CXD3715GG/GU-x
Security Target

(Public Version)

Revision: 1.04

Date of Issue: **January 26, 2006**

FeliCa Business Center

Sony Corporation

Table of Contents

(Chapter 2. continued)

List of Tables & Illustrations

References

CC

Common Criteria for Information Technology Security Evaluation
(Comprising Parts 1-3, [CC1], [CC2], [CC3])

CC1

Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and Generation Model
CCIMB-99-031, Version 2.1, August 1999

CC2

Common Criteria for Information Technology Security Evaluation
Part 2: Security Functional Requirements
CCIMB-99-032, Version 2.1, August 1999

CC3

Common Criteria for Information Technology Security Evaluation
Part 3: Security Assurance Requirements
CCIMB-99-033, Version 2.1, August 1999

Interpretation

All Interpretations that apply to CC v2.1

FIPS

Federal Information Processing Standards Publications
http://www.itl.nist.gov/fipspubs/index.htm

DES

Data Encryption Standard (DES)
National Bureau of Standards
Federal Information Processing Standards Publication FIPS PUBS 46-3
25 October 1999
http://csrc.nist.gov/fips/fips46-3.pdf

DES Modes of Operation

The standard for DES modes of operation
National Bureau of Standards
Federal Information Processing Standards Publication FIPS PUBS 81
2 December 1980
http://www.itl.nist.gov/fipspubs/fip81.htm

AIS 20

Application Notes and Interpretation of the Scheme 20 (AIS 20)
Functionality classes and evaluation methodology for deterministic random number generators.
Version 1, 2 December 1999
http://www.bsi.bund.de/zertifiz/zert/interpr/ais_cc.htm

(This page is intentionally left blank)

Chapter 1. Introduction

This document is compiled from CXD3715GG/GU-x Security Target as public version.

Identification of ST (Security Target) and TOE (Target of Evaluation)

This section provides the information necessary for identification and control of this Security Target and FeliCa products.

Title of Security Target:	CXD3715GG/GU-x Security Target Public Version
Identification of TOE:	IC Chip with Operating System for Mobile
Version:	0701
IC Chip:	CXD3715GG/GU-x
Version:	2.1
Operating System:	Mobile FeliCa OS Version 1.0
Rev:	R9
Identification of CC:	ISO15408 standard, Common Criteria for IT Security Evaluation
Creator of ST:	Sony Corporation
Evaluator of ST:	LogicaCMG plc

ST (Security Target) Overview

The Target of Evaluation (TOE), the CXD3715GG/GU-x, version 0701, consists of an IC Chip with Embedded Software for Mobile Device. IC Chip portion is CXD3715GG/GU-x (version 2.1) of the TOE Hardware, and Embedded Software portion is Mobile FeliCa OS as the TOE Software.

Description on TOE's Nomenclature (Package Types and Suffixes)
This TOE is available in two molding types: the one is BGA (Ball Grid Array) and the other is LGA (Land Grid Array). CXD3715 "GG" represents the BGA type, and CXD3715 "GU" represents LGA type, respectively. Although there are differences in the thickness of moldings and the height of external terminal pins, these two types of TOE are compatible having the same specifications such as the security functions, allocations / distances between the external terminal pins, etc. The suffix "-X" appended to CXD3715GG/GU is the symbol or the number indicating the differences between the issue data.

This TOE is designed so that it is mainly installed to Mobile Device such as mobile phone. Taking the installation of this TOE to the Mobile Device into account, this TOE is designed /manufactured as the product intending to function as contactless / contact IC Chip to which Mobile Device is able to store various types of tickets and / or electric money.
The TOE provides the security for protection of the secrecy and the integrity of the important data internal to or transferred within the TOE, or those transferred between the TOE and the IT product. This intends that the TOE is able to provide the secure operation in the usage for transport systems and / or finance systems (the operating environment assumed for this TOE). The product is developed and designed by Sony.

This IC chip is a 1-chip LSI of analog/digital hybrid type, and an original 8-bits RISC type CPU is built in it. This CPU is specially designed by Sony Corporation, and combines built-in EEPROM, SRAM, MaskROM, an encryption engine and various RF functions into a single IC chip.
Communication between this IC chip and the carrier on which this IC is mounted is implemented through a UART I/F. Communication between this IC chip and the external devices is done through a RF system utilizing SONY original communication protocol.
This data communication adopts Ask10% data modulation system, and the carrier frequency is 13.56MHz. For bit coding, Manchester system is adopted.

Communication of important data between the carrier (on which this IC chip is mounted) and the external devices (such as the external R/W, and the internal controller) is protected by an encryption system. This encryption system prevents "wiretapping", "modification" and/or "fraudulent use" of the IC. In the encryption processes, Triple DES and Single DES are applied at the authentication, and during the communication after the successful authentication. Should any transaction be interrupted during writing process of a new data to the memory on FeliCa chip, the original data is saved as it was due to various built-in safety protection functions.
In addition, Mobile FeliCa OS is installed to the IC chip is originally developed by Sony Corporation.
This OS provides both the flexible management of file system and the high-speed communication process. These are the features of Sony FeliCa products.
In the case of CXD3715GG/GU-x, powerful security functions are also installed to counter against the physical and logical attacks and to demonstrate the features enumerated above to the maximum.

Conformance to CC

This security target conforms to Part1and Part 3 of Common Criteria v2.1 (ISO15408) with Part2 extended.
Part2 extended: FCS_RNG.1 and FMT_PUT.1 (for 5.1.1. TOE Hardware Security Functional Requirements).
The evaluation level is EAL4.This security target does not conform to any Protection Profiles.

Applicability

The configuration of this document is as defined in [CC] Part 1, Annex C:

- Chapter 2 "Definition of TOE" describes the explanation of TOE (Target Of Evaluation).
- Chapter 3 "TOE Security Environment" describes the statements on TOE Security Environment.
- Chapter 4 "Security Objective" describes the statements on Security Objective.
- Chapter 5 "IT Security Requirements" describes Requirements on IT Security.
- Chapter 6 "TOE Summary Specification" describes the TOE Summary Specification.
- Chapter 7 "Rationale of Security Objective" describes the Rationale of Security Objectives.
- Chapter 8 "Rationale of Security Requirements" describes the Rationale of Security Requirements.
- Chapter 9 "Rationale of TOE Summary Specification " describes the Rationale of TOE Summary Specification.
- Chapter 10 “Appendix A” provides the explanation of the Extended IT Security Function Requirements.
- Chapter 11 "Revision Information" describes the official history of revision-up of this ST.

Terminology

This section contains the definitions of technical/technological terms used in this document to indicate specific meanings. Unless otherwise specified, terms defined in Common Criteria [CC] are not contained in this section.

Access Key:
This is the key to be used for encryption of the communication data at the time of authentication performed under the file access control.

Activation:
Process to assign the operating capabilities (to TOE) necessary for TOE Holders.

Area Key:
This area key is the key for identifying and protecting area file.

Assets:
Information and/or resources to be protected by countermeasures of TOE.

Assignment:
Specification of identified parameters within components.

Assurance:
Basis of trust that the security objective is implemented by the entity.

Attack Potential:
Possibility that an attack is successful should such attack be mounted, represented from the viewpoints of attacker's expertise, resources and motives.

Augmentation:
Adding one or multiple assurance components in Part 3 to EAL or to an assurance package.

Authentication data:
Information used to verify the necessary identification information of the user.

Authentication Lock:
This is the function to reject further reception of mutual authentication command and the commands necessary for mutual authentication in the case when the number of sequential failed times of mutual authentication trials reached to the prescribed value.

Authorized user:
The user capable to execute the operation in accordance with TSP.

Carrier (=Mobile Device):
A device into which an operational integrated circuit (IC) is incorporated:
For the purpose of this Security Target, the carrier is the Mobile Device.
I.e., a mobile phone is assumed as the carrier.

Class:
A group of families that share common objects.

Component:
Minimum set of selectable elements that may be included in PP, ST or a package.

Connectivity:
TOE's characteristics that allow dialogue with IT entity external to TOE:
This includes data exchange with RF or UART measures in an environment or in a configuration over a distance.

Controller:
Controls card Reader/Writer via UART I/F and is part of the host (e.g. a PC connected to the card Reader/Writer).

Dependency:
Relationship between requirements that, in order to implement the object of requirement of depending side, the requirement of depended side must be normally satisfied.

Die (pl Dice):
Semiconductor IC in a state not sealed into a package yet, or no connection is done with external devices.

Differential power analysis (DPA):
One of techniques for identification of IC's detailed operating conditions through combination of the physical measurement of IC parameters such as power consumption and the statistical signal processing techniques:
With DPA, information for restoration of various operating parameters and keys in the IC may be available.

Electrically Erasable Programmable Read Only Memory (EEPROM):
One of non-volatile type memory technologies that allows electrical erasure and re-writing of data.

Element:
The smallest (or basic) unit of a component.

Evaluation:
Evaluation of PP, ST or TOE against the specified standard(s).

Evaluation Assurance Level, EAL:
A package comprising of assurance components in Part 3 that represent the level in the defined assurance stage of CC.

Evaluation authority:
Organization to perform CC to a specific community in accordance with the evaluation plan, to define the standard based upon it, and to monitor the quality of evaluation performed by organizations within such a community.

Evaluation scheme:
The framework of management and control to be the norm in the application of CC by an evaluation authority to a specific community.

Extension:
Adding a function requirement not included in Part 2 of CC, or adding a function requirement not included in Part 3 of CC (or both) to ST or PP.

External Card:
Products existing external to TOE, and is compatible with FeliCa card or FeliCa products.

External IT entity:
An IT product or a system existed external to TOE and dialogues with TOE regardless of its trust level.

External Reader/Writer:
Device existing external to TOE, and is used to perform reading/writing TOE's data.

Family:
A group of components that share security objectives but are different in emphasis or in definition.

Failure analysis:
Generic term for various techniques used in laboratories for development and testing of semiconductor devices for identification of points of failure on operations of integrated circuit (IC).
Such techniques include not only the observation (to determine what is inadequately operating) but also the modification of internal structure of IC (to determine whether such failure is removed / resolved or not).

FeliCa Technology System
"FeliCa Technology System" is the contactless IC card technology uniquely developed by Sony Corporation.

First use indication:
IC function to set a specific audit bit to indicate that the TOE is issued already, in a state possible to operate, and possible to use for its intended functions.

Formal:
Representation by the restricted syntax language of which meanings are defined based upon established mathematical concepts.

Human user:
Any person who dialogues with TOE.

Identification:
Representation (character string, for example) for unique identification of the authorized user such as full name, abbreviation or alias of the user.

Informal:
Representation by natural language.

Internal communication channel:
For the purpose of this ST, "Internal Communication Channel" means the bus line operating as the communication channel between the separate components that configure the IC Chip such as the CPU, various types of memories.

Internal Controller (Controller for Mobile Device):
"Controller for Mobile Device" exists in the carrier to which the TOE is installed, and it is connected with the TOE via the UART interface.
The mobile controller is the control device to access to the external controller (the server) from the internal controller.

Internal TOE transfer:
Data communication done between different areas of TOE.

Inter-TSF transfers:
Data communication done between TOE and the security function of other trusted IT product.

Iteration:
Using a component twice or multiple times during various operations.

Integrated Circuit (IC):
An electronic component designed to be accommodated on a single semiconductor chip for execution of various types of data processing and / or of memory function.

Integrated Circuit Card (ICC):
A card comprised of a carrier into which an IC and an antenna incorporated.

Initialization:
A series of procedures done at the time of IC manufacture for the purposes to write specific information to the non-volatile memory, to test, and to protect the security.

Issue Data:
The process to write specific information to the non-volatile memory as a preparatory procedure for issuance of IC to Users.

Non-volatile memory:
A type of semiconductor memories that maintains the content (of stored data) even if the supply of electric power stopped (that is, ROM, EEPROM, FLASH MEMORY, etc.).

Object:
Entity within TSC that contains or receives information, and to be the object of execution of operations by the subject.

Operational Keys:
Cryptographic key loaded internal to an assembled TOE product, and to be used by TOE Holder during normal operation (of the TOE).

Operating Software (OS):
Software that resides on TOE, and is necessary for TOE's operation including the support to secure loading of data.
This may or may not include the complete operating system in its normal meaning.

Organizational security policies:
One or multiple numbers of rules, procedures, practices or guidelines on the security imposed by an organization to tasks.

Package:
A set of re-usable function components or assurance components (EAL, for example) combined for implementation of the identified security objective.

Personalization:
The process to write specific information to the non-volatile memory as a preparatory procedure for issuance of IC cards to Users.

Product:
A package of IT software, firmware or hardware (or all of them) that provides the functionality designed to

be used or embedded in various systems.

Protection Profile, PP:
A set of security requirements independent of implementation to satisfy the needs of a specific user concerning a TOE category.

Photomask:
A sort of mask used to protect the selected area(s) on a silicon wafer from (exposure to) the light source as well as to expose other (i.e., not to be protected) areas on the wafer surface to the light source.
Purpose of this mask is to expose photo-resist coated on the silicon wafer, and to produce the desired substrate structure during the etching process to be done next (i.e., after the exposure process).
Photomask is the measure to produce IC chip circuitry so that various functions of IC are implemented on that IC chip.

Pilot:
One of applications for testing purpose that makes a system is deployed to restricted area(s) of IC structure or to restricted TOE Holder(s) so that collection of following data becomes possible before introduction of the system in its complete form.
(a) whether the system is in a satisfactory condition or not, and
(b) its operating capabilities.

Post-issuance:
Period of time in which TOE Holder possesses the TOE:
In some types of TOE, it is possible to load several additional functions to such TOE after its issuance.

Production keys:
Cryptographic key loaded to IC during its production for the purpose to maintain the security.

Random Access Memory (RAM):
A memory of volatile type (to be used internal to IC) possible to be randomly accessed but requires the electric power to be supplied to maintain the data stored to it.

Read Only Memory (ROM):
A memory of non-volatile type (to be used internal to IC) that requires no electric power to maintain the data stored to it.
ROM data may be often included in one of photomasks to be used in IC manufacturing.

Reference Monitor:
Concept of an abstract equipment to implement access control policy of TOE.

Reference validation mechanism:
Implementation of a reference monitor having the characteristics simple enough to prevent unauthorized operation, to be always recalled, and to be analyzed and tested in detail.

Refinement:
Adding detailed elements to a component.

Reverse engineering:
Generic term for various techniques used by laboratories for development and testing of semiconductor

devices for preparation of design documents and specifications of unknown integrated circuits:
If "reverse engineering" is performed in its most perfect form, it is possible to identify all the production packages starting the work from an unidentified integrated circuit.

RF:
Acronym of Radio Frequency.

RISC:
Acronym of Reduced Instruction Set Computer (that is, a computer chip having a reduced set of instructions compared to the case of computer chip of ordinary type).

Role:
A set of defined rules that governs the dialogue allowed between the user and TOE.

Secret:
Information allowed to be disclosed only to the authorized user or TSF (or both) to implement a specific SFP.

Security attribute:
Information related to subject, user or object (or all of them) to be used for the purpose of implementation of TSP.

Security Function, SF:
One or multiple parts of TOE dependent on implementation of a sub-set of closely related rules of TSP

Security Function Policy, SFP:
Security policy implemented by SF.

Security Objective:
Statement intending opposition against the clarified threat, or implementation of clarified organizational security policies and assumptions (or both).

Security Target, ST:
A set of security requirements and specifications to be used as the reference of TOE evaluation.

Select function:
Select function is test function that is used during both wafer and package level selection test.

Selection:
Specifying one or multiple items out of the list within a component.

Semiformal:
Representation by restricted syntax language of which meanings are defined.

Service Key:
This service key is the key for identifying and protecting service file.

Simple Power Analysis (SPA):
A technique for detailed identification of IC's operating conditions by physical measurement of changing

power consumption of IC: With SPA, information possible to reset various operating parameters and keys internal to IC to their original status may be available.

SmartCard:
A carrier made of plastics or other materials into which a computer chip of small size is embedded.
In this document, terms "IC Card" and "SmartCard" are used having the same meaning.

SOF-basic:
The level of strength of TOE function recognized by analysis that the function has a sufficient resistance against temporary intrusion to TOE security mounted by an attacker with low attack potential.

SOF-medium:
The level of strength of TOE function recognized by analysis that the function has a sufficient resistance against direct or intentional intrusion to TOE security mounted by an attacker with medium attack potential.

SOF-high:
The level of strength of TOE function recognized by analysis that the function has a sufficient resistance against planned or organizational intrusion to TOE security mounted by an attacker with high attack potential.

Strength of Function, SOF:
Rating of TOE security function represented by the minimum effort regarded as necessary to disable the expected behavior of security through a direct attack against the security mechanism in the lower level.

Subject:
Entity within TSC that initiates execution of the operation.

System:
Specific IT facilities associated with specific objective and operating environment.

Target of Evaluation, TOE:
IT product or system and related guidance documents for administrator/users to be the target of evaluation.

Terminal:
The device used at the time of transaction together with a Card Reader/Writer (i.e., communication terminal).

TOE block (Card block):
IC function related to the temporary restriction imposed to several functions that allowed for a TOE.
TOE blocking (Card blocking) is of temporary nature, and possible to reset to the original state by personnel with appropriate privilege.

TOE disablement (Card disablement):
IC function related to termination of all the functions of a TOE (card) except some of limited audit functions.
"TOE Disablement (Card Disablement)" is of permanent nature.

TOE embedded (Card embedded):
Manufacturer engaging in assembly of the TOE (cards) and the integrated circuits (IC).

TOE Holder (Mobile Device Holder):
Person (i.e., user) to whom the TOE is issued with authorized procedures.

TOE issuer (IC issuer):
Organization that issues the cards to TOE (IC with embedded OS) holders.

TOE Operating System (Operating System: OS):
Codes specific to the developer of Operating System written to the microprocessor in a characteristic form or as machine codes.

TOE resource:
Usable or consumable item(s) in TOE.

TOE Security Functions, TSF:
A set comprising all of hardware, software, and firmware of TOE to be dependent for precise implementation of TSP.

TOE Security Functions Interface, TSFI:
A set of interfaces through which access to TOE resources or acquisition of information from TSF is done, or TSF performs mediation regardless of dialogue (man-machine-interface) or programming (application-programming-interface).

TOE security policy model:
Structured representation of security policies to be implemented by TOE.

Transfer outside TSF control:
Data communication between TOE and an entity not under the control of TSF.

Transport keys:
Cryptographic key loaded internal to IC for the purpose to maintain the security during transportation of ICs, modules and assembled products before IC card issuance.

Trusted channel:
A measure of communication between TSF and the trusted IT product in counter side at a sufficient level of security necessary in supporting TSP.

Trusted path:
A measure for communication at a level of security that the user and TSF require to support TSP.

TSF data:
Data created by TOE or data created in relation to TOE that may affect TOE's operation.

TSF Scope of Control, TSC:
A set of dialogues possible to perform to TOE or within TOE and under the rules of TSP.

UART Interface
"UART Interface" is the interface to establish the communication between the TOE and the controller for Mobile Device.

User:
Entity external to TOE and dialogues with TOE (human user, or external IT entity).

User data:
Data created by the user or data created in relation to the user that do not affect operation of TSF.

