme.

Message Digest:
- API for the Message Digest algorithms SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.

Pseudorandom Bit Generator:
- An API that provides random number generation using output from the DRBG.

Signature and Verification:
- RSA with SHA-1 digest using the padding schemes ISO/IEC 9796, PKCS#1 and RFC 2409.
- RSA with the digests SHA-224, SHA-256, SHA-384, and SHA-512 using the PKCS#1 padding scheme.
- ECDSA in GF(p) 192 with SHA-1: An API to generate a 20-bytes SHA digest and perform signature generation or verification using ECDSA with the P-192 curve.
- ECDSA in GF(p) 224 with SHA-1: An API to generate a 20-bytes SHA digest and perform signature generation or verification using ECDSA with the P-224 curve.
- ECDSA in GF(p) 256 with SHA-1: An API to generate a 20-bytes SHA digest and perform signature generation or verification using ECDSA with the P-256 curve.
- ECDSA in GF(p) 224 with SHA-224: An API to generate a 28-byte SHA-224 digest and sign/verify the digest using ECDSA with the P-224 curve.
- ECDSA in GF(p) 256 with SHA-256: An API to generate a 32-byte SHA-256 digest and sign/verify the digest using ECDSA with the P-256 curve.

Bulk Encryption and Decryption:
- Triple-DES API that offers
  - 2-key and 3-key Triple-DES in ECB and CBC modes.
  - 3-key Triple-DES in outer CBC mode.
- AES encryption and decryption with block sizes 128, 192, and 256 bits in ECB and CBC modes.

The above stated algorithms are available for use in the FIPS approved mode of operation and undergo FIPS 140-2 validation testing.

The GP specification [GPCS2.1.1] defines various 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 Cryptographic Functions

Sm@rtCafé Expert 6.0 provides the following cryptographic services:

**Triple-DES (2-key and 3-key Triple-DES)**
- A 2-key Triple-DES MAC is provided for DAP verification.
- Triple-DES encryption and decryption services are provided to applets through the Java Card API.

**AES (128, 192 and 256 bits key sizes)**
- AES encryption and decryption is provided as services to applets through Java Card API.
- AES for message data field decryption and response encryption is provided for Secure Channel confidentiality.

**Message Digest**
- The SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 Message Digest algorithms are provided as a service to applets through the Java Card API.

**Message Authentication**
- CMAC is provided for Secure Channel Protocol 03 message integrity and data origin authentication.
- Triple-DES MAC is provided for DAP verification services.

**RSA (1024 to 2048 bits modulus length)**
- RSA with 1024 bits modulus length is provided for signature verification services during DAP verification.
- RSA signature generation and signature verification functions are provided as services to applets through the Java Card API. The applet shall use the RSA algorithm only for key wrapping/unwrapping or signature generation/verification.

3.2.7 Random Bit Generator

The Sm@rtCafé Expert 6.0 cryptographic module offers a NIST SP 800-90 Deterministic Random Bit Generator as approved security function that meets the requirements of FIPS 140-2 and SP 800-90.

DRBG implementation is a CTR_DRBG without prediction resistance based on 3-key Triple-DES. The output block length is 64 bits, the key length is 168 bits, seed length is 232 bits and the security strength for the Triple-DES block cipher algorithm with 3 keys is 112 bits.

A personalization string is not provided as an input value to the Instantiate function. There is no option for additional input to the Generate function. The Reseed function is not supported. Once the reseed counter has reached $2^{32}$ (the reseed interval), the Instantiate function is invoked that acquires fresh entropy input and combines it with a nonce to create a new seed with the help of the derivation function. The derivation function is implemented using a block cipher algorithm.

