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

SERTIT-082 CR Certification Report

Issue 1.0 5th September 16

Mobile FeliCa OS 3.0 on S3CS9AB/0114_5329

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

FeliCa Networks, Inc Mobile FeliCa OS 3.0 on S3CS9AB is an integrated circuit with Security IC Embedded Software. The Security IC Embedded Software is the FeliCa OS and the integrated circuit is the Samsung chip S3CS9AB.

FeliCa Networks Mobile FeliCa OS 3.0 on S3CS9AB version 0114_5329 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 4+ augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.4 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended by FAU_SAS.1, and FCS_RNG.1 functionality.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Arne Høye Rage Quality Assurance Arne H. Rage
Approved	Kristian Steinfeld Bae Head of SERTIT
Date approved	5th September 2016

2 Abbreviations

ACL	Access Control List
AES	Advanced Encryption Standard
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
CLF	Contactless Front End
CPU	Central Processing Unit
CR	Certification Report
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ESE-IF	Embedded Secure Element Interface
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
HW	Hardware
IC	Integrated Circuit
IT	Information Technology
OS	Operating System
PP	Protection Profile
RAM	Random-Access Memory
SERTIT	Norwegian Certification Authority for IT Security
SFR	Security Functional Requirements
ST	Security Target
SW	Software
TOE	Target of Evaluation
TSF	TOE Security Functions

3 References

[1] F03S-ASE01-E01-70 Security Target for Mobile FeliCa OS 3.0 on S3CS9AB, 1.70, August 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] JIL Attack Methods for Smartcards and Similar Devices, Version 2.2, January 2013

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

[9] Evaluation Technical Report of Mobile FeliCa OS 3.0 on S3CS9AB, 16-RPT-325 Version 1.0, 11 August 2016.

[10] Mobile FeliCa OS Version 3.0 User Manual, 1.00, March 2014

[11] Mobile FeliCa OS Version 3.0 User's Manual - Cautions for Operational Usage -, 1.10, February 16, 2016

[12] Product Acceptance Procedure, 1.2, January 11, 2016

[13] BSI-PP-0035 Security IC Platform Protection Profile , Version 1.0, June 2007

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Mobile FeliCa OS 3.0 on S3CS9AB version 0114_5329 to the Sponsor, FeliCa Networks, Inc, 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 Mobile FeliCa OS 3.0 on S3CS9AB and version 0114_5329.

This product is also described in this report as the Target of Evaluation (TOE). The developer was FeliCa Networks, Inc.

The TOE is an integrated circuit with an embedded smartcard operating system. The operating system is the FeliCa Networks Mobile FeliCa Operating System (referred to in this document as FeliCa OS) and the integrated circuit is the Samsung Electronics Co., Ltd (referred to in this document as Samsung) chip S3CS9AB.

The TOE manages several data sets, each having a different purpose, on a single TOE. The TOE has a file system consisting of Areas and FeliCa Services, which organise files in a tree structure. Multiple Service Providers can use an Area or a FeliCa Service. Access keys enable access to data, via the Areas and FeliCa Services. This prevents unauthorised access to the User Services of other Service Providers. By organising these keys in a specific manner, multiple Area and FeliCa Services can be authenticated simultaneously.

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 does not claim conformance to any Protection Profile, but it is written to be fully consistent with the BSI-PP-0035 Security IC Platform Protection Profile [13].

4.5 Assurance Level

The Security Target [1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 4, augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.4 and extended by FAU_SAS.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 3.4.

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 Profile [13]: FAU_SAS.1 and FCS_RNG1.

4.8 Threats Countered

All threats that are countered are described in the Security Target [1], chapter 3.2.

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 3.4.

4.12 IT Security Objectives

The security objectives that apply to this TOE are described in the Security Target [1], chapter 4.1.

4.13 Non-IT Security Objectives

The security objectives for the environment are described in the Security Target [1], chapter 4.2.

