SONY®

FeliCa

IC Chip for Card

RC-S962/1

Composite Security Target

Public Version

Version 1.10

No. 962-STL-E01-10

Table of Contents

List of Tables

List of Figures

Definition of Terms

(Terms of TOE)

Smartcard:
Smartcard is a credit card sized plastic card that has a non-volatile memory and a processing unit embedded within it.

Contactless IC card:
This is one of IC card types having an antenna built in the IC card, and performs transmission / reception of data utilizing the electromagnetic field radiated from the external terminal.

FeliCa technology:
This is the Contactless IC card technology system developed by Sony Corporation, and Sony proprietary technology.
(Refer to Web site (http://www.sony.net/Products/felica/))

Controller:
An IT product that controls Smartcard via the Reader / Writer.

Reader / Writer:
An IT product that communicates with cards via radio frequency interface.

UART (Universal Asynchronous Receiver Transmitter):
The communication line used for a serial port etc.
The parallel signal sent out of a system is changed into a serial signal, or the serial signal conversely sent from peripheral equipment is changed into a parallel signal.

ROM (Read Only Memory):
This is a non-volatile type memory (to be used internal to the IC) that requires no supply of electrical power to maintain the data stored to it.

RAM (Random Access Memory):
A volatile-type memory device capable of random access (to be used internal to the IC) and requires supply of electrical power to maintain the data stored to it.

SRAM (Static Random Access Memory):
SRAM is a type of RAM that uses the flip-flop circuits as its memory elements.

FRAM (Ferroelectric Random Access Memory):
FRAM is a type of non-volatile memories manufactured utilizing the ferroelectrics substance.

OS (Operating System):
"Operation System" is the embedded software used for control of the Smartcard.

CRC (Cyclic Redundancy Check):
Cyclic Redundancy Check. "CRC" is one of methods for inspection whether transfer (or read / write) of the data was correctly performed or not during data transfer or data read from / write to memory.

Hash Code:
A fixed-size data generated by digest function (hash function) from variable-size data. It can be used as the methods detecting modification of data because it is infeasible to reverse original data from hash code and to find other data which generates same hash code.

Issue ID (IDi):
Identification data written when the Smartcard is issued.

Issue ID information
Information containing the Issue ID (IDi) and Issue Parameter (PMi) determined when issuing the Smartcard.

Issue Parameter (PMi):
Information written when the Smartcard is issued.

Manufacture ID (IDm):
A Smartcard-unique discrimination code written by the card manufacturer.

Manufacture ID Information:
Information containing the Manufacture ID (IDi) and Manufacture Parameter (PMm) written at the time of manufacturing a Smartcard.

Manufacture Parameter (PMm):
Written by the Smartcard manufacturer provides information on the functions and transfer characteristics of the card.

Mutual Authentication:
A process required for checking that the Smartcard and Reader/Writer have the same access key.

Package:
Encrypted data for registration of area / service and change of the area key / service key.

Package Key:
The key used for encrypting package.

Parity:
A message digest of communication data.

Parity of Package:
A message digest of package.

Patch Program:
Modification program written at the time of manufacturing a Smartcard.

Area:
The scheme used to enable hierarchical management of services and other areas.

Area0000:
The area in the highest layer.

Area0000 Key:
The key that authenticates the use of an Area0000.

Area Code:
A code to identify Area.

Area Definition Information:
The information that defines the scope of service codes, number of available user blocks and authorities granted to the card system administrator.

Area Key:
The key that authenticates the use of an Area.

Area Key Version:
Version of Area Key.

Area / Service Code List:
A list used to declare the right to use areas and/or services.

Area0000 Definition Information:
The information that defines the number of available user blocks and authorities granted to the Smartcard system administrator.

Authorised area list:
A list of areas that succeed mutual authentication.

Authorised service list:
A list of services that succeed mutual authentication.

Block:
A minimum unit of information used for writing and reading.

Service:
The method of accessing the memory of FeliCa system cards.

Service Code:
A code to identify Service.

Service Definition Information:
The information used to specify the access attribute, as well as the position and number of accessible user blocks, for a specific service.

Service Key:
The key that authenticates the use of a Service.

Service Key Version:
Version of Service Key.

Service Type:
An access method of a specific service.

System Definition Information:
Information containing the system code and system key determined when issuing a Smartcard.

System Key:
The key that authenticates the use of a Smartcard.

Transaction ID:
An ID of communication data. It is composed of random number generated in each mutual authentication and the number incremented in each transaction. It prevents from illegal access recycling communication data.

Transaction Key:
The key used for encrypting communication data. It is generated each time in mutual authentication.

User Block:
The block allocated in the memory using a specific service.

Access Key:
The key used for Mutual Authentication.

Access with Security:
Access which needs Mutual Authentication.

Access without Security:
Access which does not need Mutual Authentication.

Identification of User:
Identification of the user and his roles by TOE.

Identification of TOE:
Identification of TOE by user.

Personalisation:
Injecting data used for identify each Smartcard.
In this ST, personalisation is registering manufacture ID.

Personaliser:
Personaliser performs personalisation. The Card Manufacturer is assumed as the Personaliser.

Pre-personalisation:
Injecting data used for traceability and/or secure shipment between phases.

Smartcard Issuer:
Smartcard Issuer registers data necessary for cards to be used.

Card Manufacturer:
The customer who receives the IC (TOE) and manufactures cards. The card Manufacturer has the following roles.

(i) The Smartcard Product manufacture (Phase 4, 5)
(ii) The Personaliser (Phase 6)

DTV (Day Timer Vector):
DTV is used for generation of deterministic random numbers.

(Terms of Common Criteria)

Authorised User:
A user who may, in accordance with the TSP, perform an operation.
In this ST, a generic name of card manufacturer, card issuer, and card user.

External IT entity:
Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Guidance documentation:
Guidance documentation describes the delivery, installation, configuration, operation, management and use of the TOE as these activities apply to the users, administrators, and integrators of the TOE. The requirements on the scope and contents of guidance documents are defined in a PP or ST.

Human user:
Any person who interacts with the TOE.

Inter-TSF transfers:
Communicating data between the TOE and the security functions of other trusted IT products.
In this ST, communicating data between the TOE and authorised user.

Object:
An entity within the TSC that contains or receives information and upon which subjects perform operations.

Remote trusted IT product:
An IT product outside the TOE which is able to provide secure communication between TOE.

Role:
A predefined set of rules establishing the allowed interactions between a user and the TOE.

Security Attribute:
Characteristics of subjects, users, objects, information, and/or resources that are used for the enforcement of the TSP.

Security Function Policy, SFP:
The security policy enforced by an SF.

Security Function, SF:
A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security objective:
A statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions.

Subject:
An entity within the TSC that causes operations to be performed.

TOE Security Functions Interface, TSFI:
A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.

TOE security policy model:
A structured representation of the security policy to be enforced by the TOE.

TOE security Policy, TSP:
A set of rules that regulate how assets are managed, protected and distributed within a TOE.

Transfers outside TSF control:
Communicating data to entities not under control of the TSF.

Trusted channel:
A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.

Trusted path:
A means by which a user and a TSF can communicate with necessary confidence to support the TSP.

TSF Scope of Control, TSC:
The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

User:
Any entity (human user or external IT entity) outside the TOE that interacts with the TOE. In this ST, the user is the controller or the reader / writer that communicates with card.

Assets:
Asset means the information or the resource to be protected by countermeasures of TOE.

Dependency:
Dependency means the relationship between the requirements where the requirements of depended side shall be normally satisfied to accomplish the purpose of the requirements of depending side.

Environment stress:

Increasing loads to the environment in which the system operates, for example, applying abnormal voltage or abnormal temperature to the system

Extension (or Addition):

Extension (or Addition) means to add functional requirements not included in Part 2 of CC and / or assurance requirement not included in Part 3 of CC to ST or PP.

PP (Protection Profile):

PP means a set of security requirements that satisfy the needs of a specific user about a category of TOE independent from its implementation

SOF-Basic:

This is the strength of function level of TOE of which, as a result of analysis, the functions are recognized to have sufficient resistance against temporary invasions to TOE's security launched by attackers with low-level of attack potential.

SOF-Medium:

This is the strength of function level of TOE of which, as a result of analysis, the functions are recognized to have sufficient resistance against direct or intentional invasions to TOE's security launched by attackers with medium level of attack potential

SOF-High:

This is the strength of function level of TOE of which, as a result of analysis, the functions are recognized to have sufficient resistance against planned and / or organisational invasions to TOE's security launched by attackers with high level of attack potential.

ST (Security Target):

ST means a set of security requirements and specifications used as the clarified evaluation criteria of TOE.

SOF (Strength of Function):

SOF is the rating of security functions of TOE expressed by the minimum effort necessary to put the expected behavior of security functions illegal by launching direct attack against security mechanism in low-level of hierarchy.

TOE (Target of Evaluation):

TOE is the object of evaluation at the time of acquiring the certification.

TSF (TOE Security Functions):

TSF is a set of all the hardware, the software, and the firmware of TOE upon which accurate implementation of TSP should depend.

TSF Data:

This is the data created by TOE and the data created in relation with TOE that may affect the operation of TOE.

User data:

This is the data created by users and the data created in relation with the users that do not affect the operation of TSF.

User is Smartcard Product Manufacturer or Personaliser or Smartcard Issuer.

List of Abbreviations

API:	Application Program Interface
CBC:	Cipher Block Chaining
CC:	Common Criteria
CISC:	Complex Instruction Set Computer
CPU:	Central Processing Unit
CRYPTO:	Cryptographic
DES:	Data Encryption Standard
DFA:	Differential Fault Analysis
DPA:	Differential Power Analysis
DMA:	Direct Memory Access
SPA:	Simple Power Analysis
DEMA:	Differential Electro Magnetic Analysis
SEMA:	Simple Electro Magnetic Analysis
EAL:	Evaluation Assurance Level
ECB:	Electronic Code Book
HAL:	Hardware Abstraction Layer
IC:	Integrated Circuit
IT:	Information Technology
FRAM:	Ferroelectric Random Access Memory
I/F:	Interface
NIST:	National Institute of Standards and Technology
OS:	Operating System
PP:	Protection Profile
RAM:	Random Access Memory
RF:	Radio Frequency
RNG:	Random Number Generator
ROM:	Read Only Memory
SOF:	Strength of Function
SPA:	Simple Power Analysis
SRAM:	Static Random Access Memory
ST:	Security Target
TSF:	TOE Security Functions
TSFI:	TSF Interface
TOE:	Target of Evaluation
TSC:	TSF Scope of Control
TSP:	TOE Security Policy
UART:	Universal Asynchronous Receiver/Transmitter
DTV:	Day Timer Vector

(This page is intentionally left blank.)

1. ST Introduction

This is the Security Target for CC evaluation of IC Chip product RC-S962/1 as public version. Roles to be accomplished by this Security Target during the development and evaluation stages are as described in CC Version 2.3 and ISO/IEC 15408.

This Security Target is applicable to this product only.

1.1 ST and TOE Identification

ST Identification

Title of Security Target:	RC-S962/1 Composite Security Target
Version number:	1.10
Reference number:	962-STL-E01-10
Date of creation:	May 28, 2008
ST Author:	Sony Corporation

TOE Identification

Composite TOE

Product name:	RC-S962/1
Version:	1.0
Product type:	IC Chip for Contactless IC card

Configuration of composite TOE

TOE 1

Hardware name:	Smartcard Integrated Circuit CXD9916H3/MB94RS403, FR01 0001
IC Dedicated Software:	HAL Library Version 01

TOE 2

OS name:	FeliCa OS
OS version:	3.31
ROM version:	01

(There is no Patch Program.)

Guidance Document:

Document name	Revision
RC-S962 Series FeliCa OS Command Reference Manual	1.0
RC-S962 Series FeliCa OS Status Flag Manual	1.0
Security Reference Manual – Group Service Key & User Service Key Generation	1.00
Security Reference Manual – Mutual Authentication & Packet Cryptography	1.00
Security Reference Manual – Issuing Package Generation	1.00
Security Reference Manual – Changing Key Package Generation	1.00
FeliCa Card IC Security Operation Guidelines	1.0
FeliCa Card Rewriting Transport Key	1.1
RC-S962 Series Manufacture ID Writing Procedure	1.0
RC-S962 Series Inspection/Verification Procedure	1.0

CC identification: Common Criteria version 2.3 for Information Technology Security Evaluation
ST created by: Sony Corporation
Evaluation body: Thales CEACI
(Information components evaluation and analysis center)
Certification body: DCSSI (Central Information System Security Division)

1.2 ST Overview

This ST is the composite ST with the TOE of [CXD9916H3/MB94RS403 ST].
The intended TOE of this ST is the IC Chip product RC-S962/1 embedded to Contactless IC card conforming to FeliCa technology, and this TOE consists of Hardware and Software.
Hardware portion of the TOE is CXD9916H3/MB94RS403 (hereinafter referred to as "TOE1"), and Software portion of the TOE is the OS (hereinafter referred to as "TOE 2") operating on TOE1.
This TOE can be used for various types of applications including finance fields.
This TOE provides the security functions for protection of important data such as customer's information stored to the TOE from disclosure or modification.
The ST (a) provides a description of the TOE, (b) defines the security environment of the TOE during its different phases of the life cycle, (c) identifies the assets to be protected, the threats to be countered by the TOE or its environment, (d) describes the security objectives for the TOE and for its environment, (e) specifies the security requirements including TOE security functional requirements and TOE security assurance requirements, and (f) provides a summary specification of the TOE.

1.3 CC Conformance

This Composite Security Target is compliant with Common Criteria V2.3, and is Part2 extended (TOE 1 is Part2 extended and TOE 2 is Part2 conformant) and Part3 conformant.

The evaluation assurance level is EAL4.
This Composite Security Target does not conform to any protection profiles.
In addition, TOE1 conforms to [SSVG].
The evaluation assurance level of TOE1 is EAL4 Augmented (AVA_VLA.4, ADV_IMP.2, ALC_DVS.2, AVA_MSU.3).

1.4 Reference

[CC Part1] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001
(CC Part1: Common Criteria Part1)

[CC Part2] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002
(CC Part2: Common Criteria Part2)

[CC Part3] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003
(CC Part3: Common Criteria Part3)

[SSVG] Smartcard IC Platform Protection Profile, Version 1.0, BSI-PP-0002, July 2001

[ISO/IEC 18092] Information technology - - Telecommunications and information exchange between system - - Near Filed Communication - - Interface and Protocol (NFCIP-1)

[FIPS PUB 46-3] DATA ENCRIPTION STANDARD, Reaffirmed 1999 October 25

[FIPS PUB 81] Announcing the standard for DES MODES OPERATION, 1980 December 2

[AIS20] Functionality classes and evaluation methodology for deterministic random number generators, Version 1, 2 December 1999, BSI

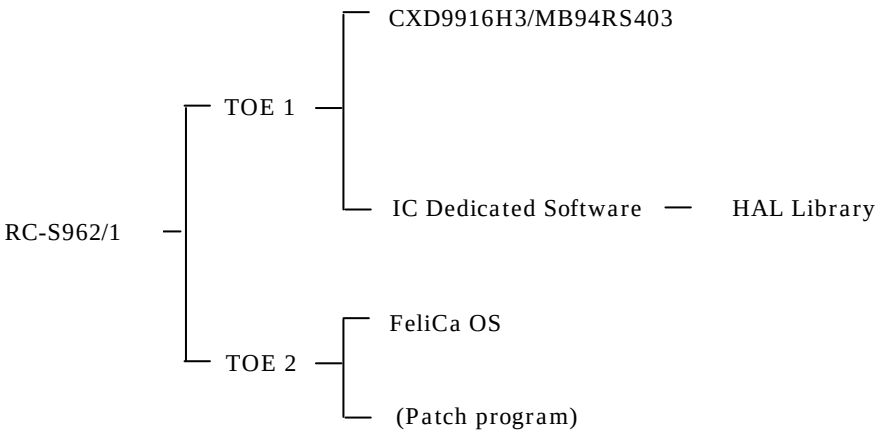
[AIS31] Functionality classes and evaluation methodology for physical random number generators, Version 1, 25 September 2001, BSI

[CXD9916H3/MB94RS403 ST] IC Platform of FeliCa Contactless Smartcard CXD9916H3 / MB94RS403 Security Target, Version 6, May 20th, 2008

2. TOE Description

2.1 Product type of TOE

This TOE is the IC Chip product RC-S962/1 embedded to Contactless IC card conforming to FeliCa technology, and the TOE consists of Hardware and Software.
TOE 1(Hardware of the TOE) is independently evaluated / certified to the evaluation assurance level of EAL4 Augmented. With the assumption mentioned above, Software portion of the TOE is the OS (TOE 2) necessary for providing control to the Hardware. The OS (TOE 2) is developed in accordance with the LSI specification and HAL Library specification.

