SONY

FeliCa

Secure Application Module for Reader/Writer

Security Target RC-S251/SO2

Version: 1.1

Public Version

No. 251-STP-E01-10

Introduction

This document is the Security Target for the RC-S251/SO2 product.

(Blank Page)

Table of contents

List of figures

List of tables

1. Introduction

This document is the Security Target for the RC-S251/SO2 product.

This Security Target is provided in accordance with “Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model” [CC Part 1]

For definitions of the terms, abbreviations, and literary references used in this document, see Chapter 7, "*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, the RC-S251/SO2.

Table 1: ST identification

Attribute	Value
Name	Security Target RC-S251/SO2
Version	1.1
Date	July 2009
Provided by	Sony Corporation

Table 2: TOE identification

Attribute	Value
Product name	RC-S251/SO2
Version	1.0
Product type	Smartcard
Form factor	ID-1/000 card

1.2. Conformance claims

The evaluation is based on the following:

- "Common Criteria for Information Technology Security Evaluation", Version 3.1 (composed of Parts1-3, [CC Part 1], [CC Part 2], and [CC Part 3])
- "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1, Revision 2, September 2007 [CC CEM]

The chosen level of assurance is: Evaluation Assurance Level 4 (EAL4) augmented with ALC_DVS.2 and AVA_VAN.5.

This Security Target claims the following conformances:

- [CC Part 2] conformant
- [CC Part 3] conformant
- No conformance to any PP

This Security Target does not contain any extended security requirements.

1.3. Ideology

The arrival of Version 3.1 of the "Common Criteria for Information Technology Security Evaluation" made us rethink how we specify the security functionality of our product. The CC ideology calls for a specific description of the security functionality provided to the user of the product. The security functionality required for the self-protection, non-bypassability and domain separation, however, is now considered to be implicitly included in the security functionality of the device.

Therefore, this Security Target specifies only the security functionality that directly benefits the user of the TOE. This functionality is related to the secure storage of the data and the provision of both access control and secure communication. All other functions (such as protection against invasive physical attacks, logical attacks, and side-channel analysis) are relegated to the architectural design because they are implied by the class of the device (that is, the smartcard). Such self-protection measures are evaluated according to “Common Criteria Supporting Document Mandatory Technical Document Application of Attack Potential to Smartcards” [AAPS] and shall be fully present for the smartcard TOE to obtain the certification. Therefore, we do not mention them explicitly in this Security Target.

2. TOE description

This chapter describes the following aspects of the TOE:

- overview
- physical scope
- delivery
- user roles
- logical scope
- lifecycle

2.1. Overview

The TOE is used as a secure application module for the reader/writer device. The TOE includes a secure IC chip with an embedded operating system. The secure IC chip is the AE57C1 developed by Renesas Technology Corporation. This IC chip is certified in CC v2.3 as EAL4 augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

Figure 1 shows the functional configuration of the reader/writer and the TOE.