4.14 Security Functional Requirements

The security functional requirements are described in the Security Target [1], chapter 5.1.

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

Security Functional Requirements	
FMT_SMR.1	Security roles
FIA_UID.1	Timing of identification
FIA_UAU.1	Timing of authentication
FIA_UAU.4	Single-use authentication mechanisms
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FMT_MSA.1	Management of security attributes
FMT_SMF.1	Specification of Management Functions
FDP_SDI.2	Stored data integrity monitoring and action
FTP_ITC.1	Inter-TSF trusted channel
FRU_FLT.2	Limited fault tolerance
FPT_FLS.1	Failure with preservation of secure state
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FAU_SAS.1	Audit storage
FPT_PHP.3	Resistance to physical attack
FDP_ITT.1	Basic internal transfer protection
FDP_IFC.1	Subset information flow control
FPT_ITT.1	Basic internal TSF data transfer protection
FCS_RNG.1	Random number generation

4.15 Security Function Policy

User data in Files shall not be accessible for user operations except when the Service Access Policy is satisfied.

The Service Access Policy will enforce that only Subjects, namely a User or the Administrator, with the proper security attributes can access Files with security attributes ACL.

Operations on files include authentication, read, write and reset mode operations. A Subject can only perform read, write and reset mode operations on files when the Subject is successfully authenticated, and the operation is listed in the File's ACL.

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]. Interpretations [7][8] are used as part of the vulnerability analysis.

SERTIT monitored the evaluation which was carried out by Brightsight B.V. as Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[9] to SERTIT on 11th August 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 EAL4 assurance package augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.4.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
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.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined life-cycle model
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
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: security Enforcing Modules
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.4	Methodical vulnerability analysis

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 [9] 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 [10][11].

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 [10][11] 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:

- The code review was performed focusing on key security functionalities of the TOE (key functionalities are covering the SFRs claimed by the ST and Security Mechanisms claimed in ARC and chip manufacturer guidance compliance. The goal of the code review is to identify potential vulnerabilities that are later taken into account during the vulnerability analysis. As part of the code review the proper implementation of the IC guidance for secure programming recommendations has been verified.

- The vulnerability analysis is then performed using the findings of the code review and the hardware ETR for composition, resulting in a test plan. Other available information was also taken into consideration as input for the vulnerability analysis including Attack Methods for Smartcards and Similar Devices (controlled distribution) and internal knowledge on former FeliCa specification related products.
- The penetration tests are performed according to the penetration test plan.
- The evaluator performs a continuous follow-up on advances on attack methods as well as for new attack methods that are published during the time of the evaluation. When a new attack method is identified to impact the TOE, an impact assessment is performed.

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 emulators.

Defined tests are identified in a set of 5 different test suites using an automated test tool:

- Test suite for commands defined in FSP
- Test suite for additional testing in commands defined in FSP using emulators
- Test suite for identification of potential vulnerabilities (such as using invalid commands)
- Test suite for terminating the TOE using emulators
- Test suite for the transaction mechanism

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 the choice was made to perform the evaluator independent testing by repetition of a portion of the developer's test cases, using the developer's tools, at the premises of the EVIT.

The evaluator employs a sampling strategy to select developer tests to validate the developer's test results. The developer was required to prepare test environment to sample the following.

- The sampling strategy was focused on authentication commands, to verify the correct behaviour of the access control mechanism and write commands, for further assurance of the access control policies.

In addition to this, the evaluator has defined additional test cases, prompted by study of the developer documentation. The test strategy is as shown below.

- The authentication commands in which combinations of services are authenticated
- The read and write commands in which authentication is verified

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR [9], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that FeliCa Networks Mobile FeliCa OS 3.0 on S3CS9AB version 0114_5329 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4+ augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.4 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended by FAU_SAS.1 and FCS_RNG.1 functionality in the specified environment described in the Security Target [1].