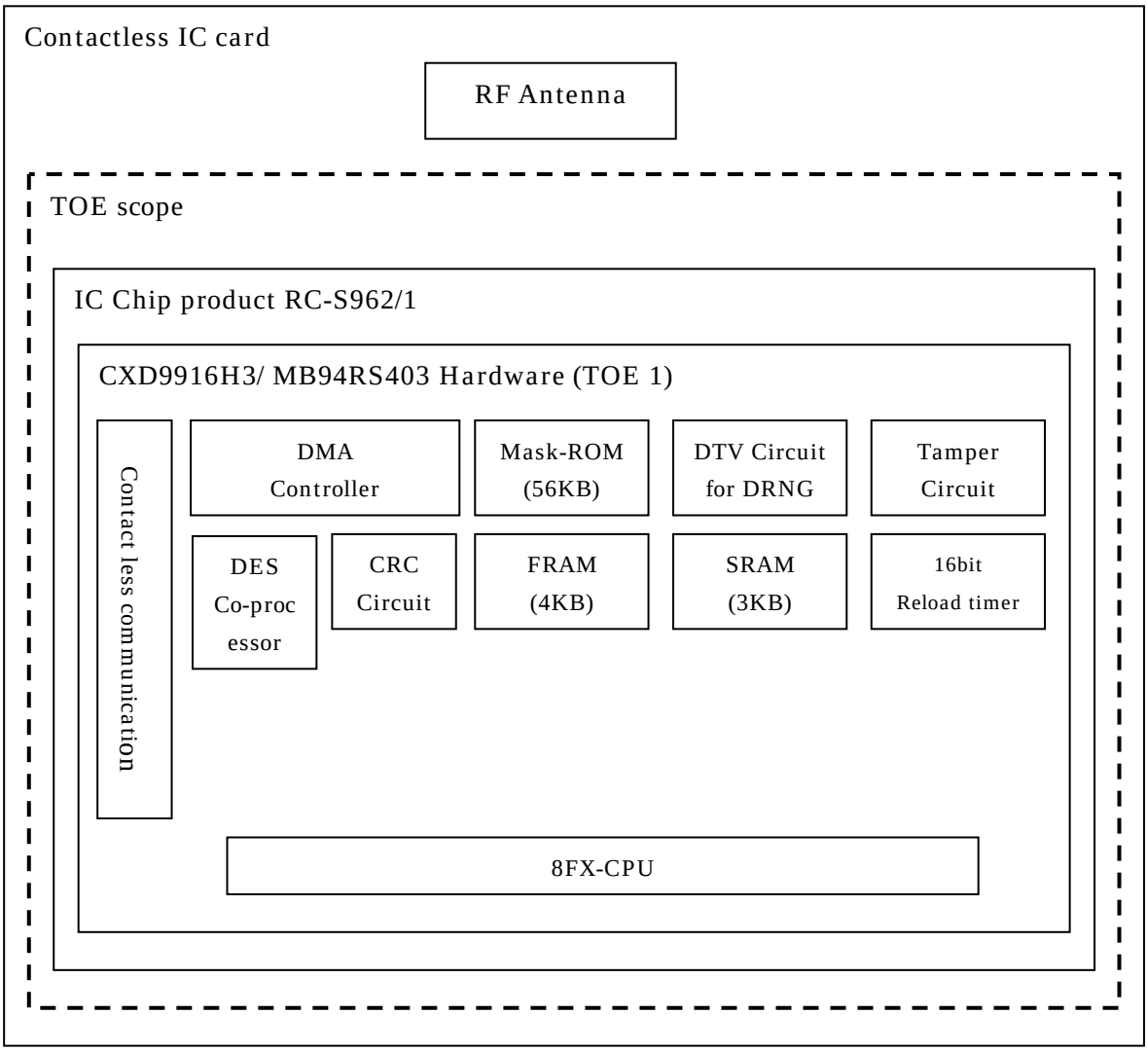


2.1.1 Physical scope of TOE

The physical scope of the TOE is as illustrated in Figure 2-1.

Figure 2-1 Physical scope of TOE

The physical range of TOE is the portion surrounded by the dotted line.



TOE 2 is stored in Mask-ROM.

CPU: Central Processing Unit
Mask-ROM: Mask Read Only Memory
FRAM: Ferroelectric Random Access Memory
SRAM: Static Random Access Memory
DES Coprocessor: Data Encryption Standard Coprocessor
DMA controller: Direct Memory Access controller
CRC Circuit: Cyclic Redundancy Check Circuit
DTV Circuit: Day Time Vector Circuit

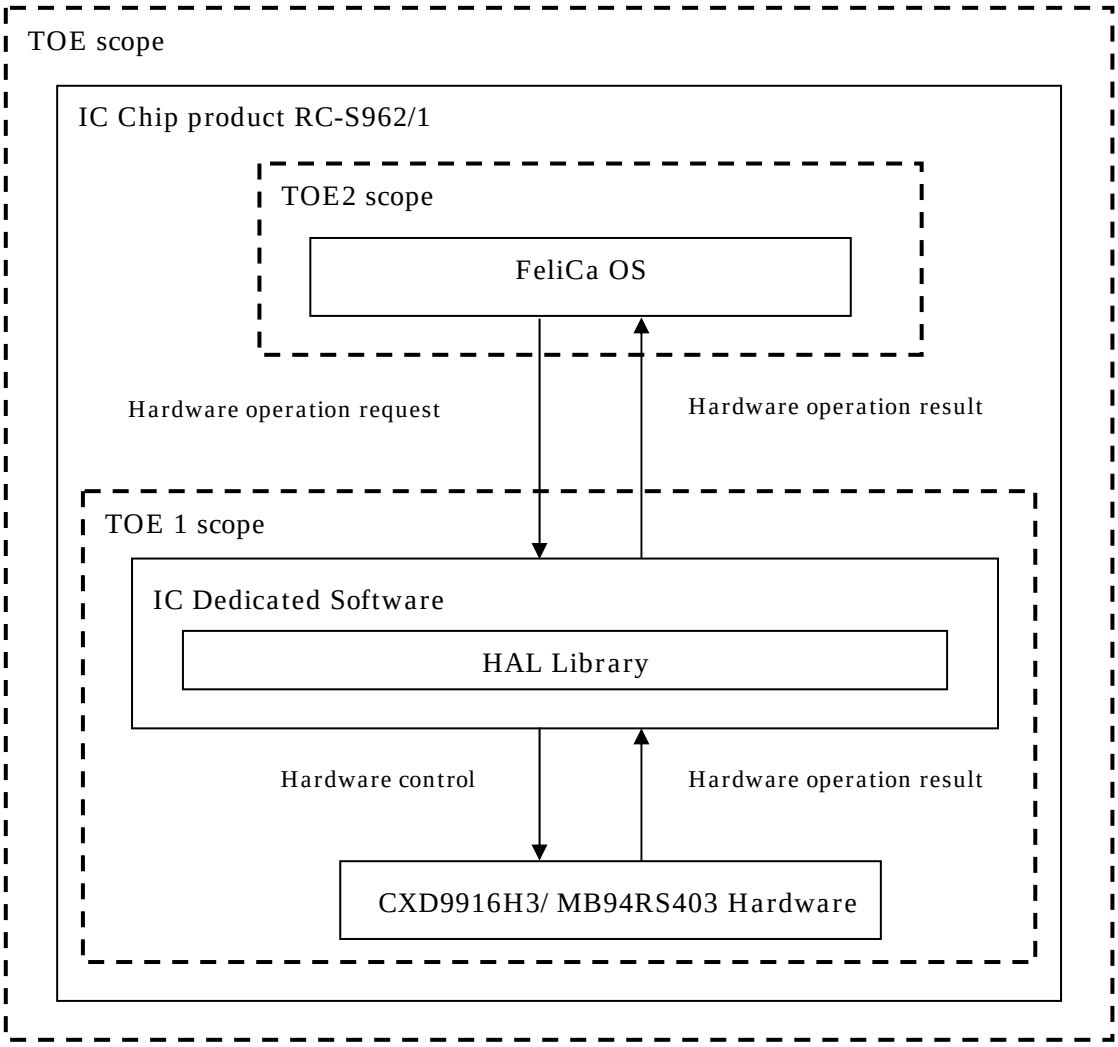
For the detail of CXD9916H3/ MB94RS403 Hardware (TOE 1), refer to “2.1 TOE Definition” in [CXD9916H3/MB94RS403 ST].

2.1.2 Logical scope of TOE

The logical scope of the TOE is as illustrated in Figure 2-2.

Figure 2-2 Logical scope of TOE

The logical range of TOE is the portion surrounded by the dotted line.



HAL: Hardware Abstraction Layer

HAL Library is a part of configuration of TOE 1, and developed by the developer of TOE 1.
HAL Library is saved to the Mask-ROM, and it has the function for TOE 2 to use Hardware of TOE 1 easily and securely.
HAL Library contains a function to operate a random number generator correctly. Its function is conformed to [AIS20], functionality class K3.

2.1.3 Functions of TOE 1

For the functions of TOE 1, refer to “2.1.1 Hardware Description”, “2.1.2 TOE Software Description” and “2.1.3 TOE Test Features” in [CXD9916H3/MB94RS403 ST].

2.1.4 Functions of TOE 2

Major functions of the TOE 2 are as enumerated below.

- Communication data flow control
- File access control
- File system management

(1) Communication data flow control

This function performs flow control to the communication data transmitted / received between the TOE and the Reader / Writer.

(2) File access control

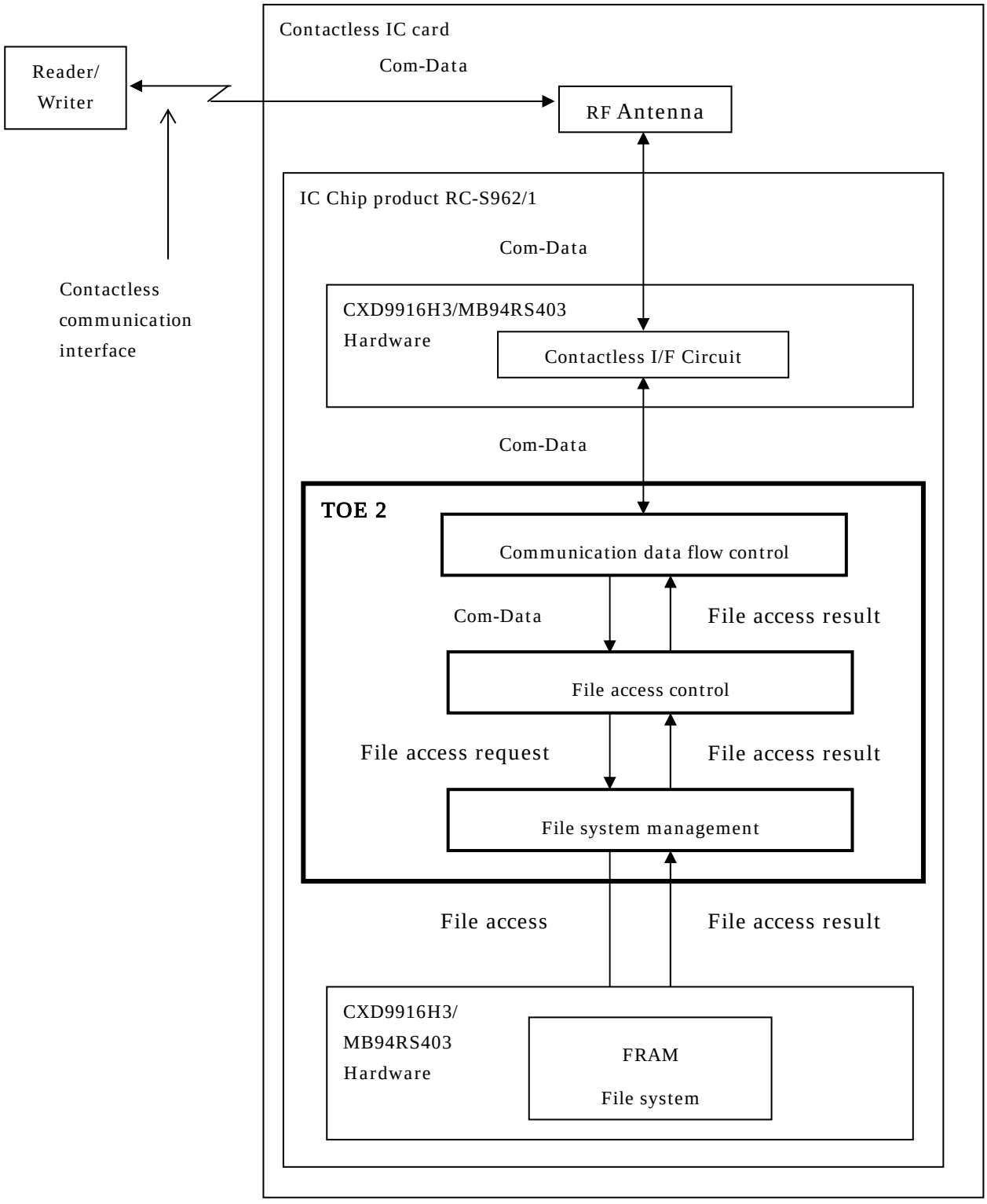
This function performs control to registration / read / write / deletion of files saved to FRAM in accordance with the access right.

(3) File system management

This function constructs the file system to FRAM, and performs management to the file system.

Functional configuration of the TOE 2 is as illustrated in Figure 2-3.

Figure 2-3 Functional configuration of the TOE 2

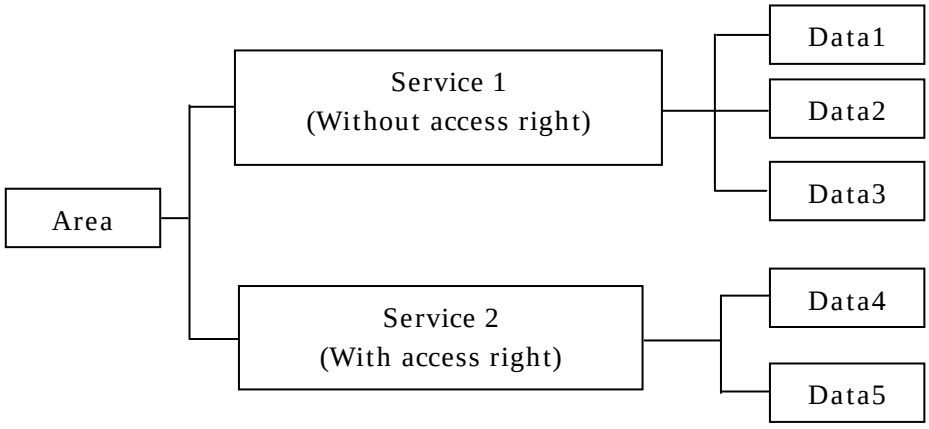


※ Com-Data: Communication data

2.1.5 File System

The TOE performs management to the multi-purpose data utilizing the file system.
The file system is hierarchically structured in accordance with “Area” and “Service”, and it is possible to provide protection to the secret data from illegal access by assigning the access right to each of Service.
An example of the file system structure is as illustrated in Figure 2-4.

Figure 2-4 Example of file system structure



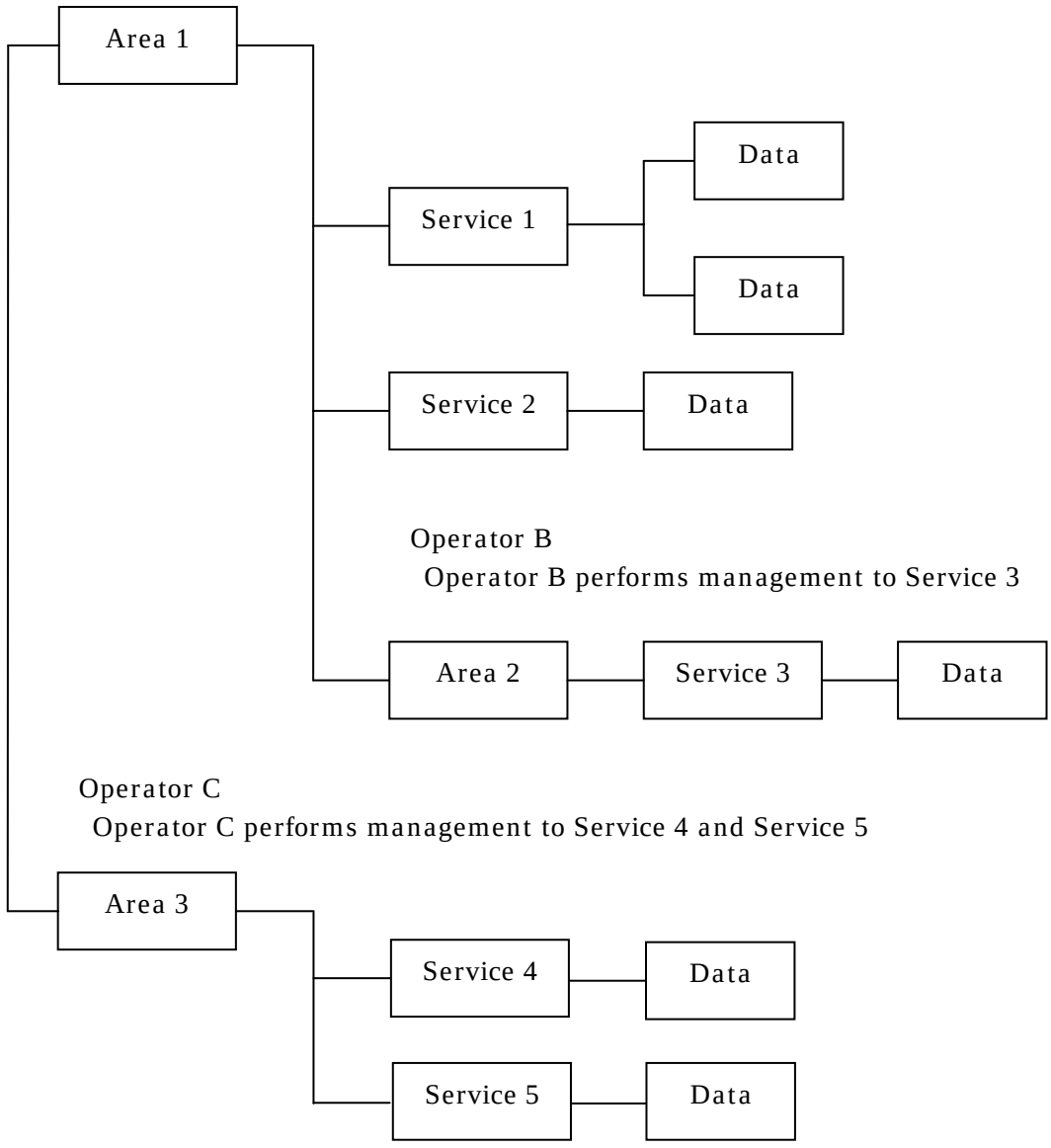
Access to "data 4" and "data 5" is allowed only to the personnel authorised so.