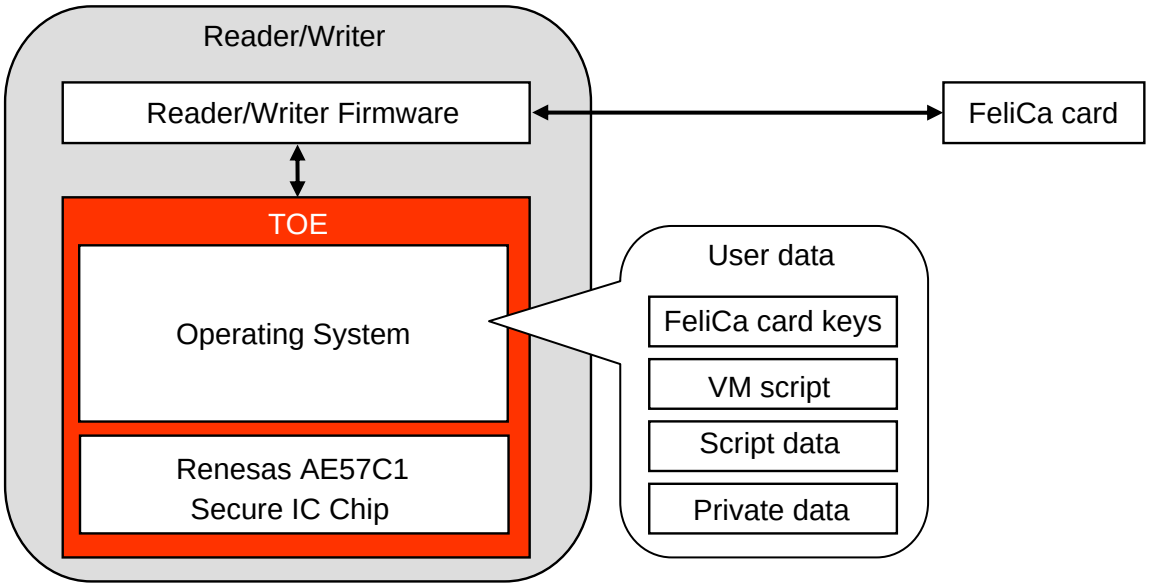

Figure 1: Functional configuration of the reader/writer and the TOE

The main function of the TOE is to encrypt and decrypt packet-based data in accordance with the FeliCa technology. By inserting the TOE into a Subscriber Identity Module (SIM) slot of a

reader/writer, the reader/writer can use the functions offered by the TOE through the interface while conforming to the specification of ISO/IEC 7816 (see “Information technology – Identification cards – Integrated circuit(s) cards with contacts” [ISO 7816]). Therefore, with the help of the TOE, the reader/writer can communicate with the FeliCa card. For the FeliCa-card user, this enables the provision of various services, such as transportation services and financial services.

To start communication with the FeliCa card, the Reader/Writer Firmware must mutually authenticate the TOE and then establish the encrypted secure-communication channel with the TOE. Then, to continue the communication after successful authentication, the TOE provides the encryption/decryption function to the authenticated Reader/Writer Firmware. This function enables the Reader/Writer Firmware to encrypt or decrypt packet-based data in accordance with the FeliCa technology. Therefore, the reader/writer can communicate with the FeliCa card and it is possible for the user to provide various services that use the FeliCa card.

For executing the encryption or decryption, the TOE allows the registration of FeliCa card keys. To securely execute encryption or decryption, the TOE has security measures that aim to maintain the confidentiality and integrity of FeliCa card keys.

In addition, the TOE allows the registration and execution of Virtual Machine (VM) scripts, so the user of the reader/writer can add bespoke functions to the TOE. VM scripts are used for two distinct purposes, as follows:

- Generate a signature from supplied input information.
  The signature algorithm runs on the VM on the TOE.
- Generate a unique value based on a proprietary individualization algorithm.
  This value is used during mutual authentication with the FeliCa card. The individualization algorithm runs on the VM on the TOE.

These algorithms are implemented by VM scripts. The TOE also allows registration of Script data and Private data, which is necessary to execute the signature algorithm and individualization algorithm with VM scripts.

To register and execute VM scripts, Script data and Private data securely, the TOE has security measures that aim to maintain the confidentiality and integrity of VM scripts, Script data and Private data.

The TOE has several self-protection mechanisms sufficient to satisfy all requirements for self-protection, non-bypassability and domain separation for the smartcard security.

2.2. Physical scope

Figure 1 illustrates the TOE scope. In the figure:

- The boundary of the TOE is indicated in red. The form factor of the TOE is the ID-1/000 card, as listed in Table 2. The ID-1/000 card is specified in [ISO 7810]. It is an ID-1 size card containing an ID-000-size card. Its physical characteristics are specified in [ISO 7810].
- “Operating System” is the part of the TOE that is responsible for executing both the processing related to the VM scripts and the packet encryption/decryption for communication with the FeliCa card. It has security measures that aim to maintain the confidentiality and integrity of FeliCa card keys, VM scripts, Script data and Private data.

- o “Renesas AE57C1” is the hardware platform (the IC) and is part of the TOE. It has detectors, sensors, and circuitry to protect the TOE. For details of “Renesas AE57C1”, see “2.1 TOE Description” in “AE57C1 (HD65257C1) Version 01 Smartcard Security Target” [ST-HW].
- o “Reader/Writer Firmware” is responsible for execution of both the reader/writer application and the packet control that conforms to the [ISO 7816] and [ISO 18092]. “Reader/Writer Firmware” is out of scope of the TOE.

