Certification Report

TOMITA Tatsuo, Chairman
Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo

IT Product (TOE)

Reception Date of Application (Reception Number)	2018-05-23 (ITC-8673)
Certification Identification	JISEC-C0660
Product Name	JREM 6K Contactless Smart Card IC chip with fast processing function for transport
Version and Release Number	1.00
Product Manufacturer	Sony Imaging Products & Solutions Inc.
Evaluation Sponsor	JR EAST MECHATRONICS CO, LTD.
Conformance of Functionality	PP conformant functionality, CC Part 2 Extended
Protection Profile Conformance	Public Transportation IC Card Protection Profile Version 1.12 (Certification Identification: JISEC-C0612)
Assurance Package	EAL5 Augmented with ALC_DVS.2, AVA_VAN.5
Name of IT Security Evaluation Facility	ECSEC Laboratory Inc., Evaluation Center

This is to report that the evaluation result for the above TOE has been certified as follows.
2019-12-25

SATO Shinji, Technical Manager
IT Security Technology Evaluation Department
IT Security Center

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme Document."

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 5
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 5

Evaluation Result: Pass

"JREM 6K Contactless Smart Card IC chip with fast processing function for transport" has

been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1 Executive Summary 1
1.1 Product Overview 1
1.1.1 Protection Profile or Assurance Package 1
1.1.2 TOE and Security Functionality 1
1.1.2.1 Threats and Security Objectives 5
1.1.2.2 Configuration and Assumptions 6
1.1.3 Disclaimers in Certification 6
1.2 Conduct of Evaluation 6
1.3 Certification 7
2 TOE Identification 8
3 Security Policy 9
3.1 Security Functional Policies 9
3.1.1 Threats and Security Functions 9
3.1.1.1 Threats 9
3.1.1.2 Security Functions against Threats 10
3.1.2 Organisational Security Policies and Security Functions 12
3.1.2.1 Organisational Security Policies 12
3.1.2.2 Security Functions for Organisational Security Policies 12
4 Assumptions and Clarification of Scope 13
4.1 Usage Assumptions 13
4.2 Environmental Assumptions 13
4.3 Clarification of Scope 14
5 Architectural Information 15
5.1 TOE Boundary and Components 15
5.2 IT Environment 16
6 Documentation 17
7 Site Security 18
8 Evaluation conducted by Evaluation Facility and Results 19
8.1 Evaluation Facility 19
8.2 Evaluation Approach 19
8.3 Overview of Evaluation Activity 19
8.4 IT Product Testing 20
8.4.1 Developer Testing 20
8.4.1.1 Platform IC Developer Testing 20
8.4.1.2 FeliCa OS Developer Testing 21
8.4.2 Evaluator Independent Testing 23
8.4.2.1 Platform IC Independent Testing 23

8.4.2.2 FeliCa OS Independent Testing 24
8.4.3 Evaluator Penetration Testing 25
8.5 Evaluated Configuration 27
8.6 Evaluation Result 27
8.7 Evaluator Comments/Recommendations 28
9 Certification 29
9.1 Certification Result 29
9.2 Recommendations 29
10 Annexes 30
11 Security Target 30
12 Glossary 31
12.1 Abbreviation relating to CC 31
12.2 Definitions of terms and abbreviations used in this report 31
13 Bibliography 33

1 Executive Summary

This Certification Report describes the content of the certification results in relation to the IT Security Evaluation of "JREM 6K Contactless Smart Card IC chip with fast processing function for transport, Version 1.00" (hereinafter referred to as the "TOE") developed by Sony Imaging Products & Solutions Inc., and the evaluation of the TOE was finished on 2019-11-28 by ECSEC Laboratory Inc., Evaluation Center(hereinafter referred to as "Evaluation Facility"). It is intended to report to the sponsor, JR EAST MECHATRONICS CO, LTD., provide security information to users (Administrator and Passenger) who are interested in the TOE.

Readers of this Certification Report are advised to read to the Security Target (hereinafter referred to as the "ST") described in Chapter 11. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements for the TOE are described in the ST.

This Certification Report assumes "general consumers who purchase this TOE" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

Reference should be made to Chapter 12 for the terms used in this Certification Report.

1.1 Product Overview

An overview of the TOE functions and operational conditions is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Protection Profile or Assurance Package

The TOE conforms to the following Protection Profile [14] (referred to as the "Conformance PP").

> Public Transportation IC Card Protection Profile Version 1.12
> (Certification Identification: JISEC-C0612)

Assurance Package of the TOE is EAL5 Augmented with ALC_DVS.2, AVA_VAN.5.

1.1.2 TOE and Security Functionality

The Conformance PP [14] describes that this TOE consists of an integrated circuit with a contactless interface and a smart card embedded software called "PT Software". The integrated circuit is the Toshiba Electronic Devices & Storage Corporation (hereinafter referred to as "Toshiba") chip T6ND8 and PT Software is the FeliCa OS developed by Sony

Imaging Products & Solutions Inc.(hereinafter referred to as "Sony") including the application for services of the Public Transportation Operator.

This TOE is used as a public transportation IC card in Japan. This TOE can be used for a stored fare card, one-day ticket card and seasonal ticket for public transportation, e-money and ID card. A public transportation operator can implement their own services while maintaining interoperability with other public transportation operators. This TOE provides flexible file system that realizes the multi-application for their services where a public transportation operator can configure access permissions and access rules to the internal data of this TOE.

Figure 1-1 shows an example operation to provide a Ticket Service. Typical operation of the ticket gate starts from detection of the card by an external entity[1]. If the mutual authentication is successfully completed, the ticket gate reads the ticket information from the card. If the ticket is valid, the ticket gate writes necessary information to the card and then allows the Passenger to pass through the gate.

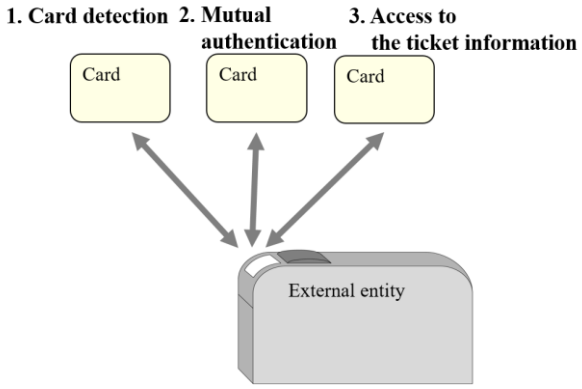


Figure 1-1 An example operation of Ticket Service

Figure 1-2 shows the physical scope of this TOE, which is indicated in blue. The components of this TOE are explained as follows:

- "FeliCa OS" constitutes the part of the TOE that is embedded software that provides the public transportation application and the operating system that is responsible for managing and providing access to a file system.
- "IC Dedicated Software" is the IC proprietary software that controls and restricts access from the FeliCa OS to T6ND8 as stated below.