"Area" is assigned in operator-by-operator basis. The operator performs management to Service and Data within the scope of assigned area. It is also possible to set child Area(s) to an Area.
An example of management structure of Services is as illustrated in Figure 2-5.

Figure 2-5 Example of management structure of Services

Operator = Smartcard Issuer
In this example, Area 1 is assigned to Operator A, Area 2 is assigned to Operator B, and Area 3 is assigned to Operator C, respectively.

Operator A
Operator A performs management to Service 1, Service 2, and Area 2.



2.1.6 Documents

The user guidance documentation consists of following.

[M247]	RC-S962 Series FeliCa OS Command Reference Manual
[M294]	RC-S962 Series FeliCa OS Status Flag Manual
[SR]	Security Reference Manual
[M292]	FeliCa Card IC Security Operation Guidelines
[Tec01]	FeliCa Card Rewriting Transport Key
[M248]	RC-S962 Series Manufacture ID Writing Procedure
[M252]	RC-S962 Series Inspection/Verification Procedure

2.2 Life Cycle

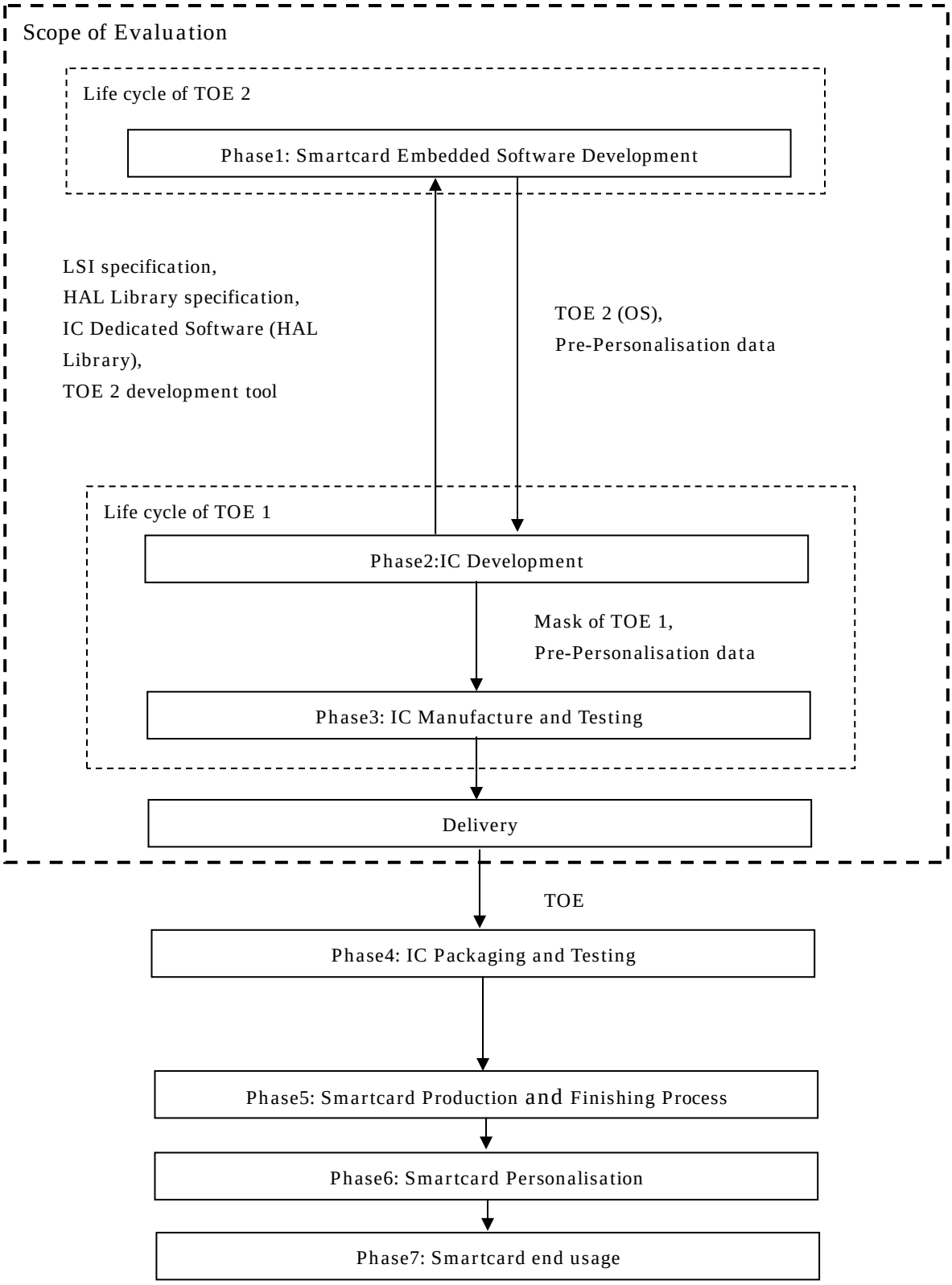
2.2.1 Life cycle of Contactless IC card

The life cycle of Contactless IC card can be divided into following 7 Phases. Out of these 7 Phases, Phase1 corresponds with the life cycle of TOE 2, and Phase2 and Phase3 correspond with the life cycle of TOE 1.

Phase1: Smartcard Embedded Software Development
Phase2: IC Development
Phase3: IC Manufacturing and Testing
Phase4: IC Packaging and Testing
Phase5: Smartcard Production and Finishing Process
Phase6: Smartcard Personalisation
Phase7: Smartcard end usage

The flow diagram of the life cycle of Contactless IC card is as illustrated in Figure 2-6.

Figure 2-6 Flow diagram of the life cycle of Contactless IC card



The overview of each phase of TOE life cycle is as shown in Table 2-1 below.

Table 2-1 Overview of each phase of the TOE life cycle

Phase	Work	Product	Related Personnel	Deliverables
Phase1: Smartcard Embedded Software Development	Design and Development of TOE 2.	TOE 2 (OS), TOE 2 design/development documents, User guidance documentation, Pre-Personalisation data	Designer / Developer of TOE 2	TOE 2(OS) (to Phase2)
	Testing of TOE 2.			
				Pre-Personalisation data (to Phase2)
Phase2: IC Development	Design and Development of TOE 1.	TOE 1 design/development documents, LSI specification, HAL Library specification, Mask data of TOE 1, IC Dedicated Software	IC developer (IC Designer)	LSI specification, HAL Library specification (to Phase1),
				IC Dedicated Software (HAL Library) (to Phase1)
				TOE 2 development tool (to Phase1)
				Pre-Personalisation data (to Phase3)
	Mask development of TOE.	Mask of TOE	Mask Developer	Mask of TOE (to Phase3)
Phase3: IC Manufacturing and Testing	Wafer manufacture of TOE	IC bare chip of TOE	IC Manufacturer	TOE (to Phase4)
	Testing Wafer of TOE			
	Write of the TOE 1 identification data			
	Write of the Initial seed for DRNG			
	Write of the Pre-Personalisation data			
	Cut of wafer to die of TOE			

Phase1: Smartcard Embedded Software Development

This Phase1, concerning to Design and Development of TOE 2 and Testing of TOE 2, is managed by Designer/Developer of TOE 2.

Design and Development of TOE 2(including pre-personalisation data) is performed on this phase. HAL Library, tools and guidance documentation for Design and Development of TOE 2 are delivered from IC developer to Designer/Developer of TOE 2 by secure means.
Designer/Developer of TOE2 develops TOE2 and he delivers TOE 2 (FeliCa OS and Pre-Personalisation data) to IC Designer (Phase 2) by secure means.

Phas2: IC Development

This Phase2, concerning to IC design, IC Dedicated Software and Mask development, is managed by IC developer (IC Designer).

In this phase, TOE 2 (OS ((written on Mask-ROM of CXD9916H3)) is transferred from Designer/Developer of TOE 2 (on Phase1) to IC developer by secure means, and is installed on Chip after compiling.

IC design includes a series of logical design, circuit design and layout design.

IC Dedicated Software means HAL (Hardware Abstraction Layer), which are developed by IC developer.

On Mask development, Mask data is delivered from IC designer to Mask manufacturer, which is Fujitsu's subcontractor, by secure means. Then, Mask is manufactured in the secure environment. Produced Mask is sent to IC manufacturer (on Phase3) by secure means.

Phase3: IC Manufacturing

This Phase3, concerning to Manufacturing/Testing/Delivery of Wafer of CXD9916H3 (developed by Fujitsu), is managed by IC Manufacturer.

In this phase, The Mask is delivered from Mask manufacturer by secure means and the wafers (IC chips) are securely manufactured in secure environment.

In the wafer testing, TOE 1 identification data (Chip manufacturing information) is written on specific FRAM area which is prohibited to write access. Also, initial seed that is used for the Deterministic Random Number Generator (DRNG) are injected to the TOE.

Pre-personalisation data that includes customer's confidential data is injected into the TOE at the testing.

After the wafer testing, bump is built up and wafer is diced.

At the end of the Phase3, Test features (including IC dedicated test software, test circuits and secure scan logic) are deactivated.

After Phase3, TOE (IC chips) is delivered to Smartcard Product manufacturer (Phase4 and followings) by secure means, since this Security Target covers from Phase1 to TOE Delivery after Phase3.

The overview of each Phase outside TOE life cycle is shown below.

（Phase4, Phase5）

These phases are outside the scope of TOE. In these phases, the smartcard is produced at a smartcard manufacturing facility.
These phases include IC packaging, testing module, and incorporation of module into the plastic card body, and the IC Packaging Manufacturer and the Smartcard Product Manufacturer are responsible for those things.
Smartcard Product Manufacturer is also called as “Card Manufacturer” in this ST.

（Phase6）

This phase is the final step necessary to prepare the smartcard for issue to users consists of personalisation of smartcard.
In this ST, Registration of Manufacture ID Information is defined as personalisation.
The Personaliser is responsible for the above things.
“Card Manufacturer” is assumed to have the role of the Personaliser.

（Phase7）

This phase is the end-user phase where the smartcard is issued to end-users for operational deployment.
The end-user phase contains also the end of life process of the smartcard, which is critical aspect in the life cycle.
The end-user consists of Card Issuer, Area Administrator, and Service User.
The Card Issuer is responsible for issuing card that means registration of the Issue ID Information, System Definition Information, and Area0000 Definition Information. He also has the capability to change the System Key and Area0000 Key.
The Area Administrator is responsible for registration of area and service definition information. He also has the capability to change the Area Key and Service Key.
The Service User has the capability to access (read and write) service.

2.2.2 Role and Responsibility of Authorised User

The role and responsibility of authorised user is as shown in Table 2-2 below.

Table 2-2 The Role of Authorised User

Role	Identification & Authentication	Responsibility
Card Manufacturer	Card Manufacturer is authenticated using System Key and Area0000 key.	
		Registration of Manufacture ID Information
Card Issuer	Card Issuer is authenticated using System Key and Area0000 Key	Registration of Issue ID Information
		Registration of System Definition Information
		Registration of Area0000 Definition Information
		Change of System Key
		Change of Area0000 Key
Area Administrator	Area Administrator is authenticated using Area key and Service Key. (Area Administrator manages specific Area.)	Registration of Area Definition Information
		Registration of Service Definition Information
		Change Area Key
		Change Service Key
Service User	Service User is authenticated using the access key to access specific Service. (Service User can access to the information in the Service)	Read Service
		Write Service
Authorised User	-	General name of above roles

2.3 Development Environment of TOE

2.3.1 Development Environment of TOE 1

For Development Environment of TOE 1, refer to “2.3 TOE Environment” in [CXD9916H3/MB94RS403 ST].

2.3.2 Development Environment of TOE 2

Development environment of the TOE 2 corresponds with Phase1 of the life cycle of Contactless IC card.
In the development environment of the TOE 2, following security measures are applied to maintain the integrity as well as the confidentiality of the TOE 2.

(1) Secure physical environment

- Design, development and testing of the TOE 2 are performed in a physically protected area(s), and entry to / exit from such area(s) are under the secure control of the entry / exit management system.

(2) Secure Network environment

- To prevent alteration or leakage of data, TOE 2 design / development document, TOE 2 itself and LSI specification, HAL Library specification, HAL Library as well as TOE 2 development tools are under the management of a secure computer system.

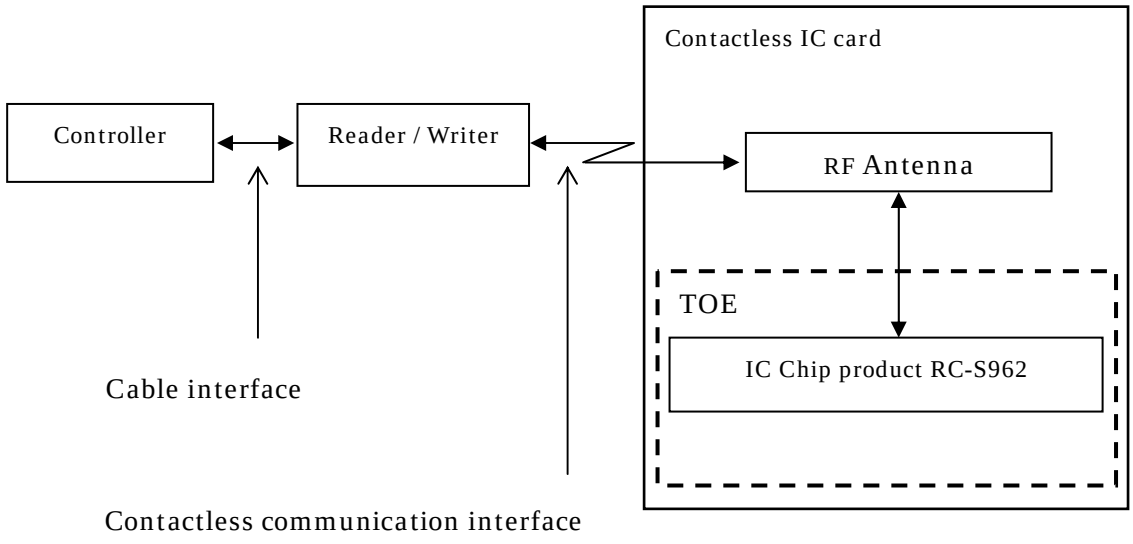
2.4 Manufacture Environment of TOE

For Manufacture Environment of TOE 1, refer to “2.3 TOE Environment” in [CXD9916H3/MB94RS403 ST].

2.5 System configuration of the intended use of TOE

The system configuration example of the intended use of TOE is as illustrated in Figure 2-7.

Figure 2-7 System configuration example of the intended use of TOE



(Controller)

The controller is the terminal used for providing control to the TOE via the Reader / Writer.

The controller may be in various forms such as "Issuance Terminal", "operating terminal", "automated ticket gate", "cash register", etc.

(Reader / Writer)

The Reader / Writer is located between the controller and the TOE, and issues request for access to the TOE in accordance with the instructions sent from the controller.

The Reader / Writer also supplies the electric power to the TOE.

The contactless communication interface conforms to [ISO/IEC 18092] Passive Communication Mode 212/424 kbps.

Mutual authentication of the TOE is performed between the TOE and the controller, or between the TOE and the Reader / Writer. It is assumed that, in some cases, a Host Controller is connected at a level in the system's hierarchy higher than the controller and mutual authentication is performed between the TOE and the Host Controller. Configuration of equipment external to the TOE depends upon the system configuration of customer, and it is out of the range of this evaluation.
In any cases, protection to the confidentiality and the integrity of communication data is provided to the communication signal transferred over the paths between the TOE and the equipment that succeeded in mutual authentication with the TOE.

2.6 Interface

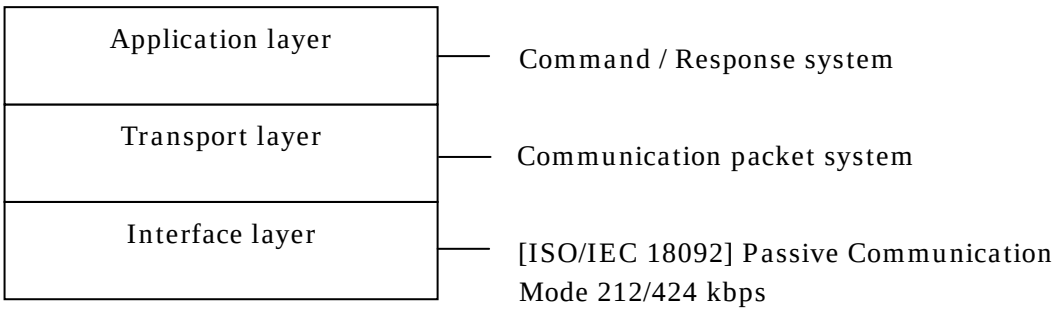
2.6.1 External Interface

(1) Physical Interface
Physical Interface is all the surfaces of the IC Chip.

