SONY

Contactless Smartcard IC

Security Target

RC-SA20, RC-SA21 and RC-SA24 Series

Version 1.02

Public Version

No. SA2-STP-E01-02

Introduction

This document is the Security Target for CC evaluation of IC chip product "RC-SA20, RC-SA21 and RC-SA24 Series".

Contents

1 Introducing the Security Target

This document is the Security Target for CC evaluation of IC chip product RC-SA20, RC-SA21 and RC-SA24 Series.

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, RC-SA20, RC-SA21 and RC-SA24 Series.

Table 1: ST identification

ST attribute	Value
Name	Security Target RC-SA20, RC-SA21 and RC-SA24 Series
Version	1.02
Reference	SA2-STP-E01-02
Issue Date	June 2020

Table 2: TOE identification

TOE attribute	Value
Name	RC-SA20, RC-SA21 and RC-SA24 Series
Version	1.00
Product type	Contactless Smartcard IC
Form Factor	Bare chip with bump on sawn wafer Bare chip without bump on sawn wafer

1.2 TOE Overview

The TOE is an integrated circuit with a contactless interface and a smartcard embedded software called "FeliCa OS". The TOE is used as a public transportation IC card, an e-money card, an identification card and so on.

The integrated circuit is the Fujitsu Semiconductor Limited (hereinafter referred to as "Fujitsu") chip CXD90056 and FeliCa OS is the FeliCa Operating System developed by Sony Imaging Products & Solutions Inc. (hereinafter referred to as "Sony") including the application for services of the Service Provider.

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].

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

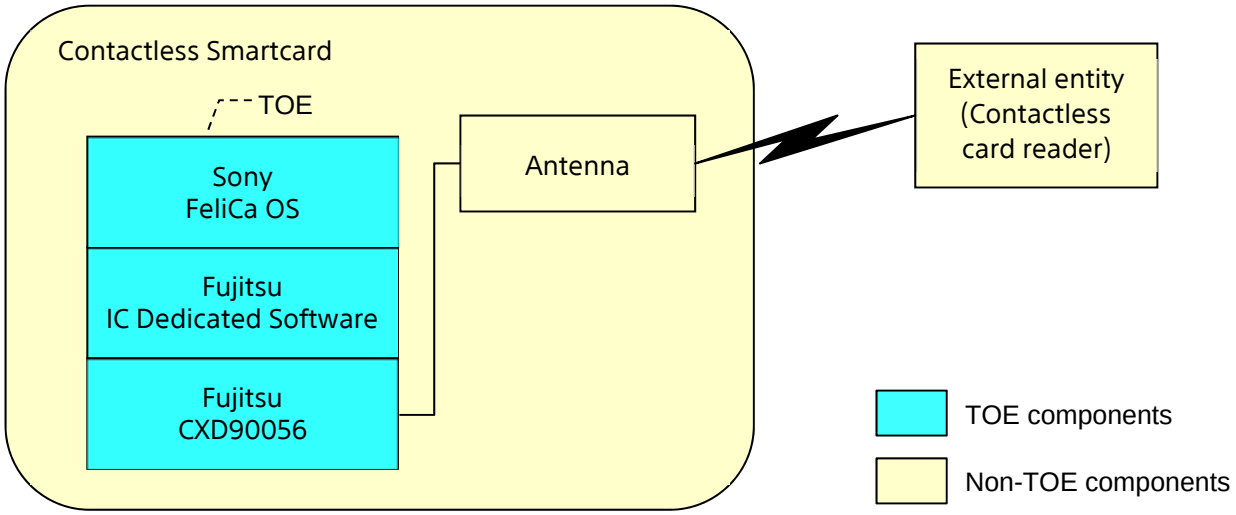

Figure 1: TOE physical scope

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 FeliCa application and the operating system that is responsible for managing and providing access to file systems.
- "IC Dedicated Software" is the IC proprietary software that controls and restricts access from the FeliCa OS to the Fujitsu hardware platform. It is also used for testing purposes during production.
- "Fujitsu CXD90056" is a security integrated circuit which is composed of a 32-bit architecture processing unit, cryptographic co-processor which supports AES and DES[1] operation, security components (e.g., security detectors, sensors and circuitry to protect the TOE), a contactless interface, and ROM, RAM and FRAM memory.