“FeliCa card” is an external contactless IC card that conforms to the [ISO 18092]. “FeliCa card” is out of scope of the TOE.

2.3. Delivery

The TOE delivery items are listed in Table 3.

Table 3: TOE delivery items for RC-S251/SO2

Delivery item type	Identifier	Version	Medium
Hardware	AE57C1	01	Smartcard integrated circuit
Software	Operating System	1203	ROM and EEPROM
Manuals	RC-S251 Command Interface Manual	1.0	Document
	RC-S251 Important Requirements for an Operation	1.0	Document
	RC-S251 Rewriting Transport Key (Maintenance mode)	1.01	Document
	RC-S251 Rewriting Transport Key (Admin/Normal mode)	1.01	Document
	RC-S251 Procedure Manual for Receipt Confirmation	1.0	Document

2.4. User roles

The user roles are as shown in Table 4.

Table 4: Product-specific roles

Role	Permitted operations
Maintenance user	The Maintenance user is responsible for maintaining the Operating System, such as upgrading the Operating System.
Administrator	The Administrator is responsible for management of the TOE. He maintains user data such as FeliCa card keys and VM scripts, as well as mutual authentication keys used in the TOE.

Role	Permitted operations
Normal user	The Normal user can execute the packet encryption/decryption using FeliCa card keys. He can also execute the signature and individualization algorithm using VM scripts.

2.5. Logical scope

This section describes the logical security features provided by the TOE.

The security functions are as follows:

- **Secure storage of user data**
  The TOE protects the integrity of user data stored internally in the TOE. If the TOE detects an integrity error, it enters the error state and becomes inoperative, to ensure the security of user data.
- **Secure management of user data**
  The TOE protects the confidentiality of user data stored internally in the TOE, as follows:
  - **User identification and authentication**
    The TOE identifies the user, based on the type of roles to which the user requested authentication. Then the TOE authenticates the user, based on a mutual authentication mechanism and, after successful mutual authentication, subsequently assigns the operation authority to the user.
  - **Access control**
    To ensure the confidentiality and integrity of user data, the TOE controls the access from the authenticated user, based on the access control policy. This policy defines the rules to determine whether an operation involving the authenticated user and the user data is allowed.
  - **Key management**
    The TOE manages the keys that are necessary for user authentication and user data registration. The TOE allows only the Maintenance user and the Administrator to change the keys.
- **Secure transfer (communication) of user data**
  The TOE protects the confidentiality and integrity of user data exchanged with the Reader/Writer Firmware. The exchange of user data is performed in a secure way where the TOE and the Reader/Writer Firmware set up an encrypted session. The session allows the user data to be exchanged in a manner protected from eavesdropping and alteration.

2.6. Lifecycle

The lifecycle of the TOE is best explained using the smartcard lifecycle as defined in “Eurosmart Smartcard IC Platform Protection Profile” [BSI-PP-0035], which includes the phases listed in Table 5.

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

An explanation of each phase of the TOE lifecycle (see Table 5) follows:

Phase 1: The TOE contains the IC embedded software, which is developed in Phase 1 by Sony. Sony delivers the IC embedded software to Renesas. The TOE also contains a Renesas IC.

Phase 2 and Phase 3: The IC is developed and manufactured in Phase 2 and Phase 3 by Renesas. In these phases the IC embedded software is injected.

Phase 4: The IC, including the software, is packaged and delivered to the smartcard manufacturer by Renesas.

Phase 5: The ID-1/000 card including the IC, that is, the TOE is manufactured by the smartcard manufacturer. After Phase 5 the TOE is delivered to the customer.

Phase 6: The personalisation is performed by the Administrator, to provide a specific service.

Phase 7: Finally, the product is delivered to both the terminal vendor and merchant.

(Blank Page)

3. Security problem definition

The statement of 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 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 sensitive user data (that is, FeliCa card keys, VM scripts, Script data and Private data). The user data are stored in the volatile and non-volatile memory. The user data are essential for the communication with the FeliCa card, and are used for executing processing such as packet encryption/decryption and mutual authentication.
- All assets used to protect the primary assets are secondary assets (such as cryptographic keys for the communication channel, and so on).

