SONY®

FeliCa

Contactless Smartcard IC

Security Target
RC-SA01/1 Series and
RC-SA01/2 Series

Version: 1.10

Public Version

Document no.: A01-STP-E01-10

Introduction

This document is the Security Target for CC evaluation of IC chip product "RC-SA01/1 Series and RC-SA01/2 Series".

(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 RC-SA01/1 Series and RC-SA01/2 Series.

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

For definitions of the terms, abbreviations, and literary references used in this document, see Chapter 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, FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series.

Table 1: ST identification

ST attribute	Value
Name	Security Target RC-SA01/1 Series and RC-SA01/2 Series
Version	1.10
Issue Date	November 2012

Table 2: TOE identification

TOE attribute	Value
Name	FeliCa Contactless Smartcard IC RC-SA01/1 Series and RC-SA01/2 Series
Version	1.0
Product type	Contactless Smartcard IC
Form Factor	• bare chip with bump on wafer • bare chip with bump in tray • bare chip without bump on wafer • bare chip without bump in tray

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

1.2.2. Package claim

The chosen level of assurance is:

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

1.2.3. PP claim

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

- “Security IC Platform Protection Profile”, Version 1.0 [BSI-PP-0035]

1.2.4. PP claim rationale

The TOE type defined in section 2.3 of this Security Target is an integrated circuit including software package, together with guidance manual. This is consistent with the TOE type defined in section 1.2.2 of [BSI-PP-0035]. This Security Target claims strict conformance to the Protection Profile.

2. TOE description

This chapter describes the following aspects of the TOE:

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

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 Toshiba Corporation (Toshiba) chip T6ND8.

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.

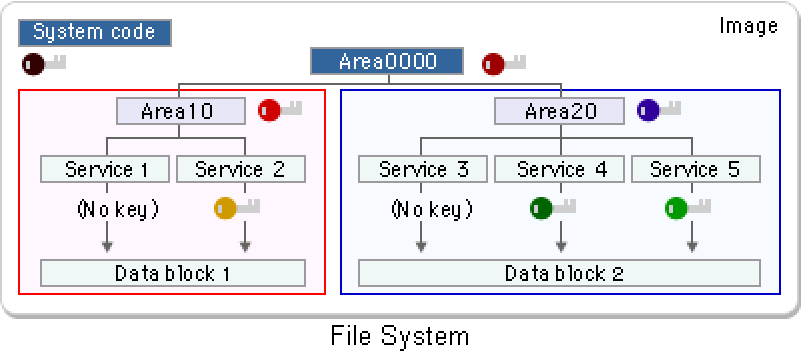

Figure 1: The FeliCa file system

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.

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 212/424kbps) [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 Toshiba chip T6ND8.

The following figure illustrates the physical scope of the TOE:

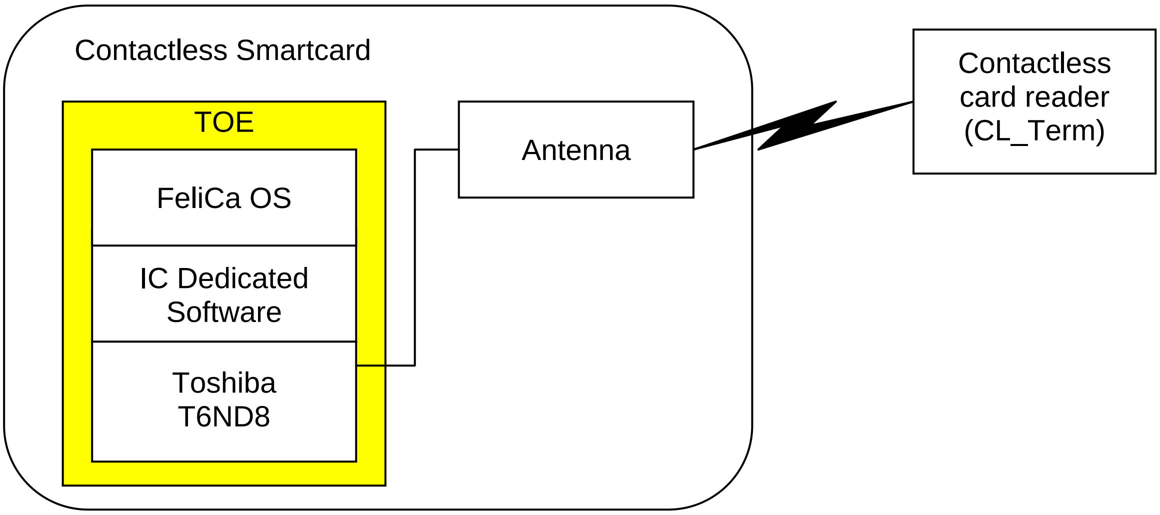

Figure 2: TOE physical scope

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 Toshiba hardware platform.
- "Toshiba T6ND8" is the hardware platform of the TOE, which provides a contactless interface. The CPU of the hardware platform “Toshiba T6ND8” has a 32-bit architecture. The hardware platform includes ROM, RAM, EEPROM memory and the cryptographic co-processor which supports AES operation. The hardware platform also includes security 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 smart card.

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 3: TOE delivery items

Delivery item type	Identifier	Version	Medium
Hardware	Toshiba T6ND8 Smartcard IC – Hardware	6.0	Smartcard integrated circuit
Software	Toshiba T6ND8 Smartcard IC – IC Dedicated Software	4.0	Embedded in hardware
	FeliCa OS v5.0	3403, 3503	Embedded in hardware
Manuals	FeliCa Card User's Manual	1.01	Document
	RC-SA01 Series Inspection Procedure	1.10	Document
	RC-SA01 Series Inspection and IDm Writing Procedure	1.00	Document
	RC-SA01 Series Acceptance Procedure	1.10	Document
	FeliCa Card Application Note for Random ID	1.00	Document
	Security Reference Manual – Group Key Generation (AES 128bit)	1.21	Document
	Security Reference Manual – Mutual Authentication & Secure Communication (AES 128bit)	1.21	Document
	Security Reference Manual – 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
- privacy protection against Card holder behaviour tracking
- 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 4: 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 Toshiba.

Phase 2 and Phase 3: The IC is developed and manufactured in Phase 2 and Phase 3 by Toshiba. 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 the configuration that allows the system administrator to choose an option of privacy protection mechanism, which provides random ID. The administrator may use either unique ID or random ID during the anti-collision sequence between the TOE and CL_Term. Unique ID may be used for tracking of Card holder, but random ID can prevent Card holder from being tracked.

The TOE is evaluated in both with or without privacy protection mechanism.

2.7. Evaluated derivative products

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

The product type names which are subject of the evaluation are listed in the following table:

Table 5: Product name comprising the group of derivatives

Product name	IC Code	Specifications
RC-SA01/1A	3403	8pF input capacity, 4KB EEPROM, bare chip with bump on wafer.
RC-SA01/1B		8pF input capacity, 4KB EEPROM, bare chip with bump in tray.
RC-SA01/1C		8pF input capacity, 4KB EEPROM, bare chip without bump on wafer.
RC-SA01/1D		8pF input capacity, 4KB EEPROM, bare chip without bump in tray.
RC-SA01/2A	3503	50pF input capacity, 4KB EEPROM, bare chip with bump on wafer.
RC-SA01/2B		50pF input capacity, 4KB EEPROM, bare chip with bump in tray.
RC-SA01/2C		50pF input capacity, 4KB EEPROM, bare chip without bump on wafer.
RC-SA01/2D		50pF input capacity, 4KB EEPROM, bare chip without bump in tray.

IC Code listed in the above table is the identifier to discriminate the TOE derivatives. A number of TOE derivatives are supported in this Security Target and all product type names listed in the table above are subject of the evaluation.

3. Security problem definition

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

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

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

3.1. Assets

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

- the primary asset of the TOE is the 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).

In addition to the above assets, since this Security Target claims conformance to “Security IC Platform Protection Profile” [BSI-PP-0035], the assets defined in section 3.1 of the Protection Profile are also expected to be protected.