[1] External entity is the entity outside the TOE, which interacts with the TOE.

- "T6ND8" consists of a security integrated circuit which is composed of a 32-bit architecture processing unit, cryptographic co-processor which supports AES and DES[2] operation, security components (e.g., security detectors, sensors and circuitry to protect the TOE), a contactless interface, and ROM, RAM and EEPROM memory.

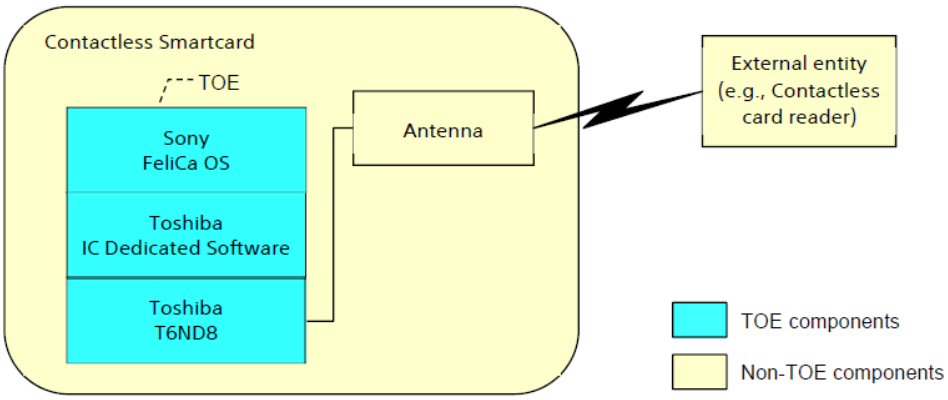


Figure 1-2 TOE physical scope

This TOE manages several data sets, each having a different purpose, on a single TOE. This TOE has a file system consisting of Areas and Services, which organises files in a tree structure as shown in Figure 1-3. The security measures of the TOE aim at protecting the access to the Areas and Services (including associated user data), and maintaining the confidentiality and integrity of assets such as the user data and Access Key.

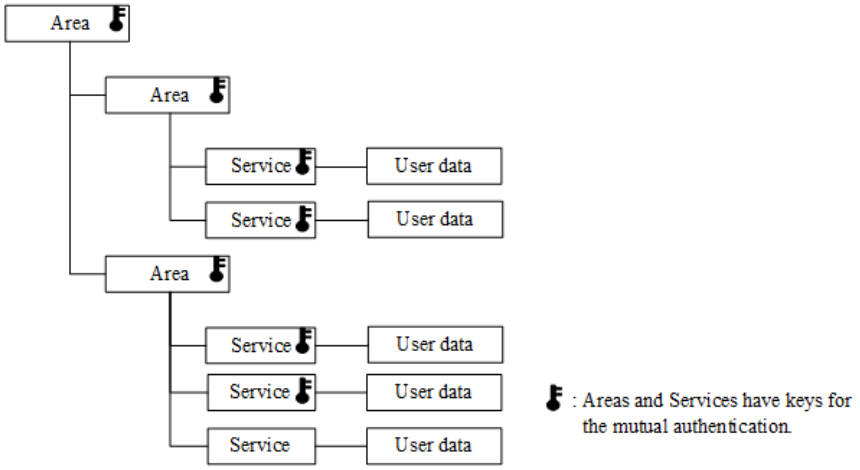


Figure 1-3 File system

[2] The functionality using DES is out of scope of the evaluation.

A Service has the Service Attribute that defines the type of access to the user data and the security condition to access the user data. If a Service requires authentication, the external entity and this TOE shall authenticate each other by using Access Key that corresponds to the Service. When the authentication is successfully completed, this TOE allows the external entity to access the user data according to the Service Attribute. This mechanism prevents unauthorised access to the user data. The summary of the access control to the user data is shown in Table 1-1.

Table 1-1 Level of access control to the user data

No.	Authentication status of the external entity	Service Attribute	Operation permitted
1	Not authenticated	Read Only Access: authentication not required	Read user data
2		Read/Write Access: authentication not required	Read/Write user data
3	Successfully authenticated with the Access Key corresponding to the Service	Read Only Access: authentication required	Read user data
4		Read/Write Access: authentication required	Read/Write user data

An Area defines the management operation of the Area and the Service. The external entity and this TOE shall authenticate each other by using Access Key that corresponds to the Area. When the authentication is successfully completed, the TOE allows the external entity to perform the management operation (e.g., setting Service Attribute).

The lifecycle of this TOE is divided into seven phases as Table 1-2.

Table 1-2 TOE lifecycle

Phase	Description
Phase 1	IC embedded software development
Phase 2	IC development
Phase 3	IC manufacturing
Phase 4	IC packaging
Phase 5	Composite product integration
Phase 6	Personalisation
Phase 7	Operational usage

- Phase 1: The TOE contains the FeliCa OS, which is developed in Phase 1 by Sony. After Phase 1, Sony delivers the FeliCa OS, its Initialisation Data and Pre-personalisation Data to Toshiba.
- Phase 2: IC development (T6ND8 design and IC Dedicated Software development) is performed by Toshiba.
- Phase 3: IC manufacturing (integration and photomask fabrication, IC production, IC testing, initialisation including injection of Initialisation Data, and Pre-personalisation) is performed by Toshiba. After Phase 3, the TOE is delivered in form of sawn wafers (dice) to the IC packaging manufacturer.
- Phase 4: IC packaging (antenna mounting and inspection) is performed by the IC packaging manufacturer.
- Phase 5: The smartcard manufacturer integrates this TOE into its public transportation IC card product and then delivers that product to the Administrator (e.g., Public Transportation Operator).
- Phase 6: The Administrator (e.g., Public Transportation Operator) performs the personalisation (issuing this TOE) where the user data, the Service Attribute and the Access Keys are loaded into this TOE memory.
- Phase 7: The public transportation IC card product is delivered to Passenger for operational use.

