SONY®

Contactless Smart Card IC

Security Target
JREM 6K Contactless Smart Card IC chip with fast processing function for transport

Version 2.0

Public Version

No. J6K-STP-E02-00

- Information in this document is subject to change without notice.
- Sony assumes no liability for damages arising from, or in connection with, the use of this document.

Introduction

This document is the Security Target for CC evaluation of IC chip product "JREM 6K Contactless Smart Card IC chip with fast processing function for transport".

Contents

1 Introducing the Security Target

This document is the Security Target for CC evaluation of IC chip product JREM 6K Contactless Smart Card IC chip with fast processing function for transport.

This Security Target is provided in accordance with "Common Criteria for Information Technology Security Evaluation" [CC].

For definitions of the terms, abbreviations, and literary references used in this document, see Chapter 8, "Glossary and references".

1.1 ST and TOE Identification

This section provides the information necessary to identify and control this Security Target and its TOE, FeliCa Contactless Smart Card IC JREM 6K Contactless Smart Card IC chip with fast processing function for transport.

Table 1: ST identification

ST attribute	Value
Name	Security Target JREM 6K Contactless Smart Card IC chip with fast processing function for transport
Version	2.0
Reference	J6K-STP-E02-00
Issue Date	November 2019

Table 2: TOE identification

TOE attribute	Value
Name	JREM 6K Contactless Smart Card IC chip with fast processing function for transport
Version	1.00
Product type	Contactless Smart Card IC
Form Factor	bare chip with bump on wafer

1.2 TOE Overview

The TOE is an integrated circuit with a contactless interface and a smart card embedded software called "PT Software" in the Protection Profile [PTPP]. The TOE is used as a public transportation IC card in Japan.

The integrated circuit is the Toshiba Electronic Devices & Storage Corporation (hereinafter referred to as "Toshiba") chip T6ND8 and PT Software is the FeliCa Operating System developed by Sony Imaging Products & Solutions Inc. (hereinafter referred to as "Sony") including the application for services of the Public Transportation Operator (referred to in this document as FeliCa OS).

All operations on the TOE are performed through a contactless card reader. Under the control of the FeliCa OS the TOE communicates with the contactless card reader according to ISO/IEC 18092 (Passive Communication Mode 212/424kbps) [ISO 18092].

In this Security Target, the contactless card reader is expressed as CC term external entity[1], which can be a standalone card reader, or a contactless interface device that is connected to the controller where command processing is performed.

The following figure illustrates the physical scope of the TOE, which is indicated in blue:

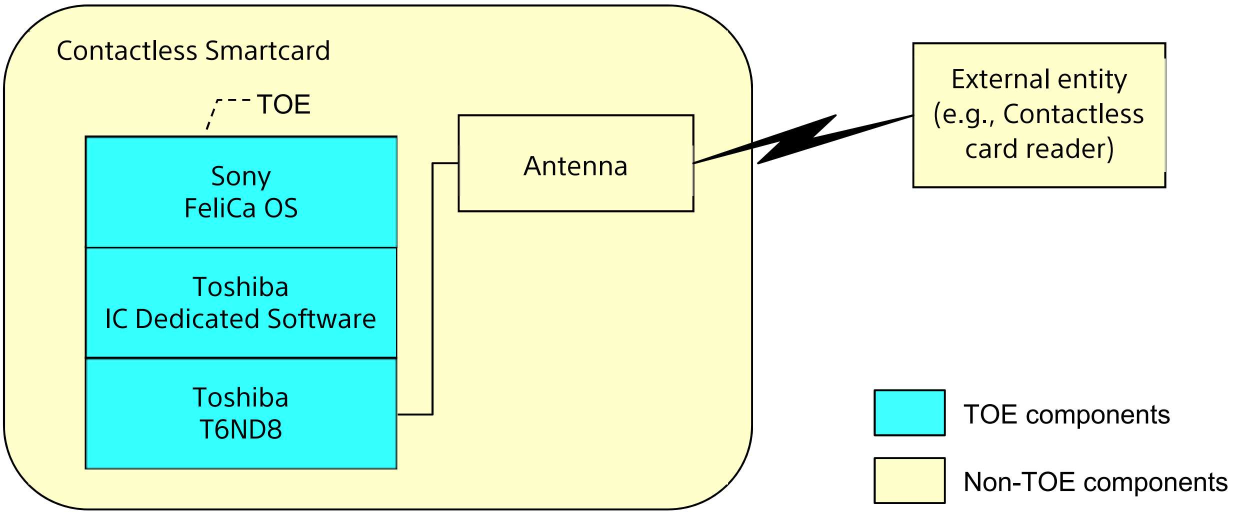

Figure 1: TOE physical scope

The components of the TOE are explained as follows:

- "FeliCa OS" constitutes the part of the TOE that is an 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 the Toshiba hardware platform. It is also used for testing purposes during production.
- "Toshiba T6ND8" is 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.

