



## **FIPS 140-2 Level 3**

# **Security Policy of Java Card Platform Implementation for Infineon on SLE 78 (SLJ 52GxxyyyzR) V1.0f**

August 2015

Version 2.3



**Title:** Security Policy of Java Card Platform Implementation for Infineon on SLE 78 (SLJ 52GxyyyzR),v1.0f  
**Contributing Authors:** Roland Atoui, Clifford Wayne

Oracle Corporation  
World Headquarters  
500 Oracle Parkway  
Redwood Shores, CA 94065  
U.S.A.  
Worldwide Inquiries:  
Phone: +1.650.506.7000  
Fax: +1.650.506.7200  
oracle.com



Copyright © 2014, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document.

CIPURSE is a registered trademark of the OSPT - Open Standard for Public Transportation Alliance e.V.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

**Hardware and Software, Engineered to Work Together**



# Contents

<b>Contents .....</b>	<b>1</b>
<b>1 Introduction .....</b>	<b>5</b>
1.1 Context .....	5
1.1 Distribution Policy .....	6
1.2 Document Structure .....	6
<b>2 Cryptographic Module Overview.....</b>	<b>7</b>
2.1 CM Description .....	7
2.1.1 CM Purpose.....	9
2.1.2 Core Functionalities.....	9
2.1.2.1 Applet Downloading.....	9
2.1.2.2 Card Management .....	9
2.1.2.3 Services to Applets.....	10
2.1.3 Security Level.....	10
<b>3 Cryptographic Module Specification .....</b>	<b>11</b>
3.1 CM Architecture .....	11
3.1.1 IC Hardware and Firmware.....	12
3.1.2 Java Card Platform.....	13
3.2 Cryptographic Boundary.....	14
3.3 CM Cryptographic Functions .....	14
3.3.1 Cryptographic Keys.....	15
3.3.2 Public Keys .....	17
3.3.3 PIN .....	17
3.3.4 Audit events and data .....	17
3.4 FIPS 140-2 Approved Modes of Operation .....	17
3.4.1 Versions and Mode of Operation .....	18
3.4.2 CM Identification .....	19
<b>4 Cryptographic Module Ports and Interfaces.....</b>	<b>21</b>

4.1	<i>Communication Interfaces</i> .....	21
4.1.1	Logical Interfaces.....	21
4.1.2	Physical Interfaces.....	22
4.2	<i>Packages</i> .....	25
<b>5</b>	<b>Roles, Services and Authentication</b> .....	<b>27</b>
5.1	<i>Roles</i> .....	27
5.2	<i>Services</i> .....	28
5.2.1	Card Management Services Available to off Card Entities .....	28
5.2.1.1	Non Authenticated Services .....	29
5.2.1.2	Services Requiring Authentication and Manipulating CSPs .....	29
5.2.2	Cryptographic Services Available via Java Card API .....	30
5.2.2.1	FIPS 140-2 Approved Algorithms .....	31
<b>6</b>	<b>Security Requirements</b> .....	<b>33</b>
6.1	<i>Identification and Authentication of Roles</i> .....	33
6.1.1	Identification.....	33
6.1.2	Authentication.....	33
6.2	<i>Integrity and Confidentiality of Loaded Application Code</i> .....	34
6.3	<i>Authentication of Loaded Application Code</i> .....	34
6.3.1	DAP Verification.....	34
6.4	<i>CSP Secure Management</i> .....	35
6.4.1	Cryptographic Key and PIN Entry .....	35
6.4.2	Cryptographic Keys and User PIN Contents Zeroization.....	35
6.4.3	Key Generation.....	35
6.4.4	Key Loading.....	35
6.4.5	Key Storage.....	35
6.4.6	Key Establishment .....	36
6.4.7	Key Distribution .....	36
<b>7</b>	<b>Physical Security</b> .....	<b>37</b>
7.1	<i>Physical Security Mechanisms</i> .....	37
<b>8</b>	<b>Mitigation of Other Attacks</b> .....	<b>38</b>
8.1	<i>Power and Electromagnetic Analysis Attacks</i> .....	38
8.1.1	Countermeasures .....	38
8.2	<i>Timing Analysis Attacks</i> .....	39
8.2.1	Countermeasures.....	39
8.3	<i>Fault Induction Attacks</i> .....	39

8.3.1	Countermeasures .....	39
<b>9</b>	<b>Self-Tests .....</b>	<b>41</b>
9.1	<i>Power Up Self -Tests .....</i>	<i>41</i>
9.1.1	Deterministic Random Number Generator Test .....	41
9.1.2	Cryptographic Algorithm Known Answer Tests.....	42
9.1.3	Software/Firmware Integrity KAT .....	42
9.1.4	Critical Functions Tests .....	42
9.2	<i>Conditional Self-Tests.....</i>	<i>42</i>
9.2.1	Pair-wise Consistency Test (for public and private keys) .....	42
9.2.2	Firmware Load Test.....	42
9.2.3	Key Entry Tests.....	43
9.2.4	Continuous RNG Testing .....	43
9.2.5	Bypass Testing .....	43
<b>10</b>	<b>Security Policy - Check List Tables .....</b>	<b>44</b>
10.1	<i>Roles and Required Identification and Authentication.....</i>	<i>44</i>
10.2	<i>Strength of Authentication Mechanisms.....</i>	<i>44</i>
10.3	<i>Services Authorized for Roles .....</i>	<i>45</i>
10.4	<i>Access Rights Within Services.....</i>	<i>45</i>
10.5	<i>Physical Security Requirements.....</i>	<i>48</i>
10.6	<i>Mitigation of Other Attacks.....</i>	<i>48</i>
<b>A</b>	<b>References.....</b>	<b>49</b>
<b>B</b>	<b>Acronyms.....</b>	<b>52</b>

## List of Tables

Table 1: Security Level.....	10
Table 2: Cryptographic Algorithms.....	15
Table 3: Critical Security Parameters - Secret Symmetric Keys.....	16
Table 4: Critical Security Parameters - Public Assymetric Keys.....	17
Table 5: Critical Security Parameters - Global PIN .....	17
Table 6: Critical Security Parameters - Counters.....	17
Table 7: Product and Package Combination.....	18
Table 8: Versions and Mode of Operations Indicators .....	19
Table 9: Tag 'DF10' .....	20
Table 10: Tag 'DF11' .....	20
Table 11: <i>Logical Interface</i> .....	21
Table 12: CM ISO 7816 Interface Contact Assignments .....	23
Table 13: IC Pad Descriptions and Logical Interface Types.....	24
Table 14: Logical Interfaces With Physical Interface Connections.....	25
Table 15: Supported Packages.....	26
Table 16: Roles.....	28
Table 17: Unauthenticated Services.....	29
Table 18: Card Content Manager Services and their CSP Usage.....	30
Table 19: Cryptographic Services and Authentication services available to applet through the standard Java Card API.....	31
Table 20: FIPS Approved Cryptographic Algorithms.....	32
Table 21: Roles and Required Identification and Authentication - Check-List.....	44
Table 22: Strength of Authentication Mechanisms - Check-List .....	44
Table 23: Services Authorized for Roles - Check-List .....	45
Table 24: Access Rights Within Services - Check-List.....	48
Table 25: Physical Security Requirements - Check-List.....	48
Table 26: Mitigation of Other Attacks - Check-List .....	48

## Table of Figures

Figure 1. CM Architecture Overview.....	11
Figure 2. Cryptographic Boundary – Hardware Architecture.....	12
Figure 3. Relationship of CM Software Module and Supporting Applications.....	13
Figure 4. Cryptographic Module Boundary.....	14
Figure 5: ISO 7816 Interface Contact Pad Designations and Locations .....	23
Figure 6: IC Die Pad Designations and Locations.....	24

# 1 Introduction

*This document describes how the Cryptographic Module (CM) meets all the requirements for level 3 validation criteria specified in [FIPS PUB 140-2]. The CM is a Java Card Platform Implementation for Infineon on SLE 78 (SLJ 52GxxyyyzR).*

*This Security Policy is intended to specify the security rules under which the CM operates and does not describe the security requirements for the entire product.*

## 1.1 Context

This is a non-proprietary Cryptographic Module Security Policy for the Cryptographic Module (CM) which consists of the Infineon Technologies Dual Interface Security Controller M7892 with RSA, EC and SHA cryptographic libraries and the Java Card Platform Implementation for Infineon on SLE 78 (SLJ 52GxxyyyzR) binary code.

The Dual Interface Security Controller M7892 is a member of the Infineon Technologies AG high security controller family SLE70 meeting the highest requirements in terms of performance and security. The SLE70 family provides a common architecture upon which specific products can be tailored for different usages such as high security and contactless applications which can be identified by SLE78 which is the family of the IC that we are targeting in this evaluation.

This Security Policy describes how the Dual Interface Security Controller SLE78 and Java Card Platform binary code meets the security requirements of FIPS 140-2 and CM's operation in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 3 FIPS 140-2 validation of 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 National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at <http://csrc.nist.gov/cryptval/>.

The Dual Interface Security Controller SLE78 with the Java Card Platform implementation binary code is referred to in this document as CM, Cryptographic Library, Software Library, Cryptographic module, software module, or module.



## 1.1 Distribution Policy

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Oracle Corporation and is releasable only under appropriate non disclosure agreements. For access to these documents, please contact Oracle Corporation.

## 1.2 Document Structure

This document is structured as follows:

- Chapter 2 describes the Cryptographic Module (CM), defines its main purpose, and identifies its security levels.
- Chapter 3 describes the CM architecture, boundary, functions, CSPs and modes of operation.
- Chapter 4 describes the ports and interfaces (physical and logical) and the information passing over them.
- Chapter 5 describes the roles, services and authentication provided by the CM.
- Chapter 6 describes the security policy for the enforcement of identity based authentication and data, cryptographic key and code integrity and confidentiality.
- Chapter 7 describes physical security mechanisms provided by the CM.
- Chapter 8 describes how the cryptographic module provides protection for the CSPs against non-invasive attacks and the effectiveness of the mitigation techniques.
- Chapter 9 describes self-tests ensuring that the CM is functioning properly.
- Chapter 10 summarizes the security policy check list tables.



# 2 Cryptographic Module Overview

*This chapter provides a global description of the Cryptographic Module (CM), defines its main purpose and security level.*

## 2.1 CM Description

The CM is a Java Card Platform Implementation for Infineon on SLE 78 (SLJ 52GxxyyyzR) mounted in a smart card form factor.

