SONY

FeliCa

Dual Interface IC Chip

Security Target RC-S957/2 Series

with contact-based operating system out of scope

Public Version

Version: 1.1

No. 957-2-STP-E01-10

Introduction

This document is the Security Target for the RC-S957/2 Series product.

(Blank Page)

Contents

List of Figures

List of Tables

1. Security Target Introduction

1.1. ST Identification

ST identification

ST Name:	Security Target RC-S957/2 Series with contact-based operating system out of scope
Version:	1.1
Date:	June 2009

TOE identification

TOE Name:	RC-S957/2 Series with contact-based operating system out of scope
Version:	1.0
Product type:	Dual Interface IC Chip for smartcard
Form factor:	Antenna Module (IC with antenna)

Provided by: Sony Corporation

1.2. ST Overview

This Security Target presents the following TOE: RC-S957/2 Series with contact-based operating system out of scope.

The TOE is a dual interface integrated circuit with an antenna and an embedded smartcard operating system. The operating system is the Sony FeliCa Operating System and the integrated circuit is the Renesas AE45X1-C [ST-HW].

The security measures of the TOE aim to:

- prevent unauthorised access to the User Services (including associated user data)
- maintain the confidentiality and integrity of the user data.

The User Services are defined by Service Providers. For example, a public transport Service Provider can incorporate the RC-S957/2 Series product into a ticketing system, to offer a ticket-payment User Service. A single TOE can be used by multiple Service Providers. A Service Provider can provide multiple User Services.

The TOE can be personalised to support the following:

- various User Services to Users
- functionalities, such as cash-purse and transport-payment solutions

1.3. CC Conformance

The evaluation is based upon the following:

- Common Criteria for Information Technology Security Evaluation, Version 2.3, Part 1: General model
- Common Criteria for Information Technology Security Evaluation, Version 2.3 Part 2: Security functional requirements
- Common Criteria for Information Technology Security Evaluation, Version 2.3 Part 3: Security assurance requirements
- Common Methodology for Information Technology Security Evaluation, Version 2.3: Evaluation Methodology

The chosen level of assurance is: **Evaluation Assurance Level 4 (EAL4)**

This Security Target claims the following conformances:

- **CC Part 2 conformant**
- **CC Part 3 conformant**
- **No conformance to any PP.**

1.4. Glossary of terms and abbreviations

This section lists and describes TOE-specific terms and abbreviations, in alphabetical order.

1.4.1. Terms and definitions

Administrator

The entity responsible for personalisation of the TOE. In most cases, this is a smartcard manufacturer. Synonymous with Personaliser. See also User.

Area

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

Contactless card reader (CL_Term)

A contactless smartcard reader/writer that interacts with the FeliCa RF contactless interface. CL_Term enables the Administrator and the User to access the TOE.

Contact-based card reader (CB_Term)

A contact-based smartcard reader/writer that interacts with the Global Platform contact-based interface. CB_Term provides access for the Administrator and the User to the TOE.

FeliCa file system

The structure of data in the TOE.

FeliCa Service[1]

The part of the FeliCa 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.

Personaliser

See Administrator (in this list).

Product mode

This mode provides the Administrator and the User with a specific set of commands based on the cryptographic keys they possess.

Service Provider

An entity that provides a specific service to a User.

Test mode

This mode is Administrator-specific. The Administrator receives the TOE in this mode, in which the Administrator is able to perform all commands.

User

For this product, an entity using any User Service that a personalised TOE offers. See also Administrator.

User Service

A specific service to a User that is made technically possible by the TOE. Each User Service is provided by a Service Provider to a User. An example of a User Service is a virtual train ticket or an electronic purse.

1.4.2. Abbreviated terms and definitions

ACL	Access Control List
APDU	Application Protocol Data Unit
CB	Contact-based
CL	Contactless
COT	Chip On Tape
CRC	Cyclic Redundancy Check

[1] In this context, "Service" is used in line with the FeliCa standard, i.e. in a technical sense. In "User service" and "Service provider" it is used in the sense of human-business interaction.

EEPROM	Electronically Erasable Programmable Read-Only Memory
GP	Global Platform
MAC	Message Authentication Code
O	Objective
OE	Objective for the Environment
OS	Operating System
PP	Protection Profile
RF	Radio Frequency
SAR	Security Assurance Requirement
SF	Security Function
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation

2. TOE Description

2.1. Overview

The TOE (i.e., RC-S957/2 Series with contact-based operating system out of scope) is a dual interface COT package for an integrated circuit with an embedded smartcard operating system. The operating system is the Sony FeliCa Operating System and the integrated circuit is the Renesas AE45X1-C [ST-HW].

The TOE is intended for use in the smartcard products manufactured in accordance with ISO/IEC 7810 "Identification cards - Physical characteristics".
The TOE has the following form factor: Antenna Module (an IC with antenna) shown in Figure 1.

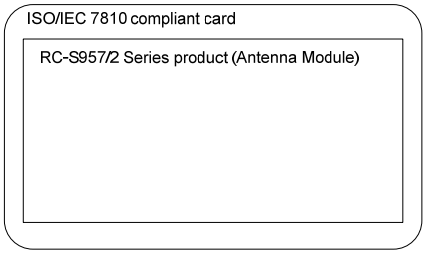

Figure 1 Antenna Module (IC with antenna)

The TOE is part of the RC-S957/2 product of Sony. The RC-S957/2 product contains the FeliCa Operating System (included in the TOE) and the Global Platform Operating System. (excluded from the TOE).

The TOE manages several data sets, each having a different purpose, on a single TOE. The TOE has a file system consisting of Areas and FeliCa Services, which organise files in a tree structure (as shown in Figure 2). Multiple Service Providers can use an Area or a FeliCa Service. Access keys enable access to data, via the Areas and FeliCa Services. This prevents unauthorized access to the User Services of other Service Providers. By organizing these keys in a specific manner, multiple Area and FeliCa Services can be authenticated simultaneously.

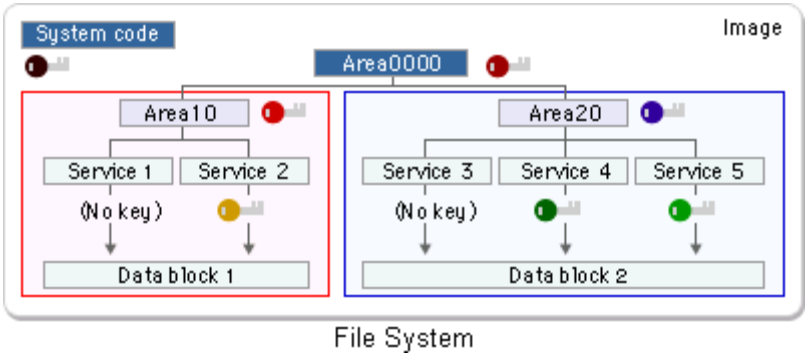

Figure 2 FeliCa file system

The security measures of the TOE aim at protecting the access to the User Services (including associated user data) and to maintain the confidentiality and integrity of the user data. The User Services are defined by Service Providers. For example, a public transport Service Provider can incorporate the RC-S957/2 product into a ticketing system, to offer a ticket-payment User Service. A single TOE can be used by multiple Service Providers. A Service Provider can provide multiple User Services.