The Conformance PP [14] defines assurance requirements from "TOE development" (Phase 1) to "TOE delivery" (after Phase 3).

For these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance requirements required by the Conformance PP [14].

The threats and the assumptions which are assumed by this TOE are described below.

1.1.2.1 Threats and Security Objectives

This TOE counters the various threats by using the security functions as follows.
Attack Potential [12] describes Physical Attack, Side Channel Attack and Perturbation Attack as attacks against IC cards. These attacks can be applied to the TOE. The Conformance PP [14] requires the tamper-resistant functionalities that protect IC chip itself and counter the impairment of the assets.
During the mutual authentication shown in Figure 1-1, attackers may try to access the assets in the TOE by bypassing the authentication. The Conformance PP [14] requires

protection of the confidentiality and the integrity of the assets stored in the TOE by mutual authentication function and the service-dependent access control function.
The TOE connects the external antenna and communicates with an external entity via contactless interface. Attackers may try to disclose and manipulate the communication data. The Conformance PP [14] requires to counter these attacks by establishing the secure channel.
Attacker may try to access the assets in the TOE by bypassing the security functions and by exploiting the functions that are unavailable after the TOE delivery. The Conformance PP [14] requires protection from the exploitation of the functions.

1.1.2.2 Configuration and Assumptions

It is assumed that the evaluated product is used in operation under following configuration and assumptions:
The TOE is configured in a manner that the level of access control to the assets is set explicitly, and the mutual authentication mechanism between external entities and the TOE is provided. In addition, the confidentiality and the integrity of the TOE and of its manufacturing and test data must be maintained by security procedures after the TOE delivery to the personalisation.

1.1.3 Disclaimers in Certification

The TOE is out of scope of assurance in the following operations:

- Operation on the state where the operational environment of the TOE shown in "4.1 Usage Assumptions " is not secure.
- Operation under conditions which does not fill those indicated in "8.7 Evaluator Comments/Recommendations".

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility has conducted IT security evaluation and completed on 2019-11, based on functional requirements and assurance requirements of the TOE according to the publicized documents, "IT Security Evaluation and Certification Scheme Document"[1], "Requirements for IT Security Certification"[2] and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [33] and the Observation Reports [28][29][30] prepared by the Evaluation Facility, as well as evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The certification oversight reviews have also been prepared for those concerns found in the certification process. The Certification Body confirmed that all the concerns were fully resolved and the TOE evaluation has been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of[10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report and fully concluded certification activities.

2 TOE Identification

The TOE is identified as follows:

Name of TOE:	JREM 6K Contactless Smart Card IC chip with fast processing function for transport
Version:	1.00
Developer:	Sony Imaging Products & Solutions Inc.

Users can verify that a product is this TOE, which is evaluated and certified, by the following means that is described in the guidance documentation attached to the product.

Users can verify the version of T6ND8, IC Dedicated Software and FeliCa OS by using the specific command in accordance with the procedure written in [19].

The boot process of the command is common to all commands, and users enter a command by using the IC Card reader/writer. The specifications for the IC Card reader/writer are described in Chapter 2 of [18].

3 Security Policy

This chapter describes the security functional policies adopted by the TOE to counter threats, and organisational security policies.

The TOE provides the following security functionalities to be satisfied with requirements of the Conformance PP [14]:

(1) Tamper-resistant functions

(2) Access control functions to the assets

(3) Mutual authentication and secure communication functions between the external entity and the TOE

(4) Protection from abuse of the functions unavailable after the TOE delivery

3.1 Security Functional Policies

The assets to be protected in the TOE can be classified into two categories as follows:

(1) the primary asset of the TOE is the user data stored in the TOE

(2) all the assets employed to protect confidentiality and/or integrity of the primary assets are secondary assets (such as Access Key, Initialisation Data, Pre-personalisation Data, IC Dedicated Software and FeliCa OS)

The user data that should be protected is defined by Administrator in Phase 6 of the lifecycle.

The TOE counter the threats described in the section 3.1.1 and have the security functionalities satisfying the security policies described in the section 3.1.2.

3.1.1 Threats and Security Functions

3.1.1.1 Threats

Table 3-1 shows the threats to be countered by the TOE. The TOE provides security functionalities to counter them.

Table 3-1 Assumed Threats

No.	Identifier	Threats
1	T.Hardware_Attack	An attacker may perform physical attacks, perturbation attacks and side channel attacks against IC chips in order to (i) disclose or manipulate the assets of the TOE of (ii) manipulate (explore, bypass, deactivate or change) security service of the TOE.
2	T.Logical_Attack	In the operational environment after issuing the TOE, an attacker may try to (i) disclose the assets of the TOE or (ii) alter the assets of the TOE without authentication.
3	T.Comm_Attack	An attacker may try to (i) disclose the assets that are sent or receive through the communication channel or (ii) alter the messages on the communication channel.
4	T.Abuse_Func	An attacker may use functions of the TOE which may not be used after TOE delivery in order to (i) disclose or manipulate the assets of the TOE, (ii) manipulate (explore, bypass deactivate or change) security services of the TOE, (iii) manipulate (explore, bypass deactivate or change) functions of the TOE or (iv) enable an attack disclosing or manipulating the assets of the TOE.

3.1.1.2 Security Functions against Threats

The TOE counters the threats shown in Table 3-1 by the following security functions.

(1) Countering the threat T.Hardware_Attack

The TOE provides protection against the physical interaction, physical manipulation, physical probing to the hardware, and disclosing/manipulating of the assets stored in the TOE. In addition, the TOE ensures correct operation by preventing the operation other than under trusted operational environment and the normal operating conditions confirmed by the test.

(2) Countering the threat T.Logical_Attack

The TOE provides the functionality to authenticate the external entities, means to configure the level of access control for each asset explicitly, and access control mechanism according to the configured level of access control.

(3) Countering the threat T.Comm_Attack

The TOE receives and sends the assets over a contactless interface which is considered easy to eavesdrop and alter. Therefore, the TOE provides secure communication that enables the TOE and an external entity to communicate with each other in a secure manner. The secure communication protects the confidentiality and integrity of the transferred assets.

(4) Countering the threat T.Abuse_Func

The TOE prevents the abuse (see (i) to (iv)) of the functions of the TOE which may not be used after TOE Delivery: (i) to disclose critical assets of the TOE; (ii) to manipulate critical assets of the TOE; (iii) to manipulate FeliCa OS or (iv) to bypass, deactivate, change or explore security features or security services of the TOE.

