SONY®

FeliCa

IC Chip for Contactless Smartcard

JREM MN67S150-D Composite Security Target

Version: 1.70

Public Version

Document no.: F31-STP-E01-70

Introduction

This document is the Security Target for CC evaluation of IC chip product "JREM MN67S150-D Contactless Smart Card IC chip with fast processing function for transport".

- FeliCa is a contactless IC card technology developed by Sony Corporation.
- FeliCa is a trademark of Sony Corporation.
- All names of companies and products contained herein are trademarks or registered trademarks of the respective companies.
- No part of this document may be copied, or reproduced in any form, without the prior consent of Sony Corporation.
- Information in this document is subject to change without notice.

(Blank Page)

Table of contents

List of figures

List of tables

1. Introducing the Security Target

This document is the Security Target for CC evaluation of IC chip product "JREM MN67S150-D Contactless Smart Card IC chip with fast processing function for transport".

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

For definitions of the terms, abbreviations, and literary references used in this document, see Chapter 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, JREM MN67S150-D Contactless Smart Card IC chip with fast processing function for transport.

Table 1: ST identification

ST attribute	Value
Name	JREM MN67S150-D Composite Security Target
Version	1.70
Issue Date	December 2014

Table 2: TOE identification

TOE attribute	Value
Name	JREM MN67S150-D Contactless Smart Card IC chip with fast processing function for transport
Version	1.0
Product type	IC Chip for Contactless Smartcard
Form Factor	• Sawn wafer (die)

Table 3: Stakeholders

Stakeholder	Name
ST Sponsor	JR East Mechatronics Co, Ltd
ST Author	Sony Corporation
Evaluation body	Brightsight B.V.

1.2. Conformance claims

This section describes the conformance claims.

1.2.1. CC conformance claim

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 [CC CEM]

This Security Target claims the following conformances:

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

The TOE is a composite TOE with the certified hardware platform. Claiming CC Part 2 extended is because the underlying platform claims CC Part 2 extended.

This Security Target does not contain any extended security requirements.

1.2.2. Package claim

The chosen levels of assurance are:

- Evaluation Assurance Level 6 (EAL6) augmented with ASE_TSS.2 in Advanced operation mode
- Evaluation Assurance Level 4 (EAL4) in Backward-Compatible operation mode

1.2.3. PP claim

- No conformance to any PP

2. TOE description

This chapter describes the following aspects of the TOE:

- overview
- physical scope
- delivery
- logical scope
- lifecycle
- evaluated configurations

2.1. Overview

The TOE is an integrated circuit with an embedded smartcard operating system. The operating system is the Sony FeliCa Operating System (referred to in this document as FeliCa OS) and the integrated circuit is the Panasonic Corporation (Panasonic) chip MN67S150.

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 1). 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 unauthorised access to the User Services of other Service Providers. By organising these keys in a specific manner, multiple Area and FeliCa Services can be authenticated simultaneously.

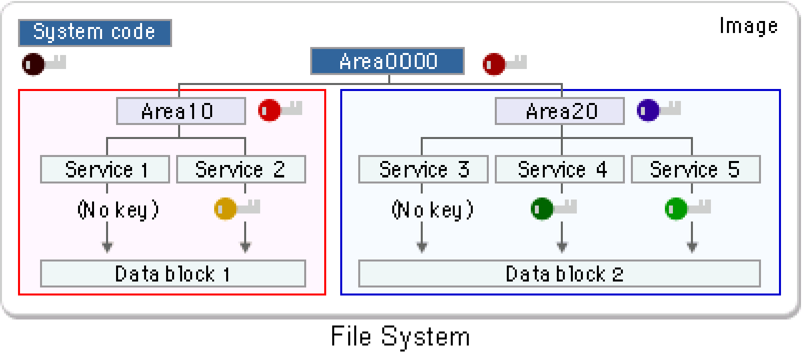

Figure 1: The FeliCa file system

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 TOE 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. After the TOE is personalised, the Users are allowed only to access the FeliCa Services defined by the Administrator.

When creating the Area or FeliCa Service, the TOE provides a very flexible configuration that allows the Administrator to choose the proper security strength for protected data: high-grade encryption or low-grade encryption, or both. Each Area and FeliCa Service can maintain two types of keys used for high-grade encryption and low-grade encryption, and the Administrator can configure each of them so as to accept only access using high-grade encryption, or only access using low-grade encryption, or both types of access using either type of encryption. This flexible configuration can be performed selectively per Area and FeliCa Service.

