FeliCa RC-S860 Contactless Smart Card Security Target (Public Version)

Version: 1.0
Control Number: 860-STP-E01-00
Issue Date: 20 August 2002

Broadband Network Center, FeliCa Division

Contents

List of tables

References

CC

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

CC1

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

CC2

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

CC3

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

FIPS

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

DES

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

DES Modes of Operation

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

DES Implementation Guidelines

GUIDELINES FOR IMPLEMENTING AND USING THE NBS DATA ENCRYPTION STANDARD
National Bureau of Standards
Federal Information Processing Standards Publication FIPS PUBS 74
1 April 1981
http://www.itl.nist.gov/fipspubs/fip74.htm

CHAPTER 1

Introduction

This document is the security target for the CC evaluation of the Sony Contactless Smart Card RC-S860 FeliCa product.

The role of the security target within the development and evaluation process is described in the ISO Standard 15408, the Common Criteria for Information Technology Security Evaluation [CC].

The smart card architecture usually contains the following logically and physically distinct components:

- The smart card;
- The smart card reader/writer device;
- The terminal device which executes service provider's applications.

This ST document is concerned with the smart card only.

ST and TOE identification

This section provides information needed to identify and control this ST and its TOE, the Sony Contactless Smart Card RC-S860 FeliCa product.

ST Title:	FeliCa RC-S860 Contactless Smart Card Security Target (Public Version)
TOE Identification:	Sony FeliCa RC-S860 Contactless Smart Card IC chip specification: SONY CXD9559 ROM: version 6 FeliCa OS: version 3.1
CC Identification:	ISO 15408 standard, Common Criteria for Information Technology Security Evaluation [CC]
ST Preparation:	Sony Corporation, Broadband Network Center, i-Card System Solution Division
ST Evaluation:	Logica UK, Ltd.

ST overview

The RC-S860 Contactless Smart Card is a thin, compact card conforming to ISO/IEC7810ID-1 dimensions. The card surface is made of PET material that has little environmental impact when incinerated.

An IC chip and antenna are built into the card. The card itself contains no battery but operates from low-power electromagnetic signals received from the reader/writer. The card thus is exceptionally durable. The card chip contains an 8-bit RISC CPU specially developed by Sony combining built-in EEPROM, RAM, ROM, encryption processing and RF functions in a single chip.

The contactless smart card, reader/writer, communication of important data between the card and the reader/writer, as well as communication between a terminal and the reader/writer are all protected by an encryption system that prevents eavesdropping and fraudulent use. Even with such encryption, processing speeds meet the strict needs of transit fare collection applications.

Built-in safeguards insure that, even if a transaction is interrupted while new data is being written to a card, the original data remains intact.

Since each card can facilitate unique access rights set by several different service providers, a single card can be used for a variety of applications while assuring individual security. Separate, unique keys providing individual access rights to different memory areas on the card control both dedicated and common files. For examples of practical functions, the tolls can be debited with a single card when a passenger changes between the lines of different transport companies. The single card acts as an “electronic wallet” that can be used for payments to the different companies.

CC Conformance

This Security Target conforms to part 2 and part 3 of the Common Criteria for Information Technology Security Evaluation [CC2][CC3]. The conformance is claimed to EAL 4.

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

Scope

The structure of this document is as defined by [CC] Part 1 Annex C.

- Chapter 2, “TOE Description,” on page 19 is the TOE description.
- Chapter 3, “TOE Security Environment,” on page 25 provides the statement of TOE security environment.
- Chapter 4, “Security Objectives,” on page 35 provides the statement of security objectives.
- Chapter 5, “IT Security Requirements,” on page 43 provides the statement of IT security requirements.
- Chapter 6, “TOE Summary Specification,” on page 55 provides the TOE summary specification.
- Chapter 7, “Removed,” on page 67 provides the security objectives rationale.
- Chapter 8, “Removed,” on page 75 provides the security requirements rationale.
- Chapter 9, “Removed,” on page 87 provides the TOE summary specification rationale.

Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Application

Intended final use for the smart card. This may include (but is not limited to) such activities as payment, telephony, identification, secure information storage, or loyalty.

Activation

A process that gives a card the required operational capability for the cardholder.

Bond-out chips

Raw ICs which have been mounted on a small board. The IC is glued by ACF to the carrier. Bond-out chips are sometimes referred to as a module.

Card block

The IC function related to limiting temporarily the functions allowed to be performed. Card blocking is temporary and can be reset by the proper authorities.

Card disablement

The IC function related to terminating all operations other than possibly some limited audit functions. Card disablement is permanent.

Card embedder

A manufacturer who assembles a card and integrated circuit.

Card holder

A person to whom a card has been legitimately issued (a user).

Card issuer

An institution which issues cards to card holders.

Card reader/writer

A machine capable of reading and/or writing to a card.

Card Operating System (COS)

Operating system developer specific code, written in the microprocessors native or machine code.

Carrier

The holder in which an operational integrated circuit is placed. This is typically the thin, credit card sized piece of plastic that is known as a smart card.

Die

The semiconductor IC without any packaging or connections.

Differential power analysis (DPA)

A technique combining physical measurements of such things as power consumption with statistical signal processing techniques to identify IC operating details. DPA can, in some instances, provide information leading to recovery of internal operational parameters, keys, etc.

Electrically Erasable Programmable Read Only Memory (EEPROM)

A non-volatile memory technology where data can be electrically erased and rewritten.

Failure analysis

The compilation of techniques used by semiconductor development and testing labs to identify the operating problems in newly designed or modified integrated circuits. Such techniques include not only observation (to determine what is not functioning properly) but also modification of IC internal structure (to determine fixes).

First use indication

The IC function related to setting a specific audit bit indicating that the smart card is now in the issued, operational state and can be used for its intended function.

Integrated Circuit (IC)

Electronic component(s) contained on a single chip and designed to perform processing and/or memory functions.

Integrated Circuit Card (ICC)

A card which consists of a carrier with an IC and an antennae inserted into it.

Initialization

The process of writing specific information into Non-Volatile Memory during IC manufacturing and testing as well as executing security protection procedures by the IC manufacturer.

Life cycle identifiers

The specific identification of chip fabricator identifier, operating software identifier, chip module identifier, chip embedder identifier, initializer identifier, initialization equipment identifier, personalizer identifier, and personalization equipment identifier.

Non-volatile memory

A semiconductor memory that retains its content when power is removed. (i. e. ROM, EEPROM, FLASH).

Operational keys

The cryptographic keys loaded into the assembled smart card product for use by the cardholder during normal operation.

Operating Software (OS)

That software resident on the TOE which is required for TOE operation up to supporting secure load. This may, or may not, be a full operating system in the conventional sense.

Personalization

The process of writing specific information into the non-volatile memory in preparing the IC for issuance to users.

PET

Poly Ethylene Terephthalate

Photomask

A mask which is used during chip manufacturing to protect selected parts of a silicon wafer from a light source while allowing other parts of the surface of the wafer to be exposed. The purpose is to expose the photoresist on the surface so that subsequent etching processes can generate the desired substrate structure.

The photomask is the means by which the chips circuits, and therefore its functionality, are placed on the chip.

Pilot

A test application in which a system is deployed to a limited geographic area or card holder population so that data on acceptability and operational capability can be gathered prior to full-scale introduction.