1.2.1 File system

FeliCa OS manages three file systems, FeliCa standard file system, FeliCa Lite-S file system and Secure ID file system. The external entity specifies the system number to access the file system.

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

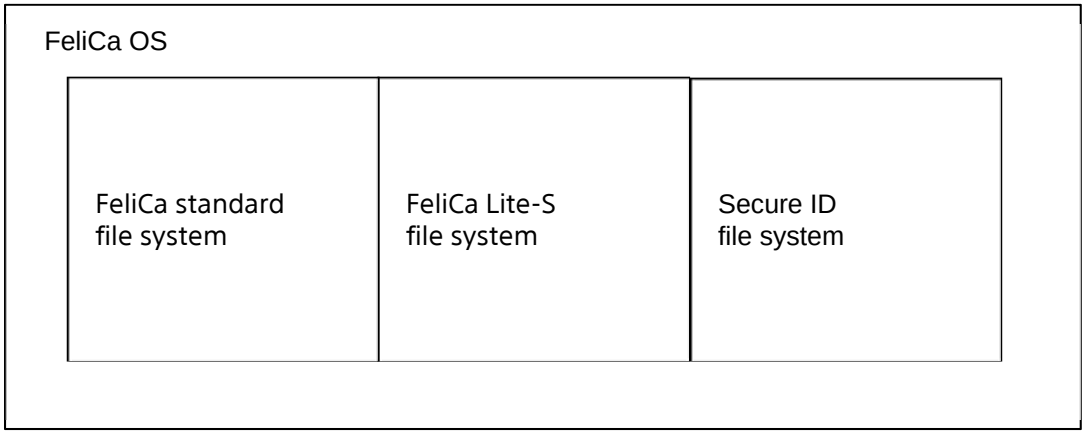

Figure 2: The structure of the file system

The TOE does not claim any asset in FeliCa Lite-S file system and does not implement any Security Functional Requirement to access FeliCa Lite-S file system. Therefore, FeliCa Lite-S file System is not part of the evaluation.

1.2.1.1 FeliCa standard file system

The TOE manages several data sets, each having a different purpose, on a single TOE. The TOE has FeliCa standard file system consisting of Areas and Services, which organise files in a tree structure (as shown in Figure 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, integrity and both 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.

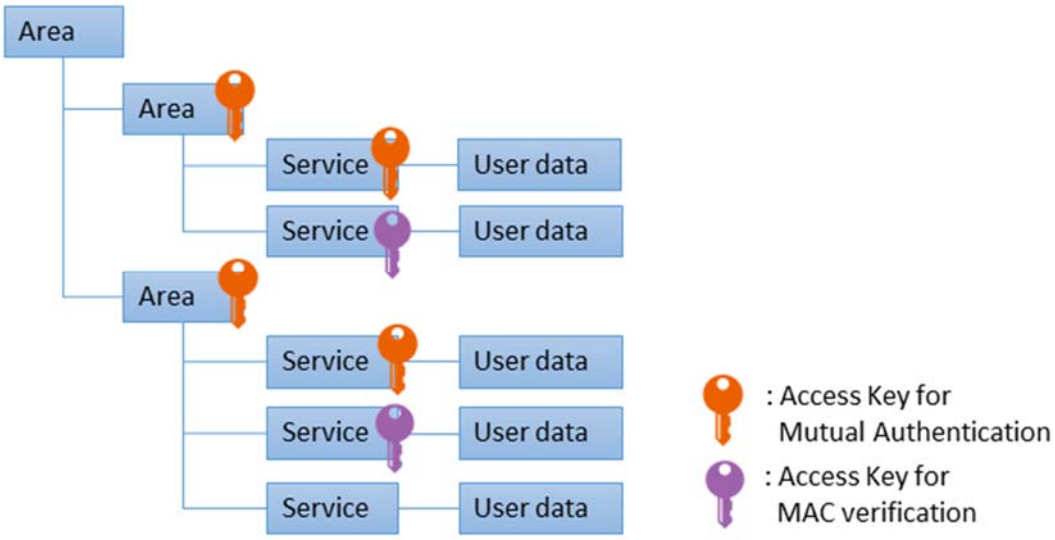

Figure 3: The FeliCa standard file system

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
Successfully MAC verification with Access Key corresponding to the Service	Write Access: MAC verification required	Write

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).