3.1.2 Organisational Security Policies and Security Functions

3.1.2.1 Organisational Security Policies

Organisational security policies required in use of the TOE are shown in Table 3-2.

Table 3-2 Organisational Security Policies

No.	Identifier	Organisational Security Policy
1	P.Configure	The TOE is a tool to be used by the Administrator in a system that shall implement specific business rules. The TOE shall provide the means for the level of the access control to be specified explicitly by the Administrator for each asset.
2	P.Identification	An accurate identification shall be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.
3	P.TOE_Auth	TOE shall be able to authenticate the external entities and authenticate itself to the external entities.

3.1.2.2 Security Functions for Organisational Security Policies

The TOE provides the security functions to satisfy the organisational security policies shown in Table 3-2.

(1) Supporting the organisational security policy P.Configure

The TOE provides the means of the access control to be specified explicitly set by the Administrator.

(2) Supporting the organisational security policy P.Identification

The TOE provides the means to store Initialisation Data in its non-volatile memory. Initialisation Data (or parts of them) are used for TOE identification.

(3) Supporting the organisational security policy P.TOE_Auth

The TOE can authenticate the external entities and authenticate itself to external entities. The operational environment supports the authentication verification mechanism and prepares authentication reference data of the TOE.

4 Assumptions and Clarification of Scope

This chapter describes the assumption and the operational environment to operate the TOE as useful information for the assumed readers to determine the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumption to operate the TOE. The effective performances of the TOE security functions are not assumed unless these assumptions are satisfied.

Table 4-1 Assumptions

No.	Identifier	Assumptions
1	A.Process	It is assumed that security procedures are used after delivery of the TOE by the TOE manufacturer up to delivery to the Passenger to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).
2	A.Keys	Access Keys for TOE use are generated outside the TOE, by the supporting system in a controlled environment. This system shall check that all such keys are suitably secure by, for example, weeding out weak keys. Access Keys are then handled correctly without misoperation. The process of key generation and management shall be suitably protected and shall be performed in a controlled environment.

4.2 Environmental Assumptions

All operations of the IC card including the TOE are performed through the contactless IC card reader/writer. The TOE gets power from 13.56MHz carrier signal that is transmitted from the IC card reader/writer. The TOE communicates with the IC card reader/writer according to ISO/IEC 18092 [31] (Passive communication Mode 212/424 kbps).

It should be noted that the reliability of the hardware and the software other than the TOE shown in this configurations is out of scope in the evaluation (It is assumed that they are fully reliable).

4.3 Clarification of Scope

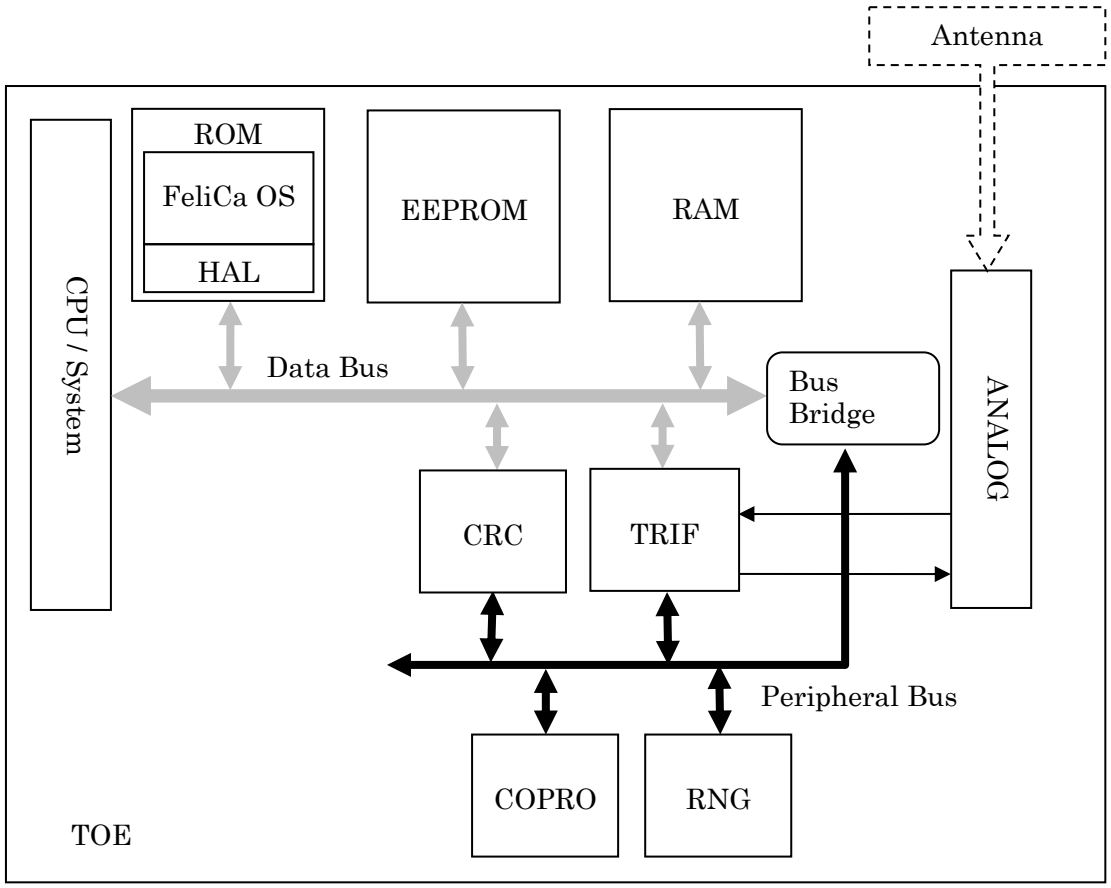
The TOE provides the command receiving function from the external entity and the response sending function to the external entity, includes the security functions countering threats shown in Table 3-1 and the security functions satisfying the organisational security policies shown in Table 3-2. However, the effective performances of the TOE security functions are not assumed unless assumptions shown in Table 4-1 are satisfied.

5 Architectural Information

This chapter explains the scope and the main components of the TOE.

5.1 TOE Boundary and Components

Figure 5-1 shows the composition of the TOE. The TOE does not include the antenna.



IC: T6ND8

Figure 5-1 Composition of the TOE

Table 5-1 shows the components of TOE.