(2) Electrical Interface
Electrical Interface is the external terminal pins of the IC Chip.

(3) Communication Interface
Communication Interface is the contactless communication interface between the TOE and the Reader / Writer.
Configuration of the contactless communication interface is as illustrated in Figure 2-8.

Figure 2-8 Contactless communication interfaces



Application Layer: This layer defines the system of access to the file system, etc. of the TOE. TOE 2 is responsible for this layer.

Transport Layer: This layer defines the transfer procedure of the communication data. TOE1 is responsible for this layer.

Interface Layer: The interface defines the physical and electrical characteristics of data transfer. TOE 1 is responsible for this layer.

2.6.2 Interface between TOE 1 and TOE 2

Interface between TOE 1 and TOE 2 is IC Dedicated Software (HAL Library).

2.7 TOE Intended Usage

Contactless IC card for communication purpose, which includes RC-S962/1, is intended to be used for financial settlement, personal identification and distribution service. For such purposes, Contactless IC card stores personal/monetary information, which requires the protection against leakage and tampering. Following list demonstrates the possible use of Smartcard.

Finance/Settlement purposes:
E-money card on pre-paid format and as credit card are imaginable

Identification purposes:
Personal identification/Company identification/Entry or Exit control are imaginable.

Distribution service purposes:
Point card/shopping card/amusement card are imaginable

For the uses above, Smartcard is expected to provide the security features and to be used effectively in various purposes to improve the service for users.

2.8 TOE IT Security Features

2.8.1 TOE 1 IT Security Features

For TOE 1 IT Security Features, refer to “2.4.2 TOE IT Security features” in [CXD9916H3/MB94RS403 ST].

2.8.2 TOE 2 IT Security Features

In order to protect the confidentiality and integrity of assets, TOE 2 provides the following security features.

(1) Access control against illegal access
(2) Sequence control against illegal access
(3) Protection to Confidentiality of Communication data
(4) Protection to Integrity of Communication data
(5) Protection to Integrity of Internal data

3. TOE Security Environment

Chapter 3 describes various aspects of the assets, the assumptions, as well as the threats of the TOE in relation with the security of (a) intended operating environment of the TOE, and (b) the mode of TOE use within such operating environment.

3.1 Assets

The assets to be protected by TOE are defined as the "Primary Assets.
The assets located external to the TOE and to be protected by TOE environment are defined as the "Secondary Assets" of the TOE. The Secondary Assets of the TOE include the data to be managed external to the TOE as well as the documents related with the TOE.

3.1.1 Primary Assets of TOE

The Primary Assets are classified into the "User data", the "TSF data" and “Software”. Table 3-1 below shows the list of Primary Assets of the TOE.

Table 3-1 Primary Assets List of TOE

Information name	User data	TSF data	Software
User information	X		
System information		X	
Smartcard Embedded Software			X
IC Dedicated Software			X
Pre-Personalisation data		X	
Transaction Key		X	

The integrity of all primary assets and confidentiality of User data, Software and some kind of TSF data such as key shall be protected.

Communication data transmitted between TOE and a Controller is also defined as assets because the following information is included in communication data.

(User data)
User information
(TSF data)
System information, Transaction Key

(1) User information

This is the information of the user of Contactless IC card, and under the management of System information.
The user information is always saved to FRAM.

(2) System information

This is the information necessary for management of the file system, and it consists of the following types of information.

- Manufacture ID information
- Issue ID information
- System definition information
- Area0000 definition information
- Area definition information
- Service definition information

(3) Smartcard Embedded Software

TOE 2 (OS)

This information is always saved to ROM.

(4) IC Dedicated Software

HAL Library

This information is always saved to ROM.

(5) Pre-Personalisation data

Pre-Personalisation data is data required for construction of the file system after IC Chip shipment.

This information is always saved to FRAM.

Note: Pre-Personalisation data is first secondary asset and become primary asset when it is injected into the TOE (end of phase 3).

(6) Transaction Key

Transaction Key is used for encryption of the communication data after a mutual authentication success.

This information is saved to SRAM.

3.1.2 Secondary Assets of TOE

Secondary Assets consist of the data located external to the TOE as well as the documents related with the TOE. Moreover, the TOE itself is contained in Secondary Assets.
The list of Secondary Assets in each Phase is shown below.

(Phase 1: Smartcard Embedded Software Development)

- TOE 2 design/development documents (refer to “6.3.2 Assurance Measures for TOE 2”)
- Administrator / User guidance documentation (refer to “6.3.2 Assurance Measures for TOE 2”)
- TOE 2 development tool
- TOE 2 test program
- TOE 2 (FeliCa OS)
- Pre-Personalisation data
- LSI specification, HAL Library specification
- IC Dedicated Software (HAL Library)

(Phase 2: IC Development)

- TOE 1 design/development document (refer to “6.3.2 Assurance Measures for TOE 1”)
- LSI specification, HAL Library specification
- TOE 1 development tool
- TOE 1 test program
- TOE 1 (CXD9916H3/MB94RS403 Hardware and IC Dedicated Software)
- TOE 2 (OS)
- Pre-Personalisation data
- Mask data of TOE
- Mask of TOE

(Phase 3: IC Manufacturing and Testing)

- Mask of TOE
- Wafer manufacture tool
- Wafer test program
- Wafer of TOE
- Pre-Personalisation data

(Phase 4 to 7)

- Administrator / User guidance documentation

3.2 Assumptions

This section describes the various types of assumptions about (a) the intended operating environment of the TOE, and (b) the intended mode of TOE use

A.Process-Card Protection during Packaging, Finishing and Personalisation

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

A.Sec_Remote Remote Trusted IT Product Secure

It is assumed that the Remote Trusted IT Product with which the Contactless IC card establishes the secure link is to be secure.

The Remote Trusted IT Product shall have the capability to establish the secure communication channel with the Contactless IC card. It is assumed that when secure communication channel is established; the Remote Trusted IT Product is adequately secure for trusted communications.

A.Ident Identification

It is assumed that the personaliser registers unique identifier to each copy of the TOE.

User data in the TOE may be controlled with the controller that controls the TOE. To perform the control to each copy of TOE, it shall be possible to uniquely identify (i.e., different from others) each of TOEs.

3.3 Threats

The TOE is required to cope with the various types of threats as classified in following sections.

3.3.1 Threats of TOE 1

For the threats of TOE 1, refer to “3.3 Threats” in [CXD9916H3/MB94RS403 ST].

3.3.2 Threats of TOE 2

3.3.2.1 Illegal Access

(1) Data disclosure by illegal access

T.Access_Disclose Disclose by Illegal Access

Attackers may disclose confidentiality data (User data, TSF data) in the TOE by illegal access.

Attackers may disclose confidentiality data (User data, TSF data) in the TOE by launching illegal access to the TOE.
As the attack methods, illegal operation of the system terminal or illegal operation with a falsified terminal is assumed.

(2) Data Modification by illegal access

T.Access_Modi Modification by Illegal Access

Attackers may modify integrity data (User data, TSF data) in the TOE by illegal access to the TOE.

Attackers may modify integrity data (User data, SF data) in the TOE by launching illegal access to the TOE.
As the attack methods, illegal operation of the system terminal or illegal operation with a falsified terminal is assumed.

(3) Replay attack

T.Replay_Data Replay Data

Attackers may disclose or modify data (User data, TSF data) by recycling the previously valid communication data and launching illegal access to the TOE.

Attackers may launch illegal access to the TOE by recycling the data acquired by monitoring of the data of communication between the TOE and the terminal.
As the attack method, re-play attack of the communication data is assumed.

3.3.2.2 Threat of Communication data

(1) Disclosure of communication data

T.Disc_ComData Disclose Communication Data

Attackers may disclose confidentiality communication data.

Attackers may perform monitoring and analysis of the communication data transferred between the TOE and the Authorised User to disclose confidentiality data (User data, TSF data).

As the attack technique, monitoring of the communication data utilizing data analyzers is assumed.

(2) Modification/Destruction of communication data

T.Modi_Dest_ComData Modify/Destroy Communication Data

Attackers may modify or destroy communication data whose integrity shall be protected.

Attackers may modify or destroy data (User data, TSF data) transferred between the TOE and the Controller.

As the attack technique, man in the middle attack and radio disturbance are assumed.

Modify: intended modification of data (i.e. data is changed)

Destroy: unintended modification of data (i.e. data is damaged)

3.3.2.3 Destruction of Data

(1) Destruction of data by power down

T.Power Power Down

Attackers may destroy integrity data (User data, TSF data) in the TOE by power down to the Contactless IC card.

Attackers may destroy integrity data (User data, TSF data) in FRAM by power down to the Contactless IC card.
As the attack technique, the power down of the Reader / Writer while performing data-write to FRAM is assumed (the Contactless IC card is supplied the electric power from the Reader / Writer).

(2) Destruction of data by application of high temperature stress

T.High_Temp_St High Temperature Stress

Attackers may destroy the data (User data, TSF data) to be the object of integrity in the TOE by applying high temperature stress.

Attackers may destroy the data (User data, TSF data) to be the object of integrity in FRAM by applying high temperature stress.

3.4 Organisational Security Policies

The TOE shall comply with the organisational security policy expressed in following paragraphs:

3.4.1 Organisational Security Policies of TOE 1

For the Organisational Security Policies of TOE 1, refer to “3.4 Organizational Security” in [CXD9916H3/MB94RS403 ST].

3.4.2 Organisational Security Policies of TOE 2

(1) Design of TOE 2

P.Plat_Appl Usage of Hardware Platform

The Smartcard Embedded Software (TOE 2) is designed so that the requirements from the following documents are met:

(i) LSI specification, HAL Library specification of CXD9916H3 and the hardware application notes,

(ii) Findings of the TOE 1 evaluation reports relevant for the Smartcard Embedded Software.

P.Key_Function Usage of Key-dependent Functions

Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software (TOE 2) in a way that they are not susceptible to leakage attacks .

P.Reg_ID Register Identification

The Smartcard Embedded Software (TOE 2) shall be designed to provide the personaliser with a means to register identification to identify each TOE uniquely.

(2) Process of TOE 2

P.Process-TOE 2 Protection during TOE 2 Development and Production

Because the Secondary Assets in TOE 2 development environment (Phase1) may be the sources of information for cloning of the TOE 2, such data/documents shall be saved in a secure environment and managed by the authorised user.

Also, TOE 2 and Secondary Assets shall be delivered from TOE 2 development environment (Phase1) by a secure method.

4. Security Objectives

4.1 TOE Security Objectives

The TOE shall conform to the security objective described in detail in the following sections.

4.1.1 TOE Security Objectives of TOE 1

For the TOE Security Objectives of TOE 1, refer to “4.1 Security Objectives for the TOE” in [CXD9916H3/MB94RS403 ST].

4.1.2 TOE Security Objectives of TOE 2

4.1.2.1 Measures to Cope with Illegal Access

(1) Mutual Authentication

O.Mutual_Auth Mutual Authentication

To provide protection to the confidentiality and the integrity of data (User data, TSF data) from illegal access by unauthorised user, the TOE and the controller shall succeed in mutual authentication between them before issuing permission to the controller for access to the user information with security or the system information in the TOE.

(2) Access Control

O.Data_Acc Data Access Control

TOE 2 shall provide protection from the following matters.

(1) Illegal access making use of forged or previously valid authentication data.
(2) Disclosure and modification of user data in the TOE by illegal access.
(3) Disclosure and modification of TSF data in the TOE by illegal access.

As the measures to cope with illegal access, the TOE 2 shall have the security function to provide protection to integrity and confidentiality of the data (the User Data, TSF Data) in the TOE.
As the measures to cope with illegal access, the identification/authentication of User and the access control is assumed.

(3) Measures to cope with Replay Attack

O.Replay_Protection Protection against Replay

The TOE 2 shall provide protection to confidentiality data (User data, TSF data) and integrity data (User data, TSF data) from Replay Attacks launched utilizing the previously valid communication data.

As the measures to cope with Replay Attacks, the TOE 2 shall have the security function to detect Replay Attacks and deny the access.
As the measures to cope with Replay Attacks, the sequence control to communication data is assumed.

4.1.2.2 Measures to Cope with Threat of Communication data

(1) Measures to cope with disclosure of transmission data

O.Enc_ComData Encryption of Communication data

The TOE 2 shall provide protection to the confidentiality of data transmitted by the TOE to the Controller, or vice versa.

As the measures to cope with the monitoring of data, the TOE 2 shall have the security function to provide protection to the confidentiality of data transmitted by the TOE to the Controller, or vice versa.
As the measures to cope with data disclosure, encryption of the transmission data is assumed.

(2) Measures to cope with modification/destruction of communication data

O.ComData_Check Communication Data Check

The TOE 2 shall provide protection to the integrity of the communication data transferred between the TOE and the Controller.

The TOE 2 shall have the security function to provide protection to the integrity of the communication data transferred between the TOE and the Controller.
As the measures to cope with data destruction, (a) attach of parity to the communication data at the time of data transfer, and (b) parity check to the communication data in receiving data are assumed.

4.1.2.3 Measures to Cope with Data Destruction

(1) Measures to cope with destruction of data caused by power loss

O.Power Power Loss Recovery

The TOE 2 shall provide protection to integrity data (User data, TSF data) from the power loss, and shall maintain the TOE in its secure state.

The TOE 2 shall have the security function for prevention of destruction of integrity data (the User data, TSF data) in FRAM, and maintains the TOE in its secure state.
As the measures to cope with the power loss, (a) Atomic function when the TOE writes data to FRAM, and (b) CRC check and recovery to the file system information when the power is turned ON to the Contactless IC card.

(2) Measures to cope with destruction of data caused by High temperature stress

O.TOEdata_Valid TOE data Validity

TOE 2 shall provide the data that can be used as the evidence for assurance of validity of the data in the TOE.

TOE 2 shall have the security function to provide the data that can be used as the evidence for assurance of validity of the data stored the FRAM.

O.TOEdata_Check TOE data Check

TOE 2 shall be able to check the integrity of data in the TOE, and shall preserve a secure state of TOE when integrity error is detected.

TOE 2 shall be equipped with the security function capable to check the integrity of data stored to FRAM and to preserve a secure state of TOE.

4.1.2.4 Measures to Register Identification

(1) Measures to register identification

O.Reg_ID Register Identification

The TOE 2 shall provide the personaliser with a means to be uniquely identified.

The TOE 2 shall have the security function for registering the manufacture ID.

4.2 Security Objectives for Environment

4.2.1 Security Objectives for Environment of TOE 1

For the Security Objectives for Environment of TOE 1, refer to “4.2 Security Objectives for Environment” in [CXD9916H3/MB94RS403 ST].

4.2.2 Security Objectives for Environment of TOE 2

4.2.2.1 IT Security

This sub-section describes the IT security objectives to be satisfied by imposing technical requirement(s) to the TOE environment. The security objectives mentioned above are those that requested by the ST set to the TOE environment. These security objectives are included in the ST as necessary to support the security objective of the TOE.

(1) Measure for secure communication

OE.Sec_Remote Remote Trusted IT Product Secure Communication

The Remote Trusted IT Product shall provide a trusted channel for secure communication with the TOE.

4.2.2.2 Non-IT Security

This sub-section describes the non-IT security objectives to be satisfied without imposing technical requirements to the TOE. That is, these non-IT security objectives do not require achievement of hardware functions or software functions. By addressing the security problems set to the TOE environment by these security objectives, the non-IT security objectives are included in the ST as necessary.

(1) Usage of Hardware Platform

OE.Plat_Appl Usage of Hardware Platform

To ensure that TOE 1 is used in a secure manner the Smartcard Embedded Software (TOE 2) shall be designed so that the requirements from the following documents are met;

(i) LSI specification, HAL Library specification of CXD9916H3 and the hardware application notes,
(ii) Findings of the TOE 1 evaluation reports relevant for the Smartcard Embedded Software

(2) Design of TOE 2

OE.key_Function Usage of key-dependent Functions

Key-dependent functions of the Smartcard Embedded Software (TOE 2) shall be implemented in a way that they are not susceptible to leakage attacks .

(3) Process of TOE 2

OE.Process-TOE 2 Protection during TOE 2 Development and Production

The non-IT environment shall provide the secure management for the Secondary Assets, and the secure methods of delivery for the TOE 2 and the Secondary Assets.
Also, the Designers/developers of TOE 2 and the delivery personnel shall be carefully selected based upon their reliability, and shall be educated on an information security management system.

(4) Measure for unique identification of the TOE

OE.Ident TOE Identification

For unique identification of the TOE, the personaliser shall register the unique manufacture ID for the TOE.

(5) After TOE Delivery

OE.Process-Card Protection during Packaging, Finishing and Personalisation

Security procedures shall be used after TOE Delivery up to delivery to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).
This means that Phases after TOE Delivery up to the end of Phase 6 (refer to Section 2.2) must be protected appropriately.

5. IT Security Requirements

5.1 TOE Security Requirements

5.1.1 TOE Functional Requirements of TOE 1

For the TOE Functional Requirements of TOE 1, refer to “5.1.1 TOE Functional Requirements” in [CXD9916H3/MB94RS403 ST].

5.1.2 TOE Functional Requirements of TOE 2

This section explains the Security Functional Requirements of TOE 2.
Following Security Functional Requirements are derived from CC Part2.