Platform

A term representing an operational smart card system.

Post-issuance

The time period during which the smart card is in the hands of the card holder. In some smart cards, additional functionality can be loaded into the smart card post-issuance.

Production keys

The cryptographic keys loaded into the IC for security during production.

Random Access Memory (RAM)

A volatile, randomly accessible memory (used in the IC) that requires power to maintain data.

Read Only Memory (ROM)

A non-volatile memory (used in the IC) that requires no power to maintain. ROM data is often contained in one of the numerous masks used during manufacture.

Reverse engineering

The compilation of techniques used by semiconductor development and testing labs to generate design documentation and specifications for an unknown integrated circuit. Reverse engineering, in its most complete sense, would allow the identification of a complete fabrication package given only an unidentified integrated circuit as a starting point.

RF

Radio Frequency

RISC

Reduced Instruction Set Computer

Simple Power Analysis (SPA)

A technique in which physical measurements of power consumption over time are used to identify IC operating details. SPA can, in some instances, provide information leading to recovery of internal operational parameters, keys, etc.

Smart card

A shaped piece of plastic or other carrier with a small computer chip embedded into it. The terms “IC Card” and “Smart Card” are used in this document interchangeably.

Terminal

The device used in conjunction with the card reader/writer at the point of transaction.

Transport keys

The cryptographic keys loaded into the IC for security during transport of ICs, modules, and assembled products prior to issuance.

CHAPTER 2

TOE Description

This part of the ST describes the TOE as an aid to the understanding of its security requirements, and addresses the product or system type. The scope and boundaries of the TOE are described in general terms both in a physical way (hardware and software components and modules) and a logical way (IT and security features offered by the TOE).

TOE Introduction

A smart card or integrated circuit card (ICC) is a computer chip embedded into a carrier. The chip is a semiconductor (silicon) integrated circuit (IC) fabricated in a complex microelectronic process, which involves repeatedly masking and doping the surface of a silicon substrate to form transistors, followed by patterning metal connections, and applying a protective overcoat. This process eventually yields a design comprising several hundred thousand transistors. The design consists of a central processing unit, a cryptographic co-processor, input and output lines, and volatile and non-volatile memory.

The chip is also designed to be secure. In order to be secure, it makes appropriate use both of specific design features that are dedicated to security, e.g. environmental sensors, and also of technological properties of the materials and processes used.

A part of the manufacturing process is the inclusion of operating software (OS). This is developer-specific code, usually written in the microprocessors native or machine code. Operating software is usually contained in one of the numerous masks used during manufacture, referred to in this document as the Read-Only Memory (ROM).

The IC itself is packaged. The chip together with the antennae is encapsulated in a board made of protective material (PET). The board conforms to the ISO/ IEC7810ID-1 standard credit card size. The resulting PET board can be applied with printing, magnetic stripe, security features such as holograms which are outside the scope of the current evaluation.

The communication channel of the RC-S860 Contactless Smart Card is implemented using electromagnetic wave coupling on a single frequency. This communication channel is used for both communication between the card and the reader / writer and the power supply of the card.

The RC-S860 has a built-in high-speed, power-efficient RISC microprocessor and dedicated hardware for cryptographic operations like encryption and random number generation. The dedicated hardware allows for the encryption of wireless communication path with reader/writer and processing of the mutual authentication at a high speed as required by some applications.

The RC-S860 Contactless Smart Card IC contains the software pre loaded during manufacturing. The software cannot be altered at a later stage in the life cycle of the card. The application download is not supported by this IC.

Intended Use

The TOE is intended to be suitable for use in financial services systems, but is not limited to that application. The applications can be developed by the card issuers independently and multiple applications can use the same card.

The card supports a wide range of applications. The simplest application would be a value check for a stored value application. In this function, the card reader/writer performs a simple query on the card returning the amount of value remaining on the card. Such application does not support or require a write capability and no other function is possible.

More complex applications require a write capability. For example, an application may read some stored value from the card, perform some operation, and write it back to the card. In an electronic purse application, the reader/writer would issue a command that makes the card subtract a given value from the amount stored for some value.

TOE Environment Introduction

The environment of the TOE is represented by the carrier in which the chip is embedded and the environment of the resulting smart card. The carrier is made of PET material and helps to prevent the chip from the damage during normal use.

Smart card environments are highly variable and to some extent application dependent. In general, a smart card is assumed to be in the uncontrolled possession of the cardholder. The card must therefore protect its assets against unauthorized alteration that may be accomplished with standard IT equipment or with laboratory equipment used without any supervision.

Cryptographic functions are necessary to support some applications. These include storing the keys; providing cryptographic operations such as encryption and decryption; or processing secure card data for transmission over the RF link between the card and the reader/writer. In order to maintain the security of these operations, the card is equipped with security modules providing protection to this information.

Summary of IT and Security Features

The RC-S860 Contactless Smart Card provides secure storage for user data and associates security attributes with the stored data. These attributes are used to determine whether the access to particular block of data should be granted or not.

The memory of the card is partitioned into files which are organized into a hierarchical file structure. Each file may be accessed independently of the others providing flexible support for multiple applications. The card supports simultaneous access to a maximum of 8 files for writing or 12 files for reading in a single operation.

The software allows a user to access the files of three basic service types:

- Random Access File, where the files can be accessed freely by specifying the desired block number;
- Cyclic Access File, where the access is controlled by the wrap-around type of block numbers and all blocks are arranged in chronological order;
- Purse Access File, where the access is limited to special actions like subtracting from the specified data, adding a value within the range subtracted before etc.

Each type of service is also attributed for access in secure mode, insecure mode, read-only mode, or read/write mode.

Files may be protected by an access key for secure storage of the data while other files that need not be protected may be read and written without cryptographic support. Various access right attributes can be set to a file providing flexible support for such applications that require, e.g., shared file access.

A service provider may allocate service files in the area that was granted to it. A service provider may also reallocate space inside it's area to other service providers.

An occasional power loss while writing data into non-volatile memory is unavoidable in a contactless smart card that does not have an internal power supply and operates on the power supplied by the reader/writer via electromagnetic waves. The RC-S860 preserves the data in the non-volatile memory at the state before the interrupted writing transaction took place and guarantees the consistency of the data. The system is guaranteed to automatically return to the state before the power failure.

The RC-S860 Contactless Smart Card supports a special separation function that allows to divide the memory of the card into 2 areas. The resulting areas are used completely independently from each other just like if two cards were used. This allows for a complete isolation of information stored by different providers on different 'virtual cards'.

Evaluated Configurations

For the purposes of this evaluation the physical boundary of the system is defined to be the physical boundary of the IC embedded in the carrier. The carrier itself is

considered to be the TOE environment and is not included in the evaluation. Logically, the target of evaluation (TOE) for this security target is an operational smart card platform, consisting of the integrated circuit and operating software, including the mechanisms that allow communication with the outside world. The TOE consists of sufficient hardware and software elements to be capable of establishing a secure channel to a trusted source for application execution or for other potentially privileged commands.

The evaluated configuration constitutes the RC-S860 Contactless Smart Card as it is delivered by Sony to the card issuer. In this configuration the card does not contain any applications. The assurance of the security of the applications is a responsibility of the card issuer. The card only provides for the confidentiality and integrity of the data stored by an application. The card in the evaluated configuration is configured.