Table 5-1 Components of TOE

No.	Component	Description
1	FeliCa OS	Embedded software that provides the public transportation application and the operating system.
2	IC Dedicated Software	Dedicated software embedded in a security IC. HAL (Hardware Abstract Layer) providing FeliCa OS with the APIs of functions of hardware.
3	T6ND8	A security integrated circuit which is composed of CPU/System, EEPROM, RAM, ROM, TRIF, COPRO, CRC, RNG and ANALOG.

5.2 IT Environment

The TOE is packaged in an IC card and used. Operation of the TOE does not rely on other IT environment, except for the power supplied from an external entity. The public transportation operators are required to prepare IC card reader/writer depending on their purpose.

6 Documentation

The identification of documentations attached to the TOE is listed below. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

[18] FeliCa Card User's Manual Version 1.04, August 2017

[19] RC-S114 Inspection Procedure Version 1.00, January 2018

[20] RC-S114 Inspection and IDm Writing Procedure Version 1.00, January 2018

[21] Product Acceptance Procedure Version 1.0, February 2015

[22] FeliCa Card AES Encryption Mechanism Transition Guide Version 1.0, August 2012

[23] RC-S114 Important Notice for customers Version 1.1, November 2019

[24] Security Reference Manual – Group Key Generation (AES 128bit) Version 1.21, January 2019

[25] Security Reference Manual – Mutual Authentication & Secure Communication (AES 128bit) Version 1.21, January 2019

[26] Security Reference Manual – Package Generation (AES 128bit) Version 1.21, January 2019

[27] Security Reference Manual – Changing Key Package Generation (AES 128bit) Version 1.21, January 2019

7 Site Security

In the evaluation of this TOE, Minimum Site Security Requirements [13] were applied in the evaluation of ALC_DVS.2. Sites related to the TOE are shown in Table 7-1.

Table 7-1 Sites related to the TOE

No.	Site	Activity	Date of site audit
1	Sony Imaging Products & Solutions Inc. (Osaki Shinagawa-ku, Tokyo)	FeliCa OS development, OS Delivery	2018-08-20
2	Toshiba Electronic Devices & Storage Corporation (Kawasaki-city, Kanagawa)	IC development	2018-10-11
3	D.T.Fine Electronics Co., Ltd Kitakami operations (Kitakami-city, Iwate)	Photomask fabrication	2019-04-02
4	JAPAN SEMICONDUCTOR CORPORATION Oita operations (Oita-city, Oita)	Wafer production, Delivery	2018-10-25, 2018-10-26

8 Evaluation conducted by Evaluation Facility and Results

8.1 Evaluation Facility

ECSEC Laboratory Inc. Evaluation Center that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which joins Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

8.2 Evaluation Approach

The evaluation was conducted by using the evaluation methods prescribed in the CEM and CC supporting documents [12][13] and proprietary methods [32] of the Evaluation Facility in accordance with the assurance components in the CC Part 3.

Details for evaluation activities were reported in the Evaluation Technical Report [33].

The Evaluation Technical Report explains the summary of the TOE as well as the content of the evaluation and the verdict of each work unit in the CEM, CC supporting documents [12][13] and proprietary methods [32]of the Evaluation Facility [32].

8.3 Overview of Evaluation Activity

The history of the evaluation activities is described in the Evaluation Technical Report as follows.

The evaluation started on 2018-05 and concluded upon completion of the Evaluation Technical Report dated 2019-11. The Evaluation Facility received a set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidences in relation to a series of evaluation conducted.

Additionally the evaluator directly visited the development and manufacturing sites on 2018-08, 2018-10 and 2019-04, and examined procedural status conducted in relation to each work unit for configuration management, delivery and development security by investigating records and interviewing staff. Furthermore, the evaluator conducted the sampling check 2018-08, 2018-10 and 2019-10, the independent testing by the evaluator on 2018-06, 2018-09, 2019-07 and 2019-09 and the penetration test from 2018-05 to 2019-09.

Concerns found in evaluation activities for each work unit were all issued as the Observation Reports, and those were reported to the developer. Those concerns were reviewed by the developer, and all the concerns were solved eventually.

Concerns in the evaluation process that the Certification Body found were described as the certification oversight reviews, and they were sent to the Evaluation Facility.

The Evaluation Facility and the developer examined them, which were reflected in the Evaluation Technical Report.

8.4 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed. As a result of the evidence shown in the process of the evaluation and after confirmation of the validity, the evaluator performed the reproducibility testing, additional testing and penetration testing based on vulnerability assessments judged to be necessary. In this section, T6ND8 and IC Dedicated Software are collectively denoted as "platform IC".

8.4.1 Developer Testing

Developer testing was performed by the platform IC developer and the FeliCa OS developer respectively. The evaluator evaluated by the integrity of the developer testing that the developer performed and the documentation of actual test results. The content of the developer testing evaluated by the evaluator is explained as follows.

8.4.1.1 Platform IC Developer Testing

a) Test Summary

The platform IC developer performed testing on the platform IC of the TOE. A part of the developer testing is performed in the test mode. The evaluator analysed that it was a valid alternative method to demonstrate the behaviour of the TSF.

Figure 8-1 shows the developer testing environment. The testing is performed by observing responses to the commands to the platform IC. The calibration of the LSI tester was confirmed by the tester calibration record dated 2018-10-14.

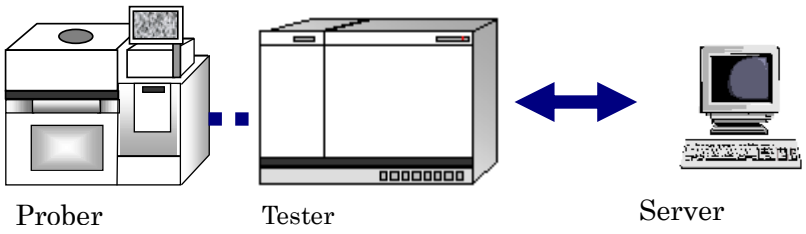


Figure 8-1 Platform IC Developer Testing Environment

The developer submitted the developer testing documentation including the test plan, the test procedure, the expected test results and the actual test results to the evaluators. The evaluators verified whether the test configuration was consistent with the ST, whether all the expected results were written, and whether the actual test results matched the expected results in the documentation. In addition, the evaluators performed the sampling test (see Table 8-1) using the developer testing environment.