3.2. Threats

The threats are directed against the assets and the security functions of the TOE. Since this Security Target claims conformance to “Security IC Platform Protection Profile” [BSI-PP-0035], the threats defined in section 3.2 of the Protection Profile are applied for this Security Target. The following table shows the threats of the Protection Profile.

Table 6: Threats defined in the Protection Profile

Threats	Titles
T.Phys-Manipulation	Physical Manipulation
T.Phys-Probing	Physical Probing
T.Malfunction	Malfunction due to Environmental Stress
T.Leak-Inherent	Inherent Information Leakage

Threats	Titles
T.Leak-Forced	Forced Information Leakage
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers

3.3. Assumptions

The customer is responsible for the secure administration of the TOE. 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. So the following assumption defined in section 3.4 of the Protection Profile [BSI-PP-0035] is applied for this Security Target.

Table 7: Assumptions defined in the Protection Profile

Assumption	Title
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation

In addition to the above assumption, the Protection Profile defines the assumptions A.Plat-Appl and A.Resp-Appl which are intended to the developer of the Security IC Embedded Software. These assumptions are re-assigned to the organisational security policies P.Plat-Appl and P.Resp-Appl because the TOE does include the Security IC Embedded Software which fulfils these assumptions.

3.4. 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 smart card, 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.

P.Untrackability The TOE shall provide the means to prevent the tracking of the Card holder through the TOE-specific information

At the Service Provider’s discretion, the Card holder is protected from being tracked with the TOE-specific information by the unauthorised user. The TOE shall provide the capabilities to provide such measures. Typically the TOE-specific information may be unique ID of the TOE.

In addition to the above organisational security policies, since this Security Target claims conformance to “Security IC Platform Protection Profile” [BSI-PP-0035], the organisational security policies defined in section 3.3 of the Protection Profile are applied for this Security Target. The following table shows the organisational security policies of the Protection Profile:

Table 8: Organisational security policies defined in the Protection Profile

Policy	Title
P.Process-TOE	Protection during TOE Development and Production

The TOE includes Security IC Embedded Software which fulfils the assumptions A.Plat-Appl and A.Resp-Appl defined in [BSI-PP-0035] and thereby these assumptions are re-assigned to the following organisational security policies for this Security Target.

P.Plat-Appl **Usage of hardware platform**

The Security IC Embedded Software of the TOE shall be designed so that the requirements from the hardware platform of the TOE are met according to the assumption A.Plat-Appl defined in [BSI-PP-0035].

P.Resp-Appl **Treatment of user data**

The Security IC Embedded Software of the TOE shall treat user data according to the assumption A.Resp-Appl defined in [BSI-PP-0035].

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.

O.Untrackability **The TOE shall provide configurable privacy protection mechanism against Card holder tracking.**

The TOE shall provide the means to protect the Card holder from being tracked. This shall be done by providing an option that protects the TOE-specific information from the Card holder tracking by any unauthorised third party.

In addition to the above security objectives, since this Security Target claims conformance to “Security IC Platform Protection Profile” [BSI-PP-0035], the security objectives defined in section 4.1 of the Protection Profile are valid for this Security Target. The following table shows the security objectives of the Protection Profile:

Table 9: Security objectives defined in the Protection Profile

Security objectives	Titles
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunctions
O.Phys-Manipulation	Protection against Physical Manipulation
O.Leak-Forced	Protection against Forced Information Leakage
O.Abuse-Func	Protection against Abuse of Functionality
O.Identification	TOE Identification
O.RND	Random Numbers

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.

In addition to the above environment objectives, since this Security Target claims conformance to “Security IC Platform Protection Profile” [BSI-PP-0035], the objectives defined in section 4.2 and 4.3 of the Protection Profile are valid for this Security Target. The following table shows the environment objectives of the Protection Profile:

Table 10: Security objectives for the environment defined in the Protection Profile

Security objectives	Titles
OE.Plat-Appl	Usage of hardware platform
OE.Resp-Appl	Treatment of user data
OE.Process-Sec-IC	Protection during composite product manufacturing

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 11: Policies versus Security Objectives

Policy	Policy text	Objective	Objective text
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.