To set up the User Services and the access to those services, the Administrator (also known as a Personaliser) configures the TOE. This configuration work enables the TOE to offer various User Services, such as cash purse and transport-payment solutions. The Administrator receives a dedicated cryptographic key from Sony for this purpose. After the TOE is personalised, the Users are allowed only to access the FeliCa Services defined by the Administrator. For example, after personalisation the public transport company can issue the RC-S957/2 product to Users.

The TOE has two interfaces: contact-based and contactless. All operations on the TOE are performed through a card reader (either a contact-based or a contactless card reader). Under the control of the FeliCa Operating System the integrated circuit communicates with a FeliCa RF card reader according to ISO/IEC18092 (Passive Communication Mode 212kbps) [ISO18092]. The TOE can be accessed either directly, through the contactless interface, or indirectly, through the contact-based interface via the Global Platform Operating System. Under control of the Global Platform Operating System the integrated circuit communicates with a contact-based card reader, according to the ISO/IEC7816 (T=1) protocol [ISO7816-3].

The card reader and the TOE authenticate each other, and only then shall the TOE allow the card reader access, according to the access policy defined by the Administrator. This policy is named Service Access Policy. After authentication the communication between the TOE and the card reader is encrypted (based on single DES).

The TOE has several self-protection mechanisms, as follows:

- Common smartcard self-protection mechanisms, such as security sensors, protect the integrated circuit.
- Integrity mechanisms ensure the integrity of data is preserved and prevent bypassing of the access control mechanism. On both start-up and any read access, a CRC check is performed on the database information.
- The writing of data to the database is an atomic operation.

2.2. TOE Boundaries

2.2.1. Physical Scope and Boundaries of the TOE

Figure 3 presents the physical scope and boundaries of the TOE, which is indicated in green. The form factor RC-S957/2 Series of the TOE is indicated in yellow. The form factor of the smartcard is indicated in gray. The GP OS, which is out of scope of the TOE, is indicated in blue.

The components of the TOE "FeliCa Operating System" constitute the part of the TOE that is responsible for managing and providing access to the Areas and Services. "Boot control" is the part of the TOE that is responsible for the start-up of the operating systems. "Contactless dispatcher" is the part of the TOE that is responsible for the processing of received commands, including those from the contact-based interface through the GP OS. "Renesas AE45X1-C integrated circuit" is the hardware platform of the TOE, which provides a contact-based interface and a contactless interface. Via the interfaces, APDU and FeliCa commands are exchanged; these commands are processed by the FeliCa OS. The hardware has detectors, sensors, and circuitry to protect the TOE. The antenna provides the RF interface on the smartcard.

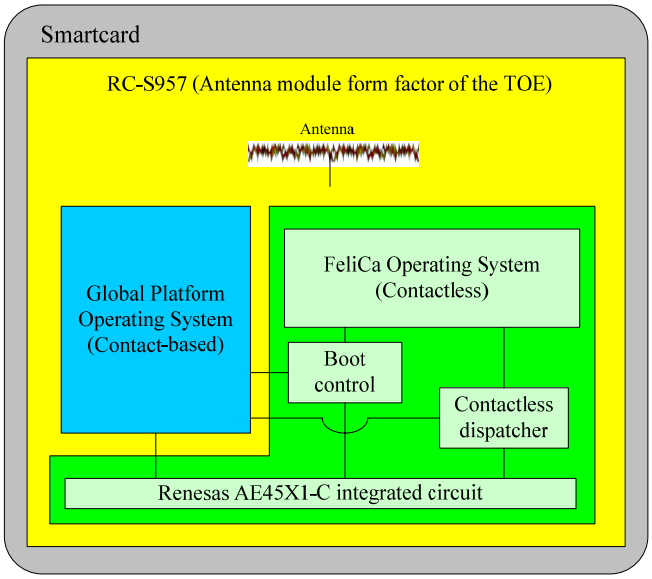

Figure 3 The RC-S957/2 product, showing the relationships between its internal components and external entities

Table 1 TOE delivery items

Delivery item type	Identifier	Version	Medium
Hardware	AE45X1-C (HD65145X1)	03	Smartcard integrated circuit

Delivery item type	Identifier		Version	Medium
Software	ROM		0C06	ROM of hardware
		FeliCa Operating System, Dual OS v1.1	06	
		Global Platform OS, v2.0.1' with Boot control and Contactless dispatcher	2005-08-02	
Manuals	RC-S957A/2 Product Specifications		1.00	Document
	RC-S957A/2 Manufacture ID Writing Procedure		1.0	Document
	RC-S954 Series FeliCa OS Command Reference Manual		1.0	Document
	RC-S957 Series FeliCa OS Inspection/Initialization Command Specifications		2.0	Document
	FeliCa Card Rewriting Transport Key		1.1	Document
	FeliCa Card Cautions for Application Development		1.0	Document
	Cross Access Functional Specifications		1.0	Document
	RC-S954/2MV Cross Access Functional Specifications Errata		1.0	Document
	Security Reference Manual Group Service Key & User Service Key Generation Procedure		1.0	Document
	Security Reference Manual Mutual Authentication & Packet Cryptography		1.01	Document
	Security Reference Manual Issuing Package Generation		1.0	Document
	Security Reference Manual Changing Key Package		1.0	Document

2.2.2. Logical Scope and Boundaries of the TOE

The TOE offers the following features:

- it can receive a command for initialisation from the GP OS
- it can receive FeliCa formatted commands from the GP OS
- it can send APDU commands to the GP OS
- it enables the set-up and maintenance of FeliCa User Services by Service Providers
- it enables the use of FeliCa User Services (e.g., decrement, cash-back)

The TOE offers the following security features:

- authentication of users
- controlled access to data stored internally in the TOE
- secure communication with smartcard reader/writer
- protection of integrity of data stored internally in the TOE
- anti-tearing and rollback
- protection against excess environment conditions
- protection against information leakage
- protection against probing and alteration

The security features are partly provided by the underlying hardware (see [ST-HW]) and partly by the FeliCa Operating System. The HW features are underlined in the previous list.

2.2.3. TOE life-cycle

The life-cycle of the TOE is best explained using the smartcard life-cycle as defined in [BSI-PP-0002], which includes the following phases:

- **Phase 1** — Smartcard-embedded software developer
- **Phase 2** — IC developer
- **Phase 3** — IC manufacturer
- **Phase 4** — IC packaging manufacturer
- **Phase 5** — Smartcard product manufacturer
- **Phase 6** — Personaliser
- **Phase 7** — Smartcard issuer

The RC-S957/2 product contains the smartcard-embedded software FeliCa Operating System (included in the TOE) and the Global Platform Operating System. This smartcard-embedded software is developed in **Phase 1**. Sony delivers the smartcard-embedded software and its pre-personalisation data to Renesas. The TOE contains a Renesas IC. The IC is developed and manufactured in **Phase 2** and **Phase 3** by Renesas. In these phases the smartcard-embedded software and its pre-personalisation data are injected. After Phase 3 the IC including operating systems is delivered to Sony. In **Phase 4** the RC-S957/2 (Antenna Module) product is assembled by Sony. In **Phase 5** Sony delivers the RC-S957/2 product to the Administrator. The Administrator is responsible for personalisation (**Phase 6**) and finally delivers the product to the User (**Phase 7**).

3. TOE Security Environment

3.1. Assets

The primary asset of the TOE is the integrity and confidentiality of sensitive user data (i.e., data from Users and Service Providers). All assets used to protect the primary assets are secondary assets (for example cryptographic keys).

3.2. Assumptions

A.Benign

It is assumed that the GP OS is benign.

