Certification Report

JPKI applet v1.0 on Combo CE 4.2.3 ST54J/K

Sponsor: ***The Government of Japan***
Digital Agency, Tokyo Garden Terrace Kioicho 19F
Kioicho 1-3, Chiyoda-ku
Tokyo 102-0094
Japan

Ministry of Internal Affairs and Communications,
Kasumigaseki 1-2-1, Chiyoda-ku
Tokyo 100-8926
Japan

Developer: ***FeliCa Networks, Inc.***
West Tower 16F, Gate City Osaki, 1-11-1
Osaki, Shinagawa-ku,
Tokyo 141-0032
Japan

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-2300012-01-CR**

Report version: **1**

Project number: **NSCIB-2300012-01**

Author(s): **Kjartan Jæger Kvassnes**

Date: **27 April 2023**

Number of pages: **11**

Number of appendices: **0**

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the JPKI applet v1.0 on Combo CE 4.2.3 ST54J/K. The developer of the JPKI applet v1.0 on Combo CE 4.2.3 ST54J/K is FeliCa Networks, Inc. located in Tokyo, Japan and The Government of Japan was the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a Java Card system that provides a secure signature creation device (SSCD) with key generation for creating an electronic signature and authenticating users. The TOE is embedded as a secure element (eSE) on the mobile phones.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 27 April 2023 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the JPKI applet v1.0 on Combo CE 4.2.3 ST54J/K, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the JPKI applet v1.0 on Combo CE 4.2.3 ST54J/K are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the JPKI applet v1.0 on Combo CE 4.2.3 ST54J/K from FeliCa Networks, Inc. located in Tokyo, Japan.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Thales Combo CE 4.2.3	1.1
		1.2
	JPKI applet	1.0
Hardware	ST54J / ST54K	Rev C & Rev D

To ensure secure usage a set of guidance documents is provided, together with the JPKI applet v1.0 on Combo CE 4.2.3 ST54J/K. For details, see section 2.5 “Documentation” of this report.

The ST54J / ST54K identified in *[HW-MAINT]* is the same version as the one mentioned in the IC certificate *[HW-CERT]* which was confirmed to be identical for the scope of the composite TOE.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.5.

2.2 Security Policy

The TOE is a Java Card configured to provide a contact and contactless integrated-circuit (IC) chip containing components to securely create, use and manage signature-creation data (SCD) with key generation. The TOE is embedded as a secure element on the mobile phone.

The TOE has the following features:

- generates SCD for digital signature and the correspondent SVD;
- generates SCD for user certification and the correspondent SVD;
- exports the SVDs for certification;
- is able to receive and store certificate info;
- is able to switch the TOE from a non-operational state to an operational state;
- creates digital signatures; and
- authenticates user for user certification.

2.3 Assumptions and Clarification of Scope

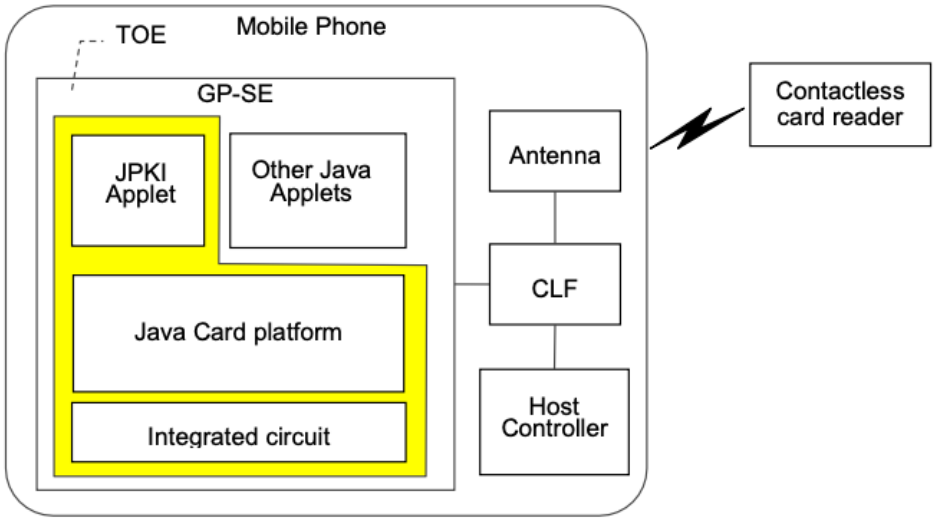
2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information



