0122

Common Criteria Certification Report

No. CRP298

Mobile FeliCa Applet on SkySIM CX Virgo platform

Version 2.0

Issue 1.0

December 2016

CESG Certification Body
Industry Enabling Services, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme ('the Scheme') and has met the specified Common Criteria (CC) requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this Certification Report.

Sponsor	FeliCa Networks Inc.	Developer	FeliCa Networks Inc.
Product Name, Version	Mobile FeliCa Applet on SkySIM CX Virgo platform Version 2.0		
Platform/Integrated Circuit	SkySIM CX Virgo v2.0		
Description	FeliCa Applet on SkySIM CX Virgo platform		
CC Version	Version 3.1 Release 4		
CC Part 2	Extended	CC Part 3	Conformant
PP(s) or (c)PP Conformance	None		
EAL	CC EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5		
CLEF	UL Transaction Security		
CC Certificate	P298	Date Certified	20 December 2016

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the Target of Evaluation (TOE) in meeting its Security Target [ST], which prospective consumers are advised to read. To ensure that the ST gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against that baseline. Both parts of the evaluation were performed in accordance with supporting documents [JIL], CC Parts 1, 2 and 3 [CC], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issuing of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

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

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] 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[1] contained in the certificate and in this Certification Report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

SENIOR OFFICIALS GROUP – INFORMATION SYSTEMS SECURITY (SOGIS) MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (MRA)

The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to the above Agreement [MRA] and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Agreement.

The judgments[1] contained in the certificate and this Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the logo does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

[1] All judgements contained in this Certification Report are covered by the CCRA [CCRA] recognition for components up to EAL 2 only, i.e. all other components, including the augmentations ALC_DVS.2 and AVA_VAN.5, are not covered by the CCRA. All judgements in this Certification Report are covered by the SOGIS MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of the above product at the stated version, to the Sponsor as summarised on Page 2 'Certification Statement' of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers of the above product at the stated version should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST]/[ST-Lite], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product completed evaluation to CC EAL4 assurance level augmented by ALC_DVS.2 and AVA_VAN.5 on 20 December 2016:

Mobile FeliCa Applet on SkySIM CX Virgo platform Version 2.0

4. The Developer of the TOE was FeliCa Networks Inc.

5. The Target of Evaluation (TOE) is an an embedded Secure Element (eSE) comprising an integrated circuit running the FeliCa Applet on a smart card operating system. The TOE manages several data sets, each having a different purpose, on a single instance of the TOE. The TOE has a file system consisting of Areas and FeliCa Services, which organise files in a tree structure. Further details are provided in Chapter IV 'TOE Architecture'.

6. The evaluated configuration of this product is described as the TOE. Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluation Configuration'.

7. An overview of the TOE and its product architecture can be found in Chapter IV 'TOE Architecture'. Configuration requirements are specified in Section 2 of the Security Target [ST]/[ST-Lite].

Security Target

8. The Security Target [ST]/[ST-Lite] fully specifies the TOE's Security Objectives, the Organisational Security Policies (OSPs) which these Objectives counter or meet and the Security Functional Requirements (SFRs) that refine the Objectives. Most of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products.

9. Additional SFRs are added into [ST]/[ST-Lite] to restrict the usage of debug and testing features; these additional SFRs are taken from [IC_PP].

10. The assurance requirements are taken from CC Part 3 [CC3].

11. The OSPs that must be met are specified in Section 3.3 of [ST]/[ST-Lite].

12. The environmental objectives and assumptions related to the operating environment are detailed in Chapter III (in 'Environmental Requirements').

Evaluation Conduct

13. The evaluation used the following documents as appropriate: the CCRA supporting documents, the SOGIS supporting documents defined in [JIL], international interpretations and relevant UK interpretations.

14. The source code of the application was reviewed at UL Transaction Security's (UL's) premises in Basingstoke (UK).

15. The Evaluator's independent security functional tests, and the repeat of a sample of the Developer's tests overseen by the Evaluator, were performed in Basingstoke (UK).

16. Penetration testing of the TOE was performed entirely at UL Transaction Security's premises in Basingstoke, UK, using final samples of the TOE. The test approach used advanced techniques, incorporating the latest attack methods including those described in [JIL_AM].

