RC-S940
Security Target (Public Version)

Version: 2.04
Control number: 9768-ST-E02-04
Date of issue: May 13, 2005

Sony Corporation

May 13, 2005
FeliCa Business Center
Sony Corporation

(This page is intentionally left blank.)

Table of Contents

List of Tables

List of Figures

Definition of Terms

1: Assets

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

2: Carrier

This is an IT product to which TOE is installed.
In the case of an IC Chip to be embedded to the card, the carrier is a case made of plastics.
In the case of an IC Chip to be installed to a reader /writer, the carrier is the reader / writer itself (excluding TOE).

3: Contact Smart Card

Integrated Circuit Card with contacts.

4: Contactless Smart Card

Integrated Circuit Card without contacts.

5: Controller

Controls Reader/Writer via UART I/F and is part of the host.

6: Data Bus

This is the signal path used for handling of instructions and / or data between each of blocks internal to the IC Chip and under the control of CPU.

7: Dependency

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

8: EEPROM (Electrically Erasable Programmable Read Only Memory)

One of non-volatile memory technologies that allows erasure and re-write of data by electronic methods

9: Environment stress

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

10: Extension (or Addition)

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

11: External Interface

Device that interfaces between the IC and external devices
RF CARD I/F is also an external interface.
UART I/F is also an external interface.

12: FeliCa protocol

This means the communication protocol (ISO/IEC 18092).
This is the communication protocol to establish a secure channel between the Controller and the TOE, and between the TOE and the Card.

13: Formal

Formal means the expression by a syntax language with restriction of meanings imposed based upon the established mathematical concept.

14: IC (Integrated Circuit)

"IC" is an electronic component accommodated into a single semiconductor chip, and designed to perform processing of various data and / or to perform memory function.

15: Internal Interface

An internal interface connects between the CPU and other blocks in the IC.
Data Bus Line functions as the internal interface.

16: IPL Authentication

Mutual authentication necessary in entering to IPL Mode

17: Reader / Writer

This is an IT product for communication between the controller and the card.
To accomplish the communication between the controller and the card, the reader / writer converts the format of data packets of the controller and the card to make transmission and reception of both data packets possible.

18: PP (Protection Profile)

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

19: RAM (Random Access Memory)

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

20: RF CARD I/F

RF is the acronym of Radio Frequency (high frequency), and RF CARD I/F means the radio frequency communication interface. RF CARD I/F is mainly used for communication with the contactless smart card.

21: ROM (Read Only Memory)

This is a non-volatile type memory (to be used internal to the IC) that requires no supply of electrical power to maintain the data stored to it. ROM data may be contained one of many photo masks used for IC manufacturing.

22: Semiformal

Semiformal means the expression by a syntax language with restriction of defined meanings.

23: SOF-Basic

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

24: SOF-Medium

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

25: SOF-High

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

26: ST (Security Target)

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

27: Strength of Function (SOF)

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

28: TOE (Target of Evaluation)

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

29: TOE Security Functions (TSF)

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

30: TSF Data

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

31: UART I/F

This is the name of a wired interface used for communication with the controller.
UART I/F is mainly used for communication with the controller.

32: User data

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

List of Abbreviations

ATR:	Answer to Reset
CBC:	Cipher Block Chaining
CC:	Common Criteria
CPU:	Central Processing Unit
CRYPTO:	Cryptographic
DES:	Data Encryption Standard
DFA:	Differential Fault Analysis
DPA:	Differential Power Analysis
EAL:	Evaluation Assurance Level
ECB:	Electronic Code Book
EEPROM:	Electrically Erasable Programmable ROM
IC:	Integrated Circuit
I/F:	Interface
IPL:	Initial Program Loader
NIST:	National Institute of Standards and Technology
PP:	Protection Profile
RAM:	Random Access Memory
RF:	Radio Frequency
ROM:	Read Only Memory
SOF:	Strength of Function
SPA:	Simple Power Analysis
SRAM:	Static Random Access Memory
ST:	Security Target
TSF:	TOE Security Functions
TOE:	Target of Evaluation
UART:	Universal Asynchronous Receiver/Transmitter

(This page is intentionally left blank.)

1.ST Introduction

This is the Security Target for CC evaluation of RC-S940 (CXD9768GG) product. Roles to be accomplished by this Security Target during the development and evaluation stages are as described in ISO/IEC 15408:CC.

This Security Target is applicable to this product only.

1.1.ST and TOE Identification

ST Identification

Title of Security Target:	RC-S940 Security Target
Version number:	2.04
Date of creation:	May 13, 2005
ST Author:	Sony Corporation

TOE Identification

Product name:	RC-S940
Product code:	CXD9768GG
Version:	Ver.4 (ROM ver.3, Mask set ver.3)
Product:	IC chip for the reader / writer
Guidance documentation:	
	RC-S940 Operation Guideline, Version 1.1, February 20, 2004
	RC-S940 IPL User's Manual, Version 1.0, March 4, 2004
	RC-S940 Administrator Tools Manual, Version 1.0, February 19, 2004
CC identification:	ISO15408 standard Common Criteria for Information Technology Security Evaluation [CC]
ST created by:	Sony Corporation
Evaluation body:	TÜV Informationstechnik GmbH evaluation body
Certification body:	Bundesamt für Sicherheit in der Informationstechnik

1.2. ST Overview

The Target of Evaluation (TOE), the RC-S940 (CXD9768GG) Ver.4 (ROM ver.3, Mask set ver.3) is a platform IC-Chip dedicated for Reader/Writer for application in transportation systems, distribution systems, a commodities selling, financial systems, and site security. The IC-Chip provides security functionality for a secure download of firmware to the EEPROM and for secure communication between the controller and the IC-Chip. The product is developed and designed by Sony.
In this security target the TOE is described and a summary specification is given.
The security environment of the TOE is also defined. The assets are identified which have to be protected through the security policy. The threats against these assets are described.
The security objectives as the objectives of the security policy are defined as well as the security requirements. The requirements are built up of the security functional requirements as a part of the security policy and the security assurance requirements as the steps during the evaluation and certification to show the TOE meets its requirements. The functions of the TOE to meet the requirements are described. The security enforcing functions are defined here in the security target as property of this specific TOE. Here it is shown how this specific TOE fulfils the corresponding requirements.

1.3. CC Conformance

This security target is conformant to Common Criteria V2.1 (ISO15408) part 2 conformant, part 3 conformant. The assurance level is EAL4.

This Security Target does not claim conformances to any Protection Profile.

1.4. References

[CC] Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031
(CC Part1: Common Criteria Part1 / ISO/IEC 15408 Part1)

Common Criteria for Information Technology Security Evaluation
Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032
(CC Part2: Common Criteria Part2 / ISO/IEC 15408 Part2)

Common Criteria for Information Technology Security Evaluation
Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033
(CC Part3: Common Criteria Part3 / ISO/IEC 15408 Part3)

2. TOE Description

To facilitate reader's understanding to the requirements on security, Chapter 2 provides the description on TOE (Target of Evaluation) and in addition, accesses to the types of product or system. For the applicability and the boundary of the TOE, description is given as viewed from standpoints in both the physical configuration (hardware and firmware as well as interface configuration) and the logical configuration (IT and security features of the TOE).

2.1. Product Type

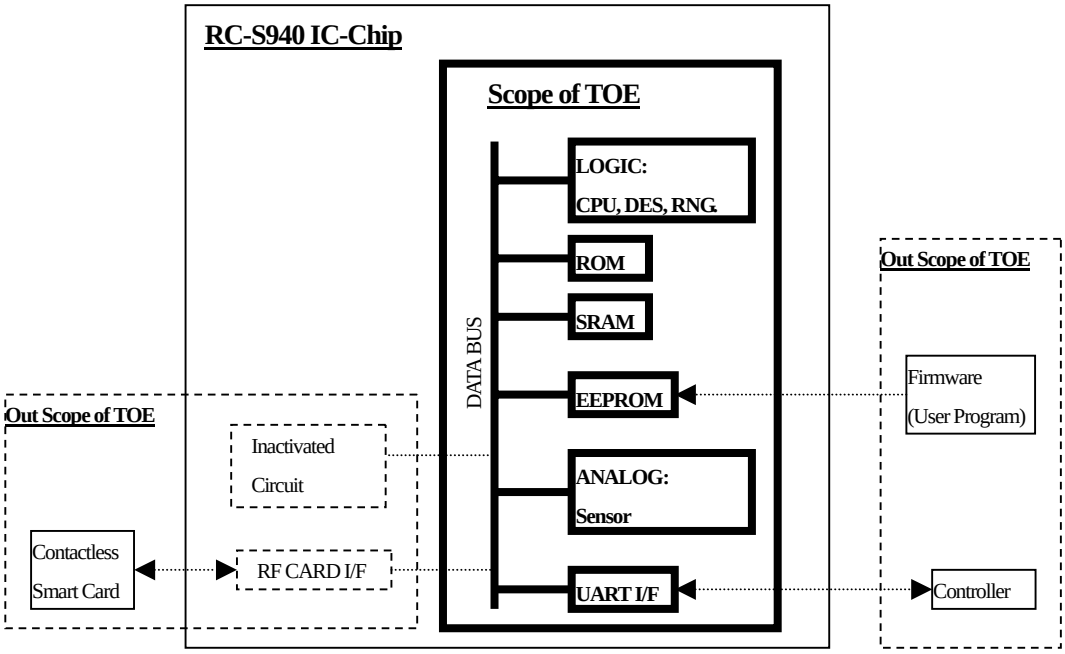


Figure 1: Block Diagram of RC-S940 IC-Chip

The product type of the TOE is an IC-Chip embedded into the Reader / Writer.

The IC chip (refer to Figure 2: Block Diagram of TOE (IC-chip)), that is, the TOE consists of memories, data bus, security logic, peripheral devices, I/O interface, a dedicated CPU, etc.
Although RF CARD Interface and Inactivated Circuit (for future use) is implemented in this IC chip, they are out scope of TOE in this evaluation.

As the CPU, an original 16-bit CPU is contained in this IC chip.
As memories, ROM, EEPROM, and SRAM are contained in this IC chip.

To 16kBytes of ROM, the ROM Program for control to the IC chip is stored.
To 128kBytes of EEPROM, cryptographic keys, firmware (out scope of the TOE), etc. are stored.
To 4kBytes of SRAM area, the communication data and the process data are stored as temporary data.

In addition, the security logic (Random Number Generator, CRYPTO Engine and Illegal Voltage, Frequency, Temperature sensors) and the peripheral devices (Timer, interrupt controller, Clock Gear and Reset Generator) are used for maintaining the performance and the security.

The security functions implemented to the IC-chip are (SF.1) Detection of illegal operation, (SF.2) Protection to information leakage, (SF.3) Physical protection, (SF.4) Encryption of data, (SF.5) Mutual authentication, (SF.6) Protection of data passing through the interface, (SF.7) self test, and (SF.8) Protection of internal data.

The RC-S940 has three operational modes, Normal Mode, IPL Mode, and STOP Mode.
The Normal Mode allows normal communication with the controller and/or card, which is executed by firmware stored to EEPROM.
The IPL Mode is used to download firmware from the controller to RC-S940. In this mode, it is deactivated communication interface with the card.
The STOP Mode is entered automatically when, for example, the internal EEPROM data is damaged. The STOP Mode prevents the RC-S940 from being used under abnormal conditions. All commands except maintenance command cannot therefore be executed.
The RC-S940 also has Test Mode that is used in manufacturing process. The Test Mode is prohibited after TOE delivery.

The RC-S940 provides a secure platform for running reader / writer firmware. The firmware must be developed by a trustworthy developer that observes the requirements and hints given in the guidance documentation. (see assumption A.Priv). As the firmware is not part of the TOE, the operation with firmware loaded in the TOE (i.e. TOE is operating in Normal Mode) is out of scope of this evaluation. Nevertheless, the assumption A.Priv is necessary to ensure, that no malicious firmware is loaded that might offend or violate the security policy of the TOE in IPL mode.
Some of the security features provided by the TOE Security functions are also present in Normal Mode, these are: Detection of illegal operation, physical protection, and self tests.