Table 5-1 TOE Security Functional Requirements of TOE 2

Functional Component ID	SFR Name	Operation
FIA_ATD.1	User attribute definition	Assignment
FIA_UID.1	Timing of identification	Assignment
FIA_UAU.1	Timing of authentication	Assignment
FIA_UAU.3	Unforgeable authentication	Selection
FIA_UAU.4	Single-use authentication mechanisms	Assignment
FIA_USB.1	User-subject binding	Assignment
FCS_CKM.1.A	Cryptographic key generation	Assignment
FCS_COP.1.A	Cryptographic operation	Assignment
FMT_SMR.1	Security roles	Assignment
FDP_ACC.1	Subset access control	Assignment
FDP_ACF.1	Security attribute based access control	Assignment
FMT_MTD.1.A	Management of TSF data	Selection Assignment
FMT_MTD.1.B	Management of TSF data	Selection Assignment
FMT_MTD.1.C	Management of TSF data	Selection Assignment
FMT_MTD.1.D	Management of TSF data	Selection Assignment
FMT_SMF.1	Specification of Management Functions	Assignment
FTP_ITC.1	Inter-TSF trusted channel	Assignment
FCS_CKM.1.B	Cryptographic key generation	Assignment
FCS_COP.1.B	Cryptographic operation	Assignment
FPT_RPL.1	Replay detection	Assignment
FPT_RCV.4	Function recovery	Assignment
FDP_SDI.2	Stored data integrity monitoring and action	Assignment
FDP_DAU.1	Basic data authentication	Assignment

Threats: T.Access_Disclose, T.Access_Modi

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:
[*Area Code*, *Service Code*].

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [*Identification of TOE, Access of Service without Security, Verify Operation*] 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-medicated actions on behalf of that user.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [*Identification of TOE, Access of Service without Security, Verify Operation*] 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.

Refinement 1 on FIA_UID.1 and FIA_UAU.1
There are following information as identification information of TOE.
IDm, PMm, System Code, Area Code, Service Code
Refinement 2 on FIA_UID.1 and FIA_UAU.1
Identification of user is performed by the list of Area codes and Service codes by which the Authentication Request is carried out.

FIA_UAU.3 Unforgeable authentication

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

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

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [*the Authentication mechanism in FeliCa Technology employed for the mutual authentication with the controller*].

FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*list of Area Code and Service Code*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*List of Area Code and Service Code shall be associated with subject*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*none*].

Application Note on FIA_USB.1

The access key is generated from system key, area keys and service keys.

FCS_CKM.1.A Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Access key generation method*] and specified cryptographic key sizes [*112 bits*] that meet the following: [*FeliCa Technology*].

FCS_COP.1.A Cryptographic operation

FCS_COP.1.1 The TSF shall perform [*encryption / decryption of data*] in accordance with a specified cryptographic algorithm [*Triple Data Encryption Standard (Triple DES)*] and cryptographic key sizes [*112 bits*] that meet the following: [*[FIPS PUB 46-3]*].

Application Note on FCS_COP.1.A

FCS_COP.1.A describes cryptographic operation of mutual authentication.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [*Card Manufacturer, Card Issuer, Area Administrator, Service User*].

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

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [***Access Control Policy***] on [***subjects: Authorised User; object: User Block; operations: (1) Write, (2) Read***].

Application Note on FDP_ACC.1:

"Block" is a minimum unit of information used for writing and reading.
"User Block" is the block allocated in the memory using a specific service.
"Authorised User" means a user whose mutual authentication has succeeded. (See the related roles at Table 2-2.)

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [***Access Control Policy***] to objects based on the following [
Subjects: Authorised User;
Objects: User Block;
Security attributes of subjects: Authorised Service list
Security attributes of objects: (1) Service Code, (2) Service Type, (3) Number of Block
]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled object is allowed:
[***(1) The service code of the User Block requested by the Authorised User shall be included into its Authorised Service list.***
(2) A read or write operation on a User Block requested by the Authorised User is permitted at the following conditions, based upon the security attributes of the service of which the User Block is depending: (a) the operation requested is one of the access mode authorized by Service Type; (b) the User Block to be accessed is in the range defined by Number of Block".]

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [***none***].

Application Note on FDP_ACF.1.3 and 1.4

The TSF does not have addition or exceptions to the rules defined in FDP_ACF.1.1 and 1.2.

FMT_MTD.1.A Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [*register*] the [*Manufacture ID information, Issue ID information, System definition information, Area 0000 definition information*] to [*Card Manufacturer or Card Issuer*].

FMT_MTD.1.B Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [*register*] the [*Area definition information, Service definition information*] to [*Area Administrator*].

FMT_MTD.1.C Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [*modify*] the [*System Key, System Key Version, Area0000 Key, Area0000 Key Version*] to [*Card Manufacturer or Card Issuer*].

Application Note on FMT_MTD.1.C

TSF does not distinguish Card Manufacturer and Card Issuer.Their distinction is managed by the operation.

FMT_MTD.1.D Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [*modify*] the [*Area Key, Area Key Version, Service Key, Service Key Version*] to [*Area Administrator*].

Application Note on FMT_MTD.1.A and FMT_MTD.1.B

Out of the information that configures System definition information, Area0000 definition information, Area definition information, and Service definition information, it is possible to change the key and the key version. The change function is provided by FMT_MTD.1.C and FMT_MTD.1.D.

FMT_SMF.1 Specification of Management Functions

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

(1) Registration of the Manufacture ID information,
(2) Registration of the Issue ID information, System definition information and Area 0000 definition information
(3) Registration of the Area definition information and Service definition information,
(4) Modification of the System Key, System Key Version, Area0000 Key and Area0000 Key Version,
(5) Modification of the Area Key, Area Key Version, Service Key and Service Key Version

].

Threats: T.Disc_ComData, T.Modi_Dest_ComData, T.Replay_Data

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*Access to user data or TSF data in TOE*].

Application Note on FTP_ITC.1

The protection against disclosure is ensured with a cryptographic means, and the protection against modification is ensured with parity check.

Threats: T.Disc_ComData

FCS_CKM.1.B Cryptographic key generation

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

FCS_COP.1.B Cryptographic operation

FCS_COP.1.1 The TSF shall perform [*encryption / decryption of data*] in accordance with a specified cryptographic algorithm [*Data Encryption Standards (DES)*] and cryptographic key sizes [*56 bits (DES)*] that meet the following: [*[FIPS PUB 46-3]*].

Threats: T.Replay_Data

FPT_RPL.1 Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [*Input communication data*].

FPT_RPL.1.2 The TSF shall perform [*Abandonment of the processing of the replayed entity*] when replay is detected.

Threats: T.Power

FPT_RCV.4 Function recovery

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

Threats: T.High_Temp_St

FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for [*Accidental modification or Intentional modification*] on all objects, based on the following attributes: [*CRC of the data stored in FRAM*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [*inform the error status to the user*].

Threats: T.High_Temp_St, T.Access_Modi

FDP_DAU.1 Basic data authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [*Patch Program in FRAM, and parameter data in FRAM that TOE 2 use*].

FDP_DAU.1.2 The TSF shall provide [*Authorised User*] with the ability to verify evidence of the validity of the indicated information.

5.1.3 TOE Security Assurance Requirements

5.1.3.1 TOE Security Assurance Requirements of TOE 1

For The TOE Security Assurance Requirements of TOE 1, refer to “5.1.2 TOE Assurance Requirements” in [CXD9916H3/MB94RS403 ST].

5.1.3.2 TOE Security Assurance Requirements of TOE 2

This section explains the security assurance requirements of TOE 2.
The assurance level for TOE2 is EAL4. In the table below, the security assurance requirements of EAL4 extracted from Part 3 of CC are enumerated.
The minimum strength of security functions for the TOE2 is SOF-Basic (Strength of Functions Basic). However, the TOE2 does not equipped with security functions that are realised by a probabilistic or permutational mechanism.

Table 5-2 TOE Security Assurance Requirements of TOE 2

Assurance component ID	Assurance Requirement Name
ACM_AUT.1	Partial CM automation
ACM_CAP.4	Generation support and acceptance procedures
ACM_SCP.2	Problem tracking CM coverage
ADO_DEL.2	Detection of modification
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.2	Fully defined external interfaces
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.1	Subset of the implementation of the TSF
ADV_LLD.1	Descriptive low-level design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Informal TOE security policy model
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: High-level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_MSU.2	Validation of analysis
AVA_SOF.1	Strength Of TOE security functional evaluation
AVA_VLA.2	Independent vulnerability analysis

5.2 Security Requirements for Environment

5.2.1 Security Requirements for IT Environment

Table 5-3 Security Requirements for IT Environment

Functional component ID	SFR Name	Operation	Strength Of Functions
FTP_ITC.1	Inter-TSF trusted channel	Assignment	

A.Sec_Remote

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*Access of the data in TOE*].

5.2.2 Security Requirements for the Non-IT Environment

In this section, security requirements for the non-IT-environment are described according to [BSI-PP-0002, Section 5.2.2].

In the following security requirements for the Non-IT-Environment are defined for the Smartcard Packaging, Finishing and Personalisation (Phases after TOE Delivery up to Phase 7).

The responsible parties for the Phases 4-6 are required to support the security of the TOE by appropriate measures:

RE.Process-Card Protection during Packaging, Finishing and Personalisation

The Card Manufacturer (after TOE Delivery up to the end of Phase 6) shall use adequate security measures to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

6. TOE Summary Specification

This chapter describes the security functions provided by the TOE to achieve the conformance to the "security functional requirements to the TOE" as specified in Chapter 5. "IT Security Requirements". Labels are attached to each of security functions to facilitate the reference with the specific functions.

6.1 TOE Security Functions of TOE 1

For the TOE Security Functions of TOE 1, refer to “6.1 TOE Security Functions” in [CXD9916H3/MB94RS403 ST].

6.2 TOE Security Functions of TOE 2

Table 6-1 TOE Security Functions for TOE 2 relevant to TOE Security Functional Requirements for TOE 2

TOE Security Functions for TOE 2	TOE Security Functional Requirements for TOE 2 (Functional Component ID)
SF.1 Access Control	FIA_ATD.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.3, FIA_UAU.4, FIA_USB.1, FCS_COP.1.A, FMT_SMR.1, FDP_ACC.1, FDP_ACF.1, FMT_MTD.1.A, FMT_MTD.1.B, FMT_MTD.1.C, FMT_MTD.1.D, FMT_SMF.1
SF.2 Sequence Control	FPT_RPL.1
SF.3 Protection to Confidentiality of Communication Data	FCS_CKM.1.A, FCS_CKM.1.B, FCS_COP.1.B, FTP_ITC.1
SF.4 Protection to Integrity of Communication Data	FTP_ITC.1
SF.5 Protection to Integrity of Internal Data	FPT_RCV.4, FDP_SDI.2, FDP_DAU.1

Table 6-2 TOE Security Functions for TOE 2 relevant to TOE Security Objective for TOE 2

TOE Security Functions for TOE 2	TOE Security Objective for TOE 2
SF.1 Access Control	O.Mutual_Auth
	O.Data_Acc
SF.2 Sequence Control	O.Replay_Protection
SF.3 Protection to Confidentiality of Communication Data	O.Enc_ComData
	O.ComData_Check
SF.4 Protection to Integrity of Communication Data	O.ComData_Check
SF.5 Protection to Integrity of Internal Data	O.Power
	O.TOEdata_Check
	O.TOEdata_Valid

SF.1: Access Control

SF.1-1: Identification of User

At the time of mutual authentication, the TOE performs identification of the controller based upon the list of the area codes and the service codes to which the controller requested authentication.

The security functional requirement to be satisfied:

FIA_UID.1, FMT_SMR.1

SF.1-2: Mutual Authentication

When the controller tried to access to the user information with security or to the system information located in the TOE, the TOE performs mutual authentication with the controller utilizing the access key.
Mutual authentication is implemented in a manner that the controller encrypts random number and the TOE decrypts it, and vice versa. Triple DES with 2 keys compliant with FIPS PUB 46-3 is used for encryption and decryption of random number.
The encryption / decryption key is called access key which is generated based upon the system key, the area key and the service key.
The security attributes of controller (i.e. list of area code and service code) is associated with the TOE at the end of this process.
The controller is recognized as authorized user after successful mutual authentication.
The following operations are permitted before successful mutual authentication: identification of TOE, access to service without security, and verify operation.

The security functional requirement to be satisfied:
FIA_ATD.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.3, FIA_UAU.4, FIA_USB.1, FCS_COP.1.A, FMT_SMR.1

SF.1-3: Access control to User information

To provide the Authorised User with capability for access to the permitted area, the TOE provides the access control function.
The TOE issues permission for access to the user information from the controller only when the following conditions are satisfied:

(1) The TOE and the controller has previously succeeded in mutual authentication performed by SF.1-2 for the areas and services to be the object of the access request from the controller (after the successful mutual authentication completed, the controller becomes the Authorised User).

(2) The service that corresponds with the service code requested by the controller actually exists.
(3) The access mode sent from the controller matches with the service type in the service definition information that controls the user information.
(4) The user information to which the controller requested access actually exists in the TOE.

The security functional requirement to be satisfied:
FIA_ATD.1, FMT_SMR.1, FDP_ACC.1, FDP_ACF.1

SF.1-4: Registration of Area/Service

The TOE provides only the Authorised User (Area Administrator) with the registration function of area or service.
The TOE issues permission for registration of area service requested by the controller when the following conditions are satisfied:

(1) The TOE and the controller has previously succeeded in mutual authentication performed by SF.1-2 (after successful mutual authentication completed, the controller becomes the Authorised User).
(2) The area service registration information sent from the controller is packaged with the correct package key which is known only by Area Administrator.

Note: The Area Administrator is authorised by TOE if the package key he used is equal to TOE's one. Package key is unique for each area.

The security functional requirement to be satisfied:
FMT_SMR.1, FMT_MTD.1.B, FMT_SMF.1

SF.1-5: Key Change

The TOE provides only the Authorised User (Card Manufacturer, Card Issuer or Area Administrator) with the key information change function for the system key, area0000 key, area key or the service key.
The TOE issues permission for change of the key information requested by the controller when the following conditions are satisfied:

(1) The TOE and the controller has previously succeeded in mutual authentication performed by SF.1-2 for system / area / service to be the object of key change (after successful mutual authentication completed, the controller becomes the Authorised User).

(2) The key change information sent from the controller is packaged with the correct package key which is known only by Card Issuer or Area Administrator.

Note: System key and Area0000 key are managed by Card Issuer and area keys and service keys are managed by its Area Administrator. They are authorised by TOE if the package key they used is equal to TOE's one. Package key is unique for each area (including system and area0000).

The security functional requirement to be satisfied:
FMT_SMR.1, FMT_MTD.C, FMT_MTD.D, FMT_SMF.1

SF.1-6: Registration of Manufacture ID

The TOE provides only the Card Manufacturer or the Card Issuer with the registration function of manufacture ID.
The TOE issues permission for registration of manufacture ID when the following conditions are satisfied:

(1) The TOE and the controller has previously succeeded in mutual authentication performed by SF.1-2 (after successful mutual authentication completed, the controller becomes the Authorised User).
(2) The manufacture ID registration information sent from the controller is packaged with the correct package key which is known only by the Card Manufacturer or the Card Issuer.(only for registration of manufacture ID)
(3) The manufacture ID has not been registered.

Note: After the registration of manufacture ID, this function is disabled. Therefore, only the Card Manufacturer can perform registration of manufacture ID if he perform this operation before passing the TOE to the Card Issuer.

The security functional requirement to be satisfied:
FMT_SMR.1, FMT_MTD.A, FMT_SMF.1

SF.1-7: Registration of Issue ID, System and Area0000

The TOE provides only the Card Manufacturer or the Card Issuer with the registration function of issue ID, system and area 0000.
The TOE issues permission for registration of issue ID, system and area 0000 requested by the controller when the following conditions are satisfied:

(1) The TOE and the controller has previously succeeded in mutual authentication performed by SF.1-2 (after successful mutual authentication completed, the controller becomes the Authorised User).
(2) The registration information sent from the controller is packaged with the correct package key which is known only by the Card Manufacturer or the Card Issuer.

Note: Only the Card Manufacturer or the Card Issuer knows keys and package keys for issue ID, system, and area0000. Therefore, this function can be performed only by the Card Manufacturer or the Card Issuer.

The security functional requirement to be satisfied:
FMT_SMR.1, FMT_MTD.A, FMT_SMF.1

SF.2: Sequence Control

"Sequence Control" is the function for prevention of illegal access to the TOE by Replay Attack utilizing the previously valid communication data.
After the successful mutual authentication completed, the TOE performs collation of the transaction ID attached to the communication data sent from the controller with the transaction ID internal to the TOE. In the case where the value of transaction ID attached to the communication data is incorrect, the TOE rejects the request of access to the user information and the file system information.
When the TOE transmits response data to controller, it increments the sequence number of transaction ID which received from the controller and attaches the incremented transaction ID to response data.

The security functional requirements to be satisfied:
FPT_RPL.1

SF.3: Protection to Confidentiality of Communication Data

This function performs the following processes to provide protection to the confidentiality of the communication data transferred between the TOE and the controller.

SF.3-1: Data Encryption Key Generation

The timing for generating various types of data encryption key is as shown below:

(Access Key)

Access key is generated each time when performed mutual authentication according to the requirement FCS_CKM.1.A.

(Transaction Key)

Transaction key is generated from random number each time at successful mutual authentication according to the requirement FCS_CKM.1.B.

The security functional requirement to be satisfied:
FCS_CKM.1.A, FCS_CKM.1.B

SF.3-2: Encryption/Decryption of the communication data

(In transmitting the communication data)

After the mutual authentication completed

The TOE performs encryption (DES, CBC mode) to the communication data with the transaction key according to the requirement FCS_COP.1.B.

(In receiving the communication data)

After the mutual authentication completed

The TOE performs decryption (DES, CBC mode) to the communication data with the transaction key according to the requirement FCS_COP.1.B.