17. Part of the evaluation process is to examine the security of the development environment to confirm whether or not the implemented security measures are sufficient to protect the confidentiality and integrity of the TOE. A site audit was therefore performed at the Developer's facilities located at West Tower 10F Gate City Osaki 1-11-1 Osaki Shinagwa-ku, Tokyo, 141-0032 Japan. The site was evaluated using the Common Criteria site visit guidance in [CEM] and the Minimum Site Security Requirements specified in [MSSR].

18. The CESG Certification Body monitored the evaluation, which was performed by the UL Transaction Security Commercial Evaluation Facility (CLEF), and witnessed a sample of Evaluator tests. The evaluation addressed the requirements specified in the Security Target [ST]/[ST-Lite]. The results of this work, completed in December 2016, were reported in the Evaluation Technical Report [ETR].

Evaluated Configuration

19. The TOE should be used in accordance with the environmental assumptions specified in the Security Target [ST]/[ST-Lite]. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

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

Conclusions

21. The conclusions of the CESG Certification Body are summarised in the 'Certification Statement' on page 2.

Recommendations

22. Chapter II 'TOE Security Guidance' includes a number of recommendations regarding the secure delivery, receipt, installation, configuration and operation of the TOE.

23. The TOE relies on the certified underlying platform Operating System and IC Chip for authentication, cryptographic libraries and security mechanisms. System integrators and risk owners should make sure they have confidence in the mechanisms of the platform, in particular paying attention to any patches or updates.

24. Any further recommendations are included in the TOE Security Guidance in Chapter II, Paragraph 38.

Disclaimers

25. This Certification Report and associated Certificate applies only to the specific version of the product in its evaluated configuration (i.e., the TOE). This is specified in Chapter III 'Evaluation Configuration'. The ETR on which this Certification Report is based relates only to the specific items tested.

26. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability that exploitable vulnerabilities may be discovered after the Evaluators' penetration tests were completed. This report reflects the CESG Certification Body's view on that date (see Chapter V, Paragraph 65).

27. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the date of the penetration tests (as detailed in Chapter V) and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

28. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE but should only be applied in accordance with a consumer's risk management approach. Unevaluated patches are not covered by this certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a certificate-authorising Scheme under relevant mutual recognition agreements.

29. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

30. Note that the opinions and interpretations stated in this report under 'Recommendations' and 'TOE Security Guidance' are based on the experience of the CESG Certification Body in performing similar work.

II. TOE SECURITY GUIDANCE

Introduction

31. The following sections provide guidance that is of particular relevance to consumers of the TOE.

Delivery and Installation

32. On receipt of the TOE, the consumer should check that the evaluated version has been supplied, and that the security of the TOE has not been compromised during delivery. Specific advice on delivery and installation is provided in the TOE documents detailed below:

- Section 2.2 of [AG_PRE];
- Section 2.2 of [ST]/[ST-Lite].

Guidance Documents

33. Specific configuration advice is included in the smart card guidance documents listed in this section.

34. The User Guide and Administration Guide documentation is in the smart card guidance listed below.

35. The guidance documentation for the Pre-personalization phase is as follows:

- [AG_PRE] Product Acceptance Procedure for Mobile FeliCa Applet on SkySIM CX Virgo platform.
- [AG_IDI] Individual Data for Issuer.

36. The guidance documentation for the Personalization phase is as follows:

- [UG_PERSO] Mobile FeliCa Applet Personalisation Specification.
- [UG_AUM] Mobile FeliCa Applet User's Manual;
- [UG_UM] FeliCa Card User's Manual;

37. The guidance documentation for the Operational phase is as follows:

- [UG_AUM] Mobile FeliCa Applet User's Manual;
- [UG_UM] FeliCa Card User's Manual;
- [UG_SRM-E1] Security Reference Manual – Group Key Generation (AES 128bit);

- [UG_SRM-E2] Security Reference Manual – Mutual Authentication & Secure Communication (AES 128bit);
- [UG_SRM-E3] Security Reference Manual – Package Generation (AES 128bit);
- [UG_SRM-E4] Security Reference Manual - Changing Key Package Generation (AES 128bit).

Recommendations

38. To maintain secure operation, the consumer is recommended to follow the smart card guidance detailed in the [AG] and [UG] documentation listed above.