The TOE has a contactless interface. All operations on the TOE are performed through a contactless card reader (CL_Term). Under the control of the FeliCa Operating System the integrated circuit communicates with the CL_Term according to ISO/IEC 18092 (Passive Communication Mode 212kbps/424kbps) [ISO 18092].

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. After authentication the communication between the TOE and the card reader is encrypted.

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

2.2. Physical scope

The TOE is an integrated circuit with IC Dedicated Software and Security IC Embedded Software. The Security IC Embedded Software is the FeliCa OS and the integrated circuit is the Panasonic chip MN67S150.

The following figure illustrates the physical scope of the TOE:

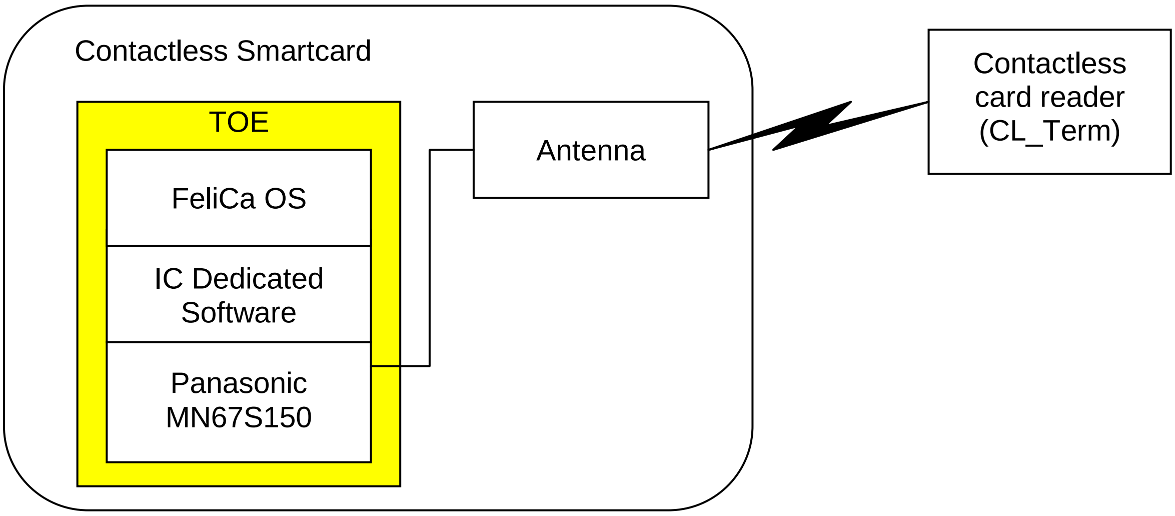

Figure 2: TOE physical scope

The components of the TOE are explained as follows:

- "FeliCa OS" constitutes the part of the TOE that is responsible for managing and providing access to the Areas and FeliCa Services.
- "IC Dedicated Software" is the specific IC-dedicated software that controls and restricts access from the FeliCa OS to the Panasonic hardware platform.
- "Panasonic MN67S150" is the hardware platform of the TOE, which provides a contactless interface. The hardware has detectors, sensors, and circuitry to protect the TOE.

The contactless interface enables the exchange of FeliCa commands, which are processed by the FeliCa OS. The antenna, which is out of scope of the TOE, provides the RF interface on the smartcard.

All components of the TOE including guidance manuals are listed in the following section.

2.3. Delivery

The TOE delivery items are listed in the following table:

Table 4: TOE delivery items

Delivery item type	Identifier	Version	Medium
Hardware	Panasonic MN67S150 Smart Card IC in sawn wafer (die) form	RV08	Smartcard integrated circuit
Software	Panasonic MN67S150 Smart Card IC – IC Dedicated Software	FV0C	Embedded in hardware
	FeliCa OS v5.0	3105	Embedded in hardware
Manuals	FeliCa Card User's Manual	1.02	Document
	FeliCa OS for MN67S150 Inspection and IDm Writing Procedure	1.01	Document
	FeliCa OS for MN67S150 Acceptance Procedure	1.00	Document
	Security Reference Manual – Group Service Key & User Service Key Generation	1.00	Document
	Security Reference Manual – Mutual Authentication & Packet Cryptography	1.01	Document
	Security Reference Manual – Issuing Package Generation	1.00	Document
	Security Reference Manual – Changing Key Package Generation	1.00	Document
	Security Reference Manual – Group Key Generation (AES 128bit)	1.21	Document
	Security Reference Manual – Mutual Authentication & Packet Cryptography (AES 128bit)	1.21	Document
	Security Reference Manual – Issuing Package Generation (AES 128bit)	1.21	Document
	Security Reference Manual – Changing Key Package Generation (AES 128bit)	1.21	Document