CHAPTER 3

TOE Security Environment

The statement of TOE security environment describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed.

To this end, the statement of TOE security environment identifies and lists the assumptions made on the environment and the intended method of use of the TOE, defines the threats that the TOE is designed to counter, and the organizational security policies with which the TOE is designed to comply.

Assets

The primary asset of concern for this Security Target is the user data representing the information to be protected. In the context of this TOE, user data may be defined as the ultimate end user (card holder) data or as application data that was loaded to the TOE by the card issuer. The actual final user of the data is not visible for the TOE operations.

Certain data is required to support the secure operations regarding the above defined user data. This TSF data includes security attributes, authentication data,

access control attributes, and the various cryptographic keys which are used in the security processes of the TOE.

The use characteristics of smart cards require them to be in the uncontrolled possession of the users for prolonged periods of time. This can be considered a hostile environment as discussed in “TOE Environment Introduction” on page 21. It is therefore necessary to consider the protection of those characteristics of the TOE and its design that support the preservation of security for the primary assets. These secondary assets of concern include:

- the IC design and specifications;
- the software design and specifications, implementation, and related documentation;
- the IC and software development tools and technology.

All assets are to be protected in terms of confidentiality and integrity.

Environmental and Method of Use Assumptions

This section describes the assumptions about the environment in which the TOE is to be used and its intended method of use. Each assumption is stated in bold type font and is followed by an application note, in normal font, which supplies additional information and interpretation.

A.Carrier Tamper detecting carrier

It is assumed that the carrier of the TOE is produced in such a way as to permit tamper-detection.

Removal, modification, and re-insertion of that TOE into a carrier could be used to pass such a combination as an original. This might then be used to access the assets to be protected. We assume that the carrier of the TOE is produced using special techniques that allow detection of tampering with the carrier, especially an indication of chip removal and re-insertion.

A.Sec_Com Card Reader / Writer Secure

A Card Reader / Writer to which the TOE establishes a secure link is assumed to be secure.

The Reader/Writer may have the capability to establish a secure communication channel with the TOE. This may be accomplished through shared private keys, public/private key pairs, and/or generation of session keys derived from other stored or generated keys. It is assumed that when such a secure link is established, the TOE may consider the Reader/Writer to be adequately secure for trusted communications. The Reader/Writer is considered to be beyond the scope of this Security Target.

A.Data_Store Off-TOE Data Storage

Management of TOE data off of the TOE is assumed to be performed in a secure manner.

Significant information regarding TOE profile, personalization, ownership may be held by issuers or service providers in data bases 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.

A.Key_Supp Cryptographic Key Support

All imported cryptographic keys are assumed to be supported off-card in a secure manner.

A variety of keys may be imported for use by, and in conjunction with, the TOE. These are shared secret keys and synthetic combined keys. These keys will be supplied from the various bodies controlling the operation of the system in which the TOE is functioning. It is assumed that the generation, distribution, maintenance, and destruction of these keys is adequately secure.

A.Power Power Supply

Power supply comes from the Reader/Writer. This is not considered a reliable source.

The TOE is internally unpowered, so support must be delivered to the card from the card Reader/Writer. The power can be interrupted or reset in the normal course of business. The Reader/Writer is independent from the TOE and may belong to a different entity that can be considered in some way hostile. Power may deviate from the design level and may be supplied intermittently.

A.Priv Abuse by Privileged Users

It is assumed that administrators and other privileged users are trustworthy and competent individuals.

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

Assumed Threats

The TOE will be required to counter threats categorized below. Each threat is stated in bold type font and is followed by an application note, in normal font, which supplies additional information and interpretation.

T.P_Probe Physical Probing of the IC

An attacker may perform physical probing of the TOE to reveal design information and operational contents.

Such probing is done using mechanical or electrical functions but is referred to here as physical since it requires direct contact with the chip internals. Physical probing may entail reading data from the chip through techniques commonly employed in IC failure analysis and IC reverse engineering efforts. The goal of the attacker is to identify such design details as hardware security mechanisms, access control mechanisms, authentication systems, data protection systems, memory partitioning, or cryptographic programs. Determination of software design, initialization data, personalization data, passwords, or cryptographic keys may also be a goal.

T.P_Modify Physical Modification of the IC

An attacker may physically modify the TOE in order to reveal design or security related information.

This modification may be achieved through techniques commonly employed in IC failure analysis and IC reverse engineering efforts. The goal is to identify such design details as hardware security mechanisms, access control mechanisms, authentication systems, data protection systems, memory partitioning, or cryptographic programs. Determination of software design, including initialization data, personalization data, passwords, or cryptographic keys may also be a goal. This threat is distinguished from *T.P_Probe Physical Probing of the IC* by the actual modification of the IC rather than only observation.

T.Power Power Supply Failure Data Protection

Power supply comes from the Reader/Writer. Power failure may cause data corruption.

The TOE is internally unpowered, so the power is delivered to the card from the card Reader/Writer. The power can be interrupted or reset in the normal course of business. The power failure during a transaction may cause corruption of data stored in the TOE memory.

T.E_Manip Electrical Manipulation of the IC

An attacker may utilize electrical probing and manipulating of the TOE to modify security critical data so that the TOE can be used fraudulently.

This modification may include manipulation of the IC circuits through techniques commonly used in IC failure analysis and IC reverse engineering efforts. The goal is to modify the chip in such a way as to defeat the security of the TOE and to be able to use the TOE for fraudulent purposes. This threat is distinguished from T.P_Probe and T.P_Modify by the intent to utilize a modified TOE rather than to derive information from the TOE.

T.Forced_Rst Forced Reset

An attacker may force the TOE into a non-secure state through inappropriate termination of selected operations.

Attempts to generate a non-secure state in the TOE may be made through premature termination of transactions or communications between the TOE and the card reader/writer, by insertion of interrupts, or by withdrawal of power supply.

T.Logic_Atk Logical Attack

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

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

T.Reuse Replay Attack

An unauthorized user may penetrate the TOE through reuse of previously valid authentication data.

Attempts to replay a completed (or partially completed) operation may be used in an attempt to bypass security mechanisms or to expose security-related information.

T.Access Invalid Access

A user or an attacker of the TOE may access information or resources without having permission from the person who owns or is responsible for the information or resources.

Each authorized role has certain specified privileges which allow access only to selected portions of the TOE and its contained information. Access beyond those specified privileges could result in exposure of secure information.

T.First_Use Fraud on First Use

An attacker may gain access to TOE information by unauthorized use of a new, previously unissued TOE.

The process of issuance involves setup of the TOE and/or loading security-related information to the TOE. Attempts to use an unissued TOE without such mandated approval could result in fraudulent use.

T.LC_Ftn Use of Unallowed Life Cycle Functions

An attacker may exploit interactions between life-cycle functions to expose sensitive TOE or user data.

Interactions are characterized by execution of commands that are not required or allowed in the specific phase of operation being executed. Examples are use of test, debug, or native COS functions that are unnecessary or that could compromise security.

T.Crypt_Atk Cryptographic Attack

An attacker may defeat security functions through a cryptographic attack against the algorithm or through a brute-force attack.

This attack concentrates on either encode/decode functions or random number generators.

T.I_Leak Information Leakage

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

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

T.Env_Strs Environmental Stress

An attacker may exploit failures in the TOE induced by environmental stress.