2.2. Scope of TOE

This section describes which IC-chip components are scopes of TOE and which are out of scope based on the "2.1 Product Type".
Be careful that only a part of the IC-Chip components are scope of TOE (Product Name: RC-S940, Product Code: CXD9768GG), not whole of the IC-Chip.

Components listed below are scope of the TOE.

CPU, ROM, SRAM, EEPROM, Security Logic, Peripheral Equipment, UART I/F, General propose ports, Data-bus, whole surface of IC-Chip, all the external terminal pins of IC-chip, ROM Program, IPL authentication key and IPL execution key, and Security Function Activated data are physical scope of TOE.

Operation of IPL Mode, STOP Mode、 firmware download function, Command Packet data, Response Packet data, Detection of illegal operation, Protection information leakage, Physical protection, Encryption of data, Mutual authentication, Protection of data passing through the interface, Self Test, and Protection of internal data are logical scope of TOE.

Guidance Documentation is also part of TOE. It consists of [OG], [IPL-UM], and [ATM].

[OG] RC-S940 Operation Guideline, Version 1.1, February 20, 2004
[IPL-UM] RC-S940 IPL User's Manual, Version 1.0, March 4, 2004
[ATM] RC-S940 Administrator Tools Manual, Version 1.0, February 19, 2004

These documentations are supplied to customer as administrator guidance and/or user guidance.
[OG] summarizes the procedures necessary in performing a secure operation of the system utilizing Sony RC-S940, that is, an IC-Chip for the reader / writer of contactless card system that comprises to Sony **FeliCa** specification. [IPL-UM] and [ATM] provides information about security features and usage of RC-S940 IPL Mode. [ATM] describes requirement to firmware development.

The components listed below are out scope of the TOE.

The reason why these components listed here out scope of the TOE is to expand the radius of operation / usage of this IC-Chip by giving the customers with some degree of flexibility.
The interface to be used depends upon the operating environment of the IC-Chip.
Because of this, the interface and the firmware for activation of the interface as well as Normal Mode to start up the firmware are determined.

RF CARD I/F and inactivated circuit are physical out scope of TOE. Normal Mode operated by Firmware is logical out scope of TOE.

TOE deliverables are summarized in the following table.

Item Type	Item	Version / Date	Form of delivery
Hardware	RC-S940 (CXD9768GG)	4	BGA Package
Software	RC-S940 ROM program	3	Embedded in ROM of RC-S940
Documentation	[OG] RC-S940 Operation Guideline	1.1 / February 20, 2004	Paper or electronic data
	[IPL-UM] RC-S940 IPL User's Manual	1.0 / March 4, 2004	Paper or electronic data
	[ATM] RC-S940 Administrator Tools Manual	1.0 / February 19, 2004	Paper or electronic data

2.3. Hardware of TOE

2.3.1. Block Diagram

Block diagram of the TOE is as shown in Figure 2 below.

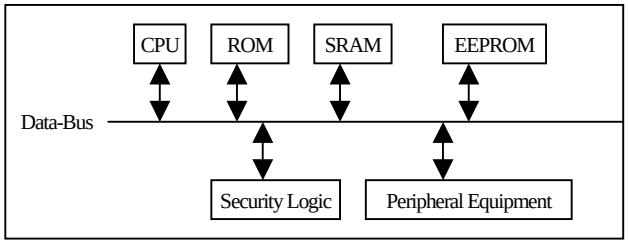


Figure 2: Block Diagram of TOE

2.3.2. Functional blocks of TOE

Configuration of the functional blocks of TOE are as listed below.

CPU:
16bit CPU with 16Mbytes of linear address space.

SRAM:
4kB SRAM built in the IC-Chip.

ROM:
16kB ROM built in the IC-Chip.
ROM program stored in the ROM.

EEPROM:
128kB (64kB x 2) EEPROM built in the IC-Chip.
A part of data (cryptographic keys and security function active data) stored in the EEPROM.
Firmware (out scope of the TOE) stored in the EEPROM.

Security Logic:
The security logic contains a cipher co-processor (Triple DES), random number generation function, and detect function (illegal voltage detect function, illegal frequency detect function, illegal temperature detect function).

Peripheral Equipment:
Peripheral equipment contains a timer, interrupt controller, reset controller, and clock gear.

2.4.ROM Program of TOE

TOE starts up the program stored to the internal ROM at the time of power-ON or reset. After performed a sequence of processes such as initialization, self-test for security function, EEPROM status checking, the ROM program acquires the terminal status to determine its operating mode.

Execution of operations in IPL Mode and STOP Mode is performed by the ROM program.

Initialization:

After the power-ON, the ROM program performs initialization of the hardware for example, (a) initialization of internal registers, and (b) initialization of SRAM area.

Power-ON Self Test

TOE executes Power-ON Self Test, i.e., one of the security functions.

If the result of Power-ON Self Test were failed, the process after that is not executed and immediately moves to STOP Mode.

Determination of Operating Mode

This function checks the integrity of the whole EEPROM and determines if double buffering (see SF.8) is activated. Furthermore it determines the selected operating mode (IPL Mode or Normal Mode) and starts the TOE in this mode. If an error occurs, TOE enters STOP Mode.

ATR Generation / Transmission

When TOE started up in IPL Mode, ATR (Answer To Reset) packet is transmitted from TOE to the controller. This is the packet to know the internal status (IPL, STOP or Normal Mode) of RC-S940.

IPL Mode

IPL Mode is the operating mode for downloading the firmware to EEPROM internal to RC-S940.

STOP Mode

STOP Mode is the operating mode to enter if any problems were detected that interferes RC-S940 from operating.

Normal Mode (Out of scope in this evaluation)

Normal Mode is the operating mode in which the downloaded reader / writer firmware starts up.

Firmware of IC-Chip (Out scope of the TOE)

The firmware downloaded to EEPROM during IPL Mode out of scope the TOE.

Only the administrator who is privileged by the Controller is able to download the firmware to EEPROM area by establishing the communication with the IC-Chip after encrypted mutual authentication and transiting to IPL Mode.

If the designated operating mode was Normal Mode, the process of data is delegated to the firmware (stored to EEPROM) from the ROM Program by re-starting the IC-Chip after download of the firmware completed.

Through the RF CARD I/F activated by this firmware, it is possible to establish the communication with a Contactless Smart Card.

This is the function to download the firmware to EEPROM area of the IC-Chip.

Only the administrator is able to download the firmware by establishing the communication with the IC-Chip after encrypted mutual authentication.

The firmware thus downloaded is the software developed by Sony Corporation or by the customer to make the communication possible between the IC-Chip and a Contactless Smart Card.

Be careful that the firmware out scope of the TOE.

2.5. Interface of the TOE

The TOE is equipped with physical interface, electrical interface, logical interface as well as communication interface.

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

Electrical Interface:
The electrical interface of TOE is all the external terminal pins of the IC-Chip.
The external terminal pins of the IC can be grouped into (a) power supply pins, (b) logic pins, and (c) analog pins.

Logical Interface:
The logical interface of TOE is (1) UART interface, (2) Mode set Interface, and (3) Data bus interface.

Note: The RC-S940 contains some function blocks (RF Card I/F and inactivated circuit shown in Figure.1) that are out scope of TOE because they are not activated in IPL Mode. The TOE has the interface with these blocks and that is Data Bus Interface.

Communication Interface:
The Communication interface of TOE is realized by commands passing through the UART interface.

2.6. Life-cycle of IC-Chip

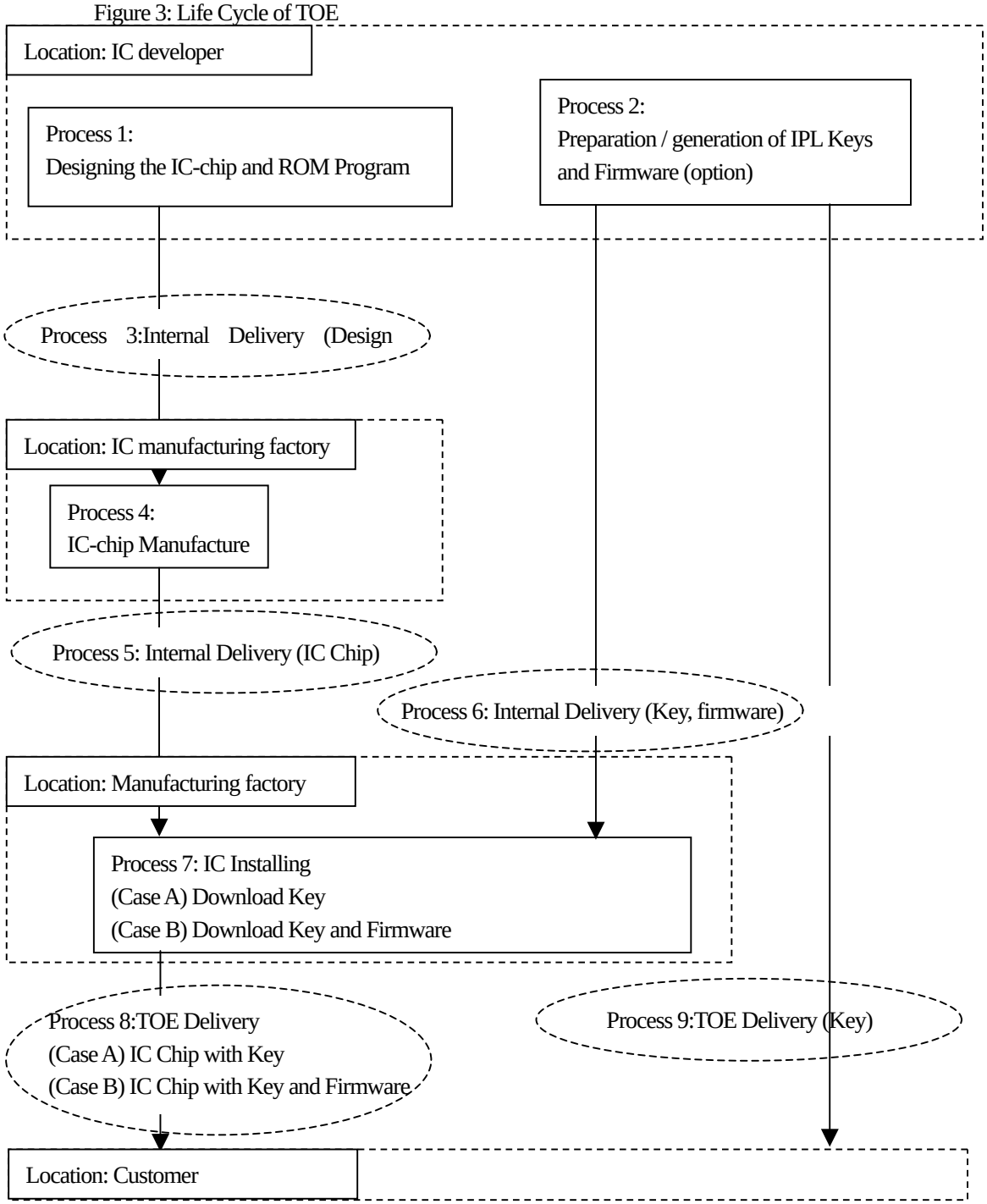
The life cycle of the TOE covers steps from the IC development to manufacturing factory.

The TOE's life cycle consists of Process 1 to Process 4.

Be careful that Process 5 to Process 9 constitutes the life cycle of the IC-Chip including the TOE.

The table below shows life cycle of the TOE. "Firmware (=Customer's own application which would be downloaded into the EEPROM through IPL Function)" is out scope of the TOE.

Figure 3: Life Cycle of TOE



The internal delivery processes 3, 5, and 6 are manufacturer internally only and are not meant to be the delivery according to CC class ADO. The TOE is delivered to the customer in processes 8 “TOE Delivery (IC Chip)” and 9 “TOE Delivery (Key)”.