The security functional requirements to be satisfied:
FCS_COP.1.B, FTP_ITC.1

SF.4: Protection to Integrity of Communication Data

This function is used to perform the following processes to provide protection to the integrity of the communication data transferred between the TOE and the controller.

(In transmitting the communication data)

The TOE attaches parity (these data is calculated based on the communication data) to the communication data to generate the communication data packet, and transmits the communication data packet to the controller.

(In receiving the communication data)

When received a communication data packet from the controller, the TOE calculates parity based upon the communication data contained in the communication data packet, and performs collation of the parity thus calculated with the parity contained in the communication data packet.

When it is found that the parity thus calculated coincides with the parity contained in the communication data packet as a result of collation mentioned above, the TOE accepts the communication data. If not, the communication data is discarded.

The security functional requirements to be satisfied:

FTP_ITC.1

SF.5: Protection to Integrity of Internal Data

This function is used to perform the following process to provide protection to the integrity of the user information and the file system information saved to FRAM.

SF.5-1: Atomic Updating of FRAM Data

FRAM data is updated with atomic updating function in order to guarantee the integrity of the data even if the writing procedure is interrupted.

At the start-up of the TOE, this function performs CRC check to the file system information saved to FRAM, and if CRC error is detected, this function restores the file system information to its secure state.

If the file system information cannot be restored to secure state, the TOE enters the state that access to the user data is inhibited.

The security functional requirements to be satisfied:

FPT_RCV.4

SF.5-2: Check to the data in FRAM at read / write of data

(Data read)

At the time of reading data stored to FRAM, performs CRC check to the data to be the object of data read.

TOE informs error status to the user when CRC error is detected.

(Data write)

At the time of writing data to FRAM, reads the written data out of FRAM and performs CRC check.

TOE informs error status to the user when CRC error is detected.

Security functional requirements to be satisfied: FDP_SDI.2

SF.5-3: Check to Validity of Data in FRAM

This security function provides the user (Smartcard Product Manufacturer, Personaliser, Smartcard Issuer) with the capability to check the validity of data in FRAM utilizing the hash code.

The security functional requirements to be satisfied: FDP_DAU.1

Calculation of CRC is performed in conformity with the standard algorithm of CCITT CRC-16.

6.3 Assurance Measures

6.3.1 Assurance Measures for TOE 1

For the Assurance Measures for TOE 1, refer to “6.2 Assurance Measures” in [CXD9916H3/MB94RS403 ST].

6.3.2 Assurance Measures for TOE 2

In this section, the applicable assurance requirements to satisfy EAL4 for TOE 2 assurance requirements in Part 3 of CC as well as the documents to satisfy it are enumerated.

Table 6-3 Assurance Measures for TOE 2 (1/6)

SAR ID	Assurance Requirement Name	Document	
		Name	Version
ACM_AUT.1	Partial CM automation	Quality Document Process	5.0
ACM_CAP.4	Generation support and acceptance procedures	RC-S962 Configuration Management Plan	1.01
ACM_SCP.2	Problem tracking CM coverage	RC-S962 Management Configuration List	1.10
		ClearCase Introduction Support Program Operation Procedure	1.90
ADO_DEL.2	Detection of modification	Product Delivery Specification	3
		Material Delivery Specification	4
		RC-S962 IC Delivery Rules	1.20
		RC-S962 Document Delivery Rules	1.00
ADO_IGS.1	Installation, generation, and start-up procedures	RC-S962 Series Inspection/Verification Procedure	1.0
		RC-S962 Series Manufacture ID Writing Procedure	1.0
ADV_FSP.2	Fully defined external interfaces	RC-S962 Function Specifications	1.01

Table 6-3 Assurance Measures for TOE 2 (2/6)

SAR ID	Assurance Requirement Name	Document	
		Name	Version
ADV_HLD.2	Security enforcing high-level design	RC-S962 High Level Design (Overview)	1.00
		RC-S962 High Level Design (Kernel Subsystem)	1.00
		RC-S962 High Level Design (Activation Subsystem)	1.00
		RC-S962 High Level Design (Commnad Dispatcher Subsystem)	1.00
		RC-S962 High Level Design (State Management Subsystem)	1.00
		RC-S962 High Level Design (SRM Subsystem)	1.00
		RC-S962 High Level Design (File System Subsystem)	1.00
		RC-S962 High Level Design (Command Subsystem)	1.00
		RC-S962 High Level Design (Basin Libray Subsystem)	1.00
		RC-S962 High Level Design (MISC Subsystem)	1.00
ADV_IMP.1	Subset of the implementation of the TSF	Source Code	01 (ROM Version)

Table 6-3 Assurance Measures for TOE 2 (3/6)

SAR ID	Assurance Requirement Name	Document	
		Name	Version
ADV_LLD.1	Descriptive low-level design	RC-S962 Low Level Design (Kernel Sub-system)	1.00
		RC-S962 Low Level Design (Acivation Sub-system)	1.00
		RC-S962 Low Level Design (Command Dispatcher Sub-system)	1.00
		RC-S962 Low Level Design (State Management Sub-system)	1.00
		RC-S962 Low Level Design (SRM Sub-system)	1.00
		RC-S962 Low Level Design (File System Sub-system)	1.00
		RC-S962 Low Level Design (Command Sub-system)	1.00
		RC-S962 Low Level Design (Basin Sub-system)	1.00
		RC-S962 Low Level Design (MISC Sub-system)	1.00
		RC-S962 Low Level Design (Data Definition)	1.00
ADV_RCR.1	Informal correspondence demonstration	RC-S962 Representation Correspondence	1.00
ADV_SPM.1	Informal TOE security policy model	RC-S962 Security Policy Model	1.00

Table 6-3 Assurance Measures for TOE 2 (4/6)

SAR ID	Assurance Requirement Name	Document	
		Name	Version
AGD_ADM.1	Administrator guidance	Security Reference Manual -Group Service Key & User Service Key Generation	1.00
		Security Reference Manual -Mutual Authentication & Packet Cryptograhy	1.00
		Security Reference Manual -Issuing Package Generation	1.00
		Security Reference Manual -Changing Key Package Generation	1.00
		RC-S962 Series Command Reference Manual	1.0
		RC-S962 Series FeliCa OS Status Flag Reference	1.0
		FeliCa Card IC Security Operation Guidelines	1.0
		FeliCa Card Rewiting Transport key	1.1
AGD_USR.1	User guidance	RC-S962 Series Command Reference Manual	1.0
		Security Reference Manual -Group Service Key & User Service Key Generation	1.00
		Security Reference Manual -Mutual Authentication & Packet Cryptograhy	1.00
		Security Reference Manual -Issuing Package Generation	1.00
		Security Reference Manual -Changing Key Package Generation	1.00
ALC_DVS.1	Identification of security measures	FeliCa Business Center Information Security Policy	June 18, 2007
		RC-S962 DVS Gate City Osaki	1.00
		RC-S962 DVS Toyosato	1.00
ALC_LCD.1	Developer defined life-cycle model	RC-S962 Lifecycle Model	1.00

Table 6-3 Assurance Measures for TOE 2 (5/6)

SAR ID	Assurance Requirement Name	Document	
		Name	Version
ALC_TAT.1	Well-defined development tools	RC-S962 Development tool Definition	1.00
		FR/F2MC FAMILY SOFTUNE CANALYZER MANUAL for V3	-
		FR/F2MC FAMILY SOFTUNE C CHECKER MANUAL for V3	-
		F2MC-8L FAMILY 8-BIT MICROCONTROLLER EMBEDDED C PROGRAMMING MANUAL for fcc896	
		F2MC-8L FAMILY 8-BIT MICROCONTROLLER PROGRAMMING MANUAL	-
		F2MCTM-8L/8FX FAMILY SOFTUNETM ASSEMBLER MANUAL for V3	-
		F2MCTM-8L/8FX FAMILY 8-BIT MICROCONTROLLER SOFTUNETM C COMPILER MANUAL	-
		F2MCTM-8L/8FX FAMILY SOFTUNETM LINKAGE KIT MANUAL for V3	-
		F2MCTM-8L/8FX FAMILY SOFTUNETM WORKBENCH COMMAND REFERENCE MANUAL	-
		F2MCTM-8L/8FX FAMILY SOFTUNETM USER'S MANUAL	-
		F2MCTM-8L/8FX FAMILY SOFTUNETM WORKBENCH OPERATIONMANUAL	-

Table 6-3 Assurance Measures for TOE 2 (6/6)

SAR ID	Assurance Requirement Name	Document	
		Name	Version
ATE_COV.2	Analysis of coverage	RC-S962 Test Coverage Analysis	1.00
ATE_DPT.1	Testing: High-level design	RC-S962 Test Depth Analysis	1.00
ATE_FUN.1	Functional testing	RC-S962 Test Specification	1.00
		RC-S962 Test Procedure	1.00
		RC-S962 Test Report	1.00
ATE_IND.2	Independent testing – sample	TOE	01 (ROM Version)
AVA_MSU.2	Validation of analysis	RC-S962 Misuse Analysis	1.00
AVA_SOF.1	Strength Of TOE security functional evaluation	RC-S962 SOF Analysis	1.00
AVA_VLA.2	Independent vulnerability analysis	RC-S962 Vulnerability Analysis	1.00
		Protocol Vulnerability Analysis Sony FeliCa Technology	1.10
		Potential Vulnerabilities List Sony FeliCa Smart Card	1.00

7. PP Claims

There is no PP (Protection Profile) to which this ST conforms.

8. Rationale

8.1 Security Objective Rationale

This chapter demonstrates that both the security objectives and the environmental security objectives of the TOE are adequately selected, and that these security objectives conform to all the identified threats and all the assumptions.

8.1.1 Adequacy of Security Objectives for Assumptions

<Relation with Assumptions>

Table 8-1 Assumptions relevant to Security Objectives for Environment of TOE 2

Assumptions	Security Objectives for Environment
A.Sec_Remote	OE.Sec_Remote
A.Ident	OE.Ident
A.Process-Card	OE.Process-Card

Table 8-2 Security Objectives for Environment of TOE 2 relevant to Assumptions

Security Objectives for Environment of TOE 1	Assumptions
OE.Sec_Remote	A.Sec_Remote
OE.Ident	A.Ident
OE.Process-Card	A.Process-Card

Since **OE.Process-Card** requires the Card Manufacturer to implement those measures assumed in **A.Process-Card**, the assumption is covered by this objective.

A.Sec_Remote indicates the assumption that the Remote Trusted IT Product is provided with the capability to perform the secure communication with the TOE. **OE.Sec_Remote** provides the capabilities ensuring to establish a trusted communication link for the secure communication between the Remote Trusted IT Product and the TOE, and to use the communication link.

A.Ident indicates that the TOE shall be clearly, completely, and uniquely identified. **OE.Ident** makes the reference to this to ensure the personaliser that identification of the TOE is executed in such a manner.

Since **OE.Process-Card** requires the Card Manufacturer to implement those measures assumed in **A.Process-Card**, the assumption is covered by this objective.

8.1.2 Adequacy of Security Objectives for Threats

8.1.2.1 Adequacy of Security Objectives for Threats of TOE 1

For the Adequacy of Security Objectives for Threats of TOE 1, refer to “8.1 Security Objectives Rationale” in [CXD9916H3/MB94RS403 ST].

8.1.2.2 Adequacy of Security Objectives for Threats of TOE 2

<Relation with Threats>

Table 8-3 Threats relevant to TOE Security Objective for TOE 2

Threats		TOE Security Objective of TOE 2
Illegal Access	T.Access_Disclose	O.Mutual_Auth
		O.Data_Acc
	T.Access_Modi	O.Mutual_Auth
		O.Data_Acc
		O.TOEdata_Valid
	T.Replay_Data	O.Replay_Protection
Threat of Communication data	T.Disc_ComData	O.Enc_ComData
	T.Modi_Dest_ComData	O.ComData_Check
Destruction of Data	T.Power	O.Power
	T.High_Temp_St	O.TOEdata_Check
		O.TOEdata_Valid

Table 8-4 TOE Security Objective for TOE 2 relevant to Threats

TOE Security Objective of TOE 2		Threats
Measures to Cope with Illegal Access and Cloning	O.Mutual_Auth	T.Access_Disclose
		T.Access_Modi
	O.Data_Acc	T.Access_Disclose
		T.Access_Modi
	O.Replay_Protection	T.Replay_Data
Measures to Cope with Threat of Communication data	O.Enc_ComData	T.Disc_ComData
	O.ComData_Check	T.Modi_Dest_ComData
Measures to Cope with Data Destruction	O.Power	T.Power
	O.TOEdata_Check	T.High_Temp_St
	O.TOEdata_Valid	T.Access_Modi
		T.High_Temp_St

T.Access_Disclose is the threat intending the disclosure of confidentiality data in the TOE.
O.Mutual_Auth and **O.Data_Acc** cope with this threat.
O.Mutual_Auth implements the mutual authentication between the TOE and the controller when the controller tried to access to the user information with security or to the system information in the TOE.
O.Data_Acc provides protection to the confidentiality of data by performing the operation defined in the access control security policy.

T.Access_Modi is the threat intending the modification of integrity data in the TOE.
O.Mutual_Auth, O.Data_Acc and **O.TOEdata_Valid** cope with this threat.
O.Mutual_Auth implements the mutual authentication between the TOE and the controller when the controller tried to access to the user information with security or to the system information in the TOE.
O.Data_Acc provides protection to the integrity of data by performing the operation defined in the access control security policy.
O.TOEdata_Valid generates the data that can be used as the evidence for assurance of validity of the data stored the FRAM.

T.Replay_Data is the threat intending the disclosure or falsification of data by recycling previously valid communication data.
O.Replay_Protection copes with this threat.
This security objective provides protection to the confidentiality and the security of data internal to the TOE by performing the sequence control to the data transferred over the communication channel.

T.Disc_ComData is the threat intending the disclosure of the communication data being transferred over the communication channel.
O.Enc_ComData copes with this threat.
This security objective provides protection to the confidentiality of the communication data by performing encryption to the data transferred over the communication channel.

T.Modi_Dest_ComData is the threat intending modification or destruction of communication data existed on the communication paths.
O.ComData_Check copes with this threat.
This security objective provides protection to the integrity of communication data by detecting any modification or destruction of the communication data.

T.Power is the threat intending the destruction of data saved to FRAM by power-down to the TOE.
O.Power copes with this threat.
This security objective provides protection to the integrity of the data saved to FRAM and maintains the TOE in its secure state by performing (a) CRC check to the data saved to FRAM at the time of power-ON to the TOE, and (b) Atomic function after

detection of CRC error of the data saved to FRAM.

T.High_Temp_St is the threat intending the destruction of data saved to FRAM by High Temperature Stress to the TOE.
O.TOEdata_Valid and **O.TOEdata_Check** cope with this threat.
O.TOEdata_Valid generates the data that can be used as the evidence for assurance of validity of the data stored the FRAM.
O.TOEdata_Check checks the integrity of data stored to FRAM, and preserves a secure state of TOE.

8.1.3 Adequacy for Organisational Security Policies

8.1.3.1 Adequacy for Organisational Security Policies of TOE 1

For the Adequacy of Organisational Security Policies of TOE 1, refer to “8.1 Security Objectives Rationale” in [CXD9916H3/MB94RS403 ST].

8.1.3.2 Adequacy for Organisational Security Policies of TOE 2

Table 8-5 Organisational Security Policies of TOE 2 relevant to TOE Security Objective of TOE 2

Organisational Security Policies of TOE 2	Security Objective of TOE 2
P.Reg_ID	O.Reg_ID

Table 8-6 TOE Security Objective of TOE 2 relevant to Organisational Security Policies of TOE 2

TOE Security Objective of TOE 2	Organisational Security Policies of TOE2
O.Reg_ID	P.Reg_ID

Table 8-7 Organisational Security Policies of TOE 2 relevant to TOE Security Objective for Environment of TOE 2

Organisational Security Policies of TOE 2	Security Objective for Environment of TOE2
P.Plat_Appl	OE.Plat_Appl
P.Key_Function	OE.Plat_Appl
	OE.Key_Function
P.Process-TOE 2	OE.Process-TOE 2

Table 8-8 TOE Security Objective for Environment of TOE 2 relevant to Organisational Security Policies of TOE 2

Security Objective for Environment of TOE2	Organisational Security Policies of TOE 2
OE.Plat_Appl	P.Plat_Appl
	P.Key_Function
OE.Key_Function	P.Key_Function
OE.Process-TOE 2	P.Process-TOE 2

The justification related to the organisational security policy "Register Identification (P.Reg_ID)" is as follows:

Since **O.Reg_ID** requires the TOE to provide the personaliser with the security function for registering the unique manufacture ID assumed in **P.Reg_ID**, the organizational security policy is covered by the objective.

The justification related to the organisational security policy "Usage of Hardware Platform (P.Plat_Appl)" is as follows:

Since **OE.Plat_Appl** requires the Smartcard Embedded Software developer to implement those measures assumed in **P.Plat_Appl**, the organisational security policy is covered by the objective.

The justification related to the organisational security policy "Usage of Key-dependent Function (P.Key_Function)" is as follows:

(a) **OE.Key_Function** requires the Smartcard Embedded Software to implement key-dependent functions in a way that they are not susceptible to leakage attacks; and (b) **OE.Plat_Appl** contributes to this requiring for the smartcard embedded software developer to apply security measures of TOE1's guidance.Therefore, **P.Key_Function**, the organisational security policy is covered by these objective.