Policy	Policy text	Objective	Objective text
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.
P.Untrackability	The TOE shall provide the means to prevent the tracking of Card holder through the TOE specific information.	O.Untrackability	The TOE shall provide a configurable privacy protection mechanism against user tracking
		O.AC	The TOE shall configurable access control mechanism to prevent unauthorised access to the TOE-specific information.

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 P.Untrackability requires that the user shall be protected from tracking if the TOE specific information is compromised. Tracking can be performed with identification (ID) number stored in the TOE. This policy is upheld by two objectives for the TOE: O.Untrackability and O.AC, which provide the means to protect the disclosure of TOE specific information (ID number) that leads to user tracking by unauthorised third party.

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 following table maps the security problem to the security objectives defined in the Protection Profile [BSI-PP-0035]. The section 4.4 of the Protection Profile gives the rationale of showing that the security objectives are sufficient and suitable to address the threats, assumptions, and policies.

Table 12: Assumptions, Threats or Policies versus Security Objectives defined in the PP

Assumption, threat or policy	Objective	Notes
P.Plat-Appl (re-assigned from A.Plat-Appl)	OE.Plat-Appl	Phase1 See discussion below
P.Resp-Appl (re-assigned from A.Resp-Appl)	OE.Resp-Appl	Phase 1 See discussion below
P.Process-TOE	O.Identification	Phase 2 – 3
A.Process-Sec-IC	OE.Process-Sec-IC	Phase 4 – 6
T.Leak-Inherent	O.Leak-Inherent	
T.Phys-Probing	O.Phys-Probing	
T.Malfunction	O.Malfunction	
T.Phys-Manipulation	O.Phys-Manipulation	
T.Leak-Forced	O.Leak-Forced	
T.Abuse-Func	O.Abuse-Func	
T.RND	O.RND	

The following explanation shows the reason why the re-assigned policies P.Plat-Appl and P.Resp-Appl are sufficiently addressed by OE.Plat-Appl and OE.Resp-Appl respectively.

The policy P.Plat-Appl requires that the Security IC Embedded Software shall be designed so that the requirements from the hardware platform are met according to the assumption A.Plat-Appl defined in [BSI-PP-0035]. This policy is directly covered by the objective for the environment OE.Plat-Appl for secure usage of hardware platform. In the Protection Profile, the Phase 1 (Security IC Embedded Software development) is identified as the operational environment. However this TOE includes the Security IC Embedded Software development in the scope. In the development of the Security IC Embedded Software, the requirements from the hardware platform of the TOE are taken into account and therefore the security objective for the environment is fulfilled.

The policy P.Resp-Appl requires that the Security IC Embedded Software shall treat user data according to the assumption A.Resp-Appl defined in [BSI-PP-0035]. This policy is directly covered by the objective for the environment OE.Resp-Appl which requires the Security IC Embedded Software to treat the security relevant user data as required by the security needs. In the Protection Profile, the Phase 1 is identified as the operational environment. However this TOE includes the Security IC Embedded Software development in the scope. The Security IC Embedded Software implements measures for secure treatment of user data through the security objectives O.AC, O.SC and O.Integrity, and therefore the security objective for the environment is fulfilled.

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

Table 13: Security Objectives versus Assumptions, Threats or Policies

Objectives	Assumptions, threats or policies
O.AC	P.Confidentiality P.Integrity P.Configure
O.SC	P.TransferSecret P.TransferIntegrity
O.Integrity	P.Integrity
O.Untrackability	P.Untrackability
OE.Keys	P.Keys
O.Leak-Inherent	T.Leak-Inherent
O.Phys-Probing	T.Phys-Probing
O.Malfunction	T.Malfunction
O.Phys-Manipulation	T.Phys-Manipulation
O.Leak-Forced	T.Leak-Forced
O.Abuse-Func	T.Abuse-Func
O.Identification	P.Process-TOE
O.RND	T.RND
OE.Plat-Appl	P.Plat-Appl (re-assigned from A.Plat-Appl)
OE.Resp-Appl	P.Resp-Appl (re-assigned from A.Resp-Appl)
OE.Process-Sec-IC	A.Process-Sec-IC

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).