2.4. Logical scope

The TOE offers the following features:

- it can receive FeliCa formatted commands from the contactless interface
- it can send FeliCa formatted responses to the contactless interface
- it enables the set-up and maintenance of FeliCa Services by Service Providers
- it enables the use of FeliCa 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 the 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 provided partly by the underlying hardware and partly by the FeliCa Operating System.

2.5. Lifecycle

The lifecycle of the TOE is explained using the smartcard lifecycle as defined in “Security IC Platform Protection Profile” [BSI-PP-0035], which includes the phases listed in the following table:

Table 5: Phases of the TOE lifecycle

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

The TOE is delivered at the end of **Phase 3**.

An explanation of each phase of the TOE lifecycle follows:

Phase 1: The TOE contains the Security IC Embedded Software, which is developed in Phase 1 by Sony.

At the end of this phase, Sony delivers the Security IC Embedded Software and its pre-personalisation data to Panasonic.

Phase 2 and Phase 3: The IC is developed and manufactured in Phase 2 and Phase 3 by Panasonic. In these phases the Security IC Embedded Software and its pre-personalisation data are injected.

At the end of Phase 3, the TOE can be delivered to the Smartcard Manufacturer.

Sony views the Smartcard Manufacturer and the Administrator jointly as the Administrator role.

Phase 4: The Smartcard Manufacturer assembles the TOE into its antenna module product.

Phase 5: The Smartcard Manufacturer integrates the antenna module into its smartcard product and then delivers that product to the Administrator.

Phase 6: The Administrator performs the personalisation.

Phase 7: The product is delivered to the Card holder for operational use.

2.6. Evaluated configurations

The TOE provides a very flexible access control configuration system that allows the system administrator to choose from several options when creating the services. The administrator may create (i) unprotected files (i.e., public access files), (ii) files that are protected by advanced high-grade encryption, (iii) files that are protected by low-grade encryption and (iv) files that are protected by both advanced high-grade encryption and low-grade encryption. In the above case (iv), the files are practically regarded as being protected by low-grade encryption.

The TOE is evaluated in two modes of operation, to verify the level of protection provided to all cases that can be implemented by the administrator. The different cases afford different levels of protection, so the TOE is operated in two distinct modes of operation — Advanced and Backward-Compatible — to ensure that the TOE can provide the required level of protection.

In the Advanced operation mode, the TOE is accessed via a channel using advanced high-grade encryption for the protected data, or no encryption for the public data.

In the Backward-Compatible operation mode the TOE is accessed via a channel using low-grade encryption for the protected data, or no encryption for the public data.

The operation mode depends on the configuration of the TOE (as set by the Administrator).

3. Security problem definition

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

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

- primary and secondary assets
- the 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 (i.e., data from Users and Service Providers) loaded into the volatile and non-volatile memory.
- all assets employed to protect the primary assets are secondary assets (such as cryptographic keys, the operating system code, data, 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 both the TOE and the 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 unauthorised 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 the means to protect the confidentiality of the stored assets.**

The TOE shall have some security measures that can protect the stored user data from unauthorised 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 the means to protect the integrity of the stored assets.**

The integrity of the stored assets shall be protected during operation in a hostile environment. The possibility of attacks trying to alter specific data cannot be discounted but, for a contactless smartcard, there are other considerations that already make the integrity a prime concern, such as the very real possibility of power cut-off at any point during processing. To ensure the integrity, the TOE shall have some security measures that can protect the stored user data from unauthorised modification and destruction.

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

At the user’s discretion, user data that is sent or received through the communication channel needs protection from unauthorised disclosure. The TOE shall provide the capabilities to provide such measures.