Location: IC developer
Responsible Personnel: IC developer
Process 1: Designing the IC-chip
Process 2: Preparation / generation of IPL Keys and Firmware (option)
Contents: In Processes 1, design of the IC chip is, performed in locations under the security management in the development security environment.
In Process 2, in addition, preparation / generation of IPL Keys are performed. In the case of firmware-installed model of TOE, the reader/writer firmware is developed under the security management environment by Firmware Developer.

Location: -
Responsible Personnel: IC developer and IC manufacturing factory.
Items to be delivered: Hardware design and ROM program
Process 3: Internal Delivery (Design Information)
Contents: After the completion of design / development processes, hardware design information and ROM program are delivered to the IC manufacturing factory with the secure delivery procedures in Process 3.

Location: IC manufacturing factory
Responsible Personnel: IC manufacturer
Process 4: IC-chip Manufacture
Contents: In Process 4, the IC chip (TOE) is manufactured using hardware information and ROM program supplied from the IC developer.

Location: -
Responsible Personnel: Delivery personnel (company)
Items to be delivered: IC-chip (blank chip)
Process 5: Internal Delivery (IC Chip)
Contents: In Process 5, the IC chip (blank chip) manufactured in Process 4 is delivered to the manufacturing factory.

Location: -
Responsible Personnel: IC developer and manufacturing factory
Items to be delivered: IPL keys, Firmware (option)
Process 6: Internal Delivery (Key and firmware)
Contents: IPL keys and firmware (option) prepared in Process 2 are delivered to the manufacturing factory (writing the keys and the firmware to the IC) with the secure delivery procedures in Process 6.

Location: Manufacturing factory
Responsible Personnel: manufacturer
Process 7: IC Installing (Key and Firmware download)
Contents: In Process 7, IPL Keys and the firmware (option) are written to the IC chip delivered from the IC manufacturing factory in the previous process.

Location: -
Responsible Personnel: Delivery personnel (company)
Items to be delivered: IC Chip (containing key and firmware)
Process 8: TOE Delivery (IC Chip)
Contends: In Process 8, the IC chip (containing key and firmware) produced in Process 7 is delivered to the customer.

Location: -
Responsible Personnel: IC developer and customer
Items to be delivered: IPL keys
Process 9: TOE Delivery (Key)
Contents: IPL keys prepared in Process 2 are delivered to the customer with the secure delivery procedures in Process 9.

Roles and Responsibilities of Personnel:

IC developer:

IC developer is responsible for design work of the IC and development of the ROM program for the IC at the site of IC development manufacturer (in which physical security measures are provided).
IC developer is the personnel to whom the authorities to perform design, development and related jobs in the site of IC development manufacturer (in which physical security measures are provided).

IC Manufacturing factory:

The IC manufacturing factory is responsible for manufacturing IC chip (TOE) at the IC manufacturing factory (in which physical security measures are provided).

Manufacturing factory :

The Manufacturing factory is responsible for the installation of the key and firmware (option).

Delivery personnel (company):

The delivery personnel (company) are responsible for delivery of the IC chip (blank chip) from the IC manufacturing factory to the manufacturing factory and (b) delivery of the IC chip (contain key and firmware) from the manufacturing factory to the customer.

Customer (also called “Administrator”):

The customer is responsible for receiving the TOE and TOE operation after TOE delivery.

Firmware Developer (Customer or IC developer)

The firmware developer is responsible for developing firmware running on the TOE in Normal Mode. The firmware must be developed by a trustworthy developer that observes the requirements and hints give in the guidance documentation. (see assumption A.Priv).

2.7. Intended Usage

It is assumed that RC-S940 will be used in the form of a reader / Writer product manufactured utilizing the IC-Chip including the TOE as well as the other components.
Because of this, be careful that the following paragraphs describe the TOE's usage where the components are included that out of scope the TOE.

Customers are able to create the firmware to be downloaded to EEPROM of the IC-Chip.
The firmware can be created utilizing the Sony-provided library.
The firmware created utilizing this library is categorized into "RC-S940 Reader / Writer Standard Firmware" and "Firmware (developed by Customer)".

"Firmware (developed by Customer)" is the firmware developed and created by the customers.
The firmware created in conformance with the specific purpose can be used after downloading it from the controller to EEPROM in the IC-Chip and re-starting the IC-Chip.
With this, it is possible to accomplish the TOE operation as a system or as a unit that provides the secure communication utilizing mutual authentication as well as data encryption.

Be careful that, however, the firmware out of scopes the TOE.

The list below shows an example of operation as a system or a unit provided by the methods described above.

Transport System – 1:
In the case of using the TOE in transport systems, the TOE can be used at the entrance gate, or as money depositing / new card issuing device in railway stations.

Transport System – 2:
In the case of using the TOE in transport systems, the TOE can be used as transport fare box or new card issuing device in omnibus (in this case, TOE-equipped carrier is installed in stand-alone style).

Financial System:
In the case of using the TOE in financial systems, the TOE can be used as an ATM or payment device for electronic payment.

Sales System:
In the case of using the TOE in sales systems, the TOE can be used as payment device for electronic payment at station stands or convenience stores.

3. TOE Security Environment

Chapter 3 describes assets, assumptions, and threats of the TOE viewed from standpoints such as (a) the environment in which the TOE is intended to use, and (b) various aspects related with security that in what manner the TOE is used in such environment.

The TOE described in this ST is a product intended for any kind of commercial use where a basic security level is sufficient.

Note: The reader is reminded that the operation of the TOE in Normal Mode is out of scope of this evaluation.

3.1. Assets

Assets that must be protected by TOE are defined as the “Primary Assets”. Primary Assets consist of User data and TSF data. Assets other than above are defined as “Secondary Assets”.
Secondary Assets consist of data managed external to TOE, and the related documents.

3.1.1. Primary Assets of TOE

TOE’s assets are the **“User data”** and the **“TSF data”**.
The User data includes especially firmware and other data used by firmware. TSF data is security relevant data (e.g. cryptographic keys) used by TOE.

Because the User data and/or TSF data is transferred through external and internal interface and stored in the TOE, **“external communication data”**, **“internal communication data”** and **“data stored in the TOE”** shall be protected. External communication data is transferred between the Controller and the TOE and internal communication data is transferred through the data bus within the TOE. USER data and TSF data are stored to the EEPROM.

In order to protect integrity of User data and TSF data, **“results of data processing”** is defined as assets to be protected. Data processing by TOE includes encryption, decryption, generation of random number, calculation of check sum and CRC.

3.2. Assumptions

3.2.1. Physical Assumptions

A.External_Data External TOE Data

It is assumed that the management of external TOE data is performed in a secure manner.

Significant information regarding TOE profile, key information, and the firmware by administrator in databases not associated with the TOE. This information could contribute to a cloning attack. It is therefore important that the security of such data be adequately maintained.

3.2.2. Personnel Assumptions

A.Priv Abuse by Privileged Users

IC designer / developer, IC manufacturer, delivery personal, Administrator, and firmware developer are assumed to be trustworthy.

It is assumed that IC designers, IC developers, IC manufacturers, IC delivery personal, Administrator, and firmware developer who are privileged to operate and to manage the TOE are trained about operate and management of TOE, do not perform illegal operate of TOE and keep confidentiality of IC design information, ROM program, firmware and cryptographic keys.
It is also assumed that firmware developer designs firmware to meet requirements from guidance documentation.

3.2.3. Connectivity Assumption

A. CoSec_Com Controller Secure Communication

It is assumed that the Controller is capable to establish a secure communication channel.

The controller should have the capability of establishing a secure communication channel with TOE. This can be accomplished by mutual authentication and encryption technique. Once such a secure channel is established, the controller is authenticated and the communication is protected in confidentiality and in integrity.
The controller is outside the scope of this evaluation.

3.3. Threats

In the following the threats to the TOE are described. As the TOE may be used in many different environments and use cases, nature and value of the data to be protected are not known yet. Therefore it is impossible to estimate motivation of attackers and the possible attack potential the TOE has to face.
Therefore from the start this TOE is just intended to provide a basic protection level, i.e. its security functionality is claimed to be SOF-basic and any vulnerabilities shall not be exploitable by attackers possessing a low attack potential.

3.3.1. Threats to IC-Chip

Threats to IC-Chip during the operational phases are listed below:
"Expert" level is assumed in this ST for the level of attackers who may launch attacks to the TOE.
This is because knowledge and techniques on the IC-Chip are required since the TOE is an IC-Chip.
Dedicated tools are necessary, in addition, to attack the IC-Chip. This means that knowledge and techniques for utilization of these tools are also necessary to launch attacks to the TOE.
For attackers with such levels of knowledge and techniques, it is necessary to assume that they will launch attacks to the TOE with a distinct objective such as to gain money.
It is assumed that the overall attack potential is assumed to be low, as the AVA_VLA.2 component is used.

T.Malfunction Malfunction due to Environmental Stress

Attackers may modify the results of processing performed by the TOE.
Attackers may deactivate the security functions of the TOE.

Attackers may modify the processing results of encryption or computation performed by the TOE by applying environmental stresses to the TOE. Attackers also may deactivate the security functions of the TOE by applying environmental stresses to the TOE.
As attacking methods, generation of illegal voltage, illegal temperature, or illegal frequency is assumed.

T.Leak_Forced Forced Information Leakage

Attackers may disclose the data stored to EEPROM (i.e., cryptographic keys).

Attackers may disclose the data stored to EEPROM (i.e., cryptographic keys) through acquisition and analysis of forcibly leaked information.
As the attacking methods, DFA (Differential Fault Analysis, i.e., a method of searching by comparison between the normal and the corrupted data of encryption / computation process results) is assumed.
Note: The reader is reminded that the operation of the TOE in Normal Mode is out of scope of this evaluation.

T.Leak_Inherent Inherent Information Leakage

Attackers may disclose the data stored internal to EEPROM (i.e., cryptographic keys).

Attackers may disclose the data stored internal to EEPROM (i.e., cryptographic keys) during encryption or computation processes by acquiring and analyzing the inherently

leaking information.
As attacking methods, DPA: Differential Power Analysis (statistical analysis method of power consumption during encryption or computation processes) or SPA: Simple Power Analysis (analysis method by a single observation of the power consumption graph during encryption or computation processes) is assumed.
Note: The reader is reminded that the operation of the TOE in Normal Mode is out of scope of this evaluation.

T.Phys_Prob Physical Probing

Attackers may disclose the data in the TOE.

Attackers may disclose the data in the TOE through physical attack (i.e., analysis) to the TOE itself.
As attacking methods, analysis through direct observation with an electron microscope or an optical microscope and direct electrical measurement is assumed.

T.Phys_Manip Physical Manipulation

Attackers may manipulate the IC chip circuit or the data in the TOE.

Attackers may manipulate the IC chip circuit or the data on Data Bus of the TOE using the results of physical attack (i.e., analysis) to the TOE itself.
As attacking methods, FIB (Focused Ion Beam, i.e., a method for manipulating the IC chip circuit and data using ion beam) is assumed.

T. Clon Cloning

Attackers may create clones of the TOE itself, of a part of the TOE, of the security functions, or of a part of the security functions.

Attackers may create clones of the TOE by physical attack (i.e., analysis) to the TOE itself.
Attacking methods of “T.Phys_Prob” and “T.Phys_Manip” is assumed.

3.3.2. Threats to ROM Program

Threats during the operational phases to ROM Program of the chip are listed below:

T.Access **Invalid Access**

Attackers may disclose or / and modify the data in the TOE.

This threat assumes that attackers may disclose or modify the data in the TOE by illegally accessing the data in the TOE via the UART interface.
An attacker impersonating an administrator can illegally modify (re-write of IPL keys) data in the TOE.

T.Monitoring_Data **Monitoring Data**

Attackers may disclose the external communication data.

Attackers may disclose the data transferred between the TOE and the IT product (controller) by monitoring the external interface.
As the attack method, monitoring of the transferred data utilizing an analyzer is assumed.

T.Power_Down **Power Down**

Attackers may destroy the external communication data being transferred and / or the internal communication data (firmware) being written to the EEPROM of TOE. Attackers also may destroy such data by unintentional accidents.