Wired:

A type of interfaces to establish the communication between the IC chip and the carrier through wired connection.

Wireless:

A type of interfaces to establish the communication between the IC chip and the carrier without wired connection. This interface utilizes Sony original communication protocol.

(This page is intentionally left blank.)

Chapter 2. Definition of TOE

To help readers' understanding of FeliCa security requirements, this chapter provides the description of TOE.

For the applicability and the boundary of this TOE, description will be given on both physical (hardware and software components) as well as logical (IT and security features provided by TOE) aspects using general terms.

TOE's Configuration

For the purpose of this ST, the TOE is the IC chip with Operating system for Mobile Device developed by Sony Corporation.
The TOE's configuration is as shown in the following paragraphs.

The diagram below illustrates the TOE's configuration.

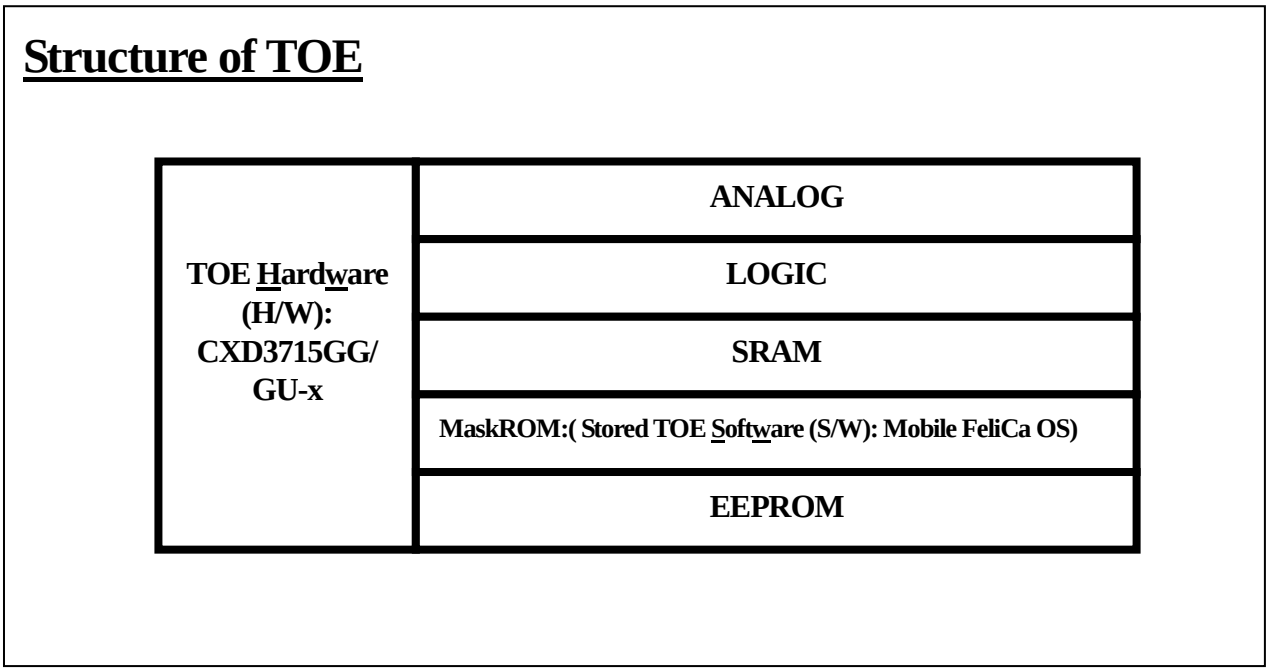


Figure 1. TOE's Configuration

Coverage of the TOE

The coverage of this TOE is an "IC Chip with Embedded Software for Mobile Device".
TOE consists of an IC Chip as hardware, and an Mobile FeliCa OS as embedded software running on that hardware.
TOE Hardware identification is CXD3715GG/GU-x; TOE Software identification is Mobile FeliCa OS.

TOE operates with the electromagnetic signal received from the external card Reader / Writer, or at Power ON from the carrier.
To the TOE, a 8-bit RISC CPU is incorporated. This CPU is specially designed by Sony Corporation, and it is the product that combines a built-in MaskROM (48k Bytes), a SRAM (2k Byte), an EEPROM (9k Bytes), analog circuits, and security logic circuits onto a single IC Chip.

TOE is designed to be installed mainly to Mobile Device such as mobile phone.
With the installation of this IC Chip to a Mobile Device, the Mobile Device functions as a contactless / contact IC Chip conforming to FeliCa Technologies System to store various types of tickets and electric money.
It also provides, in addition, the triplicate communication function to utilize the TOE as a storage media.

Process Steps of TOE from Manufacturing to Shipping in its End Form

The life cycle of the TOE covers "Process 1" to "Process 6" (**Scope of TOE**) performed in the IC Chip Design / OS Development Site and in the IC Chip Manufacturing Factory.
Be careful of the fact that "Process 7" to "Process 9" (**Out Scope of TOE**) is covered by the life cycle of the Mobile Device including the TOE.

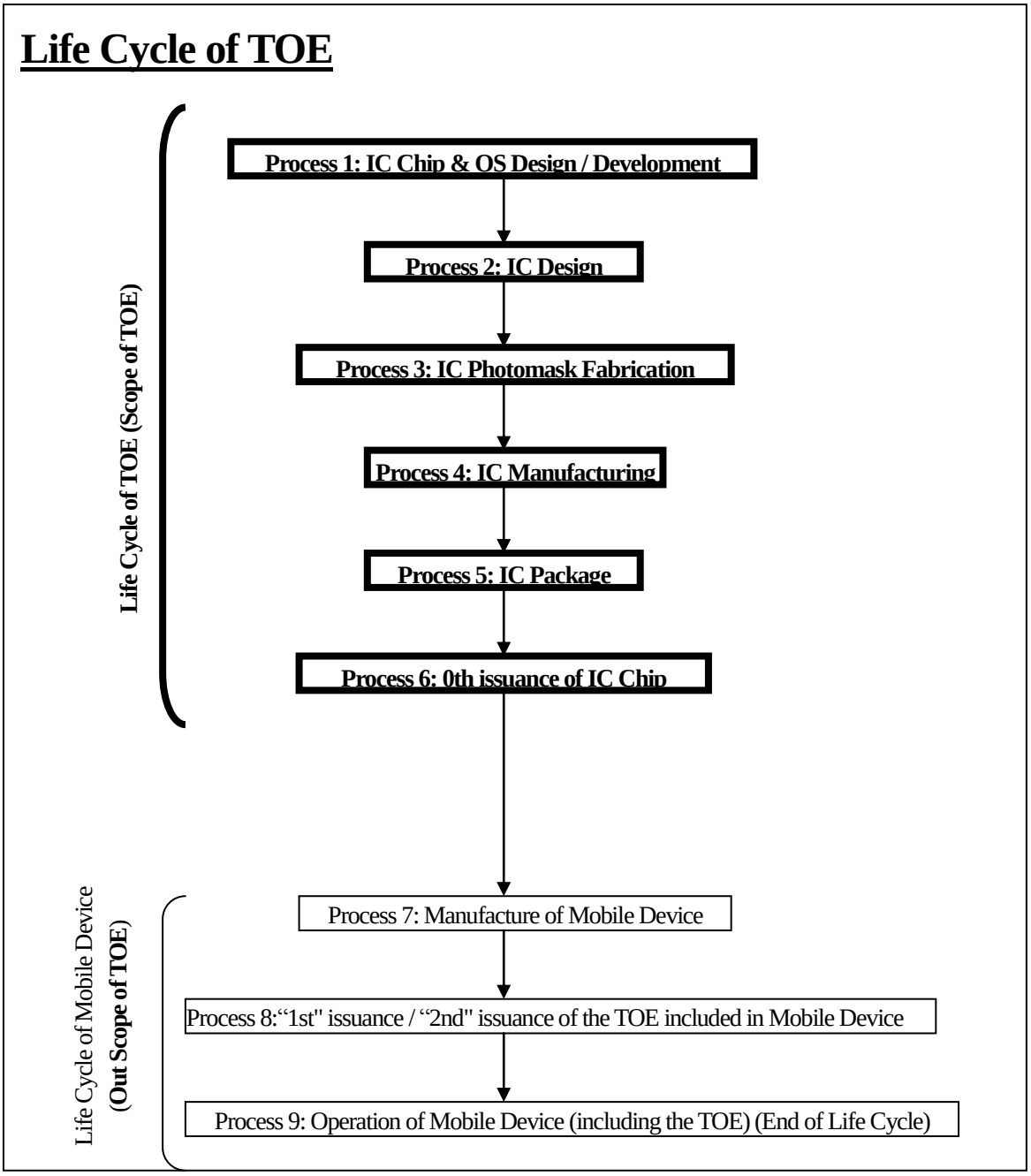


Figure 2. Process diagram from manufacturing to shipping of TOE

Life Cycle Scope of TOE (Scope of TOE)

Process 1: IC Chip & OS Design / Development

IC Chip:

Personnel involved:	IC Chip designers (trusted personnel with security training / education)
Works:	IC Chip design work.
Deliverables:	IC Chip design information

OS:

Personnel involved:	Designer / Development Engineer of the Mobile FeliCa OS (trusted personnel with security training and education)
Works:	Design / Development work of the Mobile FeliCa OS
Deliverables:	Mobile FeliCa OS

Process 2:IC Design

Personnel involved:	Hardware designer (trusted personnel with security training and education)
Works:	Design data, and Layout data process of the IC Chip
Deliverables:	Layout Data

Process 3:IC Photomask Fabrication

Personnel involved:	Production personnel (trusted personnel with security training and education)
Works:	Converting Design Data to EB Data and manufacture of Mask for the IC Chip
Deliverables:	IC Mask

Process 4:IC Manufacturing

Personnel involved:	Production personnel (trusted personnel with security training and education)
Works:	manufacture of the IC Wafer, and IC Chip
Deliverables:	IC Chip (CXD3715GG/GU-x)

Process 5:IC Packaging

Personnel involved:	Production personnel (trusted personnel with security training and education)
Works:	Packaging of the IC Chip for IC Products
Deliverables:	IC Product (including the IC Chip)

Process 6:0th Issuance of IC Chip

Personnel involved:	"0th" Issuer and Primary Issuer (trusted personnel with security training and education)
Works:	Creation of Issue Data (The process to write specific information to the non-volatile memory as a preparatory procedure for issuance of IC to Users). "0th" issuance of the IC product (IC Chip)
Deliverables:	IC Products (including the IC Chip‘0th" issued).

- By the trusted delivery operator (company), secure delivery of the deliverables between each of sites is achieved while maintaining the confidentiality and the integrity of the deliverables.
- By the trusted personnel in charge, secure delivery of the deliverables within the IC manufacturing factory is achieved while maintaining the confidentiality and the integrity of the deliverables.

Life Cycle Scope of Mobile Device (Out Scope of TOE)

Process 7: Manufacture of Mobile Device

Personnel involved:	Mobile Device manufacturer (trusted personnel with security training and education)
Works:	Manufacture of Mobile Device
Deliverables:	Mobile Device (including the TOE)

Process 8:“1st" issuance / “2nd" issuance of the TOE included in Mobile Device

Personnel involved:	“1st" issuer and / or “2nd" issuer (trusted personnel with security training and education)
Works:	“1st" issuance and / or “2nd" issuance of the TOE included in Mobile Device
Deliverables:	Mobile Device (including the TOE)

Process 9: Operation of Mobile Device (including the TOE) (End of Life Cycle)

Personnel involved:	End User

TOE's Hardware

The hardware of this TOE (scope of the TOE) consists of MaskROM, SRAM, EEPROM, Logic circuits, and Analog circuits.

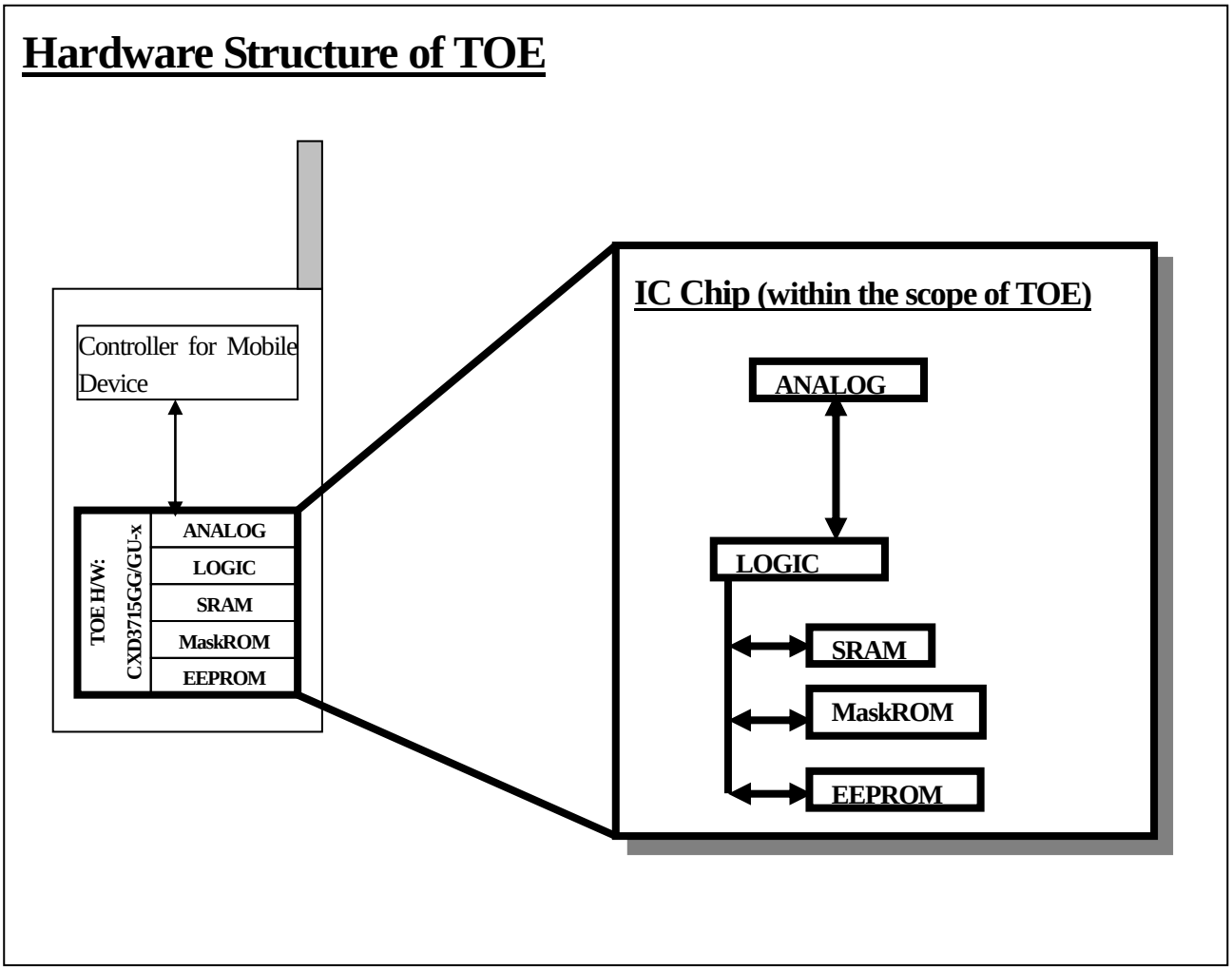


Figure 3. Hardware Structure of the TOE

IC Chip (TOE) is named CXD3715GG/GU-x.

CXD3715GG/GU-x is an accessible LSI to SONY original protocol for contactless card (with wired access function), and have 8-bit RISC CPU, nonvolatile memory (EEPROM), SRAM, MaskROM, ANALOG wireless card I/F and DES coprocessor.

CXD3715GG/GU-x can be divided for the following

LOGIC: Logic circuit is constructed of the followings;

CPU: The CPU is 8bit RISC CPU and the features are the followings;

- Data Bus: 8 bits, Address Bus: 16 bits
- Normal operation mode: 847 KHz (sixteenth of 13.56MHz divided)
- Double-speed operation mode 1.69MHz (eighth of 13.56MHz divided)

SPU: communicate with ANALOG Card I/F block
CRC: generate and check CRC by 16-bit CRC resister
DES: DES encrypt and decrypt by the dedicated instruction from the CPU
RNG: Pseudo random number generator of 11-bit LFSR
UART: Serial I/F to communicate with the controller for personal digital assistance
IBO: General-purpose IO port of open drain

SRAM: 2Kbytes
used as the memory for CPU work area or communication buffer

MaskROM: 48Kbytes
read-only memory stored instruction code

EEPROM: 9Kbytes
rewritable nonvolatile memory
Read is done by one byte and Erase and Write are done by 1 Page (=72bytes)

ANALOG: Analog circuit has the following functions;

- Dataset suitable to Manchester method
- Power supply voltage in interior of LSI generating from outside battery
- Sampling 13.56MHz clock
- Detecting the tampering

TOE's Software

The software of this TOE means “Embedded Software: Mobile FeliCa OS” stored to MaskROM of IC Chip developed for use on Mobile Device.
The software of this TOE (scope of the TOE) consists of Data transfer, File Access and File System Management.

This Mobile FeliCa OS is the code specific to the IC Chip developer, and it is written with the code system specific to the microprocessor or, so to speak, with the machine code. This Mobile FeliCa OS does not provide support to the application download function.

Start-Up Method of Mobile FeliCa OS:
Two start-up methods of Mobile FeliCa OS are available, and selection of Mobile FeliCa OS functions is possible depending upon the start-up method.

1) Start-Up of Mobile FeliCa OS with card Reader/Writer:
With the detection of valid electromagnetic energy transmitted from the external card Reader / Writer by the antenna connected to the TOE, the power is turned ON and the TOE starts it operation. After the start-up, the TOE functions as a contactless IC Chip.

2) Start-Up of Mobile FeliCa OS with Power on:
With the input of valid signal to Power ON terminal pin of the TOE, the power is turned ON and the TOE starts its operation. After the start-up, the TOE functions as a contact IC Chip operating via UART interface.

TOE’s Interface

The interface of this TOE consists of (a) the physical interface, (b) the electrical interface, (c) the logical interface, and (d) the communication interface, (e) the I/O interface.

Physical Interface:
The physical interface of the TOE is whole of surfaces of the IC Chip.

Electrical Interface:
The electrical interface of the TOE is whole of external terminal pins of the IC Chip.
The external terminal pins of the IC Chip comprise of (a) Power Supply pins, (b) Logic pins, and (c) Analog pins.

Logical Interface:
The logical interface of the TOE comprises of (a) the UART interface, and (b) the RF interface.

Communication Interface:

The communication interface of the TOE is achieved by the commands that pass through the RF interface or through the UART interface.

I/O Interface:

I/O Interface of the TOE is the interface for the control to the hardware from the software.

Intended Use of TOE

This ST assumes the operating condition where the TOE is installed to a Mobile Device product. Therefore, be careful that this document describes operation of the TOE where IT products falling outside the scope of the TOE are included.