- CM name/version: Java Card Platform Implementation for Infineon on SLE 78 (SLJ 52GxxyyyzR) V1.0f
- CM Hardware ID: M7892B11 (Smart Card IC)
- CM Platform Commercial ID's: SLE78CLFX400VP(M), SLE 78CLFX408AP(M)
- CM Interface Package ID's:
  - P-MCS8-2-1 (ISO/IEC 14443)
  - P-MCC8-2-6 (ISO/IEC 14443)
  - S-MFC6.8-8-1 (ISO/IEC 7816-3)
  - S-COM8.6-6-1 (ISO/IEC 7816-3 and 14443)
  - P-M8.4-8-3 (ISO/IEC 7816-3 and 14443)
  - S-MID4.8-8-1 (ISO/IEC 7816-3)
  - S-COM10.6-6-1 (ISO/IEC 7816-3 and 14443)
  - PG-USON10-1 (ISO/IEC 7816-3)

The CM name/id consists of the following placeholder:

- the first x is for the available interface (can be 'C', 'L', or 'D' for the Contact based, contact Less or Dual Interface)
- the second x is for the available cryptography (can be 'A' for symmetric and asymmetric cryptography, and 'B' for only symmetric cryptography)
- The number yyy the available user memory (it is '160' for 160 kB)
- the last letter z represents the product (can be 'A' for ePassport, 'B' for eDriving License, 'C' for National eID Open Platform, or 'D' for National eID with applications)



The CM is a single-chip cryptographic module mounted in a smart card and sets a new, improved standard of integrated security features, thereby meeting the requirements of all smart card and other related applications or form factors, such as information integrity, access control, mobile telephone and identification, as well as uses in electronic funds transfer and healthcare systems.

The Java Card Platform is secure execution environment consisting of a Java Card Runtime, Java Card Virtual Machine, Java Card API and Global Platform Card Manager along with native cryptographic library calls made available to applets through Java Card APIs. The CM is compliant with Java Card specifications version 3.0.1 Classic Edition ([JCVM3], [JCRE3], [JCAPI3]) and the Global Platform card specification version 2.2 [GP]. In particular, it implements the GlobalPlatform ID Configuration 1.0 [GP\_ID]. The cryptographic services offered by the CM are provided to the applets through the Java Card API.

The Infineon Technologies Dual Interface Security SLE78 consists of integrated circuits manufactured by Infineon Technologies AG in a 90 nm CMOS-technology (L90) and provides real 16-bit CPU-architecture that is compatible with Intel 80251 architecture. The SLE78 dual interface controller meets the highest requirements in terms of performance and security and provides maximum flexibility in using the communication protocols such as ISO 7816, ISO 14443 Type A and Type B. The Security Controller M7892 can communicate using either the contact based or the contactless interface, enabling user implementation of contact based or contactless communication.

The SLE78 is used in smart cards for security-relevant applications. It has also been used as a development platform for smart card operating systems in accordance with the lifecycle model from [1]. The term Smartcard Embedded Software is used in this document to refer to all operating systems and applications stored and executed on the IC regardless whether it is a smartcard or another application of form factor.

The following is a list of features provided by the SLE78 Smart Card IC:

- 24-bit linear addressing
- Up to 16 MByte of addressable memory
- Register-based architecture (registers can be accessed as bytes, words (2 bytes), and double words (4 bytes))
- 2-stage instruction pipeline
- Extensive set of powerful instructions, including 16-bit and 32-bit arithmetic and logic instructions
- CACHE with single-cycle access searching
- 16-bit ALU

### 2.1.1 CM Purpose

The main purpose of the CM is to provide cryptographic services to applets through the Java Card API to perform on-device cryptographic operations in a FIPS 140-2 compliant runtime environment where highly secure applications are in use and of course in any other application as well. This CM is intended for use by governmental, corporate, transport and payment markets, or wherever a secure root of trust is required. Various types of applications can use this CM, for example in closed loop logical access controls, physical access controls, secure internet access control and internet authentication, or as multi-application token or simply as encrypted storage.

Operating system(s) the module was tested on: Java Card Platform Implementation for Infineon on SLE 78 (SLJ 52GxxyyzR), v1.0f

Data integrity and security are provided through the cryptographic services and defensive characteristics of the CM implementation. The CM supports standard AES, TDES, DSA, RSA, ECDSA, and SHA cryptographic algorithms. Both CM firmware and hardware provide module security. In addition, the CM hardware provides tamper-resistance and tamper-evidence features that meet FIPS 140-2 Level 3 physical security requirements. However, FIPS 140-2 validation does not include privileged applications.

### 2.1.2 Core Functionalities

The main functionalities provided by the CM are applet downloading, card management, and specific security Java Card API services provided to the applets.

#### 2.1.2.1 Applet Downloading

The Card Manager is a privileged applet defined in the GlobalPlatform specification that enables secure downloading of applications. The card manager implements the policies and security aspects of the card issuer and contains the keys needed to download an applet or a package to the smart card. In accordance with [JCRE3], the installer is the CM component that loads, links, and installs new packages. Once selected, the installer receives the CAP file, stores the classes of the package on the card, initializes any static data, and installs any applets contained in the package.

#### 2.1.2.2 Card Management

In accordance with the Global Platform Card Specification 2.2 [GP], the card manager supports a multi-application runtime environment and provides the Global Platform framework facilities required for secure loading and interoperability of different applications. The card manager is responsible for the administration of the smart card and is conformant to the Global Platform Card Specification 2.2 [GP]. In accordance with [JCRE3] and [GP], the card manager provides administration of the smart card by:

- Managing the life cycle of the installed applications (applets) and the card.
- Managing the security domains and enforcing card issuer security policies.



- Ensuring secure communication between the application instances on the card and the card administrator.

The Card can be set to run in GP mode or GP ID mode. If the card is configured for GP mode, SSDs follow the GlobalPlatform Card Specification v2.2 requirements [GP]. If the card is configured for GP ID mode, SSDs behave in accordance with the GlobalPlatform ID Configuration specification [GP\_ID]. When GP\_ID mode is enabled, the ISD is required to use SCP 03 option 0x10.

Optionally, the TOE can be configured to behave like a static Java Card Platform where loading of applets is disabled.

### 2.1.2.3 Services to Applets

The Java Card Platform provides the applets with a set of security services in order to enforce a certain security level for applets execution. These security services are available to the applets through the Java Card API.

### 2.1.3 Security Level

Security Requirement	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. EMI/EMC	3
9. Self-Tests	3
10. Design Assurance	3
11. Mitigation of Other Attacks	3

*Table 1: Security Level*

# 3 Cryptographic Module Specification

*This chapter describes the Cryptographic Module architecture, its boundary, functions, and modes of operation.*

## 3.1 CM Architecture

The CM architecture consists of several abstraction layers build on the SLE78 Smart Card and acting in concert to create an environment that provides data integrity and security for the downloading and execution of applets. Figure 1 provides an overall view of the CM architecture.

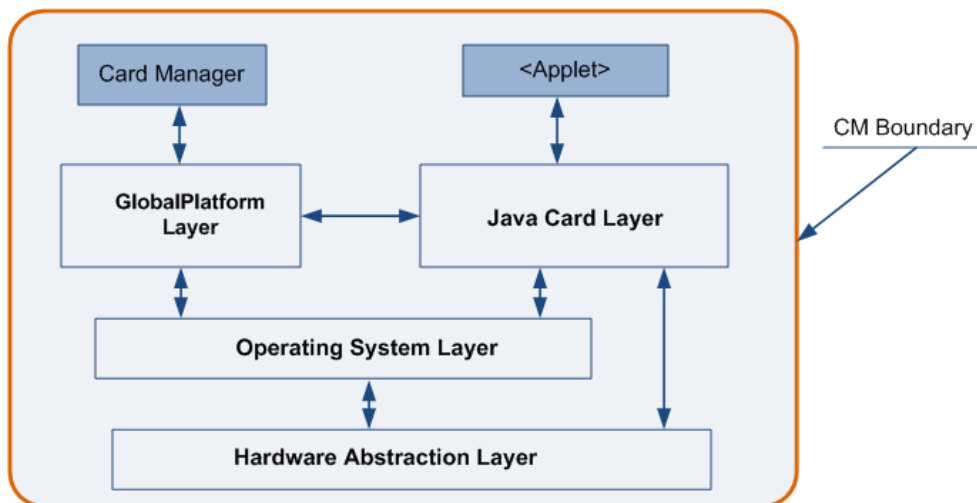


Figure 1. CM Architecture Overview

- The GlobalPlatform (GP) services rely on both the Java Card platform and the operating system services. This component implements the GlobalPlatform card specification, version 2.2, which

defines the infrastructure for development, deployment and management of smart cards. The GP supports Security domains and secure channel protocols.

- Java Card services rely on the operating system and the HAL services. It complies with the specifications for the Java Card Platform, Version 3.0.1, Classic Edition. These services include the security inherent in the Java Card programming language.
- The Operating System services rely on the Hardware Abstraction Layer. It provides a memory manager, cryptography engine and input/output.
- The Hardware Abstraction Layer (HAL) interacts directly with the hardware represented in Section 3.1.1. The HAL implements CPU control, card initialization, memory operations, interruption control, and support for cryptography on the chip.

### 3.1.1 IC Hardware and Firmware

The IC portion of the CM contains specific IC dedicated firmware along with RSA, EC and SHA cryptographic libraries. Figure 2 provides a view of the hardware architecture of the CM.

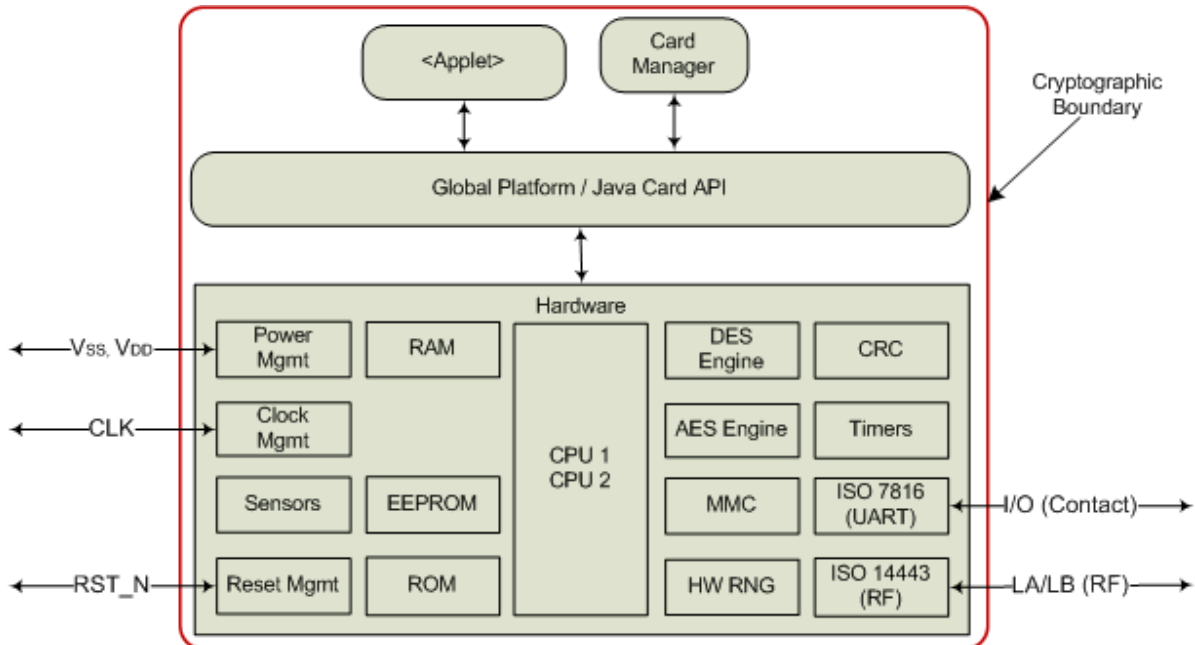


Figure 2. Cryptographic Boundary – Hardware Architecture

### 3.1.2 Java Card Platform

Figure 3 describes the relationship of the Cryptographic Module (CM) software module and supporting applications.

