SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-091 CR Certification Report

Issue 1.0   22 November 2016

Feitian FT-JCOS v1.0/0.106.13 running on Infineon M7892 B11

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.1   11.11.2011

SERTIT, Postboks 814, 1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09   E-mail: post@sertit.no   Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognized under the terms of the CCRA July 2nd 2014. The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual recognition under SOGIS MRA applies to components up to EAL 4.

Contents

1 Certification Statement

Feitian Technologies Co., Ltd FT-JCOS v1.0/0.106.13 is an open Java Card Platform that is compliant with Java Card Specification v2.2.2 and GlobalPlatform Specification v2.1.1 supporting post-issuance functionalities for downloading Java Card compliant applets.

Feitian FT-JCOS v1.0 version 0.106.13 running on Infineon M7892 B11 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 5+ augmented with AVA_VAN.5 and ALC_DVS.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended by FPT_EMSEC.1, and FCS_RNG.1 functionality in the specified environment when running on the platforms specified in Annex A. It has also met the requirements of Protection Profile Java Card Protection Profile - Open Configuration Version 3.0.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Arne Høye Rage Quality Assurance Arne H. Rage
Approved	Kristian Bae Head of SERTIT Bae
Date approved	22 November 2016

2 Abbreviations

ATR	Answer to Reset
AES	Advanced Encryption Standard
CAP	Converted Applet
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
CPU	Central Processing Unit
CR	Certification Report
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
GP	GlobalPlatform
HAL	Hardware Abstraction Layer
HW	Hardware
IC	Integrated Circuit
ISD	Issuer Security Domain
IT	Information Technology
JCP	Java Card Platform
JCRMI	Java Card Remote Method Invocation
MED	Memory Encryption/Decryption Unit
MMU	Memory Management Unit
NVM	Non-volatile Memory
OS	Operating System
PP	Protection Profile

RAM	Random-Access Memory
RSA	Rivest, Shamir, Adleman Public Key Encryption
SCP	Secure Channel Protocol
SERTIT	Norwegian Certification Authority for IT Security
SFR	Security Functional Requirements
SSD	Supplementary Secure Domain
ST	Security Target
SW	Software
TOE	Target of Evaluation
TSF	TOE Security Functions

3 References

[1] FT-JCOS v1.0/0.106.13 Security Target, Version 1.0.12, 8 April 2016

[2] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[7] Composite product evaluation for Smartcards and similar devices, Supporting document, CCDB-2012-04-001, Version 1.2, April 2012

[8] JIL Attack Methods for Smartcards and Similar Devices, Version 2.2, January 2013

[9] JIL Application of Application Attack Potential to Smart Cards, Version 2.9, May 2013

[10] Evaluation Technical Report of FT-JCOS v1.0/0.106.13, 16-RPT-425 Version 2.0, 2 November 2016.

[11] FT-JCOS v1.0/0.106.13 User Manual, version 1.0.4, 4 March 2016

[12] FT-JCOS v1.0/0.106.13 Administrator Manual, version 1.0.5, 4 March 2016

[13] Java Card Protection Profile – Open Configuration, Version 3.0, May 2012

[14] Security IC Platform Protection Profile with Augmentation Packages Version 1.0. 2014.

[15] Machine Readable Travel Document with "ICAO Application", Basic Access Control. March 2009.

[16] Machine Readable Travel Document with "ICAO Application", Extended Access Control, Version 1.10. March 2009.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of FT-JCOS v1.0 version 0.106.13 to the Sponsor, Feitian Technologies Co., Ltd, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target [1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was FT-JCOS v1.0 and version 0.106.13.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Feitian Technologies Co., Ltd.

The TOE is a Java Card Platform compliant with Java Card Specification v.2.2.2 and GlobalPlatform Specification v.2.1.1. The TOE allows post-issuance downloading of applications that have been previously verified by an off-card trusted IT component.

It constitutes a secure generic platform that supports multi-application runtime environment and provides facilities for secure loading and interoperability between different applications.

The TOE does not implement JCRMI and does not include any software on the application layer.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

An overview of the TOE's security architecture can be found in Annex B.

4.3 TOE scope

The TOE scope is described in the Security Target [1], chapter 2.