This document assumes the following operating conditions where the TOE is installed to a Mobile Device product:

- the case where the TOE accesses as the electronic train pass to the card Reader / Writer installed at a railway station, or
- the case where the TOE accesses as the electronic wallet to the card Reader / Writer installed at a convenience store, or
- the case where the TOE accesses as the electronic wallet to the remote server for electronic payment, and
- the case where the TOE is used as the storage media for data exchange between the server and the card Reader / Writer.

Overview of TOE Environment

This TOE is the "IC Chip and Embedded Software" for use in the Mobile Device. Thus, the operating environment (outside the TOE) of this TOE is Mobile Device to which this TOE is installed, Controller for Mobile Device, RF Antenna, card Reader / Writer, Controller (for card Reader/Writer) and Server.

System Structure of TOE (Out Scope of TOE)

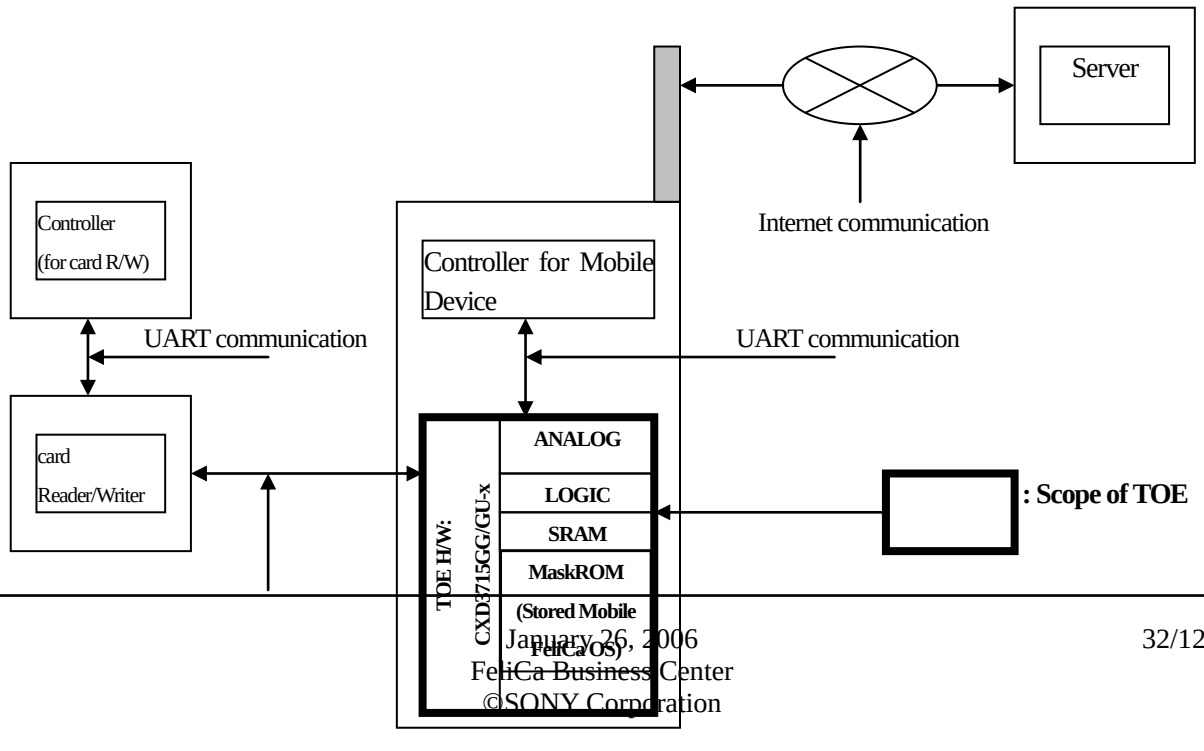


Figure 4. Product and System structure of the TOE

System structure of TOE (IT products outside the scope of TOE)

Mobile Device:
The Mobile Device is the carrier for installation of the CXD3715GG/GU-x product (the TOE).

Controller for Mobile Device (internal controller):
This is the controller installed to the Mobile Device, and used as the controller to provide control to the communication between the TOE and the server.
In accessing to the TOE, a secure access can be established utilizing the authentication function.

Server (external controller):
The server (external controller) is the IT product installed in a remote location, and provides various types of services.
In accessing to the server from the TOE, a connection is established utilizing the communication function of the Mobile Device.
In the communication between the server and the Mobile Device, secure Internet communication can be established utilizing cipher.
This server is the capable of accomplishing secure management of data transmitted from the TOE.
It is possible, in addition, to import (or export) the data from this server to EEPROM area in the TOE.

RF Antenna:
This is the antenna to establish the RF communication between the TOE and the card Reader / Writer.

card Reader/Writer:
"card Reader / Writer" is the IT product installed to the local environment to provide various types of services.
In accessing to the card Reader / Writer from the TOE, connection is established utilizing RF communication by RF antenna installed to the Mobile Device.
This card Reader / Writer is the capable of establishing secure management of data transmitted from the TOE.
It is possible, in addition, to import (or export) the data from this card Reader / Writer to EEPROM area in the TOE.

Controller (for card Reader/Writer):
Controls card Reader/Writer via UART I/F and is part of the host (e.g. a PC connected to the card Reader/Writer).

Personnel involved in the intended operation of TOE

1) **"0th" Issuer**: the "0th" issuer is given the authority and takes the responsibility to a part of security functions during manufacture and operation of the TOE.
   - the "0th" issuer is given the authority to set up the upper limit for the authentication trial times.

2) **"1st" Issuer**: the "1st" issuer is given the authority and takes the responsibility for issuance of the TOE.
   - the "1st" issuer is given the authority for release of the lock to authentication.
     the "1st" issuer is given the authority to set up the area files and the service files to which a key is added.

3) **"2nd" Issuer**: the "2nd" issuer is given the authority and takes the responsibility for operation of the TOE.
   - Within the area assigned by the "1st" issuer (or the "2nd" issuer), authority for setting the area file (with a key added to it) as well as the service files is given to the 2nd issuer.

4) **End User**:
   - The end user is the person who utilizes the carrier to which the TOE is installed.

IT and Security Features

Product type of this TOE is "IC Chip for Mobile Device".
The IC Chip for Mobile Device is the IC Chip that incorporates, in addition to the functions of IC card manufactured utilizing FeliCa technologies, the capability for RF communication with the external card Reader / Writer as well as for UART communication with the controller for Mobile Device.
The functions of this IC Chip can be classified into following categories:

Contactless IC Chip Function:
With the addition of antenna for RF communication, this IC Chip functions as the contactless IC Chip conforming to FeliCa Technologies System, and it is possible to access to the internal non-volatile memory.

Contact IC Chip Function:
With the use of UART interface, this IC Chip functions as the contact IC Chip conforming to FeliCa Technologies System, and it is possible to access to the internal non-volatile memory.

Triplicate Communication Function:
With the addition of antenna for RF communication, it is possible to provide the channel for communication between the controller for Mobile Device (connected with the TOE via UART interface) and the external card Reader / Writer.

To this contactless / contact IC Chip functions, functions such as Multiple Division Function of File System are added while succeeding the communication system, the file system and the command set used in the conventional FeliCa Technologies System.

TOE provides a secure storage for user data, and associates the security attributes with the stored data. Such attributes are used to determine whether to allow access to the specific block of the data or not.

TOE's memory is partitioned into several files, and these files are configured in a hierarchical file structure. Access to each of these files is possible independent of other files.

Some types of files may be protected using an access key for secure storage of data, and in the case of other files that require no protection of data, read / write of data will be possible with no restriction. By setting attributes concerning various access rights to each of files, it is possible to provide flexible support to applications, for example, that require access to common files.

Each of service providers is capable to assign various service files to area(s) approved to the service provider. Each of service providers is also capable to re-assign any space(s) located in the area(s) assigned to him to service provider(s) other than himself.

Configuration to be evaluated

In this evaluation, the physical boundary of the system is defined by the physical boundary of the IC chip embedded into the carrier. The carrier itself belongs to TOE environment, and not included in this evaluation. Logically, TOE for the purpose of this Security target is the IC chip comprised of an integrated circuit (IC) and software (Mobile FeliCa OS). This includes various mechanisms that make communication with the world external to TOE possible.

Because this TOE executes applications with the configuration comprised of sufficient elements of hardware and software, it is possible to establish a secure channel between itself and the trusted sources.

The configuration to be evaluated is comprised of IC chip and Mobile FeliCa OS provided by Sony Corporation. No application software is included in the configuration to be evaluated.

Assurance to the security of various types of application software is the responsibility of the issuer of the carrier. This IC chip provides only the secrecy and the integrity of data stored to the IC chip utilizing the applications. The IC chip in this configuration to be evaluated is configured as described above.

The Target of Evaluation (TOE), the CXD3715GG/GU-x, version 0701, consists of an IC Chip with Embedded Software for Mobile Device. IC Chip portion is CXD3715GG/GU-x (version 2.1) of the TOE Hardware, and Embedded Software portion is Mobile FeliCa OS of the TOE Software.

(This page is intentionally left blank)

Chapter 3. *TOE Security Environment*

This chapter provides the identification of "TOE Security Environment". Description on "TOE's Security Target" as well as "TOE Environment" that correspond with the security needs will be provided in this chapter.

Security Target for TOE is satisfied by technical / technological countermeasures implemented by TOE.
Security Target for environment is satisfied by technical / technological measures or by non-IT measures implemented by IT environment.

Assumptions about Assets

This section describes assumptions about assets to which TOE shall provide protection.

Assets of TOE in this Security target can be categorized into three (3) types: that is, the physical asset, the logical asset, and the secondary asset.
The physical asset indicates TOE's hardware. The logical asset indicates TOE's software and data. The secondary asset indicates development materials, design materials, testing materials, and materials for generation of personalization.

TOE's Physical Asset

The IC chip is assumed to be TOE's physical asset in this Security target.

1. IC chip

1-1.	CPU:	Operational circuitry for data processing.
1-2.	EEPROM:	Memory element capable to electrically write/delete the content of program.
1-3.	SRAM:	RAM (Random Access Memory) element that requires no data refreshing cycle.
1-4.	MaskROM:	Memory element of non-volatile type exclusive for use of data read-out
1-5.	Co-processor:	Auxiliary processor with extended capability for cryptographic processing.
1-6.	Bus-line:	Communication lines for data transfer between each of circuits in the IC chip.
1-7.	I/O Ports:	Interfaces with external devices.

TOE's Logical Asset

The data to be stored, processed and transferred on TOE's physical asset is assumed to be TOE's logical asset in this Security target.

2. Mobile FeliCa OS

2-1. User data

4-1:	Area0000 File
4-2:	Area File
4-3:	Service File
4-4:	Service Block Data

3.TSF data

3-1:	Access Key
3-2:	Execution Key

TOE's Secondary Asset

Materials / data to be controlled external to TOE are assumed to be TOE's secondary asset in this Security target.

5-1: TOE's development materials / data
5-2: TOE's design materials / data
5-3: TOE's testing materials / data
5-4: TOE's materials / data for generation of personalization

Assumptions about Environment & Method of Use

This section provides the description of various assumptions about (a) intended TOE environment, and (b) intended methods of TOE use.
Assumptions are presented with bold fonts followed by application notes.
Application notes are presented with non-bold fonts, and provide additional information as well as description on assumptions.

Assumptions about human factors

A.Priv Abuse by Privileged Users
Administrators and other privileged users are trustworthy.

A privileged user or administrator could directly implement or facilitate attacks based on any of the threats described here. We assume that this threat is handled through the organizational policies and controls.

Assumptions about physical factors

A.Data_Store Off-TOE Data Storage
It is assumed that management of TOE data that stored external to TOE is done in a secure manner.

The carrier issuer or the service provider may store important information concerning TOE's profile, personalization and proprietary rights to a database not associated with TOE.
Such information may be useful for cloning attacks, and because of this, it is important to maintain the security of such data in an adequate manner.

A.Key_Supp Cryptographic key Support
It is assumed that all the imported cryptographic keys are supported in a secure manner even on a database external to TOE.

Various keys are imported for use on TOE. These keys are shared secret keys and synthesized composite keys.
These keys are provided from various organizations that control the operations of system on which TOE is functioning. It is assumed that generation, delivery, maintenance, and destruction of these keys are done in an appropriate and secure manner.

Assumptions about connection

A.Sec_Extrw External Reader/Writer Secure

It is assumed that the external Reader/Writer (with which TOE establishes a secure link) is secure.

It is possible to make the External Reader/Writer be equipped with the capability of establishing a secure channel of communication with TOE.
This may be realized utilizing the shared private key, a pair of public key and private key or other stored key, or a generated session key.
Once such a secure link was established, TOE may assume such an External Reader/Writer to be adequate and secure for execution of trusted communication.
The external Reader/Writer is considered to be outside the coverage of this ST.

A.Sec_Intcontroller Internal Controller Secure

It is assumed that the internal controller (with which the TOE establishes a secure link) is secure.

It is possible that the internal controller have capability to establish a secure communication channel with the TOE.
This may be realized utilizing the shared private key, a pair of public key and private key or other stored key, or a generated session key.
Once such a secure link was established, TOE may assume such an Internal Controller to be adequate and secure for execution of trusted communication.
The internal controller is considered to be outside the coverage of this ST.

Assumed Threats

This section provides the description about threats against which TOE shall counter. Each of threats is presented with bold fonts followed by application notes. Application notes are presented with non-bold fonts, and provide additional information as well as descriptions on threats.

T.Inherent Inherent information leakage

It is possible that information leaked from the TOE during using is abused to disclose confidential data (User Data, TSF Data)

TOE must be prevented from direct contact to internals. It is possible that Leakage is occurred through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements.

T.Physical_Probing Physical Probing

It is possible that physical probing of TOE is performed for the following;

(i) disclosing User Data,

(ii) disclosing other critical operational information especially TSF data.

Direct contact is needed to the TOE circuit structure in physical probing. Before the attacks, hardware security mechanisms and layout characteristics need to be identified.

T.Physical_Manipulation Physical Manipulation

It is possible that hardware is modified for the following;

(i) modifying security features or functions of the TOE,

(ii) modifying User Data.

It is possible that the modification is achieved through common techniques as failure analysis and reverse engineering for IC Chip, and causes unworking of a security function. As with T. Physical Probing, before the attacks, hardware security mechanisms and layout characteristics need to be identified. Circuitry and/or data is able to be changed permanently or temporarily.

T.Malfunction Malfunction caused from Environmental Stress

It is possible that a malfunction of the TSF or the Software is caused by environmental stress applied and result in the following;

(i) unworking or modifying security features or functions of the TOE
(ii) unworking or modifying security functions of the Software.

This may be archived by operating the IC Chip outside its normal operating conditions. Unlike T. Physical Manipulation, there is possible that attacks based on environmental stress are done without significant knowledge of the IC's internal construction. And, there is possible that CPU malfunctions as below, as the result of TOE malfunction attributed to malfunction caused from Environmental Stress
(i) to access an undefined memory address
(ii) to execute an undefined instruction code

It is possible that confidential information is outputted or changed by TOE if the condition is left.

T.Forced_Leak Forced Information Leakage

It is possible that information leaked from the TOE during using is abused to disclose confidential data (User Data, TSF Data). The cause of leakage is not inherent but by someone aiming to attack.

This threat related with "T. Malfunction caused from Environmental Stress)" and/or "T. Physical Manipulation" causes leakage from signals without significant information normally.
And, there is possible that CPU malfunctions as below, as the result of TOE malfunction attributed to leakage Forced and such as software failure.
(i) to access an undefined memory address
(ii) to execute an undefined instruction code

It is possible that confidential information is outputted or changed by TOE if the condition is left.

T.Abuse Abuse function

It is possible that an attacker use test functions of Hardware after shipping in order to disclose or manipulate User Data.

T.Crypto_Analysis Crypto Analysis

It is possible that the session key is analyzed in brute-force in the cipher communication after two-way authentication.
If the decrypting is successful, the confidential information in the TOE can be gotten out of or tampered.

T.Leak Leak Information

An attacker may exploit information which is leaked from the TOE during normal usage.

Leakage may occur through emanations, variations in power consumption, I/O characteristics, and clock frequency or by changes in processing time requirements.
This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from direct (contact) measurements or measurement of emanations and can then be related to the specific operation being performed.

T.Forced_Rst Forced Reset

Attackers may cause TOE to be insecure through inappropriate termination of the selected operation.

Attempts to generate an insecure state within TOE may be accomplished by inserting an interrupt or stopping the supply of electric power. Such actions will terminate transaction or communication between TOE and an External Reader/Writer, or TOE and an Internal Controller before its completion, and result in a defective state of TOE.

T.Power Power Supply Failure data Protection

When an External Reader/Writer is used, the electric power is supplied from the External Reader/Writer. In this case, data may be damaged because of faulty power supply.

When an External Reader/Writer is used, the electric power is supplied from the External Reader/Writer to TOE. This electric power may be interrupted during normal execution of tasks.
If any faults of electric power supply occurred during transaction, the data stored to the memory within TOE may be damaged.

T.OP_Ftn Use of Unallowed Operation Function

Attackers may execute a command of different type during TOE's normal operation to generate abnormality in the life cycle intending leakage, falsification, destruction, or peeping of user data and/or TSF data.

Interaction between different phases of the operation is so characterized that a command (or commands) unnecessary or inhibited to the specific phase(s) of operation can be executed.
For example, functions (such as functions for testing/debugging, or native COS function) generally unnecessary or may deteriorate the level of security may be utilized.

T.Access Invalid Access

TOE's users or attackers may attempt to tamper the objective user data or TSF data through access to information and/or assets without permission by the owner or the personnel responsible to such information or assets.

Personnel of authorized position is given the specific privilege as adequate to access to the selected area(s) within each of TOE as well as to access to the information stored to that area(s).
With the access beyond such specified privilege, some of data having the value of its own (such as the data of electronic money) may become the target of attack intending to tamper the data without damage to TOE.

T.Inteface_Prob External Interface Probing

Attackers may attempt analysis of user data and/or TSF data through wiretapping of data transferred via the interface established between TOE and the secure External Devices (External R/W, External Controller).

Attackers may attempt to perform analysis of the transferred data by wiretapping of data being transferred via the interface established between TOE and the External Devices.

T.Reuse Replay Attack

Unauthorized user(s) or authorized user(s) may intrude into the TOE through re-use of previously valid data, invalid data, or deleted file(s)/data utilizing completed or partially completed operation.

To bypass various security mechanisms or to expose the information related with the security, attackers may access to previously valid data, invalid data, or deleted file(s)/data with the intention to re-use them utilizing completed or partially completed operation.

T.Repeat Repeat Attack

Unauthorized user(s) may intrude into the TOE by repeated execution of the same command.

Unauthorized user(s) may execute the same command repeatedly, intending acquisition of the security data and user data.

T.First_Use Fraud on First use

Attackers may attempt to access to TOE information through unauthorized use of a new TOE not issued yet.

The process of issuing carriers includes the work of TOE be set up, or loading of security-related information to TOE.
Using a TOE not issued yet without such mandatory approval, attackers may attempt fraudulent use of TOE.

T. Crypt_Atk Cryptographic Attack

Attackers may attempt to break the security function through attacks or forced attack measures against the cryptographic algorithm.

This type of attack will be focused to either the Encode/Decode function or the Random Number Generator.