The following section 5.1.1 and 5.1.2 separately describe the SFRs defined in this Security Target and Protection Profile [BSI-PP-0035].

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

- The refinement operation is used in many cases, to make the requirements easier to read and understand. All these cases are indicated and explained in footnotes.
- Selections appear in **bold type** font.
- Assignments appear in **Tahoma bold** font.

5.1.1. SFRs defined in the Security Target

This section describes the SFRs which are defined in the Security Target. All of the SFRs described in this section are taken from [CC Part2].

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**

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.**

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_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **enable, disable** the functions **random ID function** to **Administrator**.

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, management of random ID function**.

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**.

FPR_UNL.1 Unlinkability

FPR_UNL.1.1 The TSF shall ensure that **unauthorised third parties** are unable to determine whether **any operation of the TOE were caused by the same Card holder**[1].

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 **by an attacker with High attack potential**.

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**.

[1] Refinement operation is done. In this Security Target, “user” is consistently used as the term of representing User and Administrator. To state the requirement accurately without misunderstanding, the term “user” is replaced by “Card holder”.

5.1.2. SFRs from the Protection Profile

The following table shows SFRs which are directly taken from the Protection Profile [BSI-PP-0035]. Some of the SFRs are CC Part 2 extended and defined in the Protection Profile. This is shown in the third column of the table

Table 14: SFRs taken from the Protection Profile

SFR	Titles	Defined in
FRU_FLT.2	Limited fault tolerance	CC, Part 2
FPT_FLS.1	Failure with preservation of secure state	CC, Part 2
FMT_LIM.1	Limited capabilities	PP, Section 5.2 (Extended)
FMT_LIM.2	Limited availability	PP, Section 5.2 (Extended)
FAU_SAS.1	Audit storage	PP, Section 5.3 (Extended)
FPT_PHP.3	Resistance to physical attack	CC, Part 2
FDP_ITT.1	Basic internal transfer protection	CC, Part 2
FDP_IFC.1	Subset information flow control	CC, Part 2
FPT_ITT.1	Basic internal TSF data transfer protection	CC, Part 2
FCS_RNG.1	Quality metric for random numbers	PP, Section 5.1 (Extended)

All assignment and selection operations on these SFRs are completely specified in the Protection Profile except the following SFRs.

- FAU_SAS Audit storage
- FCS_RNG Random number generation

These SFRs are defined as follows:

FAU_SAS.1 Audit storage

FAU_SAS.1.1 The TSF shall provide **the test process before TOE Delivery** with the capability to store **the Initialisation Data and/or Pre-personalisation Data** in the **EEPROM**.

FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a **physical** random number generator that implements **total failure test of the random source.** [2]

FCS_RNG.1.2 The TSF shall provide random numbers that meet **the functionality class K4 of [BSI-AIS-20].** [3]

[2] Application note 20 in [BSI-PP-0035] requires that the Security Target assigns the security capabilities how the results of the total failure test are provided to the Security IC Embedded Software. The total failure tests are automatically performed on the seeding data. The results of the total failure test are provided to the Security IC Embedded Software as a pass or fail status.

[3] The TOE uses the physical random processes for its entropy and post-processes this with AES deterministic random number generator for additional security. [BSI-AIS-20] describes this construction exactly, therefore [BSI-AIS-20] is chosen as quality metric and evaluation methodology.

5.2. TOE security assurance requirements

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.

According to application note 21 of [BSI-PP-0035], the Protection Profile allows to add higher hierarchical components. This Security Target claims conformance to the Protection Profile. The differences in the SARs between the Protection Profile and the Security Target are identified in the following table.