Exposure of the IC to conditions outside its specified operating range may result in malfunction or failure of security critical components, allowing manipulation of programs or data. These conditions could either be extremes (high or low) in normal parameters such as temperature, voltage, or clock frequency, or could be abnormal conditions such as external energy fields. The goal may be to generate an immediate failure leading to unauthorized exposure of secure information, or simulation of premature aging, thereby generating an end of life failure.

T.Clon Cloning

An attacker may clone part or all of a functional TOE to develop further attacks.

The information necessary to successfully clone part or all of a TOE may derive from detailed inspection of the TOE itself or from illicit appropriation of design information.

T.Delivery Attacks during delivery

The TOE may be intercepted and/or modified by an attacker during delivery.

An attacker may intercept the software and/or hardware that comprise the TOE during delivery. The attacker may be able to uncover information pertaining to the design of the TOE and security information contained in the delivered parts. The attacker also may be able to induce changes into the TOE security mechanisms that can be used later to mount an attack.

Organizational Security Policies

The TOE must comply with the organizational security policies stated below. Each policy is stated in bold type font and is followed by an application note, in normal font, which supplies additional information and interpretation.

P.Crypt_Std Cryptographic Standards

Cryptographic entities, data authentication, and approval functions must be in accordance with ISO and associated industry or organizational standards.

Various cryptographic operations such as DES, triple DES, and RSA are well defined. These, or others of similar maturity and definition, should be used for all cryptographic operations in the TOE.

P.Data_Acc Data Access

Except for a well-defined set of allowed operations, the right to access specific data and data objects is determined on the basis of: the owner of the object, the identity of the subject attempting the access, and the implicit or explicit access rights to the object granted to the subject by the object owner. Once established, conditions for access to data and data objects will never be reduced.

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

P.Ident Identification

The TOE must be capable of being uniquely identified.

The TOE consists of hardware and software elements. The software might be stored in a hard mask (through incorporation in the ROM photomask) or could be stored in non-volatile memory. The hardware could have optional features which might or might not be enabled. An accurate identification must therefore be established for the exact instantiation of the final product compliant to this ST. This requires unique identification for the TOE.

P.Sec_Com Secure Communications

Secure communications protocols and procedures shall be supported between the TOE and a trusted terminal.

The TOE may engage in a variety of communications ranging from simple status checking through secure data transfer. Under the variety of communications we understand the multitude of scenarios for communication between the TOE and the card reader/writer that is carried out using the command interface of the card. At the minimum, the TOE must be capable of establishing a secure channel to a trusted source for execution of potentially privileged commands.

CHAPTER 4

Security Objectives

This section describes the security objectives for the TOE and the TOE environment in response to the security needs identified in the “TOE Security Environment” section.

Security objectives for the TOE will be satisfied by technical countermeasures implemented by the TOE. Security objectives for the environment are to be satisfied by either technical measures implemented by the IT environment, or by non-IT measures.

Security Objectives to be met by the TOE

The TOE will meet the security objectives detailed below. Each objective is stated in bold type font. It is followed by an application note, in normal font, which supplies additional information and interpretation.

O.Crypt Cryptography

The TOE must support cryptographic functions in accordance with *P.Crypt_Std Cryptographic Standards*.

The TOE must perform any cryptographic operations consistent with established cryptographic usage policies and standards in order to maintain the security level provided by the basic cryptographic functions in accordance with *P.Crypt_Std Cryptographic Standards*.

O.Data_Acc Data Access Control

The TOE must provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the P.Data_Acc Security Policy.

The TOE may have a variety of users, administrators, card issuers, associations, etc., each requiring some control over the assets being handled. Some rules will apply in all cases. These are represented in security functional requirement FDP_ACF.1. The remainder must be explicitly stated as required by the needs of the owners of the data.

O.Env_Strs Environmental Stress

The TOE must protect itself against compromise by having a structure which neither reveals security information nor operates in an insecure fashion when exposed to out of standard conditions (high or low) in the environment represented by the following factors: temperature, voltage, clock frequency, or external energy fields.

The basic TOE must be designed and fabricated so that it continues to provide security to its critical information comprised of user assets and internal security information (as detailed in chapter “Assets” on page 25), even when exposed to environmental stress. Environmental stress may be a result of the normal environment in which the TOE is used, but may also be representative of an attack against it. In the event of attack, stress may be the only driving force or it may be used in conjunction with one or several other attacks. This objective should work to prevent disclosure of secure information in any of these conditions.

O.HW_Test Hardware testing

The TOE must be able to demonstrate that the hardware and firmware operates correctly when requested.

The TOE must be capable of demonstrating that the hardware and firmware that supports the application software of the system operates correctly. For this purpose the TOE must support loading and executing suits of tests.

O.I_Leak Information Leakage

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

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

O.Ident TOE Identification

The TOE must support the recording and preservation of identification information.

The TOE consists of hardware and software elements. The software is stored in a hard mask (through incorporation in the ROM photomask). The hardware and software features differ for different versions of the product. It is therefore essential that an accurate identification be established for the exact instantiation of the final product compliant to this Security Target. This requires unique identification for the TOE.

O.Init Initialization

The TOE must assume its initial state immediately upon power-up, reset, or after other restart conditions.

The TOE must always start in a defined and controlled state regardless of how it was reset. This objective works to prevent attacks which attempt to upset the operation and leave the TOE in an undefined state.

O.Life_Cycle Life Cycle Functions

The TOE must provide means of controlling and limiting the use of life-cycle-specific commands to the life cycle stages in which they are intended.

The design and implementation of the TOE must be such that the only commands available to a specific operation are related to the life-cycle appropriate to that application. Thus, the debug functions or one time loading of identification information functions should never be available during operational TOE use.

O.Log_Prot Logical Protection

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

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

O.Phys_Prot Physical Protection

The TOE must be resistant to physical attack or be able to create difficulties in understanding the information derived from such an attack.

The TOE must be designed and fabricated so that it requires a combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or contents of memory which could contribute to a compromise in TOE security through a physical attack on the IC. This objective should work to prevent disclosure of secure information.

O.Power Power Loss Recovery

The TOE shall protect the integrity of data from accidental power loss.

The TOE is not internally powered. The power is supplied by the reader/writer and the power supply can be interrupted during a transaction. The TOE shall recover from power loss in such a way that the stored data is not corrupted.

O.Reuse Replay

The TOE shall protect its resources against replay attacks.

The TOE must act so that no assets can be compromised through an attacker's attempt to replay or restart an operation which might have been completed successfully or interrupted in process.

O.Sec_Com Secure Communications

The TOE must be able to support secure communication protocols and procedures with a trusted terminal.

The TOE must provide a mechanism for establishing and maintaining a secure information link into the Card Reader/Writer.

O.Set_Up Set-Up Sequence

The TOE must require a defined sequence of operations prior to general utilization.

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

Security Objectives to be met by the TOE Environment

IT Security Objectives for the TOE Environment

The following are IT security objectives that are to be satisfied by imposing technical requirements on the TOE Environment. These security objectives are required by the Security Target to be in place in the TOE environment. They are included as necessary to support the TOE security objectives in addressing the security problem defined in the TOE security environment. Each objective is stated in bold type font. It is followed by an application note, in normal font, which supplies additional information and interpretation.