T.Clon Cloning

Attackers may attempt cloning a part or whole of fully functioning TOE, intending to perform further attacks.

The information necessary in cloning a part or whole of TOE may be acquired through the detailed inspection of TOE or unauthorized use of the design information of TOE.

T.Logic_Atk Logical Attack

An attacker or authorized user of the TOE may compromise the security features of the TOE by defeating the logic of the TOE.

The attacker may be able to determine the logical structure and operation of the TOE through a number of techniques.
Insertion of selected inputs followed by monitoring the output for changes is a Relatively well known attack method for cryptographic devices that can be applied to this TOE as well.
The intent is to determine user and TSF related information based on how the TOE responds to the selected inputs.
Invalid input may take the form of operations which are not formatted correctly, requests for information beyond register limits, or attempts to find and execute undocumented commands.

T.Delivery Attacks during delivery

Attackers may attempt interception or tampering of the contents of TOE during delivery of TOE.

Attackers may attempt interception of software or hardware comprising of TOE during delivery of the TOE.
Attackers may be capable to disclose the information related to TOE design as well as the security information contained in the part(s) being delivered.
In addition, attackers may be capable to induce changes in TOE's security mechanism and to mount attacks to TOE utilizing these changes.

Organizational Security Policies

TOE shall comply with the organizational security policies stated in the following paragraphs.
Each of security policies is presented with the bold-fonts followed by application notes.
Application notes are presented with non-bold fonts, and provide additional information and description of security policies.

P.Info_Protect Information Protection
The important information for the development and production of TOE should be treated as the confidentiality to prevent it from leakage, falsification and loss. The procedures should be prepared and the appropriate education should be provided to the personnel needed.

P.Crypto_Std Cryptographic Standards
Where cryptography is required to provide mutual authentication and to protect confidentiality, the TOE this shall use DES and triple DES algorithms, on the basis that they are well-defined and mature.

P.Data_Acc Data Access
Except for a well-defined set of allowed operations, the right to access specific data and data objects is determined on the basis of: the owner of the object, the identity of the subject attempting the access, and the implicit or explicit access rights to the object granted to the subject by the object owner.

The TOE may be associated with a number of different authorities which are the system integrator, the card issuer, and the system manager. Each of these may have specific rules for accessing the data contained in the TOE. Certain rules can be established in all cases as represented in the access control SFP detailed in security functional requirement FDP_ACF.1. Others need to be explicitly supplied in policy statements determined by the owner of the object in question.

P.Ident Identification

TOE shall be capable to be uniquely identified (i.e., distinct from others).

TOE is comprised of hardware (IC Chip) and software (Mobile FeliCa OS) elements.
The Mobile FeliCa OS stored to MaskROM of IC Chip developed for use on Mobile Device.
The software may be stored to a hardware mask (i.e., integrated into a photo-mask for ROM) or may be stored to a non-volatile memory.
Hardware may have optional features, and it is possible to activate or deactivate such options.
For correct implementation of the end product conforming to this ST, TOE is required to be set up so that correct identification of TOE is possible.
Because of this, TOE is required to be uniquely identified (i.e., distinct from others).

P.Sec_Com Secure Communications

Protocols and procedures for the secure communication between TOE and trusted terminals shall be supported.

TOE may engage in various types of communication ranging from the simple checking of status to the secure transfer of data.
Because TOE's communication covers rather a wide range, it is recognizable that the scenario of TOE's communication performed utilizing TOE's RF or UART interfaces between TOE and External Reader/Writer as well as TOE and Internal Controller will be a wide-ranging one.
TOE shall be capable to establish a secure channel with trusted sources at least to execute various commands executed by personnel who may have privilege.

(This page is intentionally left blank.)

Chapter 4. Security Objective

This chapter provides the description of TOE's Security Objective as well as TOE's Environment that correspond with the Security Needs identified in Chapter 3 "TOE Security Environment" of this document.

The security objective for TOE is satisfied by the technical and technological measures to be implemented by TOE.
The security objective for TOE environment should be satisfied by the technical and technological measures or the non-IT measures to be implemented by IT environment.

Security Objectives to which TOE should conform

TOE should conform to the security objectives detailed in the following paragraphs.
Each of the security objectives is presented with bold fonts followed by application notes.
Application notes are presented with non-bold fonts, and provide additional information and descriptions of security objective.

O.Physical_Probing Physical Probing

TOE shall be designed and manufactured to resist physical probing on the hardware.

TOE shall have a resistivity to physical probing from the chip surface, which might leads to disclosure of User Data and/or TSF Data, by implementing physical shielding.

O.Physical_Manipulation Physical Manipulation

TOE shall be designed and manufactured to resist physical manipulation on the hardware.

TOE shall have a resistivity to physical manipulation from the chip surface, which might leads to manipulation and/or disclosure of User Data and/or TSF Data, by implementing physical shielding.

O.Env_Protect Environment Protect

TOE shall generate reset signal internally, if it is exposed to the environment out side of the guarantee of proper operation, and then it stops its operation by the reset.

TOE shall protect itself from revealing security information or operating in an insecure fashion when exposed to out of standard conditions by having a structure which can detect abnormal environmental conditions. The factors of environmental conditions are voltage, clock frequency or continuous access time to TOE.

O. Forced_Protection Forced Information Protect

TOE shall generate reset signal internally, if the malfunction of TOE is detected, and then it stops its operation by the reset.

As the method of protection against environmental stress, TOE shall be equipped with the security functions for protection against malfunction. Possible malfunctions are

(a) errors in DES calculation

(b) execution of undefined instruction codes

(c) access to undefined memory address.

O.Leak_Information Leak Information Protect

TOE should be implemented the measure to prevent form leaking the confidential information during the normal performance, and TOE shall protect its session key from Brute force attacks.

This Normal operation includes operations such as (a) to maintain any type of keys, (b) to provide cryptographic procedures such as encryption and or decryption, or (c) to process the data stored in TOE in a secure manner when performing data transfer between TOE and external devices through an RF interface and UART Interface.

O.Abuse Abuse function protect

TOE should be implemented the measures to prevent from abusing (aiming at destruction or an unauthorized use) the Hardware Test mode and SCAN function of TOE

O.Power Power Loss Recovery

Even if the supply of electric power to TOE stopped because of an accident, TOE shall protect the integrity of data.

When used an External Reader/Writer, the electric power to TOE is supplied from the External Reader/Writer, and interruption of the supply of electric power may occur during transaction. TOE shall recover from the interruption of electric power in a manner so that no corruption of the stored data occurs.

O.Init Initialization

TOE shall enter into its initialization sequence just after the power-on, reset or other re-start conditions.

Regardless of the process how it was reset, TOE shall always start its operation from the defined and controlled status.
This security objective shall act to protect TOE against any attacks intending to put TOE into faulty operation and to cause undefined state.

O.Sec_Com Secure Communication

TOE shall protect its resources from attacks mounted to the data being transferred via an External Interface by providing support to the protocols and the procedures for secure communication between TOE and trusted External Devices.

TOE shall provide mechanisms to establish and maintain the secure information link with External Devices to make difficult the analysis of data transferred through interfaces established between TOE and External Devices even if attackers succeeded to intercept such data.

O.Data_Acc Data Access Control

TOE shall provide users with measures to control and restrict the access to objects and assets owned by the users (or to which the users are responsible) in accordance with the rule(s) as defined in P.Data_Acc Data Access, in user-by-user (or users identified as a group of users) basis.

TOE may have various types of users, administrators, TOE issuers or organizations, and requires some control to the assets handled by each of them. Some of rules for asset control are applicable to all the cases.
These rules shall be explicitly stated depending upon the needs of data owners.

O.Mode Mode Functions

The TOE shall provide measures to control and restrict the command(s) specific to the normal operation can be used only in the intended phase(s) of operation.

The TOE shall be designed and implemented so that the command(s) possible to use only in specific operation phase(s) be associated with the appropriate operation phase(s). In this way, Debug function or Load function of identification information only once shall be so designed that such functions are impossible to use after that.

O.Reuse Replay

TOE shall protect its resources from Replay attacks.

Even if attackers attempted attacks to TOE intending deterioration of the security through replay or re-start of operation that completed to its end or interrupted midway, TOE shall act so that the security of its assets is not deteriorated by such attacks.

O.Limit Command Repeat Limit

TOE shall prevent sequential execution of illegal mutual authentication by counting the number of failed times of mutual authentication trials.

Upper limit for the number of failed times of mutual authentication trials shall be determined beforehand, and in the case when the number of failed times of mutual authentication trials reached to the upper limit mentioned above, the TOE shall reject further reception of mutual authentication command after that.

O.Set_Up Set-Up Sequence

TOE shall require a series of defined operations before entering into its general use state.

The TOE shall be placed into operation in a controlled and defined manner. This objective acts to prevent use of TOE before all of the protective measures may be enabled.

O. Crypt Cryptography

TOE shall support cryptographic functions in accordance with P. Crypt_Std Cryptographic Standards.

To maintain the security level provided by the basic cryptographic function in accordance with **P.Crypt_Std Cryptographic Standards,** TOE shall execute the cryptographic operations conforming to the policy of use and the specification of the cryptography set up.

O.Log_Prot Logical Protection

The TOE must protect itself against logical compromise by having a structure which is resistant to logical manipulation or modification.

The TOE must be designed and programmed so that it resists attempts Compromise its security features through attacks on its logical operation.
The TOE must prevent the release of secure information while it is operating properly in the presence of logical probes and command modifications.

O.I_Leak Information Leakage

The TOE must provide the means of controlling and limiting the leakage of information in the TOE so that no useful information is revealed over the power or I/O lines.

The TOE must be designed and programmed so that analysis of power consumption or communication patterns does not reveal information about processing operations or compromise secure information.

O.Ident TOE Identification

TOE shall support Save and Store operations of the identification information.

TOE is comprised of hardware and software elements.
The software is stored to a hard mask (integrated into a photo mask of ROM).
Hardware and software features vary depending upon the version of products.
So, accurate identification is indispensable for the demonstration that a product is the end product conforming to this Security Target.
Because of this, the identification claiming that TOE is unique (i.e., distinct from others) is necessary.

Security Objectives to which Environment should conform

IT Security Objectives for TOE Environment

This sub-section provides the description of IT security objectives necessary to be satisfied by imposing technical and technological requirements to TOE environment.
These security objectives are necessary because of Security target set up for TOE environment.
To support TOE's security objective, these security targets are included in ST as required (i.e., at the time of Security Target preparation).
Each of the security objectives is presented with bold fonts followed by application notes (with non-bold fonts). Application notes provide additional information and descriptions.

OE.Sec_Extrw External Reader/Writer Secure Communication
A trusted External Reader/Writer shall be made available to provide secure communication with TOE.

The External Reader/Writer is capable to accept and maintain the secure communication link with TOE. Secure communication can be established utilizing cipher and authentication.

OE.Sec_Intcontroller Internal Controller Secure Communication

A trusted Internal Controller (Controller for Mobile Device) shall be made available to provide secure communication with TOE.

The Internal Controller (Controller for Mobile Devoice) is capable to accept and maintain the secure communication link with TOE. Secure communication can be established utilizing cipher and authentication.

OE.Key_Supp Cryptographic Key Support
All the cryptographic keys imported in association with TOE shall be supported in accordance with the needs of the owner.

Various types of shared keys may be imported for use on TOE or in association with TOE. These keys are provided from various organizations that control the operation of system on which TOE is operating. The personnel and systems responsible to these keys shall provide the security necessary in generation, delivery, maintenance and destruction of such keys.

Non-IT Security Objectives for TOE Environment

This sub-section provides the description of "non-IT security objectives" to be satisfied without imposing technical and technological requirements to TOE.
That is, these non-IT security objectives do not require implementation of TOE's hardware or software functions. By addressing the points of security issue set by these security objectives in the TOE environment, such points of security issue are included in the Security target as necessary in ST (Security Target) at the time of its generation.
Each of Security Objectives is presented with bold fonts followed by application notes. Application notes are presented with non-bold fonts. These application notes provide additional information and descriptions.

OE.Pers Personnel

Administrators and/or other personnel who work as privileged personnel shall be carefully chosen regarding their confidence and be given good training.

Administrators and/or other personnel who work as privileged personnel shall be carefully chosen and be given good training so that they would act to detect, prevent or take adequate countermeasures to any attacks mounted to TOE from outside world.

OE.Data_Store Off-TOE Data Storage

All the TOE data stored outside TOE shall be controlled to maintain the secrecy and the integrity of such data in accordance with the needs of owner of such data.

Various types of TOE information may be stored separate from TOE. The information relates with proprietary rights, issuer's data, and personalization. Personnel and the systems that handle the information shall be responsible to maintain the security needed by such information.

OE.Delivery Delivery procedures
TOE shall be delivered by secure procedures.

TOE's software and hardware shall be delivered by secure and approved procedures ensuring that attacker's interception to information contained in TOE or some parts of it is difficult with a simple method.
The procedures shall include the procedure for checking the integrity and the secrecy of TOE.

OE.Phys_Sec Physical Security
Through Development and production of TOE, the measures to protect information appropriately are implemented including the physical aspects.

(This page is intentionally left blank.)

Chapter 5. *IT Security Requirements*

IT Security Requirements include following items:

1. **TOE's Security Function Requirements (SFR)**:
   That is, the requirements concerning security functions such as Information Control, Identification, and Authentication.

2. **Extended SFR (FCS_RNG.1 and FMT_PUT.1):**
   That is, the newly created requirements concerning security functions such as Random numbers generator and Hardware Test Mode Protect

3. **Strength of Function**:
   The minimum strength of function conforming to the security target is required, and functions implemented through probabilistic or permutational mechanisms shall be provided.

4. **Requirements concerning with TOE's Security Assurance (SARs, Security Assurance Requirements)**:
   That is, justification for the claim that TOE is conforming to the Security Target (for example, configuration management of the system, testing, and evaluation of vulnerability) shall be provided.

5. **Security Requirements on TOE's Environment**:
   That is; hardware, software external to TOE, procedures and policies for operation, and those necessary in the fulfillment of TOE's Security Target.

Discussions on these requirements will be found in the following paragraphs in item-by-item basis.

TOE Security Function Requirements

This section describes SFR (Security Function Requirements) for TOE.

Table 1. Summary of TOE's Security Function Requirements (SFR)

SFR ID	SFR Name	TOE Hardware	TOE Software
FCS_CKM.1	Cryptographic key generation		X
FCS_CKM.4	Cryptographic key destruction		X
FCS_COP.1	Cryptographic operation	X	X
FCS_RNG.1	Random numbers generator		X
FDP_ACC.1	Subset access control		X
FDP_ACF.1	Security attribute based access control		X
FDP_ETC.1	Export of user data without security attributes		X
FDP_IFC.1	"Subset information flow control"	X	X
FDP_IFF.1	Simple security attribute		X
FDP_ITC.1	Important of user data without security attributes		X
FDP_ITT.1	Basic internal transfer protection	X	
FDP_UCT.1	Basic data exchange confidentiality		X
FDP_UIT.1	Data exchange integrity		X
FDP_SDI.1	Stored data integrity monitoring		X
FIA_AFL.1	Authentication failure handling		X
FIA_UAU.2	User authentication before any action		X
FIA_UID.1	Timing of identification		X
FMT_PUT.1	Hardware Test Mode Protect	X	
FMT_MOF.1	Management of security functions behavior		X
FMT_MSA.1	Management of security attributes		X
FMT_MSA.2	Secure security attributes		X
FMT_MSA.3	Static attributes initialization		X
FMT_MTD.1	Management of TSF data		X
FMT_MTD.2	Management of limits on TSF data		X
FMT_MTD.3	Secure TSF data		X
FMT_SMF.1	Specification of Management Functions		X
FMT_SMR.1	Security roles		X
FPT_FLS.1	Failure with preservation of secure state	X	X
FPT_ITC.1	Inter-TSF confidential during transmission		X
FPT_ITI.1	Inter-TSF detection of modification		X
FPT_ITT.1	"Basic internal TSF data transfer protection"	X	
FPT_PHP.3	Resistance to physical attack	X	
FPT_RCV.4	Function recovery		X
FPT_RPL.1	Replay detection		X
FPT_SEP.1	TSF domain separation	X	
FPT_TDC.1	Inter-TSF basic TSF data consistency		X
FRU_FLT.1	Degraded fault tolerance	X	
FTP_ITC .1	Inter-TSF trusted channel		X

TOE Hardware Security Function Requirements

The minimum level of the functional strength requested for the TOE's Hardware security requirements is "SOF-Basic".

Table 2. TOE Hardware Security Functional Requirements

Functional component ID	SFR Name	Operation	Strength Of Functions
FRU_FLT.1	Degraded fault tolerance	Assignment	
FPT_FLS.1.1A	Failure with preservation of secure state	Assignment	
FPT_SEP.1	TSF domain separation	N/A	
FPT_PHP.3	Resistance to physical attack	Assignment	
FPT_ITT.1	"Basic internal TSF data transfer protection"	Selection	
FDP_IFC.1.1A	"Subset information flow control"	Assignment	
FDP_ITT.1	Basic internal transfer protection	Assignment Selection	
FCS_COP.1.1A	Cryptographic operation	Assignment	
FMT_PUT.1	Hardware Test Mode Protect	N/A	

FRU_FLT.1 Degraded fault tolerance

FRU_FLT.1.1 The TSF shall ensure the operation of [TOE's capabilities shown below] when the following failures occur: [exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1)].

Refinement : The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined below. TOE's capabilities are

-against abnormal supply voltage : all functions
-against abnormal clock frequency : all functions
-against abnormal clock duty ratio : all functions
-against malfunction of DES calculation : detection of DES malfunction and reset function
-against undefined instruction codes and undefined memory address : detection of undefined instruction codes and undefined memory address and reset function
-against longer-than-expected access to TOE : all functions

The component supporting the SFRs Degraded fault tolerance (FRU_FLT.1) and Failure with preservation of secure state (FPT_FLS.1) shall be protected from interference of the Embedded Software.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1A The TSF shall preserve a secure state when the following types of failures occur: [exposure to operating conditions which may not be tolerated according to the requirement Degraded fault tolerance (FRU_FLT.1)].

Refinement: The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" shown below.

-abnormal supply voltage
-abnormal clock frequency
-abnormal clock duty ratio
-malfunction of DES calculation
-attempt to execute undefined instruction codes
-attempt to access undefined memory address
-longer-than-expected access to TOE

The component supporting the SFRs Degraded fault tolerance (FRU_FLT.1) and Failure with preservation of secure state (FPT_FLS.1) shall be protected from interference of the Embedded Software.

FPT_SEP.1 TSF domain separation

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

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

Refinement: The component supporting the SFRs Degraded fault tolerance (FRU_FLT.1) and Failure with preservation of secure state (FPT_FLS.1) shall be protected from interference of the Embedded Software.

FPT_PHP.3 Resistance to physical attack

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

Refinement: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of the attacks, the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "responding automatically" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [disclosure] when it is transmitted between separate parts of the TOE.

Refinement: Memories, Resisters, I/Os are seen as separated parts of the TOE.

FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1 The TSF shall enforce the [Data Processing Policy] to prevent the [disclosure] of user data when it is transmitted between physically-separated parts of the TOE.