3.3 Critical Security Parameters (CSP)

Table 6 CSP Information
<table>
<thead>
<tr>
<th>Key</th>
<th>Key type</th>
<th>Generation</th>
<th>Entry</th>
<th>Storage</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto Officer Initial keys</td>
<td>128 bits AES keys</td>
<td>External by manufacturing</td>
<td>Pre-configured</td>
<td>Veiled in the module's non-volatile memory</td>
<td>Authentication of Crypto Officer and Sensitive Data Decryption</td>
</tr>
<tr>
<td>(K_{KINIT_ENC}, K_{KINIT_MAC}, K_{KINIT_DEK})</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crypto Officer Static keys</td>
<td>AES keys of the supported sizes (128, 192, 256 bits)</td>
<td>External by Crypto Officer</td>
<td>Loaded in encrypted form with PUT KEY</td>
<td>Veiled in the module's non-volatile memory</td>
<td>Authentication of Crypto Officer Sensitive Data Decryption</td>
</tr>
<tr>
<td>(K_{ENC}, K_{MAC}, K_{DEK})</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crypto Officer Session keys</td>
<td>AES keys of the supported lengths (128, 192, 256 bits)</td>
<td>Generated after authentication of Crypto Officer</td>
<td>Dynamically derived by the module during Secure Channel establishment</td>
<td>Temporarily, veiled in volatile memory</td>
<td>Secured communication (confidentiality- and/or integrity-protected) between terminal and module</td>
</tr>
<tr>
<td>(S_{ENC}, S_{MAC})</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delegated Management Token Key</td>
<td>1024 bits RSA key</td>
<td>External by Crypto Officer</td>
<td>Loaded in encrypted form with PUT KEY</td>
<td>Veiled in the module's non-volatile memory</td>
<td>Authorization of Delegated Management commands</td>
</tr>
<tr>
<td>(K_{Token})</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delegated Management Receipt Key</td>
<td>112 bits Triple-DES key</td>
<td>External by Crypto Officer</td>
<td>Loaded in encrypted form with PUT KEY</td>
<td>Veiled in the module's non-volatile memory</td>
<td>Confirmation of command execution</td>
</tr>
<tr>
<td>(K_{Receipt})</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA DAP public key</td>
<td>1024 bits RSA key</td>
<td>External by Crypto Officer</td>
<td>Loaded in encrypted form with PUT KEY</td>
<td>Protected with GHC checksum in module's non-volatile memory</td>
<td>Signature verification of Load File Data Block Hash</td>
</tr>
<tr>
<td>(PK_{DAP})</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Triple-DES DAP key</td>
<td>112 bits Triple-DES key</td>
<td>External by Crypto Officer</td>
<td>Loaded in encrypted form with PUT KEY</td>
<td>Veiled in the module's non-volatile memory</td>
<td>Signature verification of Load File Data Block Hash</td>
</tr>
<tr>
<td>(K_{DAP})</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Static keys</td>
<td>AES keys of the supported lengths (128, 192, 256 bits)</td>
<td>External by Crypto Officer</td>
<td>Loaded in encrypted form with PUT KEY</td>
<td>Veiled in the module's non-volatile memory</td>
<td>Secure Channel Authentication, Encryption and MAC Verification; Sensitive Data Decryption</td>
</tr>
<tr>
<td>(SDK_{ENC}, SDK_{MAC}, SDK_{DEK})</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Session keys</td>
<td>AES keys of the supported lengths (128, 192, 256 bits)</td>
<td>Generated after User authentication</td>
<td>Dynamically derived on card during Secure Channel establishment</td>
<td>Temporarily, veiled in volatile memory</td>
<td>Secured communication (confidentiality- and/or integrity-protected) between terminal and module</td>
</tr>
<tr>
<td>(KSC_{ENC}, KSC_{MAC})</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global PIN</td>
<td>PIN</td>
<td>External – entered by Crypto Officer</td>
<td>Loaded in encrypted form with CHANGE / UNBLOCK PIN</td>
<td>Veiled in the module's non-volatile memory</td>
<td>Card Holder verification</td>
</tr>
</tbody>
</table>

No secret keys and no private keys are output by the module.
If the Security Domain is personalized with Triple-DES keys and not with AES keys, FIPS validation is lost since the smart card operating system will automatically use the SCP 02 for securing communications instead of the FIPS approved AES-based SPC 03.
4 Security Rules

4.1 Identification and Authentication Security Rules

Sm@rtCafé Expert 6.0 implements Identity-based Access Control Rules for identifying and authenticating the Crypto Officer and the User/Applet provider role.

**Crypto Officer Authentication.** The Crypto Officer must prove possession of the Card Manager key set composed of three AES keys (KENC, KMAC and KDEK). KENC, KMAC are used to derive the session keys that are used to encrypt, authenticate and check the integrity of the command data. KDEK is used to decrypt sensitive data (e.g., secret keys) transported within an APDU command. This is the same process as the User authentication and follows the GP specifications [GPCS2.1.1] and [GP2.2, Amendment D].

**User/Applet Provider Authentication.** The User/Applet Provider must prove possession of the G&D Security Domain key set composed of three AES keys (SDKENC, SDKMAC). SDKENC, SDKMAC are used to derive the session keys that are used to encrypt, authenticate and check the integrity of the command data. This is the same process as the Crypto Officer authentication (via the INITIALIZE UPDATE and EXTERNAL AUTHENTICATE commands) but it uses the AES keys of the G&D Security Domain rather than the Issuer Security Domain keys.

Once it is manufactured, the cryptographic module belongs to the Crypto Officer until it is ultimately issued to the User.