6.2 Recommendations

Prospective consumers of Mobile FeliCa OS 3.0 on S3CS9AB version 0114_5329 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.

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

These guidance documents include a number of recommendations relating to the secure receipt, installation, service configuration and operation of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Component	Name	Version	Package
Hardware	S3CS9AB 32-Bit RISC Microcontroller for Smart Card	0	Wafer or Module
Software	Mobile FeliCa OS Version 3.0	0114_5329	Embedded in hardware
Document	Mobile FeliCa OS Version 3.0 User Manual	1.00	document
	Mobile FeliCa OS Version 3.0 User Manual - Cautions for Operational Usage -	1.10	document
	Product Acceptance Procedure	1.2	document
	3rd Generation Mobile FeliCa IC Chip System SAM Chip Pre-Issuance Requirements Specification	1.04	document
	SAM Chip Pre-Issuance Requirements Specification Samsung-Specific Requirements	0.93	document
	Security Reference Manual – Group Key Generation (AES 128bit)	1.21	document
	Security Reference Manual – Mutual Authentication & Secure Communication (AES 128bit)	1.21	document
	Security Reference Manual – Package Generation (AES 128bit)	1.21	document
	Security Reference Manual – Changing Key Package Generation (AES 128bit)	1.21	document

TOE Documentation

The supporting guidance documents evaluated were:

[a] Mobile FeliCa OS Version 3.0 User Manual, 1.00, March 2014

[b] Mobile FeliCa OS Version 3.0 User Manual - Cautions for Operational Usage – , version 1.10, February 16, 2016

[c] Product Acceptance Procedure, version 1.2, January 11, 2016

[d] 3rd Generation Mobile FeliCa IC Chip System SAM Chip Pre-Issuance Requirements Specification, 1.04

[e] SAM Chip Pre-Issuance Requirements Specification Samsung-Specific Requirements, version 0.93

[f] Security Reference Manual - Group Key Generation (AES128bit), 1.21, February 2011

[g] Security Reference Manual - Mutual Auth. And Encryption (AES128bit), 1.21, February 2011

[h] Security Reference Manual - Issue Package Generation (AES128bit), 1.21, February 2011

[i] Security Reference Manual - Changing Key Package Generation(AES128bit), 1.21, February 2011

TOE Configuration

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

Parameter name	Data length	Expected value
IC Type	1	14h
ROM Type	1	01h
Hardware version	2	34FFh
Reserved	2	0000h
ROM version	2	0503h
Update program version	2	0000h

Annex B: TOE's security architecture

Architectural overview

The TOE is an integrated circuit with an embedded smartcard operating system (as shown in Figure 1). The operating system is the FeliCa Networks Mobile FeliCa Operating System (referred onwards as FeliCa OS) and the integrated circuit is Samsung Electronics Co., Ltd (referred onwards as Samsung) chip S3CS9AB.