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1A The TSF shall enforce the [Data Processing Policy] on [all confidential data when they are processed or transferred by the TOE or by the Embedded Software].

Data Processing Policy: User Data and TSF data shall not be accessible from the TOE except when the Embedded Software decides to communicate the User Data via such an external interface. The protection shall be applied to confidential data only, but without the distinction of attributes controlled by the Embedded Software.

Application note: Part 2 of the Common Criteria defines the dependency of FDP_IFC.1 (information flow control policy statement) on FDP_IFF.1 (Simple security attributes). The specification of FDP_IFF.1 would not capture the nature of the security functional requirement nor add any detail. As stated in the Data Processing Policy referred to in FDP_IFC.1.1A there are no attributes necessary. The security functional requirement for the TOE is sufficiently described using FDP_ITT.1, FPT_ITT.1 and its Data Processing Policy (FDP_IFC.1). Therefore the dependency is considered satisfied.

FCS_COP.1 Cryptographic operation

FCS_COP.1.1.A The TSF shall perform [encryption / decryption of data] in accordance with a specified cryptographic algorithm [Data Encryption Standards (DES) and CBC-Mode] and cryptographic key sizes [112 bits (Triple-DES) or 56 bits (DES)] that meet the following: [FIPS-PUB 46-3, 1999 October 25, DATA ENCRYPTION STANDARD (DES).

Application Note: FCS_COP.1.1A

TOE has a co-processor for DES calculation as hardware, which supports Mobile FeliCa OS in various DES calculations as described in TOE Software Security Function Requirements.

Extended SFR: FMT_PUT.1

FMT_PUT.1 Hardware Test Mode Protect

FMT_PUT.1 The TSF shall be designed in a manner that prevents the hardware test function availability after the hardware production lifecycle.

Application Note: FMT_PUT.1

Availability of the hardware test function is up to the process 4 of the hardware production lifecycle that is defined in “Life Cycle Scope of TOE.” in Chapter 2.

TOE Software Security Function Requirements

The minimum level of the functional strength requested for the TOE's Software security requirements is "SOF-Basic".

Table 3. TOE Software Security Functional Requirements

Functional component ID	SFR Name	Operation	Strength Of Functions
FPT_FLS.1.1B	Failure with preservation of secure state	Assignment	
FPT_RCV.4	Function recovery	Assignment	
FPT_TDC.1	Inter-TSF basic TSF data consistency	Assignment	
FTP_ITC .1	Inter-TSF trusted channel	Selection Assignment	SOF-Basic
FIA_UAU.2	User authentication before any action	N/A	
FIA_UID.1	Timing of identification	Assignment	
FDP_ACC.1	Subset access control	Assignment	
FDP_ACF.1	Security attribute based access control	Assignment	
FMT_SMR.1	Security roles	Assignment	
FMT_MOF.1	Management of security functions behavior	Selection Assignment	
FMT_MSA.1	Management of security attributes	Selection Assignment	
FMT_MSA.2	Secure security attributes	N/A	
FMT_MSA.3	Static attributes initialization	Selection Assignment	
FMT_MTD.1	Management of TSF data	Selection Assignment	
FMT_MTD.2	Management of limits on TSF data	Assignment	
FMT_MTD.3	Secure TSF data	N/A	
FMT_SMF.1	Specification of Management Functions	Assignment	
FDP_IFC.1.1B	Subset information control	Assignment	
FDP_IFF.1	Simple security attribute	Assignment	
FPT_ITC.1	Inter-TSF confidential during transmission	N/A	
FDP_UCT.1	Basic data exchange confidentiality	Selection Assignment	
FCS_CKM.1	Cryptographic key generation	Assignment	SOF-Basic
FCS_CKM.4	Cryptographic key destruction	Assignment	
FCS_COP.1.1B	Cryptographic operation	Assignment	
FCS_RNG.1.1	Random Number Generator		SOF-Basic
FPT_ITI.1	Inter-TSF detection of modification	Assignment	
FDP_UIT.1	Data exchange integrity	Selection Assignment	
FDP_SDI.1	Stored data integrity monitoring	Assignment	
FDP_ETC.1	Export of user data without security attributes	Assignment	

FDP_ITC.1	Important of user data without security attributes	Assignment	
FPT_RPL.1	Replay detection	Assignment	

Table 3. TOE Software Security Functional Requirements (continued)

Functional component ID	SFR Name	Operation	Strength Of Functions
FIA_AFL.1	Authentication failure handling	Selection Assignment	SOF-Basic

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1B The TSF shall preserve a secure state when the following types of failures occurred: [Power failure, communication failure].

FPT_RCV.4 Function recovery

FPT_RCV.4.1 TSF shall ensure that [failure in power supply, failure in communication] have property that the SF either completes successfully, or for the indicated failures scenarios, recovers to a consistent and secure state.

FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [security attributes: access key] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [algorithm for creation of the access key] when interpreting the TSF data from another trusted IT product.

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 [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 [protection of the secret data from abuse by monitoring].

Application Note: FTP_ITC.1.2

Remote trusted IT product: (a) card Reader/Writer (External Reader/Writer),
(b) Controller for Mobile Device (Internal Controller), (c) Server (External Controller).

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [Authentication Command] on behalf of the user to be performed before the user is identified

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

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note: FIA_UAU.2 and FIA_UID.1

FIA_UAU.2 and FIA_UID.1 The card Reader/Writer and Controller are defined as the users for Mobile Device in this ST. Identification of the subject who accesses to the TOE though the card reader/writer and controller is required as the primary action of the Identification and Authentication among the card Reader/Writer, Controller and TOE by comparing the key that stored in the TOE with the key that send from the card Reader/Writer and the controller to TOE.

Application note: FIA_UAU.2

PIN authentication is not User authentication.

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [File Access Control Policy] on [
"Subject: "0th issuer, Object: number of trial times of authentication, Operation: data write (set)",
"Subject: "1st issuer", Object: counter parameter (for authentication lock), Operation: data write (release)",
"Subject: "1st" issuer, and "2nd" issuer, Object: area file, service file, Operation: generation as well as deletion of files"]

Table 4. Subset access control table

Subject / Object	0th issuer	1st issuer	2nd issuer
number of trial times of authentication	data write (set)	N/A	N/A
counter parameter (for authentication lock)	N/A	data write (release)	N/A
Area File	N/A	File generation	File generation
	N/A	File deletion	File deletion
Service File	N/A	File generation	File generation
	N/A	File deletion	File deletion

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [File Access Control Policy] to objects based on the following: [
"Subject: "0th issuer", Object: number of trial times of authentication, Security attributes: none,
"Subject: "1st issuer", Object: counter parameter (for authentication lock), Security attributes: access key for data write (release),
"Subject: "1st" issuer, and "2nd" issuer, Object: area file, service file, Security attributes: access key].

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

subjects and controlled objects is allowed: [

File Access Control Policy:

-Only the "0th" issuer shall be able to set the upper limit for the number of trial times of authentication.

-Only the "1st" issuer shall be able to release the counter parameter (for authentication lock).

-The access key provided from the subject ("1st" issuer, and "2nd" issuer) shall be the one that corresponds with the access key of the object in the TOE.

]

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

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

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles ["0th" issuer, "1st" issuer, and "2nd" issuer].

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

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behavior of] the functions of [number of trial times of authentication] to ["0th" issuer].

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [data write (release)] the [counter parameter (for authentication lock)] to ["1st" issuer].

FMT_MTD.2 Management of limits on TSF data

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [the number of trial times of authentication] to ["0th" issuer].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [authentication lock].

Application note: FMT_MTD.2

When Authentication Lock activated, TOE rejects reception of the command for execution of mutual authentication as well as the commands of which execution is allowed only after successful mutual authentication. It is possible, however, to execute commands that require no mutual authentication.

FMT_MTD.3 Secure TSF data

FMT_MTD.3.1 The TSF shall ensure that only the secure values are accepted for TSF data.

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1A The TSF shall enforce the [File Access Control Policy] to restrict the ability to [creation of the access key in accordance with the combination of area file and service file in the destination of access] the security attributes [access key] to ["1st" issuer and "2nd" issuer].

FMT_MSA.1.1B The TSF shall enforce the [File Access Control Policy] to restrict the ability to [creation of the access key in accordance with the combination of area file and service file for "1st"

issuer identification] the security attributes [access key for data write (release)] to [“1st” issuer].

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only the secure values are accepted for security attributes.

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [File Access Control Policy] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [“1st” issuer, “2nd” issuer] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [the number of trial times of authentication].

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1B The TSF shall enforce the [Data transmission policy] on [Subject: TOE, the card Reader / Writer, controller for Mobile Device. Information: transmission data from the controller for Mobile Device to TOE, transmission data from TOE to the controller for Mobile Device, transmission data from the card Reader / Writer to TOE, transmission data from TOE to the card Reader / Writer. Operation: transmission and reception of data].

Application Note: FDP_IFC.1B

Data Transmit Policy:

-TOE shall give the user permission for access to the data and to TSF data only when such an access was done via a UART or a RF interfaces under the control of the Mobile FeliCa OS.

-TOE shall provide protection to the confidentiality of the user data and TSF data transferred within the TOE regardless of attributes of such user data / TSF data under the control of the Mobile FeliCa OS.

-TOE shall provide protection to the confidentiality and the authenticity of the user data to be transmitted external to the TOE.

-When received user data from a device outside the TOE, the TOE shall verify the integrity of such user data.

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [Data transmit policy] based on the following types of subject and information security attributes: [Subject: TOE, the card Reader / Writer, the controller for Mobile Device. Information: transmission data from the controller for Mobile Device to TOE, transmission data from TOE to the controller for Mobile Device, transmission data from the card Reader / Writer to TOE, transmission data from TOE to

the card Reader / Writer. Security attributes: CRC, checksum, parity check].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- In transmitting the data from the TOE to the controller for Mobile Device, checksum shall be added to the communication data.
- In transmitting the data from the TOE to a card Reader / Writer, CRC shall be added to the communication data.
- In receiving the data from a controller for Mobile Device, TOE shall check the checksum added to the communication data.
- In receiving the data from a card Reader / Writer, TOE shall check CRC added to the communication data.
- In transmitting the cryptographic data from the TOE to the controller for Mobile Device, parity shall be added to the cryptographic data.
- In transmitting the cryptographic data from the TOE to a card Reader / Writer, parity shall be added to the encrypted data.
- In receiving a cryptographic data from the controller for Mobile Device, the parity added to the cryptographic data shall be checked.
- In receiving a cryptographic data from a card Reader / Writer, the parity added to the cryptographic data shall be checked.

].

FDP_IFF.1.3 The TSF shall enforce the [***none***].

FDP_IFF.1.4 The TSF shall provide the following [***none***].

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: [***none***].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [***none***].

FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1 The TSF shall enforce the [Data transmit policy] to be able to [transmit and receive] the objects in a manner protected from unauthorized disclosure.

FCS_COP.1 Cryptographic operation

FCS_COP.1.1B The TSF shall perform [encryption / decryption of data] in accordance with a specified

cryptographic algorithm [Triple Data Encryption Standard (Triple DES) and TCBC-Mode or Data Encryption Standards (DES) and CBC-Mode] and cryptographic key sizes [112 bits (Triple-DES) or 56 bits (DES)] that meet the following: [FIPS-PUB 46-3, 1999 October 25, DATA ENCRYPTION STANDARD (DES), and FIPS-PUB 81, 1980 December 2, DES MODES OF OPERATION].

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [internal random number generation] and specified cryptographic key sizes [112 bits (Triple-DES) or 56 bits (DES)] that meet the following: [AIS20, Functionality class K2, Strength of mechanism high].

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [physical overwriting of keys with a different value by key update function] that meets the following: [none, i.e. there is no standard applicable here].

Extended SFR: FCS_RNG.1

FCS_RNG.1 Random numbers generator

FCS_RNG.1.1 The TSF shall provide [pseudo random numbers] that meet the requirements of [the monobit, poker, run, long run and autocorrelation tests in [AIS20] for Functionality class K2, Strength of mechanism high].

Application Note: FCS_RNG.1
This is supported by an LFSR mechanism provided by the TOE hardware.

FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [check of CRC, check-sum, and parity].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transferred between the TSF and a remote trusted IT product and to perform [destruction of the communication data, and terminating operation of the connection between remote IT product (card Reader/Writer and Controller for Mobile Device)] if modifications are detected.

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the [Data transmit policy] to be able to [transmit and receive] the user data in a manner protected from [modification and replay] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [modification and replay] has occurred.

FDP_SDI.1 **Stored data integrity monitoring**

FDP_SDI.1.1 The TSF shall monitor the user data stored to TSC for [integrity errors: accidental modification or intended unauthorized modification] on all objects, based on the following attributes: [check-sum and CRC check].

FDP_ETC.1 **Export of user data without security attributes**

FDP_ETC.1.1 The TSF shall enforce the [Data transmit policy] when exporting the user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2 **The TSF shall export the user data without the user data's associated security attributes.**

FDP_ITC.1 **Import of user data without security attributes**

FDP_ITC.1.1 The TSF shall enforce the [Data transmit policy] when importing user data, controlled under the SFP, from outside of the TSC.

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

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

FPT_RPL.1 **Replay detection**

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [all the commands to be used after authentication completed].

FPT_RPL.1.2 The TSF shall perform [destruction of the identical command by checking the sequence numbers in IDtc] when replay is detected.

FIA_AFL.1 **Authentication failure handling**

FIA_AFL.1.1 The TSF shall detect when ["an administrator configurable positive integer within [range of values defined by the service provider]"] unsuccessful authentication attempts occur related to [authentication command].

FIA_AFL.1.2 When the specified number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [authentication lock] function.

Application note: FIA_AFL.1

Use can decide the value of the limit number of the Authentication number Lock function. The value can be set at the time of 0^{th} issue.

Strength of Function

Total strength of functions needed for TOE shall be SOF- Basic, in accordance with the recommendation as defined in [CC Part 3].

In the evaluation of hardware aspects of the platform, "Request for CC interpretation number 142 (RI142)" shall be used.
This automatically results in recalling JIL (Joint Interpretation Library), and the evaluation of hardware is done in accordance with the recommendation defined in JIL.

The functional strength level requested for the security functions of this TOE is “SOF-Basic”.
Following functions are required as the TOE’s security functions operating based on the probability and the permutation:

1) SEF.7: Data Encryption (Random number generation)
2) SEF.9: Authentication (Limitation to authentication trial times).
3) SEF.4: Protect against leakage (in DES process)

TOE Security Assurance Requirements

In Table 5 shown in this page, security assurance components extracted from CC Part 3 are enumerated.

Requirements concerning security assurance are described using the presentation extracted from CC Part 3 as they are.

Table 5. Summary of TOE Security Assurance Requirements

Assurance Component ID	Nomenclature of Assurance Components
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 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 function evaluation
AVA_VLA.2	Independent vulnerability analysis

TOE Environment Security Requirements

TOE environment security requirements are based upon the requirements specified in CC Part 2.

TOE environment security requirements are as enumerated in Table 6 below.
These requirements are regarded as the requirements for TOE issuance systems.

The requirements do not conclude in this part.
Conclusion of requirements is entrusted to the service providers to allow them sufficient flexibility in selecting their own environments.

All the requirements stated here are so presented that correct meanings of these requirements can be conveyed to readers without misunderstanding by replacing term "TSF" with term "IT environment".
TOE security requirements on IT environment will be discussed in following paragraphs in detail.

Table 6. Summary of Security Requirements on IT Environment

Functional Component ID	Nomenclature of Functional Component	Operation	Strength of function (SOF)
FCS_CKM.1	Cryptographic key generation	Assignment	
FCS_CKM.4	Cryptographic key destruction	Assignment	
FCS_COP.1	Cryptographic operation	Assignment	
FTP_ITC.1	Inter-TSF trusted channel	Selection Assignment	SOF-Basic

TOE security requirements on IT environment will be discussed in following paragraphs in detail.

FCS_COP.1	**Cryptographic operation**
FCS_COP.1.1	IT environment shall perform [encryption / decryption of data] in accordance with a specified cryptographic algorithm [Triple Data Encryption Standard (Triple DES) and TCBC-Mode or Data Encryption Standards (DES) and CBC-Mode] and cryptographic key sizes [112 bits (Triple-DES) or 56 bits (DES)] that meet the following: [FIPS-PUB 46-3, 1999 October 25, DATA ENCRYPTION STANDARD (DES), and FIPS-PUB 81, 1980 December 2, DES MODES OF OPERATION].
FCS_CKM.1	**Cryptographic key generation**
FCS_CKM.1.1	IT environment shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [random number generation] and specified cryptographic key sizes [112 bits (Triple-DES) or 56 bits (DES)] that meet the following: [none].
FCS_CKM.4	**Cryptographic key destruction**
FCS_CKM.4.1	IT environment shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [physical overwriting of keys with zero bytes or a different key value] that meets the following: [none].
FTP_ITC.1	**Inter-TSF trusted channel**
FTP_ITC.1.1	IT environment 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 any modification or disclosure.
FTP_ITC.1.2	IT environment shall permit [remote trusted IT product] to initiate communication via the trusted channel.
FTP_ITC.1.3	IT environment shall initiate communication via the trusted channel for [protection of the secret data from abuse by monitoring].

(This page is intentionally left blank)

Chapter 6. *TOE Summary Specification*

This chapter describes "IT Security Functions" provided by the TOE to conform to the requirements on the security functions specified in Chapter 5, "IT Security Requirements" of this document.
Each of the security functions is labeled to facilitate reference with the specific function.

This chapter also describes the assurance measures to be taken to ensure the security of development, transportation and operation of the TOE.

IT Security Functions

TOE Hardware Security Functions

Table 7. TOE Hardware Security Functions

Hardware Security Functions	Security Functional Requirements								
	FPT_PHP.3	FRU_FLT.1	FPT_FLS.1.1A	FPT_SEP.1	FPT_ITT.1	FDP_ITT.1	FDP_IFC.1.1A	FCS_COP.1.1A	FMT_PUT.1
SEF.1	X								
SEF.2		X	X	X					
SEF.3					X	X	X		
SEF.4					X	X	X	X	
SEF.5					X	X	X		
SEF.6									X

[SEF.1: Physical Protect]

TOE uses physical shielding in order to resist "Physical Probing" and "Physical Manipulation".

Functional requirement to be satisfied: FPT_PHP.3.

[SEF.2: Protect against failure]

When detected any failures, this security function restores the TOE to the initial condition of LSI and stops operation of the TOE.
"Failures" in this case are as follows:
abnormal voltage
abnormal clock frequency
abnormal clock duty ratio
malfunction of DES calculation
undefined instruction codes are executed.
Undefined memory addresses are accessed.

Functional requirement to be satisfied: FRU_FLT.1, FPT_FLS.1.1A, FPT_SEP.1.

[SEF.3: Protect against cryptoanalysis]

This security function protects the secret information from brute-force cryptoanalysis (cipher decoding technique by attempting all the possible character combinations for keyword) by imposing the restriction to communication session time.
Functional requirement to be satisfied: FPT_ITT.1, FDP_ITT.1, FDP_IFC.1.1A.

[SEF.4: Protect against leakage (in DES process)]

Functions designed to alter the power consumption of the devices.
This security function protects the secret information from leakage forced by DPA during DES computation.