The justification related to the organisational security policy "Protection during TOE 1 Development and Production (P.Process-TOE 1)" is as follows:

OE.Process-TOE 2 requires the TOE 2 Manufacturer to implement those measures assumed in **P.Process-TOE 2**. Therefore, the organisational security policy is covered by this objective.

8.2 Security Requirements Rationale

8.2.1 TOE Security Functional Requirements Rationale

Verifies that the security policy and the security functional requirements for TOE are adequately selected and the TOE meets the policy and the requirements above.

8.2.1.1 TOE Security Functional Requirements of TOE 1 Rationale

For the TOE Security Functional Requirements of TOE 1, refer to “8.2.1 Rationale for the security functional requirements” in [CXD9916H3/MB94RS403 ST].

8.2.1.2 TOE Security Functional Requirements of TOE 2 Rationale

< Relation with TOE Security Objective of TOE 2>

Table 8-9 Relationship between TOE Security Functional Requirements of TOE 2 and TOE Security Objectives of TOE 2

Security Objectives / SFR	O.Mutual_Auth	O.Data_Acc	O.Enc_ComData	O.ComData_Check	O.Replay_Protection	O.Power	O.TOEdata_Check	O.TOEdata_Valid	O.Reg_ID
FIA_ATD.1	X								
FIA_UID.1	X								
FIA_UAU.1	X								
FIA_UAU.3		X							
FIA_UAU.4		X							
FIA_USB.1	X								
FCS_CKM.1.A	X								
FCS_COP.1.A	X								
FMT_SMR.1	X	X							
FDP_ACC.1		X							
FDP_ACF.1		X							
FMT_MTD.1.A		X							X
FMT_MTD.1.B		X							
FMT_MTD.1.C		X							
FMT_MTD.1.D		X							
FMT_SMF.1		X							
FTP_ITC.1			X	X					
FCS_CKM.1.B			X						
FCS_COP.1.B			X						
FPT_RPL.1					X				
FPT_RCV.4						X			
FPT_SDI.2							X		
FDP_DAU.1								X	

<Adequacy of the security objectives of the TOE 2 and of the functional requirements of the TOE 2>

(1) O.Mutual_Auth

O.Mutual_Auth implements the security objective to perform mutual authentication between the TOE and the controller when the controller tried to access to the user information with security or to the system information in the TOE.

This security objective performs identification of the controller in accordance with **FIA_UID.1 Timing of identification** and performs mutual authentication between the controller and TOE in accordance with **FIA_UAU.1 Timing of authentication**, before issuing permission to the controller for access to the user data with security or the system information in the TOE.

The security attributes necessary for identification of the controller and at the time of mutual authentication are defined in **FIA_ATD.1 User attribute definition**.

Generation of the authentication data is implemented in accordance with **FCS_CKM.1.A Cryptographic key generation**, and **FCS_COP.1A Cryptographic operation**.

After successful mutual authentication completed, the user is associated with security roles by **FMT_SMR.1 Security roles** and their attributes are combined with the subject in the TOE utilizing **FIA_USB.1 User-subject binding**.

(2) O.Data_Acc

O.Data_Acc implements the security objective to provide protection to the integrity and the confidentiality of data (User data, TSF data) in the TOE. This security objective performs control to (a) access to the user data with security based upon the security attributes enumerated in **FDP_ACF.1 Security attribute based access control** and in accordance with the access control policy described in **FDP_ACC.1 Subset access control**, (b) access to TSF data in accordance with **FMT_MTD.1.A**, **FMT_MTD.1.B**, **FMT_MTD.1.C**, and **FMT_MTD.1.D Management of TSF data**.

In addition, this security objective performs management of roles with **FMT_SMR.1 Security roles**, and specifies the control function for the security attributes and to TSF data with **FMT_SMF.1 Specification of Management Functions**.

Forged authentication data is detected with **FIA_UAU.3 Unforgeable authentication**.

Re-play of the authentication data is prevented in accordance with **FIA_UAU.4 Single- use authentication mechanisms**.

(3) O.Enc_ComData

O.Enc_ComData implements the security objective to provide protection to the confidentiality of the communication data exchanged between the TOE and the

controller.
This security objective is satisfied by **FTP_ITC.1 Inter-TSF trusted channel.** Protection to the confidentiality of the communication data is provided through encryption of the communication data in accordance with **FCS_CKM.1.B Cryptographic key generation**, and **FCS_COP.1.B Cryptographic operation**.

(4) O.ComData_Check
O.ComData_Check implements the security objective to provide protection to the integrity of communication data exchanged between the TOE and the controller.
This security objective is satisfied by **FTP_ITC.1 Inter-TSF trusted channel.**

(5) O.Replay_Protection
O.Replay_Protection implements the security objective to detect the replay attack in order to protect the confidentiality and the integrity of data (User Data, TSF data) internal to the TOE.
Detection of re-play attack is achieved by checking the transaction ID attached to the communication data after successful mutual authentication in accordance with **FPT_RPL.1 Replay detection**.

(6) O.Power
The security objective performed by **O.Power Power Loss Recovery** provides protection to the integrity of the data internal to FRAM at occurrence of "power down".
This security objective maintains the TOE in its secure state by **FPT_RCV.4 Function recovery.**

(7) O.TOEdata_Check
O.TOEdata_Check implements the security objective to check the integrity of the data stored to FRAM and to preserve a secure state of TOE.
This security objective is implemented in accordance with **FDP_SDI.2 Stored data integrity monitoring and action**.

(8) O.TOEdata_Valid
The security objective performed by **O.TOEdata_Valid** generates the data that can be used as the evidence for assurance of validity of the data in the FRAM. This Security objective is carried out by **FDP_DAU.1 Basic data authentication.**

(9) O.Reg_ID
The security objective performed by **O.Reg_ID** provides the personaliser with a means to be uniquely identified. This Security objective is carried out by **FMT_MTD.1.A Management of TSF data** for registering Manufacture ID information.

8.2.2 Security Functional Requirements for Environment Rationale

This sub-section demonstrates that the environmental security requirement for the environmental security objective is adequately selected, and that the environmental security requirement conforms to the environmental security objective.

8.2.2.1 Security Functional Requirements for Environment of TOE 1 Rationale

For the Security Functional Requirements for Environment of TOE 1, refer to “8.2.1 Rationale for the security functional requirements” in [CXD9916H3/MB94RS403 ST].

8.2.2.2 Security Functional Requirements for Environment of TOE 2 Rationale

< Relation with Security Objective of TOE 2>

Table 8-10 Security Objectives for Environment of TOE 2 relevant to Security Functional Requirements for Environment of TOE 2

Security Objectives for Environment of TOE 2	Security Functional Requirements for Environment of TOE 2 (Functional Component ID)
OE.Sec_Remote	FTP_ITC.1
OE.Plat_Appl	N/A
OE.Key_Function	N/A
OE.Process-TOE 2	N/A
OE.Ident	N/A

Table 8-11 Security Functional Requirements for Environment of TOE 2 relevant to Security Objectives for Environment of TOE 2

Security Functional Requirements for Environment of TOE 2		Security Objectives for Environment of TOE 2
Functional Component ID	SFR Name	
FTP_ITC.1	Inter-TSF trusted channel	OE.Sec_Remote

(1) OE.Sec_Remote

OE.Sec_Remote implements the security objective to provide the remote trusted IT product with the secure channel for communication between itself and the TOE.
This security objective provides the trusted channel for communication between the TOE and the remote trusted IT product in accordance with **FTP_ITC.1 Inter-TSF trusted channel**.

8.2.3 TOE Security Functional Requirements Dependencies

This section explains the dependability of TOE Security Functional Requirements.

8.2.3.1 TOE Security Functional Requirements of TOE 1 Dependencies

For the Security Functional Requirements of TOE 1 Dependencies, refer to “8.2.2 Dependencies of security functional requirements” in [CXD9916H3/MB94RS403 ST].

8.2.3.2 TOE Security Functional Requirements of TOE 2 Dependencies

Table 8-12 TOE Security Functional Requirements of TOE 2 Dependencies (1/2)

TOE Security Functional Requirement of TOE 2	Dependencies	Fulfilled by security Requirements in this ST
FIA_ATD.1	None	No dependency
FIA_UID.1	None	No dependency
FIA_UAU.1	FIA_UID.1	Yes
FIA_UAU.3	None	No dependency
FIA_UAU.4	None	No dependency
FIA_USB.1	FIA_ATD.1	Yes
FCS_CKM.1.A	FCS_CKM.2 or FCS_COP.1	Yes (FCS_COP.1.A)
	FCS_CKM.4	See discussion (c) below
	FMT_MSA.2	See discussion (b) below
FCS_COP.1.A	FDP_ITC.1 or FCS_CKM.1	Yes (FCS_CKM.1.A)
	FCS_CKM.4	See discussion (c) below
	FMT_MSA.2	See discussion (b) below
FMT_SMR.1	FIA_UID.1	Yes
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1	Yes
	FMT_MSA.3	See discussion (a) below
FMT_MTD.1.A	FMT_SMR.1	Yes (FMT_SMR.1)
	FMT_SMF.1	Yes
FMT_MTD.1.B	FMT_SMR.1	Yes (FMT_SMR.1)
	FMT_SMF.1	Yes
FMT_MTD.1.C	FMT_SMR.1	Yes (FMT_SMR.1)
	FMT_SMF.1	Yes
FMT_MTD.1.D	FMT_SMR.1	Yes (FMT_SMR.1)
	FMT_SMF.1	Yes
FMT_SMF.1	None	No dependency

Table 8-12 TOE Security Functional Requirements of TOE 2 Dependencies (2/2)

TOE Security Functional Requirement of TOE 2	Dependencies	Fulfilled by security Requirements in this ST
FTP_ITC.1	None	No dependency
FCS_CKM.1.B	FCS_CKM.2 or FCS_COP.1	Yes (FCS_COP.1.B)
	FCS_CKM.4	See discussion (c) below
	FMT_MSA.2	See discussion (d) below
FCS_COP.1.B	FDP_ITC.1 or FCS_CKM.1	Yes (FCS_CKM.1.B)
	FCS_CKM.4	See discussion (c) below
	FMT_MSA.2	See discussion (d) below
FPT_RPL.1	None	No dependency
FPT_RCV.4	ADV_SPM.1	Yes
FDP_SDI.2	None	No dependency
FDP_DAU.1	None	No dependency

(a) Reason why FMT_MSA.3 is not selected in FDP_ACF.1:
FDP_ACF.1 depends upon FMT_MSA.3 Static Attribute Initialisation. Although FMT_MSA.3 requests to implement the access control policy so that the default values are assigned to the security attributes, the default values defined in FDP_ACF.1 are always determined by the User external to the TOE (specified by command parameters). Because of this, FDP_ACF.1 does not require FMT_MSA.3.

(b) Reason why FMT_MSA.2 is not selected in FCS_CKM.1.A and FCS_COP.1.A:
FCS_CKM.1.A and FCS_COP.1.A depend upon FMT_MSA.2 Secure Security Attributes. FMT_MSA.2 requests that only the secure values are accepted as the security attributes. Because the security attribute of FCS_CKM.1.A and FCS_COP.1.A is key length, and since key length becomes 112 bits (fixation) in Triple Data Encryption Standards (Triple DES), FCS_CKM.1.A and FCS_COP.1.A do not require FMT_MSA.2.

(c) Reason why FCS_CKM.4 is not selected in FCS_CKM.1.A, FCS_COP.1.A, FCS_CKM.1.B and FCS_COP.1.B:
The data in the TOE is protected from unauthorised disclosure by O.Phys-Manipulation Protection against Physical manipulation against disclosure by physical probing and O.Data_Acc Data Access Control against disclosure by illegal access.
Therefore, there is no need to perform cryptographic key destruction according to FCS_CKM.4 and the dependency in the requirement FCS_CKM.1.A, FCS_COP.1.A, FCS_CKM.1.B and FCS_COP.1.B is therefore considered to be satisfied.

(d) Reason why FMT_MSA.2 is not selected in FCS_CKM.1.B and FCS_COP.1.B:
FCS_CKM.1.B and FCS_COP.1.B depend upon FMT_MSA.2 Secure Security Attributes. FMT_MSA.2 requests that only the secure values are accepted as the security attributes. Because the security attribute of FCS_CKM.1.B and FCS_COP.1.B is key length, and since key length becomes 56 bits (fixation) in Data Encryption Standards (DES), FCS_CKM.1.B and FCS_COP.1.B do not require FMT_MSA.2.

8.2.4 TOE Security Assurance Requirements Dependencies

This section explains the dependability of TOE Security Assurance Requirements.

8.2.4.1 TOE Security Assurance Requirements of TOE 1 Dependencies

For the Security Assurance Requirements of TOE 1 Dependencies, refer to “8.2.3 Assurance Requirements and the Strength of Function Level” in [CXD9916H3/MB94RS403 ST].

8.2.4.2 TOE Security Assurance Requirements of TOE 2 Dependencies

Table 8-13 TOE Security Assurance Requirements of TOE 2 Dependencies (1/2)

TOE Security Assurance Requirements of TOE 2	Depends on:	Satisfied by:
ACM_AUT.1	ACM_CAP.3	Included as ACM_CAP.4
ACM_CAP.4	ALC_DVS.1	Included
ACM_SCP.2	ACM_CAP.3	Included as ACM_CAP.4
ADO_DEL.2	ACM_CAP.3	Included as ACM_CAP.4
ADO_IGS.1	AGD_ADM.1	Included
ADV_FSP.2	ADV_RCR.1	Included
ADV_HLD.2	ADV_FSP.1	Included as ADV_FSP.2
	ADV_RCR.1	Included
ADV_IMP.1	ADV_LLD.1	Included
	ADV_RCR.1	Included
	ALC_TAT.1	Included
ADV_LLD.1	ADV_HLD.2	Included
	ADV_RCR.1	Included
ADV_RCR.1	Non	N/A
ADV_SPM.1	ADV_FSP.1	Included as ADV_FSP.2
AGD_ADM.1	ADV_FSP.1	Included as ADV_FSP.2
AGD_USR.1	ADV_FSP.1	Included as ADV_FSP.2
ALC_DVS.1	Non	N/A
ALC_LCD.1	Non	N/A
ALC_TAT.1	ADV_IMP.1	Included
ATE_COV.2	ADV_FSP.1	Included as ADV_FSP.2
	ATE_FUN.1	Included
ATE_DPT.1	ADV_HLD.1	Included as ADV_HLD.2
	ATE_FUN.1	Included
ATE_FUN.1	Non	N/A
ATE_IND.2	ADV_FSP.1	Included as ADV_FSP.2
	AGD_ADM.1	Included
	AGD_USR.1	Included
	ATE_FUN.1	Included
AVA_MSU.2	ADO_IGS.1	Included
	ADV_FSP.1	Included as ADV_FSP.2
	AGD_ADM.1	Included
	AGD_USR.1	Included

Table 8-13 TOE Security Assurance Requirements of TOE 2 Dependencies (2/2)

TOE Security Assurance Requirements of TOE 2	Depends on:	Satisfied by:
AVA_SOF.1	ADV_FSP.1	Included as ADV_FSP.2
	ADV_HLD.1	Included as ADV_HLD.2
AVA_VLA.2	ADV_FSP.1	Included as ADV_FSP.2
	ADV_HLD.2	Included
	ADV_IMP.1	Included
	ADV_LLD.1	Included
	AGD_ADM.1	Included
	AGD_USR.1	Included

8.2.5 TOE Security Assurance Requirements Rationale

The security assurance level for this Security Target is EAL4.

(Reason why EAL4 is selected)

This TOE consisting of TOE 1 and TOE 2 can be used for operations of various commercial fields.

Because of this, the highest evaluation assurance level of EAL4 for commercial purposes is regarded as suitable for this TOE.

8.2.6 Claims on TOE Strength of Function Rationale

This TOE is the product intending the operation for commercial use.
Because of this, EAL4 is regarded as appropriate for this TOE.
EAL4 claims that SOF-Basic is required for the product to which security functions are installed.
It can be said that, for this TOE intending the operation in commercial use, the sufficient security strength will be attained by SOF-Basic necessary in maintaining the security in the operational environment.

8.2.7 Mutual Support between Security Requirements

8.2.7.1 Mutual Support between Security Requirements of TOE 1

For the Mutual Support between Security Requirements of TOE 1, refer to “8.2.4 Mutually Supportive and Internally Consistent” in [CXD9916H3/MB94RS403 ST].

8.2.7.2 Mutual Support between Security Requirements of TOE 2

The selection of security requirements for TOE 2 can be regarded to be reasonable as shown in sub-sections "8.2.1.2. TOE Security Functional Requirements of TOE 2 Rationale", "8.2.2.2. Security Functional Requirements for Environment of TOE 2 Rationale", "8.2.3.2. TOE Security Functional Requirements of TOE 2 Dependencies", and "8.2.4.2. TOE Security Assurance Requirements of TOE 2 Rationale" of this document.
The selection of SFRs (Security Functional Requirements) and SARs (Security Assurance Requirements) is performed based upon (a) threats to TOE 2 and security environment and (b) various assumptions regarding security objectives.

Therefore, the previous sections of this rationale have already shown the internal consistency of the SFRs and the mutual support of the SFRs covering each of the objectives. In addition, the following is going to show the mutual support between security requirements related to various objectives.

The TOE shall provide protection against illegal access of user data and TSF data. The SFRs required to control the data access meet the security objective O.Data_Acc. These SFRs exercise data access control based upon authorised users, therefore they need the support of the SFRs that meet the security objective O.Mutual_Auth. Furthermore, the mutual authentication might be abused if a replay attack succeeds, and because of the dependency on the data access control, a weakness on the mutual authentication function can make vulnerable the access control on the sensitive data. This shows that the SFRs required to control the data access need the support of both the SFRs related to the mutual authentication and those related to the protection against replay attacks (FIR_UAU.3 and FIR_UAU.4).