1.2.1.2 Secure ID file system

The TOE has Secure ID file system that stores user data in Blocks. Each Block has the access control policy called "Secure ID System Policy" described in Table 4. When Secure ID authentication is successfully completed, the external entity can write user data stored in Block that writing is not prohibited. The external entity can read user data stored in Block that reading is not prohibited without authentication.

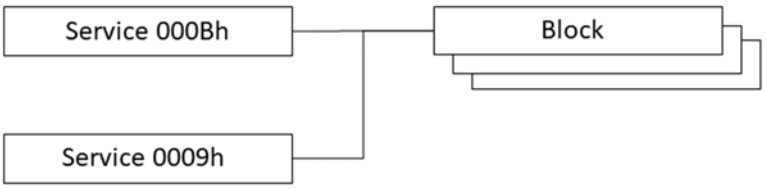

Figure 4: Secure ID file system

Table 4: Secure ID System Policy

Block Number	Block Name	Read access	Write access
C0h	RC_A	Reading prohibited	Authentication not required
C1h	RC_B	Authentication not required	Writing prohibited
C2h	MAC_B	Authentication not required	Writing prohibited
C3h	ID_S	Authentication not required	Authentication required
C4h	CK_A	Reading prohibited	Authentication required
C5h	MC_A	Authentication not required	Authentication required
C8h	DATA	Authentication not required	Authentication required

1.2.1.3 FeliCa Lite-S file system

FeliCa Lite-S file system consists of streamlined security function and an optimized file system. FeliCa Lite-S can be used for any NFC Forum Type 3 Tag solution, such as handover connection and smart poster. The TOE does not claim any asset in FeliCa Lite-S file system and does not implement any Security Functional Requirement to access FeliCa Lite-S file system. Therefore, FeliCa Lite-S file System is not part of the evaluation.

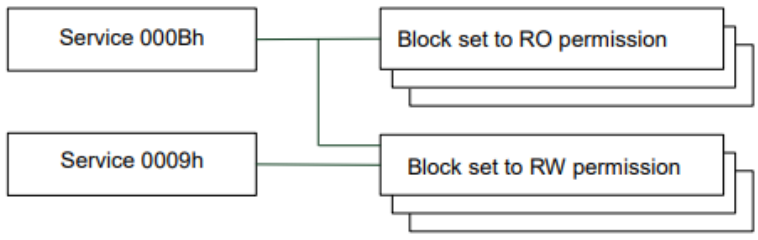

Figure 5: Conceptual Diagram of FeliCa Lite-S file system

1.2.2 TOE security features

The TOE has several self-protection mechanisms sufficient to satisfy all requirements for self-protection, non-bypassability, and domain separation as described by the CC supporting documents for the smartcard security evaluations [AAPS].

The TOE offers the following features:

- it can receive FeliCa commands from the card reader
- it can send FeliCa responses to the card reader

The TOE offers the following security features:

- mutual authentication between the external entity and the TOE
- authentication proof of the identity of the TOE to an external entity
- 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 5: Phases of the 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

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 Fujitsu.

Phase 2: IC development (IC design and IC Dedicated Software development) is performed by Fujitsu.

Phase 3: IC manufacturing (integration and photomask fabrication, IC production, IC testing, initialisation including injection of Initialisation Data, and Pre-personalisation) is performed by Fujitsu.

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 FeliCa IC card product and then delivers that product to the Administrator (e.g., the service provider).

Phase 6: The Administrator (e.g., the service provider) performs the personalisation where the user data, the Service Attribute and the Access Keys are loaded into the TOE memory.

Phase 7: The FeliCa IC card product is delivered to a card holder for operational use.

1.4 Delivery

The TOE delivery items are listed in the following table:

Table 6: TOE delivery items

Delivery item type	Identifier	Version	Medium
Hardware	Fujitsu CXD90056 Smartcard IC – Hardware	20 00	Smartcard integrated circuit
Software	Fujitsu CXD90056 Smartcard IC – IC Dedicated Software	0B 00	Embedded in hardware
	FeliCa Operating System 5.0	DF 0D	Embedded in hardware
Manuals	FeliCa Card User's Manual	1.20	PDF or Paper
	RC-SA20 Series Inspection Procedure	1.00	PDF or Paper
	RC-SA20 Series Inspection and IDm Writing Procedure	1.00	PDF or Paper
	RC-SA21 Series Inspection Procedure	1.00	PDF or Paper
	RC-SA21 Series Inspection and IDm Writing Procedure	1.00	PDF or Paper
	RC-SA24 Series Inspection Procedure	1.00	PDF or Paper
	RC-SA24 Series Inspection and IDm Writing Procedure	1.00	PDF or Paper
	Secure ID User's Manual	0.90	PDF or Paper
	RC-SA20, RC-SA21, RC-SA24 Series Secure ID Inspection Procedure	0.90	PDF or Paper
	Product Acceptance Procedure	1.0	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
	Security Reference Manual – Group Key Generation for Communication with MAC (AES 128bit)	1.00	PDF or Paper
	Security Reference Manual – Communication with MAC (AES 128bit)	1.00	PDF or Paper
	Security Reference Manual – Secure ID	1.00	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.

The service providers are required to prepare card readers depending on their purposes.

1.6 Evaluated derivative products

The TOE comprises the group of derivatives, which can be clearly identified by different product type names.

The Table 7 shows the product type names which are subject of the evaluation. The "x" of the product name indicates its product form, whose definitions are listed in Table 8.

Table 7: Product name comprising the group of derivatives

Product name	IC Code	Specifications
RC-SA20/1x RC-SA20/3x	4401	Supports both Advanced-operation mode and Backward-Compatible operation mode, 6KB FRAM, Parasitic input capacitance.
RC-SA20/2x RC-SA20/4x	4501	Supports both Advanced-operation mode and Backward-Compatible operation mode, 6KB FRAM, 50pF input capacitance.
RC-SA21/2x	4601	Supports Advanced-operation mode, 4KB FRAM, 50 pF input capacitance.
RC-SA21/2x1	4801	Supports Advanced-operation mode, 6KB FRAM, 50 pF input capacitance.
RC-SA24/1x RC-SA24/3x	4301	Supports both Advanced-operation mode and Backward-Compatible operation mode, 10KB FRAM, Parasitic input capacitance.
RC-SA24/1x1 RC-SA24/3x1	4701	Supports both Advanced-operation mode and Backward-Compatible operation mode, 6KB FRAM, Parasitic input capacitance.

Table 8: Product form definitions

Form name	Descriptions
A	Bare chip with bump on sawn wafer
C	Bare chip without bump on sawn wafer

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

This Security Target claims conformance to assurance package:

- Evaluation Assurance Level 6 (EAL6) augmented with ASE_TSS.2

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

Since this Security Target claims conformance to the Protection Profile [PTPP], the threats defined in section 3.2 of the Protection Profile are applied for this Security Target. The threats of the Protection Profile are listed below.

- T.Hardware_Attack
- T.Logical_Attack
- T.Comm_Attack
- T.Abuse_Func

No additional threat is defined in this Security Target.

3.3 Organisational Security Policies

Since this Security Target claims conformance to the Protection Profile [PTPP], the organisational security policies defined in section 3.3 of the Protection Profile are applied for this Security Target. The organisational security policies of the Protection Profile are listed below.

- P.Configure
- P.Identification
- P.TOE_Auth

This security target adds the following organisational security policy.

P. SecureID_System

TOE shall prove the identity of the TOE to an external entity and prevent unauthorised writing of the user data.

3.4 Assumptions

Since this Security Target claims conformance to the Protection Profile [PTPP], the assumptions defined in section 3.4 of the Protection Profile are applied for this Security Target. The assumptions of the Protection Profile are listed below.

- A.Process
- A.Keys

No additional assumption is defined in this Security Target.

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

Since this Security Target claims conformance to the Protection Profile [PTPP], the TOE security objectives defined in section 4.1 of the Protection Profile are applied for this Security Target. The TOE security objectives of the Protection Profile are listed below.

- O.Hardware_Attack
- O.AC
- O.Auth
- O.Configure
- O.Comm_Attack
- O.Abuse_Func
- O.Identification

This security target adds the following TOE security objective.

O. SecureID_System

The TOE shall provide the means of the proof of the identity of the TOE to an external entity and prevent unauthorised writing of the user data.

4.2 TOE Operational Environment Security Objectives

Since this Security Target claims conformance to the Protection Profile [PTPP], the TOE operational environment security objectives defined in section 4.2 of the Protection Profile are applied for this Security Target. The TOE operational environment security objectives of the Protection Profile are listed below.

