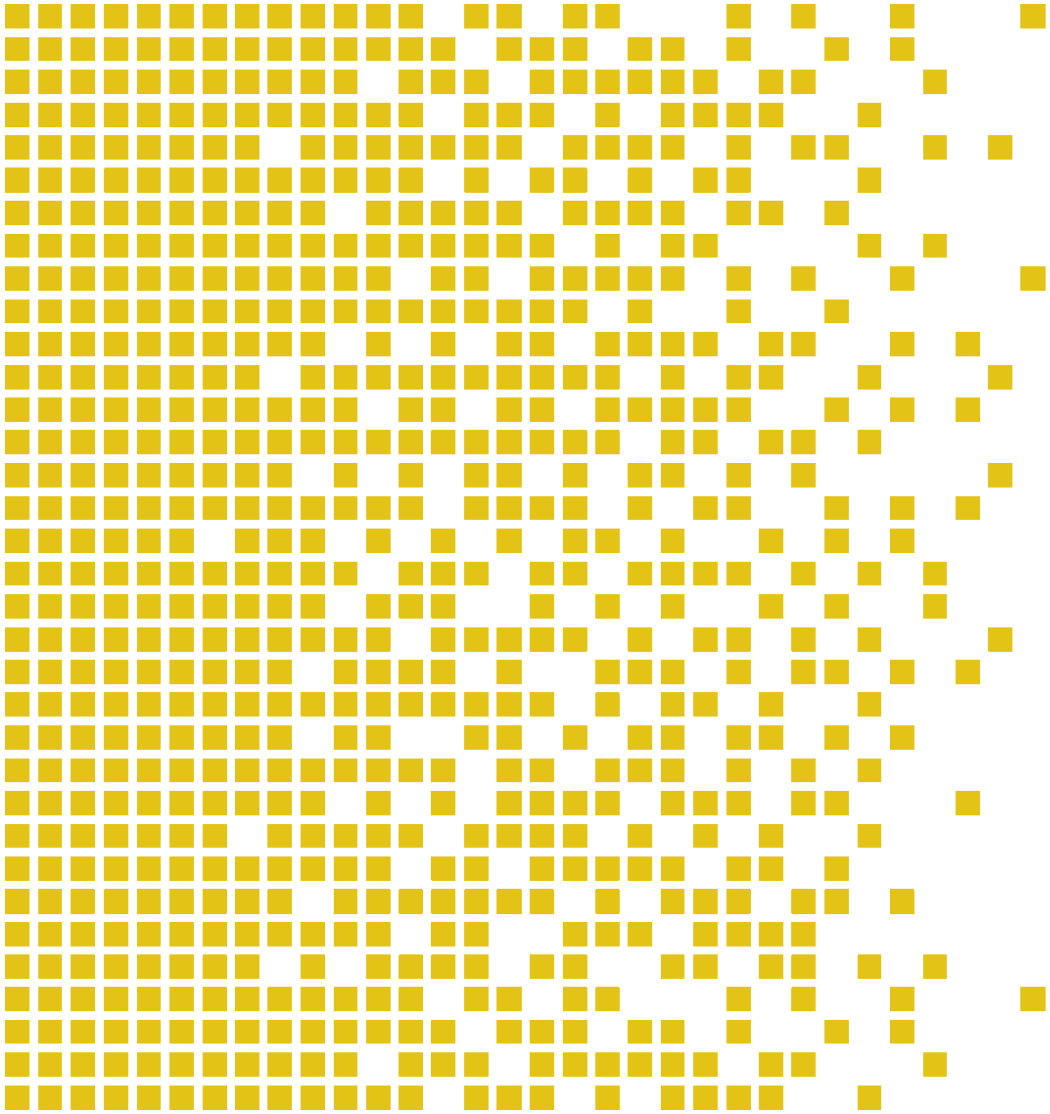
SERTIT-116 CR Certification Report

Issue 1.0 17 September 2018

Expiry date 17 September 2023

Feitian FT-JCOS v5.0/5.0.9 running on Infineon M7794 A12/G12



SERTIT, P.O. Box 814, N-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 (CCRA)

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 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 recognition under CCRA is limited to cPP related assurance packages or components up to EAL 2 with 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 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

Certification Statement

Feitian Technologies Limited FT-JCOS v5.0 is Java Card Open Platform that is compliant with Java Card Specification v3.0.4 and GlobalPlatform Specification v2.3 supporting post-issuance functionalities for downloading of single Java Card applets of the e-passport type or similar applications, such as eID and driving licence.

FT-JCOS v5.0 version v5.0.9 has been evaluated under the terms of the Norwegian Certification Authority for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant components of Evaluation Assurance Level EAL5+ 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.