By power-down to the TOE or to the IT product (controller), attackers may destroy the data being transferred through external interfaces, or the data being written to the EEPROM of TOE.
As the attack method, forced power-down to the TOE or to the IT product (controller) is assumed.
The power-down may occur because of unintentional accidents that result in destruction of data.

3.3.3. Threats Assumed to Environment

Threats assumed at the time of TOE delivery are as listed below:

TE.Delivery **Attacks during delivery**

Attackers may disclose or manipulate the data in the TOE.

Attackers may disclose or manipulate the data in the TOE by illegally accessing to the TOE under delivery, that is, by embedding illegal data to the TOE, exchanging with cloned TOE, manipulating the data in the TOE, or intercepting the information in the TOE.
As attacking methods, spoofing as the delivery personnel of the TOE is assumed.

3.4. Organizational Security Policies

None.

4. Security Objectives

This chapter describes the security objectives against threats identified in “Chapter 3. TOE Security Environment” of this document.
Note: The reader is reminded that the operation of the TOE in Normal Mode is out of scope of this evaluation.

4.1. Security Objectives for the TOE

4.1.1. Security Objectives for the IC-Chip

O.Malfunction Protection against Malfunction

TOE shall provide protection to (a) results of TOE’s encryption and computation processes from modification, and (b) deactivation of the security functions caused by environmental stresses.

As the method of protection against environmental stresses, TOE shall be equipped with the security functions for protection of (a) results of data processing internal to TOE (i.e., encryption and computation) from modification, and (b) deactivation of the security functions. As the method of protection, detection of illegal operating condition is assumed.

O.Leak_Protection Protection against Inherent Information Leakage

Note: The reader is reminded that the operation of the TOE in Normal Mode is out of scope of this evaluation.
TOE shall provide protection to the data in the TOE from leakage of information.

As the method of protection from information leakage, TOE shall be equipped with the security functions to provide protection to the confidentiality of the data internal to EEPROM (i.e., cryptographic keys).
As the methods of protection, countermeasures against SPA/DPA are assumed.

O.Phys_Protection Protection against Physical Probing

TOE shall provide protection to the data in the TOE from physical probing and manipulation.

As the method of protection from physical probing and manipulation, TOE shall be equipped with the security functions to protect the integrity and the confidentiality of data in the TOE.
As the method of protection, Tamper Resistance Layout and Test Mode Protecting Functions are assumed.

4.1.2. Security Objectives for the ROM Program

O.Data_Acc Data Access Control

TOE shall provide protection to the data internal to TOE from illegal access.

As the method of protection from illegal access, TOE shall be equipped with the security functions to provide protection to the integrity and the confidentiality of data internal to TOE.
As the method of protection, Authentication and Identification functions are assumed.

O.Prot_Interface Protection Interface

The TOE shall provide protection to the external communication data being transferred on the external interface from monitoring.

As the countermeasures against monitoring, the TOE shall be equipped with the security functions to provide protection to the secrecy of the data being transferred on the external interface.
As the method of protection, encryption of transferred data is assumed.

O.Self_Test Self Test

TOE shall provide protection to the data stored in the TOE from unauthorized modification and to TSF from failures and deactivation.

As the method of protection to the integrity of the stored data in the TOE and protection to TSF from failures and deactivation, TOE shall be equipped with the functions to perform self validation to ROM, EEPROM, encryption / decryption of communication data, and generation of pseudo random numbers at the time of initial start up.
As the method of protection, Self-Test at the time of initial start up is assumed.

O.InData_Pro Internal Data Protection

The TOE shall provide protection to the external communication data and the data stored to the TOE from destruction and / or failure of data writing.

As the countermeasures against destruction of external and internal communication data and / or failure of data writing to the EEPROM, the TOE shall be equipped with the security function to provide protection to the integrity of external and internal communication data from destruction or failure of data writing.
As the method of protection, check sum and parity check of external communication data, “verify at the time of data write” or Rollback function is assumed.

4.2. Security Objectives for the Environment

IT Security Target for IT environment

OE. CoSec_Com Controller Secure Communication

IT environment shall provide a secure communication channel to maintain the authenticity with the TOE.

As the capability of maintaining the authenticity with the TOE, the Controller shall provide the mutual authentication and encryption functions.

Non-IT Security Target for IT Environment

OE.External_Manage Management of External TOE data

Non-IT environment shall provide the secure management to the data external to TOE.

External environment stored external TOE data (key information and firmware) must be controlled for confidentiality and integrity according to the owner's needs. The personnel and systems in charge of this information are responsible for the maintenance of its required security.

OE.Pers Personnel

Non-IT environment shall provide the secure management and manipulation of data outside the TOE.

For example, non-IT environment (an administrator, IC designer / developer, IC manufacturer, delivery personal, Administrator and firmware developer) shall provide the capability to perform secure management and manipulation of data outside the TOE. The firmware developer shall design firmware to meet guidance documentation.

OE. Delivery Delivery procedures

Non-IT environment shall provide the secure delivery procedure of TOE.

For example, non-IT environment (delivery procedure) shall provide the capability to perform the secure delivery of TOE. The delivery selects specific transporters that perform transportation of the TOE. And the delivery attaches seals to the package of the TOE.

5. IT Security Requirements

5.1. TOE Security Requirements

5.1.1. TOE Security Functional Requirements

The claimed minimum strength of functions level for the TOE security functional requirements is SOF-basic.

Table 1. TOE Security Functional Requirements

Functional Component ID	SFR Name	Operation	Strength of Functions
FPT_FLS.1	Failure with preservation of secure state	Assignment	
FPT_PHP.3	Resistance to physical attack	Assignment	SOF-basic
FDP_IFC.1	Subset information flow control	Assignment	
FDP_IFF.1	Simple security attribute	Assignment	
FDP_ITT.1	Basic internal transfer protection	Selection Assignment	
FPT_ITT.1	Basic internal TSF data transfer protection	Selection	
FDP_SDI.1	Stored data integrity monitoring	Assignment	
FPT_RCV.4	Function recovery	Assignment	
FDP_UIT.1	Data exchange integrity	Selection Assignment	
FDP_UCT.1	Basic data exchange confidentiality	Selection Assignment	
FCS_COP.1	Cryptographic operation	Assignment	
FCS_CKM.1	Cryptographic key generation	Assignment	SOF-basic
FCS_CKM.4	Cryptographic key destruction	Assignment	
FPT_TST.1	TSF testing	Selection Assignment	
FTP_ITC.1	Inter-TSF trusted channel	Selection Assignment	SOF-basic
FIA_UID.1	Timing of identification	Assignment	SOF-basic
FIA_UAU.2	User authentication before any action	N/A	SOF-basic
FIA_AFL.1	Authentication failure handling	Assignment	
FDP_ACC.1	Subset access control	Assignment	
FDP_ACF.1	Security attribute based access control	Assignment	
FMT_SMR.1	Security roles	Assignment	
FMT_MTD.1	Management of TSF data	Selection Assignment	

Table 2. TOE Security Functional Requirements (continued)

Function Component ID	SFR Name	Operation	Strength Of Functions
FMT_MSA.2	Secure security attribute	N/A	
FMT_MSA.3	Static attribute initialization	Selection Assignment	
FMT_MSA.1.A	Management of security attributes	Selection Assignment	
FMT_MSA.1.B	Management of security attributes	Selection Assignment	
FMT_SMF.1	Specification of Management Functions	Assignment	

Threats: T.Malfunction, T.Power_Down

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [***Illegal temperature, Illegal voltage, Illegal frequency, Encryption failure, Pseudorandom number failure, Power failure and communication failure***].

Threats: T.Malfunction

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self-tests that [***during initial start-up***] to demonstrate the correct operation of the TSF.

Application note for FPT_TST.1: The following self tests are performed:

-Single testing of encryption and decryption during the initial start-up using a known Combination of plain text / cipher text / key.

- Comparison between random numbers of 16 Bytes sequentially generated twice during the initial start-up to check whether these two random numbers have different values or not.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of [***TSF data***].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

Threats: T.Malfunction, T.Phys_Prob & T.Phys_Manip

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist [***T.Malfunction, Physical Probing and Physical Manipulation***] to the [***TSF***] by responding automatically such that the TSP is not violated.

Threats: T.Leak_Inherent, T.Leak_Forced, T.Power_Down and T.Monitoring_Data

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [***Data Processing Policy***] on [***subjects: controller, TOE; information: User Data; operation: transmit or receive between controller and TOE***].

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [***Data Processing Policy***] based on the following types of subject and information security attributes: [***transaction key, parity, and checksum***].

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:
[***Subject TOE is allowed to transmit data dedicated for the controller to subject Controller, and receive data dedicated for the TOE from the Controller via the UART I/F if it holds following rules.***
1) communication data shall be encrypted by transaction key;
2) transaction key shall be changed for each authentication .].

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 authorize 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:
[***1) If the communication data has not been encrypted by transaction key, it is denied.***
2) If the parity of the communication data is not correct, it is denied.
3) If the checksum of the communication data is not correct, it is denied .
].

FDP_ITT.1 Basic internal transfer protection

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

FPT_ITT.1 Basic internal TSF data transfer protection

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

Application Note for FDP_ITT.1 and FPT_ITT.1

Because the Communication data between controller and the TOE is also transferred in the TOE between physically separated parts of the TOE, internal transfer protection is required to protect communication data. The refor, FDP_ITT.1 and FPT_ITT.1 are related to the Data Processing Policy (defined in FDP_IFF.1) because both SFRs ensure that this policy is not bypassed even in the case that User or TSF data is transmitted between physically separated parts of the TOE.

Note: The reader is reminded that the operation of the TOE in Normal Mode is out of scope of this evaluation.

Threats: T.Power_Down

FPT_RCV.4 Function recovery

FPT_RCV.4.1 The TSF shall ensure that [***Illegal temperature, Illegal voltage, Illegal frequency, Encryption failure, Pseudorandom number failure, Power Failure and Communication Failure scenarios***] have property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

Threats: T.Power_Down, T.Monitoring_Data

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: [***checksum and parity of the transmit data, CRC check of the ROM, and parity check of the writing data to EEPROM***].

FDP_UIT.1 Data exchange integrity

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

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

FDP_UCT.1 Basic data exchange confidentiality

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

Application Note for FDP_UIT.1 and FDP_UCT.1

Thus, these transferred data are addressed in ***Data Processing Policy*** defined in FDP_IFC1.1.

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [***encryption / decryption of data***] in accordance with a specified cryptographic algorithm [***Triple Data Encryption Standard (Triple DES)***] and cryptographic key size [***112 bits (Triple-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)***] that meet the following: [***AIS20, Functionality Class K2, strength of mechanism medium***].

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***].

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 [***IPL Authentication***].

Threats: T.Access

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [***IPL authentication 1 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.

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect [***when a configurable number of***] unsuccessful authentication attempts occur related to [***IPL authentication***].

FIA_AFL.1.2 When the specified number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [***perform IPL Lock state***].

Application Note for FIA_AFL.1

Customer specifies number of times of successive failure of IPL mutual authentication, which is then set by IC manufacturer during fabrication. In order to disable IPL Lock function data (number of times of successive failure of IPL mutual authentication) shall be set to 0.

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [***Access Control Policy***] on [***subject: administrator; objects: firmware; operations: download***].

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [***Access Control Policy***] to objects based on [***security attributes: subject role (administrator/unauthenticated user), IPL execution key, IPL Lock State (locked / not locked)***].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine whether an operation to controlled subjects and controlled objects is allowed or not: [
In accordance with Access Control Policy, it is possible to perform following operations.
1) The administrator is authorized to download firmware;
2) ***An unauthenticated user is not authorized to download firmware.***]

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [***following rules:***
1) If the firmware download package has not been created using the IPL Execution key, firmware download is denied.
2) If the TOE is in IPL Locked state, firmware download is denied].

Application Note for FDP_ACC.1 and FDP_ACF.1

Access Control Policy defines the object usage rules (i.e., rules applicable to the subjects that use the objects). Thus, only the personnel who satisfy the conditions defined in this policy is capable to use this function.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the role of [***administrator***].

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

FMT_MSA.2 Secure security attributes

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

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [***modify***] the [***IPL authentication key and IPL execution key***] to [***administrator***].