3.2. Assumptions

A.Process **The TOE is administered in a secure manner after the TOE delivery.**

The customer is responsible for the secure administration of the TOE and protected storage. It is assumed that security procedures are used between delivery of the TOE by the TOE manufacturer and delivery to the customer, to maintain the confidentiality and integrity of the TOE and its manufacturing and test data (to prevent any possible copying, modification, retention, theft for unauthorized use). This means that assets after TOE delivery are assumed to be protected appropriately.

3.3. Organisational security policies

To record the security problem definition in terms of policies, we state what protection the TOE shall afford to the user, as follows:

P.Confidentiality **The TOE shall provide means to protect the confidentiality of the stored assets.**

The TOE shall have some security measures that can protect the stored user data from unauthorized disclosure. We do not expect the TOE to enforce these security measures on any or all user data, but those measures shall be available when the user decides that they shall be used for some of the user data.

P.Integrity **The TOE shall provide means to protect the integrity of the stored assets.**

The integrity of the stored assets shall be protected during operation in a hostile environment. To ensure the integrity, the TOE shall have some security measures that can protect the stored user data from unauthorized modification and destruction.

P.TransferSecret **The TOE shall provide means to protect the confidentiality of assets during transfer from the outside of TOE.**

Should the user decide so, user data that is sent or received through the communication channel needs protection from unauthorized disclosure. The TOE shall provide the capabilities to provide such measures.

P.TransferIntegrity **The TOE shall provide means to protect the integrity of assets during transfer from the outside of TOE.**

The integrity of the messages on the communication channel shall take into account both the possibility of benign interference and malicious interference in various forms, such as: RF noise, spikes in the field, short removals of the field, ghost transmissions, replay, and injection of data into the channel. The TOE shall provide the means to ensure the integrity of user data transferred.

P.Execute **The TOE shall allow only authorized users to execute packet encryption and decryption functions.**

The TOE shall have some security measures to protect the functions that use the stored user data from execution by an unauthorized user. To prevent illegal use, the TOE shall provide only the authorized user with access to the packet encryption and decryption functions, which use the user data.

P.Keys **The keys generated for the use by TOE shall be secure. The keys for the use by TOE shall be generated and handled in a secure manner.**

Some keys are generated for the TOE externally, by the supporting system in a controlled environment. This system shall check that the keys are suitably secure, for example, by weeding out weak keys. Some keys are generated outside the TOE for use by the TOE. These keys are then loaded into the TOE. The process of key generation and management shall be suitably protected and shall occur in a controlled environment.

.

4. Security objectives

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

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

4.1. TOE security objectives

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

O.AC **The TOE shall provide configurable access control system to prevent unauthorized access to stored user data.**

The TOE shall provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for in a configurable and deterministic manner.
This objective combines all aspects of authentication and access control.

O.SC **The TOE shall provide configurable secure channel mechanisms for the protection of user data when transferred between the TOE and an outside entity.**

The TOE receives and sends user data over a wired interface that is considered easy to tap and alter. Therefore, the TOE shall provide mechanisms that shall allow the TOE and an external entity to communicate with each other in a secure manner. The secure channel mechanisms shall include protection of the confidentiality and integrity of the transferred user data.

O.Integrity **The TOE shall provide mechanisms for detecting integrity errors in stored user data.**

The TOE operates in a highly unstable and hostile environment. All precautions shall be taken to ensure that all user data stored in the TOE (and any associated security data) are always in a consistent and secure state.

4.2. TOE operational environment security objectives

This section identifies the IT security objectives that are to be satisfied by the imposing of technical or procedural requirements on the TOE operational environment. These security objectives are assumed by the Security Target to be permanently in place in the TOE environment. They are included as necessary to support the TOE security objectives in addressing the security problem defined in Chapter 3, "*Security problem definition*". Each objective is stated in **bold type** font; it is followed by an application note, in regular font, which supplies additional information and interpretation.

OE.Keys **The handling of the keys outside the TOE shall be performed in accordance to the specified policies.**

Specific keys for use by the TOE are generated externally (that is, beyond control of the TOE). The generation and control of the keys shall be performed in strict compliance to the specific policies set for such operations.