A.Process-Card[2]

It is assumed that security procedures are used between delivery of the TOE by the TOE Manufacturer and delivery to the User, to maintain the confidentiality and integrity of the TOE and its manufacturing and test data (to prevent any possible copying, modification, retention, theft or unauthorised use). This means that assets after TOE Delivery are assumed to be protected appropriately.

Secure-Key

It is assumed that all cryptographic keys generated outside the TOE are kept secret and secure.

3.3. Threats

T.Logical_Attack

An attacker might load software on to the TOE, to exploit vulnerabilities in the TOE with the intention to violate the integrity and confidentiality of sensitive user data.

T.Eavesdropping

An attacker might passively monitor external TOE communication and might actively inject data, to capture and modify sensitive user data sent over the communications channel.

T.Physical_Probing

An attacker might physically modify the TOE, to bypass its protection mechanisms.

T.Leak_Inherent

An attacker might use unintentional leakage from the TOE to deduce sensitive user data.

3.4. Organisational Security Policies

P.Access_controls

The Administrator can create Areas and FeliCa Services (as shown in Figure 2) and can configure an access control policy that links those Areas and FeliCa Services with the operations allowed on them.

P.Mode

The Administrator receives the TOE in test mode and shall deliver the TOE in product mode to the User.

P.Usage

The customer expects the TOE to be administered in a positively-managed environment and used in an environment where a moderate-to-high level of independently-assured security is sufficient. The protected information of the User Services is important to the service provider, but has a relatively low commercial value.

[2] In line with the assumption of [BSI-PP-0002].

4. Security Objectives

4.1. TOE Security Objectives

O.Physical_Tamper

The TOE shall resist physical tampering, that is, physical manipulation and physical probing.

O.Side_channel

The TOE shall not leak information that can allow an attacker to bypass the security mechanisms of the TOE.

O.Logical_Tamper

The TOE shall resist logical tampering (and any bypassing) of its security mechanisms.

O.Secure_Communication

The TOE shall protect all communication that involves the TOE assets.

O.Set_Access_Control

The TOE shall provide the means for the Administrator to set the Access Control Policy.

O.Access_Control

The TOE shall provide access to user data, subject to the Access Control Policy.

O.Mode

The TOE shall provide the Administrator with the means to change the TOE from test mode to product mode and shall prevent any reversal of that change (i.e., from product mode to test mode).

4.2. Security Objectives for the Environment

OE.Benign

The developers of the GP OS and the FeliCa OS have an agreement in place: to determine that the GP OS does not interfere with the operation of TOE; to make sure that the GP OS is not interfering [ICR].

OE.Process-Card

The environment of the TOE shall maintain confidentiality and integrity of the TOE and its manufacturing and test data, by means of procedural measures between delivery of the TOE by the TOE manufacturer and delivery of the TOE to the User.

OE.Secure-Key

The environment of the TOE shall keep all cryptographic keys generated outside the TOE secret and secure.

OE. Moderate_Assurance

The TOE shall be evaluated to a moderate-to-high level of independently-assured security.

5. IT Security Requirements

5.1. TOE Security Functional Requirements

All SFRs are from part 2 of the CC.

About the Notation used for Security Functional Requirements (SFRs)

- Whenever an iteration is denoted, the component is numbered FXX_XXX.X+1 to FXX_XXX.X+n (for the n^{th} iteration). A similar numbering scheme is used for the elements in each component.
- 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 appear in **bold**.
- Assignments appear in **[bold brackets]**.

Definitions

- *Object***:** File with security attributes: Access Mode (a list of operations with authentication values). If an operation that has the appropriate authentication value is in the Access Mode list of a file, a card reader having that authentication value is allowed to execute that operation on that file.
- *Subject*:
  - User with security attribute “authentication”
  - Administrator with security attribute “authentication”

5.1.1. Requirements for Roles and the Access Control Policy for those Roles

Application note	
FMT_SMR.1	The TOE distinguishes between Administrators and Users. This SFR defines these two security-relevant roles. The Administrator and the User both use CL_Term or CB_Term to interact with the TOE.
FIA_UID.1	To be able to associate users with roles, the users must identify themselves to the TOE. This SFR specifies the list of all actions that each user can do before identifying himself. After identification the user is assumed to fulfil the associated role.
FIA_UAU.1	To identify a user before the user is authenticated, the TOE must allow users to identify themselves to the TOE. This SFR specifies the list of all actions the TOE allows a User to do before the user is authenticated.
FIA_UAU.3	To prevent forgery or copying, the TOE uses the random number for authentication data. This SFR specifies that the TOE prevents the use of authentication data that has been forged or copied.
FDP_ACC.1 and FDP_ACF.1	The TOE allows some operations only in specific circumstances, as defined in a set of rules (the access control policy) that the TOE enforces. These SFRs define the access control policy and the rules. The policy is named Service Access Policy. Each Administrator and User must obey this policy.
FDP_ITC.1	To support the cryptographic operations, the TOE must import cryptographic keys. This SFR defines the characteristics for that process. The imported keys are used for authentication.
FMT_MSA.1	The values of security attributes can be set only by the Administrator.
FMT_MSA.3	The default values of security attributes can be defined only by the Administrator. The Administrator sets the Service Access Policy. This SFR specifies that the Administrator is allowed to set the file structure that defines what a User is allowed to access. This SFR implies SFRs FMT_MSA.1 and FMT_SMF.1.
FMT_SMF.1	This SFR lists the security management functions.
FCS_COP.1+1	Authentication of the card reader to the TOE, and vice versa, is done with Triple-DES. This SFR defines the algorithm for the cryptographic operations required by that process.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **[User and Administrator]**[3].

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

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification *(Included in "Requirements for Roles and the Access Control Policy for those Roles" SFRs)*

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow **[**

- **Polling**
- **Requests**
- **Public_read**
- **Public_write**
- **Echo Back]**[4] 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.

Hierarchical to: No other components

Dependencies: None

[3] Assignment: the authorized identified roles
[4] Assignment: list of TSF-mediated actions

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **[**

- **Polling**
- **Requests**
- **Public_read**
- **Public_write**
- **Echo Back]**[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.

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification *(included in "Requirements for Roles and the Access Control Policy for those Roles" SFRs)*

FIA_UAU.3 Unforgeable authentication

FIA_UAU.3.1 The TSF shall **prevent** use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall **prevent** use of authentication data that has been copied from any other user of the TSF.

Hierarchical to: No other components

Dependencies: None

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **[Service Access Policy]**[6] on **[**

- **subjects: User and Administrator;**
- **object: Files;**
- **operations: Authentication, Read, Write, Diagnosis, Requests, Echo Back]**[7].

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control *(included in "Requirements for Roles and the Access Control Policy for those Roles" SFRs)*

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **[Service Access Policy]**[8] to objects based on the following: **[**

- **subjects: User with security attribute authentication**
  Administrator with security attribute authentication;
- **object: Files with security attribute ACL]**[9].

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

[5] Assignment: list of TSF-mediated actions
[6] Assignment: access control SFP.
[7] Assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP.
[8] Assignment: access control SFP.
[9] Assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes.

objects is allowed: **[**

- **A User executes an operation (that is, Read, Write, Decrement, or Cashback)**
- **A User can do this operation on a file when:**
  - **the User is successfully authenticated, and**
  - **the operation is part of the operations listed in the service access mode]**[10].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[none]**[11].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **[no additional explicit rules]**[12].