4.4 Protection Profile Conformance

The Security Target [1] claimed conformance to the following protection profile:

Java Card Protection Profile - Open Configuration Version 3.0

4.5 Assurance Level

The Security Target [1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 5+, augmented by AVA_VAN5 and ALC_DVS.2 and extended by FPT_EMSEC.1, and FCS_RNG.1

functionality. Common Criteria Part [4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [2].

4.6 Security Policy

The TOE security policies are detailed in Security Target [1] , chapter 5.3.

4.7 Security Claims

The Security Target [1] fully specifies the TOE's security objectives, the threats and OSP's which these objectives counter or meet and security functional requirements and security functions to elaborate the objectives. Most of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

The following SFR's are defined in the Protection Profiles [14] and [15]/[16]: FCS_RNG.1 and FPT_EMSEC.1.

4.8 Threats Countered

All threats that are countered are described in the Security Target [1], chapter 5.2.

4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

4.10 Threats and Attacks not Countered

No threats or attacks are described that are not countered.

4.11 Environmental Assumptions and Dependencies

The assumptions that apply to this TOE are described in the Security Target [1], chapter 5.4.

4.12 IT Security Objectives

The security objectives that apply to this TOE are described in the Security Target [1], chapter 6.1.

4.13 Non-IT Security Objectives

The security objectives for the environment are described in the Security Target [1], chapter 6.2.

4.14 Security Functional Requirements

The security functional requirements are described in the Security Target [1], chapter 7.1.

Below, it is copied the list of the claimed SFR.

Security Functional Requirements	
FAU_ARP.1	Security alarms
FCO_NRO.2/CM	Enforced proof of origin
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.3	Cryptographic key access
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FCS_RNG.1	Quality metric for Random Numbers
FDP_ACC.1/GPG	Subset access control
FDP_ACC.2/ADEL	Complete access control
FDP_ACC.2/FIREWALL	
FDP_ACF.1/ADEL	Security attribute based access control
FDP_ACF.1/FIREWALL	
FDP_ACF.1/GPG	
FDP_IFC.1/JCVM	Subset information flow control
FDP_IFC.2/CM	Complete information flow control
FDP_IFF.1/CM	Simple security attributes
FDP_IFF.1/JCVM	
FDP_ITC.2/INSTALLER	Import of user data with security attributes
FDP_RIP.1/ABORT	Subset residual information protection
FDP_RIP.1/ADEL	
FDP_RIP.1/APDU	
FDP_RIP.1/bArray	
FDP_RIP.1/KEYS	
FDP_RIP.1/OBJECTS	

FDP_RIP.1/ODEL	
FDP_RIP.1/TRANSIENT	
FDP_ROL.1/FIREWALL	Basic rollback
FDP_SDI.2	Stored data integrity monitoring and action
FDP_UIT.1/CM	Data exchange integrity
FIA_UID.1/CM	Timing of identification
FIA_UID.1/GPG	
FIA_UID.2/AID	User identification before any action
FIA_USB.1/AID	User-subject binding
FMT_MSA.1/ADEL	Management of security attributes
FMT_MSA.1/CM	
FMT_MSA.1/GPG	
FMT_MSA.1/JCRE	
FMT_MSA.1/JCVM	
FMT_MSA.2/FIREWALL_JCVM	Secure security attributes
FMT_MSA.3/ADEL	Static attribute initialization
FMT_MSA.3/CM	
FMT_MSA.3/FIREWALL	
FMT_MSA.3/GPG	
FMT_MSA.3/JCVM	
FMT_MTD.1/JCRE	Management of TSF data
FMT_MTD.3/JCRE	Secure TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMF.1/ADEL	
FMT_SMF.1/CM	
FMT_SMF.1/GPG	
FMT_SMR.1	Security roles
FMT_SMR.1/ADEL	
FMT_SMR.1/CM	

FMT_SMR.1/GPG	
FMT_SMR.1/INSTALLER	
FPR_UNO.1	Unobservability
FPT_EMSEC.1	TOE Emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_FLS.1/ADEL	
FPT_FLS.1/INSTALLER	
FPT_FLS.1/ODEL	
FPT_RCV.3/INSTALLER	Automated recovery without undue loss
FPT_RCV.3/SCP	
FPT_RCV.4/SCP	
FPT_TDC.1	Inter-TSF basic TSF data consistency
FTP_ITC.1/CM	Inter-TSF trusted channel

4.15 Security Function Policy

User data and TSF data shall not be accessible/created/modified/deleted from the TOE except when the card issuer's policy and Java Card System policy are satisfied as defined by GlobalPlatform 2.1.1 specification and Java Card 2.2.2 specification respectively.