OE.Process **The handling of the TOE after the TOE delivery shall be performed in a secure manner.**

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

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 tables provide a mapping of security objectives to the security problem, which is defined by the threats, policies, and assumptions, illustrating that each security objective covers at least one threat, policy or assumption and that each threat, policy, or assumption is covered by at least one security objective.

Table 6: Environmental considerations related to security objectives

Assumption or policy	Assumption or policy text	Objective	Objective text
A.Process	The TOE is administered in a secure manner after the TOE delivery.	OE.Process	The handling of the TOE after the TOE delivery shall be performed in a secure manner.
P.Confidentiality	The TOE shall provide means to protect the confidentiality of the stored assets.	O.AC	The TOE shall provide configurable access control system to prevent unauthorized access to stored user data.

Assumption or policy	Assumption or policy text	Objective	Objective text
P.Integrity	The TOE shall provide means to protect the integrity of the stored assets.	O.AC	The TOE shall provide access control system to protect integrity of the stored user data from unauthorized access.
		O.Integrity	The TOE shall provide mechanisms for detecting integrity errors in stored user data.
P.TransferSecret	The TOE shall provide means to protect the confidentiality of assets during transfer to and from the TOE.	O.SC	The TOE shall provide configurable secure channel mechanisms for the protection of user data transferred between the TOE and an external entity.
P.TransferIntegrity	The TOE shall provide means to protect the integrity of assets during transfer to and from the TOE.	O.SC	The TOE shall provide configurable secure channel mechanisms for the protection of user data transferred between the TOE and an external entity.
P.Execute	The TOE shall allow only authorized users to execute packet encryption and decryption functions.	O.AC	The TOE shall provide an access control system to prevent unauthorized access to stored user data.
P.Keys	The keys generated for the use of the TOE shall be secure. The keys for the use of the TOE shall be generated and handled in a secure manner.	OE.Keys	The handling of the keys outside the TOE shall be performed in accordance with the specified policies.

Table 7: Security objectives related to environmental considerations

Objective	Assumption or policy
O.AC	P.Confidentiality P.Integrity P.Execute
O.SC	P.TransferSecret P.TransferIntegrity
O.Integrity	P.Integrity
OE.Keys	P.Keys
OE.Process	A.Process

The following explanation shows that the chosen security objectives are sufficient and suitable to address the identified threats, assumptions, and policies.

The policies for the TOE call for protection of user data when stored in the TOE and when in transit between the TOE and an external security product. Additionally, the policies require that the system used for protection of the assets when stored within the TOE be flexible and configurable. These policies are upheld by defining the following two objectives for the TOE: O.AC and O.SC. The first makes sure that the TOE shall implement an access control system that shall protect the stored user data from illegal access (as required by P.Confidentiality) and allow only authorized users to execute the packet encryption and decryption function (as required by P.Execute). The O.SC objective provides a secure channel that shall be established between the TOE and an external entity; this secure channel shall protect all transmitted user data from disclosure (as required by P.TransferSecret) and from integrity errors, whether as a result of an attack or environmental conditions (such as loss of power), as required by P.TransferIntegrity.

In addition, the policy P.Integrity requires that user data shall be protected from integrity errors when stored in the TOE. This policy is upheld by the following two objectives for the TOE: O. AC and O.Integrity. The first provides the access control system, which allows only authorized users to access stored user data and protects the integrity of stored user data from illegal access. The O.Integrity objective provides an integrity-monitoring mechanism to detect errors in stored user data.

The policy for the environment that requires secure generation and handling of keys, P.Keys, is similarly directly translated into the objective for the environment OE.Keys for the secure handling of keys and generation of secure keys.

The security problem defined for the TOE calls for the protection of assets by the TOE. There are several security measures implemented by the TOE itself, but the proper administration of the TOE's security measures and proper handling of the TOE are essential, as stated in the A.Process assumption. That assumption is upheld through defining the objective for the environment OE.Process, which ensures that secure procedures are used by the TOE environment to ensure both the security of the assets and the proper administration of the TOE security measures.

5. IT security requirements

IT security requirements include the following:

- TOE security functional requirements (SFRs)
  That is, requirements for security functions such as information flow control, identification and authentication.
- TOE security assurance requirements (SARs)
  Provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, vulnerability assessment.)