OE.Sec_Com Reader/Writer Secure Communication

A trusted Reader/Writer is available for secure communication with the TOE.

The Reader/Writer is capable of accepting and maintaining a secure communications link with the TOE.

OE.Key_Supp Cryptographic Key Support

All imported smart card related cryptographic keys must be supported according to the owners' needs.

A variety of shared keys may be imported for use by, and in conjunction with, the TOE. These keys will be supplied from the various bodies controlling the operations of the system in which the TOE is functioning. The personnel and systems in charge of these keys are responsible for the required security of their generation, distribution, maintenance, and destruction.

Non-IT Security Objectives for the TOE Environment

The following are non-IT security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they do not require the implementation of functions in the TOE hardware or software. These security objectives are assumed by the Security Target to be in place in the TOE environment. They are included as necessary to support the TOE security objectives in addressing the security problem defined in the TOE security environment. Each objective is stated in bold type font. It is followed by an application note, in normal font, which supplies additional information and interpretation.

OE.Data_Store Off-TOE Data Storage

All TOE data stored off of the TOE must be controlled for confidentiality and integrity according to the owner's needs.

A variety of TOE information may be stored separately from the TOE. This information is related to ownership, issuer data, personalization data. The personnel and systems in charge of this information are responsible for the maintenance of its required security.

OE.Pers Personnel

Personnel working as administrators or in other privileged positions shall be carefully selected and trained for reliability.

Careful selection and training of administrators and others in privileged positions works to detect, prevent, or counter other attacks.

OE.Power Power Supply

The Reader/Writer supplies power to the TOE.

The TOE is internally unpowered, so support must be delivered to the card from the card Reader/Writer device.

OE.Tamper Tamper Indication

The carrier for the TOE shall provide an indication of tampering if the TOE has been removed and re-inserted.

The personnel in charge of inspecting the TOE carrier are responsible for the detection of tampering with the carrier. This objective can only apply in those

cases when the carrier is presented to such personnel and it is physically available for inspection.

OE.Delivery Delivery procedures

The TOE must be delivered in a secure way.

The TOE software and hardware must be delivered using approved procedures that ensure that an attacker cannot easily intercept the TOE or parts of it. The procedure must include measures for verification of the TOE integrity and confidentiality.

CHAPTER 5

IT Security Requirements

IT security requirements include:

1. TOE security functional requirements (SFRs), that is, requirements for security functions such as information flow control, identification and authentication.
2. Strength of function, claims a minimum strength level consistent with the security objectives that the functions realized using a probabilistic or permutational mechanism must provide.
3. TOE security assurance requirements (SARs), provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, vulnerability assessment.)
4. Security requirements for the TOE's environment (that is, for hardware, software, or firmware external to the TOE, as well as operating procedures and policies, and upon which satisfaction of the TOE's security objectives depends.)

These requirements are discussed separately below.

TOE Security Functional Requirements

This section presents the SFRs for the TOE. In accordance with the methodology described in Section 1.4, Security Target Preparation Methodology, this section presents the following three types of SFRs:

1. Restated SFRs: those CC security functional requirements with which the ST claims compliance and for which no additional operations are to be performed. These CC SFRs are included in the ST verbatim.
2. Tailored SFRs: those CC security functional requirements with which the ST claims compliance but for which additional operations are to be performed.
3. SFRs with Strength of Function (SOF) declarations: any security functional requirements that require a SOF declaration.

TABLE 1. TOE Security Functional Requirements summary

Functional Component ID	Functional Component Name	Functional Component Use	Operation	Strength of Function
FCS_CKM.1	Cryptographic key generation	tailored refined	assignment	basic
FCS_CKM.4	Cryptographic key destruction	tailored refined	assignment	
FCS_COP.1	Cryptographic operation	tailored refined	assignment iteration	basic
FDP_ACC.1	Subset access control	tailored	assignment iteration	
FDP_ACF.1	Security attribute based access control	tailored	assignment iteration	
FDP_DAU.1	Basic data authentication	tailored	assignment	basic
FDP_ETC.1	Export of user data without security attributes	tailored	assignment	
FDP_IFC.1	Subset information flow control	tailored	assignment	
FDP_IFF.1	Simple security attributes	tailored refined	assignment	

TABLE 1. TOE Security Functional Requirements summary

Functional Component ID	Functional Component Name	Functional Component Use	Operation	Strength of Function
FDP_ITC.1	Import of user data without security attributes	tailored	assignment	
FDP_SDI.1	Stored data integrity monitoring	tailored	assignment	
FPT_AMT.1	Underlying abstract machine test	tailored refined	selection	
FPT_FLS.1	Failure with preservation of secure state	tailored	assignment	
FPT_ITC.1	Inter-TSF confidentiality during transmission	restated	-	
FPT_ITI.1	Inter-TSF detection of modification	tailored	assignment	basic
FPT_RCV.4	Function recovery	tailored	assignment	
FPT_RPL.1	Replay detection	tailored	assignment	
FTP_ITC.1	Inter-TSF trusted channel	tailored	selection assignment	

The TOE shall satisfy the SFRs stated below.

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 ***Session Key Generation Algorithm*** and specified cryptographic key sizes ***56*** that meet the following ***standards***: ***[]***, ***[DES Implementation Guidelines]***.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified key destruction method ***volatile memory erasure at the end of session*** that meets the following ***standard***: ***[DES Implementation Guidelines]***.

FCS_COP.1 Cryptographic operation

FCS_COP.1.1A The TSF shall perform ***data encryption and decryption*** in accordance with a specified cryptographic algorithm ***DES*** and cryptographic key sizes *56* that meet the following ***standards***: ***[DES], [DES Modes of Operation], and [DES Implementation Guidelines]***.

FCS_COP.1.1B The TSF shall perform ***cryptographic key encryption and decryption*** in accordance with a specified cryptographic algorithm ***triple DES*** and cryptographic key sizes ***112*** that meet the following ***standards***: ***[DES], [DES Modes of Operation], and [DES Implementation Guidelines]***.

FDP_ACC.1 Subset access control

FDP_ACC.1.1A The TSF shall enforce ***Access Control Policy*** on ***any subject's read and write access to service areas and service files***.

FDP_ACC.1.1B The TSF shall enforce ***Reader/Writer Authentication Policy*** on ***Reader/Writer's access to the card***.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1A The TSF shall enforce ***Access Control Policy*** to objects based on ***access key***.

FDP_ACF.1.2A The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1). The access key provided by the subject must correspond to the access key of the object.

or

2) The object must be marked with the "insecure access" attribute.

FDP_ACF.1.1B The TSF shall enforce ***Reader/Writer Authentication Policy*** to objects based on ***authentication key***.

FDP_ACF.1.2B The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***the authentication key provided by the Reader/Writer corresponds to the authentication key stored in the card***.

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

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

FDP_DAU.1 Basic data authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of ***the firmware***.

FDP_DAU.1.2 The TSF shall provide ***an authenticated Reader/Writer*** with the ability to verify evidence of the validity of the indicated information.

FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the ***Access Control Policy and Reader/ Writer Authentication Policy*** when exporting user data, controlled under the SFP(s), outside the TSC.

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

Application Note for FDP_ETC.1 and FDP_ITC.1.