III. EVALUATED CONFIGURATION

TOE Identification

39. The TOE is the Mobile FeliCa Applet on SkySIM CX Virgo platform Version 2.0, which consists of a FeliCa Java Card Applet in composition with the certified underlying platform SkySIM CX Virgo v2.0.

TOE Documentation

40. The relevant guidance documents for the evaluated configuration are identified in Chapter II (in 'Guidance Documents').

TOE Scope

41. The TOE Scope is defined in the Security Target Section 2. Functionality that is outside the TOE Scope is defined in Section 2.1. The TOE boundaries are shown in Figure 1 below.

TOE Configuration

42. The evaluated configuration of the TOE is defined in the Security Target Section 2.2 and specific configuration advice is provided in the guidance [UG].

43. The evaluated TOE configuration is composed of:

- FeliCa Mobile Applet, version 615100;
- SkySIM CX Virgo v2.0 Java Card Open Platform;
- BCM_SPS02 C0, Firmware/Bootloader v002.020.

Environmental Requirements

44. The environmental objectives for the TOE are stated in Section 4.2 of [ST]/[ST-Lite].

45. The environmental assumptions for the TOE are stated in Section 3.2 of [ST]/[ST-Lite].

Test Configurations

46. The Developers and Evaluators used successive development versions of the SkySIM CX Virgo v2.0 Java Card Open Platform code during evaluation. However, the Evaluator's independent results derived from vulnerability analysis, profiling analysis and comparison tests demonstrated that the test configurations were all consistent with the following configuration:

- The TOE configuration as defined in Paragraph 42 above.

IV. TOE ARCHITECTURE

Introduction

47. This Chapter gives an overview of the product and the TOE's main architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration'.

TOE Description and Architecture

48. The TOE is an integrated circuit running the FeliCa Applet on a smart card operating system. The latter Security IC Embedded Software is SkySIM CX Virgo and the integrated circuit is BCM_SPS02, as described in Section 1.3 of [ST]/[ST-Lite].

49. The following figure illustrates the physical scope of the TOE, which is indicated in yellow, and the product, which is indicated in blue:

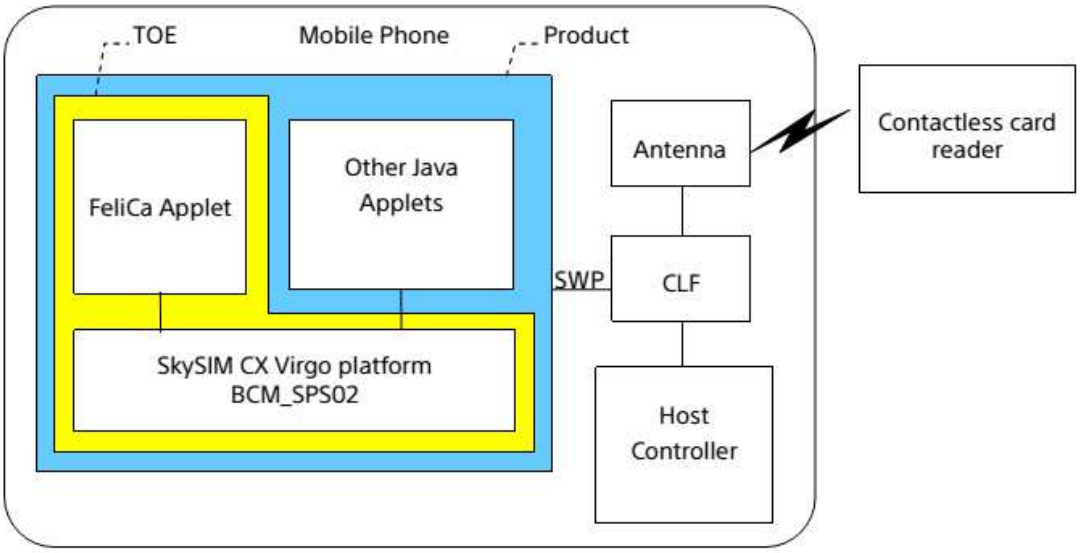

Figure 1 TOE physical scope

50. The TOE is comprised of the following:

- "FeliCa Applet" constitutes the part of the TOE that is responsible for managing and providing access to the Areas and FeliCa Services.