Certification team	Kjartan Kvassnes, SERTIT Arne Høye Rage, SERTIT
Date approved	17 September 2018
Expiry date	17 September 2023

1 Abbreviations

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
cPP	collaborative Protection Profile
CPU	Central Processing Unit
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
GP	GlobalPlatform
HAL	Hardware Abstraction Layer
HW	Hardware
IC	Integrated Circuit
ISD	Issuer Security Domain
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
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
POC	Point of Contact
PP	Protection Profile

QP	Qualified Participant
RAM	Random-Access Memory
RSA	Rivest, Shamir, Adleman Public Key Encryption
SCP	Secure Channel Protocol
SERTIT	Norwegian Certification Authority for IT Security
SOGIS MRA	SOGIS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates
SPM	Security Policy Model
ST	Security Target
SW	Software
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

2 References

[1] SERTIT (2018), *The Norwegian Certification Scheme*, SD001E, Version 10.4, SERTIT, 20 February 2018.

[2] CCRA (2017), *Common Critera for Information Technology Security Evaluation, Part 1: Introduction and general model*, CCMB-2017-04-001, Version 3.1 R5, CCRA, April 2017.

[3] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*, CCMB-2017-04-002, Version 3.1 R5, CCRA, April 2017.

[4] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*, CCMB- 2017-04-003, Version 3.1 R5, CCRA, April 2017.

[5] CCRA (2017), *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, CCMB-2017-04-004, Version 3.1 R5, CCRA, April 2017.

[6] CCRA (2006), *ST sanitising for publication*, 2006-04-004, CCRA, April 2006.

[7] SOGIS Management Committee (2010), *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, Version 3.0, SOGIS MC, January 8th 2010.

[8] CCRA (2014), *Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security*, CCRA, July 2nd 2014.

[9] FT-JCOS v5.0 Security Target, v1.0.8, 2018-08-10.

[10] Evaluation Technical Report of FT-JCOS v5.0/5.0.9, 18-RPT-525 Version 1.1, 15th August 2018.

[11] FT-JCOS v5.0 User Manual, version 1.0.4, 2 August 2018.

[12] FT-JCOS v5.0 Administrator Manual, version 1.0.2, 10 August 2018.

[13] Composite product evaluation for Smartcards and similar devices, Supporting document, Version 1.5.1, May 2018.

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

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

[16] Java Card System - Open Configuration Protection Profile, Version 3.0.5. December 2017

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

[18] Machine Readable Travel Document with “ICAO Application”, Basic Access Control. March 2009.

[19] Machine Readable Travel Document with “ICAO Application”, Extended Access Control, Version 1.10. March 2009.

3 Executive Summary

3.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of FT-JCOS v5.0 version v5.0.9 to the Sponsor, Feitian Technologies Limited, 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 ST[9] which specifies the functional, environmental and assurance evaluation components.

3.2 Evaluated Product

The version of the product evaluated was FT-JCOS v5.0 and version v5.0.9.

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.3.0.4 and GlobalPlatform Specification v.2.3. The TOE allows post-issuance downloading of e-passport or similar applications such as eID and driving license that have been previously verified by an off-card trusted IT component.

It constitutes of a secure platform for only one application in the operational environment (excluding ISD).

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.

3.3 TOE scope

The TOE scope is described in the Security Target[9], chapter 2.

3.4 Protection Profile Conformance

The ST[9] did not claim conformance to any protection profile/cPP.

3.5 Assurance Level

The ST[9] specified the assurance components for the evaluation. The assurance incorporated predefined evaluation assurance level EAL5+, augmented by AVA_VAN5 and ALC_DVS.2 and extended by FPT_EMSEC.1 and FCS_RNG.1. Common Criteria Part 3[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].

3.6 Security Policy

The TOE security policies are detailed in Security Target[9], chapter 5.3.

3.7 Security Claims

The ST[9] fully specifies the TOE's security objectives, the threats which these objectives counter and security functional components 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 extracted from the Protection Profiles [17] and [18]/[19]: FCS_RNG.1 and FPT_EMSEC.1.

3.8 Threats Countered

All threats that are countered are described in the Security Target[9], chapter 5.2.

3.9 Threats Countered by the TOE's environment

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

3.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

3.11 Environmental Assumptions and Dependencies

The assumptions that apply to this TOE are described in the Security Target[9], chapter 5.4.

3.12 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 3.0.4 specification and Java Card 2.3 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.

3.13 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[1]. 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 both the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, CCRA[8], and the Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, SOGIS MRA[7] and the evaluation was conducted in accordance with the terms of these Arrangements.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its ST[9], which prospective consumers are advised to read. To ensure that the ST[9] 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 the Common Evaluation Methodology (CEM)[5]. Supporting documentation guidance is followed in accordance to Composite product evaluation for Smart Cards and similar devices [13]. Interpretations [14][15] are used as part of the vulnerability analysis.