- OE.TOE_Auth
- OE.Keys
- OE.Process

No additional TOE operational environment security objective is defined in this Security Target.

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 9: Assumptions, Threats or Policies versus Security Objectives

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

The O.Secure ID_System objective provides the means of the proof of the identity of the TOE to an external entity and prevention of unauthorised writing of the user data. Thus, the P.Secure_ID_System policy is covered by the objective.

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 10: 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.SecureID_System	P.SecureID_System
O.Configure	P.Configure

Objectives	Assumptions, threats or policies
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 Components 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:
  - o Security functional requirements rationale
  - o 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 FRAM**.

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**.

Application note: The following Security Function Policy (SFP) Data Processing Policy is defined for the requirement "Subset information flow control (FDP_IFC.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 [2], Secure_write[3], 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[4], Echo Back[5], Reset Mode[6]** 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[4], Echo Back[5], Reset Mode[6]** 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 **the authentication mechanisms shown in Table 11**.

---

[2] Secure_read is a read operation to the user data files that require authentication with the Access Key corresponding to the Service.

[3] Secure_write is a write operation to the user data files that require authentication with the Access Key corresponding to the Service.

[4] Requests is an operation to retrieve a configure, status or version information from the TOE that does not required authentication.

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

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

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide **the list of multiple authentication mechanisms shown in Table 11** to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to **the rules describing how the multiple authentication mechanisms provide authentication shown in Table 11.**

Table 11: List of Multiple authentication mechanisms

Authentication mechanism	Rules
Mutual authentication (AES)	If a Service requires authentication, the external entity and the TOE shall authenticate each other by using Access Key that corresponds to the Service.
Mutual authentication (CMAC)	If a Service requires MAC verification, the external entity and the TOE shall authenticate each other by using MAC verification by using Access Key that corresponds to the Service
Secure ID authentication	If the external entity requests to write user data to Block in Secure ID file system, the external entity and the TOE shall authenticate each other by using MAC verification with CK_A.

FDP_ACC.1a Subset access control

FDP_ACC.1.1a The TSF shall enforce the **Service Access Policy 1** on:

- **Subjects: subjects shown in Table 12**
- **Objects: objects shown in Table 12**
- **Operations: operations shown in Table 12**

FDP_ACF.1a Security attribute based access control

FDP_ACF.1.1a The TSF shall enforce the **Service Access Policy 1** to objects based on:

- **Subjects: subjects shown in Table 12**
- **Objects: objects shown in Table 12**
- **SFP relevant security attributes for each subject and object: security attribute authentication status and security attribute ACL shown in Table 12**

FDP_ACF.1.2a 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.1.3a The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

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

Table 12: Service Access Policy 1

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

FDP_ACC.1b Subset access control

FDP_ACC.1.1b The TSF shall enforce the **Service Access Policy 2** on:

- **Subjects: subjects shown in Table 13**
- **Objects: objects shown in Table 13**
- **Operations: operations shown in Table 13**

FDP_ACF.1b Security attribute based access control

FDP_ACF.1.1b The TSF shall enforce the **Service Access Policy 2** to objects based on:

- **Subjects: subjects shown in Table 13**
- **Objects: objects shown in Table 13**
- **SFP relevant security attributes for each subject and object: security attribute authentication status and security attribute ACL shown in Table 13**

FDP_ACF.1.2b 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.1.3b The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

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

Table 13: Service Access Policy 2

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 MAC verification with the Access Key corresponding to the Service	User data file	Write, MAC verification with the Access Key corresponding to the Service required	Write

FDP_ACC.1/SecureID Subset access control

FDP_ACC.1.1/SecureID The TSF shall enforce the **Secure ID System Policy** on:

- **Subjects: subjects shown in Table 14**
- **Objects: objects shown in Table 14**
- **Operations: operations shown Table 14**

FDP_ACF.1/SecureID Security attribute based access control

FDP_ACF.1.1/SecureID The TSF shall enforce the **Secure ID System Policy** to objects based on:

- **Subjects: subjects shown in Table 14**
- **Objects: objects shown in Table 14**
- **SFP relevant security attributes for each subject and object: security attribute authentication status and security attribute ACL shown in Table 14**

FDP_ACF.1.2/SecureID 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/SecureID The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

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

Table 14: Secure ID System Policy

Subject	Security attribute Authentication status	Object	Security attribute ACL	Operation
	Not authenticated	RC_B MAC_B	Read,	Read

Process representing User		ID_S MC_A DATA	Authentication not required	
	Any status	RC_A CK_A	Read, prohibited	none
		RC_B	Write, prohibited	none
	Successfully MAC verification with CK_A	RC_A MAC_B ID_S CK_A MC_A DATA	Write, MAC verification with CK_A	Write

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **Service Access Policy 1** 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 **FRAM**.