The only security related attributes of the data are the access key and "secure access" attribute. These attributes are not exported together with the data when the data is read. The attributes are set on the data storage rather than the data itself and those attributes are never exported or imported with the data.

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the ***Information Separation Policy*** on ***all operations with the virtual cards***.

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the ***Information Separation Policy*** based on the following types of subject and information security attributes: ***System Code***.

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: ***none.***

Application note for FDP_IFC.1 and FDP_IFF.1.

The information flow is not allowed between the parts that implement ‘virtual cards’ under any circumstances. The virtual cards that result from the separation are accessed completely independently. The use of this separation function is optional and this requirement applies only in the case when such separation has been applied to the card.

The requirements FDP_IFF.1.3 to FDP_IFF.1.6 are not applicable since there are no additional policies, capabilities or rules associated with this requirement.

FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the ***Access Control Policy and Reader/ Writer Authentication Policy*** when importing user data, controlled under the SFP, from outside the TSC.

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

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

FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for ***integrity errors*** on all objects, based on the following attributes: ***CRC checksum***.

FPT_AMT.1 Abstract machine testing

FPT_AMT.1.1 The TSF shall run a suite of tests ***[other conditions]*** to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Application note for FPT_AMT.1

The TSF must allow loading and executing suites of tests at any time to demonstrate the correct operation of the hardware. The TSF must prevent the disclosure of the information stored on the card before the execution of the tests.

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: ***power failure, communication failure***.

FPT_ITC.1 Inter-TSF confidentiality during transmission

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

FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: ***the strength of the modification metric shall be as provided by DES***.

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform ***data discard and connection termination*** if modifications are detected.

FPT_RCV.4 Function recovery

FPT_RCV.4.1 The TSF shall ensure that ***Power Failure and Communication Failure scenarios*** have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

FPT_RPL.1 Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: ***card ordinary commands, card issue commands, reader/writer operation commands, reader/writer management commands***.

FPT_RPL.1.2 The TSF shall perform ***command discard*** when replay is detected.

FTP_ITC.1 Inter-TSF trusted channel

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

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for ***user data exchange and TSF data exchange***.

Strength of Function

The overall Strength of Function claim for the TOE is SOF-basic in accordance with the recommendations of [CC3].

"Request for CC interpretation number 142" (RI142) shall be used for the evaluation of the hardware aspects of the platform. This automatically invokes the Joint Interpretation Library (JIL) and specifies that the hardware evalaution is done in accordance with JIL recommendations.

TOE Security Assurance Requirements

Table 2 on page 50 identifies the security assurance components drawn from CC part 3: Security Assurance Requirements, EAL4.

The assurance requirements are stated verbatim from [CC3].

TABLE 2. TOE Security Assurance Requirements summary

Assurance Component ID	Assurance Component Name
ACM_AUT.1	**Partial CM automation**
ACM_CAP.4	**Generation support and acceptance procedures**
ACM_SCP.2	**Problem tracking CM coverage**
ADO_DEL.2	**Detection of modification**
ADO_IGS.1	**Installation, generation, and start-up procedures**
ADV_FSP.2	**Fully defined external interfaces**
ADV_HLD.2	**Security enforcing high-level design**
ADV_IMP.1	**Subset of the implementation of the TSF**

TABLE 2. TOE Security Assurance Requirements summary

Assurance Component ID	Assurance Component Name
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 function evaluation
AVA_VLA.2	Independent vulnerability analysis

Security Requirements for TOE Environment.

The requirements for the TOE environment are based on those specified in the [CC2].

Security requirements in the TOE environment are described in the Table 3 on page 52. These requirements are handled as requirements for the issuing system of TOE.

Requirements are not completed in this part. The completion of the requirements will depend on the application of the TOE and the service provider. Therefore the completion of the requirements is left to the service provider to provide for sufficient flexibility in choosing their own environment.

The requirements stated here were all refined to replace “TSF” with “IT Environment” so that there is no misunderstanding as to what they refer to.

TABLE 3. TOE Security Requirements for IT Environment Summary

Functional Component ID	Functional Component Name	Functional Component Use	Operation	Strength of function
FCS_CKM.1	Cryptographic key generation	tailored	assignment	basic
FCS_CKM.2	Cryptographic key distribution	tailored	assignment	
FCS_CKM.4	Cryptographic key destruction	tailored	assignment	
FCS_COP.1	Cryptographic operation	tailored	assignment	basic
FTP_ITC.1	Inter-TSF trusted channel	tailored	selection assignment	

The TOE Security Requirements for IT Environment are discussed further in detail.

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The *IT Environment* shall generate cryptographic keys in accordance with a specified key generation algorithm [**assignment: cryptographic key generation algorithm**] and specified cryptographic key sizes ***56 bits or 112 bits as appropriate*** that meet the following ***standard(s)***: ***[DES], [DES Implementation Guidelines]***.

FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The *IT Environment* shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method

[**assignment: cryptographic key distribution method**] that meets the following: ***[DES Implementation Guidelines]***.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The *IT Environment* shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**assignment: cryptographic key destruction method**] that meets the following: ***[DES Implementation Guidelines]***.

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The *IT Environment* shall perform ***data encryption and decryption*** in accordance with a specified cryptographic algorithm ***DES*** and cryptographic key sizes ***56 bits or 112 bits as appropriate*** that meet the following: ***[DES], [DES Modes of Operation], and [DES Implementation Guidelines] standards***.

FTP_ITC.1 Inter-TSF trusted channel

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

FTP_ITC.1.2 The TSF shall permit ***the TSF*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for ***user data exchange and TSF data exchange***.

CHAPTER 6

TOE Summary Specification

This chapter describes the IT security functions provided by the TOE to meet the security functional requirements specified in “IT Security Requirements” on page 43. Every security function is given a label that allows to refer to a particular function.

This chapter also describes the Assurance Measures that are taken to ensure the safety of development, delivery, and operation of the TOE.

IT Security Functions

TABLE 4. Security Functions and Security Functional Requirements

Security Functions / Group	Security Functional Requirements																	
	FCS-CKM.1	FCS-CKM.4	FCS-COP.1	FDP-ACC.1	FDP-ACF.1	FDP_DAU.1	FDP-ETC.1	FDP_IFC.1	FDP_IFF.1	FDP-ITC.1	FDP-SDI.1	FPT_AMT.1	FPT-FLS.1	FPT-ITC.1	FPT-ITI.1	FPT-RCV.4	FPT-RPL.1	FTP-ITC.1
Access Control				**X**	**X**		**X**	**X**	**X**	**X**								
Data Encryption			**X**											**X**	**X**		**X**	**X**
Data Protection						**X**					**X**	**X**	**X**	**X**		**X**		**X**
Mutual Authentication			**X**				**X**			**X**				**X**	**X**		**X**	**X**
File Registration	**X**	**X**	**X**	**X**	**X**			**X**	**X**									
Key Change	**X**	**X**	**X**															

[AC] Access Control

The access control features of the RC-S860 Contactless Smart Card were developed to allow for special operations vital for the contactless smart cards:

- hierarchical allocation of resources;
- simultaneous access to multiple areas;
- fine-grained access control rules;
- special access modes.