4.2 Applet Loading Security Rules

Only applets validated according to FIPS 140-2 shall be loaded onto the cryptographic module. Applets can only be loaded through a secure channel thus requiring CMAC verification over each Load block. The applet is always loaded by the Issuer (Crypto Officer) or authorized by Issuer in case of Delegated Management.

4.2.1 GP Delegated Management

If Delegated Management is used, the Crypto Officer has to set Delegate Management Keys for Token verification (KToken) and Receipt generation (KReceipt), to install the G&D Security Domain with Delegated Management privilege and to set Secure Channel keys of this Security Domain.

The User of G&D Security Domain can load packages or install applications on the module only after Secure Channel initiation and presentation of a module with a Token during the INSTALL for LOAD command. The Token is an RSA signature generated by the Card Issuer using the Card Issuer’s private key that allows ensuring that the Card Issuer has authorized the load process and the loading of the content of the Load File Data Block and that the Card Issuer has authorized the installation process. If token verification was successful, the module processes the appropriate commands for delegated loading or installation and answers with a receipt, i.e., a Triple-DES MAC generated by the module acknowledging that the operation was performed successfully. For details see [GPCS2.1.1].

4.2.2 GP 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 always required.

The mechanism designated as “DAP” in [GPCS2.1.1] enables the applet provider to check, independently of the Issuer (Crypto Officer), that his applet has been correctly loaded. This check is done by MAC verification on the Load File. DAP may be generated either using Triple-DES or RSA.

As identified in Section 3.2.1, only DAP verification using full Triple-DES or RSA may be used in the approved mode of operation.

This process is described in the Sm@rtCafé Expert 6.0 Reference Manual [SCE60 RefMan].
4.3 Access Control Security Rules

Keys must be loaded through a Secure Channel and encrypted with the $K_{DEK}$ or $SDK_{DEK}$. Therefore the keys are always loaded in encrypted form.

Global PIN might only be set or changed in the context of a Secure Channel and encrypted with the key used for sensitive data decryption. Therefore the PIN block is always encrypted with $K_{DEK}$ when transferred into the module. It is double-encrypted (with $K_{DEK}$ and $S_{ENC}$) if the Secure Channel security level requires command encryption.

4.4 Physical Security Rules

The physical security of the cryptographic module is designed to meet FIPS 140-2 level 3 requirements. Opaque tamper-evident enclosure is provided at the die level (P5Cxx081, P5CD145) and at package level (SSOP20-packaged P5CC081 chip), see also Section 2.3.2.

4.5 Key Management Security Policy

4.5.1 Cryptographic key generation

AES session key for Secure Channel derivation is conforming to [GP2.2, Amendment D]. The random data required for opening a Secure Channel is generated using the DRBG.

RSA and RSA CRT key pair generation is according to [ANSI X9.31] using the DRBG as the approved RNG.

4.5.2 Cryptographic key entry/output

Keys shall always be loaded after having been encrypted with the Sensitive Data Decryption key with the same or higher security strength. The PUT KEY command for adding or replacing keys or key sets may only be issued within a Secure Channel. During this process, the keys are double encrypted (using the session key $S_{ENC}$ or $KSC_{ENC}$ and the sensitive data encryption key $K_{DEK}$ or $SDK_{DEK}$), provided that the Secure Channel security level is set to C_MAC and C_DECRYPTION.

The Security Domain key sets that were loaded onto the cryptographic module can be replaced after successful authentication by loading another key set for Crypto Officer or User using the PUT KEY command.

The PUT KEY command is used to replace the Crypto Officer’s initialization keys $K_{INIT\_ENC}$, $K_{INIT\_MAC}$, and $K_{INIT\_DEK}$ with the first new static key set composed of $K_{ENC}$, $K_{MAC}$, and $K_{DEK}$.

The module outputs public keys in non-encrypted form. Other than public keys, no secret keys and private keys or PINs can be output from the module.

4.5.3 Cryptographic key storage

Cryptographic keys stored with the cryptographic module have the following attributes:

- Key Identifier, which identifies each key within an on-card entity,
- An associated Key Version Number, which is used to differentiate between versions of the same key,
- Algorithm Identifier, which determines the associated cryptographic algorithm,
- Integrity Check Value for that key.

Symmetric keys are veiled by XOR calculation with card individual random number.

Exponent of RSA private key is veiled by multiplication with card individual random number.

DP and DQ of RSA CRT private key is veiled by multiplication with card individual random number.

P and Q of RSA CRT private key is veiled by modulo calculation with card individual random number.
PQ of RSA CRT private key is veiled by XOR calculation with card individual random number.

RSA public keys are stored in plaintext along with a generalised Hamming code (GHC) for each key.

ECC keys are veiled by multiplying them with card individual random number and dividing them (modulo the group order) by card individual random number and by XORing them with a card individual random byte string.