[1] Human or IT entity possibly interacting with the TOE from outside of the TOE boundary

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

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 Services, which organise files in a tree structure (as shown in Figure 2). 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.

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 the TOE shall authenticate each other by using Access Key that corresponds to the Service. When the authentication is successfully completed, the 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 3.

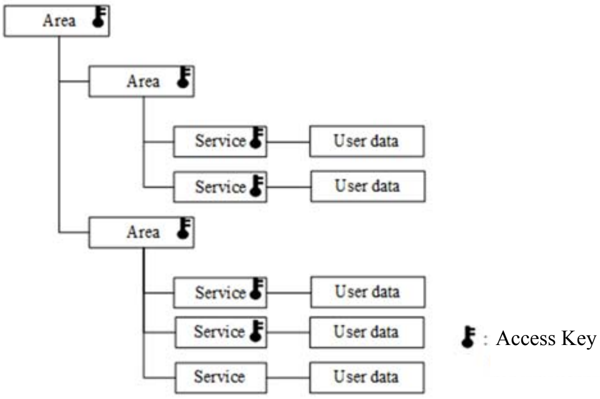

Figure 2: The FeliCa file system

Table 3: Level of access control to the user data

Authentication status of the external entity	Service Attribute	Operation permitted
Not authenticated	Read Only Access: authentication not required	Read user data
	Read/Write Access: authentication not required	Read/Write user data
Successfully authenticated with the Access Key corresponding to the Service	Read Only Access: authentication required	Read user data
	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 the 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 TOE offers the following features:

- it can receive FeliCa commands from the external entity
- it can send FeliCa responses to the external entity

The TOE offers the following security features:

- mutual authentication between the external entity and the TOE
- management of Services (e.g., setting Service Attribute)
- controlled access to the user data stored internally in the TOE
- trusted communication channel between the external entity and the TOE
- protection of confidentiality and integrity of assets stored internally in the TOE
- anti-tearing and rollback mechanism
- protection against excess environment conditions
- protection against information leakage
- protection against probing and alteration
- prevent abuse of function
- support of unique identification of the TOE

The security features are provided partly by the FeliCa OS and partly by the underlying hardware.
The lifecycle of the TOE is explained in Section 1.3.
The delivery items of the TOE are explained in Section 1.4.
The assets that the TOE is expected to protect are described in Section 3.1.
The threats to be countered by the TOE, the assumptions about the TOE environment, the organisational security policies with which the TOE is designed to comply are described in Section 3.2, 3.3, and 3.4.

1.3 Lifecycle

The lifecycle of the TOE is explained using the smartcard lifecycle as defined in the Protection Profile [PTPP], which includes the phases listed in the following table:

Table 4: Phases of the TOE lifecycle

Phase	Description
Phase 1	IC embedded software development
Phase 2	IC development
Phase 3	IC manufacturing

Phase	Description
Phase 4	IC packaging
Phase 5	Composite product integration
Phase 6	Personalisation
Phase 7	Operational usage

The FeliCa OS is developed in Phase 1. The IC and IC Dedicated Software is developed in Phase 2 and produced in Phase 3. Then the TOE is delivered in form of sawn wafers (dice) at the end of **Phase 3**.

The Protection Profile [PTPP] defines assurance requirements for the TOE's development and production environment up to TOE Delivery.

An explanation of each phase of the TOE lifecycle follows:

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 (IC 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 the 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 the TOE) where the user data, the Service Attribute and the Access Keys are loaded into the TOE memory.

Phase 7: The public transportation IC card product is delivered to Passenger for operational use.