FMT_MSA.3 Static attribute initialization

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

FMT_MSA.3.2 The TSF shall allow the [***following authorized roles: none***] to specify alternative initial values to override the default values when an object or information is created.

Application Note for FMT_MSA.3

The TOE cannot create new objects. The only object is the firmware, which is update during download operation. The access conditions for this operation is restrictive (i.e., access is only granted when the correct IPL execution key has been used) and cannot be changed.

FMT_MSA.1.A Management of security attributes

FMT_MSA.1.1.A The TSF shall enforce the [***Access Control Policy***] to restrict the ability to [***modify***] the security attributes [***IPL execution key***] to [***administrator***].

FMT_MSA.1.B Management of security attributes

FMT_MSA.1.1.B The TSF shall enforce the [***Access Control Policy***] to restrict the ability to [***clear***] the security attributes [***IPL Locked state***] to [***Administrator***].

FMT_SMF.1 Specification of Management Functions

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

[

1) change the IPL authentication key and IPL execution key.

2) release IPL Lock state.

].

5.1.2. TOE Security Strength of Function Claims

The strength of function expected to TOE is SOF-Basic in accordance with the recommendation in Part 3 of CC when selected EAL4.

5.1.3. TOE Security Assurance Requirements

The security assurance level for TOE is EAL4.
In the table below, the security assurance requirements of EAL4 extracted from Part 3 of CC are enumerated:

Table 2. TOE Security Assurance Requirements

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

5.2. Security Requirements for the IT Environment

The security requirements for the IT environment are extracted out of the requirements in Part 2 of CC. All the requirements stated here define the security requirements for TSF environment, not for TSF itself, by replacing the term "TSF" with the term "IT environment".

Table 3. Security Requirements for the IT Environment

Functional component ID	SFR Name	Operation	Strength Of Functions
FCS_COP.1	Cryptographic operation	Assignment	
FCS_CKM.1	Cryptographic key generation	Assignment	SOF-basic
FCS_CKM.4	Cryptographic key destruction	Assignment	
FTP_ITC.1	Inter-TSF trusted channel	Selection Assignment	SOF-basic

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 cryptographic key sizes [***112 bits (Triple-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)***] 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, i.e. there is no standard applicable here***].

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 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 [***IPL authentication***].

6. TOE Summary Specification

6.1. TOE Security Functions

This section describes the TOE security functions that satisfy the security functional requirements enumerated in Chapter 5.
The claimed minimum strength of functions level for the TOE security functions is SOF-basic.
The security functions based on permutational or probabilistic mechanisms are SF3 (the Tamper Resistance Layout part of SF3), SF4-1, SF4-2, SF4-3, SF5-1 and SF6. The encryption/decrypt part of SF4-2 and entire SF6 are purely based on cryptographic mechanisms (encrypt of arbitrary plain texts) and therefore do not have to be SOF-rated. The claimed minimum strength of function for the remaining ones SF3, pseudo random number part of SF4-1, SF4-3 and SF5-1 is SOF-basic. For rating of SF4-1 and SF4-3 the corresponding requirements from AIS20, "Functionality classes and evaluation methodology for deterministic random number generators", Version 1, 1999-12-02, will be applied with a target of Functionality Class K2 and strength of mechanism medium according to AIS20.

6.1.1. Security Functions of IC-Chip

SF.1 Detection of illegal operation

This function detects illegal temperature, voltage, and frequency of TOE that outside the normal operating scope of TOE because of trouble, accident, or intentional act during data processing by TOE. When detected any abnormal values, the TOE performs a system reset.

Security functional requirements satisfied: FPT_PHP.3, FPT_FLS.1, FPT_RCV.4.

SF.2 Protection to information leakage

To convert the information leaked out of hidden channels located within TOE during encryption process and computation process into non-beneficial information, the SPA/DPA-resistant CRYPTO Engine is used as the countermeasures against power consumption analysis to provide protection to the confidentiality of data during encryption process and computation process.

Security functional requirements satisfied: FDP_IFC.1, FDP_IFF.1, FDP_ITT.1, FPT_ITT.1.

SF.3 Physical protection

A special TOE design and construction ("Tamper Resistant Layout" which uses glue logic layout, shield layers, etc.) makes physical analysis (reverse engineering) or modification (tampering) of the TOE difficult.
In addition entry into Test Mode is protected by different protection functions.
These features protect the integrity of the complete TOE including SRAM, ROM, and EEPROM.
It therefore protects all User and TSF Data against disclosure by physical probing when stored or while being processed by the TOE.

SF.3 supports the correct and secure operation of all other security functions and is effective in all operational modes permitted after TOE delivery.

Security functional requirements satisfied: FPT_PHP.3

SF4 Encryption of data

To perform the encryption of communication data, "CRYPTO Engine" and "Pseudorandom Number Generator" provide support to the encryption as well as the generation of pseudo random numbers.
Note: The functionality of SF4 (Pseudo random number generation and DES engine) described in the following is limited to the operation of the TOE in IPL mode.

SF4-1 CRYPTO Engine

CRYPTO Engine performs encryption / decryption processes of communication data using the pseudo random numbers generated by Pseudorandom Number Generator.
Generation of this pseudo random number conforms to the following standards.

- “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications” (except 2.6 Discrete Fourier Transform (Spectral) Test), NIST Special Publication 800-22 (with revisions dated May 15,2001).
- "Application Notes and Interpretation of the Scheme (AIS), Functionality classes and evaluation methodology for deterministic random number generators”, AIS 20, Version 1 as of 1999-12-02.

SF4-2 Cipher system supported

Triple DES Cipher system
For the mutual authentication in IPL mode between TOE and the controller, a secure communication is achieved using Triple DES cipher system in which a 112-bit key is used.
Secure communication in IPL mode between TOE and the controller is achieved using Triple DES cipher system. The mode of operation is CBC mode.

SF4-3 Processes supported

The pseudo random number is used for encryption / decryption processes of the communication data and as the data for noise generation as the countermeasures against DPA.

Security functional requirements satisfied: FCS_CKM.1, FCS_COP.1

6.1.2. Security Functions of ROM Program

SF.5 Mutual authentication

This is the authentication function for prevention of illegal access.

SF5-1 IPL mutual authentication

IPL mutual authentication is performed between the controller and TOE when the administrator who knows IPL authentication key executed IPL mutual authentication from the terminal to which the controller is connected.

During IPL mutual authentication, the confidentiality of communication data on the interface is protected by Triple DES cipher system. This is also true for the case of communication data after successful IPL mutual authentication.

SF 5-2 IPL Lock Function

In this IPL mode, IPL Lock function is activated to prevent illegal data access by spoofing an administrator during IPL mode. If IPL mutual authentication successively failed, this function locks the system and after that, execution of IPL mutual authentication is impossible.

Allowable limit of successive failures of IPL mutual authentication is set up at the time of shipping of TOE.

Security functional requirements satisfied: FIA_UID.1, FIA_UAU.2, FIA_ALF.1, FDP_ACC.1, FDP_ACF.1, FMT_SMR.1, FMT_MTD.1, FMT_MSA.1.A, FMT_MSA.1.B, FMT_MSA.2, FMT_MSA.3, FMT_SMF.1., FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FTP_ITC.1

SF.6 Protection of data passing through the interface

External interface used: UART I/F

Communication in IPL mode

Communication data during IPL mutual authentication is protected by Triple DES cipher system.

Communication data after successful IPL mutual authentication is also protected by Triple DES cipher system.

Parity check is used for checking the communication data packet.

Checksum is used for checking the communication data.

Security functional requirements satisfied: FCS_COP.1, FDP_SDI.1, FTP_ITC.1, FDP_UIT.1, FDP_UCT.1, FPT_FLS.1, FPT_RCV.4, FDP_IFC.1, FDP_IFF.1.

SF.7 Self Test

At the initial start-up of the TOE, performs self-test on pseudo-random number generation.
At the initial start-up of the TOE, performs self-test on encryption / decryption functions.
At the initial start-up of the TOE, performs CRC check to the ROM.
At the initial start-up of the TOE, performs Checksum test or CRC check to EEPROM.
At the initial start-up of the TOE, performs CRC check to EEPROM if the firmware is downloaded in EEPROM of TOE.

Security functional requirements satisfied: FPT_TST.1, FDP_SDI.1, FPT_FLS.1, FPT_RCV.4.

SF.8 Protection of internal data

Even if the data being written to EEPROM during loading firmware is corrupted, "Double Buffering" protects the integrity of written data. Double Buffering detects the corrupted data, and restores the data to the state before data writing, i.e. when loading firmware to one buffer fails, still the previously loaded firmware in the other buffer will be active.
By setting "One Time Write" function to "Enable" state, it is possible to inhibit illegal data write to EEPROM to protect parameters that define the behaviour of the security functions from being modified any further. At the time of data write to EEPROM, in addition, "Verify" process is performed.

Security functional requirements satisfied: FDP_SDI.1, FPT_FLS.1, FPT_RCV.4.

6.2. Assurance Measures

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

Table 4. Assurance Measures

SAR ID	Assurance Requirement Name	Document Name
ACM_AUT.1	Partial CM automation	Development Configuration Management Document
ACM_CAP.4	Generation support and acceptance procedure	
ACM_SCP.2	Problem tracking CM coverage	
ADO_DEL.2	Detection of modification	Delivery Procedure Document
ADO_IGS.1	Installation, generation, and stat-up procedure	Development Environment Document
ADV_FSP.2	Fully defined external interfaces	Interface Specifications
ADV_HLD.2	Security enforcing high-level design	Higher Hierarchy Design Document
ADV_IMP.1	Subset of the implementation of the TSF	Source Code Block Diagram
ADV_LLD.1	Descriptive low-level design	Lower Hierarchy Design Document
ADV_RCR.1	Informal correspondence demonstration	Development Relationship Diagram
ADV_SPM.1	Informal TOE security policy model	Security Policy Model document.
AGD_ADM.1	Administrator guidance	Documents for Administrator use
AGD_USR.1	User guidance	
ALC_DVS.1	Identification of security measures	Development Environment Document
ALC_LCD.1	Developer defined life-cycle model	Life Cycle Document
ALC_TAT.1	Well-defined development tools	Tool Document
ATE_COV.2	Analysis of coverage	Test Document
ATE_DPT.1	Testing: High-level design	
ATE_FUN.1	Functional testing	
ATE_IND.2	Independent testing – sample	
AVA_MSU.2	Validation of analysis	Analysis Document
AVA_SOF.1	Strength Of TOE security functional evaluation	Strength of Functions Document
AVA_VLA.2	Independent vulnerability analysis	Vulnerability Analysis Document

7. PP Claims

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

7.1. PP Reference

None.

7.2. PP Tailoring

None.

7.3. PP Additions

None.

8. Rationale

8.1. Security Objectives Rationale

This section certifies that (a) the security objectives for TOE and the security objectives for environment are adequately selected, and (b) they correctly correspond with all the identified threats and the Assumptions.

Table 5. Security Protection Rationale

Assumption / Threats	Addressed by Objectives (TOE / TOE Environment)
A.External_Data	OE.External_Manage
A.Priv	OE.Pers
A.CoSec_Com	OE.CoSec_Com
T.Malfunction	O.Malfunction, O.Self_Test
T.Leak_Inherent	O.Leak_Protection
T.Leak_Forced	O.Malfunction
T.Phys_Prob	O.Phys_Protection
T.Phys_Manip	O.Phys_Protection
T.Access	O.Data_Acc
T.Monitoring_Data	O.Prot_Interface
T.Power_Down	O.InData_Pro
T.Clon	O.Phys_Protection, OE. External_Manage
TE.Delivery	OE.Delivery

Table 6. Assumptions Rationale

Objectives (TOE / TOE Environment)	Addressed by Assumption
OE.External_Manage	A.External_Data
OE.Pers	A.Priv
OE.CoSec_Com	A CoSec_Com

Table 7. Threats Rationale

Objectives (TOE / TOE Environment)	Addressed by Threats
O.Malfunction	T.Malfunction, T.Leak_Forced
O.Self_Test	T.Malfunction
O.Leak_Protection	T.Leak_Inherent
O.Phys_Protection	T.Phys_Prob
O.Phys_Protection	T.Phys_Manip
O.Data_Acc	T.Access
O.Prot_Interface	T.Monitoring_Data
O.InData_Pro	T.Power_Down
O.Phys_Protection, OE.External_Manage	T.Clon
OE.Delivery	TE.Delivery

Adequacy of Assumptions and Security Objectives

A.External_Data External Data of TOE assumes the necessity of secure handling and management procedures of data to be managed external to TOE. ***OE.External_Manage Management of External TOE data*** provides such capability within the environment.