Table 8-1 Platform IC Sampling Test

No.	Test contents
1	Set the IC into the test mode using the LSI tester and confirm its behaviour after setting test parameters.

b) Coverage of Developer Testing

The evaluators confirmed that the coverage of the developer testing satisfied the assurance component ATE_COV.2 and the scope of the performed testing was appropriate. The relating test contents and results are shown in the Evaluation Technical Report [33].

c) Result

The evaluators confirmed the approach of the performed developer testing and the appropriateness of test items, and confirmed consistencies between the testing approach described in the testing plan and the actual testing approach. The evaluators confirmed consistencies between the testing results expected by the developer and the actual testing results performed by the developer.

8.4.1.2 FeliCa OS Developer Testing

a) Test Summary

The FeliCa OS developer performed testing on the TOE with FeliCa OS. Figure 8-2 shows the developer testing environment.

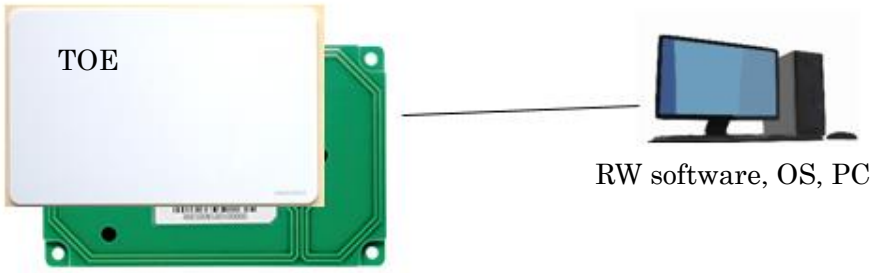


Figure 8-2 Sampling Test Environment and Independent Testing Environment of FeliCa OS

The developer submitted the developer testing documentation including the test plan, the test procedure, the expected test results, and the actual test results to the evaluators. The evaluators verified whether the test configuration was consistent with the ST, whether all the expected results were documented, and whether the actual test results matched the expected results in the documentation. In addition, the evaluators performed the sampling test (see Table 8-2) of the FeliCa OS developer test using testing environment shown in Figure 8-2 assuming the TOE after delivery to a Passenger.

Table 8-2 Sampling Test on FeliCa OS

No.	Test contents
1	Send the commands that can be used in the operational phase to the TOE and confirm that the responses from the TOE satisfy the command specification.
2	Send the commands that are mainly used in the manufacturing phase to the TOE and confirm that the responses from the TOE satisfy the command specification.
3	Taking into account the life cycle of the TOE, search all the command codes and conform that the TOE behaves as expected for each command code.
4	Obtain random numbers from the TOE and perform statistical testing.

b) Coverage of Developer Testing

The evaluators confirmed that the coverage of the developer testing satisfied the assurance component ATE_COV.2 and the scope of the performed testing was appropriate. The relating test contents and results are shown in the Evaluation Technical Report [33].

c) Result

The evaluators confirmed the approach of the performed developer testing and the appropriateness of test items, and confirmed consistencies between the testing approach described in the testing plan and the actual testing approach. The evaluators confirmed consistencies between the testing results expected by the developer and the actual testing results performed by the developer.

8.4.2 Evaluator Independent Testing

The evaluators performed the sample testing to reconfirm the execution of security functions by the test items extracted from the developer testing. In addition, the evaluators performed the evaluator independent testing (hereinafter referred to as "independent testing") to gain further assurance that security functions are certainly implemented, based on the evidence shown in the process of the evaluation, on Platform IC and FeliCa OS.

The independent testing performed by the evaluator is explained below.

8.4.2.1 Platform IC Independent Testing

1) Configurations in the Independent Testing

The evaluators performed Platform IC independent testing using the test environment shown in Figure 8-3.

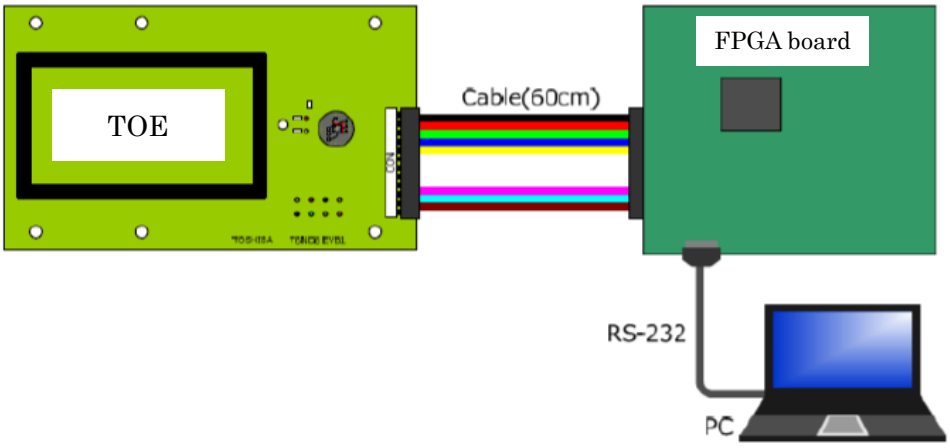


Figure 8-3 Platform IC Independent Testing Environment

2) Summary of the Independent Testing

The independent testing performed by the evaluator is as follows:

a) Viewpoints of the Independent Testing

Viewpoints of the independent testing that the evaluators designed from the developer testing and the provided evaluation documentation are described below.

- Confirm the quality of the random numbers generated and used by the TOE.
- Confirm the correctness of its implementation of the algorithms that become targets of the cryptographic algorithm testing of the CAVP (Cryptographic Algorithm Validation Program).

b) Independent Testing Outline

The evaluators devised the additional independent testing from the above viewpoints, based on the developer testing and the provided evaluation documentation.

The list of the independent testing that the evaluator performed is shown in Table 8-3.

Table 8-3 Platform IC Independent Testing

No.	Test contents
1	Measurement of the entropy of random numbers
2	Cryptographic algorithm testing

c) Result

The measured random number entropy was higher than the expected value. And, all targets of cryptographic algorithm testing passed (CAVP Validation Number 5691).

As stated above, all independent testing performed by the evaluator completed correctly, and the evaluators confirmed the behaviour of the TOE. The evaluator confirmed that all testing results were corresponding with the expected behaviour.