1.4 Delivery

The TOE delivery items are listed in the following table:

Table 5: TOE delivery items

Delivery item type	Identifier	Version	Medium
Hardware	Toshiba T6ND8 Smartcard IC – Hardware	5106	Smartcard integrated circuit
Software	Toshiba T6ND8 Smartcard IC – IC Dedicated Software	5401	Embedded in hardware

Delivery item type	Identifier	Version	Medium
	FeliCa OS v5.0	A201	Embedded in hardware
Manuals	FeliCa Card User's Manual	1.04	PDF or Paper
	RC-S114 Inspection Procedure	1.00	PDF or Paper
	RC-S114 Inspection and IDm Writing Procedure	1.00	PDF or Paper
	Product Acceptance Procedure	1.0	PDF or Paper
	FeliCa Card AES Encryption Mechanism Transition Guide	1.0	PDF or Paper
	RC-S114 Important Notice for customers	1.1	PDF or Paper
	Security Reference Manual – Group Key Generation (AES 128bit)	1.21	PDF or Paper
	Security Reference Manual – Mutual Authentication & Secure Communication (AES 128bit)	1.21	PDF or Paper
	Security Reference Manual – Package Generation (AES 128bit)	1.21	PDF or Paper
	Security Reference Manual – Changing Key Package Generation (AES 128bit)	1.21	PDF or Paper

The TOE is delivered by a trustworthy courier delivery.

The PDF-formatted document is delivered through e-mail, and the paper document is delivered by handover or post.

1.5 Available non-TOE hardware/software/firmware

The TOE is used as the IC card. Operation of the TOE does not rely on other IT environment, except for power supply from an external entity.

Public Transportation Operators are required to prepare card readers depending on their purposes.

2 Conformance Claims

This chapter describes the conformance claims.

2.1 CC Conformance Claim

The evaluation is based on the following:

- "Common Criteria for Information Technology Security Evaluation", Version 3.1 Release 5 (composed of Parts 1-3, [CC Part 1], [CC Part 2], and [CC Part 3])
- "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1 [CC CEM]

This Security Target claims the following conformances:

- [CC Part 2] extended
- [CC Part 3] conformant

2.2 Package Claim

The minimum level of assurance is:

- Evaluation Assurance Level 5 (EAL5) augmented with ALC_DVS.2 and AVA_VAN.5

2.3 PP Claim

This Security Target and the TOE claim strict conformance to the following Protection Profile (PP):

- "Public Transportation IC Card Protection Profile", Version 1.12 [PTPP]

2.4 PP Claim Rationale

This Security Target claims strict conformance to the Protection Profile [PTPP].

The TOE type defined in section 1.2 of this Security Target is an integrated circuit including software package, together with guidance manual. This is consistent with the TOE type defined in section 1.2 of the Protection Profile [PTPP].

The items of security problem definitions, security objectives and security requirements are taken from the Protection Profile [PTPP].

3 Security Problem Definition

The statement of the security problem describes the assets that the TOE is expected to protect and the security measures that are to be enforced by the TOE or its operational environment.

To this end, the security problem definition (this chapter) identifies and lists the following:

- primary and secondary assets
- the threats to be countered by the TOE
- the assumptions about the TOE environment
- the organisational security policies with which the TOE is designed to comply.

3.1 Assets

The assets that the TOE is expected to protect are as follows:

- the primary asset of the TOE is the user data stored in the TOE
- all the assets employed to protect confidentiality and/or integrity of the primary assets are secondary assets (such as Access Key, FeliCa OS, Initialisation Data and Pre-personalisation Data)

The user data that shall be protected is defined by the Administrator in the personalisation phase. The TOE allows a flexible, configurable access control system, and therefore, a user data can be public or kept confidential according to access control policy.

3.2 Threats

This section describes threats. The threats shall be countered by the TOE, or/and its operational environment.

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 or (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE.

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.

T.Comm_Attack

An attacker may try to (i) disclose the assets that are sent or received through the communication channel or (ii) alter the messages on the communication channel.

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.

3.3 Organisational Security Policies

This section describes organisational security policies that apply to TOEs and operational environment.

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.

P.Identification

An accurate identification shall be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.

P. TOE_Auth

TOE shall be able to authenticate the external entities and authenticate itself to the external entities.

3.4 Assumptions

This section describes assumptions to be addressed in the operational environment of the TOE. These assumptions need to be true for the effective security functionality of the TOE.

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).

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 Security Objectives

This chapter describes the security objectives for the TOE and the TOE environment in response to the security needs identified in Chapter 3, "Security problem definition".

Security objectives for the TOE are to be satisfied by technical countermeasures implemented by the TOE. Security objectives for the environment are to be satisfied either by technical measures implemented by the IT environment, or by non-IT measures.

4.1 TOE Security Objectives

The following TOE Security Objectives have been identified for the TOE, as a result of the discussion of the Security Problem Definition. Each objective is stated in bold type font. It is followed by an application note, in regular font, which provides additional information and interpretation.

O.Hardware_Attack

The TOE shall provide protection against in place to handle the physical interaction, physical manipulation and physical probing to the hardware and disclosure/reconstruction of assets while stored and/or processed in the IC chips. In addition, the TOE shall ensure its correct operation by preventing its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested.