Table 15: TOE SARs versus SARs chosen in Protection Profile

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

5.2.1. Refinements of the TOE Assurance Requirements

The Protection Profile defines the refinements for some SARs in section 6.2.1 of [BSI-PP-0035]. This Security Target selects the higher level assurance components compared to the Protection Profile. The following table shows the SARs that have the refinements in the Protection Profile and provides the overview of analysis results of whether the refinements are still applicable to higher hierarchical component.

Table 16: Applicability analysis of refinement of assurance requirements

TOE SARs	SARs chosen in PP	Level difference	Refinement applicability
ADV_ARC.1	ADV_ARC.1	None	still applicable
ADV_FSP.5	ADV_FSP.4	Higher hierarchical component	still applicable
ADV_IMP.2	ADV_IMP.1	Higher hierarchical component	still applicable
AGD_OPE.1	AGD_OPE.1	None	still applicable
AGD_PRE.1	AGD_PRE.1	None	still applicable
ALC_CMC.5	ALC_CMC.4	Higher hierarchical component	still applicable
ALC_CMS.5	ALC_CMS.4	Higher hierarchical component	still applicable
ALC_DEL.1	ALC_DEL.1	None	still applicable
ALC_DVS.2	ALC_DVS.2	None	still applicable
ATE_COV.3	ATE_COV.2	Higher hierarchical component	still applicable
AVA_VAN.5	AVA_VAN.5	None	still applicable

The following five refinements from the Protection Profile are analysed here in the Security Target, as the higher hierarchical components are selected.

- Refinement regarding functional specification (ADV_FSP)

  The refinement is still applicable to higher assurance component ADV_FSP.5. The refinement of the Protection Profile is performed only to provide a more clear explanation about what to be described in functional specification and show no necessity of describing test functions of the IC Dedicated Test Software. ADV_FSP.5 requires semi-formal functional specification with additional error messages which do not result from an invocation of a TSFI. Since ADV_FSP.5 has influence only on the formality of description and the scope of error messages, the refinements remains unaffected and still applicable.

- Refinement regarding implementation representation (ADV_IMP)

  The refinement is still applicable to higher assurance component ADV_IMP.2. The refinement of the Protection Profile is performed only to ensure that analysis activities are not curtailed due to lack of information of implementation representation. ADV_IMP.2 requires the complete mapping between TOE design description and the entire implementation representation. Since ADV_IMP.2 has influence only on the scope of mapping with implementation representation, the refinement remains unaffected and still applicable.

- Refinement regarding CM capabilities (ALC_CMC)

  The refinement is still applicable to higher assurance component ALC_CMC.5. The refinement of the Protection Profile is performed only to provide a more clear explanation about the scope of configuration item and production control system. ALC_CMC.5 requires justification of acceptance procedures, version identification of the implementation representation and automated means to identify which configuration items are affected by modifications. Since ALC_CMC.5 only includes these additional requirements, the refinement remains unaffected and still applicable.

- Refinement regarding CM scope (ALC_CMS)

  The refinement is still applicable to higher assurance component ALC_CMS.5. The refinement of the Protection Profile is performed only to provide a more clear explanation about the scope of the configuration items. ALC_CMS.5 requires to add the development tools and related information into the scope of configuration items. Since ALC_CMS.5 only enlarges the scope of configuration items, the refinement remains unaffected and still applicable.

- Refinement regarding test coverage (ATE_COV)

  The refinement is still applicable to higher assurance component ATE_COV.3. The refinement of the Protection Profile is performed only to provide a more clear explanation about the test operating conditions and evidence required to demonstrate the effectiveness against physical attacks. ATE_COV.3 requires to demonstrate that the tests exercise all of the parameters of all TSFIs. Since ATE_COV.3 only includes the additional requirement, the refinement remains unaffected and still applicable.

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 17: 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 “Inter-TSF trusted channel”
O.Integrity	- FDP_SDI.2 “Stored data integrity monitoring and action”
O.Untrackability	- FMT_MOF.1 "Management of security functions behavior" - FMT_SMR.1 “Security roles” - FMT_SMF.1 “Specification of Management Functions” - FPR_UNL.1 “Unlinkability”

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 between the TOE and the external device.