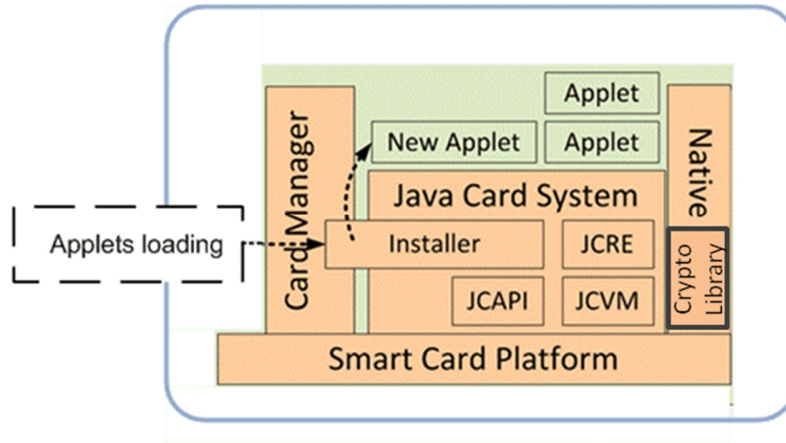


Figure 3. Relationship of CM Software Module and Supporting Applications

The Java Card Platform includes the Java Card RE (JCRE), Java Card VM (JCVM), Java Card API (JCAPI), Card Manager, and Global Platform. The Java Card System along with additional native code is embedded in a Java Card Platform (JCP) as part of the CM and is compliant with Java Card specifications versions 3 Classic Edition, including post-issuance downloading of applications verified off-card.

Components of JCP can be grouped into core and optional components. Core components implement core functionality of the JCP and are required for all possible configurations. The core component group consists of modules from the Java Card Platform, version 3.0.1 and Global Platform 2.2. The operating system and native primitives are tightly integrated with the Infineon libraries and hardware to provide maximum security and performance. Optional components implement optional functionality and are included in configurations only as their functionality is required. Components of the JCP include the following:

- JCAPI - The application programming interface for Java Card.
- JCVM - The Java Card virtual machine is a subset of the Java virtual machine, and is designed to be run on smart cards and other resource-constrained devices. The Java Card virtual machine acts as an engine that loads Java class files and executes them with a particular set of semantics.
- JCRE - A framework for running Java programs on the card.
- Extended Crypto - Cryptographic capabilities have been extended in several ways. Oracle has added additional algorithms and key type support beyond that called out in the Java Card 3.0.1

specifications. In addition, some proprietary Infineon cryptographic acceleration classes have been integrated in the JCP.

### 3.2 Cryptographic Boundary

Figure 4 below illustrates (in a red-dashed box) the cryptographic boundary of one IC package example. The cryptographic boundary includes the outer perimeter of the IC package (This is valid for all the supported packages).

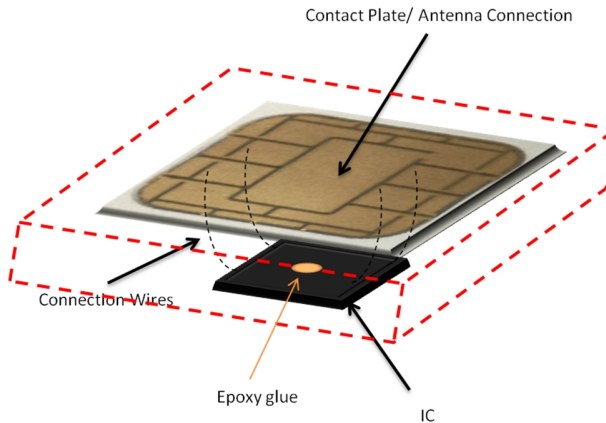


Figure 4. Cryptographic Module Boundary

### 3.3 CM Cryptographic Functions

The module provides cryptographic services to end-user applications. Only those cryptographic algorithms marked as “Available in FIPS mode” in Table 2 s are made available to applets through the Java Card APIs. Once the module has entered a FIPS-approved mode of operation, all access to non-approved algorithms is denied to the Java Card applets at runtime except for the key establishment function. Note that in our CM, only the ISD is considered as a runtime instantiated applet, therefore, security services not used by the ISD are not available to any of the current users of the module.

Table 2 describes the cryptographic algorithms, modes, and keys provided by the CM.

Algorithm	Reference	Modes	Keys Lengths	Available in FIPS Mode
<b>Symmetric Key – Encryption</b>				
AES	[2] and [3]	ECB,CBC	128 bit,192 bit,256 bit	YES
TDES	[4]	ECB,CBC	168 bit	YES
<b>Asymmetric Key – Signature</b>				



Algorithm	Reference	Modes	Keys Lengths	Available in FIPS Mode
DSA	[5]	N/A	L=2048, N=256	YES
RSA	[6] and [7]	N/A	2048 bit (CRT)	YES
ECDSA	[5]	N/A	224 bit- 521 bit	YES
Hashing				
SHA-1 <sup>1</sup>	[8]	N/A	160 bit	YES
SHA-224, SHA-256, SHA-384, SHA-512	[8]	N/A	224-512 bit	YES
Random Number Generators				
CTR_DRBG (AES-128)	[12]	N/A	AES-128 bit	YES
Nondeterministic TRNG (Seeding Only)	[17] Class P2	N/A	N/A	YES
Message Authentication				
TDES MAC	[13]	CBC-MAC	168 bit	YES
AES CMAC	[14]	CMAC	128 bit, 192 bit, 256 bit	YES
Key Establishment				
ECDH <sup>2</sup>	[18]	N/A	224 bit - 521 bit	YES <sup>3</sup>

Table 2: Cryptographic Algorithms

### 3.3.1 Cryptographic Keys

The following cryptographic keys are critical to security as the mechanisms for authentication, data integrity and confidentiality heavily rely on them. All cryptographic keys are stored in plaintext relying on hardware countermeasures for its integrity protection. The CO and Dev keysets are used for administrative purposes, i.e. card content management and key loading and are the root keys in the creation of session keys used to establish a secure channel. All keys including CO and Dev keysets can be loaded or replaced with the GP's PUT\_KEY APDU command. Such key handling is secured by the Security Domain's symmetric crypto algorithm (128-bit AES).

<sup>1</sup> SHA-1 is used during RSA signature verification only.

<sup>2</sup> EC Diffie-Hellman key establishment methodology provides between 112 and 256 bits of encryption strength.

<sup>3</sup> This algorithm is non-FIPS approved but allowed cryptographic function.

Additional details regarding each cryptographic key and CSP are provided in the following tables.

Key	Description and Usage
OS-MKEK	AES 128 Master key used to encrypt only the PIN objects stored in flash memory. This key is generated on OS startup using CTR_DRBG, unique for each card.
OSD-KENC	AES 128 (SCP03) Master key used by the Crypto Officer to generate SD-SENC (session keys during secure channel establishment). The key belongs to the Issuer Security Domain keyset.
OSD-KMAC	AES 128 (SCP03) Master key used by the Crypto Officer to generate SD-SMAC. The key belongs to the Card Issuer Security Domain.
OSD-DEK	AES 128 (SCP03) Master key used by the Crypto Officer. Used to directly unwrap the encrypted key being loaded via the PUT KEY command.
OSD-SENC	AES 128 (SCP03) Session encryption key used by the Crypto Officer to decrypt secure channel data. The role of this key is to preserve confidentiality and authenticity of transmitted data. The key belongs to the Card Issuer Security Domain.
OSD-SMAC	AES 128 (SCP03) Session MAC key used by the Crypto Officer to verify inbound secure channel data's integrity. The key belongs to the Card Issuer Domain.
SD-KENC	AES 128 (SCP03) Master key used by Dev (represented on the card by its respective Application Provider Security Domain) to generate SD-SENC session key.
SD-KMAC	AES 128 (SCP03) Master key used by Dev (represented on the card by its respective Application Provider Security Domain) to generate SD-SMAC session key.
SD-DEK	AES 128 (SCP03) Master key used by the Dev. Used to directly unwrap the encrypted key being loaded via the PUT KEY command.
SD-SENC	AES 128 (SCP03) Session Encryption key used by Dev (represented on the card by its respective Application Provider Security Domain) used to decrypt secure channel data. The role of this key is to preserve confidentiality and authenticity of transmitted data.
SD-SMAC	AES 128 (SCP03) Session MAC key used by Dev (represented on the card by its respective Application Provider Security Domain) to verify inbound secure channel data integrity.

Table 3: Critical Security Parameters - Secret Symmetric Keys

### 3.3.2 Public Keys

Key	Description / Usage
OS-DAP	RSA 2048 Global Platform Data Authentication Public Key. The Mandated DAP feature is defined by Global Platform and is used to verify the signature of packages loaded into the Module prior to linking them against built-in Java APIs. It is done under the Dev role. Loaded on card with PUT KEY APDU. This key belongs to the Controlling Authority.

Table 4: Critical Security Parameters - Public Assymmetric Keys

### 3.3.3 PIN

OS-GPIN	7 to 16 character string card global PIN represents the contents of Java object that belongs to a PIN instance. This object is always stored encrypted with OS-MKEK key and is never decrypted during PIN match operations. Instead, the candidate PIN value is encrypted in the same fashion and presented for comparison in encrypted form.  The OS-MKEK key is used only if the Global PIN is used by a loaded application.
---------	--

Table 5: Critical Security Parameters - Global PIN

### 3.3.4 Audit events and data

OS-EXP-COUNTER	The counter that increments each time Java engine handles runtime exception to protect against excessive exception throwing by the applet. When a threshold is reached the applet execution stops.
----------------	--

Table 6: Critical Security Parameters - Counters

## 3.4 FIPS 140-2 Approved Modes of Operation

The CM operates in only one FIPS 140-2 Approved Mode (standard operating mode) entered implicitly upon successful completion of power-on self-tests, i.e. no special action or command is necessary. Only FIPS-approved crypto algorithms are used when providing services to Crypto Officer or User/Application Developer. No other mode of operation exists when a card containing the CM has been issued to an application developer. The reasons behind this approach were to simplify usage and deployment, application development and streamline the validation phase. The internal code also prevents non-authorized use of cryptographic keys in operations for which they were not intended.