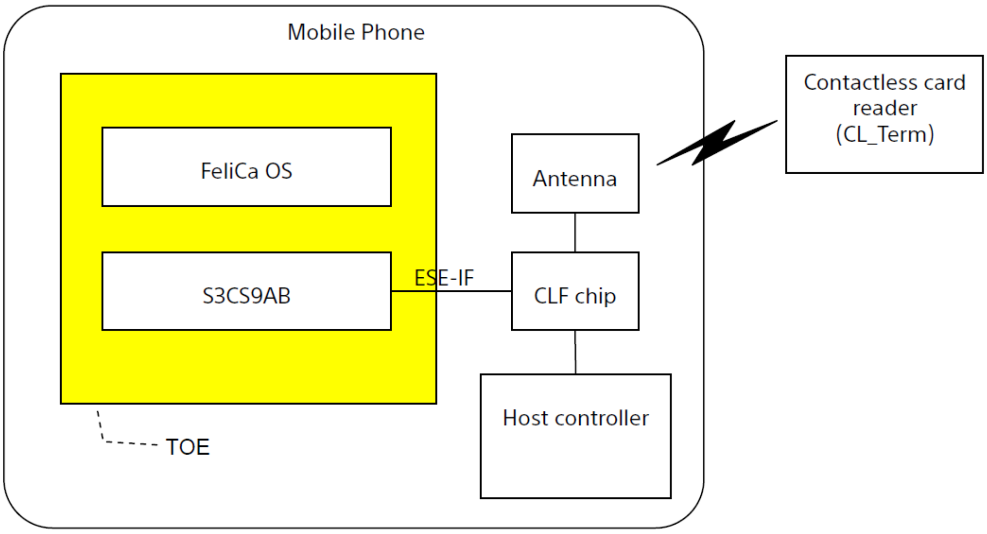

Figure 1 TOE physical scope

From a logical perspective, the TOE manages several data sets, each having a different purpose. The TOE implements a file system consisting of Areas and FeliCa Services, which organise files in a tree structure (as shown in Figure 2).

Multiple Service Providers can use an Area or a FeliCa Service. Access keys enable access to data, via the Areas and FeliCa Services. This prevents unauthorised access to the User Services of other Service Providers. By organising these keys in a specific manner, multiple Area and FeliCa Services can be authenticated simultaneously.

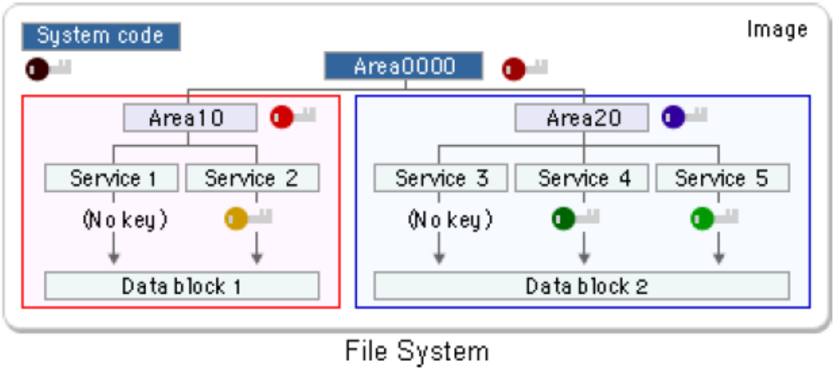

Figure 2 FeliCa file system

Non-TOE software requirements

The TOE is smart card intended to be embedded into a mobile handset. It is identified in Figure 1 that the TOE has an external interface named Embedded Secure Element interface (ESE-IF).

The ESE-IF interface is SPI compliant enabling the exchange of FeliCa commands, which are processed by the FeliCa OS. It communicates with a contactless frond end (CLF chip) being the responsible of managing the communication through the contactless antenna (with a contactless reader) and the host controller (mobile handset) via contact communication.

The CLF is necessary to enable the communication with TOE.

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.

Product Manufacturer: FeliCa Networks, Inc.

Product Name: Mobile FeliCa 3.0 on S3CS9AB/0114_5329

Type of Product: IC

Version and Release Numbers: Versions are detailed in the Certification Report

Assurance Package: EAL 4 augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.4

Evaluation Criteria: Common Criteria v. 3.1 R4

Name of IT Security Evaluation Facility: Brightsight B.V.

Name of Certification Body: SERTIT

Certification Report Identifier: SERTIT-082 CR Issue 1.0, 5. September 2016

Certificate Identifier: SERTIT-082 C

Date Issued: 5. September 2016

Kjartan Jæger Kvassnes
Certifier

Arne H. Rage
Arne Høye Rage
Quality Assurance

Kristian Bae
Kristian Steinfeld Bae
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security

CCRA recognition for components up EAL 2 and ALC_FLR only.

SOGIS MRA recognition for components up to EAL 4.