6.2 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are those taken from the Evaluation Assurance Level 6 (EAL6) and augmented by taking the component ASE_TSS.2. The assurance requirements are shown in the following table.

Table 15: Assurance components

Assurance class	Assurance components
Development	ADV_ARC.1
	ADV_FSP.5
	ADV_IMP.2
	ADV_INT.3
	ADV_SPM.1
	ADV_TDS.5
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle support	ALC_CMC.5
	ALC_CMS.5
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.3
Security Target evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.2
Tests	ATE_COV.3
	ATE_DPT.3
	ATE_FUN.2
	ATE_IND.2
Vulnerability assessment	AVA_VAN.5

Among the set of assurance components chosen for EAL6, the assignment appears only in ADV_SPM.1. The assignment used in ADV_SPM.1 is defined as follows:

ADV_SPM.1 Formal TOE security policy model

ADV_SPM.1.1D The developer shall provide a formal security policy model for the **Service Access Policy 1**.

ADV_SPM.1.2D For each policy covered by the formal security policy model, the model shall identify the relevant portions of the statement of SFRs that make up that policy.

ADV_SPM.1.3D The developer shall provide a formal proof of correspondence between the model and any formal functional specification.

ADV_SPM.1.4D The developer shall provide a demonstration of correspondence between the model and the functional specification.

This Security Target claims conformance to the Protection Profile [PTPP]. The differences in the SARs between the Protection Profile and the Security Target are identified in the following table.

Table 16: TOE Security Functional Requirements versus Security Objectives

TOE SARs	SARs chosen in PP	Level difference
ADV_ARC.1	ADV_ARC.1	None
ADV_FSP.5	ADV_FSP.5	None
ADV_IMP.2	ADV_IMP.1	Higher hierarchical component
ADV_INT.3	ADV_INT.2	Higher hierarchical component
ADV_SPM.1	---	Higher hierarchical component
ADV_TDS.5	ADV_TDS.4	Higher hierarchical component
AGD_OPE.1	AGD_OPE.1	None
AGD_PRE.1	AGD_PRE.1	None
ALC_CMC.5	ALC_CMC.4	Higher hierarchical component
ALC_CMS.5	ALC_CMS.5	None
ALC_DEL.1	ALC_DEL.1	None
ALC_DVS.2	ALC_DVS.2	None
ALC_LCD.1	ALC_LCD.1	None
ALC_TAT.3	ALC_TAT.2	Higher hierarchical component
ASE_CCL.1	ASE_CCL.1	None
ASE_ECD.1	ASE_ECD.1	None
ASE_INT.1	ASE_INT.1	None
ASE_OBJ.2	ASE_OBJ.2	None
ASE_REQ.2	ASE_REQ.2	None
ASE_SPD.1	ASE_SPD.1	None
ASE_TSS.2	ASE_TSS.1	Higher hierarchical component
ATE_COV.3	ATE_COV.2	Higher hierarchical component
ATE_DPT.3	ATE_DPT.3	None
ATE_FUN.2	ATE_FUN.1	Higher hierarchical component
ATE_IND.2	ATE_IND.2	None
AVA_VAN.5	AVA_VAN.5	None

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 17: 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"
	FIA_UAU.5	”Multiple authentication mechanisms”
	FDP_ACC.1a	"Subset access control"
	FDP_ACF.1a	"Security attribute based access control"
	FDP_ACC.1b	"Subset access control"
	FDP_ACF.1b	"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"
	FIA_UAU.5	”Multiple authentication mechanisms”
	FTP_ITC.1	"Inter-TSF trusted channel"
O.SecureID_System	FIA_UAU.5	”Multiple authentication mechanisms”
	FDP_ACC.1/SecureID	"Subset access control"
	FDP_ACF.1/SecureID	"Security attribute based access control"
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"

Objective	TOE Security Functional Requirements
O.Identification	FAU_SAS.1 "Audit storage"

The objective O.SecureID_System is achieved by the SFR FIA_UAU.5, FDP_ACC.1/SecureID and FDP_ACF.1/SecureID. The external entity and the TOE authenticate each other by FIA_UAU.5, if authentication is successfully completed, the external entity write user data in accordance with the policy that defined FDP_ACC.1/SecureID and FDP_ACF.1/SecureID.