For the CM operating in the FIPS 140-2 approved mode, the CM does not allow loading application feature unless there is a Security Domain with MDAP privilege requiring the mandatory DAP Verification of the loaded application to ensure its authenticity using only FIPS approved crypto algorithms.

During the chip manufacturing process (design and deployment phases) of the card, the CM is still not in the FIPS 140-2 approved mode. Once the module enters operational phase (after being delivered to the customer) specifically when the card is in the SECURED life cycle state as defined by [GP] it enters the FIPS 140-2 approved mode of operation until the card is terminated (Card Mute).

The M7892 executes its code out of flash and CRC16 program integrity check is performed on code flash contents before entering an operational mode. The contents of various key sets and critical security parameters are stored in available EEPROM data memory with each data structure having a validation field (CRC16) that is checked for consistency before each use and recalculated upon any changes in the contents of this structure. Any applet loaded on this CM must undergo its own FIPS 140-2 validation to maintain FIPS 140-2 certification as a module.

The lifecycles and state transitions follow industry standard implementations specified in Global Platform documentation, version 2.2. The Global Platform specification defines module and application life cycle states and state transitions. Each of the on-module cryptographic algorithms including DRNG, TDES, SHA, AES, RSA and ECC has been individually validated for compliance with FIPS requirements [FIPS140-2 Appendix A, FIPS140-2 Appendix C].

### 3.4.1 Versions and Mode of Operation

Firmware: Java Card Platform Implementation for Infineon on SLE 78 (SLJ 52GxxyyzR)V1.0f

Hardware: The hardware is identified by a combination of interface package ID, internal hardware part number and commercial part number.

Packaging Id	Product and Package Combination
with ISO/IEC 7816-3 Interface Only	
S-MID4. 8-8-1	M7892B11, SLE 78CLFX400VPM
S-MFC6. 8-8-1	M7892B11, SLE 78CLFX400VPM
PG-USON10-1	M7892B11, SLE 78CLFX400VPM
with ISO/IEC 14443 Interface Only	
P-MCS8-2-1	M7892B11, SLE 78CLFX400VPM
P-MCC8-2-6	M7892B11, SLE 78CLFX400VPM
with ISO/IEC 7816-3 and ISO/IEC 14443 Interfaces	
S-COMB. 6-6-1	M7892B11, SLE 78CLFX408APM
P-MB. 4-8-3	M7892B11, SLE 78CLFX400VPM
S-COM10. 6-6-1	M7892B11, SLE 78CLFX408APM

Table 7: Product and Package Combination

During the power-on process, the CM performs all necessary self-tests and either enters the approved mode of operation or, if any self-test fails, enters a deadlock state until the next reset or power-on.

To verify that a module is in the approved mode of operation, an operator authenticated to the Card Manager role sends the GET STATUS command with P1 = 1 and P2 = 0. For example: 80F2010000. The CM responds to the GET STATUS command with the format and information described in Table 8.

Data Element	Length (bytes)	Value	Associated Version
Approved mode indicator	1	Var	0xAA – module is in approved mode 0xFF – module is in deadlock state
Security Status Word	2	Var	Each bit of this word stands for self-test results (1 – test passed, 0 – test failed). In approved mode Security Status Word is equal to Test Permission Word
Test Permission Word	2	Var	Each bit of this word allows or disallows relative self-test (1 – test is allowed, 0 – test is disallowed)
Test Parameters	4	Var	Each pair of bits contains some parameters for relative self-test (for example length of key for test, etc.)

Table 8: Versions and Mode of Operations Indicators

### 3.4.2 CM Identification

After Card initialization the CM is identified using the command GET DATA. It retrieves the chip and configuration data from the card. The configuration data is retrieved using GET DATA tags 0xDF10 and 0xDF11. The response is coded as TLV object. The offsets given in the tables below refer to the offset inside the value part of the TLV object.

Example for GET DATA ('DF10') command / response pair:

```

Ⓜ 80CA DF10 00
└ DF10 81E0 090000...8340 9000
  
```

```

DF10      is the tag
81E0      codes the value length of 224 in two bytes
0900..8340 is the value part (224 bytes)
9000      is the status word
Offset 0 corresponds to the value '09', offset 223 to '40'
  
```

All listed items below must have (one of) the expected value(s).

Offset	Length (bytes)	Description	Expected value
66	2	Build information (major / minor version)	'0x007c'
69	1	Security profile - FIPS 140-2 level 3 mode	'D2'
88	1	Dynamic reconfiguration disabled	'E1'
89	1	Templating disabled	'E1'
91	1	Reflashing disabled	'E1'

Table 9: Tag 'DF10'

Offset	Length (bytes)	Description	Expected value
32	1	GP Secure Channel Protocol of ISD	'02' or '03'
33	1	GP SCP implementation option of ISD - SCP 03	'00' or '10'
131	1	ISD supports GP command format	'E1'
132	1	GP configuration (GP ID or general GP)	'E1' or 'D2'

Table 10: Tag 'DF11'

# 4 Cryptographic Module Ports and Interfaces

*This chapter describes the ports and interfaces (physical and logical), the information passing over the four logical interfaces, data that pass over the physical ports, and the Trusted Channel.*

## 4.1 Communication Interfaces

### 4.1.1 Logical Interfaces

The Cryptographic Module works as a slave processor in order to process and respond to the reader's commands through a well-defined set of Application Protocol Data Units (APDUs) specified in the [GP] standard and some additional Infineon Proprietary APDUs.

Logical Interface	Description
Data input	The input data field of the APDU command involves the data input interface of the module. All input parameters must pass through this interface.
Data output	The output data field of the Response APDU command involves the data output interface of the module. All output data must pass through this interface.
Control input	The APDU command header (consisting of the CLA, INS bytes and control-related command parameters) involves the control input interface.
Status output	The status words SW1 and SW2 of the response APDU command involve the status output interface. All error codes and output indicators pass through this interface.

Table 11: *Logical Interface*

Moreover, the Cryptographic Module provides services to applets through a set of defined APIs:

1. Java Card API: This interface is defined by the specification of the basic functions in the Java Card run-time environment, this interface is used by the Applet Developer for the implementation of an applet that is installed in the TOE. Details can be found in [JCAPI].
2. IFX API: This API Packages build an API extensions that facilitate APDU processing and certain interactions with the IC platform
3. GlobalPlatform API: These interfaces extend the Java programming language with the `org.globalplatform.GPSystem` interfaces specified in [GP]. The API provides services to Applications (e.g. Cardholder verification, personalization, or security services). It also provides Card Content management services (e.g. card locking or Application Life Cycle State update) to Applications.

### 4.1.2 Physical Interfaces

The data-oriented I/O interface to the CM is formed by the I/O pad and by the various RF options. The RF interface (radio frequency power and signal interface) enables contactless communication between a PICC (proximity integration chip card, PICC) and a PCD reader/writer (proximity coupling device, PCD). The PCD must be compliant to ISO 14443 1-4 Type A or B. Power supply is received and data are received or transmitted by an antenna which consists of a coil with a few turns directly connected to the IC. Depending on customer orders, the contactless interface options are set by means of blocking either at Infineon premises or at the premises of the user.

The CM communicates with the Card Acceptance Device or card reader (CAD) through a contact-based interface (Figure 5) or a contactless-based interface. The CAD must be compliant with the ISO 7816 1-3 standard. At no time are private and secret keys, authentication data, or CSPs imported or exported in plaintext. The dedicated path is available by means of a GlobalPlatform Secure Channel.

At start-up, an ISO 7816 interface is established as the communication channel with the host for the duration of the session. During a session, all logical paths are carried on the chosen physical path. The interface with the host computer is a command-response interface, where all communication with the host is inhibited until a command is executed. In particular, a command to generate a key or key pair causes communication with the host to be suspended until the key generation is either completed successfully or aborted. At the conclusion of most operations, a response message is returned to the host containing only the return status code.

The CM has 8 ISO 7816 compliant electrical contacts referred to as C1 through C8 in Figure 5 and described in Table 12 below. However, C4, C6, and C8 are not electrically connected to the embedded IC pads shown in Figure 6 and are unused. Table 13 describes the IC pads and their logical interface type.





Figure 5: ISO 7816 Interface Contact Pad Designations and Locations

Contact	Designation	Use
C1	Vcc	Power connection through which operating power is supplied to the microprocessor chip in the card
C2	RST	Reset line through which the IFD can signal to the smart card's microprocessor chip to initiate its reset sequence of instructions
C3	CLK	Clock signal line through which a clock signal can be provided to the microprocessor chip. This line controls the operation speed and provides a common framework for data communication between the IFD and the ICC
C4	NC	Not used.
C5	GND	Ground line providing common electrical ground between the IFD and the ICC
C6	NC	Not used. Programming power connection only used to program EEPROM of first generation ICCs.
C7	I/O	Input/output line that provides a half-duplex communication channel between the reader and the smart card
C8	NC	Not used.

Table 12: CM ISO 7816 Interface Contact Assignments

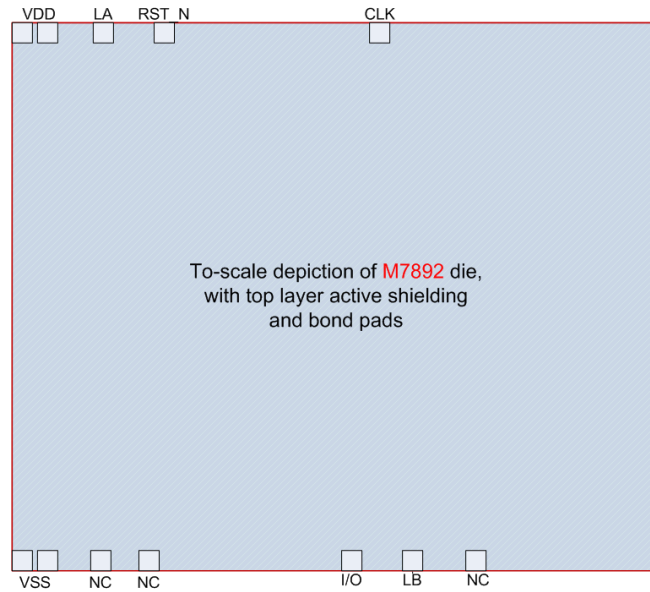


Figure 6: IC Die Pad Designations and Locations

Pad	Description	Logical Interface Type
VSS, VDD	ISO 7816: Power and ground	Power
CLK	ISO 7816: Clock	Control in
RST_N	ISO 7816: Reset	Control in
IO	ISO 7816: Serial interface	Data in, data out, control in, status out
LA, LB	ISO 14443: Antenna	Data in, data out, control in, status out, power
NC	No connect	Not used

Table 13: IC Pad Descriptions and Logical Interface Types

The minimum contact surface area is 1.7mm \* 2.0 mm. Contact dimensions for C1 through C8 are:

- Length - 85.5mm
- Width - 54.0mm
- Thickness - 0.80mm

Table 14 describes the connections between the logical interfaces and the physical interfaces.