The card issuer's policy is implemented by the TOE as part of the card content management functionalities, specifically by the card manager. Access to card content management functionalities are enforced by the requirement of mutual authentication with the related security domain.

The Java Card System policy is enforced by the firewall which is implemented by TOE as part of the Java Card virtual machine. The policy is always active during runtime.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [1], which prospective consumers are advised to read. To ensure that the Security Target [1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [4] and Common Evaluation Methodology (CEM) [6]. Supporting documentation guidance is followed in accordance to Composite product evaluation for Smart Cards and similar devices [7]. Interpretations [8][9] are used as part of the vulnerability analysis.

SERTIT monitored the evaluation which was carried out by Brightsight B.V. as Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[10] to SERTIT on 2 November 2016. As a result SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target [1] with reference to the assumed operating environment specified by the Security Target [1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3 [4]. These classes comprise the EAL5 assurance package augmented with AVA_VAN.5 and ALC_DVS.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.5	Complete semi-formal functional specification with additional error information
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-structured internals
	ADV_TDS.4	Semiformal modular design
	ADV_COMP.1	Design compliance with the platform certification report, guidance and ETR_COMP
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.5	Development tools CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.2	Compliance with implementation standards
	ALC_COMP.1	Integration of the application into the underlying platform and Consistency check for delivery and acceptance procedures
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_TSS.1	TOE summary specification

	ASE_COMP.1	Consistency of Security Target
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Testing: modular design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
	ATE_COMP.1	Composite product functional testing
Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis
	AVA_COMP.1	Composite product vulnerability assessment

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target [1]. The results of this work were reported in the ETR [10] under the CC Part 3 [4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version of its constituent components has been supplied, and to check that the security of the TOE has not been compromised in delivery.

The delivery procedure is described in the supporting document [12].

5.3 Installation and Guidance Documentation

Installation procedures are described in detail in the supporting document [12].

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Security IC Embedded Software shall follow the guidance documentation [11][12] for the TOE in order to ensure that the TOE is operated in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

An independent vulnerability analysis was done, consisting of the following steps:

- A vulnerability analysis is performed using as input the findings from the previous evaluation work. The aim of the previous evaluation work is focused on the identification of potential vulnerabilities that could be exploited by attack methods documented from public and private information sources. The output of the vulnerability analysis is a penetration test plan.
- The devised penetration test plan is assessed against the penetration test of the previous evaluation work; which evaluated the same TOE version. From the results of analysis, penetration testing is adjusted.
- The penetration tests are performed according the adjusted penetration test plan.
- The evaluator performs a continuous follow-up on advances on attack methods as well as for new attack methods that is published during the time of the evaluation. When a new attack method is identified to impact the TOE, an impact assessment is performed. From this analysis, the process might return to the first point.

5.6 Developer's Tests

The developer tests consist of different parts, focused on the different core components as described in Annex B.

Testing is performed using engineering samples as well as simulators provided by the underlying platform manufacturer.

Defined test plan are identified in a set of 5 different test suites focused on:

- Java Card 2.2.2 specification compliance
- GlobalPlatform 2.1.1 specification compliance
- ISO/IEC 7816 and ISO/IEC 14443 Communication protocol compliance
- Proprietary test suite covering Java Card and GlobalPlatform functionalities
- Proprietary test suite covering Security Mechanisms using simulators
- Proprietary test suite covering Module's interactions using simulators

5.7 Evaluators' Tests

The evaluator's responsibility for performing independent testing is required by the ATE_IND class.

Since developer's testing procedures have been found to be extensive and thorough, and developer's hardware testing tools are not generally available to allow reproduction of developer test cases in the test lab, the choice was made to perform the evaluator independent testing by witnessing of the developer's test cases, using the developer's tools, at the premises of the developer.