8.4.2.2 FeliCa OS Independent Testing

1) Configurations of Independent Testing

The evaluators assumed the TOE to be delivered to the Passenger and performed FeliCa OS independent testing using the test environment shown in Figure 8-2 in the Evaluation Facility.

2) Summary of the Independent Testing

The independent testing performed by the evaluator is as follows:

a) Viewpoints of the Independent Testing

Viewpoints of the independent testing that the evaluators devised from the developer testing and the provided evaluation documentation are described below.

- Confirm the commands that shall be disabled during pre-personalisation is correctly disabled.

b) Independent Testing Outline

The evaluators devised the additional independent testing from the above viewpoints, based on the developer testing and the provided evaluation documentation.

The list of the independent testing that the evaluator performed is shown in Table 8-4.

Table 8-4 FeliCa OS Independent Testing

No.	Test contents
1	Confirming that the behaviour of the TOE is corresponding with the expected behaviour, by inputting commands the TOE that shall be disabled during per-personalisation.

c) Result

All independent testing performed by the evaluators completed correctly, and the evaluators confirmed the behaviour of the TOE. The evaluators confirmed that all testing results were corresponding with the expected behaviour.

8.4.3 Evaluator Penetration Testing

The evaluators devised and performed the necessary evaluator penetration testing (hereinafter referred to as the "penetration testing") on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level from the evidences shown in the process of the evaluation.

The penetration testing performed by the evaluator is explained as follows.

1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is as follows.

a) Identification of Vulnerabilities

The evaluator searched into the provided evidences and the publicly available information for the potential vulnerabilities, and then identified vulnerabilities which require the penetration testing based on the CC supporting documents [12][13] and proprietary methods of the Evaluation Facility [32].

b) Penetration Testing Outline

The evaluator performed the following penetration testing to identify potentially exploitable vulnerabilities.

<Penetration Testing Environment>

The penetration testing has the perturbation attack using the laser radiation and the side channel attack. Figure 8-4 and Figure 8-5 shows the rough configuration for each attack.

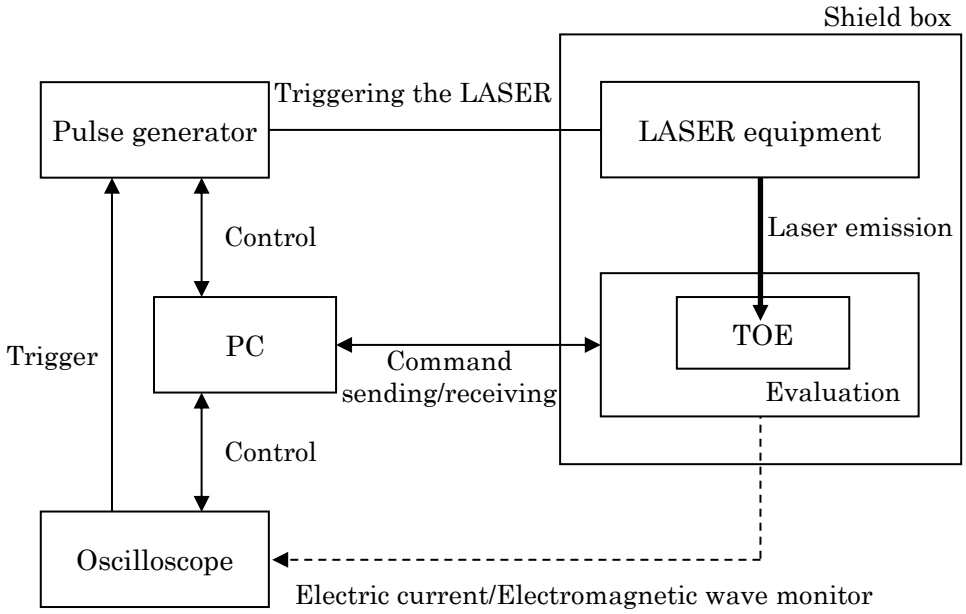


Figure 8-4 The configuration of the penetration testing for the perturbation attack

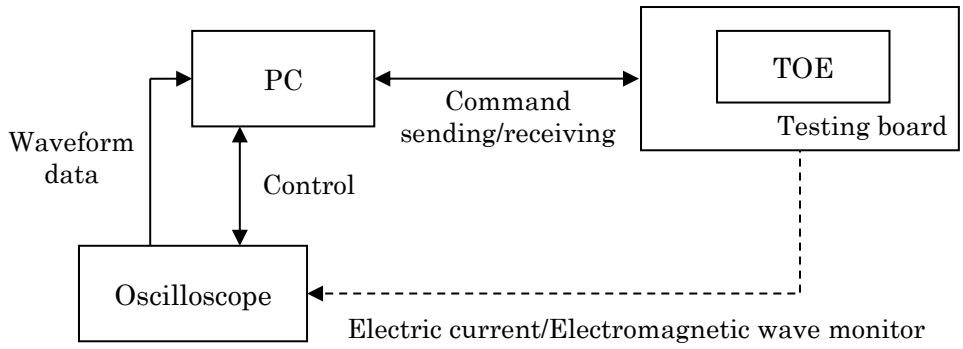


Figure 8-5 The configuration of the penetration testing for the side channel attack

<Contents of the Performed Penetration Testing>

Contents of the penetration testing are devised according to the identified vulnerabilities.

c) Result

In the penetration testing performed by the evaluator, the evaluators did not find any exploitable vulnerabilities that attackers who have the high attack potential defined in CC part3 [6] could exploit.

8.5 Evaluated Configuration

The Evaluation Facility performed evaluation with the configuration of the sampling test shown in "8.4.1 Developer Testing", the configuration shown in "8.4.2 Evaluator Independent Testing", and the configuration shown in "8.4.3 Evaluator Penetration Testing".

8.6 Evaluation Result

The evaluators have concluded that the TOE satisfies all work units prescribed in the CEM as described in the Evaluation Technical Report [33].

The following security requirements were confirmed in the evaluation:

- PP Conformance: Public Transportation IC Card Protection Profile Version 1.12 (Certification Identification: JISEC-C0612)
- Security Functional Recruitments: Common Criteria Part 2 extended
- Security Assurance Requirements: Common Criteria Part 3 conformant

As a result of the evaluation, the verdict "PASS" has been confirmed for the following assurance components:

- All assurance components of EAL5 package

- Additional assurance components ALC_DVS.2 and AVA_VAN.5

The result of the evaluation is only applied to those which are composed by the TOE corresponding to the identification described in Chapter 2.