Logical Interface	Physical Interface
Data input	Command Interface (C7)
Data output	Command Interface (C7)
Control input	Command Interface (C7)
Status output	Command Interface (C7)

Table 14: Logical Interfaces With Physical Interface Connections

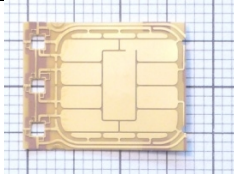
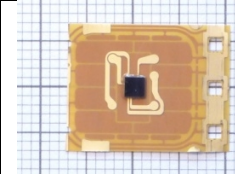
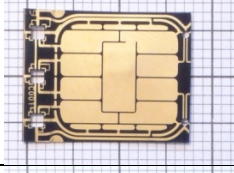
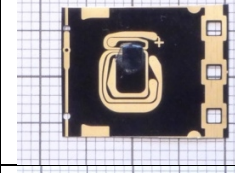
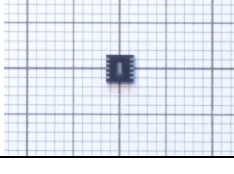
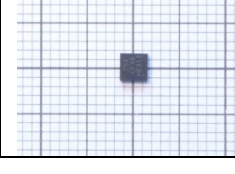
## 4.2 Packages

All product derivatives are identical from module design, layout and footprint, but are different in their possibilities to connect to different types of antennas or in their ability to be implemented in special packages for different form factors.

The CM covers 3 types of package families:

1. with ISO/IEC 7816-3 Interface Only
2. with ISO/IEC 14443 Interface Only
3. with ISO/IEC 7816-3 and ISO/IEC 14443

The following table contains the CM and Package combination Identifications:<sup>4</sup>

Packaging Id	Product and Package Combination	Front Image	Back Image
with ISO/IEC 7816-3 Interface Only			
S-MID4. 8- 8- 1	M7892B11, SLE 78CLFX400VPM		
S-MFC6. 8- 8- 1	M7892B11, SLE 78CLFX400VPM		
PG-USON10-1	M7892B11, SLE 78CLFX400VPM		

<sup>4</sup> The smallest squares of the background are 1mm x 1mm

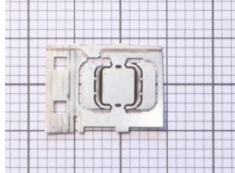
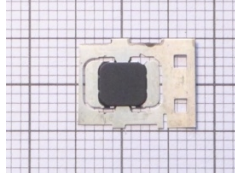
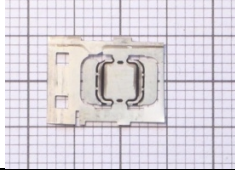
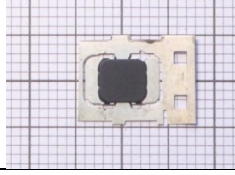
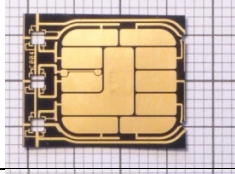
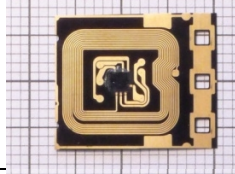
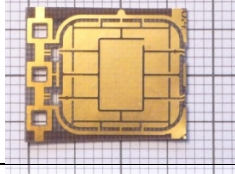
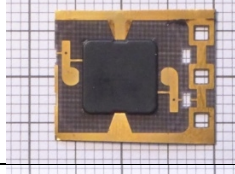
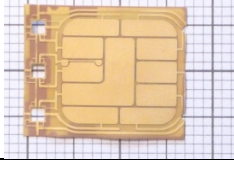
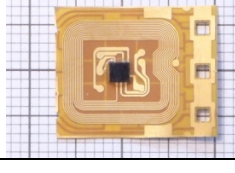
Packaging Id	Product and Package Combination	Front Image	Back Image
with ISO/IEC 14443 Interface Only			
P-MCS8-2-1	M7892B11, SLE 78CLFX400VPM		
P-MCC8-2-6	M7892B11, SLE 78CLFX400VPM		
with ISO/IEC 7816-3 and ISO/IEC 14443 Interfaces			
S-COMB. 6-6-1	M7892B11, SLE 78CLFX408APM		
P-MB. 4-8-3	M7892B11, SLE 78CLFX400VPM		
S-COM10. 6-6-1	M7892B11, SLE 78CLFX408APM		

Table 15: Supported Packages



# 5 Roles, Services and Authentication

*This chapter describes the roles, services, and authentication provided by the CM.*

## 5.1 Roles

The CM supports identity-based authentication. There are two roles that operators may assume: a Crypto Officer role and Developer role (see Table 16 below). The CM does not support concurrent operators and clears previous authentications on power cycle.

Role	Description	Authentication
Cryptographic Officer Role		
Card Manager/Crypto Officer (CO)	This role is responsible for card issuance and executable content management, security domains configuration and card content management via the Card Manager / Issuer Security Domain. The Crypto Officer authenticates to the module through the GlobalPlatform mutual authentication protocol based on symmetric cryptography (SCP-03). Once Crypto Officer is authenticated it is possible to execute the services provided by the (ISD). <u>This role can only be active when the ISD is currently selected.</u>	Identity type authentication by demonstrating the knowledge of secret AES keys such as OSD-KENC and OSD-KMAC during the first phase of Secure Channel (SCP03) Establishment with ISD.
User Role		
Applet Developer (Dev)	Considered an internal, privileged user of the platform. Entities in this role create and deploy smart card applets that utilize JavaCard APIs as the only means of	Identity type authentication based on SD-KENC and SD-KMAC during the first phase of Secure Channel (SCP03) Establishment with

	<p>communicating with OS internals. The Applet Developer is in charge of installing and managing their own applications in their respective Application Provider Security Domain (APSD) on the card. The Applet Developer must be authenticated to their respective Security Domain through GP's mutual authentication protocol based on SCP-03. They are represented on the card by their respective APSD.  <u>This role can only be active when the APSD is currently selected.</u></p>	<p>Application Provider's Security Domain. The Applet Developer must demonstrate the knowledge of secret AES keys that belong to the Application Security Domain associated with that Applet Developer.</p>
--	---	---

Table 16: Roles

## 5.2 Services

Services provided by the CM can be divided in two groups.

Services in the first group are available to off card entities. Such services are related to card content management (e.g. applet loading, installation, deletion, card data access or storage) accessed via communication protocols like ISO7816.

The second group of services is services available to on card entities, i.e. Java Card applets. These services are typically cryptographic services available via the Java Card API.

### 5.2.1 Card Management Services Available to off Card Entities

Card content management services can be further subdivided into two groups.

1) Services that do not handle CSPs and do not require authentication. For instance, applet selection or requesting publicly accessible data stored on the card. These services are accessible in CO, and DEV roles without a need for authentication.

2) The services in this group allow for modification or access of CSPs and perform card content management operations. For instance, applet installation and deletion, keyset placement and package loading/deletion. These services are critical to the overall security of the card and are accessible only to the CO and DEV roles usually by authenticating with a corresponding Security Domain.

### 5.2.1.1 Non Authenticated Services

Service	Description
CARD RESET (Self-test)	Power cycle the Module by removing and reinserting it into the contact reader slot, or by reader assertion of the RST signal. The Card Reset service will invoke the power on self-test sequence described in Section, and On any card reset, the card deletes the number of security exceptions thrown and clears its velocity checking counters.
INITIALIZE UPDATE	Initialize the Secure Channel; to be followed by EXTERNAL AUTHENTICATE when the session keys are generated. Does not use CSPs.
GET DATA	Retrieve one public data object. Does not use CSPs. GET DATA honors GP access control rules; see below for the variation of GET DATA for objects that require authentication.
SELECT	Select an applet, returning application template. Does not use CSPs.
MANAGE CHANNEL	An APDU command used over I/O interface to open or close a logical channel on that same interface.

Table 17: Unauthenticated Services

### 5.2.1.2 Services Requiring Authentication and Manipulating CSPs

Note that the only difference between the services provided to CO and those to Dev is the Security domain that they are interacting with. For instance, by sending an “EXTERNAL AUTHENTICATE” command, the CO can open an SCP session only with the ISD whereas the Dev will be only communicating with the APSD.

Service	Description	Keys and CSP's	CO	Dev	Level of Access
DELETE	Delete an applet, security domain or keyset from EEPROM. On any card reset, the card deletes the number of security exceptions and clears velocity counters.	OSD-SENC, OSD-SMAC (AES keys for GP secure channel operation)	X	X	w,e
GET STATUS	Retrieve information about the card. Does not use CSPs.	None	X	X	r,e
INSTALL	Informs the Card Manager that Card Content management steps are being processed. Uses the (GP secure channel operation).	OSD-SENC, OSD-SMAC (AES keys for GP secure channel operation)	X	X	r,w,e

Service	Description	Keys and CSP's	CO	Dev	Level of Access
LOAD	Sequence of these APDUs takes place to load a package (e.g. containing an applet).	OSD-SENC, OSD-SMAC (AES keys for GP secure channel operation)	X	X	w,e
STORE DATA	Transfer data to an application or Security Domain during command processing.	(O)SD-SENC, (O)SD-SMAC (AES keys for GP secure channel operation)	X	X	w,e
PUT KEY	This APDU command can load/add a new keyset to the card, replace one or several keys within an existing keyset or replace an existing keyset with a new key version.	(O)SD-SENC, (O)SD-SMAC (AES keys for GP secure channel operation); (O)SD-DEK (AES key for decryption of new key values).	X	X	w,e
SET STATUS	Modify the Card Manager's, Security Domain's or applet's life cycle status.	(O)SD-SENC, (O)SD-SMAC (AES keys for GP secure channel operation)	X	X	w,e
EXTERNAL AUTHENTICATE	Authenticates the operator and establishes a secure channel. Must be preceded by a successful INITIALIZE UPDATE.	(O)SD-KENC and (O)SD-KMAC to generate (O)SD-SENC and (O)SD-SMAC, respectively; (O)SD-KENC is also used in the channel authentication method (all keys mentioned are AES keys).	X	X	r,w,e

Table 18: Card Content Manager Services and their CSP Usage.

### 5.2.2 Cryptographic Services Available via Java Card API

The following cryptographic services are provided to Java Card applets installed on the card. Java Card applets are loaded and installed by the authenticated entity with the CO role or an entity authenticated with a Dev role. Therefore, Java Card applets are considered to be authenticated with a CO or Dev role when they access Java Card APIs.