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 objective O.Untrackability is addressed through the SFR FPR_UNL.1 which requires that unauthorised third party are unable to determine whether any operation of the TOE were caused by the same Card holder. The functionality provided by FPR_UNL.1 can be enabled or disabled by the Administrator through the SFRs FMT_MOF.1, FMT_SMR.1 and FMT_SMF.1.

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

Table 18: Security Functional Requirements dependencies (except SFRs from the PP)

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_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	None	
FDP_SDI.2	Stored data integrity monitoring and action	None	
FPR_UNL.1	Unlinkability	None	
FTP_ITC.1	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.

Regarding the Security Objectives defined in the Protection Profile, the section 6.3.1 of [BSI-PP-0035] provides both the rationale for choosing specific SFRs and how those requirements correspond to the specific Security Objectives. The following table gives an overview, how the SFRs are combined to meet the security objectives.

Table 19: TOE Security Functional Requirements versus Security Objectives defined in the PP

Objective	TOE Security Functional Requirements
O.Leak-Inherent	- FDP_ITT.1 “Basic internal transfer protection” - FPT_ITT.1 “Basic internal TSF data transfer protection” - FDP_IFC.1 “Subset information flow control”
O.Phys-Probing	- FPT_PHP.3 “Resistance to physical attack”
O.Malfunction	- FRU_FLT.2 “Limited fault tolerance - FPT_FLS.1 “Failure with preservation of secure state”
O.Phys-Manipulation	- FPT_PHP.3 “Resistance to physical attack”
O.Leak-Forced	All requirements listed for O.Leak-Inherent - FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 plus those listed for O.Malfunction and O.Phys-Manipulation - FRU_FLT.2, FPT_FLS.1, FPT_PHP.3
O.Abuse-Func	- FMT_LIM.1 “Limited capabilities” - FMT_LIM.2 “Limited availability” plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced - FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1
O.Identification	- FAU_SAS.1 “Audit storage”
O.RND	- FCS_RNG.1 “Quality metric for random numbers” plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced - FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1

The dependencies of SFRs defined in Protection Profile are listed in section 6.3.2 in [BSI-PP-0035]. The following table gives their dependencies and how they are satisfied.

Table 20: Security Functional Requirements dependencies taken from the PP

ID	SFR	Dependencies	Notes
FRU_FLT.2	Limited fault tolerance	FPT_FLS.1	Included
FPT_FLS.1	Failure with preservation of secure state	None	
FMT_LIM.1	Limited capabilities	FMT_LIM.2	Included
FMT_LIM.2	Limited availability	FMT_LIM.1	Included
FAU_SAS.1	Audit storage	None	
FPT_PHP.3	Resistance to physical attack	None	

FDP_ITT.1	Basic internal transfer protection	FDP_ACC.1 or FDP_IFC.1	Included (FDP_ACC.1)
FDP_IFC.1	Subset information flow control	FDP_IFF.1	See section 6.3.2 in [BSI-PP-0035]
FPT_ITT.1	Basic internal TSF data transfer protection	None	
FCS_RNG.1	Quality metric for random numbers	None	

5.4. Security assurance requirements rationale

To meet the assurance expectations of customers, the assurance level EAL6 and the augmentation with the requirements 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. Explanation of the security assurance component ASE_TSS.2 follows:

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

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

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 random number generator (FCS_RNG.1). 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_MOF.1 Management of security functions behaviour" provides an option to use a random ID number during the anti-collision sequence between the TOE and CL_Term to prevent Card holder from being tracked by unauthorised third party. The TOE allows the Administrator to enable or disable the random ID function in accordance with FMT_SMF.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.
- “FPR_UNL.1 Unlinkability” is satisfied by using a random ID number during the anti-collision sequence between the TOE and CL_Term. The TOE does not send its unique ID number, but generates a new random ID number by the request from CL_Term and sends the random ID number during anti-collision sequence. Therefore, the TOE can no longer be tracked by any unauthorised third party simply by retrieving its ID number.
- “FTP_ITC.1 Inter-TSF trusted channel” requires the secure channel to be protected against attackers with High attack potential – this is provided by the TOE using the AES algorithm, which is calculated by the hardware, for encrypting and authenticating data that is sent or received through the link.
- “FRU_FLT.2 Limited fault tolerance” and “FPT_FLS.1 Failure with preservation of secure state” are satisfied by a group of security measures that guarantee correct operation of the TOE.
  The TOE ensures its correct operation and prevents any malfunction while the Security IC Embedded Software is executed and utilizes standard functions offered by the micro-controller (standard CPU instruction set including usage of standard peripherals such as memories, registers, I/O interfaces, timers etc.) and of all other specific security functionality.
  This is achieved through an appropriate design of the TOE and the implementation of filters for