[AC.1] Hierarchical file system

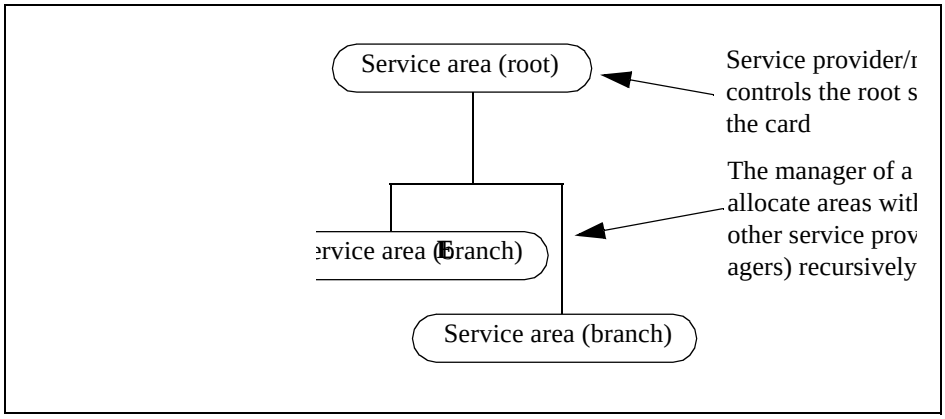
The provider can register service files, used to store various data, in the memory area where the provider is granted use in the card. Moreover, the provider is permitted to reallocate recursively the area where the provider is granted access to other

providers. This system makes it possible to register service files in a hierarchical structure. A unique access key can be set for each area and each service file.

[AC.2] Service Area and Service File access

the memory of the card in blocks that The RC-S860 Contactless Smart Card is designed to give each manager authorization to access the card. The relations between managers can be illustrated by a tree structure, in which an issuer is root and the issuer and each manager takes responsibility for own service files and the files of offspring branches, i.e. sub-managers.

FIGURE 1. Removed



Each Card manager is assigned an area, consisting of usable range of service Code and number of blocks, by its parent, i.e., issuer or higher manager, and such manager can create its own service and give a part of its area to its offspring, sub-manager.

Service without protection, i.e. without any key, can be included in the service list for accessing simultaneously but such service is not included in the pass for key generation.

[AC.3] Authentication

Mutual authentication is done utilizing the service file to be accessed and the user service key as well as the group service key synthesized from the area in which such service file is located.

Since the user service key and the group service key can be synthesized without direct disclosure of the area key or the service key, access control is done while grouping the service files up to 16 blocks during authentication providing simultaneous access to 12 blocks of a service file for reading or 8 blocks of a service file for writing at a time. Access to other services without authorization is inhibited even if such services are located within a same card. Prevention of illegal access to service files is possible.

[AC.4] Service File types

Available file types are discussed below:

1. Random Access File

The blocks of random access files can be accessed freely by specifying the desired block number.

2. Cyclic Access File

Cyclic access files are controlled by the wraparound type of block numbers. In this control system, all blocks are arranged in chronological order starting from the oldest file. A new file overwritten on the oldest block.

3. Purse Block File

Purse block files functions for subtracting the specified data, adding a value within the range of subtraction of immediately before, and others.

TABLE 5. Removed

Type of Service	Function	Types of Access	Encryption
Random Access	Any desired block can be read(/written) in service area	Read/Write	Yes or No
		Read Only	Yes or No
Cycle Access	Writing into FIFO in units of block is possible in service area	Read/Write	Yes or No
		Read Only	Yes or No

TABLE 5. Removed

Type of Service	Function	Types of Access	Encryption
Purse Access	Same as Random Access in service area	Read/Write	Yes or No
	Read/Subtraction/Cash back in service area	Cash back	Yes or No
	Only Read and Subtraction of purse in service area	Subtraction	Yes or No
	Read Only in service area	Read Only	Yes or No

Functional Requirements satisifed : FDP_ACC.1, FDP_ACF.1, FDP_ETC.1, FDP_ITC.1.

[AC.5] Card separation function

The card separation function works by creating 2 images of the card in the memory. Each image is accessed independently using own issuance information and selected by the System Code. This function allows a complete separation of the information stored on the resulting ‘virtual cards’.

Functional Requirements satisifed : FDP_IFC.1, FDP_IFF.1

[DE] Data Encryption

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

[[DE.2] Transaction ID and Transaction Key

Two random numbers obtained during the course of Mutual Authentication Process are utilized as the transaction ID (Session ID) and the transaction key (Session Key).The transaction ID is placed at the top of data to improve the security level of the encryption in CBC mode. In addition, the transaction ID is updated and checked at every transaction to restrict the same command can be used only once during a session.Using the transaction key as the key in data encryption process by DES, in addition, it is possible to use the transaction key as a key disposable at the end of each session for improvement of the security level of system.

[DE.3] Packet Parity Generation

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

[DE.4] Data Encryption System

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

Functional Requirements Satisfied: FCS_COP.1, FPT_ITC.1. FPT_ITI.1, FPT_RPL.1, FTP_ITC.1

[DP] Data Protection

[DP.1] Transaction protection

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

[DP.2] Protection of communication

All wireless communication paths are encrypted by random numbers, which provides superior protection against various illegal attacks such as wiretapping, falsification or reuse of the card session.

[DP.3] Detection of data corruption

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

[DP.4] Software and hardware validation

The correctness of additional application and system software loaded onto the card (can verify) REMOVED in the course of normal operation of the card.

The hardware operation and the correctness of the firmware are verified by loading and executing suits of tests using the special test mode of the TOE. Entering the test mode brings the TOE to the original state before issuing by erasing all data in TOE's memory.

Functional Requirements satisfied: FDP_DAU.1, FPT_ITC.1, FTP_ITC.1, FPT_FLS.1, FPT_RCV.4, FDP_SDI.1, FPT_AMT.1.

[RWMA] Reader/Writer Mutual Authentication

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

RC-S860 Contactless Smart Card uses an improved system derived from the 3-way handshake system defined in ISO9798. Based upon the confidential communication system after the mutual authentication completed, an improved security level of system is implemented.

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

All wireless communication paths are encrypted by session keys generated as random numbers, which provides superior protection against various illegal attacks such as wiretapping, falsification or reuse of the card sessions. The details of the process are described in *[DE] Data Encryption*.

Evaluation of DES's security strength is done all over the world because it is publicly open. By applying DES algorithm to the original text 3 times, Triple DES achieves the longer length of key actually used. DES encrypts a block of data consisting of 64 bits using a single key of 56 bits, and decrypts the data thus encrypted using the same key. Triple DES is able to provide a higher level of security than Single DES.

Functional Requirements Satisfied: FDP_ETC.1, FDP_ITC.1, FPT_ITC.1, FPT_ITI.1, FPT_RPL.1, FTP_ITC.1, FCS_COP.1

[FR] File Registration

The new service file or area can be registered to a card using the issue information. This issue information contains the issue parameters describing the service/area to be set up. The issue information is divided into blocks and encrypted with a synthetic key.In addition, One card can separate to logical two cards REMOVED.

Functional requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1

[KC] Key Change

[KC.1] At the time of IC card manufacturing

During the manufacturing process the IC chip is protected by a IC manufacturing key. This key must be supplied any time the information in the card needs to be changed. The identification of the manufacturer is also written to the card during the manufacturing process after the IC card was assembled.