Service	Description	Keys and CSP's	CO	Dev	Level of Access
Integrity and Data Origin Authentication	API providing to applets TDES MAC code Message Authentication Code as well as AES CMAC	TDES and AES keys	X	X	r,e
Secure Hashing	The implementation of this Java Card system API supports the [FIPS 180-4] compliant hash algorithms SHA	None	X	X	r,e
Random Number Generation	The implementation of the NIST SP 800-90A DRBG Java Card API interfaces	None	X	X	r,e
Digital Signature Generation and Verification	The implementation of this Java Card system API supports two different implementations of digital signature based on the following algorithms - EC DSA and RSA [PKCS#1] conformant with [FIPS 186-4]	DSA, RSA and ECDSA keys	X	X	r,e
Symmetric Key Generation	Generation of keys compliant with [NIST SP 800-90A]	TDES and AES keys	X	X	r,w,e
Asymmetric Key Generation	Generation of EC key pairs and RSA key pairs conformant with [FIPS 186-4]	DSA, RSA and ECDSA keys	X	X	r,w,e

Table 19: Cryptographic Services and Authentication services available to applet through the standard Java Card API

### 5.2.2.1 FIPS 140-2 Approved Algorithms

The CM implements the FIPS-approved algorithms listed in Table 20.

Algorithm	Description	Certificate
CTR_DRBG	[NIST SP 800-90A] CTR_DRBG (AES-128)	DRBG cert. #544
Triple-DES	[NIST SP 800-67] Triple Data Encryption Algorithm. The module supports the 2-Key and 3-Key options; CBC and ECB modes.	TDES cert. #1747
Triple-DES MAC	[FIPS PUB 113] TDES Message Authentication Code. Vendor affirmed, based on validated TDES.	Vendor affirmed, based on TDES cert. #1747

AES	[FIPS PUB 197] Advanced Encryption Standard algorithm. The module supports 128-, 192- and 256-bit key lengths ECB and CBC modes.	AES cert. #2941
AES CMAC	[NIST SP 800-38B] AES CMAC 128-, 192- and 256-bit key lengths (placeholder included for SCP03)	AES cert. #2941
RSA	[FIPS 186-4] RSA signature generation and verification (using scheme RSASSA-PKCS1-v1_5 from [PKCS#1]) and key pair generation. The module supports 2048-bit RSA keys.	RSA cert. #1544
RSA CRT	[FIPS 186-4] RSA CRT signature generation and verification (using scheme RSASSA-PKCS1-v1_5 from [PKCS#1]) and key pair generation. The module supports 2048-bit RSA CRT keys.	RSA cert. #1544
DSA	[FIPS 186-4] DSA key pair generation, signature generation and verification	DSA cert. #873
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm. The module supports the NIST defined P-224, P-256 curves.	ECDSA cert. #532
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms.	SHS cert. #2477

Table 20: FIPS Approved Cryptographic Algorithms

# 6 Security Requirements

*This chapter describes the security policy for the enforcement of identity based authentication and data, cryptographic key and code integrity, confidentiality and authenticity.*

## 6.1 Identification and Authentication of Roles

Identification and authentication of operators (off card entities with CO or Dev role) are done when establishing a Secure Channel via the SCP03 protocol between the off card entity and its respective Security Domain.

### 6.1.1 Identification

Identification of the CO is done via the APDU command INITIALIZE UPDATE where the CO proves his knowledge of the cryptographic key set (OSD-KENC and OSD-KMAC) that belongs to the Issuer Security Domain.

Identification of an entity with the Dev role is done via the command INITIALIZE UPDATE where the Dev proves his knowledge of the cryptographic key set (SD-KENC and SD-KMAC) that belongs to his respective Application Provider Security Domain.

### 6.1.2 Authentication

Authentication of CO is done via the APDU command EXTERNAL AUTHENTICATE which must be preceded by a successful completion of an INITIALIZE UPDATE command. In this step, the CO proves that the knowledge of the cryptographic set OSD-KENC and OSD-KMAC of the Issuer Security Domain (ISD). This is done with the OSD-KENC and OSD-KMAC (along with other information) used to derive the OSD-SENC and OSD-SMAC keys, respectively. The same is done by the ISD. The CO encrypts a message M known also by the ISD with OSD-SENC and sends the resulting encrypted message (EM) to the ISD. If the CO has the keys OSD-KENC and OSD-KMAC, the decryption of EM on the card results in the message M.

Note that authentication is mutual for both entities as the ISD proves its authenticity to the CO via the two commands INITIALIZE UPDATE and EXTERNAL AUTHENTICATE.

Authentication of Dev is done via the APDU command EXTERNAL AUTHENTICATE which must be preceded by an INITIALIZE UPDATE command. In this step, the Dev proves the knowledge of the cryptographic set SD-KENC and SD-KMAC of the Application Security Domain (APSD). This is done with the SD-KENC and SD-KMAC (along with other information) to derive the SD-SENC and SD-SMAC keys,

respectively. The same is done by the respective APSD. The Dev encrypts a message M known also by the APSD with SD-SENC and sends the resulting encryption EM to the APSD. If the Dev has the keys SD-KENC and SD-KMAC, the decryption of EM on the card will result in the message M.

Note that authentication is mutual for both entities as the APSD proves its authenticity to the Dev via the two commands INITIALIZE UPDATE and EXTERNAL AUTHENTICATE.

## 6.2 Integrity and Confidentiality of Loaded Application Code

Loading of application code is always done over SCP03. The code's integrity is protected against modification via the session key O(SD)-SMAC and for confidentiality via the session key O(SD)-SENC.

## 6.3 Authentication of Loaded Application Code

This section describes the mechanisms for loading application code on the card and the enforcement of its authentication on the card. Only FIPS validated application code shall be loaded onto the CM.

### 6.3.1 DAP Verification

The Card Manager in CO role loads and installs application code on the CM in APSD. From the perspective of the CO, the CO ensures the authenticity, confidentiality and integrity of the loaded on-card application code via a secure channel using CO keys.

DAP (short for Data Authentication Pattern) feature guarantees the authenticity of the Executable Load File by verifying on card the DAP signature of the Load File on behalf of the Controlling Authority or the respective Application Provider. On signature verification failure, the Executable File is not installed and on-card memory is reclaimed.

When an Application Provider requires that its Application code loaded on the card shall be checked for integrity and authenticity, the application code is accompanied by a DAP generated off-card by the DAP private cryptographic key of the respective Application Provider. On-card, the DAP is verified by the Application Provider public 2048 bit RSA key OS-DAP.

A Controlling Authority may also require that all Application code loaded onto the card be checked for integrity and authenticity. The latter is called Mandated DAP verification and is based on a DAP generated over the application code off-card with the Controlling Authority DAP private key. The DAP is verified on card with the Controlling Authority RSA public key. The key and algorithm used for DAP Verification or Mandated DAP Verification are implicitly known by the corresponding Security Domain and is based on RSA 2048-bit public key injected into this SD using PUT KEY APDU command. The mandated DAP verification is always active on the CM.

## 6.4 CSP Secure Management

### 6.4.1 Cryptographic Key and PIN Entry

The Module uses the SD-DEK or OSD-DEK keys to decrypt critical security parameters depending on whether it is the CO or a DEV role that performs the key entry operation. Note that SD-DEK and OSD-DEK are not used to perform encryption.

### 6.4.2 Cryptographic Keys and User PIN Contents Zeroization

All cryptographic session keys in the module used for Secure Channel operation are automatically zeroized (set to value of zero) by the Security Domain code upon closing of the Secure Channel. The persistent Crypto Officer, SSD or Applet's keysets are destroyed (set to the EEPROM's default value of 0xFF) upon hardware detection of any chip tampering either through micro-probing or FIB that results in card's lifecycle transitioned to TERMINATED. The same applies to the Global PIN value which is also zeroized by underlying hardware circuitry just prior to entering TERMINATED lifecycle.

### 6.4.3 Key Generation

The CM generates asymmetric cryptographic keys internally in accordance with FIPS 186-4 using the specified cryptographic key sizes (RSA and DSA 2048 bit and ECC from 224 to 521). If an approved key generation method requires input from an RNG, then the CTR\_DRBG is used according to NIST SP 800-90A.

### 6.4.4 Key Loading

The originating (default) keyset is placed in the non-volatile storage in the secure factory environment. Then, subsequent keys are loaded into the CM with a GlobalPlatform PUT KEY command APDU. This command is performed in the Crypto Officer (CO) role. Such command is used to accomplish the following:

- add a new keyset
- add a single key to existing keyset
- add an RSA public key used for DAP
- replace an existing keyset (when replacing default keyset, new keyset becomes a default one)
- replace a single key within an existing keyset

The keys can also be entered into the cryptographic module under the responsibility of the applets. In all instances the ISD and SSDs enforce secure entering of keys via Secure Channel protocols.

### 6.4.5 Key Storage

The on-card key storage validates key integrity before each crypto operation using a check value. In case of mismatch a security exception is generated (i.e. the security policy guarantees protection

against unauthorized substitution, modification or disclosure outside the CM). When stored, keys are treated as Java key objects where a JCRE firewall is used to guard against illegal access.

The access to cryptographic services or card keys assumes explicit authentication. After required authentication, the external entity gets the access to Security Domain. Included in the Domain are the keys accessible to authenticated user. The keys that belong to other Security Domains are not accessible per GlobalPlatform Card Specification 2.2.1, chapter 7.5 Security Domain Keys, chapter 7.6 Data and Key Management). In order to determine access rights for each key its Key Identifier and Key Version Number (section 7.5.1) is used. Therefore, access is guaranteed only to the keys in this domain. The keys used to perform API services inside the applet can exist as Java class instances. Their access is managed by JCRE Firewall based on ownership permissions.

#### 6.4.6 Key Establishment

The cryptographic module enforces key establishment via secure channel to communicate with a device where a session keyset is used. The module uses for key establishment the SCP03 protocol in FIPS mode. The SCP03 protocol is based on AES and CMAC algorithms with 128-bit, 192-bit, 256-bit keys and according to NIST SP 800-57.

#### 6.4.7 Key Distribution

The CM securely distributes keys via EC Diffie–Hellman using curves from 224 to 521.

P-Curves: P-224, P-256, P-384, P-521;

K-Curves: K-233, K-283, K-521; and

B-Curves: B-233, B-283, B-409.

Diffie-Hellman's algorithm based on Elliptic Curves cryptography and compliant with ANSI X9.63.

# 7 Physical Security

*This chapter describes the physical security provided by the CM. The CM employs physical security mechanisms that restrict unauthorized physical access to the contents of the module and deter unauthorized use or modification of the module (including substitution of the entire module) when installed. All hardware, software, firmware, and data components within the cryptographic boundary are protected.*

## 7.1 Physical Security Mechanisms

The embodiment of the Hardware part of the CM is a single chip with embedded firmware and can be delivered to the card issuer as a complete module, with or without inlay mounting, in the form of plain wafers, in an IC case (e.g. DSO20), or in bare dies. The CM design incorporates physical security mechanisms that include the following:

- Automatic zeroization.
- Tamper response and zeroization circuitry.
- Hard opaque tamper-evident coating on chip with a removal-resistant and penetration resistant enclosure.

The IC meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The IC uses standard passivation techniques and is protected by passive shielding (metal layer coverings opaque to the circuitry below) and active shielding (a grid of top metal layer wires with tamper response). A tamper event detected by the active shield places the CM permanently into the HELD IN RESET error state.