Veiled keys are considered plaintext for the purpose of FIPS 140-2 compliance.

4.5.4 Cryptographic key zeroization

The cryptographic module zeroizes cryptographic session keys $S_{MAC}$, $S_{ENC}$ and $KSC_{MAC}$, $KSC_{ENC}$ of the Security Domain (Issuer Security Domain and G&D Security Domain) when closing the Secure Channel or at card reset.

The keys for GP DAP $K_{DAP}$, $PK_{DAP}$ can only be updated. In order to delete DAP verification key(s) the Security Domain containing the key must be deleted. This operation deletes all keys contained in that 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.

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

Key Management details can be found in Section 6.

All keys and the Global PIN can be zeroized by setting the card state to TERMINATED with the SET STATUS command.

4.6 Approved mode

The cryptographic module supports FIPS approved mode of operation at all times. However, the module provides certain non-approved functions as internal services to applets loaded on the module via the Java Card API. These services are not accessible 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 validated applets shall be loaded on the module.

The non-FIPS-approved functions provided by the cryptographic module are listed in Section 7.2. No non-allowed algorithms will be used by the validated module.

The cryptographic module is conforming to the ISO/IEC 7816-3 standard, which defines the Answer-to-Reset (ATR). The Answer-to-Reset is the value of the byte string (at most 32 bytes) returned by the module when it is reset by the interface device. A reset is triggered by an electrical signal to the RST pin. The coding conventions for the ATR are defined in ISO/IEC 7816-3. The transmission and protocol parameters and capabilities and the historical bytes are encoded in the ATR. The historical bytes describe operating characteristics of the cryptographic module. Their structure is as specified in ISO/IEC 7816-4, the content is proprietary.

The Answer-to-Reset (ATR) returned by the module serves as an approved mode indicator. The ATR returned by the Sm@rtCafé Expert 6.0 firmware is different depending on the underlying chip type:

**P5CC081 ATR:** 3B FD 18 00 00 80 31 FE 45 53 43 45 36 30 2D 43 43 30 38 31 2D 46 C3

**Protocol parameters:**
3B FD 18 00 00 80 31 FE 45

**Historical bytes:**
53 43 45 36 30 2D 43 43 30 38 31 2D 46

**Checksum:**
C3

**P5CD081 ATR:** 3B FD 18 00 00 80 31 FE 45 53 43 45 36 30 2D 43 44 30 38 31 2D 46 C4

**Protocol parameters:**
3B FD 18 00 00 80 31 FE 45

**Historical bytes:**
53 43 45 36 30 2D 43 44 30 38 31 2D 46
Checksum: C4

**P5CD145 ATR:** 3B FD 18 00 00 80 31 FE 45 53 43 45 36 30 2D 43 44 31 34 35 2D 46 CD

Protocol parameters: 3B FD 18 00 00 80 31 FE 45

Historical bytes: 53 43 45 36 30 2D 43 44 31 34 35 2D 46

Checksum: CD

Essentially, only the historical bytes of the ATR are different, due to the different underlying chip type.

The response to GET DATA in the approved mode returned by the Sm@rtCafé Expert 6.0 firmware is:

```
01 02 xx xx 02 04 xx xx xx xx xx 03 02 xx xx 04 08 xx xx xx xx xx xx xx xx 05 02 xx xx 07 04 C0 8B 1F A2 08 04 xx xx xx xx 09 03 xx xx xx xx 06 02 xx xx 0A 05 xx xx xx xx xx 0B 02 xx xx 0C 08 00 00 8F 7D 00 00 00 00 10 02 xx xx
```

The GET DATA response contains relevant information for ROM mask identification and self tests settings for FIPS.

The tag for ROM mask identification is ‘07’, the associated value with that tag is always ‘C0 8B 1F A2’.

The tag for FIPS-related settings is ‘0C’; it is followed by a variable value that depends on the underlying chip hardware, the enabled cryptographic algorithms and their associated self tests (see chapter 7.4).

The value following tag ‘0C’ has the following interpretation:

- Bytes 1 and 2: self tests during ATR
- Bytes 3 and 4: self tests after ATR before first command
- Bytes 5 and 6: self tests after ATS before first command
- Bytes 7 and 8: self tests during USB mode of operation (this is RFU, not relevant with this chip hardware)

Bytes 1, 3, 5 and 7 have identical format with the following assignment:

- bit 7: SHA-512
- bit 6: not set
- bit 5: RNG
- bit 4: Indicates the RSA modulus length used in self tests on RSA. If set to “0” modulus of 1024 bits is used, else if set to "1", modulus of 2048 bits is used.
- bit 3: ECDSA
- bit 2: ECDH
- bit 1: SHA-256
- bit 0: SHA-1