Hierarchical to: No other components

Dependencies:

- FDP_ACC.1 Subset access control *(included in "Requirements for Roles and the Access Control Policy for those Roles" SFRs)*
- FMT_MSA.3 Static attribute initialization *(included in "Requirements for Roles and the Access Control Policy for those Roles" SFRs)*

FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the **[Service Access Policy]**[13] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **[none]**[14].

Hierarchical to: No other components

Dependencies:

- [FDP_ACC.1 Subset access control, or
  FDP_IFC.1 Subset information flow control] *(FDP_ACC.1 included in "Requirements for Roles and the Access Control Policy for those Roles" SFRs)*
- FMT_MSA.3 Static attribute initialization *(FCS_MSA.3 included in "Requirements for Roles and the Access Control Policy for those Roles" SFRs)*

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **[Service Access Policy]**[15] to provide **[no]**[16] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **[Administrator]**[17] to specify alternative initial values to override the default values when

[10] Assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects.
[11] Assignment: rules, based on security attributes that explicitly authorize access of subjects to objects.
[12] Assignment: rules, based on security attributes that explicitly deny access of subjects to objects.
[13] Assignment: access control SFP(s) and/or information flow control SFP(s).
[14] Assignment: additional importation control rules.
[15] Assignment: access control SFP, information flow control SFP.
[16] Selection: choose one of: restrictive, permissive,[assignment: other property]
[17] Assignment: the authorized identified roles.

an object or information is created.

Dependencies:

- FMT_MSA.1 Management of security attributes *(included in "Requirements for Roles and the Access Control Policy for those Roles" SFRs)*
- FMT_SMR.1 Security roles *(included in "Requirements for Roles and the Access Control Policy for those Roles" SFRs)*

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **[Service Access Policy]**[18] to restrict the ability to **[perform any operation on]**[19] the security attributes **[all]**[20] to **[Administrator]**[21].

Hierarchical to: No other components

Dependencies:

- [FDP_ACC.1 Subset access control, or
  FDP_IFC.1 Subset information flow control] *(FDP_ACC.1 included in "Requirements for Roles and the Access Control Policy for those Roles" SFRs)*
- FMT_SMR.1 Security roles *(included in "Requirements for Roles and the Access Control Policy for those Roles" SFRs)*
- FMT_SMF.1 Specification of management functions *(included in "Requirements for Roles and the Access Control Policy for those Roles" SFRs)*

FMT_SMF.1 Specification of Management Functions

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

- **Key Change**
- **Registers]**[22].

Hierarchical to: No other components

Dependencies: none.

FCS_COP.1+1 Cryptographic operation (authentication)

FCS_COP.1.1+1 The TSF shall perform **[authentication of a remote trusted IT product**[23] **[encryption/decryption]]** in accordance with a specified cryptographic algorithm **[Triple-DES ECB-mode]**[24] and cryptographic key sizes **[112 bits]**[25] that meet the following: **[FIPS PUB 46-3]**[26].

Hierarchical to: No other components

Dependencies:

- [FDP_ITC.1 Import of user data without security attributes, or

[18] Assignment: access control SFP, information flow control SFP.
[19] Selection: change_default, query, modify, delete,[assignment: other operations]
[20] Assignment: list of security attributes.
[21] Assignment: the authorized identified roles.
[22] Assignment: list of security management functions to be provided by the TSF.
[23] This refinement was added to show that this cryptographic operation relates to authentication (i.e., TOE, card reader).
[24] Assignment: cryptographic algorithm.
[25] Assignment: cryptographic key size.
[26] Assignment: list of standards.

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] *(FDP_ITC.1 included in "Requirements for Roles and the Access Control Policy for those Roles" SFRs)*

- FCS_CKM.4 Cryptographic key destruction *(included in "Requirements for Secure Communication with Card Readers")*
- FMT_MSA.2 Secure security attributes *(not included. For details, see section 8.2.4)*

5.1.2. Requirements for Secure Communication with Card Readers

Application note	
FTP_ITC.1	The TOE needs secure communication with a trusted card reader (CL_Term or CB_Term). This SFR defines that the card reader can request to set up such a trusted channel with the TOE. As a result the TOE and the card reader authenticate each other.
FCS_COP.1+2	After authentication of the TOE and the card reader the communication between card reader and TOE is also secured. This is done with Single-DES. This SFR defines the algorithm for the required cryptographic operations.
FCS_CKM.1	To support the cryptographic operations the TOE must generate cryptographic keys. This SFR defines the characteristics for that process. The generated keys are used for secure communication.
FCS_CKM.4	To support the cryptographic operations the TOE destroys cryptographic keys. This SFR defines the characteristics for that process.

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote 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 **the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[no functions]**.

Hierarchical to: No other components

Dependencies: None

FCS_COP.1+2 Cryptographic operation (communication)

FCS_COP.1.1+2 The TSF shall perform **secure communication between TOE and a remote trusted IT product**[27] **[encryption/decryption]** in accordance with a specified cryptographic algorithm **[DES CBC-mode]** and cryptographic key sizes **[56 bits]** that meet the following: **[FIPS PUB 46-3]**.

Dependencies:

- [FDP_ITC.1 Import of user data without security attributes, or

  FDP_ITC.2 Import of user data with security attributes, or

  FCS_CKM.1 Cryptographic key generation] *(FCS_CKM.1 included in "Requirements for Secure Communication with Card Readers" SFRs)*
- FCS_CKM.4 Cryptographic key destruction *(included in "Requirements for Secure Communication with Card Readers")*
- FMT_MSA.2 Secure security attributes *(not included. For details, see section 8.2.4)*

[27] This refinement was added to show that this cryptographic operation relates to secure communication (TOE, card reader)

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Transaction key generation method]**[28] and specified cryptographic key sizes **[56 bits]**[29] that meet the following: **[FeliCa Technology]**[30].

Hierarchical to: No other components

Dependencies:

- [FCS_CKM.2 Cryptographic key distribution, or
  FCS_COP.1 Cryptographic operation] *(FCS_COP.1 included in "Requirements for Secure Communication with Card Readers" SFRs)*
- FCS_CKM.4 Cryptographic key destruction *(included in "Requirements for Secure Communication with Card Readers")*
- FMT_MSA.2 Secure security attributes *(not included. For details, see section 8.2.4)*

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**power down**][31] that meets the following: [**none**][32].

Hierarchical to: No other components.

Dependencies:

- [FDP_ITC.1 Import of user data without security attributes, or
  FDP_ITC.2 Import of user data with security attributes, or
- FCS_CKM.1 Cryptographic key generation] *(FCS_CKM.1 included in "Requirements for Secure Communication with Card Readers" SFRs)*
- FMT_MSA.2 Secure security attributes *(not included. For details, see section 8.2.4)*

5.1.3. Requirements for Secure Operation

Application note	
FPT_FLS.1	When failures occur in the TOE, the TOE must remain in a secure state. Identified as failure are errors related to data storage (i.e., in the EEPROM) that can compromise user data. This SFR defines that the TOE must maintain the secure state when this failure occurs.
FCS_RCV.4	For the function of writing data the TOE must ensure that this function is either successfully completed or rolled back to a secure state. This SFR defines that writing data during power failure either succeeds or has no result: it is not possible to write only a part of the data.

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: **[Data Integrity Error in the EEPROM]**[33].