The IC is intended to be mounted in a plastic smartcard. Physical inspection of the card boundaries is not practical after mounting. Physical inspection of modules for tamper evidence is performed using a lot sampling technique during the card assembly process. The IC also provides a key to protect the module from tamper during transport.

# 8 Mitigation of Other Attacks

*This chapter describes how the single-chip cryptographic module and components provide protection for the CSPs against non-invasive attacks and the effectiveness of the mitigation techniques. Such types of attacks generally rely on the analysis of information obtained from sources physically external to the module. In all cases, the attacks attempt to determine some knowledge about the cryptographic keys and CSPs within the cryptographic module.*

## 8.1 Power and Electromagnetic Analysis Attacks

Attacks based on the analysis of power consumption can be divided into two general categories, Simple Power Analysis (SPA) and Differential Power Analysis (DPA).

- SPA involves a direct (primarily visual) analysis of electrical power consumption patterns and timings derived from the execution of individual instructions carried out by a cryptographic module during a cryptographic process. The patterns are obtained by monitoring variations in electrical power consumption of a cryptographic module for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently values of cryptographic keys.
- DPA utilizes advanced statistical methods and/or other techniques to analyze the variations of the electrical power consumption of a cryptographic module.

Corresponding threats (SEMA and DEMA techniques) exist from electromagnetic analysis.

### 8.1.1 Countermeasures

Countermeasures that may reduce the overall risk of Power Analysis attacks include the use of internal power sources and the manipulation of the individual operations of the algorithms or processes to level the rate of power consumption during cryptographic processing. The following items describe design features in the IC that mitigate the probability of successful Power and Electromagnetic attacks on software executing on the device.

- The IC contains an internal voltage regulator.
- The clock system enables the software to use powerful SPA, DPA, SEMA and DEMA counter measures.
- Clock system countermeasures are programmed at random during software execution through a dummy interrupt.



- The VFO output clock is jittered by random frequency jumps.
- Important parts of the IC are designed to counter leakage or side channel attacks like DPA/SPA or EMA/DEMA.

## 8.2 Timing Analysis Attacks

Timing Analysis attacks precisely measure the time required by a cryptographic module to perform specific mathematical operations associated with a cryptographic algorithm or process. Collected timing information is analyzed to determine the relationship between inputs to the module and the cryptographic keys used by the underlying algorithms or processes. Analysis of the relationship may be used to exploit the timing measurements to reveal the cryptographic key or CSPs.

### 8.2.1 Countermeasures

Timing Analysis attacks assume that the attacker has knowledge of the design of the cryptographic module. The CM design has the following characteristics that eliminate the possibility an attacker can use knowledge of the design to conduct a timing analysis attack:

- The CPU uses a non-standard command set.
- The CPU is proprietary with a non public bus protocol.
- The IC design is non-standard to mitigate attacks that use standard analysis methods.
- In the IC design, a number of components are automatically synthesized and mixed to disguise their physical borders so that external analysis is more difficult.

Manipulation of the individual operations of the algorithms or processes to reduce timing fluctuations during processing is one method to reduce the risk of this attack:

- Timing and current consumption is almost independent of the processed data and protected by other protection means.
- Collecting physical data from the IC is difficult to perform.

## 8.3 Fault Induction Attacks

Fault Induction attacks utilize external forces such as microwaves, temperature extremes, and voltage manipulation to cause processing errors within the cryptographic module. An analysis of these errors and their patterns can be used in an attempt to reverse engineer the cryptographic module, revealing certain features and implementations of cryptographic algorithms and subsequently revealing the values of cryptographic keys. This is, for example the basis of Bellcore and DFA attacks.

### 8.3.1 Countermeasures

Cryptographic modules with limited physical security appear to be at greatest risk. Proper selection of physical security features may be used to reduce the risk of this attack. The following countermeasures from Chapter 6 are also effective countermeasures for fault induction:

- Encryption - data is dynamically encrypted, masked, scrambled, transparently relocated, randomized and topologically protected.
- Error Detection Code - An error detection code (EDC) covers the memory system of RAM, ROM and SOLID FLASH™ and includes also the MED, MMU and the bus system. Introduced failures are securely detected and in terms of single bit errors in the SOLID FLASH™ also automatically corrected. An EDC value is calculated in order to prevent accidental bit faults during production writing over data stored in ROM.
- Dual CPUs - Two CPUs computing on the same data with the results of both compared at the end, requires that a fault induction attack would have to be done on both CPUs at the correct place with the correct timing. The detection of an incorrect calculation is stored and the IC enters a defined secure state which causes the chip internal reset process.
- User Mode Security Life Control - During start up, the UMSLC checks the alarm lines and number of functions and sensors for correct operation. If attempts to modify security features are detected, the UMSLC generates an alarm and the IC enters a security reset state.
- Watchdog Timer and Check Point Register - Enables the user to check the correct processing time and integrity of program flow. Another countermeasure is the implementation of backward calculation in the SCP that enables discovery of induced errors.
- Monitored Hardware Handshake - All communication via the busses in the IC is protected by a monitored hardware handshake. If the handshake is not successful an alarm is generated.

# 9 Self-Tests

*The CM uses power-up and conditional self-tests to ensure that the module is functioning properly. The power-up self-tests are initiated automatically upon reception of the first APDU command sent to the module after reset. All self-tests must be successfully completed before the module can enter FIPS-approved mode of operation. The module's power-up self-tests include a known-answer cryptographic algorithm test for each cryptographic function, such as encryption, decryption, authentication, and deterministic random number generation of each FIPS-approved cryptographic algorithm. The full set of built-in power-up self-tests are conducted. The conditional self-tests are invoked when the applicable security function or operation is required.*

*If an error occurs on any self-test, the CM transitions to Fatal Error state and does not provide any Cryptographic or User services until reset.*

## 9.1 Power Up Self -Tests

The power-up self-tests are initiated automatically upon reception of the first APDU command sent to the module after reset or power up. The full set of self-tests must be successfully completed before the module will respond to any commands. If an error occurs on any of the power-up self-tests, the CM transitions to Fatal Error state and does not provide any Cryptographic or User services until reset.

The power-up self-tests consist of two parts. The first part only contains a Deterministic Random Number Generator Test that runs automatically after every Reset. The second part contains various encryption algorithm tests that are executed upon receipt of the first APDU command which should be the Answer-to-Reset (ATR) APDU.

The power up self-tests are triggered any time the card is reinserted into the card terminal. All power-up self-tests are executed

### 9.1.1 Deterministic Random Number Generator Test

This test is performed immediately upon start/reset. The NIST SP 800-90A compliant Deterministic Random Number Generator is tested to ensure that the relevant crypto algorithms can use it during normal operations. If the test fails, the module transitions to the Fatal Error state where it stays until the next Reset or Power off.

### 9.1.2 Cryptographic Algorithm Known Answer Tests

- TDES CBC MAC KAT
- TDES Encrypt/Decrypt KAT
- AES CMAC KAT
- AES Encrypt/Decrypt KAT
- SHA-1 KAT
- SHA-224 KAT
- SHA-256 KAT
- SHA-384 KAT
- SHA-512 KAT
- RSA 2048 KAT
- DSA KAT
- ECC KAT

### 9.1.3 Software/Firmware Integrity KAT

The checksum of the entire code in the flash memory is calculated using CRC16 and the result is compared with the expected checksum. If the checksums do not match, the module transitions to the Fatal Error state. The module does not provide any Cryptographic or User services in this state.

### 9.1.4 Critical Functions Tests

A CRC-16 Known Answer Test is also performed at power up.

## 9.2 Conditional Self-Tests

The CM performs the following self-tests whenever the conditions specified for the tests occur. If an error occurs on any of the conditional self-tests, the CM transitions to Fatal Error state and does not provide any Cryptographic or User services until reset.

### 9.2.1 Pair-wise Consistency Test (for public and private keys)

The following pair-wise consistency tests are performed on generation of a key pair:

- RSA pair-wise consistency test with sign/verify operation
- ECDSA pair-wise consistency test with sign/verify operation
- DSA pair-wise consistency test with sign/verify operation

### 9.2.2 Firmware Load Test.

When an application is loaded, its code is also transmitted through APDU commands to the card. This is done when the (I)SD receives an INSTALL[for load] command, followed by a sequence of LOAD

commands. When installing an application, the CO provides a DAP RSA 2048 bit signature that is verified at the end of the loading process. If the DAP RSA signature verification fails, then the loading is aborted.

Whenever a new software module (CAP file) is downloaded to the card, the CRC-16 checksum is calculated and saved in a registry associated with the CAP file. Multiple CAP files can be downloaded to the card. At this stage, none of the software in the modules is active. The software becomes activated when an APDU is received to select any of the applets contained in the module.

In addition, when an APDU is received to select an applet, the CM determines which CAP file contains the applet and recalculates the CRC-16 checksum on the CAP file. If the newly calculated checksum matches the one in the registry, the applet is selected and is available for processing. If the test fails, the CM transitions to Fatal Error state and will not provide any user services until reset.

As part of Card Administration functions, it is also possible to download Supplemental Security Domains (SSD). The SSD can be downloaded through the Issuer Security Domain (ISD). If downloaded through the ISD, the Load File Data Hash Block is checked. If the SSD is downloaded through another SSD which has integrated Card Management privileges, then the Load File Data Hash Block is checked as well as its cryptographic signature (DAP). The Load File Data Hash Block is verified with a FIPS-approved algorithm.

Note that the entire Templating mechanism which has the capability to pre-personalize the CM in a fast process is only available in OP\_READY state during production (Phase 5 of the smart card life-cycle) and is deactivated once the card is initialized. Template is not available in the field (after delivery) which is why a dedicated SW/FW Load Test is not required.

### 9.2.3 Key Entry Tests

All key operations are handled by the PUT KEY operation.

Symmetrical Keys (AES) are transmitted encrypted together with a (Key Check Value) that is checked by the module to verify correct decryption of the key. The KCV is the first 3 bytes of the cryptogram generated when encrypting 8 bytes of '00' with the symmetrical key.

### 9.2.4 Continuous RNG Testing

The CM uses the NIST SP 800-90A CTR\_DRBG using AES for generating random numbers. The seed value is generated by a hardware register. The AES algorithm is tested only once during the power up self tests (See section 9.1.1. Deterministic Random Number Generator Test.) The hardware register seed value is tested each time a new random number is generated. The test consists of generating two values from the hardware register and verifying that the values are different.

### 9.2.5 Bypass Testing

The CM does not allow any bypass capability.