A.Priv Abuse by Privileged Users indicates the necessity of assigning the adequately trained and trustworthy personnel to the privileged positions. ***OE.Pers Personnel*** provides such capability within the environment.

A.CoSec_Com Controller Secure Communication indicates the assumption that the controller is equipped with the capability for a secure communication. ***OE.CoSec_Com Controller Secure Communications*** address these assumptions. They ensure the controller device and the card device capable of establishing and using such a link.

Adequacy of threats and security objectives

T.Malfunction Malfunction due to Environmental Stress is the threat intending modification of TOE's processing results as well as deactivation of the security functions. ***O.Malfunction Protection against Malfunction*** copes with this threat. These security objectives protect TOE's processing results of encryption or computation by detecting the environmental stress to TOE and performing the procedure to prevent occurrence of illegal operation. ***O.Self_Test TSF Self Test*** is also used to cope with this threat. This security objectives maintains the operation and the functions of TOE and TSF by performing self-tests for TOE's memories and encryption / decryption functions as well as pseudo random number generation.

T.Leak_Inherent Inherent Information Leakage is the threat intending disclosure of the data internal to EEPROM (cryptographic keys). ***O.Leak_Protection Protection against Inherent Information Leakage*** copes with this threat. This security objective protects the confidentiality of data internal to EEPROM by converting the leaked information into non-beneficial information form. As the method of protection from inherent information leakage, TOE shall be equipped with the security functions against SPA/DPA to protect the confidentiality of the data internal to EEPROM (i.e., cryptographic keys).

T.Leak_Forced Forced Information Leakage is the threat intending disclosure of the data internal to EEPROM (cryptographic keys). ***O.Malfunction Protection against Malfunction*** copes with this threat. This security objective protects the confidentiality of data internal to EEPROM (cryptographic key) by protecting TOE's processing results of encryption or computation by detecting the environmental stress to TOE and performing the procedure to prevent occurrence of illegal operation.

T.Phys_Prob Physical Probing and T.Phys_Manip Physical Manipulation is the threat intending disclosure and manipulation of data in the IC-Chip or on Data Bus of TOE. ***O.Phys_Protection Physical Protection*** is used to cope with this threat These security objectives protects the confidentiality and integrity of data stored to ROM using "Tamper Resistance Layout" and " Test Mode Protecting Functions" that make the analysis of data difficult even if any physical attack against TOE is launched by an attacker.

T.Power_Down Power Down is the threat intending destruction of data being written to the TOE.
In addition, this threat includes destruction of data resulted from unintentional accidents. ***O.InData_Pro TOE Data Protection*** is used to cope with this threat. These security objectives protects the integrity of data internal to TOE using "Roll Back" to maintain the data in a state before it is written to the memory even if the data processing is interrupted during data writing to TOE.
As the method of protection, check sum and parity check of external communication data, “verify at the time of data write” or Rollback function is assumed.

T.Access Invalid Access is the threat intending disclosure and modification of data internal to TOE.
O.Data_Acc Data Access Control is used to directly cope with this threat. These security objectives protect the confidentiality of data internal to TOE by performing the operation defined in Access Control Policy. As the method of protection, Authentication and Identification functions are assumed.

T.Monitoring_Data Monitoring Data is the threat intending the disclosure of transferred data.
O.Prot_Interface Protection Interface is used to cope with this threat. These security objectives protect the confidentiality of TOE data by encrypting TOE data passing through the interface. As the method of protection, encryption of transferred data is assumed.

T.Clon Cloning is the threat intending clone creation of TOE itself, a part of TOE, security functions, or a part of security functions. ***O.Phys_Prot Physical Protection*** is used to cope with this threat. These security objectives protects the integrity of data internal to ROM using "Tamper Resistance Layout" and " Test Mode Protecting Functions " that make analysis of data difficult even if any physical attacks were launched to TOE by attackers. In addition, ***OE.External_Manage Management of External TOE data*** provides assistance to opposition against this threat. With these non-IT environment security objectives, protection is provided to the data external to TOE.

Adequacy of Threats and Security Objectives for non-IT Environment

TE.Delivery During attack delivery is the threat intending disclosure and manipulation of TOE. ***OE.Delivery Delivery procedure*** is used to cope with this threat. These security objectives for non-IT environment protect the integrity and the confidentiality of the TOE itself by performing delivery of TOE with the secure and approved delivery procedures.

8.2. Security Requirements Rationale

8.2.1. TOE Security Functional Requirements Rationale

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

Table 8. TOE Security Functional Requirements Rationale

TOE Objectives	Addressed by SFR
O.Malfunction	FPT_PHP.3, FPT_FLS.1, FPT_RCV.4.
O.Self_Test	FPT_TST.1,FDP_SDI.1, FPT_FLS.1, FPT_RCV.4.
O.Leak_Protection	FDP_IFC.1, FDP_IFF.1, FDP_ITT.1, FPT_ITT.1.
O.Phys_Protection	FPT_PHP.3
O.InData_Pro	FDP_SDI.1, FPT_FLS.1, FPT_RCV.4, FDP_UIT.1.
O.Data_Acc	FIA_UID.1, FIA_UAU. 2, FIA_AFL.1, FDP_ACC.1, FDP_ACF.1, FMT_SMR.1, FMT_MTD.1, FMT_MSA.1.A, FMT_MSA.1.B, FMT_MSA.2, FMT_MSA.3, FMT_SMF.1., FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FTP_ITC.1
O.Prot_Interface	FDP_IFF.1, FDP_IFC.1, FCS_COP.1, FTP_ITC.1, FDP_UCT.1

Table 9. Security Objectives Rationale

SFR	Addressed by TOE Objectives
FPT_FLS.1	O.Malfunction, O.Self_Test, O.InData_Pro
FPT_PHP.3	O.Malfunction, O.Phys_Protection
FPT_TST.1	O.Self_Test
FDP_IFC.1	O.Leak_Protection, O.Prot_Interface
FDP_IFF.1	O.Leak_Protection,O.Prot_Interface
FDP_ITT.1	O.Leak_Protection
FPT_ITT.1	O.Leak_Protection
FPT_RCV.4.	O.Malfunction, O.Self_Test, O.InData_Pro
FDP_SDI.1	O.InData_Pro
FCS_COP.1	O.Data_Acc, O.Prot_Interface
FCS_CKM.1	O.Data_Acc
FCS_CKM.4	O.Data_Acc
FTP_ITC.1	O.Data_Acc, O.Prot_Interface
FDP_UIT.1	O.InData_Pro
FDP_UCT.1	O.Prot_Interface

Table 10. Security Objectives Rationale (continued)

SFR	Addressed by TOE Objectives
FIA_UID.1	O.Data_Acc
FIA_UAU.2	O.Data_Acc
FIA_AFL.1	O.Data_Acc
FDP_ACC.1	O.Data_Acc
FDP_ACF.1	O.Data_Acc
FMT_SMR.1	O.Data_Acc
FMT_MTD.1	O.Data_Acc
FMT_MSA.2	O.Data_Acc
FMT_MSA.3	O.Data_Acc
FMT_MSA.1.A	O.Data_Acc
FMT_MSA.1.B	O.Data_Acc
FMT_SMF.1	O.Data_Acc

Table 10. Security Functional Requirements for IT Environment Rationale

TOE Objectives	Addressed by SFR
OE.CoSec_Com	FCS_COP.1, FCS_CKM.1, FCS_CKM.4, FTP_ITC.1.

Table 11. Security Objectives for IT Environment Rationale

TOE Objectives	Addressed by SFR
FCS_COP.1	OE.CoSec_Com
FCS_CKM.1	OE.CoSec_Com
FCS_CKM.4	OE.CoSec_Com.
FTP_ITC.1	OE.CoSec_Com.

Table 12. Security Objectives for non-IT Environment Rationale

TOE Environment (Non-IT) Objectives
OE.External_Manage
OE.Pers
OE.Delivery

Adequacy of Security policy and Security Functions Requirements

Table 13. Adequacy of the security objectives and SFR - 1

The relationship between the security objectives and the security functional requirements is as shown in the table below:		
O.Malfunction Protection against Malfunctions intends implementation of providing protection to (a) results of TOE's encryption and computation processes from modification, and (b) deactivation of the security functions caused by environmental stresses. This security policy detects the environmental stress with ***FPT_PHP.3 Resistance to physical attack*** and maintains the TOE in secure conditions with ***FPT_FLS.1 Failure with preservation of secure state***. And ***FPT_RCV.4 Function recovery*** provide for secure operation in case of environmental stress.		
This TOE assumes the following threats.		
TOE Threats	T.Malfunction	Attackers may destroy the results of processing performed by the TOE. Attackers may deactivate the security functions of the TOE.
	T.Leak_Forced	Attacker may disclose the data (Key) in EEPROM.
Following security objectives is used to cope with this threat.		
TOE Objectives	O.Malfunction	TOE shall provide protection to the processing results of TOE's encryption and computation from modification, and to the security functions from deactivation caused by environmental stresses.
The following security functional requirements meet this objective.		
SFR	FPT_FLS.1	This maintains the secure status of TOE when environmental stress occurred.
	FPT_RCV.4	Automated recovery of TOE when environmental stress occurred.
	FPT_PHP.3	If environmental stress occurred, TOE itself automatically detects the stress occurrence and executes a reset to TOE itself to maintain the secure status of TOE.

Table 14. Adequacy of the security objectives and SFR - 2

<table>
<tr><td colspan="3">The relationship between the security objectives and the security functional requirements is as shown in the table below:</td></tr>
<tr><td colspan="3">O.Self_Test Self Test intends implementation of maintaining the reliability of the TOE as well as TSF function. This security policy maintains the reliability of TSF by performing encryption / decryption tests and self-generation test of pseudo-random number using FPT_TST.1 TSF testing.
This security policy also performs self-validation to ROM and EEPROM using FDP_SDI.1 Stored data integrity monitoring at the initial start-up of the TOE. And maintains the TOE in secure conditions with FPT_FLS.1 Failure with preservation of secure state. And FPT_RCV.4 Function recovery provide for secure operation mode in case of Encryption failure, Pseudorandom number failure</td></tr>
<tr><td colspan="3">This TOE assumes the following threat.</td></tr>
<tr><td>TOE Threats</td><td>T.Malfunction</td><td>Attackers may destroy the results of processing performed by the TOE. Attackers may deactivate the security functions of the TOE.</td></tr>
<tr><td colspan="3">Following security objectives is used to cope with this threat.</td></tr>
<tr><td>TOE Objectives</td><td>O.Self_Test</td><td>TOE shall provide protection to TSF and the memories from failures and deactivation.</td></tr>
<tr><td colspan="3">The following security functional requirements meet this objective.</td></tr>
<tr><td rowspan="4">SFR</td><td>FPT_TST.1</td><td>This performs self-verification to following items at the time of initial start-up of TOE:
- Pseudo random number generation function,
- Encryption / decryption function,
- ROM,
- EEPROM.</td></tr>
<tr><td>FPT_SDI.1</td><td>This performs checksum and party checking at the time of self-verification of TOE.</td></tr>
<tr><td>FPT_FLS.1</td><td>This maintains the secure status of TOE when Encryption failure, Pseudorandom number failure occurred.</td></tr>
<tr><td>FPT_RCV.4</td><td>Automated recovery of TOE when Encryption failure, Pseudorandom number failure occurred.</td></tr>
</table>

Table 15. (removed)