O.AC

The TOE shall be able to authenticate the external entities. And the TOE shall provide the means of controllable limited access to the objects and resources they own or are responsible for in a configurable and deterministic manner. This objective combines all aspects of authentication and access control.

O.Auth

The TOE shall be able to authenticate the external entities and authenticate itself to external entities.

O.Configure

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

O.Comm_Attack

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

O.Abuse_Func

The TOE shall prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order to (i) disclose critical assets of the TOE, (ii) manipulate critical assets of the TOE, (iii) manipulate PT Software or (iv) bypass, deactivate, change or explore security features or security services of the TOE. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

O.Identification

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

4.2 TOE Operational Environment Security Objectives

This section identifies the IT security objectives that are to be satisfied by the imposing of technical or procedural requirements on the TOE operational environment. Each objective is stated in bold type font; it is followed by an application note, in regular font, which supplies additional information and interpretation.

OE.TOE_Auth

The operational environment shall support the authentication verification mechanism and know authentication reference data of the TOE.

OE.Keys

Access Keys for use by the TOE are generated externally (that is, beyond control of the TOE). The generation and handling of the keys shall be performed in a secure manner.

OE.Process

In the TOE environment, confidentiality and integrity of the TOE and its manufacturing and test data shall be maintained by means of procedural measures between delivery of the TOE by the TOE manufacturer and delivery of the TOE to the Passenger.

4.3 Security Objectives Rationale

This section demonstrates the suitability of the choice of security objectives and that the stated security objectives counter all identified threats, policies, or assumptions.

The following table maps the security objectives to the security problem, which is defined by the relevant threats, policies, and assumptions. This illustrates that each threat, policy, or assumption is covered by at least one security objective. The section 4.3 of the Protection Profile [PTPP] gives the rationale of showing that the security objectives are sufficient and suitable to address the threats, assumptions, and policies.

Table 6: Assumptions, Threats or Policies versus Security Objectives

Threat, Policy or Assumption	Objective
T.Hardware_Attack	O.Hardware_Attack
T.Logical_Attack	O.AC

Threat, Policy or Assumption	Objective
T.Comm_Attack	O.Comm_Attack
T.Abuse_Func	O.Abuse_Func
P.TOE_Auth	O.Auth
	OE.TOE_Auth
P.Identification	O.Identification
P.Configure	O.Configure
A.Keys	OE.Keys
A.Process	OE.Process

The explanation showing that the chosen security objectives are sufficient and suitable to address the identified threats, assumptions, and policies is described in section 4.3 of [PTPP].

The following table maps all security objectives defined in the Protection Profile [PTPP] to the relevant threats, policies, and assumptions. This illustrates that each security objective covers at least one threat, policy or assumption.

Table 7: Security Objectives versus Assumptions, Threats or Policies

Objectives	Assumptions, threats or policies
O.Hardware_Attack	T.Hardware_Attack
O.AC	T.Logical_Attack
O.Auth	P.TOE_Auth
O.Configure	P.Configure
O.Comm_Attack	T.Comm_Attack
O.Abuse_Func	T.Abuse_Func
O.Identification	P.Identification
OE.TOE_Auth	P.TOE_Auth
OE.Keys	A.Keys
OE.Process	A.Process

5 Extended Component Definitions

This Security Target does not define extended components in addition to the components defined in the Protection Profile [PTPP].

Chapter 5 of the Protection Profile [PTPP] defines extended SFRs listed below, which are included in this Security Target.

- FDP_SDC.1 Stored data confidentiality
- FMT_LIM.1 Limited capabilities
- FMT_LIM.2 Limited availability
- FAU_SAS.1 Audit storage

6 IT Security Requirements

IT security requirements include the following:

- Security functional requirements (SFRs)
  That is, requirements for security functions such as information flow control, identification and authentication.
- Security assurance requirements (SARs)
  Provide grounds for confidence that the TOE meets its security objectives (such as configuration management, testing, vulnerability assessment.)
- This chapter discusses these requirements in detail. It also explains the rationales behind them, as follows:
  - Security functional requirements rationale
  - Security assurance requirements rationale

6.1 Security Functional Requirements

The Security Objectives result in a set of Security Functional Requirements (SFRs).

This section describes the SFRs which are defined in the Protection Profile [PTPP].

About the notation used for Security Functional Requirements (SFRs):

- The refinement operation is used in many cases, to make the requirements easier to read and understand. All these cases are indicated and explained in footnotes.
- Selections are denoted as underlined text.
- Assignments are denoted as **underlined text and bold**.