[28] Assignment: cryptographic key generation algorithm.
[29] Assignment: cryptographic key size.
[30] Assignment: list of standards.
[31] Assignment: cryptographic key destruction method
[32] Assignment: list of standards
[33] Assignment: list of types of failures in the TSF.

Hierarchical to: No other components

Dependencies: ADV_SPM.1 Informal TOE security policy model *(included by default in an EAL4 evaluation)*

FPT_RCV.4 Function recovery

FPT_RCV.4.1 The TSF shall ensure that **[power failure during the writing of data]**[34] have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

Hierarchical to: No other components

Dependencies: ADV_SPM.1 Informal TOE security policy model *(included by default in an EAL4 evaluation)*

5.1.4. Requirements for Logical and Physical Protection and Non-Bypassability

Application note	
FPT_PHP.3	The TOE protects against physical attacks, as defined by this SFR. This SFR builds on the [BSI-PP-0002].
FPT_RVM.1	The security functions of the TOE should always be enforced. This SFR defined that security functions are not allowed to be bypassed.
FPT_SEP.1	The TOE provides a distinct protected domain for the execution of the security functions and it separates the User from the Administrator. This SFR defines that there is such a domain and separation.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **[physical manipulation and physical probing]**[35] to the **[TSF]**[36] by responding automatically such that the TSP is not violated.

Hierarchical to: No other components

Dependencies: None

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Hierarchical to: No other components

Dependencies: None

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Hierarchical to: No other components

Dependencies: None

[34] Assignment: list of SFs and failure scenarios.
[35] Assignment: physical tampering scenarios.
[36] Assignment: list of TSF devices/elements.

5.2. Strength-of-Function Claim

The strength-of-function (SOF) claim for the TOE is SOF-medium. With respect to a CC evaluation the SOF claim does not apply to the algorithmic strength of cryptographic mechanisms (FCS_COP.1+1, FCS_COP.1+2 and FCS_CKM.1), with the exception of the random number security mechanism (FIA_UAU.3).

5.3. IT Security Requirements for the Environment

There are no IT security requirements for the environment. The security objectives for the environment are realised by procedures.

5.4. TOE Security Assurance Requirements

The TOE security assurance requirements (SARs) consist of those defined by the CC Evaluation Assurance Level 4 (EAL4).

6. TOE Summary Specification

6.1. TOE Security Functions

The TOE contains the following security functions:

SF1. Access Control and Authentication

SF2. Secure Communication

SF3. Secure Data Storage

SF4. Anti-Tearing and Rollback

SF5. Protection Against Excess Environment Conditions

SF6. Protection Against Information Leakage

SF7. Protection Against Probing and Alteration

6.1.1. SF1. Access Control and Authentication

This security function controls the access to the user data stored in the FeliCa file system and performs authentication between the FeliCa OS and the card readers. The TOE distinguishes between Users and Administrators.

Operations that are allowed before successful identification and authentication are: Polling, Requests, Public_read, Public_write, and Echo Back. The TOE enforces the Service Access Policy by means of a list of area codes and service codes, which can be given to the TOE as part of a mutual authentication, specifies for which group of areas and services in the FeliCa file system authentication is requested. After successful mutual authentication the TOE has also agreed a Transaction Key with the card reader, which is the basis for secure communication and for the following operations on files by Users and Administrators: Authentication, Read, Write, Diagnosis, Requests, Echo Back, Decrement, and Cashback. A user can have access to a file only when that user is successfully authenticated and the requested operation is listed in the service access mode.

The mutual authentication and the access control to specific user data is based on cryptographic operations of Triple-DES with 112-bit keys conformant to FIPS PUB 46-3. The mutual authentication includes a random number to prevent replay attacks (forging or copying of authentication data). The random numbers are conformant to K.3 of [AIS20]. The random number uses the random number generator of the underlying hardware, see [ST-HW], to create a seed.

This security function also includes secure Key Loading, which enables the concept of providing access to a group of Areas and FeliCa Services during authentication. Only the Administrator can set the Service Access Policy.

6.1.2. SF2. Secure Communication

This function provides encipherment of information in interactions with external entities, to protect the confidentiality and integrity of information. The encryption and decryption is based on a DES CBC mode cipher using the 56-bit Transaction Key resulting from the mutual authentication. The cryptographic operations are conformant to FIPS PUB 46-3. The Transaction Key is conformant to FeliCa Technology. User information in secure communication also includes a MAC, a random number, and a sequence number, to

protect the integrity of user data and to protect against replay attacks.

6.1.3. SF3. Secure Data Storage

This function ensures the integrity of user data stored in the FeliCa file system. This function provides a mechanism to ensure data integrity of data stored in EEPROM, based on the CRC checksum parameter stored in the file system for each block of user data and on the verification of that parameter.

6.1.4. SF4. Anti-Tearing and Rollback

This function ensures that the writing of data is either successfully completed or rolled back to a consistent state. Anti-Tearing and Rollback is a protective mechanism to avoid loss of data integrity due to power loss during complex transactions. If power loss occurs during a complex transaction, all data modifications made during the transaction are rolled back.

6.1.5. SF5. Protection Against Excess Environment Conditions

This function ensures the detection of tampering with the TOE due to environmental conditions, that is, physical manipulation and physical probing. This function is based on detectors and sensors on the integrated circuit, for protection of working conditions in which the TOE functions reliably and for protection against manipulation of external conditions (e.g., excess voltage) that cause the TOE to function in an unreliable manner. The TOE can react to excess environmental conditions by either resetting the chip or giving an error response to commands. The function relies on the security measures in the chip, as described in [ST-HW].

6.1.6. SF6. Protection Against Information Leakage

This function ensures the protection against information leakage from the TOE. This function is based on circuitry on the integrated circuit, to protect the TOE against leakage of information via side channels. Externally these protective mechanisms show as noise on the chip connectors. These protective mechanisms have scramble data. The function relies on the security measures in the chip, as described in [ST-HW].

6.1.7. SF7. Protection Against Probing and Alteration

This function ensures the protection against physical attacks from physical manipulation and physical probing. This function is based on circuitry on the integrated circuit, to protect the TOE against observation or tapping of TOE-internal data. This function also protects the TOE against physical alteration of chip circuitry that aims to weaken or by-pass security mechanisms.

6.2. Probabilistic functions and mechanisms

The TOE uses a deterministic pseudo random number generator to generate random numbers.

Table 2 summarizes the SOF claim for the Security Functions that are realised by using the random number generator.

Table 2 Strength of Function claims

Security Function	SOF claim
SF1. Access Control and Authentication	Medium
SF2. Secure Communication	None
SF3. Secure Data Storage	None
SF4. Anti-Tearing and Rollback	None
SF5. Protection Against Excess Environment Conditions	None
SF6. Protection Against Information Leakage	None
SF7. Protection Against Probing and Alternation	None

6.3. Assurance Measures

Appropriate assurance measures are employed to satisfy the security assurance requirements. The assurance measures are employed partly for the hardware part and partly for the software part.

The hardware part of the TOE is the Renesas AE45X1-C integrated circuit, which has been certified by BSI, as described in the Certification Report (BSI-DSZ-CC-0351-2006) and Assurance Continuity Maintenance Report (BSI-DSZ-CC-0351-2006-MA-01). The assurance measures for the Renesas AE45X1-C integrated circuit are described in the accompanying Security Target [ST-HW]. For the composite TOE all assurance measures described remain valid.