The security functional requirement FTP_ITC.1 protects the TOE against disclosure and modification/destruction of the sensitive data transmitted between the Controller and itself. As shown in the section 8.2.1.2 above, the security functional requirements FCS_CKM.1.B and FCS_COP.1.B support FTP_ITC.1 to protect the confidentiality of the communication data. Additionally, the security functional requirements required to meet the security objectives for TOE1 O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the cryptographic algorithms implemented according to the security functional requirements FCS_CKM.1.B and FCS_COP.1.B, as well as the mechanisms implemented to protect the integrity of the

communication data. Therefore, these security functional requirements support also the secure implementation and operation of FTP_ITC.1.

Applying environmental stress to the TOE may cause a malfunction to the TSF or a leakage of sensitive data. To counter such kind of attacks, the TOE shall implement the security functional requirements required to meet the security objectives for TOE1 O.Malfunction and O.Leak-Forced. On the other hand, the security functional requirements required to meet the security objectives O.Power (FPT_RCV.4) and O.TOEdata_Check (FPT_SDI.2) allow the TOE to preserve a secure state in case of failure related to integrity of FRAM area data (due for instance to power failure or high temperature). The result is that all these security functional requirements need to support themselves mutually in order to preserve a secure state of the TOE.

8.3 TOE Summary Specifications Rationale

8.3.1 TOE Summary Specifications Rationale of TOE 1

For the TOE Summary Specifications Rationale of TOE 1, refer to “8.3 TOE Summary Specification Rationale” in [CXD9916H3/MB94RS403 ST].

8.3.2 TOE Summary Specifications Rationale of TOE 2

As demonstrated in sub-section "6.2.. TOE Security Functions of TOE 2" of this document, TOE 2 satisfies all the requirements of security functions set up in sub-section "5.1.2. TOE Functional Requirements of TOE 2" of this document.
The assurance measures described in sub-section "6.3.2. Assurance Measures for TOE 2" of this document demonstrate the reference to sub-section "5.1.3.2. TOE Security Assurance Requirements of TOE 2" of this document.

The selection of SFRs (Security Functional Requirements) and SARs (Security Assurance Requirements) is performed based upon (a) the security objectives for TOE 2 as well as for the security environment, and (b) assumptions on threats regarding to TOE 2 and its security environment.
Therefore, this ST (Security Target) provides the evidence that the security functions are capable to cope with all the threats launched against TOE 2 in collaboration with the assurance measures.

The table below shows the relationship between TOE Security Functional Requirement of TOE 2 and TOE Security Function of TOE 2.

Table 8-14 Relationship between TOE Security Functional Requirements of TOE 2 and TOE Security Functions of TOE 2

TOE Security Function / SFR	SF.1 Access Control	SF.1-1 Identification of User	SF.1-2 Mutual Authentication	SF.1-3 Access control to User information	SF.1-4 Registration of Area/Service	SF.1-5 Key Change	SF.1-6: Registration of Manufacture ID	SF.1-7: Registration of Issue ID, System and Area0000	SF.2 Sequence Control	SF.3 Protection to Confidentiality of Communication data	SF.3-1 Data Encryption Key Generation	SF.3-2 Encryption/Decryption of the communication data	SF.4 Protection to Integrity of Communication Data	SF.5 Protection to Integrity of Internal Data	SF.5-1 Atomic Updating of FRAM Data	SF.5-2 Check to the data in FRAM at read/write of data	SF.5-3 Check to Validity of Data in FRAM
FIA_ATD.1	X		X	X													
FIA_UID.1	X	X	X														
FIA_UAU.1	X		X														
FIA_UAU.3	X		X														
FIA_UAU.4	X		X														
FIA_USB.1	X		X														
FCS_CKM.1.A										X	X						
FCS_COP.1.A	X		X														
FMT_SMR.1	X	X	X	X	X	X	X	X									
FDP_ACC.1	X			X													
FDP_ACF.1	X			X													
FMT_MTD.1.A	X						X	X									
FMT_MTD.1.B	X				X												
FMT_MTD.1.C	X					X											
FMT_MTD.1.D	X					X											
FMT_SMF.1	X				X	X	X	X									
FTP_ITC.1										X		X	X				
FCS_CKM.1.B										X	X						
FCS_COP.1.B										X		X					
FPT_RPL.1									X								
FPT_RCV.4														X	X		
FDP_SDI.2														X		X	
FDP_DAU.1														X			X

(1) FIA_ATD.1

FIA_ATD.1 requires maintaining the security attributes (Area Code, Service Code) belonging to individual users.
This request is satisfied by the following TOE security functions.

(1)-1 SF.1-2 Mutual Authentication

At the time of mutual authentication, the TOE performs identification of the controller based upon the list of the area codes and the service codes to which the controller requested authentication. The TOE maintains the list of the area codes and the service codes as security attributes belonging to individual users.

(1)-2 SF.1-3 Access control to User information

To provide the Authorised User with capability for access to the permitted area, the TOE provides the access control function based on security attributes (Service Code) belonging to individual users.

(2) FIA_UID.1

FIA_UID.1 requires allowing the action (Identification of TOE, Access of Service without Security, Maintence Operation) on behalf of the user to be performed before the user is identified, and perform identification of each user before other TSF-medicated action (Access of user information with security or Access of system information) on behalf of that user.
These requests are satisfied by the following TOE security functions.

(2)-1 SF.1-1 Identification of User

At the time of mutual authentication, the TOE performs identification of the controller based upon the list of the area codes and the service codes to which the controller requested authentication.

(2)-2 SF.1-2 Mutual Authentication

The following operations are permitted before successful mutual authentication: identification of TOE, access to service without security, and verify operation.

(3) FIA_UAU.1

FIA_UAU.1 requires allowing the action (Identification of TOE, Access of Service without Security, Maintence Operation) on behalf of the user to be performed before the user is authenticated, and perform authentication of each user before other TSF-medicated action (Access of user information with security or Access of system information) on behalf of that user.
These requests are satisfied by the following TOE security functions.

(3)-1 SF.1-2 Mutual Authentication

When the controller tried to access to the user information with security or to the system information located in the TOE, the TOE performs mutual authentication with the controller utilizing the access key.

(4) FIA_UAU.3

FIA_UAU.3 requires detecting use of authentication data that has been forged by any user and use of authentication data that has been copied from other user.
These requests are satisfied by the following TOE security functions.

(4)-1 SF.1-2 Mutual Authentication

Mutual authentication utilizing the access key is implemented in a manner that the TOE and the controller alternately authenticate the authentication data created based upon random numbers generated by each of them and encrypted with triple DES utilizing the access key. Because of that, the authentication data changes at every new authentication, whatever TOE or controller it is. So the result of this is that any authentication data that has been forged or copied from another user is detected as erroneous.

(5) FIA_UAU.4

FIA_UAU.4 requires preventing resuse of authentication data related to the Autentication mechanism in FeliCa Technology employed for authentication with the controller.
This request is satisfied by the following TOE security functions.

(5)-1 SF.1-2 Mutual Authentication

Mutual authentication utilizing the access key is implemented in a manner that the TOE and the controller alternately authenticate the authentication data created based upon random numbers generated by each of them and encrypted with triple DES utilizing the access key. Because of that, the authentication data changes at every new authentication, whatever TOE or controller it is. Thus the reuse of authentication data is not possible since it will be detected as erroneous.

(6) FIA_USB.1

FIA_USB.1 requires associating the appropriate user security attributes (List of Area Code and List of Service Code) with subjects acting on behalf of that user.
This request is satisfied by the following TOE security functions.

(6)-1 SF.1-2 Mutual Authentication

The controller (user) is recognized as authorized user (subject) after successful mutual authentication.

(7) FCS_CKM.1.A

FIA_CKM.1.A requires generating the Access Key (key sizes: 112 bits) in accordance with FeliCa Technology.
This request is satisfied by the following TOE security functions.

(7)-1 SF.3-1 Data Encryption Key Generation

SF.3-1 directly implements the requirement FCS_CKM.1.A. So it is clear that SF.3-1

satisfies FCS_CKM.1.A.

(8) FCS_COP.1.A

FIA_COP.1.A requires performing encryption / decryption of data in accordance with Triple DES (cryptographic key sizes: 112 bits) that meet FIPS PUB 46-3.
This request is satisfied by the following TOE security functions.

(8)-1 SF.1-2 Mutual Authentication

Mutual authentication utilizing the access key is implemented in a manner that the TOE and the controller alternately authenticate the authentication data created based upon random numbers generated by each of them and encrypted with triple DES utilizing the access key (key size: 112 bits).

(9) FMT_SMR.1

FIA_SMR.1 requires maintaining the roles (Card Manufacturer, Card Issuer, Area Administrator, Service User) and associating users with the roles (Card Manufacturer, Card Issuer, Area Administrator, Service User).
This request is satisfied by the following TOE security functions.

(9)-1 SF.1-1 Identification of User

At the time of mutual authentication, the TOE performs identification of the controller based upon the list of the area codes and the service codes to which the controller requested authentication.

(9)-2 SF.1-2 Mutual Authentication

Mutual authentication utilizing the access key is implemented in a manner that the TOE and the controller alternately authenticate the authentication data created based upon random numbers generated by each of them and encrypted with triple DES utilizing the access key. After successful mutual authentication, the controller is recognized as authorized user. The security role is associated with user by this security function utilizing the key associated to the area/service specified during the identification in SF.1-2.

(9)-3 SF.1-3 Access control to User information

To provide the Authorised User with capability for access to the permitted area, the TOE provides the access control function. TOE allows the access to the service only to the Service User who has previously succeeded mutual authentication for the service to be accessed.

(9)-4 SF.1-4 Registration of Area/Service

The TOE provides only the Area Administrator with the registration function of area or service.

(9)-5 SF.1-5 Key Change

The TOE provides only the Area Administrator with the key information change function for the area key or the service key.

(9)-6 SF.1-6 Registration of Manufacture ID
The TOE provides only the Card Manufacturer or the Card Issure with the registration function of manufacture ID.

(9)-7 SF.1-7 Registration of Issue ID, System and Area0000
The TOE provides only the Card manufacturer or the Card Issuer with the registration function of issue ID, system and area 0000.

(10) FDP_ACC.1, FDP_ACF.1
FDP_ACC.1 requires enforcing the Access Control Policy in order to control the operation (Write or Read) to the User Block by Authorised User.
And **FDP_ACF.1** that has dependencies with **FDP_ACC.1** requires the Access Control Policy to the User Block based on the security attributes (Service Code, Service Type, Number of Block) of the User Block.
These requests are satisfied by the following TOE security functions.

(10)-1 SF.1-3 Access control to User information
To provide the Authorised User with capability for access to the permitted area, the TOE provides the access control function. SF.1-3 enforces the following rules when the user requests to access (write or read) to the user block of the service: (a) The TOE and the controller has previously succeeded in mutual authentication; (b) The service that corresponds with the service code requested by the Authorised User actually exists; (c) the access mode sent from the Authorised User matches with the service type in the service definition information that controls the user information; and (d) The user information to which the Authorised User requested access actually exists in the TOE. Therefore, SF.1-3 satisfies the requirements of FDP_ACC.1 and FDP_ACF.1.

(11) FMT_MTD.1.A
FMT_MTD.1.A requires restricting the ability to register the Manufacture ID information, the Issue ID information, System definition information and Area 0000 definition information to Card Manufacturer or Card Issuer.
This request is satisfied by the following TOE security functions.

(11)-1 SF.1-6 Registration of Manufacture ID
The TOE provides only the Card Manufacturer or the Card Issuer with the registration function of manufacture ID.

(11)-2 SF.1-7 Registration of Issue ID, System and Area0000
The TOE provides only the Card Manufacturer or the Card Issuer with the registration function of issue ID, system and area 0000.

(12) FMT_MTD.1.B

FMT_MTD.1.B requires restricting the ability to register the Area definition information and Service definition information to Area Administrator.
This request is satisfied by the following TOE security functions.

(12)-1 SF.1-4 Registration of Area/Service

The TOE provides only the Area Administrator with the registration function of area or service.

(13) FMT_MTD.1.C, FMT_MTD.1.D

FMT_MTD.1.C requires restricting the ability to modify the System Key, System Key Version, Area0000 Key and Area0000 Key Version information to Card Manufacturer or Card Issuer.
FMT_MTD.1.D requires restricting the ability to modify the Area Key, Area Key Version, Service Key and Service Key Version information to Area Administrator.
These requests are satisfied by the following TOE security functions.

(13)-1 SF.1-5 Key Change

The TOE provides only the Card Manufacturer, the Card Issuer or the Area Asministrator with the key information change function for the area key or the service key.

(14) FMT_SMF.1

FMT_SMF.1 requires to be capable of performing the following security management Functions:

-Registration of the Manufacture ID information,
-Registration of the Issue ID information, System definition information and Area 0000 definition information,
-Registration of the Area definition information and Service definition information,
-Modification of the System Key, System Key Version, Area0000 Key and Area0000 Key Version,
-Modification of the Area Key, Area Key Version, Service Key and Service Key Version.

This request is satisfied by the following TOE security functions.

(14)-1 SF.1-4 Registration of Area/Service

The TOE provides only the Area Administrator with the registration function of area or service.

(14)-2 SF.1-5 Key Change

The TOE provides only the Crad Issuer or the Area Administrator with the key information change function for the area key or the service key.

(14)-3 SF.1-6 Registration of Manufacture ID
The TOE provides only the Card Manufacturer or the Card Issuer with the registration function of manufacture ID.

(14)-4 SF.1-7 Registration of Issue ID, System and Area0000
The TOE provides only the Card Issuer with the registration function of issue ID, system and area 0000.

(15) FTP_ITC.1
FDP_ITC.1 requires providing the trusted communication channel between TOE and the trusted IT product.
This request is satisfied by the following TOE security functions.

(15)-1 SF.3-2 Encryption/Decryption of the communication data
SF.3-2 provides a communication channel and protects it from disclosure making use of an encryption/decryption mechanism. SF.3-2 allows the remote trusted IT product, i.e. the controller, to initiate the communication with the mutual authentication mechanism (but this is SF.1-2 instead), and allows accessing to user data or TSF data by exchanging communication data.

(15)-2 SF.4 Protection to Integrity of Communication Data
SF.4 provides protection against modification using parity check.

(16) FCS_CKM.1.B
FIA_CKM.1.B requires generating the Transaction key (key sizes: 56 bits) in accordance with FeliCa Technology.
This request is satisfied by the following TOE security functions.

(16)-1 SF.3-1 Data Encryption Key Generation
Transaction key is generated from random number each time at successful mutual authentication. It is generated in compliance with the Transaction key generation method specified in FeliCa Technology. Therefore, SF.3-1 wholly satisfies FCS_CKM.1.B.

(17) FCS_COP.1.B
FIA_COP.1.B requires performing encryption / decryption of data in accordance with DES (cryptographic key sizes: 56 bits) that meet FIPS PUB 46-3.
This request is satisfied by the following TOE security functions.

(17)-1 SF.3-2 Encryption/Decryption of the communication data
After the mutual authentication completed, The TOE performs encryption/decryption (DES, CBC mode) to the communication data with the transaction key in compliance with the requirement FCS_COP.1.B.

(18) FPT_RPL.1

FIA_RPL.1 requires the following processing.

1) Detect replay for the Input communication data
2) When replay of input communication data is detected, perform abandonment of the processing of the replyed Input Communication data

This request is satisfied by the following TOE security functions.

(18)-1 SF.2 Sequence Control

SF.2 detects replay for input communication data making use of a sequence number included in the transaction ID attached to the communication data. SF.2 detects the replay by comparison with its internal sequence number, and abandon the processing by rejecting the request of access to the user information and the file system information.

(19) FPT_RCV.4

FIA_RCV.4 requires ensuring that that the function of protection for internal data integrity in case of power failure during writing of data in FRAM have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

This request is satisfied by the following TOE security functions

(19)-1 SF.5-1 Atomic Updating of FRAM Data

FRAM data is updated with atomic updating function in order to guarantee the integrity of the data even if the writing procedure is interrupted.

(20) FDP_SDI.2

FDP_SDI.2 requires checking CRC of the data stored in FRAM in order to detect accidental modification or intentional modification to the data in FRAM.

These requests are satisfied by the following TOE security functions.

(20)-1 SF.5-2 Check to the data in FRAM at read/write of data

(Data read)

At the time of reading data stored to FRAM, performs CRC check to the data to be the object of data read.

TOE informs error status to the user when CRC error is detected.

(Data write)

At the time of writing data to FRAM, reads the written data out of FRAM and performs CRC check.

TOE informs error status to the user when CRC error is detected.

(21) FDP_DAU.1

FIA_DAU.1 requires providing Authorised User with the ability to verify evidence of Patch Program and parameter data (TOE 2 use) in FRAM.
This request is satisfied by the following TOE security functions

(21)-1 SF.5-3 Check to Validity of Data in FRAM

This security function provides the user (Smartcard Product Manufacturer, Personaliser, Smartcard Issuer) with the capability to check the validity of data in FRAM utilizing the hash code or CRC.

8.4 PP Claims Rationale

None

(This page is intentionally left blank.)

RC-S962/1

Composite Security Target (Public Version)

Version 1.10 ： May 2008

Sony Corporation

FeliCa Business Division

NO. 962-STL-E01-10