The TOE is a Java Card system that provides a secure signature creation device (SSCD) with key generation for creating an electronic signature and authenticating users. The TOE is embedded as a secure element (eSE) on the mobile phone.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
[AGD DA] FeliCa Networks, JPKI applet, Delivery and acceptance procedure	Version 1.0
[AGD IP] FeliCa Networks, JPKI applet, Installation procedure	Version 1.0
[AGD UG] FeliCa Networks, JPKI applet User guidance	Version 1.0

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem and module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values. The set of tests cases are defined based on the applet specifications. A decision table is devised based on a big list of conditions including command parameters, internal states and file system conditions. The test cases (scripts) are automatically created based on these decision tables. A total of 2788 test cases are executed.

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack oriented analysis the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this analysis will be performed according to the attack methods in [JIL-AP]. An important source for assurance in this step is the technical report [ETRfC] of the underlying platform.
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 21 days. During that test campaign, 16% of the total time was spent on Perturbation attacks, 33% on side-channel testing and 50% on logical attacks.

2.6.3 Test configuration

The TOE was tested in the following configurations:

- JPKI Applet v1.0 on Thales Combo CE 4.2.3 version 1.1 on ISO 7816:
  - PDM counter: D0 02 3F 15 24;
  - OSrelease:0112(1.12);
  - JPKI Applet identifier: 0402.
- JPKI Applet v1.0 on Thales Combo CE 4.2.3 version 1.2 on ISO 7816:
  - PDM counter: D0 02 3F 15 46;
  - OS release: 0110 (1.10);
  - JPKI Applet identifier: 0402.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 1 site certificate and 5 Site Technical Audit Reports.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number JPKI applet v1.0 on Combo CE 4.2.3 ST54J/K.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the JPKI applet v1.0 on Combo CE 4.2.3 ST54J/K, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profile *[EN419211-2]* and *[EN419211-4]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <none>, which are out of scope as there are no security claims relating to these.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 "high attack potential". To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The FeliCa Networks, Security Target for JPKI applet on Combo CE 4.2.3 ST54J/K, Version 1.2 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation
eSE	Embedded Secure Element
SSCD	Secure Signature Creation Device
SCD	Signature Creation Data
SVD	Signature Verification Data

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[EN419211-2]	EN 419 211-2:2013, Protection profiles for secure signature creation device - Part 2: Device with key generation, V2.0.1, registered under the reference BSI-CC-PP-0059-2009-MA-02
[EN419211-4]	EN 419 211-4:2013, Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application, registered under the reference BSI-CC-PP-0071-2012-MA-01
[ETR]	Evaluation Technical Report JPKI applet on JCOP 4.1 – EAL4+, 22-RPT-1448, Version 6.0, 25 April 2023
[HW-CERT]	ANSSI, Certificat ANSSI-CC-2019/20-S04, ST54J / ST54K A05, 01 March 2023
[HW-ETRfC]	Serma, Surveillance Technical Lite Report for ST54J/K, Version 1.0, 16 December 2022
[HW-ST]	STMicroelectronics, ST54J A01 Security Target for composition, Rev A01.3, issued in March 2019.
[HW-SUR]	ANSSI, Rapport de surveillance ANSSI-CC-2019/20-S04, ST54J / ST54K A05, 01 March 2023
[HW-MAINT]	ANSSI, Rapport de maintenance ANSSI-CC-2019/20-M03, ST54J / ST54K A05, 01 March 2023
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 22 August 2022
[PP_0084]	Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014
[ST]	FeliCa Networks, Security Target for JPKI applet on Combo CE 4.2.3 ST54J/K, Version 1.2

(This is the end of this report.)