P.TransferIntegrity **The TOE shall provide the 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.Configure **The TOE shall provide the means to configure the level of protection for each of the assets.**

The TOE is a tool to be used by the user in a system that shall implement specific business rules. The TOE may not assume the level of protection required for any asset. The TOE shall provide the means for the level of protection to be specified explicitly by the user for each asset.

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

Some keys for TOE use are generated outside the TOE, by the supporting system in a controlled environment. This system shall check that all such keys are suitably secure by, for example, weeding out weak keys. The secure 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, as a result of the discussion of the Security Problem Definition. Each objective is stated in **bold type** font. It is followed by an application note, in regular font, which provides additional information and interpretation.

O.AC **The TOE shall provide a configurable access control system to prevent unauthorised 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 wireless interface, which is considered easy to tap and alter. Therefore, the TOE shall provide mechanisms that 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 TOE environment, confidentiality and integrity of the TOE and its manufacturing and test data shall be maintained by means of procedural measures between delivery of the TOE by the TOE manufacturer and delivery of the TOE to the 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 table maps the security objectives to the security problem, which is defined by the relevant threats, policies, and assumptions. This illustrates that each threat, policy, or assumption is covered by at least one security objective.

Table 6: Assumptions or Policies versus 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 the means to protect the confidentiality of the stored assets.	O.AC	The TOE shall provide a configurable access control mechanism to prevent unauthorised access to stored user data.
P.Integrity	The TOE shall provide the means to protect the integrity of the stored assets.	O.AC	The TOE shall provide an access control mechanism to protect integrity of the stored user data from unauthorised access.
		O.Integrity	The TOE shall provide mechanisms for detecting integrity errors in stored user data.
P.TransferSecret	The TOE shall provide the 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 the means to protect the integrity of assets during transfer to and from the TOE.	O.SC	The TOE shall provide a configurable secure channel mechanism for the protection of user data transferred between the TOE and an external entity.
P.Configure	The TOE shall provide the means to configure the level of protection for each of the assets.	O.AC	The TOE shall provide a configurable access control mechanism to prevent unauthorised 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.

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. Also, 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 O.AC objective makes sure that the TOE implements an access control system that protects the stored user data from illegal access (as required by the P.Confidentiality policy), while providing the capability to configure the access rules and operations for the authorised users (as required by the P.Configure policy). 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.

The policy P.Integrity requires that user data shall be protected from integrity errors when stored in the TOE. It is upheld by two objectives for the TOE: O. AC and O.Integrity. The O.AC objective provides the access control system, which allows only authorised 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 by 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.

The following table maps all security objectives defined in this Security Target to the relevant threats, policies, and assumptions. This illustrates that each security objective covers at least one threat, policy or assumption.

Table 7: Security objectives versus Assumptions or Policies

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

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 (such as configuration management, testing, vulnerability assessment.)

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

- Security functional requirements rationale
- Security assurance requirements rationale

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].

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 nth 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 nth 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 **User and Administrator**.

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

FIA_UID.1 Timing of identification

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

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

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **Polling, Requests, Public_read, Public_write, Echo Back, Reset Mode** 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 **Service Access Policy** on the following:

- **Subjects:**
  - **User**
  - **Administrator**
- **Objects: Files**
- **Operations:**
  - **Authentication**
  - **Read**
  - **Write**
  - **Reset Mode**

FDP_ACF.1 Security attribute based access control

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

- **Subjects:**
  - **User with security attribute authentication**
  - **Administrator with security attribute authentication**
- **Objects: Files with security attributes ACL and Mode Selector**

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:

- **A Subject can do this operation on an Object when: the Subject is successfully authenticated, and the operation is listed in the Object's ACL.**
- **The operation mode is based on the Mode Selector, which is one of the Object's security attributes. The operation mode determines whether FTP_ITC.1+1 or FTP_ITC.1+2 is used.**

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

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

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **Service Access Policy** to restrict the ability to **perform any operation on** the security attributes **all** to **Administrator**.

FMT_SMF.1 Specification of Management Functions

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

FDP_SDI.2 Stored data integrity monitoring and action

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

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

FTP_ITC.1+1 Inter-TSF trusted channel

FTP_ITC.1.1+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 **by an attacker with High attack potential**.

FTP_ITC.1.2+1 The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3+1 The TSF shall initiate communication via the trusted channel for **no functions**.