FDP_SDC.1 Stored data confidentiality

FDP_SDC.1.1 The TSF shall ensure the confidentiality of the information of the user data while it is stored in the **memory areas protected by an access control system in the EEPROM**.

FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for **bit corruption on** all objects, based on the following attributes: **data integrity checksum**.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall **return an error code**.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **physical manipulation and physical probing** to the **hardware of the TOE and software composing the TSF** by responding automatically such that the SFRs are always enforced.

Refinement: The TSF will implement appropriate mechanisms to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that security functional requirements are enforced. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1 The TSF shall enforce the **Data Processing Policy** to prevent the disclosure of user data when it is transmitted between physically-separated parts of the TOE.

Refinement: The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically-separated parts of the TOE.

FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE.

Refinement: The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE.

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **Data Processing Policy** on **all confidential data when they are processed or transferred by the TOE**.

The following Security Function Policy (SFP) Data Processing Policy is defined for the requirement "Subset information flow control (FDP_IFC.1)" and “Basic internal transfer protection (FDP_ITT.1)”:

"User data of the TOE and TSF data shall not be accessible from the TOE except when FeliCa OS decides to communicate the user data of the TOE via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by FeliCa OS."

FRU_FLT.2 Limited fault tolerance

FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE’s capabilities when the following failures occur: **exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1)**.

Refinement: The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: **exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur**.

Refinement: The term "failure" above also covers "circumstances". The TOE prevents failures for the "circumstances" defined above.

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **Secure_read, Secure_write, management of security attribute**.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **User and Administrator**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow **Polling, Public_read, Public_write and Requests[3], Echo Back[4], Reset Mode[5]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **Polling, Public_read, Public_write and Requests[3], Echo Back[4], Reset Mode[5]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to **Mutual authentication between the TOE and the external entity**.

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **Service Access Policy** on:

- **Subjects: subjects shown in Table 8**
- **Objects: objects shown in Table 8**
- **Operations: operations shown in Table 8**

[3] Requests are operations to retrieve a configure, status or version information from the TOE that are not required authentication.

[4] Echo Back is an operation to perform the communication test that does not required authentication.

[5] Reset Mode is an operation to reset authentication status to “Not authenticated”.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Service Access Policy** to objects based on:

- **Subjects: subjects shown in Table 8**
- **Objects: objects shown in Table 8**
- **SFP relevant security attributes for each subject and object: security attribute authentication status and security attribute ACL shown in Table 8**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **A Subject can do this operation on an Object when: the Subject is successfully authenticated, and the operation is listed in the Object's ACL.**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

Table 8: Service Access Policy

FMT_MSA.1 Management of security attributes

Subject	Security attribute Authentication status	Object	Security attribute ACL	Operation
Process representing User	Not authenticated	User data file	Read only, Authentication not required	Read
			Read/Write, Authentication not required	Read or Write
	Successfully authenticated with the Access Key corresponding to the Service	User data file	Read only, Authentication with the Access Key corresponding to the Service required	Read
			Read/Write, Authentication with the Access Key corresponding to the Service required	Read or Write

FMT_MSA.1.1 The TSF shall enforce the **Service Access Policy** to restrict the ability to set and none the security attributes **ACL** to **Administrator**.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **management of security attributes**.

FMT_LIM.1 Limited capabilities

FMT_LIM.1.1 The TSF shall be designed and implemented in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: **Deploying Test Features after TOE Delivery does not allow user data of the TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks**.

FMT_LIM.2 Limited availability

FMT_LIM.2.1 The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: **Deploying Test Features after TOE Delivery does not allow user data of the TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks**.

FAU_SAS.1 Audit storage

FAU_SAS.1.1 The TSF shall provide **the test process before TOE Delivery** with the capability to store **Initialisation Data and none** in the **EEPROM**.

6.2 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are those taken from the Evaluation Assurance Level 5 (EAL5) and augmented by taking the components ALC_DVS.2 and AVA_VAN.5. The assurance requirements are shown in the following table.

Table 9: Assurance components

Assurance class	Assurance components
Development	ADV_ARC.1
	ADV_FSP.5
	ADV_IMP.1
	ADV_INT.2
	ADV_TDS.4
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle support	ALC_CMC.4
	ALC_CMS.5
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.2
Security Target evaluation	ASE_CCL.1

Assurance class	Assurance components
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Tests	ATE_COV.2
	ATE_DPT.3
	ATE_FUN.1
	ATE_IND.2
Vulnerability assessment	AVA_VAN.5

6.3 Security Functional Requirements Rationale

Regarding the Security Objectives defined in the Protection Profile [PTPP], the section 6.3 of the PP provides both the rationale for choosing specific Security Functional Requirements (SFRs) and how those requirements correspond to the specific Security Objectives. The following table gives an overview, how the SFRs are combined to meet the Security Objectives.