- SkySIM CX Virgo has a Java Card System which manages and executes applets. It provides APIs for developing applets in accordance with the Java Card specification [JCAPI304]. SkySIM CX Virgo has GlobalPlatform (GP) packages providing a common interface to communicate with a smart

card and manage applications in a secure way according to the GP specifications [GP221].

- "BCM_SPS02" is the hardware platform of the TOE. The hardware platform provides the following security functionality, DES, AES, RNG and CRC, although DES is out of scope of the evaluation. The hardware platform also includes security detectors, sensors and circuitry to protect the TOE.

51. The SWP interface enables the exchange of FeliCa commands, which are processed by the FeliCa Applet. The CLF chip, the Host controller and the antenna are out of scope of the TOE. The CLF chip provides contact and contactless communication among the TOE, the contactless card reader and the host controller.

52. The TOE offers the following features:

- it can receive FeliCa commands from the CLF.
- it enables the set-up and maintenance of FeliCa Services by Service Providers.
- it enables the use of FeliCa Services (e.g., decrement, cash-back).

53. The TOE offers the following security features:

- Authentication of users (AES).
- Controlled access to data stored internally in the TOE.
- Secure communication with the smartcard Reader/Writer (AES).
- Protection of integrity of data stored internally in the TOE.
- Anti-tearing and rollback.
- Protection against excess environment conditions.
- Protection against information leakage and manipulation.
- Protection against probing and alteration.

54. The security features are provided partly by the underlying hardware and partly by the Security IC Embedded Software and FeliCa Applet.

TOE Design Subsystems

55. The high-level TOE subsystems, and their security features/functionality, are:

- OS & HW: this subsystem consists of the Java Card System, OS and security IC implemented in the SkySIM CX Virgo platform that provides numerous countermeasures against attacks ([CR]). These include, for example, masking operations on keys and sensitive data to provide confidentiality of data used by the TOE. The subsystem provides card content management in line with the GlobalPlatform specification.

- Applet_Interface: this subsystem handles FeliCa commands and responses between OS & HW and Command_Execution. It also sends HCI Events to the host controller in the host device via the OS & HW subsystem.

- Command_Execution: this subsystem provides the command execution functionality, provides access control and authentication, handles the TOE data and uses FeliCa Crypto Lib to encrypt/decrypt data.

- FeliCa Crypto Lib: this subsystem decrypts or encrypts data in accordance with the FeliCa security algorithm.

TOE Dependencies

56. The TOE has no dependencies.

TOE Security Functionality Interface

57. The external TOE Security Functionality Interface (TSFI) is:

- SWP interface.

- APDU commands.

- HCI Interface.

V. TOE TESTING

Developer Testing

58. The Developer's security tests covered:

- all SFRs;
- all TOE high-level subsystems, as identified in Chapter IV (in 'TOE Design Subsystems');
- all TOE Security Functionality;
- the TSFI, as identified in Chapter IV (in 'TOE Security Functionality Interface').

59. The Developer's security tests also included those TOE interfaces which are internal to the product and thus had to be exercised indirectly. The Evaluators witnessed the Developer repeating a sample of Developer security tests.

60. The Developer security tests were run on the configuration defined in Chapter III 'Test Configurations'.

Evaluator Testing

61. The Evaluators devised and ran a total of 6 independent security functional tests, different from those performed by the Developer. No anomalies were found.

62. The Evaluators also devised and ran a total of 2 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

63. The Evaluators devised comparison tests based on profiling analysis to demonstrate that differences in two successive development versions of the SkySIM CX Virgo platform used during the evaluation produced test results consistent with the TOE Configuration detailed in Paragraph 43 above.

64. The Evaluators ran their tests on the configuration defined in Chapter III 'Test Configurations'.

65. The Evaluators completed their period of penetration tests on 17 June 2016.

Vulnerability Analysis

66. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables. The analysis of the evaluation deliverables followed the SOGIS guidance provided in the [JIL] documentation.