FTP_ITC.1+2 Inter-TSF trusted channel (not available in the TOE that supports only Advanced operation mode)

FTP_ITC.1.1+2 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 **by an attacker with Enhanced-Basic attack potential**.

FTP_ITC.1.2+2 The TSF shall permit **the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3+2 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 following two levels of assurance, depending on the operation mode:

- Advanced operation mode: Evaluation Assurance Level 6 (EAL6) augmented with ASE_TSS.2.
- Backward-Compatible operation mode: Evaluation Assurance Level 4 (EAL4).

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

ADV_SPM.1 **Formal TOE security policy model**

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

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

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

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

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 8: TOE Security Functional Requirements versus Security Objectives

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

The objective O.AC is achieved through inclusion of the SFRs FDP_ACC.1 and FDP_ACF.1, which together specify the access control policy. The operation of the access control system is supported by the SFR FIA_UAU.4 to make sure that unique authentication sessions shall be used every time. The SFRs FIA_UID.1 and FIA_UAU.1 complement the access control system operation by allowing very specific functions to be used without mutual authentication. The SFRs FMT_SMR.1 and FMT_MSA.1 in conjunction with the SFR FMT_SMF.1 allow for the implementation of a flexible, configurable access control system and specify the roles that shall be allowed to utilise the access control system configuration capabilities. 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 realised through the requirement for the secure channel SFR FTP_ITC.1+1 and FTP_ITC.1+2 between the TOE and the external device. The selection of the FTP_ITC.1+1 or FTP_ITC.1+2 is based on the configuration of the security attributes set by the administrator (FMT_MSA.1) of the TOE and happens during the access to the TOE automatically (FDP_ACF.1).

The objective O.Integrity is directly addressed through both the use of the SFR FDP_SDI.2 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 9: Security Functional Requirements dependencies

ID	SFR	Dependencies	Notes
FMT_SMR.1	Security roles	FIA_UID.1	Included
FIA_UID.1	Timing of identification	None	
FIA_UAU.1	Timing of authentication	FIA_UID.1	Included
FIA_UAU.4	Single-use authentication mechanisms	None	
FDP_ACC.1	Subset access control	FDP_ACF.1	Included
FDP_ACF.1	Security attribute based access control	FDP_ACC.1 FMT_MSA.3	Included Not satisfied
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	None	
FDP_SDI.2	Stored data integrity monitoring and action	None	
FTP_ITC.1+1	Inter-TSF trusted channel	None	
FTP_ITC.1+2	Inter-TSF trusted channel	None	

The SFR “FMT_MSA.3 Static attribute initialisation” is a dependency for the SFR FDP_ACF.1. 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 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 SFR FMT_MSA.3. Therefore, there is no need to include the SFR FMT_MSA.3 in the ST.

5.4. Security assurance requirements rationale

Customers require a flexible access control system that can be set up for two different infrastructures: Advanced operation mode and Backward-Compatible operation mode. One customer may use the TOE only in the Advanced operation mode while other ones may use both modes to migrate his system from a current infrastructure to a more advance infrastructure, which can provide stronger cryptographic protection. The provision of both operation modes in the TOE is necessary during the migration period because it takes a long time to replace current infrastructures with new ones. Considering these requirements, the assurance level EAL6 augmented with ASE_TSS.2 is chosen for Advanced operation mode and the assurance level EAL4 is chosen for Backward-Compatible operation mode.

To meet the assurance expectations of customers, the assurance level EAL6 and the augmentation with the requirement ASE_TSS.2 are chosen. The assurance level of EAL6 is selected because it provides a sufficient level of assurance for this type of TOE, which is expected to protect high value assets. Explanations of the security assurance component ASE_TSS.2 follows:

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

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

The assurance level EAL4 is chosen for Backward-Compatible operation mode because the legacy infrastructure can not operate at a level higher than EAL4. The TOE operating in a legacy infrastructure in Backward-Compatible operation mode provides a reasonable level of resistance against attacks with Enhanced-Basic potential because in Backward-Compatible operation mode, a low-grade encryption is used. Customers in a legacy infrastructure require a reasonable level of assurance, which is at the same level as the legacy FeliCa cards have provided. Therefore, the assurance level of EAL4 is selected.

The essential difference between Backward-Compatible operation mode and Advanced operation mode is that the component AVA_VAN.3 is chosen for Backward-Compatible operation mode (instead of AVA_VAN.5). Other components in EAL6 are higher or at the same level of those in EAL4, so all security requirements of the assurance level of EAL4 are satisfied.