# 10 Security Policy - Check List Tables

*This chapter provides the information required by FIPS 140-2 in terms of relation between roles, services and CSP and their security properties.*

## 10.1 Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Dev	AES authentication	AES secret keys
CO	AES authentication	AES secret keys

Table 21: Roles and Required Identification and Authentication - Check-List

## 10.2 Strength of Authentication Mechanisms

Role	Authentication Mechanism	Strength of Authentication Mechanism
CO	Based on or AES 128 (SCP03) keys	$1/2^{128}$ (See bulleted items below)
Dev	Based on AES 128 (SCP03) keys	$1/2^{128}$ (See bulleted items below)

Table 22: Strength of Authentication Mechanisms - Check-List

- The SCP03 protocol is based on AES algorithms with 128-bit, 192-bit, 256-bit key lengths. The CM derives session keys from the master keys, do a handshake, performs mutual authentication and decrypts data for internal use only. It encrypts one bloc which is the mutual authentication cryptogram over the life of the session encryption key (decrypted data is never output by the CM). Therefore, the minimum strength of the mutual authentication relies on minimum AES key length which is 128 bit. Thus, based on a single authentication attempt, there are  $2^{128}$  possible mutual authentication cryptogram blocks and the minimum probability that a random attempt at authentication will succeed is  $1/2^{128}$ .
- The probability that a random attempt will succeed over a one minute period is limited by Global Platform velocity checking: the CM detects more than 3 failed attempts and inserts

random (1 – 5 second) time delays. This mechanism limits the rate of failure in a one minute period to  $24/2^{128}$ , less than 1 in 100,000 as required by FIPS 140-2.

### 10.3 Services Authorized for Roles

Role	Authorized Services
CO	Services available for off card entities described in Section 5.2.1 and services available for applets in Section 5.2.2
Dev	Services available for off card entities described in Section 5.2.1 and services available for applets in Section 5.2.2

Table 23: Services Authorized for Roles - Check-List

### 10.4 Access Rights Within Services

CSP	Service	Role	Types of Access
OSD-KENC , OSD-KMAC (used to authenticate CO)	EXTERNAL AUTHENTICATE	CO	Execute
OSD-SENC, OSD-SMAC (CO session keys generated)	EXTERNAL AUTHENTICATE	CO	Create
SD-KENC , SD-KMAC (used to authenticate Dev)	EXTERNAL AUTHENTICATE	Dev	Execute
SD-SENC, SD-SMAC (Dev session keys generated)	EXTERNAL AUTHENTICATE	Dev	Create
No use of CSP	INITIALIZE UPDATE	CO, Dev	N/A

CSP	Service	Role	Types of Access
No use of CSP	GET STATUS	No authentication	N/A
No use of CSP	SELECT	No authentication	N/A
OSD-SENC, OSD-SMAC (Secure Channel must be already set up, keys here used to decrypt inbound data)	DELETE	CO	Execute
OSD-SENC, OSD-SMAC (Secure Channel must be already set up, keys used for preserving confidentiality and integrity of the inbound keys)  OSD-KEK (for decrypting the inbound keys)	PUT KEY	CO	Execute
SD-SENC, SD-SMAC (Secure Channel must be already set up, keys used for preserving confidentiality and integrity of the inbound keys)  SD-KEK (for decrypting the inbound keys)	PUT KEY	Dev	Execute
OSD-SENC, OSD-SMAC (Secure Channel must be already set up, keys used for enforcing integrity and confidentiality of input sent to CM)	INSTALL	CO	Execute



CSP	Service	Role	Types of Access
SD-SENC, SD-SMAC (Secure Channel must be already set up, keys used for enforcing integrity and confidentiality of input sent to CM)	INSTALL	Dev	Execute
OSD-SENC, OSD-SMAC	LOAD	CO	Execute
SD-SENC, SD-SMAC	LOAD	Dev	Execute
OSD-SENC, OSD-SMAC (Secure Channel must be already set up, keys used for integrity of the loaded data)	STORE DATA	CO	Execute
SD-SENC, SD-SMAC (Secure Channel must be already set up, keys used for integrity of the loaded data)	STORE DATA	Dev	Execute
OSD-KENC, OSD-KMAC (Secure Channel must be already set up, keys used for integrity of the loaded data)	SET STATUS	CO	Execute
SD-KENC, SD-KMAC	SET STATUS	Dev	Execute
OS-MKEK, OS-GPIN <sup>5</sup>	n/a	n/a	n/a

---

<sup>5</sup> The OS-MKEK will be used only if the OS-GPIN is used by a loaded application and the OS-GPIN is only used by a loaded application. No specific service is related to those CSPs, the CM provide only the possibility for their zeroization.

CSP	Service	Role	Types of Access
OS-DAP	PUT KEY	CO	Write

Table 24: Access Rights Within Services - Check-List

### 10.5 Physical Security Requirements

Infineon SLE 78 (SLJ 52) chip card is designed to meet FIPS 140-2 Level 3 requirements for physical security

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection Test/Guidance Details
Automatic zeroization.	N/A	N/A
Tamper response and zeroization circuitry.	N/A	N/A
Hard opaque tamper-evident coating on chip with a removal-resistant and penetration resistant enclosure	N/A	N/A

Table 25: Physical Security Requirements - Check-List

### 10.6 Mitigation of Other Attacks

Other Attacks	Mitigation Mechanisms	Specific Limitations
Power and Electromagnetic analysis	Countermeasures described in Section 9.1.1	n/a
Timing analysis	Countermeasures described in Section 9.2.1	n/a
Fault Induction	Countermeasures described in Section 9.3.1	n/a

Table 26: Mitigation of Other Attacks - Check-List



ANNEX

# A References

[JCVM3]	Java Card Platform, version 3.0.1 (May 2009), Classic Edition, Virtual Machine (Java Card VM) Specification. Published by Oracle Corporation.
[JCAPI3]	Java Card Platform, version 3.0.1 (May 2009), Classic Edition, Application Programming Interface, May 2009. Published by Oracle Corporation.
[JCRE3]	Java Card Platform, version 3.0.1 (May 2009), Classic Edition, Runtime Environment (Java Card RE) Specification. May 2009. Published by Oracle Corporation.
[GP_ID]	GlobalPlatform Card ID Configuration Version 1.0, December 2011 (GPC_GUI_039)
[JCDG]	Java Card™ applet developer's guide
[VOPS]	Open Platform Card Specification, v2.0.1', Visa International
[VOPI]	Visa Open Platform Card Implementation Specification - march 1999, Visa International
[ISO7816-1]	ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 1: Physical Characteristics
[ISO7816-2]	ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 2: Dimension and Location of the contacts
[ISO7816-3]	ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 3: Electronic signals and transmission protocol
[NIST SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators , NIST Special Publication 800-90A, January 2012.
[FIPS PUB 140-2]	National Institute of Standards and Technology, FIPS 140-2 standard. Security Requirements for Cryptographic Module.
[FIPS140-2A]	National Institute of Standards and Technology, FIPS 140-2 Annex A: Approved Security Functions.
[FIPS140-2B]	National Institute of Standards and Technology, FIPS 140-2 Annex B: Approved Protection Profiles,
[FIPS140-2C]	National Institute of Standards and Technology, FIPS 140-2 Annex C: Approved Random Number Generators
[FIPS140-2D]	National Institute of Standards and Technology, FIPS 140-2 Annex D: Approved Key Establishment Techniques

[NIST SP 800-67]	National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, January 2012
[GP]	GlobalPlatform Card Specification, Version 2.2, March 2006
[PP]	Java Card Protection Profile - Open Configuration, Version 3.0, May 2012 Oracle Corporation.
[1]	Security IC Platform Protection Profile, Version 1.0, 15.06.2007, BSI-PP-0035
[2]	National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001.
[3]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007.
[4]	National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, January 2012
[5]	National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-3, June, 2009.
[6]	RSA Laboratories, PKCS #1 v2.1: RSA Cryptography Standard, June 14, 2002
[7]	RSA Laboratories East, PKCS #1: RSA Encryption, Version 1.5, March 1998
[8]	National Institute of Standards and Technology, Secure Hash Standard (SHS), Federal Information Processing Standards Publication 180, October 2008.
[12]	National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Elaine Barker and John Kelsey, Special Publication 800-90A, January 2012
[13]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Morris Dworkin, Special Publication 800-38, May 2004
[14]	Network Working Group, The AES-CMAC Algorithm, Request for Comments: 4493, JH. Song, R. Poovendran, J. Lee, T. Iwata, June 2006
[15]	NIST: FIPS publication 186-3: Digital Signature Standard (DSS), June 2009

[16]	IETF: RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010, <a href="http://www.ietf.org/rfc/rfc5639.txt">http://www.ietf.org/rfc/rfc5639.txt</a>
[17]	Functionality classes and evaluation methodology for physical random number generators taken from AIS31, Version 1, 25.09.2001
[18]	Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography, November 20, 2001.

## ANNEX

# B Acronyms

Acronyms	Definitions
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Application Provider
APB	Advanced Peripheral Bus
API	Application Programming Interface
APSD	Application Provider Security Domain
ATR	Answer To Reset
AXI	Advanced eXtensible Interface Bus Protocol
CAD	Card Acceptance Device
CBC	Cipher Block Chaining
CI	Chip Identification Mode (STS-CI)
CIM	Chip Identification Mode (STS-CI), same as CI
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRT	Chinese Remainder Theorem
Crypto2304T	Asymmetric Cryptographic Processor

CO	Crypto Officer
CRC	Cycling Redundancy Check
CSP	Critical Security Parameters
DAP	Data Authentication Pattern
DES	Data Encryption Standard
DFA	Differential Failure Analysis
DPA	Differential Power Analysis
DRBG	Deterministic Random Bit Generator
EC	Elliptic Curve Cryptography
ECC	Error Correction Code
EDC	Error Detection Code
EDU	Error Detection Unit
ECB	Electronic Code Book
EMA	Electromagnetic analysis
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
FL	Flash Loader
Flash	SOLID FLASH™ Flash Memory
HW	Hardware
IC	Integrated Circuit
ICO	Internal Clock Oscillator
ID	Identification
IMM	Interface Management Module

ICC	Integrated Circuit Card
ISO	International Organization for Standardization
ITP	Interrupt and Peripheral Event Channel Controller
ITSEC	Information Technology Security Evaluation Criteria
I/O	Input/Output
IRAM	Internal Random Access Memory
JC	Java Card™
JCRE	Java Card™ Runtime Environment
MAC	Message Authentication Code
MED	Memory Encryption and Decryption
MMU	Memory Management Unit
NDRNG	Non Deterministic Random Number Generator
NVM	Non-volatile Memory
OS	Operating system
OP	Open Platform
PEC	Peripheral Event Channel
PC	Personal Computer
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PRNG	Pseudo Random Number Generator
PROM	Programmable Read Only Memory
RAM	Random Access Memory
RFI	Radio Frequency Interface
RFU	Reserved for Future USE



RMS	Resource Management System
RNG	Random Number Generator
ROM	Read only Memory
RSA	Rives-Shamir-Adleman Algorithm
SAM	Service Algorithm Minimal
SCP	Symmetric Cryptographic Processor
SF	Security Feature
SFR	Special Function Register, as well as Security Functional Requirement
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
STS	Self Test Software
SW	Software
SO	Security objective
TDES	Triple-DES
TM	Test Mode (STS)
TRNG	True Random Number Generator
WDT	Watch Dog Timer
XRAM	eXtended Random Access Memory

This Page Intentionally Blank