Table 10: TOE Security Functional Requirements versus Security Objectives

Objective	TOE Security Functional Requirements	
O.Hardware_Attack	FDP_SDC.1	"Stored data confidentiality"
	FDP_SDI.2	"Stored data integrity monitoring and action"
	FPT_PHP.3	"Resistance to physical attack"
	FDP_ITT.1	"Basic internal transfer protection"
	FPT_ITT.1	"Basic internal TSF data transfer protection"
	FDP_IFC.1	"Subset information flow control"
	FRU_FLT.2	"Limited fault tolerance"
	FPT_FLS.1	"Failure with preservation of secure state"
O.AC	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"
O.Auth	FIA_UID.1	"Timing of identification"
	FIA_UAU.1	"Timing of authentication"
	FIA_UAU.4	"Single-use authentication mechanisms"

Objective	TOE Security Functional Requirements	
	FTP_ITC.1	"Inter-TSF trusted channel"
O.Configure	FMT_SMR.1	"Security roles"
	FMT_MSA.1	"Management of security attributes"
	FMT_SMF.1	"Specification of Management Functions"
O.Comm_Attack	FTP_ITC.1	"Inter-TSF trusted channel"
O.Abuse_Func	FMT_LIM.1	"Limited capabilities"
	FMT_LIM.2	"Limited availability"
O.Identification	FAU_SAS.1	"Audit storage"

The dependencies of SFRs defined in Protection Profile [PTPP] are listed in section 6.3 in the PP. The following table presents the list of the SFRs with the associated dependencies and how they are satisfied.

Table 11: Security Functional Requirements dependencies

ID	SFR	Dependencies	Notes
FDP_SDC.1	Stored data confidentiality	None	
FDP_SDI.2	Stored data integrity monitoring and action	None	
FPT_PHP.3	Resistance to physical attack	None	
FDP_ITT.1	Basic internal transfer protection	FDP_ACC.1 or FDP_IFC.1	Included (FDP_IFC.1)
FPT_ITT.1	Basic internal TSF data transfer protection	None	
FDP_IFC.1	Subset information flow control	FDP_IFF.1	Not satisfied (See discussion below)
FRU_FLT.2	Limited fault tolerance	FPT_FLS.1	Included
FPT_FLS.1	Failure with preservation of secure state	None	
FMT_SMR.1	Security roles	FIA_UID.1	Included
FIA_UID.1	Timing of identification	None	
FIA_UAU.1	Timing of authentication	FIA_UID.1	Included
FIA_UAU.4	Single-use authentication mechanisms	None	
FDP_ACC.1	Subset access control	FDP_ACF.1	Included
FDP_ACF.1	Security attribute based access control	FDP_ACC.1	Included
		FMT_MSA.3	Not satisfied (See discussion below)
FMT_MSA.1		FDP_ACC.1 or FDP_IFC.1	Included (FDP_ACC.1)

ID	SFR	Dependencies	Notes
	Management of security attributes	FMT_SMR.1	Included
		FMT_SMF.1	Included
FMT_SMF.1	Specification of Management Functions	None	
FTP_ITC.1	Inter-TSF trusted channel	None	
FMT_LIM.1	Limited capabilities	FMT_LIM.2	Included
FMT_LIM.2	Limited availability	FMT_LIM.1	Included
FAU_SAS.1	Audit storage	None	

The rationale of the dependency of FDP_IFC.1 (Subset information flow control) on FDP_IFF.1 (Simple security attributes) is described in section 6.3 of [PTPP].

The rationale of the dependency of FMT_MSA.3 (Static attribute initialisation) on FDP_ACF.1 (Security attribute based access control) is described in section 6.3 of [PTPP].

6.4 Security Assurance Requirements Rationale

To meet the assurance expectations of Public Transportation Operators, the assurance level EAL5 and the augmentation with the requirements ALC_DVS.2 and AVA_VAN.5 are chosen. The assurance level of EAL5 and the augmentation with the requirements ALC_DVS.2 and AVA_VAN.5 is selected because it provides a sufficient level of assurance for this type of TOE, which is expected to be not only highly resistant for protecting high value assets but also highly reliable as a part of public transportation system, which is an important infrastructure. Explanation of the security assurance component ALC_DVS.2 and AVA_VAN.5 follows:

- ALC_DVS.2 Sufficiency of security measures:

  This Protection Profile selects ALC_DVS.2 instead of ALC_DVS.1 because it verifies the security measures that provide the necessary level of protection to maintain the confidentiality and integrity of the TOE and its assets.