This chapter discusses these requirements in detail. It also explains the rationales behind them, as follows:

- Security functional requirements rationale
- Security assurance requirements rationale

5.1. TOE security functional requirements

The TOE Security Objectives result in a set of Security Functional Requirements (SFRs), all of which are from [CC Part 2].

The Security Target takes advantage of the [CC] ideology, which concentrates on the specific security functionality of the device that is provided to the user and relegates the self-defence activities to the lower level (that is, the architecture specification). This approach enables a simple, focused set of SFRs to be used in the TOE, which clearly demonstrates the value of the product to the potential user.

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

- Whenever an iteration is denoted, the component is numbered incrementally. For example: **FXX_XXX.N+1** to **FXX_XXX.N+n** (for the n^{th} iteration).
- A similar numbering scheme is used for the elements in each component.
  For example: FXX_XXX.N.N+1 to FXX_XXX.N.N+n (for the n^{th} iteration).
- 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 type** font.
- Assignments appear in **Tahoma bold** font.

FMT_SMR.1	**Security roles**
FMT_SMR.1.1	The TSF shall maintain the roles **Maintenance user, Administrator, Normal user**.

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 **Get Chip Info, Set RWSAM Mode, Get RWSAM Mode, Get Last Error, Attention** 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 **Get Chip Info, Set RWSAM Mode, Get RWSAM Mode, Get Last Error, Attention** 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 **all authentication mechanisms**.

FDP_ACC.1 Subset access control

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

- **Subjects:**
  - **Maintenance user**
  - **Administrator**
  - **Normal user**
- **Object:**
  - **FeliCa card keys**
  - **Script data**
  - **VM scripts**
  - **Private data**
- **Operations:**
  - **Write**
  - **Read**
  - **Delete**
  - **Execute (execution of function using its object)**

FDP_ACF.1 Security attribute based access control

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

- **Subjects:**
  - **Maintenance user**

- **Administrator**
- **Normal user**

- **Object:**
  - **FeliCa card keys with security attribute mutual authentication keys**
  - **VM scripts with security attribute mutual authentication keys**
  - **Script data with security attribute mutual authentication keys**
  - **Private data with security attribute mutual authentication keys**

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

- **The permitted operation is shown in Table 8.**
- **The operation on the objects can be performed only when the subject succeeds in the mutual authentication.**

Table 8: Access Control List (ACL)

Subject	FeliCa card keys	VM scripts	Script data	Private data
Maintenance user	None	None	None	None
Administrator	Write/Delete	Write/Delete	Write	None
Normal user	Execute	Execute	Write/Execute	Write/Read/Execute

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

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

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **modify the behaviour of** the functions **which are implemented in Operating System** to **Maintenance user**.

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **Access Control Policy** to restrict the ability to **modify** the security attributes **(as shown in Table 9)**.

Table 9: Management of Security Attributes

Security attribute	Maintenance user	Administrator
Mutual authentication key for Maintenance user	Yes	No
Mutual authentication key for Administrator	No	Yes
Mutual authentication key for Normal user	No	Yes

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**.

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 **multiple 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 **immediately halt all operations and allow only Get Chip Info and Get Last Error to be performed**.
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**.

5.2. TOE security assurance requirements

The TOE Security Assurance Requirements (SARs) consist of the requirements defined by the CC Evaluation Assurance Level 4 (EAL4) augmented with the AVA_VAN.5 and ALC_DVS.2.

5.3. Security functional requirements rationale

The following table presents both the rationale for choosing specific Security Functional Requirements (SFRs) and how those requirements correspond to the specific Security Objectives.

Table 10: TOE Security Functional Requirements

ID	SFR	Security Objective
FMT_SMR.1	Security roles	O.AC
FIA_UID.1	Timing of identification	O.AC
FIA_UAU.1	Timing of authentication	O.AC
FIA_UAU.4	Single-use authentication mechanisms	O.AC
FDP_ACC.1	Subset access control	O.AC
FDP_ACF.1	Security attribute based access control	O.AC
FMT_MOF.1	Management of security functions behaviour	O.AC
FMT_MSA.1	Management of security attributes	O.AC
FMT_SMF.1	Specification of Management Functions	O.AC
FDP_SDI.2	Stored data integrity monitoring and action	O.Integrity
FTP_ITC.1	Inter-TSF trusted channel	O.SC