8.7 Evaluator Comments/Recommendations

The TOE pays no attention to the key value of Access Key written by the Administrator after the TOE delivery. The Administrator or the organisation to which the Administrator belongs shall be responsible for determination of appropriate key value and its secure control in accordance with the user manual [18].

The Administrator of the TOE should perform risk analysis as needed, by monitoring the progress of the attack techniques at the time of using a TOE.

9 Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the evaluation process.

1. Contents pointed out in the Observation Reports shall be adequate.
2. Contents pointed out in the Observation Reports shall properly be solved.
3. The submitted documentation was sampled, the content was examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.
4. The rationale for the evaluation verdict by the evaluator presented in the Evaluation Technical Report is adequate.
5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM and CC supporting documents [12][13].

Concerns found in the certification process were prepared as the certification oversight reviews, and they were sent to the Evaluation Facility.

The Certification Body confirmed such concerns pointed out in the certification oversight reviews have been solved in the ST [16] and the Evaluation Technical Report and has issued this Certification Report.

9.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report, Observation Reports and related evaluation documentation, the Certification Body has determined that the TOE satisfies all assurance requirements for EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 in the CC Part 3.

9.2 Recommendations

Procurement entities and users of the TOE should take the certification result into account in their risk management of the system where the TOE is used. For example, they should determine the timing of "re-assessment" to confirm the validity of the certificate and the other dependent certificates in accordance with the changes in attack methods or related technologies. In addition, procurement entities and users of the TOE should also review the validity of usage of the cryptographic algorithm in their risk management of the system where the TOE is used.

10 Annexes

There is no annex.

11 Security Target

The ST-Lite [17] of the TOE is provided as a separate document from this Certification Report.

> Security Target JREM 6K Contactless Smart Card IC chip with fast processing function for transport Public Version, Version 2.0, November 2019, Sony Imaging Products & Solutions Inc.

This ST-Lite is the sanitised version of the evaluated full ST [16] based on the CC supporting document, ST sanitizing for publication [15].

12 Glossary

12.1 Abbreviation relating to CC

The abbreviations relating to the CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
ST-Lite	Security Target Lite
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2 Definitions of terms and abbreviations used in this report

The definitions of terms and abbreviations relating to the TOE used in this report are listed below.

Access Key	A key that is used to access to the data used as the ticket service.
Administrator	An entity responsible for personalisation of the TOE. In most cases, a Public Transportation Operator is a representative example of Administrator.
Area	A part of the file system. An Area is similar to a directory in a general file system.
External Entity	IT entity possibly interacting with the TOE from outside of the TOE boundary.
Initialisation Data	Initialisation Data defined by the card manufacturer to identify the TOE and to keep track of the IC's production.
Pre-personalisation Data	Any data supplied by the developer of FeliCa OS that is injected into the non-volatile memory by the IC manufacturer or the IC packaging manufacturer.
Passenger	A person who uses Ticket Service.
Public Transportation Operator	An entity that provides a specific service to a Passenger.
Service	The part of the file system that contains Service Attribute. A Service is similar to a file in a general file system.
Service Attribute	Attribute to define types of accesses to user data and security conditions to access user data.

Ticket Service	A specific service to a Passenger that is made technically possible by the TOE. Each Ticket Service is provided by a Public Transportation Operator to a Passenger.
AES	Advanced Encryption Standard
API	Application Programming Interface
COPRO	Co-processor
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
EEPROM	Electrically Erasable Programmable Read-Only Memory
HAL	Hardware Abstract Layer
PT Software	Public Transportation Software
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
TRIF	Transmit & Receive Interface

13 Bibliography

[1] IT Security Evaluation and Certification Scheme Document, July 2018, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, September 2018, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, September 2018, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001, (Japanese Version1.0, July 2017)

[8] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002, (Japanese Version1.0, July 2017)

[9] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003, (Japanese Version1.0, July 2017)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 5, April 2017, CCMB-2017-04-004, (Japanese Version1.0, July 2017)

[12] Joint Interpretation Library - Application of Attack Potential to Smartcards, Version 2.9, January 2013

[13] Joint Interpretation Library – Minimum Site Security Requirements, Version 1.1 (for trial use), July 2013

[14] Public Transportation IC Card Protection Profile Version 1.12 (Certification Identification: JISEC-C0612)

[15] ST sanitising for publication, April 2006, CCDB-2006-04-004

[16] Security Target JREM 6K Contactless Smart Card IC chip with fast processing function for transport Version 2.0, November 2019
[17] Security Target JREM 6K Contactless Smart Card IC chip with fast processing function for transport Public Version, Version 2.0, November 2019
[18] FeliCa Card User's Manual Version 1.04, August 2017
[19] RC-S114 Inspection Procedure Version 1.00, January 2018
[20] RC-S114 Inspection and IDm Writing Procedure Version 1.00, January 2018
[21] Product Acceptance Procedure Version 1.0, February 2015
[22] FeliCa Card AES Encryption Mechanism Transition Guide Version 1.0, August 2012
[23] RC-S114 Important Notice for customers Version 1.1, November 2019
[24] Security Reference Manual – Group Key Generation (AES 128bit) Version 1.21, January 2019
[25] Security Reference Manual – Mutual Authentication & Secure Communication (AES 128bit) Version 1.21, January 2019
[26] Security Reference Manual – Package Generation (AES 128bit) Version 1.21, January 2019
[27] Security Reference Manual – Changing Key Package Generation (AES 128bit) Version 1.21, January 2019
[28] Observation Report SUY-EOR-0001-00, August 31, 2018, ECSEC Laboratory Inc. Evaluation Center
[29] Observation Report SUY-EOR-0002-00, January 11, 2019, ECSEC Laboratory Inc. Evaluation Center
[30] Observation Report SUY-EOR-0003-00, August 27, 2019, ECSEC Laboratory Inc. Evaluation Center
[31] Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1), ISO/IEC 18092:2013, March 2013
[32] Vulnerability Assessment for Security IC and Similar Devices, Version 1.2, January 27, 2014, ECSEC Lab. EMIC-VAN4_5-0001-02
[33] JREM 6K Contactless Smart Card IC chip with fast processing function for transport Evaluation Technical Report, Version 6.1, December 2, 2019, ECSEC Laboratory Inc. Evaluation Center, SUY-ETR-0006-01B