- AVA_VAN.5 Advanced methodical vulnerability analysis:

  The TOE might be in danger of high-level attacks such as those it might encounter in malicious laboratories. Therefore, AVA_VAN.5 is augmented to confirm that TOE has a high level of resistance against such attacks.

The dependencies of SARs added to EAL5 are described in [CC Part 3]. The following table gives their dependencies and how they are satisfied.

Table 12: Security Assurance Requirements dependencies added to EAL5

ID	SFR	Dependencies	Notes
ALC_DVS.2	Sufficiency of security measures	None	
AVA_VAN.5	Advanced methodical vulnerability analysis	ADV_ARC.1	Dependencies are covered by the assurance
		ADV_FSP.4	

ID	SFR	Dependencies	Notes
		ADV_TDS.3	components of EAL5 (ADV_ARC.1, ADV_FSP.5, ADV_TDS.4, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1 and ATE_DPT.3).
		ADV_IMP.1	
		AGD_OPE.1	
		AGD_PRE.1	
		ATE_DPT.1	

7 TOE Summary Specification

This chapter describes the TOE summary specification by summarising the architectural design.

The TOE summary specification includes the following:

- TOE summary specification rationale
  describes how the TOE meets each SFR.

7.1 TOE Summary Specification Rationale

This section describes how the TOE is intended to comply with the Security Functional Requirements.

- "FMT_SMR.1 Security roles" is met by providing an ability to distinguish between the roles of "Administrator" and "User", where the different roles allow to execute different kinds of operations. The Administrator of the TOE specifies the security attributes for Service.
- "FIA_UID.1 Timing of identification" and "FIA_UAU.1 Timing of authentication" are achieved by mutual authentication to access the restricted user data file. In addition, the TOE provides a possibility to configure a publically-accessible user data file before authentication. The TOE provides access to such specifically-configured user data file based on the security attributes of Service. The Service shall be configured, by the Administrator, to allow the specified mode of access before authentication.
- "FIA_UAU.4 Single-use authentication mechanisms" and "FTP_ITC.1 Inter-TSF trusted channel" are achieved by mutual authentication between the TOE and the external entity according to the specification of "Security Reference Manual – Mutual Authentication & Secure Communication". The TOE uses random numbers in the authentication mechanism to comply with the "FIA_UAU.4 Single-use authentication mechanisms" requirement. The random numbers are generated anew each time the authentication is started, and are discarded each time the TOE exits the authenticated state.
- "FDP_ACC.1 Subset access control" and "FDP_ACF.1 Security attribute based access control" are satisfied by providing an access control system based on security attributes of the Service. 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 the TOE shall authenticate each other by using Access Key that corresponds to the Service. When the authentication is successfully completed, the TOE allows the external entity to access the user data according to the Service Attribute. The security attributes are assigned to Services by the Administrator. The TOE allows the Administrator to access the security attributes for configuration purposes, based on the security attributes (in accordance with FMT_MSA.1 and FMT_SMR.1).
- "FMT_MSA.1 Management of security attributes" and "FMT_SMF.1 Specification of Management Functions" are met by providing configuration capabilities accessible to the Administrator. The configuration capabilities are granted based on the security attributes and allow the setting of these security attributes.
- "FDP_SDI.2 Stored data integrity monitoring and action" is satisfied through the monitoring of the user data for bit integrity errors. The TOE uses a cyclic redundancy check (CRC) based on CRC-16-CCITT to verify the correctness of the stored data at each start-up and at each access. If an error is detected, the TOE takes the appropriate action to ensure the security of the data.