The objective O.AC is achieved through inclusion of the SFR FDP_ACC.1 and FDP_ACF.1, which specify the access control policy. The operation of the access control system is supported by the FIA_UAU.4 to ensure that unique authentication sessions shall be used every time. The FIA_UID.1 and FIA_UAU.1 complement the access control system operation by allowing very specific functions to be used without mutual authentication. FMT_SMR.1 and FMT_MSA.1 in conjunction with FMT_SMF.1 allow for the implementation of a flexible, configurable access control system and specify the roles that shall be allowed to utilize the access control system configuration capabilities. Moreover, FMT_MOF allows for modifying the behaviour of the access control system (such as the mutual authentication mechanism) and realizes the modifiable access control system. The presented combination of the SFRs provides an access control system that, as required by the O.AC objective, is precisely specified, allows for very specific exceptions, and supports very flexible configuration.

The objective O.SC is directly realized through the requirement for the secure channel FTP_ITC.1 between the TOE and the external device.

The objective O.Integrity is directly addressed through both the use of the FDP_SDI.2 requirement for the monitoring of the stored user data and the requirement that an action is taken when any integrity error occurs.

The following table presents the list of the SFRs with the associated dependencies.

Table 11: Security Functional Requirements dependencies

ID	SFR	Dependencies	Notes
FMT_SMR.1	Security roles	FIA_UID.1	Included
FIA_UID.1	Timing of identification	-	-
FIA_UAU.1	Timing of authentication	FIA_UID.1	Included
FIA_UAU.4	Single-use authentication mechanisms	-	-
FDP_ACC.1	Subset access control	FDP_ACF.1	Included
FDP_ACF.1	Security attribute based access control	FDP_ACC.1 FMT_MSA.3	Included Not satisfied
FMT_MOF.1	Management of security functions behaviour	FMT_SMR.1 FMT_SMF.1	Included Included
FMT_MSA.1	Management of security attributes	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Included (FDP_ACC.1) Included Included
FMT_SMF.1	Specification of Management Functions	-	-
FDP_SDI.2	Stored data integrity monitoring and action	-	-
FTP_ITC.1	Inter-TSF trusted channel	-	-

The SFR “FMT_MSA.3 Static attribute initialization” is a dependency for FDP_ACF.1 SFR. In the TOE, however, the security attributes are always explicitly set and the notion of “default value” for a security attribute simply does not exist. The security attributes are always set explicitly by the Maintenance user or Administrator to a value appropriate for each asset without exception, so it is our opinion that the system is no less secure in the absence of the FMT_MSA.3. Therefore, there is no need to include the FMT_MSA.3 requirement in to the ST.

5.4. Security assurance requirements rationale

EAL4 is an industry standard for smartcard chips. EAL4 was augmented with the AVA_VAN.5 and ALC_DVS.2 because one of the applications of the TOE shall be used in the financial industry and the customers require additional assurance of its security.

6. TOE Summary Specification

This chapter describes how the TOE is intended to comply with the Security Functional Requirements (SFRs). The TOE shall provide the following security functions, as described in Section 2.5, "*Logical scope*":

- secure storage of user data
- secure management of user data
- secure transfer of user data

The following describes the technical mechanisms with which the TOE satisfies the Security Functional Requirements for the previously-mentioned security functions:

- **Secure storage of user data**
  - o “FDP_SDI.2 Stored data integrity monitoring and action” is satisfied through a protective mechanism to add and store a Cyclic Redundancy Check (CRC) to identify multi-bit integrity errors in the EEPROM that can compromise stored user data. If an error is detected during self-test or normal operation, the TOE immediately halts all operations and allows only Get Chip Info and Get Last Error to be performed.
- **Secure management of user data**
  - o ”FMT_SMR.1 Security roles” is met by providing an ability to distinguish between the roles of “Maintenance user”, “Administrator” and “Normal user”, where the different roles allow the subject to execute different types of operations. The roles are assigned at the time of mutual authentication and are internally associated with any one of the three authentication modes (“Maintenance mode”, “Admin mode” or “Normal mode”).
  - o The TOE requires user identification and authentication before providing the full set of functionality. Until then, the TOE allows only a limited subset of functions to be used, as required by “FIA_UID.1 Timing of identification” and “FIA_UAU.1 Timing of authentication”.
  - o “FIA_UAU.4 Single-use authentication mechanisms” is met by providing the mutual authentication mechanism with the random numbers. The authentication data is created, based on random numbers, and then encrypted with the mutual authentication key. Therefore, the authentication data changes vary at every mutual authentication trial and the reuse of authentication data is not possible because it shall be detected as erroneous.
  - o “FDP_ACC.1 Subset access control” and “FDP_ACF.1 Security attribute based access control” are satisfied by providing an access control system, based on the security attributes. The access control system enforces the following rules when the user requests access (write/delete or execute) to stored user data:
    (1) The user has previously succeeded in mutual authentication;
    (2) The access control system allows the user to access the requested user data;
    (3) The command packet sent from the user conforms to the specified data format.