The software part of the TOE is described in a series of documents containing the information needed for the fulfilment of the respective requirements. The documents provide the measures to comply with the requirements of EAL4. The documents are provided as evaluation evidence to the evaluators of the composite TOE. The following table provides a mapping between the assurance requirements and the documents in which the assurance measures are described:

Table 3 Mapping of assurance requirements to evaluation evidence

Assurance Requirement	Evaluation evidence that contains the assurance measures
ASE ADV_SPM.1	Security Target (this document)
ADV_FSP.2	Functional Specification
ADV_HLD.2	High-Level Design
ADV_LLD.1	Low-Level Design
ADV_IMP.1	Implementation Specification
ADV_RCR.1	Part of Functional Specification, High-Level Design, Low-Level Design and Implementation Specification

Assurance Requirement	Evaluation evidence that contains the assurance measures
ATE_COV.2 ATE_DPT.1	Test Coverage and Depth Analysis
ATE_FUN.1	Test Specification, Procedure and Results
ATE_IND.2	Test Coverage and Depth Analysis and Test Specification, Procedure and Results
ALC_DVS.1	Development security documentation
ALC_LCD.1	Life Cycle Model
ALC_TAT.1	Tool manuals
ACM_AUT.1 ACM_CAP.4 ACM_SCP.2	Quality Document Process Configuration Management Plan Operational procedure documents Configuration List
ADO_DEL.2	Delivery Rules
ADO_IGS.1 AGD_ADM.1 AGD_USR.1	Security Reference Manual Command Reference Manual Operational Guidelines Functional Specification Manufacturing Procedures
AVA_MSU.2	Misuse Analysis
AVA_SOF.1	Strength of Function Analysis
AVA_VLA.2	Vulnerability Analysis

7. PP Claims

This Security Target TOE does not claim conformance to any Protection Profile (PP).

8. Rationale

8.1. Security Objectives Rationale

We demonstrate that each assumption, threat and organisational security policy (OSP) is met by the security objectives. For evidence of this, see Table 4.

Table 4 Mapping Assumptions, threats and OSPs to Security Objectives

Assumption, threat or OSP	Security Objective
A.Benign	OE.Benign
A.Process-Card	OE.Process-Card
A.Secure-Key	OE.Secure-Key
T.Logical_Attack	O.Logical_Tamper
T.Eavesdropping	O.Secure_Communication
T.Physical_Probing	O.Physical_Tamper
T.Leak_Inherent	O.Side_Channel
P.Access_Controls	O.Set_Access_Control O.Access_Control
P.Mode	O.Mode
P.Usage	OE.Moderate_Assurance

The individual rationales demonstrating the effectiveness of the objectives are as follows:

A.Benign

This assumption is met by OE.Benign, which identifies an agreement that the developers of the GP OS will not interfere with the operation of the TOE and, therefore, the GP OS is benign.

A.Process-Card

This assumption is met by OE.Process-Card, which is self-explanatory because the protection is established to ensure that assets after TOE Delivery are protected appropriately.

A.Secure-Key

This assumption is met by OE.Secure-Key, which is self-explanatory.

T.Logical_Attack

This threat is countered by O.Logical_Tamper, which is self-explanatory because it prevents the loading of any software that might exploit vulnerabilities in the TOE.

T.Eavesdropping

This threat is countered by O.Secure_Communication, which is self-explanatory because it prevents attackers from injecting data to capture and modify sensitive user data sent over the communications channel.

T.Physical_Probing

This threat is countered by O.Physical_Tamper, which prevents physical manipulation and physical probing of the TOE to bypass its protection mechanisms.

T.Leak_Inherent

This threat is countered by O.Side_Channel, which is self-explanatory because a side channel is the method for an attacker to establish information leakage with which the attacker might bypass the security mechanisms of the TOE.

P.Access_Controls

This policy is implemented by O.Set_Access_Control and O.Access_Control. Together they realise who (the Administrator) can set the access control and what the access controls are.

P.Mode

This policy is being met by O.Mode, which provides the means to change the TOE from the test mode to the product mode.

P.Usage

This policy is being met by OE.Moderate_Assurance, which provides the moderate-to-high level of assurance that is sufficient to protect the information described by P.Usage.

8.2. Security Requirements Rationale

The purpose of the Security Requirements Rationale is to demonstrate that the security requirements adequately meet the Security Objectives.

8.2.1. The SFRs meet the Security Objectives for the TOE

We demonstrate that the SFRs meet each Security Objective for the TOE. The rationales provide implicit evidence of this, as summarised in Table 5.

Table 5 Mapping Security Objectives to SFRs

Security Objective	SFR
O.Physical_Tamper	FPT_PHP.3 Resistance to physical attack
O.Side_Channel	FPT_RVM.1 Non-bypassability of the TSP
O.Logical_Tamper	FPT_FLS.1 Failure with preservation of secure state FPT_RCV.4 Function recovery FPT_RVM.1 Non-bypassability of the TSP FPT_SEP.1 TSF domain separation
O.Secure_Communication	FTP_ITC.1 Inter-TSF trusted channel FCS_COP.1+2 Cryptographic operation (communication) FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction
O.Set_Access_Control	FMT_MSA.3 Static attribute initialisation FMT_MSA.1 Management of security attributes FMT_SMF.1 Specification of Management Functions
O.Access_Control	FMT_SMR.1 Security roles FIA_UID.1 Timing of identification FIA_UAU.1 Timing of authentication FIA_UAU.3 Unforgeable authentication FDP_ACC.1 Subset access control FDP_ACF.1 Security attribute based access control FDP_ITC.1 Import of user data without security attributes FCS_COP.1+1 Cryptographic operation (authentication)
O.Mode	FMT_SMF.1 Specification of Management Functions

O.Physical_Tamper

This objective is met by FPT_PHP.3 Resistance to physical attack. This SFR defines that the TOE protects against physical attacks (i.e., physical manipulation and physical probing). This SFR builds on [BSI-PP-0002].

O.Side_Channel

This objective is met by FPT_RVM.1, Non-bypassability of the TSP. This SFR defines that security functions are not allowed to be bypassed. Therefore, the TOE prevents an attacker from obtaining any means with which the attacker can bypass the TOE security mechanisms. The TOE invokes all of its security functions, to prevent information leakage.

O.Logical_Tamper

This objective is met collectively by FPT_FLS.1 Failure with preservation of secure state, FPT_RCV.4 Function recovery, FPT_RVM.1 Non-bypassability of the TSP, and FPT_SEP.1 TSF domain separation.

The SFR FPT_FLS.1 defines that the TOE must maintain the secure state when this failure occurs. When failures occur in the TOE, the TOE must remain in a secure state. Identified as failure are errors in the EEPROM that can compromise user data.

The SFR FCS_RCV.4 defines that writing data during power failure either succeeds or has no result: it is not possible to write only part of the data. For the function of writing data the TOE must ensure that this function is either successfully completed or rolled back to a secure state.

The SFR FPT_RVM.1 defines that security functions are not allowed to be bypassed and, more specifically, when power failure occurs during the writing of data. The security functions of the TOE shall always be enforced.

The SFR FPT_SEP.1 defines that there is a domain for the execution of the security functions, and separation of the roles User and Administrator.

Therefore, the collection of SFRs defines that the TOE can resist logical tampering and bypassing of the security mechanisms of the TOE.

O.Secure_Communication

This objective is met collectively by FTP_ITC.1 Inter-TSF trusted channel, FCS_COP.1+1 Cryptographic operation (authentication), FCS_COP.1+2 Cryptographic operation (communication), and FCS_CKM.1 Cryptographic key generation.