Bytes 2, 4, 6 and 8 have identical format with the following assignment:

- bit 7: DSA
- bit 6: AES
- bit 5: DES
- bit 4: RSA CRT Private
- bit 3: RSA Private
- bit 2: RSA Public
- bit 1: ROM Checksum
- bit 0: Package Checksum
5 Security Policy Check List Tables

5.1 Roles and Required Authentication

<table>
<thead>
<tr>
<th>Role</th>
<th>Type of authentication</th>
<th>Authentication data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto Officer</td>
<td>GP secure channel mutual authentication protocol</td>
<td>GP Secure Channel AES key set (Issuer Security Domain)</td>
</tr>
<tr>
<td>User / Applet Provider</td>
<td>GP secure channel mutual authentication protocol</td>
<td>GP secure channel AES key set (G&amp;D Security Domain)</td>
</tr>
</tbody>
</table>

5.2 Algorithm Strengths

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Bits of security</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECDH with ECDSA in GF(p) with P=192 curve</td>
<td>80 bits</td>
</tr>
<tr>
<td>ECDH with ECDSA in GF(p) with P=224 curve</td>
<td>112 bits</td>
</tr>
<tr>
<td>ECDH with ECDSA in GF(p) with P=256 curve</td>
<td>128 bits</td>
</tr>
<tr>
<td>AES key generation</td>
<td>128 bits to 175.5 bits</td>
</tr>
<tr>
<td>AES key wrapping, key establishment methodology</td>
<td>128 bits to 175.5 bits</td>
</tr>
</tbody>
</table>

For key generation, the module uses SP 800-90 CTR DRBG based on 3-key Triple DES. The output of the hardware RNG is used to seed the deterministic RNG at instantiation. The hardware RNG generates random numbers that meet independent bits with Shannon entropy of 7.976 bits per octet [STlite NXP]. The maximum security strength of keys generated by the module is 0.997 * (112+64) = 175.5 bits, where 0.997 is the calculated entropy strength (7.976/8), 112 is the security strength of 3-key Triple-DES in bits, and 64 is size of the DRBG’s V value in bits. The minimum security strength of keys generated by the module is 80 bits.

5.3 Strength of Authentication Mechanisms

<table>
<thead>
<tr>
<th>Authentication Mechanism</th>
<th>Strength of Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator authentication</td>
<td>probability that a random attempt will succeed:</td>
</tr>
<tr>
<td>based on AES</td>
<td>&gt; 1:2^{128} (for 128 bits key)</td>
</tr>
<tr>
<td></td>
<td>&gt; 1:2^{175.5} (for 192 and 256 bits keys)</td>
</tr>
</tbody>
</table>

5.4 Services Authorized for Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Authorized Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto Officer</td>
<td>The CO role services are listed in Sections 3.2.1, 3.2.2 and 3.2.3</td>
</tr>
<tr>
<td>User / Applet Provider</td>
<td>Services as listed in Sections 3.2.2 and 3.2.3</td>
</tr>
</tbody>
</table>

5.5 Mitigation of Other Attacks

<table>
<thead>
<tr>
<th>Other Attacks</th>
<th>Mitigation Mechanism</th>
<th>Specific Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple Power Analysis</td>
<td>Countermeasures against SPA</td>
<td>N/A</td>
</tr>
<tr>
<td>Differential Power Analysis</td>
<td>Countermeasures against DPA</td>
<td>N/A</td>
</tr>
<tr>
<td>Timing Analysis</td>
<td>Countermeasures against Timing Analysis</td>
<td>N/A</td>
</tr>
<tr>
<td>Differential Fault Analysis</td>
<td>Countermeasures against Differential Fault Analysis</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## 5.6 Access Rights within Services