The evaluator employs a sampling strategy to select developer tests to validate the developer's test results. The sampling strategy is focused especially on the proprietary test suites as the other test suites are commercial tools, widely accepted within the industry:

- Proprietary test suite covering Java Card and GlobalPlatform functionalities
- Proprietary test suite covering Module's interactions using simulators

In addition to this, the evaluator has defined additional test cases, prompted by study of the developer's documentation. Independent test suite developed by the EVIT and focused on the security requirements defined in the Java Card specification is performed.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR [10], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Feitian FT-JCOS v1.0 version 0.106.13 running on Infineon M7892 B11 meets the Common Criteria Part 3 *conformant* requirements *of* Evaluation Assurance Level EAL 5+ augmented with AVA_VAN.5 and ALC_DVS.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended by FPT_EMSEC.1 and FCS_RNG.1 functionality in the specified environment when running on the platforms specified in Annex A. It has also met the requirements of Protection Profile Java Card Protection Profile - Open Configuration Version 3.0.

6.2 Recommendations

Prospective consumers of FT-JCOS v1.0 version 0.106.13 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 4.3 "TOE Scope" and Section 5 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

The above "Evaluation Findings" include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Component	Name	Version	Package
Hardware	M7892	B11	module
Software	FT-JCOS v1.0	0.106.13	software on flash memory
Document	FT-JCOS v1.0/0.106.13 Administrator Manual	1.0.5	document
	FT-JCOS v1.0/0.106.13 User Manual	1.0.4	document

TOE Documentation

The supporting guidance documents evaluated were:

[a] FT-JCOS v1.0/0.106.13 Administrator Manual, Version 1.0.5, 4 March 2016 [11]

[b] FT-JCOS v1.0/0.106.13 User Manual, Version 1.0.4, 4 March 2016 [12]

TOE Configuration

The TOE configuration used for testing was the same used for developer tests:

TOE Reference	Expected Value	Version
Card OS version	00 6A 0D	0.106.13
Crypto library version	10 20 13	1.02.013
HW identifier	CC 78 33 AA 01 00 01 00 05 00 00 01 0B	M7892 B11
Firmware version	78 01 51 42	-

Annex B: TOE's security architecture

Architectural overview

The TOE is an open Java Card Platform (JCP) that is compliant with Java Card Specification v2.2.2 and GlobalPlatform Specification v.2.1.1. The TOE supports post-issuance functionalities for downloading Java Card compliant applets. Figure 1 shows the logical overview of the TOE:

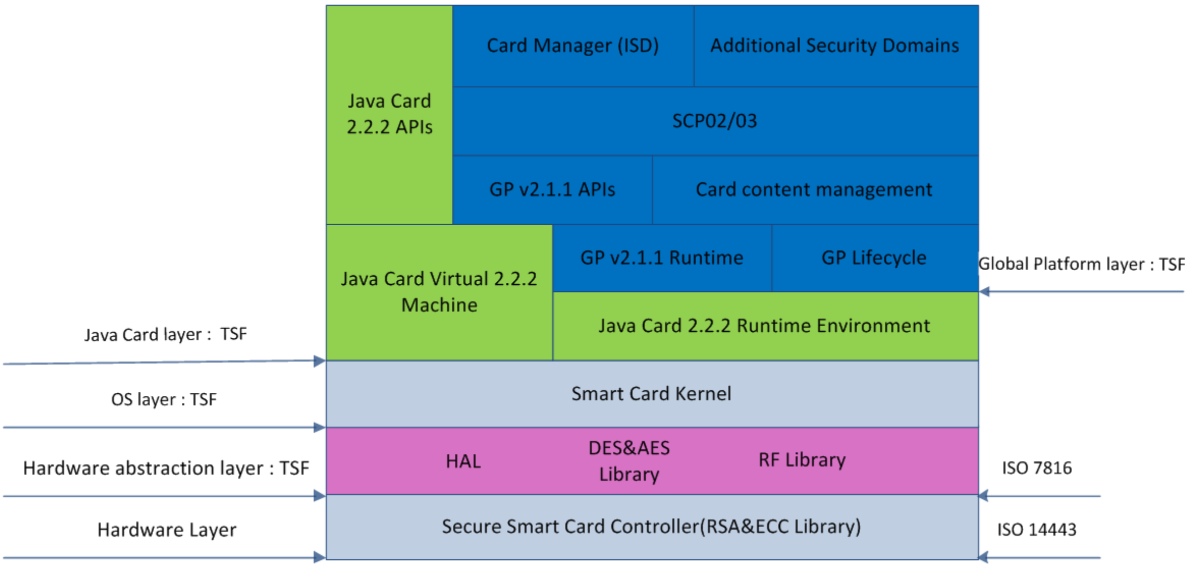

Figure 1 Logical scope of the TOE

All components of JCP are core components and are required for all possible configurations. "TSF" labelled items indicates the components that are part of the TOE Security Functionality. Extended descriptions of the components are presented below:

Layer	Description
Hardware	The Secure Smart Card Controller consists of a core system, co-processors, memories and peripherals. This layer is covered by the underlying platform certificate. ▪ Core system are the two CPUs (Central Processing Units), the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). ▪ Memories include Flash memory technology for persistent data storage and RAM memory for transient storage. ▪ The co-processor block contains the processors for RSA/EC and DES/AES processing ▪ The peripheral block contains the random number generation (True Random Number Generator) and the external interfaces service. ▪ Dual interface controller is able to communicate using either the contact based or the contactless interface.

Hardware Abstraction	Includes the firmware provided by the underlying platform and includes: - Communication protocol support for contact interface ISO 7816 (I/O Library)(TSF) - Communication protocol support for contactless interface ISO 14443 Type A and Type B (RF Library) (TSF) - Low-level cryptographic operations mostly using cryptographic hardware accelerators (Crypto Library). - Low-level basic memory operations and other system level operation (HAL).
OS	The Smart Card Kernel includes low level functionalities providing: - Memory management - Access to cryptography engine - Input/output routines.
Java Card	Includes the components of the Java Card Layer: - Java Card 2.2.2 APIs: The application programming interface for Java Card. - Java Card 2.2.2 Virtual Machine (TSF): The Java Card virtual machine is a subset of the Java virtual machine. - Java Card 2.2.2 Runtime Environment (TSF): A framework for running Java programs on the card.
GlobalPlatform	Includes the components of the GlobalPlatform specification: - Card Manager (TSF): The card manager is an application with specific rights to enable the secure downloading of applications. The card manager implements the GlobalPlatform Environment (OPEN), the Issuer Security Domain and Cardholder verification Method Services. The card manager allows life cycle management. - Additional Security Domains (TSF): Security Domains are privileged Applications. Security Domains are responsible for their own key management. The card supports multiple, dynamically configured Security Domains whose number is limited only by the available NVM. The card manager usually functions as a security domain called the Issuer Security Domain (ISD). The ISD is the leading security domain, although the card can contain additional security domains called Supplementary Security Domains (SSDs). - Secure Channels (SCP02) (TSF): A Secure channel is a communication mechanism between an off-card entity and a card that provides a level of assurance to one or both entities. The TOE supports Secure Channel Protocols. - GlobalPlatform API (GPv2.1.1 APIs) (TSF): The GlobalPlatform API provides services to applications. - Card Content Management (TSF): The card content management component is related to loading, installation, extradition, registry update and removal of card content functionalities. - GlobalPlatform Runtime Environment (GP v2.1.1 Runtime)(TSF): The runtime environment provides an API for applications as well as a secure storage and execution space for applications that ensures that each application's code and data can remain separate and secure from other applications on the card. The card's runtime environment is also responsible for providing communication services between the card and off-card entities. - GlobalPlatform Life Cycle (GP lifecycle) (TSF): The life cycle component is responsible for maintaining the overall security and administration of the card and its contents throughout its life cycle.

Non-TOE software requirements

The TOE is a stand-alone smart card product but identifies the Bytecode verifier as a required non-TOE software component. The TOE does not implement an on-card bytecode verifier and fully relies on the off-card bytecode verification that has to be performed before a file is loaded on the card.

The bytecode verifier is a program that performs static checks on the byte codes of a CAP file prior to the execution of the file on the card. Bytecode verification allows the detection of ill-formed CAP files that do not satisfy the properties of the virtual machine execution environment properties as specified in the Java Card specification.