high-frequency pulse, sensors/detectors for supplied voltage, frequency, temperature, light and glitch signal, and address area monitoring and integrity monitoring. In case that any malfunction occurred or may likely occur, the TOE stops operation or triggers system reset to preserve a secure state.

- “FDP_ITT.1 Basic internal transfer protection”, “FDP_IFC.1 Subset information flow control” and “FPT_ITT.1 Basic internal TSF data transfer protection” are satisfied by implementing several measures that provides logical protection against leakage. The TOE ensures the prevention of the disclosure of user data or TSF data through the measurement of the power consumption, electromagnetic emission or calculation time, and subsequent signal processing. This is achieved through the measures to eliminate/limit the secret information contained in power consumption, electromagnetic emission or calculation time, and small-space implementation by advanced CMOS process, and variable timing noise to randomly delay the critical operation.
- “FPT_PHP.3 Resistance to physical attack” is satisfied by implementing security measures that provides physical protection against physical probing and manipulation. The protection of the TOE is achieved through measures which comprise passive/active shield, specific encryption for the memory blocks, data scrambling between the blocks, glue logic layout of multiple blocks, sensor signal monitoring and address area monitoring. If the physical manipulation or physical probing attack is detected, the TOE stops operation.
- “FMT_LIM.1 Limited capabilities“, “FMT_LIM.2 Limited availability” and “FAU_SAS.1 Audit storage” are satisfied by implementing of a complicated test mode control mechanism that prevents abuse of test functionality delivered as part of the TOE. The test functionality is not available to the user after Phase 3 IC Manufacturing as defined in the Protection Profile [BSI-PP-0035]. The TOE has complicated access control mechanisms in place to prevent using this functionality.
- “FCS_RNG.1 Random number generation” is satisfied by providing a random number generator. The TOE contains the random number generator which comprises a physical noise source, total failure tests and online quality test on this noise source and a deterministic random number generator based on the AES algorithm. The seed data is input to the deterministic random number generator. The random number generator fulfils the requirements of functionality class K4 of [BSI-AIS-20].

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 a set of countermeasures that are specifically described for FPT_PHP.3 in the section 6.1.
- Perturbation attacks

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

- Differential fault analysis attack

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

- Exploitation attack of test function

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

- Side-channel attacks

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

- Attacks on RNG

  The hardware and software have countermeasures against attacks on RNG, which aims at predicting the output of the RNG. The countermeasure of hardware platform comprises a set of countermeasures that are specifically described for FCS_RNG.1 in the section 6.1. The software countermeasure comprises elaborate program flow checks for ensuring the complete operation of deterministic random number generator.

- Software attacks

  - Replay attacks

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

  - Bypass authentication or access control

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

  - Direct protocol attacks

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

- 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.

Area

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

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 21: 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-20] “Application Notes and Interpretation of the Scheme (AIS), AIS 20: Functionality classes and evaluation methodology for deterministic random number generators”, Version 1, December 1999

[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 3, July 2009

[CC Part 2] "Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components", Version 3.1, Revision 3, July 2009

[CC Part 3] "Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components", Version 3.1, Revision 3, July 2009

[CC CEM] "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1, Revision 3, July 2009

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

Contactless Smartcard IC

Security Target RC-SA01/1 Series and RC-SA01/2 Series

Version 1.10: November 2012

Sony Corporation
FeliCa Business Division

No: A01-STP-E01-10