SERTIT monitored the evaluation in accordance with SD001E[1] which was carried out by the Brightsight B.V. Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the final ETR[10] to SERTIT in 15 August 2018. SERTIT then produced this Certification Report.

3.14 General Points

The evaluation addressed the security functionality claimed in the ST[9] with reference to the assumed operating environment specified by the ST[9]. 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.

4 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 5 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

4.1 Introduction

The evaluation addressed the requirements specified in the ST[9]. 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.

4.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version 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 Administrator Manual document[12].

4.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance in the User Manual and Administrator Manual documents[11][12] provided by the developer.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

4.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user should always follow the guidance for the TOE in order to ensure that the TOE operates 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.

4.5 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:

- The code review of the CC evaluation was performed focusing on key security functionalities of the TOE as defined by the ST. Key functionalities are covering the SFRs claimed by the ST and Security Mechanisms claimed in ARC. The goal of the code review is to identify potential vulnerabilities that are later taken into account during the vulnerability analysis.
- The vulnerability analysis is then performed on the TOE using the code review results and the IC guidance documentation and ETR for Composition, resulting in a Penetration Test Plan. Other available information was also taken into consideration as input for the vulnerability analysis including the Attack Methods for Smart Cards and Similar Devices (controlled distribution).
- The penetration tests are performed according the 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.

4.6 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 3.0.4 specification compliance
- GlobalPlatform 2.3 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

4.7 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 Security Mechanisms using simulators
- 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 and GlobalPlatform specifications is performed.

5 Evaluation Outcome

5.1 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 FT-JCOS v5.0 version v5.0.9 meets the specified Common Criteria Part 3 conformant components of Evaluation Assurance Level EAL5+ augmented with AVA_VAN.5 and ALC_DVS.2 for the specified Common Criteria Part 2 extended by FPT_EMSEC.1 and FCS_RNG.1 functionality in the specified environment, when running on platforms specified in Annex A.

5.2 Recommendations

Prospective consumers of FT-JCOS v5.0 version v5.0.9 should understand the specific scope of the certification by reading this report in conjunction with the ST[9]. The TOE should be used in accordance with a number of environmental considerations as specified in the ST[9].

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Section 3.3 “TOE Scope” and Section 4 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance [11][12] 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	M7794	A12/G12	Module
Software	FT-JCOS v5.0	V5.0.9	Software on flash memory
Document	FT-JCOS v5.0 Administrator Manual	V1.0.2	Document
	FT-JCOS v5.0 User Manual	V1.0.4	Document

TOE Documentation

The supporting guidance documents evaluated were:

[a] FT-JCOS v5.0 User Manual, version 1.0.4, 2 August 2018 [11]

[b] FT-JCOS v5.0 Administrator Manual, version 1.0.2, 10 August 2018 [12]

TOE Configuration

The following configuration was used for testing:

TOE Reference	Expected Value	Version
Card OS version	05 00 09	5.0.9
Crypto library version	00 05 09	5.0.9
HW identifier	CC 77 33 EE 01 00 03 00 03 00 00 00 0C	M7794 A12
	CC 77 33 AE 02 00 03 00 03 00 00 06 0C	M7794 G12
Firmware version	77 01 71 22	-

Annex B: TOE security architecture

Architectural overview

The TOE is a Java Card Platform compliant with Java Card Specification v.3.0.4 and GlobalPlatform Specification v.2.3. The TOE allows post-issuance downloading of e-passport or similar applications such as eID and driving license that have been previously verified by an off-card trusted IT component. It constitutes of a secure platform for only one application in the operational environment (excluding ISD). Figure 1 shows the logical overview of the TOE:

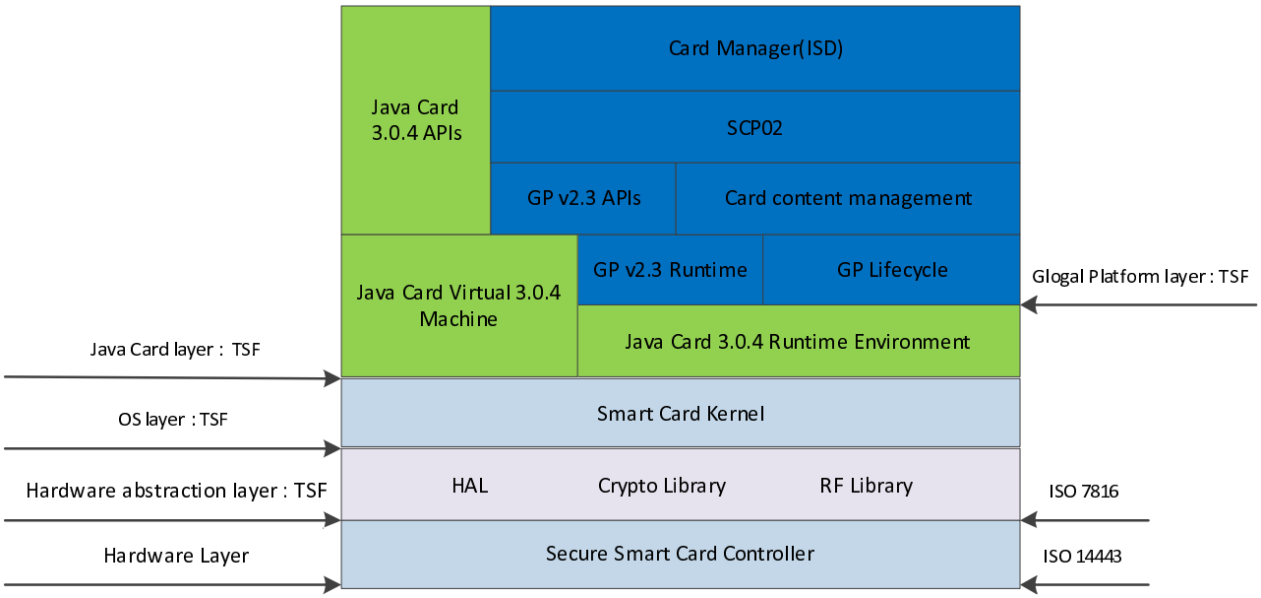


Figure 1 Logical scope of the TOE

All components of the JCP are core components. “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 CPU (Central Processing Unit), 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 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 is composed of: ▪ 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 from the underlying hardware (HAL).
OS	The Smart Card Kernel includes low level functionalities providing memory management, access to cryptography engine and input/output routines.
Java Card	Includes the components of the Java Card Layer: ▪ Java Card 3.0.4 APIs The application programming interface for Java Card. ▪ Java Card 3.0.4 Virtual Machine (TSF) The Java Card virtual machine is a subset of the Java virtual machine. ▪ Java Card 3.0.4 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, which defined in the GlobalPlatform specification 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 is in charge of the life cycle of the whole card, as well as the installed application (applet). It is the controller of the card, but relies on the TOE to manage the runtime of client applet. ▪ The card supports only one Security Domain. The card manager usually functions as a security domain called the Issuer Security Domain (ISD). The ISD is the sole security domain. ▪ 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 Protocol SCP02 as defined in the GlobalPlatform specification. ▪ GlobalPlatform API (GPv2.3 APIs)(TSF): the GlobalPlatform API provides services to applications. It also provides card content management services such as card locking and provides application life cycle state updates to applications. ▪ Card Content Management (TSF): the card content management component governs loading, installation of card content. ▪ GlobalPlatform Runtime Environment(GP v2.3 Runtime)(TSF): the runtime environment provides an API for application as well as a secure storage and execution space for application 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.

Certificate

The IT product identified in this certificate has been evaluated at the Norwegian evaluation facility described on this certificate using Common Methodology for IT Security Evaluation, according to the version number described on this certificate, for conformance to the Common Criteria for IT Security Evaluation according to the version number described on this certificate. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunctionwith the complete Certification report. The evaluation has been conducted in accordance with the provisions of The Norwegian Certification Authority for IT Security (SERTIT) and the conclusions of the evaluation technical report are consistent with the evidence adduced. Certification does not guarantee that the IT product is free from security vulnerabilities. This certificate only reflects 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 of this certificate. This certificate is not an endorsement of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

Certificate Identifier: SERTIT-116 C

Product Name: FT-JCOS V5.0

Version and Release Numbers: V5.0.9

Type of Product: Open Java Card Platform

Product Manufacturer: Feitian Technologies Limited

Assurance Type: EAL5 augmented with AVA_VAN.5 and ALC_DVS.2

Evaluation Criteria: Common Criteria Version 3.1 R5

Name of IT Security Evaluation Facility: Brightsight BV

Name of Validation Body and Certification Authority: SERTIT

Certification Report Identifier: SERTIT-116 CR, issue 1.0, 17 September 2018

Certificate Issued Date: 17 September 2018 Certificate Expiry Date: 17 September 2023

Kjartan Kvassnes
Certifier

Arne Høye Rage
Quality Assurance

Jørn Arnesen
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security

CC Recognition Arrangement for cPPs or components up to EAL 2 and ALC_FLR

SOGIS Recognition Agreement for components up to EAL 4