Platform Issues

67. The platform relevant to the TOE is detailed in Chapter III and no issues were identified.

VI. REFERENCES

[AG]	Administration Guide: [AG_PRE] Product Acceptance Procedure for Mobile FeliCa Applet on SkySIM CX Virgo platform, FeliCa Networks Inc., Issue 1.10, November 2016. [AG_IDI] Individual Data for Issuer, FeliCa Networks Inc., Issue 1.20, June 2016.
[CC]	Common Criteria for Information Technology Security Evaluation (comprising Parts 1, 2, 3: [CC1], [CC2] and [CC3]).
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1, Introduction and General Model, Common Criteria Maintenance Board, CCMB-2012-09-001, Version 3.1 R4, September 2012.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2, Security Functional Components, Common Criteria Maintenance Board, CCMB-2012-09-002, Version 3.1 R4, September 2012.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3, Security Assurance Components, Common Criteria Maintenance Board, CCMB-2012-09-003, Version 3.1 R4, September 2012.
[CCRA]	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, Participants in the Arrangement Group, 2nd July 2014.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, CCMB-2012-09-004, Version 3.1 R4, September 2012.
[CR]	Common Criteria Certification Report No. CRP292, SkySIM CX Virgo Version 2.0, UK IT Security Evaluation and Certification Scheme, CRP292, Issue 1.0, November 2016.

[ETR]	Evaluation Technical Report, UL Transaction Security, UL/SEC/ETR/10952715, Issue 1.11, 20 December 2016.
[GP221]	GlobalPlatform Card Specification, GlobalPlatform Inc, Version 2.2.1, January 2011.
[JCAPI304]	Java Card API, Classic Edition, Oracle, Version 3.0.4, September 2011.
[IC_PP]	Security IC Platform Protection Profile with Augmentation Packages, Inside, Secure Infineon Technologies AG, NXP Semiconductors Germany GmbH and STMicroelectronics, Version 1.0, January 2014.
[JIL]	Joint Interpretation Library, (comprising [JIL_AM], [JIL_AP], [JIL_ARC], [JIL_COMP] and [MSSR]).
[JIL_AM]	Attack Methods for Smartcards and Similar Devices, Joint Interpretation Library, Version 2.2, January 2013.
[JIL_AP]	Application of Attack Potential to Smartcards, Joint Interpretation Library, Version 2.9, January 2013.
[JIL_ARC]	Security Architecture requirements (ADV_ARC) for smart cards and similar devices, Joint Interpretation Library, Version 2.0, January 2012.
[JIL_COMP]	Composite product evaluation for Smart Cards and similar devices, Joint Interpretation Library, Version 1.4, August 2015.
[MRA]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Management Committee, Senior Officials Group – Information Systems Security (SOGIS), Version 3.0, 8 January 2010.
[MSSR]	Minimum Site Security Requirements, Joint Interpretation Library, Version 1.1 (for trial use), July 2013.

[ST]	Security Target for Mobile FeliCa Applet on SkySIM CX Virgo platform, FeliCa Networks Inc., MAP01-ASE01-E01-31, Issue 1.31, November 2016.
[ST-Lite]	Security Target Lite for Mobile FeliCa Applet on SkySIM CX Virgo platform, FeliCa Networks Inc., MAP01-ASEP01-E01-31, Issue 1.31, November 2016.
[UG]	[UG_PERSO] Mobile FeliCa Applet Personalisation Specification, FeliCa Networks Inc., Issue 1.20, January 2016. [UG_AUM] Mobile FeliCa Applet User's Manual, FeliCa Networks Inc., Issue 1.40, April 2016. [UG_UM] FeliCa Card User's Manual FeliCa Networks Inc., Issue 1.02. [UG_SRM-E1] Security Reference Manual – Group Key Generation (AES 128bit), FeliCa Networks Inc., Issue 1.21. [UG_SRM-E2] Security Reference Manual – Mutual Authentication & Secure Communication (AES 128bit), FeliCa Networks Inc., Issue 1.21. [UG_SRM-E3] Security Reference Manual – Package Generation (AES 128bit), FeliCa Networks Inc., Issue 1.21. [UG_SRM-E4] Security Reference Manual - Changing Key Package Generation (AES 128bit), FeliCa Networks Inc., Issue 1.21.
[UKSP00]	UK Scheme Publication No. 00, Abbreviations and References, UK IT Security Evaluation and Certification Scheme, UKSP 00, Issue 1.8, August 2013.
[UKSP01]	UK Scheme Publication No. 01, Description of the Scheme, UK IT Security Evaluation and Certification Scheme, UKSP 01, Issue 6.6, August 2014.