The SFR FTP_ITC.1 defines that the card reader (CL_Term or CB_Term) can request to set up a trusted channel with the TOE. As a result the TOE and the card reader authenticate each other.

The SFR FCS_COP.1+2 is similar to FCS_COP.1+1, but is a target at communication after authentication of the TOE and the card reader. This is done by cryptographic operations based on Single-DES.

The SFR FCS_CKM.1 and FCS_CKM.4 define the characteristics to generate and destroy cryptographic keys to support the cryptographic operations (FCS_COP) required by the TOE.

Therefore, this collection of SFRs defines the communication channels and how they protect all assets of the TOE.

O.Set_Access_Control

This objective is met by FMT_MSA.3 Static attribute initialisation, FMT_MSA.1 Management of security attributes and FMT_SMF.1 Specification of Management Functions. These SFRs define that only the Administrator can set the file structure that defines what a User is allowed to access. The default values of the security attributes can be defined only by the Administrator. Only the Administrator can set the Service Access Policy.

O.Access_Control

This objective is met collectively by FMT_SMR.1 Security roles, FIA_UID.1 Timing of identification, FIA_UAU.1 Timing of authentication, FIA_UAU.3 Unforgeable authentication, FDP_ACC.1 Subset access control, and FDP_ACF.1 Security attribute based access control.

The SFR FMT_SMR.1 defines these two security-relevant roles Administrators and Users. The Administrator and the User both use CL_Term or CB_Term to interact with the TOE.

The SFRs FIA_UID.1 and FIA_UAU.1 specify the list of all actions each user can do before identifying and authenticate himself. The list of actions is the same for both. After identification and authentication the user is assumed to fulfil the associated role.

The SFR FIA_UAU.3 prevents the use of authentication data that has been forged or copied.
The SFRs FDP_ACC.1 and FDP_ACF.1 define the access control policy and the rules. The TOE allows some operations only in specific circumstances, as defined in a set of rules (i.e., the access control policy) that the TOE enforces. The policy is called Service Access Policy. The Administrator and the User must both obey this policy.
The SFR FDP_ITC.1 defines the characteristics for importing user data. User data is imported by the authorised Administrator or the User under the access control policy named Service Access Policy. The Administrator and the User must both obey this policy.
The SFR FCS_COP.1+1 defines the algorithm for the required cryptographic operations (Triple-DES) for the authentication process between the card reader and the TOE.

O.Mode

This objective is met by FMT_SMF.1 Specification of Management Functions. This SFR defines that an Administrator is allowed to perform more commands than a User. This depends on the mode of the TOE.

8.2.2. The Security Requirements for the IT Environment meet the Security Objectives for the Environment

This section shows how all IT security objectives for the environment are addressed by security requirements for the IT environment. All security objectives (OE.Beging, OE.Process-Card and OE.Secure-Key) are non-IT and, therefore, are not addressed.

8.2.3. The Assurance Requirements and Strength of Function Claim are Appropriate

The TOE security assurance requirements match the CC Evaluation Assurance Level 4 (EAL4).

The policy P.Usage states that there must be a moderate-to-high level of assurance in the correct operation of the TOE, according to the needs of the customer and the service provider. This statement is commensurate with the intentions of CC Part 3 para 213-214. A SOF-claim of medium also supports this.

The TOE becomes operational under controlled circumstances. The security objectives are in line with the operational circumstances and the TOE level. Therefore, the SOF-claim is consistent with the security objectives of the TOE.

We consider this level to provide the best cost/assurance benefit by prospective customers for this TOE.

8.2.4. Dependencies

As shown in section 5.1 all dependencies have been met with one exception: FMT_MSA.2. This dependency is not included, because in the TOE the security attribute value of an Area or FeliCa Service establishes the authorisation relationship between user on one side and a secure Area or FeliCa Service on the other. The authorisation relationship is determined outside the TOE by the Administrator, who has the responsibility to register the correct security attribute value for each secure Area and/or FeliCa Service in the TOE. The guidance provided with the TOE describes this administrator responsibility.

The dependencies between SARs are satisfied because all dependencies in EAL4 are satisfied.
The dependencies between SFRs and SARs are limited to FPT_FLS.1 and FPT_RCV.4, which both have a dependency on

ADV_SPM.1 Informal TOE security policy model. This dependency is met by the Access Control policy defined in this Security Target.

8.2.5. The Requirements are Internally Consistent

1. The SARs are internally consistent, because they are an EAL.
2. The SFRs FPT_FLS.1 and FPT_RCV.4 have a dependency on SAR ADV_SPM.1.
   SFR ADV_SPM.1 defines the model that supports the implementation of the SFRs. Therefore, there are no inconsistencies between the SFRs.
3. All other SARs and SFRs are independent of each other, so there are no inconsistencies between them.
4. The SFRs are internally consistent because:
   a. They derive directly from the objectives.
   b. They use only the entities from the environment.

The SFRs are, therefore, considered to be internally consistent.

5. The security requirements for the IT environment are internally consistent and independent of the other requirements, because there are no requirements.
6. The SFRs, SARs and security requirements for the IT environment are all internally consistent, and no inconsistencies can be found between them. Therefore, the IT security requirements are internally consistent.

8.2.6. The Requirements are Mutually Supportive

(This argument is based on section 9.3.8 of Guide for the production of PPs and STs, PDTR 15446 N2449.)

1. The requirements meet the security objectives (see section 8.2.1 and 8.2.2).
2. The assurance requirements are appropriate (see section 8.2.3).
3. All dependencies have been met (see section 8.2.4).
4. The requirements are internally consistent (see section 8.2.5).
5. Supporting SFRs are included in the ST: notably FPT_RVM.1 (against bypass), FPT_SEP (against logical tampering), and FPT_PHP (Resistance to physical attack).

The security requirements are, therefore, considered to be mutually supportive.

8.3. TOE Summary Specification Rationale

8.3.1. The Functions meet the SFRs

We demonstrate that each SFR is met by the Security Functions. The rationales provide implicit evidence of this, as the following list and describe:

- SF1. Access Control and Authentication
- SF2. Secure Communication
- SF3. Secure Data Storage
- SF4. Anti-Tearing and Rollback
- SF5. Protection Against Excess Environment Conditions
- SF6. Protection Against Information Leakage
- SF7. Protection Against Probing and Alteration