<table>
<thead>
<tr>
<th>CSP</th>
<th>Service</th>
<th>Role</th>
<th>Type of Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES CO Static keys: $K_{ENC}, K_{MAC}, K_{DEK}$</td>
<td>PUT KEY</td>
<td>Crypto Officer</td>
<td>Write</td>
</tr>
<tr>
<td>AES CO Static keys: $K_{ENC}, K_{MAC}$</td>
<td>INITIALIZE UPDATE</td>
<td>Crypto Officer</td>
<td>Execute</td>
</tr>
<tr>
<td>AES CO key $K_{DEK}$</td>
<td>CHANGE/UNBLOCK PIN</td>
<td>Crypto Officer</td>
<td>Execute</td>
</tr>
<tr>
<td>AES CO Session keys $S_{ENC}, S_{MAC}$</td>
<td>INITIALIZE UPDATE</td>
<td>Crypto Officer</td>
<td>Create</td>
</tr>
<tr>
<td>AES CO Session Encryption key $S_{ENC}$</td>
<td>Data confidentiality</td>
<td>Crypto Officer</td>
<td>Execute</td>
</tr>
<tr>
<td>AES CO Session MAC key $S_{MAC}$</td>
<td>Data and protocol integrity</td>
<td>Crypto Officer</td>
<td>Execute</td>
</tr>
<tr>
<td>AES User Static keys: SDK$K_{ENC}, SDK_{MAC}, SDK_{DEK}, KDAP$</td>
<td>PUT KEY, STORE DATA</td>
<td>Crypto Officer and User</td>
<td>Write</td>
</tr>
<tr>
<td>AES User Static keys: SDK$K_{ENC}, SDK_{MAC}$</td>
<td>INITIALIZE UPDATE</td>
<td>User</td>
<td>Execute</td>
</tr>
<tr>
<td>AES User Session Encryption key $K_{SC_{ENC}}$</td>
<td>Data confidentiality</td>
<td>User</td>
<td>Execute</td>
</tr>
<tr>
<td>AES User Session MAC key $K_{SC_{MAC}}$</td>
<td>Data and protocol integrity</td>
<td>User</td>
<td>Execute</td>
</tr>
<tr>
<td>AES User key $SDK_{DEK}$</td>
<td>Sensitive data decryption</td>
<td>User</td>
<td>Execute</td>
</tr>
<tr>
<td>“GP DAP” RSA public key $PK_{DAP}$ and “GP DAP” Triple-DES key $K_{DAP}$</td>
<td>PUT KEY</td>
<td>Crypto Officer</td>
<td>Write</td>
</tr>
<tr>
<td>“GP DAP” Triple-DES key $K_{DAP}$</td>
<td>LOAD</td>
<td>Crypto Officer and User</td>
<td>Execute</td>
</tr>
<tr>
<td>“GP DAP” RSA public key $PK_{DAP}$</td>
<td>LOAD</td>
<td>Crypto Officer and User</td>
<td>Execute</td>
</tr>
<tr>
<td>Delegated Management keys $K_{Receipt}, K_{Token}$</td>
<td>PUT KEY</td>
<td>Crypto Officer</td>
<td>Write</td>
</tr>
<tr>
<td>Delegated Management Triple-DES key $K_{Receipt}$</td>
<td>LOAD</td>
<td>Crypto Officer</td>
<td>Execute</td>
</tr>
<tr>
<td>Delegated Management RSA key $K_{Token}$</td>
<td>LOAD</td>
<td>Crypto Officer</td>
<td>Execute</td>
</tr>
<tr>
<td>Global PIN</td>
<td>CHANGE/UNBLOCK PIN</td>
<td>Crypto Officer</td>
<td>Write</td>
</tr>
</tbody>
</table>
6 Cryptographic Key Management

The cryptographic module with one G&D Security Domain includes the following keys:

- Initialization key set (K_{INIT\_ENC}, K_{INIT\_MAC}, K_{INIT\_DEK}) that is used only for the first Card Manager key set loading.

- Security Domain (Issuer Security Domain and G&D Security Domain) key sets each containing three static AES keys stored in EEPROM. The key sets contain keys of one of the supported key sizes (128, 192, or 256 bits).

- K_{ENC}/SDK_{ENC} used for Crypto Officer/User authentication for Secure Channel initiation per GP Specification.

- K_{MAC}/SDK_{MAC} used for Crypto Officer/User authentication for Secure Channel initiation per GP Specification.

- K_{DEK} used by the Crypto Officer
  - as key wrapping key for encrypting keys input into the module using the PUT KEY command.
  - to change the Global PIN via the CHANGE / UBLOCK PIN command.

- SDK_{DEK} is the key wrapping key for encrypting keys input into the module by the User via the PUT KEY command.

- Security Domain Session Secure Channel keys are stored in RAM. These keys are derived from the Static Secure Channel keys. The supported AES key lengths for session keys are 128, 192, and 256 bits.
  - Secure Channel Session Encryption key S_{ENC} (derived from K_{ENC}) of Crypto Officer.
  - Secure Channel Session MAC Verification key S_{MAC} (derived from K_{MAC}) of Crypto Officer.
  - Secure Channel Session Encryption key KSC_{ENC} (derived from SDK_{ENC}) of User.
  - Secure Channel Session MAC Verification key KSC_{MAC} (derived from SDK_{MAC}) of User.

- “GP DAP” 112 bits Triple-DES key used for DAP verification using Triple-DES MAC.

- “GP DAP” 1024 bits RSA public key used for DAP verification using RSA signature verification.

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

- Delegated Management Triple-DES key K_{Receipt} for Receipt generation that is used to prove successful execution of Delegated Management command.