Functional requirement to be satisfied: FPT_ITT.1, FDP_IFC.1.1A, FDP_ITT.1, FCS_COP.1.1A.

[SEF.5: Protect against abuse of Test function]

This security function protects the secret information from leakage and/or falsification caused by abuse of test function present after TOE delivery.

Functional requirement to be satisfied: FPT_ITT.1, FDP_IFC.1.1A, FDP_ITT.1.

[SEF.6 TestModeControl]

This security function imposes restriction to the use of Test Mode of the hardware after manufacture of the product completed.

Functional requirement to be satisfied: FMT_PUT.1.

TOE Software Security Functions

Table 8. TOE Software Security Functions

Mobile FeliCa OS Security Functions	Security Functional Requirements																													
	FCS_COP.1.1B	FCS_CKM.1	FCS_CKM.4	FCS_RNG.1.1B	FPT_FLS.1.1B	FPT_RCV.4	FDP_SDI.1	FTP_ITC.1	FPT_TDC.1	FIA_UID.1	FIA_UAU.2	FDP_ACC.1	FDP_ACF.1	FMT_SMR.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_MTD.3	FMT_MOF.1	FMT_SMF.1	FDP_IFC.1.1B	FDP_IFF.1	FPT_ITI.1	FDP_UIT.1	FPT_ITC.1	FDP_UCT.1	FDP_ETC.1	FDP_ITC.1	FPT_RPL.1	FIA_AFL.1
SEF.7	X	X	X	X				X															X	X			X	X	X	X		
SEF.8					X	X	X	X															X	X	X	X			X	X	X	
SEF.9	X							X	X	X	X																					X
SEF.10												X	X	X	X	X	X	X	X	X	X	X										
SEF.11	X											X	X	X	X	X	X															
SEF.12												X	X	X	X	X	X															

[SEF.7: Data Encryption]

High-level data encryption technologies are employed to prevent a) illegal access to the TOE, b) counterfeiting the TOE, and c) fraudulent use of the TOE.
The high-level data encryption technologies are also adopted to keep the data confidential.

All RF and UART communication path are encrypted by random numbers, which provides superior protection against various illegal attacks such as wiretapping, falsification or reuse of the TOE session.

For the encryption/decryption processes used in the authentication, Triple DES system is adopted to achieve a higher security level of the system.

Session ID is located at the top of data for improvement of security level of the cipher in CBC mode. Session ID is updated and checked at each of sessions so that a same command is possible to use only once during a single session. IN DES, Session Key is used as the key for the encryption process of data. Session Key can be used as "one-time" key in each of sessions for improvement of security level of the system.

By calculating a parity determined depending on data, and adding the parity to the data before encryption process, it is possible to check whether any modification of the data was performed or not at decryption process of the data.

In the encryption process of data, DES in CBC mode is adopted. CBC mode is able to provide a data security level higher than that of EBC mode generally used. If a random number is placed to the top of data (i.e., randomized Session ID), the randomness of data is especially improved.

Functional requirement to be satisfied: FCS_COP.1.1B, FCS_CKM.1, FCS_CKM.4, FCS_RNG.1.1, FCS_IFC.1.1B, FDP_IFF.1, FTP_ITC.1, FPT_ITC.1, FDP_UCT.1, FDP_ETC.1, FDP_ITC.1.

[SEF.8: Data Protection]

When a session is interrupted during writing is detected, the TOE recovers all data blocks that are affected by the write command. All system and user memory blocks affected are examined and the information is restored to the original state by the memory protection mechanism.

The persistent memory of the TOE utilizes check sums for the detection of corruption of data stored in the memory.

By calculating a data-dependent parity and adding such a parity to the data before encryption process, checking whether the data was altered or not is done during the decryption process of data.

The Session ID is updated and replay checked at every transaction to restrict the same command can be used only once during a session.

Functional requirement to be satisfied: FPT_FLS.1.1B, FPT_RCV.4, FDP_SDI.1,
FCS_IFC.1.1B, FDP_IFF.1, FTP_ITC.1, FPT_ITI.1, FDP_UIT.1,
FDP_ETC.1, FDP_ITC.1, FPT_RPL.1.

[SEF.9: Authentication]

Authentication means the process to establish the access key between the card and the Reader/Writer or Controller for Mobile Device. Transmission and reception of the access key data are encrypted by generating random numbers for each other so that the key information cannot be wiretapped or reused.

TOE uses an improved system derived from the 3-way handshake system defined in ISO9798. Based upon the confidential communication system after the authentication completed, an improved security level of system is implemented.

For the encryption/decryption processes used in the authentication, Triple DES system is adopted to achieve a higher security level of the system.

Upper limit of the sequential failed times of command execution trials for mutual authentication is prescribed, and if the number of failed times of mutual authentication trials reached to the upper limit mentioned above, Authentication Lock is activated. This makes difficult to acquire samples necessary for execution of DPA.
Counting method of sequential failed times of command execution trials is as follows:
1) Counts the number of execution times of Authentication1 Command (count 1).
2) Counts the number of execution times of Authentication2 Command (count 2).
When the sum of count 1 and count 2 reached to the prescribed value, Authentication Lock is activated.

After Authentication Lock is activated, TOE rejects further reception of command for execution of mutual authentication as well as commands of which execution is allowed only after successful mutual authentication. Execution of commands that require no mutual authentication is possible, however.

Functional requirement to be satisfied: FTP_ITC.1, FPT_TDC.1, FCS_COP.1.1B,
FIA_AFL.1, FIA_UID.1, FIA_UAU.2.

[SEF.10: Access Control]
The access control features of the TOE were developed to allow for special operations vital for the TOE:

- hierarchical allocation of resources;
- simultaneous access to multiple areas;

The provider can register service files, used to store various data, in the memory area where the provider is granted use in the TOE. Moreover, the provider is permitted to reallocate recursively the area where the provider is granted access to other providers. This system makes it possible to register service files in a hierarchical structure. A unique access key can be set for each area and each service file.

Memories of the TOE are divided into several blocks, and the TOE is given with the authority for access to TOE from each of managers. The relationship between the managers can be represented with a tree diagram. In this tree diagram, the TOE issuer plays the role of "Root", and the issuer and each of the managers takes responsibilities to the service files of their own. Sub-managers take the responsibilities to the branches derived from it.
Each TOE manager is assigned an area, consisting of usable range of service code and number of blocks, by its parent, i.e., issuer or higher manager, and such manager can create its own service and give a part of its area to its offspring, sub-manager.

In TOE, access is controlled in service-by-service basis to prevent unauthorized access.
In accessing to any of services with security attributes, Access Keys are generated and authentication is performed.

For service files, multiple services are possible to authenticate at once. After normal completion of authentication, access is allowed only to service that is authenticated.
For simultaneous access to multiple services, write or read access to multiple blocks are possible.
Access to other services without authorization is inhibited even if such services are located within a same TOE. Prevention of illegal access to service files is possible.

Functional Requirements to be satisfied: FDP_ACC.1, FDP_ACF.1, FMT_SMR.1,
FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_MOF.1,
FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_SMF.1.

[SEF.11: File Registration]

Registration of a new service / area is possible not only at the time of card issuance but after started the operation of a card. Registration of a new service / area is possible only for the personnel who knows the security key of the area of separation source (i.e., parent area). With the registration of a new service / area, the issue package (this package contains information of the service / area to be registered as well as the security key) are generated and transferred to the TOE in accordance with the package generation procedure. Out of the issue package thus transferred, TOE extracts the service / area information and the security key, then generates a new service / area file.

Functional Requirements to be satisfied: FCS_COP.1.1B, FDP_ACC.1, FDP_ACF.1, FMT_SMR.1,
FMT_MSA.1, FMT_MSA.2, FMT_MSA.3.

[SEF.12: Key Change]

This function makes possible to change the security key for a file generated as a result of registration of such a file. Change to the security key is possible only for the personnel who know the security key of the file to be the object of key change. When changed the security key, the new security key generates key change information for prevention of leakage of the security key in accordance with the key change algorithm, and transferred the key change information to TOE. Out of the key change information thus transferred, TOE extracts the new security key, and replaces the old security key with the new security key.

Functional Requirements to be satisfied: FDP_ACC.1, FDP_ACF.1, FMT_SMR.1,
FMT_MSA.1, FMT_MSA.2, FMT_MSA.3.

Security Mechanism Required

The Security Function requires implementation of the following security mechanisms in the TOE:

1. SEF.7: Data Encryption (Random number generation)
2. SEF.9: Authentication (Limitation to authentication trial times).

Assurance Methods

This section describes the assurance measures adopted in TOE to satisfy the requirements concerning assurance of CC EAL4.

Configuration Management

Applicable measures for configuration management include the assignment of unique product identifiers to each of releases of the TOE.
Associated with the product identifier, there is the configuration item list of hardware and software. This configuration item is an example of TOE.
These configuration measures are documented in the following documents:

TOE Hardware

- ACM for TOE Hardware)

TOE Software

- Configuration Management Plan
- Management Process of Contract Objective Document
- Access Management
- Document Management Procedure
- Concurrent Version System
- CM List

Requirements to be satisfied: ACM_AUT.1, ACM_CAP.4, ACM_SCP.2

Development

The architecture documentation satisfies the functional requirements as well as the requirements defined in the high-level design document.
These are specified in the following documents:

TOE Hardware
- Chip Function Specification
- High Level Design Report
- High Level Design Description
- Function Specification
- Test Function Specification
- Security Function Specification
- Test Mode Design Specification
- Logic Design Report
- Anti-Tamper Circuits Design Report
- RTL Source Code
- Net List
- Layout Data
- Tools and Techniques List

TOE Software
- Functional Specification
- High Level Design
- Low Level Design
- Source Code
- Representation Correspondence

Requirements to be satisfied: ADV_FSP.2, ADV_HLD.2, ADV_LLD.1, ADV_IMP.1, ADV_RCR.1. ALC_TAT.1

Security Policy Model

The Security Policy Model is represented in this Security target.

Requirements to be satisfied: ADV_SPM.1

Guidance, Delivery, and Operation

The guidance provided together with this TOE includes the guidance for administrator and the users as well as the complete API Reference of FeliCa commands.
The delivery and operation documents describe the transportation procedures to be used for delivery of the TOE as well as the procedures for activation of the TOE.
These guidance and procedures for delivery and operation are documented in the following documents:

TOE Hardware
- ALC_DVS for TOE (Hardware)

TOE Software
- Delivery Procedure
- Instruction Manual for D3711 0th Issuer Library
- 0 issue Procedure
- RC-S951Wired/Wireless Communication Protocols
- RC-S951Memory Separation Command Specifications
- RC-S951Inspection Command Specifications (for Handset Vendors)
- RC-S951 Inspection Command Specifications (for Mobile Operators)
- CXD3715GG (RC-S951 Series) Specification
- CXD3715GG (RC-S951 Series) Packaging Guideline(Implementation Reference Manual)
- 0th-Issue Tool Manual

Requirements to be satisfied: AGD_ADM.1, AGD_USR.1, ADO_DEL.2, ADO_IGS.1
Integrity analysis on this document will be done, and the results of analysis will be provided in the following document:

- Misuse Analysis document

Requirements to be satisfied: AVA_MSU.2

Development Security

Security Measures for Development is identified in the document " H/W and S/W Site Development Security ".
Requirements to be satisfied: ALC_DVS.1

Life Cycle Model

Life Cycle Model of this TOE is represented in "Life-Cycle Document".

Requirements to be satisfied: ALC_LCD.1

Test

Testing Policy, Procedures and Test Results are defined in the following documents:

TOE Hardware

- Test Coverage
- Test Depth
- Security Evaluation Specification
- On Board Evaluation Specification
- Evaluation Report

TOE Software

- Test Tool Setup Manual
- Test Specification
- Test Results
- Test Coverage Analysis
- Test Depth Analysis
- Chip Evaluation Report
- Test Procedure Temperature Tamper Test

Requirements to be satisfied: ATE_COV.2, ATE_DPT.1, ATE_FUN.1

In addition, the test procedures and the test results reports to be performed/prepared by the evaluator to confirm that the security functions of this TOE normally functions as defined in the specification are represented in the following documents:

- Independent test procedure
- Independent test results

Requirements to be satisfied: ATE_IND.2

Strength of Function

SOF (Strength Of Function) analysis is represented in the document "Strength of Function Analysis Document".

Requirements to be satisfied: AVA_SOF.1

Vulnerability Analysis

Vulnerability Analysis by the developer is performed as a part of analysis of design and test procedures.
The goal of this analysis is to identify vulnerabilities of the security and to perform analysis.
In addition, this analysis intends to prevent fraudulent use of the TOE in the environment in which operation of the TOE is intended.
Results of this analysis are documented in the document "H/W: vulnerability Analysis, and S/W: Vulnerability Analysis of Developer".
Cautions acquired from the analysis results and related with operation of the product by customer(s) are included in the "Important Notice" document.

Requirements to be satisfied: AVA_VLA.2

(This page is intentionally left blank)

Chapter 7. Rationale of Security Objectives

This chapter demonstrates that (a) the security objectives are adequately selected, and that (b) the stated security targets correspond to all the identified threats, policies or assumptions.

Coverage of Security Objectives

The tables in the following pages show (a) the mapping of security targets that correspond with various types of threats, policies or environment defined by assumptions, and (b) each of security targets is covered by at least one of security targets.

Table 9. Threats related with Security Objectives

Threats	Is addressed by Objective(s)
T.Inherent	O.Leak_Information, O.Crypt.
T.Physical_Probing	O.Physical_Probing.
T.Physical_Manipulation	O.Physical_Manipulation.
T.Malfunction	O.Env_Protect, O.Forced_Protection.
T.Forced_Leak	O.Forced_Protection.
T.Abuse	O.Abuse.
T.Crypto_Analysis	O.Leak_Information, O.Crypt.
T.Leak	O.I_Leak, O.Limit.
T.Forced_Rst	O.Init.
T.Power	O.Power.
T.OP_Ftn	O.Mode.
T.Access	O.Data_Acc.
T.Interface_Prob	O.Sec_Com, O.Crypt, O.Leak_Information.
T.Reuse	O.Sec_Com, O.Reuse, O.Leak_Information, O.Crypt.
T.Repeat	O.Sec_Com, O.Limit.
T.First_Use	O.Set_Up.
T.Crypt_Atk	O.Physical_Probing, O.Crypt O.Leak_Information, O.Physical_Manipulation.
T.Clon	O.Physical_Probing, O.Physical_Manipulation, O.Leak_Information, O.Crypt,O.Sec_Com, OE.Data_Store.
T.Logic_Atk	O.Log_Prot.
T.Delivery	OE.Delivery, O.Ident.

Table 10. Organizational Security Policies related to Security Objectives

Organizational Security Policies	Is addressed by Objective(s)
P.Crypto_Std	O.Crypt.
P.Data_Acc	O.Data_Acc.
P.Ident	O.Ident.
P.Sec_Com	O.Sec_Com.
P.Info_Protect	OE.Phys_Sec.

Table 11. Assumptions related to Security Objectives

Assumptions	Is addressed by Environment Objective(s)
A.Priv	OE.Pers.
A.Data_Store	OE.Data_Store.
A.Key_Supp	OE.Key_Supp.
A.Sec_Extrw	OE.Sec_Extrw.
A.Sec_Intcontroller	OE.Sec_Intcontroller.

Table 12. Security Objectives related to Consideration for Environment

Security Objectives	Is necessitated by
O.Physical_Probing	T.Physical_Probing, T.Crypt_Atk, T.Clon.
O.Physical_Manipulation	T.Physical_Manipulation, T.Crypt_Atk, T.Clon.
O.Env_Protect	T.Malfunction.
O.Forced_Protection	T.Malfunction, T.Forced_Leak.
O.Abuse	T.Abuse.
O.Leak_Information	T.Inherent , T.Crypto_Analysis, T.Interface_Prob, T.Reuse, T.Crypt_Atk, T.Clon.
O.Power	T.Power.
O.Init	T.Forced_Rst.
O.Sec_Com	T.Interface_Prob, T.Reuse, T.Repeat, T.Clon, P.Sec_Com.
O.Data_Acc	T.Access, P.Data_Acc.
O.Mode	T.OP_Ftn.
O.Reuse	T.Reuse.
O.Limit	T.Leak, T.Repeat
O.Set_Up	T.First_Use.
O.Crypt	T.Interface_Prob, T.Reuse, T.Clon, T.Crypt_Atk, P.Crypto_Std, T.Inherent, T.Crypto_Analysis.
O.Log_Prot	T.Logic_Atk.
O.I_Leak	T.Leak.
O.Ident	T.Delivery, P.Ident.
OE.Pers	A.Priv.
OE.Data_Store	A.Data_Store, T.Clon.
OE.Key_Supp	A.Key_Supp.
OE.Sec_Extrw	A.Sec_Extrw.
OE.Sec_Intcontroller	A.Sec_Intcontroller.
OE.Delivery	T.Delivery.
OE.Phys_Sec	P.Info_Protect.

Adequacy of Security Objectives

This section provides the information that shows the chosen security targets sufficiently address to the identified threats, assumptions and policies.
This information is divided into following three parts:

1. The information concerning how the identified security targets provide effective countermeasures against the identified threats.
2. The information concerning how the identified security targets cover completely the organizational security policies.
3. The information concerning how the identified security targets support the identified assumptions.

Detailed discussions on each of parts will be found in the following paragraphs.

Adequacy of Security Physical Threats and Security Objectives

T.Inherent(Inherent information leakage): According to ***O.Leak_Information(Leak information protect)***, the information in the TOE should be prevented from leaking by such as DPA. So the TOE should be designed to make it difficult to observe the change which depends on the information stored in the TOE. And, TOE also counters against this threat with ***O.Crypt (Cryptography)***. This security target ensures that any cryptographic functions available are executed with a secure procedure.

T.Physical_Probing (Physical Probing): According to ***O.Physical_Probing (Physical Probing)***, there is possible to counter with designing and/or producing the TOE as preventing from physical probing.

T.Physical_Manipulation (Physical Manipulation): According to ***O.Physical_Manipulation (Physical Manipulation)***, there is possible to counter with designing and/or producing the TOE as preventing from physical manipulating.

T.Malfunction (Malfunction caused from Environmental Stress): According to ***O.Env_Protect (Environment Protect)***, there is possible to counter with designing the TOE as mounting the detector of Environment Stress and making the TOE operate in accordance with ***O.Env_Protect (Environment Protect)*** if the Stress is detected. ***O.Forced_Protection(Forced Information Protect)***, there is possible to counter with mounting the detector of the CPU malfunction and designing the TOE as making the TOE operate in accordance with ***O.Forced_Protection(Forced Information Protect)*** if the malfunction is detected.

T.Forced_Leak(Forced Information Leakage): According to ***O.Forced_Protection(Forced Information Protect)***, there is possible to counter with designing the TOE as mounting the DES coprocessor with detecting the malfunction and making the TOE operate in accordance with ***O.Forced_Protection(Forced Information Protect)*** if the malfunction is detected. ***O.Forced_Protection(Forced Information Protect)***, there is possible to counter with mounting the detector of the CPU malfunction and designing the TOE as making the TOE operate in accordance with ***O.Forced_Protection(Forced Information Protect)*** if the malfunction is detected.