- “FMT_MSA.1 Management of security attributes” and “FMT_SMF.1 Specification of Management Functions“ are met by providing configuration capabilities of mutual authentication keys to the Maintenance user and Administrator. The configuration capabilities are granted based on the security attributes; they allow changing the values of mutual authentication keys after successful mutual authentication and privilege verification.
- “FMT_MOF.1 Management of functions in TSF” is met by providing configuration capabilities of the Operating System to the Maintenance user. The configuration capabilities are granted based on the security attributes and allow changing the part of the Operating System after successful mutual authentication. These configuration capabilities enable the behaviour of functions, such as the mutual authentication mechanism of the access control system, to be modified.

- **Secure transfer of user data**
  - “FTP_ITC.1 Inter-TSF trusted channel” requires the secure channel between the TOE and the trusted IT product. This requirement is satisfied by providing a communication channel and protecting it from disclosure by making use of an encryption/decryption mechanism. The TOE also provides protection against modification, by using cryptographic Message Authentication Code (MAC). Furthermore the TOE detects replay for the input packet, by making use of a sequence number attached to the packet: the TOE compares that number with its internal sequence number and, if the two numbers do not match, then rejects the request of access to the user data. The Reader/Writer Firmware initializes the communication to the TOE, sends requests and receives responses via this trusted channel.

7. 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.

7.1. Terms and definitions

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

Administrator

See Section 2.4, "*User roles*".

FeliCa

A contactless IC card technology developed by Sony Corporation.

Maintenance user

See Section 2.4, "*User roles*".

Normal user

See Section2.4, "*User roles*".

Private data

Arbitrary data that can be used and registered only by the Normal user.

Reader/Writer

A contactless smartcard reader/writer that interacts with the smartcard via an RF chip.

Script data

The data that can be used by the VM scripts to generate the signature and the individualized key. This can be registered by either the Maintenance user or the Normal user.

7.2. Acronyms

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

Table 12: Abbreviated terms and definitions

Term	Definition
ACL	Access Control List
CC	Common Criteria
CRC	Cyclic Redundancy Check
MAC	Message Authentication Code
PP	Protection Profile
RF	Radio Frequency
RNG	Random Number Generator
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SIM	Subscriber Identity Module
ST	Security Target
TOE	Target of Evaluation
VM	Virtual Machine

7.3. Bibliography

The following list defines the literature referenced in this document:

[AAPS] “Common Criteria Supporting Document Mandatory Technical Document Application of Attack Potential to Smartcards”, Version 2.5, Revision 1, April 2008

[BSI-PP-0035] "Eurosmart Smartcard IC Platform Protection Profile", Version 1.0, June 2007

[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 1, September 2006

[CC Part 2] "Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components", Version 3.1, Revision 2, September 2007

[CC Part 3] "Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components", Version 3.1, Revision 2, September 2007

[CC CEM] "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1, Revision 2, September 2007

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

[ISO 7810] "Identification cards – Physical characteristics"

[ISO 7816] "Information technology – Identification cards – Integrated circuit(s) cards with contacts"

[ST-HW] “AE57C1 (HD65257C1) Smartcard Security Target", Version 01, Revision 3.0, July, 2006.

Secure Application Module for Reader/Writer

Security Target RC-S251/SO2

Version 1.1: July 2009

Sony Corporation
FeliCa Business Division

No. 251-STP-E01-10

Printed in Japan