The dependencies of the other 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 18: 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 [PTPP])
FRU_FLT.2	Limited fault tolerance	FPT_FLS.1	Included
FPT_FLS.1	Failure with preservation of secure state	None	
FTP_ITC.1	Inter-TSF trusted channel	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	
FIA_UAU.5	Multiple authentication mechanisms	None	
FDP_ACC.1a	Subset access control	FDP_ACF.1a	Included
FDP_ACF.1a	Security attribute based access control	FDP_ACC.1a	Included
		FMT_MSA.3	Not satisfied (See [PTPP])
FDP_ACC.1b	Subset access control	FDP_ACF.1b	Included
FDP_ACF.1b		FDP_ACC.1b	Included

ID	SFR	Dependencies	Notes
	Security attribute based access control	FMT_MSA.3	Not satisfied (See [PTPP])
FDP_ACC.1/SecureID	Subset access control	FDP_ACF.1/SecureID	Included
FDP_ACF.1/SecureID	Security attribute based access control	FDP_ACC.1/SecureID	Included
		FMT_MSA.3	Not satisfied (See [PTPP])
FMT_MSA.1	Management of security attributes	FDP_ACC.1 or FDP_IFC.1	Included (FDP_ACC.1a and FDP_ACC.1b)
		FMT_SMR.1	Included
		FMT_SMF.1	Included
FMT_SMF.1	Specification of Management Functions	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	

6.4 Security Assurance Requirements Rationale

To meet the assurance expectations of service providers, the assurance level EAL6 and the augmentation with the requirement ASE_TSS.2 are chosen. The assurance level of EAL6 and the augmentation with the requirements ASE_TSS.2 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 ASE_TSS.2 follows:

- ASE_TSS.2 TOE summary specification with architectural design summary:

  ASE_TSS.2 is augmented instead of ASE_TSS.1 to enable potential service providers to gain a general understanding of how the TOE protects itself against interference, logical tampering and bypass attacks.

The dependencies of SARs added to EAL6 are described in [CC Part 3]. The following table gives their dependencies and how they are satisfied.

Table 19: Security Assurance Requirements dependency added to EAL6

ID	SFR	Dependency	Notes
ASE_TSS.2	TOE summary specification with architectural design summary	ASE_INT.1 ASE_REQ.1 ADV_ARC.1	Dependencies are covered by the assurance components of EAL6 (ASE_INT.1, ASE_REQ.2 and ADV_ARC.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.
- TOE architectural design summary
  Describes how the TOE protects itself against interference, logical tampering and bypass.

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.5 Multiple authentication mechanisms” defines the multiple authentication mechanisms which are provided by the TOE. Each Service defines either authentication mechanism by Service Attribute to access the user data. If the external entity tries to access to the Service that requires Mutual authentication (AES), the TOE and the external entity shall perform the mutual authentication by using the Access Key corresponds to the Service. "FIA_UAU.4 Single-use authentication mechanisms" and "FTP_ITC.1 Inter-TSF trusted channel" are achieved by the mutual authentication between the TOE and the external entity according to the specification of "Security Reference Manual – Mutual Authentication & Secure Communication (AES 128bit)". 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.

  If the external entity tries to access to the Service that requires Mutual authentication (CMAC), "FIA_UAU.4 Single-use authentication mechanisms" is achieved by mutual authentication between the TOE and the external entity according to the specification of “Security Reference Manual – Communication with MAC (AES 128bit)”. 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.1a and FDP_ACC.1b Subset access control" and "FDP_ACF.1a and FDP_ACF.1b 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_ACC.1/SecureID Subset access control" and "FDP_ACF.1/SecureID Security attribute based access control" are satisfied by providing an access control system based on security attributes of Blocks. The TOE and the external entity shall perform MAC verification with CK_A(FIA_UAU.5) to write the user data.
- "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 the AES algorithm, which is calculated by the hardware platform 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 provides 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 FRAM.