T.Abuse(Abuse function): According to ***O.Abuse(Abuse function protect)***, there is possible to counter with designing the select function of the TOE and designing and producing as limiting to use the select function.

T.Crypto_Analysis(Crypto Analysis): According to ***O.Leak_Information(Leak Information Protect)***, the information in the TOE should be prevented from leaking. For that, the access should be stopped if the unexpected-long access is detected. And, TOE also counters against this threat with ***O.Crypt (Cryptography)***. This security target ensures that any cryptographic functions available are executed with a secure procedure.

Adequacy of Logical Security Threats and Security Objectives

T. Leak (Leak Information) addresses to exploitation of information unintentionally available from emanation of energy, power consumption or other operating parameters as a function of operations being executed.
This threat is countered by ***O.I_Leak (Information Leakage)***, which ensures that such information is not exposed.
TOE also counters against this threat with ***O.Limit (Limitation)*** makes the capture of data to be used as the basis of statistical analysis difficult.

T.Forced_Rst (Forced Reset) addresses to situations when TOE is reset while it is operating.
Against this threat, TOE directly counters with ***O.Init (Initialization)***. This ensures that TOE enters into the defined initialization sequence when it is reset.

T.Power (Power Supply Failure Data Protection) addresses to the threat that the data stored to the card is destroyed when the supply of electric power to TOE stopped during transaction.
O.Power Power Loss Recovery (Power Loss Recovery) is used to counter to the situation of data loss arising from the loss of electric power supply.

T.OP_Ftn Use of Unallowed Operation Functions (Use of Unallowed Operation Functions) the feature to execute command(s) not required or not allowed in the specific phases (issuance process, key update process, normal operation process) during the operation being performed. ***O.Mode (Operation Mode)*** is used to ensure that deterioration of the security level does not occur caused from unauthorized use of information that results in inadequate interactions between the elements to be used in different phases of operation.

T.Access (Invalid Access) addresses to the needs for protection of information or resources from unauthorized access. This threat is characteristic that it places emphasis on the access to specific information for the purpose of its tampering.
This relates to ***P.Data_Acc (Data Access)***.
Against this threat, TOE directly counters with ***O.Data_Acc (Data Access Control)***.
This security target sets up Access Control Policy.

T.Interface_Prob (Interface Probing) addresses to the attack against data being transferred between TOE itself and (external) devices.
Against this threat, TOE counters with ***O.Sec_Com (Secure Communication)***.
This security target intends to make analysis of data transferred between TOE and external devices difficult.
TOE also counters against this threat with ***O.Crypt (Cryptography)***.
This security target ensures that any cryptographic functions available are executed with a secure procedure. ***And, O.Leak_Information(Leak information protect)***, the information in the TOE should be prevented from session key analysis by such as Brute force attacks.

T.Reuse (Replay Attack) addresses to attacker's fraudulent attempts to replay the operation that partially completed or completed to its end utilizing the information available from such operation.
Against this threat, TOE counters with ***O.Reuse (Replay)***.
This security target ensures that deterioration of the security level on any assets does not occur even if Relay attack is mounted to TOE.
TOE also counters against this threat with ***O.Sec_Com (Secure Communication)***.
This security target intends to make the analysis of data transferred between TOE and External Devices difficult.
TOE also counters against this threat with ***O.Crypt (Cryptography)***.
This security target ensures that any cryptographic functions available are executed with a secure procedure. ***And, O.Leak_Information(Leak information protect)***, the information in the TOE should be prevented from session key analysis by such as Brute force attacks.

T.Repeat (Repeated Attack) addresses to attacker's repeated attempts to access to TOE's information utilizing partially available information by changing the remaining part of such information step-by-step.
Against this threat, TOE counters with ***O.Limit (Limit)***. This security target intends to make the repeated access difficult by imposing restriction to possible numbers of collation.
TOE also counters against this threat with ***O.Sec_Com (Secure Communication)***. This security target intends to make the analysis of data transferred between TOE and External Devices difficult.

T.First_Use (Fraud on First Use) addresses to attacker's fraudulent action through the use of TOE officially not issued yet.
Against this threat, TOE directly counters with ***O.Set_Up (Set-Up Sequence)***. These security targets ensure that TOE completes a defined and controlled series of events before it enters into operational state.

T.Crypt_Atk (Cryptographic Attack) addresses to the direct attack against the cryptographic mechanism adopted by TOE.
Against this threat, TOE counters with ***O.Physical_Probing (Physical Probing) and O.Physical_Manipulation (Physical Manipulation)***.
This security target ensures that TOE is constructed utilizing various elements such as layers for protection, special rules on layout of IC, removal of test pads, etc. These actions intend to make the misuse of IC chip-related information difficult for the purpose to decrypt such information or to deteriorate the security level even if such information was derived out of IC chip.
TOE also counters against this threat with ***O.Crypt (Cryptographic)***.
This security target ensures that any cryptographic functions available are executed with a secure procedure. ***And, O.Leak_Information(Leak information protect)***, the information in the TOE should be prevented from session key analysis by such as Brute force attacks.

T.Clon (Cloning) addresses to a threat to manufacture all or a usable part of TOE for the purpose of fraudulent use of such TOE.
Against this threat, TOE counters with ***O.Physical_Probing (Physical Probing)*** and ***O.Physical_Manipulation(Physical Manipulation)***.
This security target intends to construct TOE so that recognition of any information derived by physical attacks mounted to TOE difficult.
TOE also counters against this threat with ***O.Sec_Com (Secure Communication)***. This security target intends to make the analysis of data transferred between TOE and External Devices difficult.
In addition, ***O.Crypt (Cryptographic)*** and ***O.Leak_Informaiton***(***Leak information protect***) counter against this threat. This security objective ensures any of available encryption functions to be performed in a secure manner.
OE.Data_Store (Off-TOE Data Storage) also supports the countermeasures against this threat. This security target prevents unauthorized possession of the design information.

T.Logic_Atk (***Logical Attack***) addresses the attacks against the logic of the TOE. Such attacks may take form of the introduction of input which does not conform to the required style, content, or format. This input may have the look of accidental or erroneous entries (and that may be, in fact, the source of the data) but the result may be the misperformance of the TOE such that security is compromised. Attackers may use non-conforming data, existing but inappropriate commands, or well formatted commands with data request that refer to locations which are outside of range or not to be utilized in that operation. This threat is countered directly by ***O.Log_Prot*** (***Logical Protection***), which ensures that the TOE is constructed such that it responds in a secure manner to all probing represented by data, commands, or other input which is not fully confirming to the anticipated style and content.

Adequacy of Threats to Delivery Security and Security Objectives

T.Delivery Attacks during delivery (Attacks during Delivery) indicates the threat that attackers make attempts to access to the whole or a part of TOE during its delivery external to secure facilities used for TOE's development and manufacture. Against this threat, TOE copes with ***OE.Delivery (Delivery Procedure)***.
This uses a procedure ensuring to prevent and to detect such attacker's attempts during TOE's delivery.
To the reliability to data located in the memory area during delivery, in addition, ***O.Ident TOE Identification (TOE Identification)*** makes reference to ensure such identification to be done.

Adequacy of Security Policy and Security Objective

P.Crypt_Std (Cryptographic Standard) addresses to the policy to use accepted cryptographic standards and operating procedures in designing TOE. ***O.Crypt (Cryptography)*** addresses to this policy to ensure that such cryptographic standards are used in designing TOE.

P.Data_Acc (Data Access) addresses to the policy that a stated policy about access to data and data objects shall exist.
To this policy, ***O.Data_Acc (Data Access Control)*** addresses directly. This security objective establishes the access control policy.

P.Ident (Identification) addresses to the policy that TOE shall be clearly, completely and uniquely identified. ***O.Ident (TOE Identification)*** addresses to this policy to ensure that identification is done in such ways.

P.Sec_Com (Secure Communication) addresses to the policy that a secure communication shall exist between TOE and External Reader/Writer, and Internal Controller.
O.Sec_Com (Secure Communication) addresses to this policy. This security objective ensures that TOE establishes and uses such a link.

Through the implementation of the objective shown in ***OE.Phys_Sec (Physical Security)***, there is possible that the risk is reduced and TOE is developed in more secure environment as ***P.Info_Protect (Information Protection)***.

Adequacy of Security Assumptions and Security Objectives

A.Priv (Abuse by Privileged Users) addresses to the need of assigning well-trained and trusted personnel to the privileged positions.
OE.Pers Personnel (Personnel) provides the capability to satisfy such need in the environment.

A.Data_Store (Off-TOE Data Storage) addresses to the need to handle and store TOE information in a secure manner when such information is separated from TOE.
OE.Data_Store (Off-TOE Data Storage) provides the capability to satisfy such need in the environment.

A.Key_Supp (Cryptographic Key Support) addresses to the need of support outside TOE for generation, maintenance, delivery and destruction of cryptographic keys for the purpose of adequate use of TOE.
OE.Key_Supp (Cryptographic Key Support) provides for that key support in the environment.

A.Sec_Extrw (External Reader/Writer Secure) addresses to the assumption that External Reader/Writer has the capability to establish a secure communication.
A.Sec_Intcontroller (Internal Controller Secure) indicates the assumption that the internal controller is equipped with the capability to perform secure communication.
To these assumptions, ***OE.Sec_Extrw (External Reader/Writer Secure Communication) and OE.Sec_Intcontroller (Internal Controller Secure Communication)*** addresses.
This ensures that External Reader/Writer, Internal Controller have the capability to establish and use such a communication link.

(This page is intentionally left blank.)

Chapter 8. *Rationale of Security Requirements*

This chapter demonstrates the adequacy of selection of the security requirements. This chapter also demonstrates that each of the security targets is addressed by at least one of security requirements. In addition, this chapter demonstrates that each of the security requirements is directed to the settlement of at least one of security targets.

Coverage of Security Requirements

The tables below show the mapping of the security requirements to the security targets. These tables show that (a) each of the security requirements covers at least one of the security targets, and that (b) each of the security targets is covered by at least one of the security requirements.

Table 13. TOE Security Objectives related to Security Requirements

Security Objective	Security Functional Requirements that address to Security Objectives listed in columns to the left
O.Physical_Probing	FPT_PHP.3.
O.Physical_Manipulation	FPT_PHP.3.
O.Env_Protect	FRU_FLT.1, FPT_FLS.1.1A, FPT_SEP.1.
O.Forced_Protection	FRU_FLT.1, FPT_FLS.1.1A, FPT_SEP.1.
O.Abuse	FDP_IFC.1.1A, FMT_PUT.1.
O.Leak_Information	FDP_IFC.1.1A, FPT_ITT.1, FDP_ITT.1, FCS_COP.1.1A, FCS_COP.1.1B, FCS_RNG.1.1.
O.Crypt	FCS_CKM.1, FCS_CKM.4, FCS_COP.1.1A, FCS_COP.1.1B, FCS_RNG.1.1.
O.Init	FDP_SDI.1, FPT_RCV.4, FPT_FLS.1.1B.
O.Power	FDP_SDI.1, FPT_RCV.4, FPT_FLS.1.1B.
O.Sec_Com	FDP_IFC.1.1B, FDP_IFF.1, FPT_ITC.1, FDP_UCT.1, FDP_ETC.1, FDP_ITC.1, FPT_ITI.1, FDP_UIT.1, FTP_ITC.1.
O.Mode	FDP_ACC.1, FDP_ACF.1.
O.Reuse	FDP_ACC.1, FDP_ACF.1, FPT_RPL.1.
O.Limit	FDP_ACC.1, FDP_ACF.1, FPT_RPL.1, FIA_AFL.1.
O.Data_Acc	FDP_ACC.1, FDP_ACF.1, FPT_TDC.1, FTP_ITC.1, FIA_UID.1, FIA_UAU.2, FMT_SMR.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_SMF.1.
O.Set_Up	FDP_ACC.1, FDP_ACF.1.
O.Log_Prot	FDP_ACC.1, FDP_ACF.1, FDP_SDI.1, FPT_ITI.1, FPT_FLS.1.1B, FPT_RCV.4.
O.I_Leak	AVA_VLA.2.
O.Ident	ACM_SCP.2, ACM_CAP.4.

Table 14. Security Function Requirements related to Security Objectives

Security Functional Requirements	Security Functions needed in Security Requirements listed in columns to the left
FPT_PHP.3	O.Physical_Probing, O.Physical_Manipulation.
FRU_FLT.1	O.Env_Protect, O.Forced_Protection.
FPT_FLS.1.1A	O.Env_Protect, O.Forced_Protection.
FPT_SEP.1	O.Env_Protect, O.Forced_Protection.
FPT_ITT.1	O.Leak_Information.
FDP_IFC.1.1A	O.Abuse, O.Leak_Information.
FDP_ITT.1	O.Leak_Information.
FCS_COP.1.1A	O.Leak_Information, O.Crypt.
FMT_PUT.1	O.Abuse.

Table 14. Security Function Requirements related to Security Objectives (continued)

Security Functional Requirements	Security Functions needed in Security Requirements listed in columns to the left
FPT_FLS.1.1B	O.Init, O.Power, O.Log_Prot.
FPT_RCV.4	O.Init, O.Power, O.Log_Prot.
FPT_TDC.1	O.Data_Acc.
FTP_ITC .1	O.Data_Acc, O.Sec_Com.
FIA_UID.1	O.Data_Acc.
FIA_UAU.2	O.Data_Acc.
FDP_ACC.1	O.Mode, O.Reuse, O.Limit, O.Data_Acc, O.Set_Up, O.Log_Prot.
FDP_ACF.1	O.Mode, O.Reuse, O.Limit, O.Data_Acc, O.Set_Up, O.Log_Prot.
FMT_SMR.1	O.Data_Acc.
FMT_MSA.1	O.Data_Acc.
FMT_MSA.2	O.Data_Acc.
FMT_MSA.3	O.Data_Acc.
FMT_MTD.1	O.Data_Acc.
FMT_MTD.2	O.Data_Acc.
FMT_MTD.3	O.Data_Acc.
FMT_MOF.1	O.Data_Acc.
FMT_SMF.1	O.Data_Acc.
FDP_IFC.1.1B	O.Sec_Com.
FDP_IFF.1	O.Sec_Com.
FCS_COP.1.1B	O.Crypt, O.Leak_Information.
FCS_CKM.1	O.Crypt.
FCS_CKM.4	O.Crypt.
FCS_RNG.1.1	O.Crypt, O.Leak_Information.
FPT_ITC.1	O.Sec_Com.
FDP_UCT.1	O.Sec_Com.
FPT_ITI.1	O.Sec_Com, O.Log_Prot.
FDP_UIT.1	O.Sec_Com.
FDP_SDI.1	O.Init, O.Power, O.Log_Prot.
FDP_ETC.1	O.Sec_Com.
FDP_ITC.1	O.Sec_Com.
FPT_RPL.1	O.Reuse, O.Limit.
FIA_AFL.1	O.Limit.

Table 15. Security Assurance Requirements related to Security Objectives

Security Assurance Requirements	Security Objectives needed in Security Requirements listed in columns to the left
ACM_AUT.1	Selection of EAL4
ACM_CAP.4	Selection of EAL4
ACM_SCP.2	Selection of EAL4
ADO_DEL.2	Selection of EAL4
ADO_IGS.1	Selection of EAL4
ADV_FSP.2	Selection of EAL4
ADV_HLD.2	Selection of EAL4
ADV_IMP.1	Selection of EAL4
ADV_LLD.1	Selection of EAL4
ADV_RCR.1	Selection of EAL4
ADV_SPM.1	Selection of EAL4
AGD_ADM.1	Selection of EAL4
AGD_USR.1	Selection of EAL4
ALC_DVS.1	Selection of EAL4
ALC_LCD.1	Selection of EAL4
ALC_TAT.1	Selection of EAL4
ATE_COV.2	Selection of EAL4
ATE_DPT.1	Selection of EAL4
ATE_FUN.1	Selection of EAL4
ATE_IND.2	Selection of EAL4
AVA_MSU.2	Selection of EAL4
AVA_SOF.1	Selection of EAL4
AVA_VLA.2	Selection of EAL4

Table 16. TOE Environment Security Objectives related to Security Requirements for IT Environment

IT Environment Security Objectives	Security Requirements that address to Security Objectives listed in columns to the left
OE.Sec_Extrw	FTP_ITC.1, FCS_COP.1.
OE.Sec_Intcontroller	FTP_ITC.1, FCS_COP.1.
OE.Key_Supp	FCS_CKM.1, FCS_CKM.4.

Table 17. Non-IT Environment Security Objectives of TOE

Security Objectives
OE.Pers
OE.Data_Store
OE.Delivery

Adequacy of Security Function Requirements for Satisfaction of Security Objectives

This chapter provides discussions on the adequacy of the identified SFRs (Security Function Requirements) and SARs (Security Assurance Requirements) to satisfy the given security targets.

O.Physical_Probing (Physical Probing) and O.Physical_Manipulation (***Physical Manipulation***) are implemented by a security functional requirement. For preventing Physical Probing or Manipulating as shown ***O.Physical_Probing(Physical Probing) and O.Physical_Manipulation(Physical Manipulation)***, the function "Resistance to physical attack" ***FPT_PHP.3(Resistance to physical attack)*** is needed.

O.Env_Protect (Environment Protection), O.Forced_Protection (Forced Information Protect) and O.Leak_Information (Leak Information Protect) are implemented by multiple numbers of security functional requirements. As shown ***O.Env_Protect(Environment Protection), O.Forced_Protection(Forced Information Protect) and O.Leak_Information(Leak Information Protect)***, if TOE is not a secure state, the state must be detected and TOE must be reset and stopped immediately. For that purpose, the functions specified in ***FPT_FLS.1.1A(Failure with preservation of secure state), FRU_FLT.1(Degraded fault tolerance) and FPT_SEP.1(TSF domain separation)*** are needed.

O.Leak_Information(Leak Information Protect) is implemented by security functional requirement.
As shown ***O.Leak_Information(Leak Information Protect)***, secret information must be protected from leakage during normal operation. For that purpose, the function which prevents secret information from leakage when it is transmitted within TOE is needed and it is specified in ***FDP_IFC.1.1A (Subset information flow control), FPT_ITT.1(Basic internal TSF data transfer protection)), FDP_ITT.1(Basic internal transfer protection), FCS_COP.1.1A andFCS_COP.1.1B (Cryptographic operation), and FCS_RNG.1.1 (Random Numbers generator)***.

O.Abuse(Abuse function protect) is implemented by multiple numbers of security functional requirements.
The functions which limit test function as specified ***FDP_IFC.1.1A(Subset information flow control) and FMT_PUT.1(Hardware Test Mode Protect)*** is needed to prevent from abuse of select function as shown ***O.Abuse(Abuse function protect)***.

O.Init (Initialization) is implemented by multiple numbers of functional requirements.
FDP_SDI.1 (Stored data integrity monitoring) monitors the data of ***TOE just after the power-on, reset or restart conditions.*** ***FPT_RCV.4 (Function recovery)*** assures the memory data stored during abnormal condition of TOE.
FPT_FLS.1.1B (Failure with preservation of secure state) maintains the secure condition.