[UKSP02]	UK Scheme Publication No. 02, CLEF Requirements (comprising Parts I and II: [UKSP02P1] and [UKSP02P2]).
[UKSP02P1]	CLEF Requirements - Startup and Operations, UK IT Security Evaluation and Certification Scheme, UKSP 02: Part I, Issue 4.5, August 2013.
[UKSP02P2]	CLEF Requirements - Conduct of an Evaluation, UK IT Security Evaluation and Certification Scheme, UKSP 02: Part II, Issue 3.1, August 2013.

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. Standard CC abbreviations are detailed in CC Part 1 [CC1] and UK Scheme abbreviations and acronyms are detailed in [UKSP00].

AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
CLEF	Commercial Evaluation Facility
CLF	Contactless Frontend
DES	Data Encryption Standard
GP	GlobalPlatform
HCI	Host Card Interface
HW	Hardware
IC	Integrated Circuit
JCAPI	Java Card Application Programming Interface
JIL	Joint Interpretation Library
OS	Operating System
RNG	Random Number Generator
SWP	Single Wire Protocol
UL	Underwriters Laboratories Inc.

VIII. CERTIFICATE

The final two pages of this document contain the Certificate (front and back) for the TOE.

CESG Certified Product

Common Criteria

P298

This is to certify that

FeliCa Networks Inc

Mobile FeliCa Applet on SkySIM CX Virgo platform

Version 2.0

has been evaluated under the terms of the

Common Criteria Scheme

and complies with the requirements for

EAL4 augmented by ALC_DVS.2 and AVA_VAN.5

COMMON CRITERIA (ISO 15408) ASSURANCE LEVEL

Common Criteria

UKAS PRODUCT CERTIFICATION

SOGIS IT SECURITY CERTIFIED

AUTHORISED BY
DIRECTOR GENERAL
FOR GOVERNMENT
AND INDUSTRY CYBER SECURITY

THIS PRODUCT WAS EVALUATED BY
UL Transaction Security

DATE AWARDED
20 December 2016

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is accredited by the United Kingdom Accreditation Service (UKAS) to ISO/IEC17065:2012 to provide product conformity certification as follows:
Category: Type Testing Product Certification of IT Products and Systems.
Standards: Common Criteria for Information Technology Security Evaluation (CC) EAL1 – EAL7.
Details are provided on the UKAS Website (www.ukas.org).

Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA)

The IT Product identified in this certificate has been evaluated at an accredited and approved Evaluation Facility of the United Kingdom using the Common Methodology for IT Security Evaluation, version 3.1 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation, version 3.1. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report. The Evaluation has been conducted in accordance with the provisions of the UK IT Security Evaluation and Certification Scheme and the conclusions of the Evaluation Facility in the Evaluation Technical Report are consistent with the evidence adduced. This certificate is not an endorsement of the IT Product by CESG or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by CESG or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

All judgements contained in this certificate, and in the associated Certification Report, are covered by CCRA recognition for components up to EAL 2 only, i.e. all other components, including the augmentations ALC_DVS.2 and AVA_VAN.5, are not covered by the Arrangement.

Senior Officials Group – Information Systems Security (SOGIS) Mutual Recognition Agreement of Information Technology Security Evaluation Certificates (SOGIS MRA), Version 3.0

The CESG Certification Body is a Participant to the above Agreement. The current Participants to the above Agreement are detailed on the SOGIS Portal (www.sogisportal.eu). The mark (left) confirms that this conformant certificate has been authorised by a Participant to the above Agreement and it is the Participant's statement that this certificate has been issued in accordance with the terms of the above Agreement. The judgements contained in this certificate and in the associated Certification Report are those of the compliant Certification Body which issues them and of the Evaluation Facility which performed the evaluation. Use of the mark does not imply acceptance by other Participants of liability in respect of those judgements or for loss sustained as a result of reliance upon those judgements by a third party.
All judgements contained in this certificate, and in the associated Certification Report, are covered by the agreement.

In conformance with the requirements of ***ISO/IEC17065:2012***, the CCRA and the SOGIS MRA, the CESG Certification Body's website (www.ncsc.gov.uk) provides a reference to the CC Portal (www.commoncriteriaportal.org) for the IT products certified under the UK Scheme. The CC Portal provides additional information as follows:

- Type of product (i.e. product category); and
- Details of product manufacturer (i.e. as appropriate: vendor/developer name, postal address, website, point of contact, telephone number, fax number, email address).