Table 16. Adequacy of the security objectives and SFR - 4

<table>
<tr><td colspan="3">The relationship between the security objectives and the security functional requirements is as shown in the table below:</td></tr>
<tr><td colspan="3">O.Leak_Protection Protection against Inherent Information Leakage intends implementation of providing protection to the confidentiality of leaked data stored to EEPROM.
If the user data transferred through the TOE leaked as variation in power consumption during encryption and computation processes, FDP_ITT.1 Basic internal transfer protection makes the analysis of the leaked information difficult based upon the information flow control policy specified by FDP_IFC.1 Subset information flow control and FDP_IFF.1 Simple security attributes. In a manner similar to above, FPT_ITT.1 Basic internal TSF data transfer protection makes the analysis of the leaked TSF data difficult.</td></tr>
<tr><td colspan="3">This TOE assumes the following threat.</td></tr>
<tr><td>TOE Threats</td><td>T.Leak_Inherent</td><td>Attackers may disclose the data internal to EEPROM (i.e., cryptographic keys).</td></tr>
<tr><td colspan="3">Following security objectives is used to cope with this threat.</td></tr>
<tr><td>TOE Objectives</td><td>O.Leak_Protection</td><td>TOE shall provide protection to the processing results and the data from leakage of information.</td></tr>
<tr><td colspan="3">The following security functional requirements meet this objective.</td></tr>
<tr><td rowspan="4">SFR</td><td>FDP_IFC.1</td><td>This performs the information flow control policy to the secret data.</td></tr>
<tr><td>FDP_IFF.1</td><td>This performs the information flow control policy to the internal transmitting data.</td></tr>
<tr><td>FDP_ITT.1</td><td>This prevents exposure of user data at the time of user data transfer.</td></tr>
<tr><td>FPT_ITT.1</td><td>This prevents exposure of TSF data at the time of TSF data transfer.</td></tr>
</table>

Table 17. Adequacy of the security objectives and SFR - 5

<table>
<tr><td colspan="3">The relationship between the security objectives and the security functional requirements is as shown in the table below:</td></tr>
<tr><td colspan="3">O.Phys_Protection Physical Protection intends implementation of providing protection to the integrity and the confidentiality of TOE's IC-chip and the data on Data Bus. This security policy maintains the integrity and the confidentiality of data by automatic detection by FPT_PHP.3 Resistance to physical attack when physical attack was launched.</td></tr>
<tr><td colspan="3">This TOE assumes the following threat.</td></tr>
<tr><td rowspan="3">TOE Threats</td><td>T.Phys_Prob</td><td>Attackers may disclose the data in the IC chip or in the TOE.</td></tr>
<tr><td>T.Phys_Manip</td><td>Attackers may disclose the data in the IC chip or in the TOE.</td></tr>
<tr><td>T.Clon</td><td>Attackers may create clones of the TOE itself, of the security functions, or of a part of the security functions.</td></tr>
<tr><td colspan="3">The following security objectives are used to cope with this threat.</td></tr>
<tr><td>TOE Objectives</td><td>O.Phys_Protection</td><td>TOE shall provide protection to the data in IC-Chip and on Data Bus of TOE from physical analysis and altering.</td></tr>
<tr><td colspan="3">The following security functional requirements meet this objective.</td></tr>
<tr><td>SFR</td><td>FPT_PHP.3</td><td>If Physical Probing and Manipulation occurred, TOE itself automatically detects the occurrence of such probing and executes a reset to TOE itself to maintain the secure status of TOE.</td></tr>
</table>

(removed)

Table 18. Adequacy of the security objectives and SFR - 7

<table>
<tr><td colspan="3">The relationship between the security objectives and the security functional requirements is as shown in the table below:</td></tr>
<tr><td colspan="3">O.Data_Acc Data Access Control intends implementation of providing protection to the integrity and the confidentiality of data in the TOE. Based upon the security attributes enumerated in FDP_ACF.1 Security attribute based access control, this security policy sets the basic rule with Access Control SFRs described in FDP_ACC.1 Subset access control.
In addition, this security policy performs authentication of the TOE with FIA_UID.1 Timing of identification and FIA_UAU.2 User authentication before any action, and performs management to the security attributes and the roles of the TOE with FMT_MSA.1.A and FMT_MSA.1.B Management of security attributes, FMT_MSA.2 Secure security attributes, FMT_MSA.3Static attribute initialization, FMT_SMR.1 Security roles and FMT_MTD.1 Management of TSF data. This security policy maintains the confidentiality of data by encrypting the communication data with FCS_COP.1 Cryptographic operation. This security policy manage cryptographic key with FCS_CKM.1 Cryptographic key generation and FCS_CKM.4 Cryptographic key destruction.
Unsuccessful authentication is limited by FIA_AFL.1 Authentication failure handling.
FTP_ITC.1 Inter-TSF trusted channel is used for maintaining the integrity of high reliability channel between TSFs.</td></tr>
<tr><td colspan="3">This TOE assumes the following threat.</td></tr>
<tr><td>TOE Threats</td><td>T.Access</td><td>Attackers may disclose or / and manipulate the data in the TOE.</td></tr>
<tr><td colspan="3">The following security objectives are used to cope with this threat.</td></tr>
<tr><td>TOE Objectives</td><td>O.Data_Acc</td><td>TOE shall provide protection to the data internal to TOE from illegal access.</td></tr>
<tr><td colspan="3">The following security functional requirements meet this objective.</td></tr>
<tr><td rowspan="12">SFR</td><td>FMT_SMF.1</td><td>To prevent illegal manipulation of data internal to TOE, IPL mode (in which manipulation to data internal to TOE is possible) is specified to be the security management function.</td></tr>
<tr><td>FMT_SMR.1</td><td>TOE is maintained so that only the authorized users to operate in IPL mode are allowed to operate TSF.</td></tr>
<tr><td>FMT_MTD.1</td><td>Following TSF data are management target data and content of operation in IPL mode:
Modification of IPL authentication key and IPL execution key</td></tr>
<tr><td>FMT_MSA.2</td><td>The key used for mutual authentication has security attribute.</td></tr>
<tr><td>FMT_MSA.3</td><td>Only the personnel who authorized so shall be able to modify the value of key.</td></tr>
<tr><td>FMT_MSA.1.A</td><td>Only the personnel who authorized so shall be able to modify a key.</td></tr>
<tr><td>FMT_MSA.1.B</td><td>Only the personnel who authorized so shall be able to clear IPL Locked state.</td></tr>
<tr><td>FIA_UID.1</td><td>To prevent illegal access to TOE performs IPL authentication (IPL authentication 1 command) on behalf of users.</td></tr>
<tr><td>FIA_UAU.2</td><td>To prevent illegal access to TOE performs IPL authentication on behalf of users.</td></tr>
<tr><td>FCS_CKM.1</td><td>To prevent illegal access to TOE, this SFR performs generation of keys when used Triple DES cipher system.</td></tr>
<tr><td>FCS_COP.1</td><td>Controls encryption / decryption processes of communication data.</td></tr>
</table>

Table19. Adequacy of the security objectives and SFR - 7 (continued)

The following security functional requirements meet this objective.		
	FIA_ALF.1	If the number of successive failures of IPL authentication exceeded the specified number of times, IPL Lock is activated to control so that further trials of IPL authentication are impossible.
	FCS_CKM.4	To prevent illegal access to TOE, this SFR performs destruction of the key generated for protection of communication data.
	FTP_ITC.1	To prevent illegal access to TOE, this SFR provides secure communication channel between TOE and controller.
	FDP_ACC.1	For execution of and manipulation to codes for memories internal to IC, IPL access control policy shall be performed. This is also true for execution of and manipulation to all the related functions.
	FDP_ACF.1	Based upon IPL access control policy, performs execution of and manipulation to IPL mode.

Table 19. Adequacy of the security objectives and SFR - 8

<table>
<tr><td colspan="3">The relationship between the security objectives and the security functional requirements is as shown in the table below:</td></tr>
<tr><td colspan="3">O.Prot_Interface Protection Interface intends implementation of providing protection to the confidentiality of encrypted data passing through the interface with FDP_IFF.1 Simple security attributes based upon the information flow control policy specified by FDP_IFC.1 Subset information flow control. This security policy maintains the confidentiality of data by encrypting the communication data with FCS_COP.1 Cryptographic operation.
And, The user data exchanged between TSF with FDP_UCT.1 Basic data exchange confidentiality.
FTP_ITC.1 Inter-TSF trusted channel is used for maintaining the integrity of high reliability channel between TSFs</td></tr>
<tr><td colspan="3">This TOE assumes the following threat.</td></tr>
<tr><td>TOE Threats</td><td>T.Monitoring_Data</td><td>Attackers may perform the monitoring of transferred data.</td></tr>
<tr><td colspan="3">The following security objectives are used to cope with this threat.</td></tr>
<tr><td>TOE Objectives</td><td>O.Prot_Interface</td><td>The TOE shall provide protection to the data being transferred on the external interface from monitoring.</td></tr>
<tr><td colspan="3">The following security functional requirements meet this objective.</td></tr>
<tr><td rowspan="5">SFR</td><td>FCS_COP.1</td><td>Controls encryption / decryption processes of communication data.</td></tr>
<tr><td>FTP_ITC.1</td><td>Provides the capability for consistent interpretation of transmitted / received data.</td></tr>
<tr><td>FDP_UCT.1</td><td>Performs the External Data Transfer Protection Policy to provide protection to the external data from exposure.</td></tr>
<tr><td>FDP_IFC.1</td><td>This performs the information flow control policy to the secret data.</td></tr>
<tr><td>FDP_IFF.1</td><td>This determines whether to accept or abort the data at the time of data transmission / reception.</td></tr>
</table>

Table 20. Adequacy of the security objectives and SFR - 9

<table>
<tr><td colspan="3">The relationship between the security objectives and the security functional requirements is as shown in the table below:</td></tr>
<tr><td colspan="3">O.InData_Pro TOE Data Protection intends implementation of providing protection to the integrity of data stored to the TOE.
This security policy maintains the integrity of communication data by detecting and aborting the corrupted data passing through the communication routes using FDP_SDI.1 Stored data integrity monitoring and FDP_UIT.1 Data exchange integrity. And maintains the TOE in secure conditions with FPT_FLS.1 Failure with preservation of secure state. And FPT_RCV.4 Function recovery provide for secure operation and automated recovery in case of Power failure.</td></tr>
<tr><td colspan="3">This TOE assumes the following threat.</td></tr>
<tr><td>TOE Threats</td><td>T.Power_Down</td><td>Attackers may destroy the data written to the TOE. This threat includes the destruction of data resulted from unintentional accident.</td></tr>
<tr><td colspan="3">The following security objective is used to cope with this threat.</td></tr>
<tr><td>TOE Objectives</td><td>O.InData_Pro</td><td>TOE shall provide protection to the data internal to TOE from destruction and failure of data writing.</td></tr>
<tr><td colspan="3">The following security functional requirements meet this objective.</td></tr>
<tr><td rowspan="4">SFR</td><td>FDP_SDI.1</td><td>Performs monitoring of memory data.</td></tr>
<tr><td>FPT_FLS.1</td><td>This maintains the secure status of TOE when Power failure occurred.</td></tr>
<tr><td>FPT_RCV.4</td><td>Automated recovery of TOE when Power failure occurred.</td></tr>
<tr><td>FDP_UIT.1</td><td>Performs detection of modified communication data when it is received.</td></tr>
</table>

Adequacy of IT Environment Security objectives and Security Function Requirements

Table 21. Adequacy of the security objectives for IT environment and SFR - 1

The relationship between the security objectives for IT environment and the security functional requirements is as shown in the table below:		
OE.CoSec_Com Controller Secure Communication is provided for the purpose of maintaining secure status of TSF data exchanged and shared between trusted IT products. With them, establishment of reliable channels between the environment and the TOE becomes possible. ***FCS_COP.1 Cryptographic operation*** provides supports required for the encryption operation in accordance with the specified standards and guidance. In addition, ***FCS_CKM.1 Cryptographic key generation***, and ***FCS_CKM.4 Cryptographic key destruction*** provide supports necessary for generation, and destruction of encryption keys. ***FTP_ITC.1 Inter-TSF trusted channel*** is used for maintaining the integrity of high reliability channel between TSFs.		
This TOE assumes the following prerequisite.		
TOE Assumption	A.CoSec_Com	It is assumed that a controller can perform establishment of a secure communication channel.
Following security objectives is used to cope with this prerequisite.		
IT Environment Security objectives	OE.CoSec_Com	IT environment shall provide secure communication channel for the TOE.
The following security functional requirements meet this objective.		
SFR	FCS_COP.1	Performs encryption / decryption processes of communication data.
	FCS_CKM.1	Performs generation of encryption key.
	FCS_CKM.4	Performs disposition of the encryption key.
	FTP_ITC.1	Provides the capability for consistent interpretation of transmitted / received data.