Table 6 Mapping SFRs to Security Functions

SFR	Security Function
Requirements for roles and the access control policy for these roles	
FMT_SMR.1 Security roles	SF1. Access Control and Authentication
FIA_UID.1 Timing of identification	SF1. Access Control and Authentication
FIA_UAU.1 Timing of authentication	SF1. Access Control and Authentication
FIA_UAU.3 Unforgeable authentication	SF1. Access Control and Authentication
FDP_ACC.1 Subset access control	SF1. Access Control and Authentication
FDP_ACF.1 Security attribute based access control	SF1. Access Control and Authentication
FDP_ITC.1 Import of user data without security attributes	SF1. Access Control and Authentication
FMT_MSA.3 Static attribute initialization	SF1. Access Control and Authentication
FMT_MSA.1 Management of security attributes	SF1. Access Control and Authentication
FMT_SMF.1 Specification of Management Functions	SF1. Access Control and Authentication
FCS_COP.1+1 Cryptographic operation (authentication)	SF1. Access Control and Authentication
Requirements for secure communication with card readers	
FTP_ITC.1 Inter-TSF trusted channel	SF1. Access Control and Authentication
FCS_COP.1+2 Cryptographic operation (communication)	SF2. Secure Communication
FCS_CKM.1 Cryptographic key generation	SF1. Access Control and Authentication
FCS_CKM.4 Cryptographic key destruction	SF1. Access Control and Authentication
Requirements for secure operation	
FPT_FLS.1 Failure with preservation of secure state	SF3. Secure Data Storage
FPT_RCV.4 Function recovery	SF4. Anti-Tearing and Rollback
Requirements for logical and physical protection and non-bypassability	
FPT_PHP.3 Resistance to physical attack	SF5. Protection Against Excess Environment Conditions SF7. Protection Against Probing and Alteration
FPT_RVM.1 Non-bypassability of the TSP	SF6. Protection Against Information Leakage
FPT_SEP.1 TSF domain separation	SF5. Protection Against Excess Environment Conditions SF6. Protection Against Information Leakage SF7. Protection Against Probing and Alteration

FMT_SMR.1 Security roles

This SFR is met by SF1 Access control and authentication. This SF ensures that the TOE can interact only with Administrators and Users.

FIA_UID.1 Timing of identification and FIA_UAU.1 Timing of authentication

These two SFRs are met by SF1 Access control and authentication. This SF ensures that the Administrators and Users are authenticated before they can perform the following commands before the User or Administrator is authenticated: Polling, Requests, Public_Read, Public_Write, and Echo Back of the TOE.

FIA_UAU.3 Unforgeable authentication

This SFR is met by SF1 Access control and authentication. SF1 prevents the use of authentication data that has been forged or copied. This is supported by the use of secure random numbers.

FDP_ACC.1 Subset access control and FDP_ACF.1 Security attribute based access control

These two SFRs are met by SF1 Access control and authentication. This SF ensures that the TOE enforces an access control policy named Service Access Policy. The SF implements the rules of the defined policy.

FDP_ITC.1 Import of user data without security attributes

This SFR is met by SF1 Access control and authentication. This SF ensures the rules when importing user data from outside the TSC. The rules are defined in an access control policy named Service Access Policy. The SF also implements the rules of the defined policy.

FMT_MSA.3 Static attribute initialization, FMT_MSA.1 Management of security attributes and FMT_SMF.1 Specification of Management Functions

These SFRs are met by SF1 Access control and authentication. This SF ensures that only the Administrator can set the access control policy.

FTP_ITC.1 Inter-TSF trusted channel

This SFR is met by SF1 Access Control and Authentication. This SF ensures that a card reader can set up a channel for secure communication with the TOE.

FCS_COP.1+1 Cryptographic operation (authentication)

This SFR is met by SF1 Access Control and Authentication. SF1 provides the cryptographic algorithms to ensure that the authentication data exchanged between TOE and card readers is encrypted by Triple-DES.

FCS_COP.1+2 Cryptographic operation (communication)

This SFR is met by SF2 Secure Communication. SF2 provides the cryptographic algorithms to ensure that the user data exchanged between TOE and card readers is encrypted by Single-DES.

FCS_CKM.1 Cryptographic key generation and FCS_CKM.4 Cryptographic key destruction

These SFRs are met by SF1 Access Control and Authentication. SF1 provides the appropriate keys for the cryptographic operations of the secure channel between TOE and card readers and for the access to the User Services. On power down the keys are destroyed.

FPT_FLS.1 Failure with preservation of secure state

This SFR is met by SF3 Secure Data Storage. This SF provides a protective mechanism to add and store CRCs, to identify errors in the EEPROM that can compromise user data.

FPT_RCV.4 Function recovery

This SFR is met by SF4 Anti-Tearing and Rollback. This SF avoids loss of data integrity due to power loss during complex transactions. Writing data during power failure is either successfully completed or rolled back.

FPT_PHP.3 Resistance to physical attack

This SFR is met by SF7 Protection Against Probing and Alteration and SF5 Protection Against Excess Environment Conditions. These SFs uses detectors, sensors, and circuitry on the integrated circuit to protect the TOE against improper working conditions and physical attacks.

FPT_RVM.1 Non-bypassability of the TSP

This SFR is met by SF6 Protection Against Information Leakage. This SF uses circuitry on the integrated circuit to protect the TOE against leakage improper working conditions and physical attacks.

FPT_SEP.1 TSF domain separation

This SFR is met by SF5 Protection Against Excess Environment Conditions, SF6 Protection against Information Leakage and SF7 Protection Against Probing and Alteration. These SFs implement separation and detection of violations and subsequent actions of the separation.

8.3.2. The Assurance Measures meet the SARs

The statement of assurance measures is presented in the form of a reference to the documents that show the assurance measures have been met (CC Part 3 paragraph 186). You can find this statement in section 6.3, which also contains the required evidence.

8.3.3. The SOF-Claims for Functions meet the SOF-Claims for the SFRs

SF1 Access Control and Authentication uses a deterministic pseudo random number generator to generate random numbers. The SOF claim for this function is medium. According to E.4 of [AIS20], RNG by recursive call of a block cipher algorithm that is used by the TOE is considered to belong to class K1, passes the K2-specific tests, and fulfils the K3-specific properties d)(iii) and d)(iv).

The result of Class K1 evaluation shows that the random number generator of the TOE satisfies the requirements for Class K1; the strength of mechanism claim medium. The result of Class K2 evaluation shows that the random number generator of the TOE satisfies the requirements for Class K2. From the Class K3 justification it becomes clear the TOE utilises the Triple-DES algorithm. The description of E.4 in [AIS20] rationalises in this case that it is practically impossible for an adversary to determine the predecessor or successor of a subsequence of random vectors generated from the RNG. Therefore, the random number generator of the TOE satisfies the requirements d)(iii) and d)(iv) for Class K3; the strength of mechanism claim medium.

8.3.4. The Functions are Mutually Supportive

(This argument is based on section 9.3.8 of Guide for the production of PPs and STs, PDTR 15446 N2449.)

The amount of detail introduced by the functions beyond the SFRs is relatively small. At the points where additional detail was

introduced, it was examined whether the additional detail introduced problems affecting mutual support. This was found not to be the case.

8.4. PP Claims Rationale

This Security Target TOE does not claim conformance to any Protection Profile (PP).

9. References

[AIS20] AIS 20 (Version 1 of 2-12-1999): Functionality classes and evaluation methodology for deterministic random number generators.

[BSI-PP-0002] Eurosmart Smartcard IC Platform Protection Profile (BSI-PP-0002.), 1.0, July 2001

[FeliCa Technology] Security Reference Manual – Mutual Authentication & Packet Cryptography, Version 1.01

[FIPS PUB 46-3] Federal Information Processing Standards Publication, Data Encryption Standard (DES), 1999 October 25

[ICR] RC-S954 Interface Coding Rule between FeliCa OS and Contact OS, Version 1.0

[ISO18092] Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)

[ISO7816-3] Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols

[ST-HW] Renesas AE45X1-C (HD65145X1) Version 03 Smartcard Security Target – Public Version, Revision 4.0, August 3, 2007

(Blank Page)

Sony FeliCa Dual Interface IC Chip

Security Target RC-S957/2 Series with contact-based operating system out of scope

---

Version 1.1 : June 2009

Sony Corporation
FeliCa Business Division

NO.957-2-STP-E01-10