All keys can be zeroized by setting the card state to TERMINATED.
7 Standards-Based Cryptography

7.1 FIPS approved algorithms

The cryptographic module implements strong, standards-based cryptography. It includes the following FIPS approved algorithms:

- AES with 128, 192, and 256 bits key lengths (ECB and CBC modes), Cert. #1755
- 2 key Triple-DES (ECB and CBC modes), Cert. #1136
- 3 key Triple-DES (ECB and CBC modes), Cert. #1136
- RSA with up to 2048 bits modulus length, Cert. #874
- RSA CRT with up to 2048 bits modulus length, Cert. #874. As validated, the module does not support this algorithm (*).
- ECDSA in GF(p) with P=192, P=224 and P=256 curves, Cert. #232. As validated, the module does not support this algorithm (*).
- SHA-1 hash function, Cert #1542.
- SHA-224, SHA-256, SHA-384, and SHA-512 hash functions, Cert. #1542. As validated, the module does not support these hash functions (*).
- CMAC
- Triple-DES MAC
- DRBG (Deterministic Random Number Generator), Cert. #116

(*) This validation considers this algorithm to be dead code without an applet. Please refer to Section 2.1 for information on post-validated applets.

7.2 The non-FIPS approved algorithms

The cryptographic module includes the following non-FIPS approved algorithms:

- DES
- DSA
- RSA Encryption and Decryption
- Korean SEED
- RIPEMD-160
- MD5

As validated, the module does not use the algorithms listed here for FIPS purposes. This validation considers these algorithms to be dead code without an applet. Please refer to Section 2.1 for information on post-validated applets.

7.3 Other algorithms allowed in FIPS mode

The cryptographic module includes the following algorithms that are non-FIPS approved but allowed to be used in FIPS approved mode:

- AES key wrapping, key establishment methodology, Cert. #1755
- TRNG (nondeterministic hardware RNG)
- ECDH Key Agreement Scheme with cofactor multiplication, acc. to [IEEE P1363]. As validated, the module does not use support this algorithm. This validation considers this algorithm to be dead code without an applet. Please refer to Section 2.1 for information on post-validated applets.
7.4 Self-Tests

The cryptographic module runs start-up and conditional self tests to verify that it is functioning properly. The power-up self tests are performed when the module is powered up and before the module processes the first command it receives after reset. Conditional self-tests are be performed when an applicable security function or operation is invoked.

The operator can initiate module self-tests by issuing an APDU command after a card reset.

7.4.1 Power-Up Tests

Cryptoalgorithm test
A cryptoalgorithm test using a known answer test (KAT) is conducted when the module is powered up for the following cryptoalgorithmic functions:

- AES
- Triple-DES
- RSA Signature Generation and Signature Verification
- RSA CRT Signature Generation
- ECDSA Signature Generation and Signature Verification
- SHA-1
- SHA-256
- SHA-512
- CMAC
- DRBG

Software/Firmware integrity test
A software/firmware integrity test using an error detection code is applied to all validated software and firmware components within the cryptographic module when the module is powered up. The module checks the integrity of the following components:

- Firmware in EEPROM: 32 bits Reed Solomon EDC
- Java Code in EEPROM: 16 bits hardware CRC

A known-answer test involves operating the cryptoalgorithm on input data for which the correct output is already known and comparing the calculated output with the previously generated output (the known answer). If the calculated output does not equal the known answer, the known-answer test fails.

7.4.2 Conditional Tests

Conditional pairwise consistency test
After generating an RSA or RSA CRT key pair the cryptographic module tests the consistency of the generated keys by calculating and verifying a digital signature with those keys.

Software/firmware load test
If Java Card applets are externally loaded into the cryptographic module, then the following software load test is performed.

Loading Java code to the module is only possible by the Crypto Officer after successful authentication that is achieved through the process of initiating a Secure Channel providing assurance to both the cryptographic module and the Crypto Officer that they are communicating with an authenticated entity. If any step in the mutual authentication process fails, the process shall be restarted, i.e. new challenges and Secure Channel session keys shall be generated.
Applets shall only be loaded via a Secure Channel requiring at least MAC verification over each Load block. All commands for loading shall be secured by a MAC and/or encrypted with session keys, depending on security level for the Secure Channel session.

Java code may be secured by data authentication pattern (DAP) that is specified in [GPCS2.1.1]. Data authentication pattern (DAP) verification provides a mechanism used by a Security Domain to verify that a Load File Data Block is authentic. The following verification modes for Load File DAP are allowed in FIPS approved mode:

- 2-key Triple-DES MAC ("full Triple-DES MAC" acc. to [GPCS2.1.1], B.1.2.1) using the $K_{DAP}$ key.
- 1024-bits RSA SSA-PKCS1-v1_5 signature as defined in PKCS#1 is applied to a SHA-1 digest of the data being signed, i.e. the Load File Block ([GPCS2.1.1], B.2.1 and B.3) using the $PK_{DAP}$.