7.2 TOE architectural design summary

This section describes how the TOE protects itself against interference, logical tampering and bypass, which are classified into established attacks in the smartcard. The TOE provides the countermeasures against such attacks by the interaction of the underlying hardware platform and the software together as follows:

- Physical attacks and overcoming sensors/filters

The hardware platform has countermeasures against physical attacks and overcoming sensors/filters, which aim at disconnecting IC security features and accessing secret data by extracting internal signals or deactivating the sensors. The protection of the TOE comprises a set of countermeasures that are specifically described for FPT_PHP.3 and FDP_SDC.1 in the section 6.1.

- Perturbation attacks

The hardware platform and software have countermeasures against perturbation attacks, which change the normal IC behaviour to create an exploitable error during operation. Such attacks eventually aim to recover encryption keys, or change either the result of authentication or the program flow. The countermeasure of hardware platform comprises a set of countermeasures that are specifically described for FRU_FLT.2 and FPT_FLS.1 in the section 6.1. The software countermeasure comprises elaborate checks for the protection of critical program flow and security flags which are very difficult to manipulate to the attacker's chosen value.

- Differential fault analysis attack

The hardware platform and software have countermeasures against differential fault analysis, which aims at obtaining a secret data by comparing an error-free calculation and erroneous calculations. The software countermeasure comprises an elaborate verification process to detect the manipulation of various parameters, such as return value, data length and plain/cipher text. In combination with software countermeasure, various sensors implemented in the hardware platform make attack much harder.

- Exploitation attack of test function

The hardware platform has countermeasures against abuse of IC test function, which might lead to disclosure or corruption of memory content. The protection of the TOE comprises a set of countermeasures that are specifically described for FMT_LIM.1, FMT_LIM.2 and FAU_SAS.1 in the section 6.1.

- Side-channel attacks

The hardware platform has countermeasures against side-channel attacks, which aim at obtaining secret data by exploiting information leaked through characteristic variations in the calculation time and power consumption or electromagnetic emission. The protection of the TOE comprises a set of countermeasures that are specifically described for FDP_ITT.1, FDP_IFC.1 and FPT_ITT.1 in the section 6.1.

- Attacks on RNG

The hardware and software have countermeasures against attacks on RNG, which aims at predicting the output of the RNG. The countermeasure of hardware platform comprises the physical random number generator that implements total failure test of the random source. The software countermeasure comprises elaborate program flow checks for ensuring the complete operation of deterministic random number generator.

- Software attacks
  - Replay attacks

    The software has countermeasures against replay attack. The countermeasure against replay attack comprises using sequence numbers with integrity protection by the message authentication code, which making the reuse of recorded valid messages much harder.
  - Bypass authentication or access control

    The software has countermeasures against bypass attack. The bypass protection of authentication and access control comprises the command verification process, which does not accept commands that contain invalid command code and which prevents the execution of "unexpected" commands in the current authentication mode. The bypass protection of the secure channel includes the message authentication code, which rejects fake encrypted data.
  - Direct protocol attacks

    The software has countermeasures against direct protocol attack. An example of a direct protocol attack is an "unexpected" power off. The protection of the TOE includes the anti-tearing and rollback mechanism to ensure that the data in Flash memory is not corrupted. Whenever the power is switched off and a piece of data has been written to Flash memory only partially, the anti-tearing and rollback mechanism restores the previous state of Flash memory.
  - Editing commands

    The software has countermeasures against editing command attack. The countermeasure against editing command comprises the command verification process, which accepts only valid command.

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. In most cases, a service provider is a representative example of Administrator.

Access Key

A key that corresponds to an Area and a Service.

Area

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

Card reader

A contactless 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 card 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.

Pre-personalisation Data

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

FeliCa OS

An embedded software that provides the FeliCa application and the operating system.

Service

The part of FeliCa standard 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 via Service and the security condition to access the user data via Service.

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 20: 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 Functions

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 Smartcard IC

Security Target RC-SA20, RC-SA21 and RC-SA24 Series
Version 1.02

June 2020 First Edition FeliCa Business Division

Sony Imaging Products & Solutions Inc.

No. SA2-STP-E01-02

Printed in Japan