Although the evaluation assurance level in Backward-Compatible operation mode can be expressed as EAL4 augmented with ADV_FSP.5, ADV_IMP.2, ADV_INT.3, ADV_SPM.1, ADV_TDS.5, ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_DPT.3, and ATE_FUN.2, the developer would like to claim EAL4, to make it simple for customers to understand.

6. TOE summary specification

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

The TOE summary specification includes the following:

- TOE summary specification rationale
  Describes how the TOE meets each SFR.
- TOE architectural design summary
  Describes how the TOE protects itself against interference, logical tampering and bypass.

6.1. TOE summary specification rationale

This section describes how the TOE is intended to comply with the Security Functional Requirements. The TOE must satisfy the requirements for secure storage, transfer, and management of user data. Therefore, the TOE is implemented as a software platform on a secure chip.

The TOE includes the functions for creating secure storage containers and management of the security attributes of those containers. The TOE provides functions for populating the containers with user data in various ways that are functionally required by the customers, retrieval of the data or updating the data in situ.

The transfer of data during the operations on secure containers is performed in a secure way, where the external security product and the TOE are mutually authenticated before the operation and then connected with each other via an encrypted session. The session allows the bilateral transfer of data in a manner protected from eavesdropping and alteration.

In compliance with the requirements, the TOE also provides a capability for the unsecured storage and retrieval of user data. The security attributes can be set up in such a manner that the data can be retrieved insecurely but updated only in a secure manner, allowing for a flexible and fully-configurable access-control system.

- “FMT_SMR.1 Security roles” is met by providing an ability to distinguish between the roles of “Administrator” and “User”, where the different roles allow the subject to execute different kinds of operations. The TOE has built-in rules for distinguishing between the operations and required security attributes for various TOE and TSF data. The Administrator of the TOE specifies the security attributes for the TOE data and the TSF data. The role of the authenticated entity is assigned after the authentication has succeeded (in accordance with the requirements of FDP_ACC.1).
- “FIA_UID.1 Timing of identification” and “FIA_UAU.1 Timing of authentication” are intended to provide a possibility to configure a publically-accessible container. The TOE provides access to such specifically-configured containers based on the security attributes of the container. The container must be configured by the Administrator with special attributes that allow the specified mode of access before authentication.

- The TOE uses random numbers in the authentication mechanism to comply with the "FIA_UAU.4 Single-use authentication mechanisms" requirement; these numbers are generated by the hardware. The random numbers are generated anew each time the authentication is started, according to the requirements of FDP_ACC.1, and are discarded each time the TOE exits the authenticated state.
- "FDP_ACC.1 Subset access control" and "FDP_ACF.1 Security attribute based access control" are satisfied by providing an access control mechanism based on the attributes of security containers. The TOE grants access to the TOE data stored in the containers, based on the security attributes during the authentication phase. If the correct security attributes are used during the authentication for the requested mode of access to the specified container, the requested mode of access is granted. The granularity of access control is based on a single mode of access and a single container. A request for access may combine attributes for several containers and several modes of access in a single request. The security attributes are assigned to the containers by the Administrator. The TOE allows the Administrator to access the security attributes for configuration purposes, based on the security attributes (in accordance with FMT_MSA.1 and FMT_SMR.1).
- "FMT_MSA.1 Management of security attributes" and "FMT_SMF.1 Specification of Management Functions" are met by providing configuration capabilities accessible to the Administrator. The configuration capabilities are granted based on the security attributes and allow the changing of these security attributes to new values after successful authentication and privilege verification (in accordance with FDP_ACC.1 and FMT_SMR.1).
- "FDP_SDI.2 Stored data integrity monitoring and action" is satisfied through the monitoring of user data stored in secure containers for bit integrity errors. The TOE uses a cyclic redundancy check (CRC) based on CRC-16-CCITT to verify the correctness of the stored data at each start-up and at each access. If an error is detected, the TOE takes the appropriate action to ensure the security of the data.
- The TOE provides different grades of encryption for the different access modes. The Administrator configures the TOE such that it can be accessed in either of two operation modes: Advanced or Backward-Compatible. The trusted channel uses advanced high-grade encryption or low-grade encryption, based on both the configuration and which TOE data is being accessed. This functionality is handled by the following iterations of the FTP_ITC.1 SFR component:
    - "FTP_ITC.1+1 Inter-TSF trusted channel" (Advanced operation mode) requires the secure channel to be protected against attackers with High attack potential – this is provided by the TOE using the AES algorithm, which is calculated by the hardware, for encrypting and authenticating data that is sent or received through the link.
    - "FTP_ITC.1+2 Inter-TSF trusted channel" (Backward-Compatible operation mode) requires the secure channel to be protected against attackers with Enhanced-Basic attack potential – this is provided by the TOE using the DES algorithm, which is calculated by the hardware, for encryption and Triple DES (TDES) for authentication.