- "FTP_ITC.1 Inter-TSF trusted channel" requires the secure channel to be protected against attackers with High attack potential – this is provided by the TOE using AES, which are calculated by the IC and IC Dedicated Software of the TOE, for encrypting and authenticating data that is sent or received through the secure channel.
- "FRU_FLT.2 Limited fault tolerance" and "FPT_FLS.1 Failure with preservation of secure state" are satisfied by a group of security measures that guarantee correct operation of the TOE.
  The TOE ensures its correct operation and prevents any malfunction while the Security IC Embedded Software is executed and utilizes standard functions offered by the micro-controller (standard CPU instruction set including usage of standard peripherals such as memories, registers, I/O interfaces, timers etc.) and of all other specific security functionality.
  This is achieved through an appropriate design of the TOE and the implementation of filters for high-frequency pulse, sensors/detectors for supplied voltage, frequency, temperature, light and glitch signal, and address area monitoring and integrity monitoring. In case that any malfunction occurred or may likely occur, the TOE stops operation or triggers system reset to preserve a secure state.
- "FDP_ITT.1 Basic internal transfer protection", "FDP_IFC.1 Subset information flow control" and "FPT_ITT.1 Basic internal TSF data transfer protection" are satisfied by implementing several measures that provide logical protection against leakage. The TOE ensures the prevention of the disclosure of the user data or TSF data through the measurement of the power consumption, electromagnetic emission or calculation time, and subsequent signal processing. This is achieved through the measures to eliminate/limit the secret information contained in power consumption, electromagnetic emission or calculation time, and small-space implementation by advanced CMOS process, and variable timing noise to randomly delay the critical operation.
- "FPT_PHP.3 Resistance to physical attack" and "FDP_SDC.1 Stored data confidentiality" are satisfied by implementing security measures that provides physical protection against physical probing and manipulation. The protection of the TOE is achieved through measures which comprise passive/active shield, specific encryption for the memory blocks, data scrambling between the blocks, glue logic layout of multiple blocks, sensor signal monitoring and address area monitoring. If the physical manipulation or physical probing attack is detected, the TOE stops operation.
- "FMT_LIM.1 Limited capabilities" and "FMT_LIM.2 Limited availability" are satisfied by implementing of a complicated test mode control mechanism that prevents abuse of test functionality delivered as a part of the TOE. The test functionality is not available to the user after "Phase 3 IC Manufacturing" as described in section 1.3.
- "FAU_SAS.1 Audit storage" is satisfied by the test process before TOE Delivery that stores the unique identification data to EEPROM.

8 Glossary and References

This chapter explains the terms, definitions and literary references (bibliography) used in this document. The list entries in this chapter are ordered alphabetically.

8.1 Terms and Definitions

The following list defines the product-specific terms used in this document:

Administrator

An entity responsible for personalisation of the TOE.

Access Key

A key that corresponds to an Area and a Service.

Area

A part of the file system. An Area is similar to a directory in a general file system.

Card reader

A contactless and an optional contact smartcard Reader/Writer that interacts with the TOE.

IC Dedicated Software

IC proprietary software embedded in a security integrated circuit and developed by the IC developer. Such software is required for testing purpose but may provide additional services to facilitate usage of the hardware and to provide additional services.

Initialisation Data

Initialisation Data defined by the IC manufacturer to identify the TOE and to keep track of the IC’s production and further life-cycle phases are considered as belonging to the TSF data.

Passenger

A person who uses Ticket Service.

Pre-personalisation Data

Any data supplied by the PT Software developer that is injected into the non-volatile memory by the IC manufacturer or the IC packaging manufacturer.

PT Software

An embedded software that provides the public transportation application and the operating system.

Public Transportation Operator

An entity that provides a specific service to a Passenger.

Service

The part of the file system that contains information that stipulates the method of access to data. In this context, a Service is similar to a file in a general file system.

Service Attribute

An attribute that defines the type of access to the user data and the security condition to access the user data via Service.

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.

User

An entity using any Service and Area that a personalised TOE offers. A ticket gate is a representative example of User. See also Administrator.

8.2 Acronyms

The following table lists and defines the product-specific abbreviated terms (acronyms) that appear in this document:

Table 13: Abbreviated terms and definitions

Term	Definition
ACL	Access Control List
CC	Common Criteria
OS	Operating System
PP	Protection Profile
RF	Radio Frequency
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

8.3 Bibliography

The following list defines the literature referenced in this document:

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

[CC] "Common Criteria for Information Technology Security Evaluation", Version 3.1 (composed of Parts1-3, [CC Part 1], [CC Part 2], and [CC Part 3])

[CC Part 1] "Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model", Version 3.1, Revision 5, April 2017

[CC Part 2] "Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components", Version 3.1, Revision 5, April 2017

[CC Part 3] "Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components", Version 3.1, Revision 5, April 2017

[CC CEM] "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1, Revision 5, April 2017

[ISO 18092] "Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)"

[PTPP] "Public Transportation IC Card Protection Profile", Version 1.12, 1 August 2018

Contactless Smart Card IC

Security Target JREM 6K Contactless Smart Card IC chip with fast processing function for transport Version 2.0

November 2019 First Edition FeliCa Business Division

Sony Imaging Products & Solutions Inc.

No. J6K-STP-E02-00