8.2.2. TOE Security Functional Requirements Dependencies

Table 23. Security Functional Requirements Dependencies

SFR	Depends on:	Satisfied by:
FPT_FLS.1	ADV_SPM.1	Included.
FPT_PHP.3	Non	N/A
FDP_IFC.1	FDP_IFF.1	Included
FDP_IFF.1	FDP_IFC.1and FMT_MSA.3	Included
FDP_ITT.1	FDP_ACC .1or FDP_IFC.1	FDP_IFC.1 included
FPT_ITT.1	Non	N/A
FPT_RCV.4	ADV_SPM.1	Included
FDP_SDI.1	Non	N/A
FDP_UCT.1	FTP_ITC.1 or FTP_TRP.1	FTP_ITC.1 included
	FDP_ACC.1 or FDP_IFC.1	Both included
FDP_UIT.1	FDP_ACC.1 or FDP_IFC.1	Both included
	FTP_ITC.1 or FTP_TRP.1	FTP_ITC.1 included
FCS_COP.1	FDP_ITC.1 or FCS_CKM.1	FCS_CKM.1 included
	FCS_CKM.4 and FMT_MSA.2	Both included
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	FCS_COP.1 included
FCS_CKM.4	FDP_ITC.1 or FCS_CKM.1	FCS_CKM.1 included
FPT_TST.1	FPT_AMT.1	See “unsatisfied dependencies for FPT_AMT.1” on page 63
FTP_ITC.1	Non	N/A
FIA_UID.1	Non	N/A
FIA_UAU.2	FIA_UID.1	Included
FIA_AFL.1	FIA_UAU.1	Included (as FIA_UAU.2)
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_MTD.1	FMT_SMR.1	Included.
	FMT_SMF.1	Included.
FMT_MSA.1.A	FDP_ACC .1or FDP_IFC.1	Both included
	FMT_SMR.1	Included
	FMT_SMF.1	Included
FMT_MSA.1.B	FDP_ACC .1or FDP_IFC.1	Both included
	FMT_SMR.1	Included
	FMT_SMF.1	Included
FMT_MSA.2	ADV_SPM.1	Included
	FDP_ACC .1or FDP_IFC.1	Both included
	FMT_MSA.1.A,FMT_MSA.1.B and FMT_SMR.1	Both Included
FMT_MSA.3	FMT_MSA.1.A,FMT_MSA.1.B and FMT_SMR.1	Both included

FMT_SMF.1	Non	N/A

Unsatisfied dependencies for FPT_AMT.1

The TOE is already the lowest platform. There is no lower “underlying abstract machine” used by the TOE which can be tested. There is no need to perform testing according to FPT_AMT.1 and the dependency in the requirement FPT_TST.1 is therefore considered to be satisfied.

8.2.3. TOE Security Assurance Requirements Rationale

The assurance level for this TOE is EAL4.

With the embedment of this TOE to the carrier, the TOE is the product installed with the security functions possible to be used for operations in various commercial purposes.
Thus, the evaluation assurance level of EAL4, i.e. a reasonably high level in commercial area, is regarded as appropriate for this TOE, as it is providing evaluation of sufficient design detail (low-level design and implementation subset) and an independent vulnerability analysis.

8.2.4. TOE Security Assurance Requirements Dependencies

Table 24. Security Assurance Requirements Dependencies

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 and ADV_RCR.1	Both included (as ADV_FSP.2).
ADV_IMP.1	ADV_LLD.1	Included
	ADV_RCR.1	Included
	ALC_TAT.1	Included
ADV_LLD.1	ADV_HLD.2	Included
	ADV_RCR.1	Included
ADV_RCR.1	Non	N/A
ADV_SPM.1	ADV_FSP.1	Included as ADV_FSP.2.
AGD_ADM.1	ADV_FSP.1	Included as ADV_FSP.2.
AGD_USR.1	ADV_FSP.1	Included as ADV_FSP.2.
ALC_DVS.1	Non	N/A
ALC_LCD.1	Non	N/A
ALC_TAT.1	ADV_IMP.1	Included.
ATE_COV.2	ADV_FSP.1	Included as ADV_FSP.2.
	ATE_FUN.1	Included
ATE_DPT.1	ADV_HLD.1	Included as ADV_HLD.2.
	ATE_FUN.1	Included
ATE_FUN.1	Non	N/A
ATE_IND.2	ADV_FSP.1	Included as ADV_FSP.2.
	AGD_ADM.1 and AGD_USR.1	Both included
	ATE_FUN.1	Included
AVA_MSU.2	ADO_IGS.1	Included
	ADV_FSP.1	Included as ADV_FSP.2.
	AGD_ADM.1 and AGD_USR.1	Both 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
	ADV_LLD.1	Included
	AGD_ADM.1 and AGD_USR.1	Both included

8.2.5. Claims on TOE Strength Of Function Rationale

As stated in the “TOE Environment” this TOE is a product intended for use where a basic security level is sufficient. This is consistent with the choice of SOF-basic.
Furthermore SOF-basic is consistent with the choice of AVA_VLA.2, because both of them meanrestance against attackers possessing a low attack potential.

8.2.6. Mutual Support between Security Requirements

As shown in "TOE Security Functional Requirements Rationale (page 48 of this document) and in "TOE Security Assurance Requirements Rationale" (page 61 of this document), the selection of the security requirements can be said as reasonable.

Selection of SFRs (Security Functional Requirements) and SARs (Security Assurance Requirements) is performed based upon various assumptions regarding the threats to TOE and Security Environment as well as the security target.

SARs (Security Assurance Requirements) are appropriate for the assurance level of EAL4. EAL4 provides the security in the commercial level. Claims of SOF (Strength Of Function), in addition, are appropriate for the assurance level of EAL4.

8.3. TOE Summary Specification Rationale

As demonstrated in "TOE Security Functions" section (page 39), TOE's security functions satisfy the requirements of all the security functions defined in "TOE Security Requirements" section (page 29). The justification of the mapping between security functional requirements and the 'security enforcing functions' is given in the table below and following descriptions.

SFR	SF.1	SF.2	SF.3	SF.4	SF.5	SF.6	SF.7	SF.8
FPT_FLS.1	✓					✓	✓	✓
FPT_PHP.3	✓		✓					
FDP_IFC.1		✓				✓		
FDP_IFF.1		✓				✓		
FDP_ITT.1		✓						
FPT_ITT.1		✓						
FPT_RCV.4	✓					✓	✓	✓
FDP_SDI.1						✓	✓	✓
FDP_UCT.1						✓		
FDP_UIT.1						✓		
FCS_COP.1				✓	✓	✓		
FCS_CKM.1				✓	✓			
FCS_CKM.4					✓			
FPT_TST.1							✓	
FTP_ITC.1					✓	✓		
FIA_UID.1					✓			
FIA_UAU.2					✓			
FIA_AFL.1					✓			
FDP_ACC.1					✓			
FDP_ACF.1					✓			
FMT_SMR.1					✓			
FMT_MTD.1					✓			
FMT_MSA.1.A					✓			
FMT_MSA.1.B					✓			
FMT_MSA.2					✓			
FMT_MSA.3					✓			
FMT_SMF.1					✓			

FPT_FLS.1 requires the TOE shall preserve a secure state even in environmental stress and/or illegal operation. This requirement is satisfied by illegal condition detection function of SF.1, checking parity and check sum of communication data by SF6, SF7 (Self Test), and protection of internal data by SF.8.

FPT_PHP.3 requires TOE to be resistant to physical attack. This requirement is satisfied by illegal condition detection function of SF.1 and “Tamper Resistant Layout” and “Test Mode Protecting Functions” of SF.3.

FDP_IFC.1, FDP_IFF.1, FDP_ITT.1 and FPT_ITT.1 require TOE to enforce the Data Processing Policy to protect integrity and confidentiality of external and internal communication data. SF6: protection of data passing through the interface protects external communication data and SF2: protection for information leakage prevents leakage from internal communication data. Therefore this requirement is satisfied.

FPT_RCV.4 requires TOE to recover to a consistent and secure state from failure. This requirement is satisfied by SF.1, SF.6, SF.7 and SF.8. SF.1 resets TOE when it detects abnormal operating conditions. SF.6 detects and rejects communication packet if it fails integrity check. SF.7 provides self test function and enter secure state if it detects failure. SF.8 provides protection of internal data being written to EEPROM. Therefore this SFR is satisfied.

FDP_SDI.1 requires stored data integrity monitoring. This requirement is satisfied by SF.6, SF.7, and SF.8. Details of these SFs are described in FPT_RCV.4 paragraph.

FDP_UCT.1 and FDP_UIT.1 require TOE to enforce the Data Processing Policy to data exchange for protecting confidentiality and integrity. This policy is satisfied by SF.6: Protection of data passing through the interface.

FCS_COP.1 require TOE to perform encryption and decryption with a specified cryptographic algorithm. SF.5 and SF.6 perform encryption and decryption for mutual authentication and communication data encryption using Triple DES provided by SF.4. Therefore SF.4, SF.5 and SF.6 satisfy this requirement.

FCS_CKM.1, and FCS_CKM.4 require cryptographic key generation and destruction in secure manner. These requirements are satisfied in mutual authentication process of SF.5. Pseudo random number generator of SF.4 also satisfies FCS_CKM.1.FPT_TST.1 requires performing self-tests. SF.7: Self Test obviously satisfies this requirement.

FTP_ITC.1 requires TOE to provide a secure communication channel between itself and a remote trusted IT product and to permit remote trusted IT product to initiate communication for IPL Authentication. SF.6: Protection of data passing through the interface provides secure communication channel between TOE and controller (a remote trusted IT product). The communication is initiated by SF.5: mutual authentication. Therefore this requirement is satisfied.

FIA_UID.1, FIA_UAU.2 require timing of identification and user authentication before any action. Mutual authentication of SF.5 satisfies these requirements.
FIA_AFL.1.2 requires authentication failure handling. IPL lock function of SF.5 satisfies this requirement.
FDP_ACC.1 FDP_ACF.1, FMT_MSA.1.A, FMT_MSA.1.B, FMT_MSA.2, FMT_MSA.3 and FMT_MTD.1 require TOE to enforce Access Control Policy for access control and management of security attributes and TSF data. SF.5 mutual authentication satisfy this policy.
FMT_SMR.1 is also satisfied by SF.5 because security roles are maintained by mutual authentication.
As a result, FMT_SMF.1 specification of above management functions is satisfied by SF.5.

TOE's assurance measures detailed in "Assurance Measures" section (page 43) demonstrates that reference to "TOE Security Assurance Requirements" section (page 36) is done by such assurance measures.

The selection of SFRs (Security Functional Requirements) and SARs (Security Assurance Requirements) is performed based upon the security targets for the TOE and the security environment as well as the threats against them.
Thus, this ST (Security Target) provides the evidence for the security functions' capability to cope with all the threats launched against the TOE in collaboration with the assurance measures.

This TOE is the product intending the operation for commercial use as described in "Claims on TOE Strength of Function Rationale " (page 63 of this document). For the operation for commercial use, the security under the operating environment shall be maintained and assured by the security functions installed to the TOE.

This TOE is the product intending operation for commercial use, and because of this, the TOE is required to comply with SOF (Strength Of Function) - basic.

8.4. PP Claims Rationale

None.