6.2. TOE architectural design summary

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

- Physical attacks and overcoming sensors/filters

  The hardware platform has countermeasures against physical attacks and overcoming sensors/filters, which aim at disconnecting IC security features and accessing secret data by extracting internal signals or deactivating the sensors. The protection of the TOE comprises metal active shield and data protection with memory scramble. In case that any malfunction occurred or may likely occur, the CPU and all register are initialized to preserve a secure state.

- Perturbation attacks

  The hardware platform and software have countermeasures against perturbation attacks, which change the normal IC behaviour to create an exploitable error during operation. Such attacks eventually aim to recover encryption keys, or change either the result of authentication or the program flow. The countermeasure of hardware platform comprises sensors for supplied voltage, clock frequency, temperature, light and glitch signal, and address area monitoring and CPU instruction monitoring. The software countermeasure comprises elaborate checks for the protection of critical program flow and security flags which are very difficult to manipulate to the attacker’s chosen value.

- Differential fault analysis attack

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

- Exploitation attack of test function

  The hardware platform has countermeasures against abuse of IC test function, which might lead to disclosure or corruption of memory content. The protection of the TOE includes the control mechanism of the test function so that the test function is irreversibly disabled by the chip manufacturer as soon as the tests are completed.

- Side-channel attacks

  The hardware platform has countermeasures against side-channel attacks, which aim at obtaining secret data by exploiting information leaked through characteristic variations in the calculation time and power consumption or electromagnetic radiation. The protection of the TOE comprises elaborate hardware architecture to remove the data dependency of externally-observable information, such as the previously-mentioned parameters.

- Attacks on RNG

  The hardware platform has countermeasures against attacks on RNG, which aims at predicting the output of the RNG. The random number generator fulfils the requirements of functionality class PTG.2 of [BSI-AIS-31].

- Software attacks

  - Replay attacks

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

- Bypass authentication or access control

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

- Direct protocol attacks

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

- Editing commands

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

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

The entity responsible for personalisation of the TOE. In most cases, this is a representative of a Service Provider. Synonymous with Personaliser. *See also* User.

Advanced operation mode

The operation mode where the access to the TOE during the encrypted session is performed using advanced high-grade encryption.

Area

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

Backward-Compatible operation mode

The operation mode where the access to the TOE during the encrypted session is performed using low-grade encryption.

Card holder

A person who uses User Service.

Contactless card reader (CL_Term)

A contactless smartcard Reader/Writer that interacts with the TOE.

FeliCa file system

The structure of data in the TOE.

FeliCa Service

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.

Service Provider

An entity that provides a specific service to a User.

User

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

User Service

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

7.2. Acronyms

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

Table 10: Abbreviated terms and definitions

Term	Definition
ACL	Access Control List
ID	Identification
OS	Operating System
PP	Protection Profile
RF	Radio Frequency
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

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 2.7, Revision 1, March 2009

[BSI-AIS-31] “Application Notes and Interpretation of the Scheme (AIS), AIS 31: Functionality classes and evaluation methodology for physical random number generators”, Version 1, September 2001

[BSI-PP-0035] "Security 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 4, September 2012

[CC Part 2] "Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components", Version 3.1, Revision 4, September 2012

[CC Part 3] "Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components", Version 3.1, Revision4, September 2012

[CC CEM] "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1, Revision 4, September 2012

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

[ST-HW] MN67S150 Smart Card IC Security Target (ST-Lite), Version 1.8, 9 March 2015

IC Chip for Contactless Smartcard

JREM MN67S150-D Composite Security Target

Version 1.70: December 2014

Sony Corporation
FeliCa Business Division

Document no.: F31-STP-E01-70

Printed in Japan