O.Power (Power Loss Recovery) is implemented by multiple numbers of functional requirements.
FDP_SDI.1 (Stored data integrity monitoring) monitors the data of TOE during communication and processing. ***FPT_RCV.4 (Function recovery)*** assures the memory data during abnormal condition caused by power interruption.
FPT_FLS.1.1B (Failure with preservation of secure state) maintains the secure condition of TOE.

O.Mode (Mode Function) is implemented by multiple functional requirements.
FDP_ACC.1 (Subset Access Control) defines the access control policy to maintain the normal life cycle, and ***FDP_ACF.1 (Security Attribute Based Access Control)*** assures execution and mode transition.

O.Crypt (Cryptography) is implemented by multiple numbers of functional requirements.
FCS_COP.1.1A and FCS_COP.1.1B (cryptographic operation) are supported by ***FCS_CKM.1 (cryptographic key generation)*** and ***FCS_CKM.4 (cryptographic key destruction)*** for generation and confirmation of related secret information.
FCS_RNG.1.1 (***Random Number generator***) support the random numbers controlled by Mobile FeliCa OS.

O.Data_Acc (Data Access Control) is implemented by multiple numbers of functional requirements.
FIA_UID.1(Timing of identification) and ***FIA_UAU.2(User authentication before any action)*** identifies the user who attempted access to the TOE, In accordance with the access control policy defined by ***FDP_ACC.1 (Subset access control)***, ***FDP_ACF.1 (Security Attribute Based Access Control)*** defines the access control based upon security attribute.
In this case, ***FPT_TDC.1(Inter-TSF basic TSF data consistency)*** uses the key shared between the TOE and IT products to establish a secure communication channel as defined in ***FTP_ITC.1(Inter-TSF trusted channel)***. To perform these operations in a secure manner, operations to security functions, TSF data and security attributes of the TOE are authorized only to the specific personnel as defined in ***FMT_SMR.1(Security roles), FMT_MOF.1(Management of security functions behaviour), FMT_MSA.1(Management of security attributes), FMT_MSA.2(Secure security attributes), FMT_MSA.3(Static attribute initialization), FMT_MTD.1(Management of TSF data), FMT_MTD.2(Management of limits on TSF data), FMT_MTD.3(Secure TSF data), and FMT_SMF.1(Specification of Management Functions)***. This assures the secure control to access to the data.

O.Sec_Com (Secure Communication) is implemented by multiple numbers of functional requirements. ***FTP_ITC.1 (Inter-TSF trusted channel)*** generates a trusted channel between TOE and External Devices. In accordance with the information flow control policies defined by ***FDP_IFC.1.1B (Subset information flow control) and FDP_IFF.1 (Simple security attribute)***, transmission / reception of user data are performed on a secure communication path established between TOE and External Devices by ***FDP_ETC.1 (Export of user data without security attribute)*** and ***FDP_ITC.1 (Import of user data without security attribute)***. In addition, ***FDP_UCT.1 (Basic data exchange confidentiality)*** protects the user data transferred between TOE and External Devices from unauthorized disclosure, and ***FDP_UIT.1 (Data exchange integrity)*** protects the user data from tampering or Replay attacks. ***FPT_ITI.1 (Inter-TSF confidentiality during transmission)*** detects tampering to TSF data, and ***FPT_ITC.1 (inter-TSF confidentiality during transmission)*** assures the secrecy of TSF data.

O.Reuse (Replay) is implemented by multiple functional requirements. ***FPT_RPL.1 (Replay Detection)*** detects the repeated access with replay of the same command after authentication successes, and based upon the access control policy defined by ***FDP_ACC.1 (Subset Access Control)***, ***FDP_ACF.1 (Security Attribute Based Access Control)*** limits (limit capturing of leak information) the repeated access.

O.Limit (Command Repeat Limit) is implemented by multiple functional requirements. ***FPT_RPL.1 (Replay Detection)*** and ***FIA_AFL.1(Authentication failure handling)*** detects the repeated access with replay of the same authentication command, and based upon the access control policy defined by ***FDP_ACC.1 (Subset Access Control)***, ***FDP_ACF.1 (Security Attribute Based Access Control)*** limits (limit capturing of leak information) the repeated access.

O.Set_Up (Set-Up Sequence) is implemented by multiple numbers of functional requirements. ***FDP_ACC.1 (Subset access control)*** defines the access control policy to keep the life cycle to be normal. ***FDP_ACF.1 (Security Attribute Based Access Control)*** assures execution of each of commands and transitions between modes.

O.I_Leak (Information leakage) is provided by ***AVA_VLA.2(Independent vulnerability analysis).*** This requirement reviews vulnerabilities, including those dealing with the leakage of information from the TOE.

O.Ident (TOE Identification) is provided through the assurance requirements Security Requirements for IT Environment. And ***ACM_SCP.2*** (***Problem tracking CM coverage***), which require the developer to uniquely identify the configuration items that constitute the TOE. In addition, ***ACM_CAP.4 (Generation support and acceptance procedures)*** allows identification of TOE's physical and logical configurations.

O.Log_Prot Logical Protection is provided by the following requirements. The access control SFPs named in ***FDP_ACC.1 (Subset access control) and detailed in FDP_ACF.1 (Security Attribute Based Access Control)*** set the rules for accessing the data. ***FDP_SDI.1 (Stored data integrity monitoring)*** provides for the protection of the logical functions from the use of corrupted data.
FPT_ITI.1 (Inter-TSF detection of modification) provide for protection of the logical functions from the input of corrupted data. ***FPT_FSL.1.1B (Failure with preservation of secure state) and FPT_RCV.4 (Function recovery)*** provide for acceptably secure operation in the event of failures. The instance of power failure is of particular concern due to the stated unreliability of the power supply.

Rationale of Improvement of Security Function Requirements

Rationale of Refinement Hardware Security Function Requirements

FRU_FLT.1 The tern "failure" above means "circumstance". The TOE prevents failure for the "circumstances" defined above. TOE's capabilities are
- against abnormal supply voltage: all functions
- against abnormal clock frequency: all functions
- against abnormal clock duty ratio: all functions
- against malfunction of DES calculation: detection of DES malfunction and reset function
- against undefined instruction codes and undefined memory address
: detection of undefined instruction codes and undefined memory address and reset function
- against longer-than-expected access to TOE: all functions.

FPT_FLS.1.1A The term "failure" above means "circumstances". The TOE prevent failures for the "circumstances" shown below.
- abnormal supply voltage
- abnormal clock frequency
- abnormal clock duty ratio
- malfunction of DES calculation
- attempt to execute undefined instruction codes
- attempt to access undefined memory address
- longer-than-expected access to TOE.

FPT_SEP.1 The component supporting the SFRs Degraded fault tolerance (FRU_FLT.1) and Failure with preservation of secure state (FPT_FLS.1) shall be protected from interference of the Embedded Software.

FPT_PHP.3	The TOE will implemented appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of the attack, the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic attack" means (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.
FPT_ITT.1	Memories, Resisters, I/Os are seen as separated parts of the TOE.
FCS_CKM.1	***Cryptographic key generation*** is refined to improve the legibility of statements available as a result of data encryption.
FCS_CKM4	***Cryptographic key destruction*** is refined to improve the legibility of statements available as a result of key destruction.
FCS_COP.1	***Cryptographic operation*** is refined to improve the legibility of statements available as a result of cryptographic operation.

Adequacy of Security Assurance Requirements

The assurance level for this Security target is as discussed in EAL4.

In EAL4, a high assurance level can be reasonably maintained while the developer uses no specific processes or implementation methods for that purpose.
EAL4 is the adequate for products of commercial purpose.

Adequacy of Claims on Strength of Function

This TOE is the product intending to be used for operation in commercial field.
Because of this, EAL4 is considered as the adequate level for this TOE.
In EAL4, it is specified that SOF-Basic is necessary for a product to which security functions are installed.
Thus, it is possible to say that SOF-Basic is capable to provide a sufficient strength level of security necessary for this TOE (i.e., a product intending to be used for operation in commercial field).

Mutual Support between Security Requirements

This section provides the description on the mutual support and the dependency between security requirements.

Consistency and Mutual Support

Selection of the security requirements can be justified as shown in the sub-section "Adequacy of Security Function Requirements for satisfaction of Security Objectives" (page 106 of this document) and the sub-section "Adequacy of Security Assurance Requirements" (page 110 of this document).
Selection of SFRs and SARs is done based upon various assumptions on threats against TOE & IT environment as well as upon the security objectives.

SARs are adequate for the assurance level of EAL4.
This assurance level provides a high-level and independently assured security.
The identified measurement values and the SOF claims correspond with the assurance level of EAL4.

Dependency between Security Function Requirements

Tables in the following pages show the summary of dependency between the security function requirements. These tables also show how these requirements are satisfied.

TOE Hardware Security Functional Requirements Dependencies

Table 18. Dependency of TOE's Hardware Security Functional Requirements

SFR	Depends on:	Satisfied by:
FRU_FLT.1	FPT_FLS.1	Included.
FPT_FLS.1.1A	ADV_SPM.1	Included.
FPT_SEP.1	N/A	N/A
FPT_PHP.3	N/A	N/A
FPT_ITT.1	N/A	N/A
FDP_IFC.1.1A	FDP_IFF.1	Refer to "Unsatisfied Dependency of TOE's Hardware Security Functional Requirements" (page 112 of this document).
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Included as FDP_IFC.1.1A
FCS_COP.1.1A	FDP_ITC.1 or FCS_CKM.1	Refer to Dependency of "TOE Software Security Functional Requirements Dependencies" (page 113 of this document)
	FCS_CKM.4	Refer to Dependency of "TOE Software Security Functional Requirements Dependencies" (page 113 of this document)
	FMT_MSA.2	Refer to Dependency of "TOE Software Security Functional Requirements Dependencies" (page 113 of this document)
FMT_PUT.1	N/A	N/A

Unsatisfied Dependency of TOE's Hardware Security Functional Requirements

Part 2 of the Common Criteria defines the dependency of **FDP_IFC.1.1A** (information flow control policy statement) on **FDP_IFF.1** (Simple security attributes). The specification of **FDP_IFF.1** would not capture the nature of the security functional requirement nor add any detail. As stated in the ***Data Processing Policy*** referred to in **FDP_IFC.1.1A** there are no attributes necessary. The security functional requirement for the TOE is sufficiently described using **FDP_ITT.1** and its ***Data Processing Policy*** (**FDP_IFC.1.1A**). Therefore the dependency is considered satisfied.

TOE Software Security Functional Requirements Dependencies

Table 19. Dependency of TOE's Software Security Functional Requirements

SFR	Depends on:	Satisfied by:
FPT_FLS.1.1B	ADV_SPM.1	Included.
FPT_RCV.4	ADV_SPM.1	Included.
FPT_TDC.1	N/A	N/A
FTP_ITC.1	N/A	N/A
FIA_UID.1	N/A	N/A
FIA_UAU.2	FIA_UID.1	Included
FDP_ACC.1	FDP_ACF.1	Included.
FDP_ACF.1	FDP_ACC.1	Included.
	FMT_MSA.3	Included.
FMT_SMR.1	FIA_UID.1	Included.
FMT_MOF.1	FMT_SMF.1	Included.
	FMT_SMR.1	Included.
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Included in both.
	FMT_SMF.1	Included.
	FMT_SMR.1	Included.
FMT_MSA.2	ADV_SPM.1	Included.
	FDP_ACC.1 or FDP_IFC.1	Included in both.
	FMT_MSA.1	Included.
	FMT_SMR.1	Included.
FMT_MSA.3	FMT_MSA.1	Included.
	FMT_SMR.1	Included.
FMT_MTD.1	FMT_SMF.1	Included.
	FMT_SMR.1	Included.
FMT_MTD.2	FMT_MTD.1	Included.
	FMT_SMR.1	Included.
FMT_MTD.3	ADV_SPM.1	Included.
	FMT_MTD.1	Included.
FMT_SMF.1	N/A	N/A
FDP_IFC.1.1B	FDP_IFF.1	Included.
FDP_IFF.1	FDP_IFC.1	Included.
	FMT_MSA.3	Included.
FCS_COP.1.1B	FDP_ITC.1 or FCS_CKM.1	Included in both.
	FCS_CKM.4	Included.
	FMT_MSA.2	Included.
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1.1B	Included as FCS_COP.1.1B
	FCS_CKM.4	Included.
	FMT_MSA.2	Included.
FCS_CKM.4	FDP_ITC.1 or FCS_CKM.1.1B	Included in both.
	FMT_MSA.2	Included.

Table 19. Dependency of TOE's Software Security Functional Requirement (continued)

SFR	Depends on:	Satisfied by:
FCS_RNG.1.1	N/A	N/A
FPT_ITC.1	N/A	N/A
FDP_UCT.1	FTP_ITC.1 or FTP_TRP.1	Included as FTP_ITC.1.
	FDP_ACC.1 or FDP_IFC.1	Included in both.
FPT_ITI.1	N/A	N/A
FDP_UIT.1	FDP_ACC.1 or FDP_IFC.1	Included in both.
	FTP_ITC.1 or FTP_TRP.1	Included as FTP_ITC.1.
FDP_SDI.1	N/A	N/A
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	Included in both.
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1	Included in both.
	FMT_MSA.3	Included.
FPT_RPL.1	N/A	N/A
FIA_AFL.1	FIA_UAU.1	Included as FIA_UAU.2

Unsatisfied Dependency of TOE's Software Security Functional Requirements

For the purpose of this TOE, the dependencies of the selected security functional requirements are all satisfied.

Dependency between Security Assurance Requirements

EAL4 is an independent package.
Table below shows the summary of security assurance requirements derived from

the discussion on EAL4. This table also shows how such requirements are satisfied.

Table 20. Dependency of TOE's Security Assurance Requirements

SAR	Depends on:	Satisfied by:
ACM_AUT.1	ACM_CAP.3	Included as ACM_CAP.4.
ACM_CAP.4	ACM_SCP.1	Included as ACM_SCP.2.
	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_LLD.1	ADV_HLD.2	Included.
	ADV_RCR.1	Included.
ADV_IMP.1	ADV_LLD.1	Included.
	ADV_RCR.1	Included.
	ALC_TAT.1	Included.
ADV_RCR.1	None	None
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	None	None
ALC_LCD.1	None	None
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	None	None
ATE_IND.2	ADV_FSP.1	Included as ADV_FSP.2.
	AGD_ADM.1	Included.
	AGD_USR.1	Included.
	ATE_FUN.1	Included.

Table 20.Dependency of TOE's Security Assurance Requirements (continued)

SAR	Depends on:	Satisfied by:
AVA_MSU.2	ADO_IGS.1	Included.
	ADV_FSP.1	Included as ADV_FSP.2.
	AGD_ADM.1	Included.
	AGD_USR.1	Included.
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 as ADV_HLD.2.
	ADV_LLD.1	Included.
	AGD_ADM.1	Included.
	AGD_USR.1	Included.

Adequacy of Security Function Requirements for Implementation of Security Objects to TOE Environment (IT Environment)

OE.Sec_Extrw is implemented by **FTP_ITC.1**.
OE.Sec_Intcontroller is implemented by **FTP_ITC.1**.
With these security objects, generation of a secure channel as well as establishment of secure communication between the secure IT products and TOE become possible.
FCS_COP.1 provides supports to the necessary cryptographic operation in accordance with the specified standard and guidance.

OE.Key_Supp is provided for the purpose of multiple numbers of requirements.
FCS_CKM.1 generates the cryptographic key with a secure key generation method.
In addition, **FCS_CKM.4** performs destruction of the cryptographic key with a secure key destruction method.

Reason why Assignment is left uncompleted for TOE Security Requirements

Following operations are left uncompleted for "Security Requirements to TOE Environment (IT Environment)".

Table 21. "Assignment Uncompleted" TOE Security Requirements

Requirement for Function	Operation	Description of Operation
FCS_CKM.1	Assignment	Cryptographic key generation algorithm
FCS_CKM.4	Assignment	Cryptographic key destruction method

To support the cryptographic operations in TOE environment, these operations relate with various procedures and algorithms done by TOE environment (IT environment).
Because there may exist other algorithms / procedures that satisfy these requirements, selection of specific algorithm / procedure is left uncompleted so that it will be done depending upon the environment.

(This page is intentionally left blank.)

Chapter 9. Rationale of TOE Summary Specification

As demonstrated in "IT Security Function" (see page 78 of this document), TOE's security function satisfies all the requirements of security functions set up in "TOE's Security Functional Requirements" (see page 60 of this document). TOE's Assurance Method detailed in "Assurance Method" (see page 84 of this document) demonstrates that it refers to "TOE Security Assurance Requirements" (see page 73 of this document).

Selection of SFRs (Security Functional Requirements) and SARs (Security Assurance Requirements) are done based upon the security targets for the TOE and the security environment as well as the assumptions on the threats to them and the security environment.
Thus, this ST (Security target) provides the evidence that, in conjunction with the assurance methods, the security functions counter against all the threats launched to this TOE.

This TOE is so designed to maintain the TOE's functional strength level to be "Basic" through the combination of the restriction to TOE's operational environment detailed in "Adequacy of Claim on Strength of Function" (see page 111 of this document) as well as DES Encryption Algorithm and Security Mechanism. Security functions realized by the mechanism are ‘SEF.7: Data Encryption (Random number generation)’ and ‘SEF.9: Authentication (Limitation to authentication trial times)’.

(This page is intentionally left blank.)

Chapter 10. *Appendix A*

This chapter provides the explanation of the Extended IT Security Function Requirements.

Extended IT Security Functional Requirements:

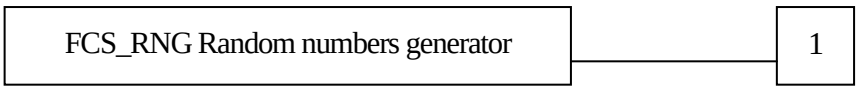
Definition of the FCS_RNG: Random numbers generator,
Definition of the FMT_PUT: Hardware Test Mode Protect.

Definition of the FCS_RNG.1

Family behaviour

This family defines quality requirements for the generation of random numbers which are intended to be use for cryptographic purposes.

Component leveling:



FCS_RNG.1	Generation of pseudo random number requires that pseudo random numbers meet a defined quality metric.
Management:	FCS_RNG.1 There are no management activities foreseen.
Audit:	FCS_RNG.1 There are no actions defined to be auditable.
FCS_RNG.1	Random numbers generator
Hierarchical to:	No other components.
FCS_RNG.1.1	The TSF shall provide [selection: random numbers, pseudo random numbers] that meet the requirements of [assignment: list of random randomness criteria].
Dependencies:	No dependencies

Definition of the FMT_PUT.1

Family behaviour

The family defines availability requirements for the design of TOE hardware, which are intended to be use for TOE Life cycle process.

Component leveling:

FMT_PUT.1

Management: FMT_PUT.1
There are no management activities foreseen.

Audit: FMT_PUT.1
There are no actions defined to be auditable.

FMT_PUT Hardware Test Mode Protect

Hierarchical to: No other components.

FMT_PUT.1 The TSF shall be designed in a manner that prevents the hardware test function availability after the hardware production lifecycle.

Dependencies: No dependencies

(This page is intentionally left blank.)

(End of the Document)