Continuous random number generator test

On every output generated by the DRBG the module performs a comparison with the previously generated random block. The first 8 bytes generated by the DRBG after power-up are saved for comparison with the next 8 bytes block to be generated and never used for any service like cryptographic key generation. The test fails if the two compared 8 bytes blocks are equal.

7.4.3 Module behaviour upon self-test failure

If the cryptographic module fails a self-test, the module enters an error state and outputs an error indicator via the status output interface. The cryptographic module will not perform any cryptographic operations while in an error state. All data output via the data output interface shall be inhibited when an error state exists.

While the module is in error state, no further communication is possible with the module. To exit the error state and to resume normal operation, the module is to be removed from the terminal and re-inserted or the terminal has to reset the module.
8 Mitigation of Attacks

The module implements countermeasures for the following 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 AES, DES and Triple-DES operations. This co-processor was specifically designed by NXP to counter SPA, DPA, and timing analysis attacks. G&D has conducted testing of the module’s AES, 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 and ECDSA implementations have been hardened against SPA, DPA, fault and timing analysis using a variety of techniques. G&D has conducted testing of the module’s RSA and ECDSA processing for resistance to these attacks and found that no information was leaked during this processing via these attacks. For timing analysis, the timing of the implementation does not correlate to the inputs to the implementation. To counter SPA, data-dependent conditional jumps are avoided. Randomization of the RSA base and exponent is employed to counter DPA. ECDSA implementation includes SPA and DPA countermeasures in the point multiplication algorithm, in the modular inversion and in the computation of the ECDSA signature components.
### 9 Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APDU</td>
<td>Application Protocol Data Unit</td>
</tr>
<tr>
<td>ATR</td>
<td>Answer-To-Reset</td>
</tr>
<tr>
<td>CBC</td>
<td>Cipher-Block Chaining</td>
</tr>
<tr>
<td>CMAC</td>
<td>Cipher-based MAC</td>
</tr>
<tr>
<td>CSP</td>
<td>Critical Security Parameter</td>
</tr>
<tr>
<td>CO</td>
<td>Crypto Officer</td>
</tr>
<tr>
<td>CO</td>
<td>Clear-On-Deselect</td>
</tr>
<tr>
<td>COR</td>
<td>Clear-On-Reset</td>
</tr>
<tr>
<td>CRT</td>
<td>Chinese Remainder Theorem</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check</td>
</tr>
<tr>
<td>DAP</td>
<td>Data Authentication Pattern</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DPA</td>
<td>Differential Power Analysis</td>
</tr>
<tr>
<td>DRBG</td>
<td>Deterministic Random Bit Generator</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Signature Algorithm</td>
</tr>
<tr>
<td>EDC</td>
<td>Error Detection Code</td>
</tr>
<tr>
<td>EEPROM</td>
<td>Electrically Erasable Programmable ROM</td>
</tr>
<tr>
<td>EMC</td>
<td>Electromagnetic Compatibility</td>
</tr>
<tr>
<td>EMI</td>
<td>Electromagnetic Interference</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communication Commission</td>
</tr>
<tr>
<td>GHC</td>
<td>Generalized Hamming Code</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
<tr>
<td>IC</td>
<td>Integrated Circuit</td>
</tr>
<tr>
<td>JCAPI</td>
<td>Java Card™ Application Programming Interface</td>
</tr>
<tr>
<td>JCRE</td>
<td>Java Card™ Runtime Environment</td>
</tr>
<tr>
<td>JCVM</td>
<td>Java Card™ Virtual Machine</td>
</tr>
<tr>
<td>KAT</td>
<td>Known Answer Test</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>N/A</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>GP</td>
<td>GlobalPlatform</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PKCS</td>
<td>Public Key Cryptography Standards</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>RNG</td>
<td>Random Number Generator</td>
</tr>
<tr>
<td>ROM</td>
<td>Read Only Memory</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest Shamir Adleman</td>
</tr>
<tr>
<td>RST</td>
<td>Reset</td>
</tr>
<tr>
<td>SCP</td>
<td>Secure Channel Protocol</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SPA</td>
<td>Simple Power Analysis</td>
</tr>
<tr>
<td>TDEA</td>
<td>Triple Data Encryption Algorithm</td>
</tr>
<tr>
<td>TDES</td>
<td>Triple-DES</td>
</tr>
<tr>
<td>TRNG</td>
<td>True RNG</td>
</tr>
</tbody>
</table>