[KC.2] At the time of IC card transportation

Before transportation the IC manfuacturing key is changed to a special transportaion key. The specified security key (IC card shipping key) protects the IC card during its transportation.

[KC.3] At the time of IC card issuance to customer

The customer has to replace the IC card shipping key with the individual customer key before setting up the card. The new security key is bundled into a special package called key issuance information. The customer has to input this information to the card and the card will be then available for the customer to set up services.

[KC.4] At the time of adding a service file

It is mandatory to make only the person who knows the security key set up to the IC card by the customer is able to add service files. To achieve this, registration of area file is done to make service files under the management of such area file can be registered only by the person who knows the key for such area.

Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1

Required Security Mechanisms

The security functions require the following security mechanisms to be implemented in the TOE:

1. A random number generator.
2. A DES encryption module.

Assurance Measures

This section describes the assurance measures applied to the RC-S860 Contactless Smart Card to satisfy the CC EAL4 assurance requirements.

Configuration Management

The configuration management measures applied include assigning a unique product identifier for each release of the TOE. Associated with this Product Identifier is a list of hardware and software configuration items that comprise a single instance of the TOE. These configuration measures are documented within the following document: “REMOVED Development Configuration Management”.

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

Development

The architecture documents satisfy the functional requirements and the high level design specification requirements. These are specified in the following documents:

- “Function Specification REMOVED”
- “High Level Design REMOVED”
- “IC Development Specification”
- “Low Level Design REMOVED”
- Implementation source code.

Requirements satisfied: ADV_FSP.2, ADV_HLD.2, ADV_LLD.1, ADV_IMP.1.

Security policy model

The Security Policy Model is represented by this Security Target. Additionally, the secure states of the card are defined in the “Security Reference Manual”.

Requirements satisfied: ADV_SPM.1.

Guidance, delivery and operation

The guidance documentation provided with the TOE includes the administrator and user guidance as well as a complete API reference of the card commands. The Delivery and Operation documentation describes the delivery procedures that are used for the delivery of the TOE and the initialization procedure for the enabling of the TOE. These guidance**,** delivery and operation measures are documented in the following documents:

- “Security Manual”;
- “Security Reference Manual”;
- “REMOVED User’s Manual”;
- “Rewriting Transport Key”;
- “REMOVED Operation Manual”;
- “Card Issue Procedure”;
- “Delivery Procedure”.

Requirements satisfied: AGD_ADM.1, AGD_USR.1, ADO_DEL.2, ADO_IGS.1.

The documentation is analysed for completeness and the results of the analysis are provided in the document “Missue Correspondence Table REMOVED”.

Requirements satisfied: AVA_MSU.2.

Development security

The development security measures are identified in the document “ICSS Division Security Policy”.

Requirements satisfied: ALC_DVS.1.

Life-Cycle Model

The Life-Cycle Model is represented by this Life-Cycle Model document.

Requirements satisfied: ALC_LCD.1

Testing

The TOE testing policies and procedures and results of the tests are presented in the following documents:

- "Test Specification";
- "Function Test Procedure";
- "Command Test Procedure";
- "Error Test Procedure";
- "Function Test Result";
- "Command Test Result";
- "Error Test Result"
- "REMOVED Test Script Tool Users Manual"
- "DES Test Specification"
- "DES Test Procedure"
- "DES Test Result"
- "Random Generator Specification"
- "Random Generator Procedure"
- "Random Generator Result"

Requirements satisfied: ATE_DPT.1, ATE_FUN.1, ALC_TAT.1.

The examination of test coverage is documented in "REMOVED Test Coverage Results" document.

Requirements satisfied: ATE_COV.2.

SOF

The Strength-Of-Function analysis is presented in the document "REMOVED Strength Of Function Analysis".

Requirements satisfied: AVA_SOF.1.

Vulnerability analysis

The developer vulnerability analysis is performed as a part of the design and testing process. The goal of the analysis is to identify and analyze security vulnerabilities and to confirm that they cannot be exploited in the TOE's intended environment. The results of the analysis are documented in "REMOVED Developer Vulnerability Analysis" document.

Requirements satisfied: AVA_VLA.2.

CHAPTER 7

Removed

This chapter demonstrates the suitability of the choice of security objectives and that the stated security objectives counter all identified threats, policies, or assumptions.

Security Objectives Coverage

The following tables provide a mapping of security objectives to the environment defined by the threats, policies, and assumptions, illustrating that each security objective covers at least one threat, policy or assumption and that each threat, policy, or assumption is covered by at least one security objective.

TABLE 6. Removed

Threat	Is addressed by Objective(s)
T.P_Probe	O.Phys_Prot
T.P_Modify	O.Phys_Prot
T.E_Manip	O.Phys_Prot, O.HW_Test

TABLE 6. Removed

Threat	Is addressed by Objective(s)
T.Forcd_Rst	O.Init
T.Logic_Atk	O.Log_Prot
T.Reuse	O.Reuse
T.Access	O.Data_Acc
T.First_Use	O.Data_Acc, O.Set_Up
T.LC_Ftn	O.Life_Cycle
T.Crypt_Atk	O.Crypt
T.I_Leak	O.Env_Strs, O.I_Leak, O.HW_Test
T.Env_Strs	O.Env_Strs
T.Clon	O.Phys_Prot, OE.Data_Store
T.Power	O.Power
T.Delivery	OE.Delivery

TABLE 7. Removed

Policy	Is addressed by Objective(s)
P.Crypt_Std	O.Crypt
P.Data_Acc	O.DAC
P.Ident	O.Ident
P.Sec_Com	O.Sec_Com

TABLE 8. Removed

Assumption	Is addressed by Objective(s)
A.Sec_Com	OE.Sec_Com
A.Carrier	OE.Tamper
A.Data_Store	OE.Data_Store
A.Key_Supp	OE.Key_Supp

TABLE 8. Removed

Assumption	Is addressed by Objective(s)
A.Power	OE.Power
A.Priv	OE.Pers

TABLE 9. Removed

Security Objective	Is necessitated by
O.Crypt	T.Crypt_Atk, P.Crypt_Std
O.Data_Acc	T.Access, T.First_Use, P.Data_Acc
O.Env_Strs	T.I_Leak, T.Env_Strs
O.HW_Test	T.E_Manip, T.I_Leak
O.I_Leak	T.I_Leak
O.Ident	P.Ident
O.Init	T.Forced_Rst
O.Life_Cycle	T.LC_Ftn
O.Log_Prot	T.Logic_Atk
O.Phys_Prot	T.P_Probe, T.P_Modify, T.E_Manip, T.Clon
O.Power	T.Power
O.Reuse	T.Reuse
O.Sec_Com	P.Sec_Com
O.Set_Up	T.First_Use
OE.Sec_Com	A.Sec_Com
OE.Data_Store	A.Data_Store, T.Clon
OE.Key_Supp	A.Key_Supp
OE.Pers	A.Priv
OE.Power	A.Power
OE.Tamper	A.Carrier
OE.Delivery	T.Delivery

Security Objectives Sufficiency

This chapter provides information that shows that the chosen security objectives are sufficient to address the identified threats, assumptions, and policies. The information is divided into the following parts:

1. How the identified security objectives provide for effective countermeasures to the identified threats.
2. How the identified security objectives provide the complete coverage of organizational security policies.
3. How the identified security objectives uphold identified assumptions.

The detailed discussion of each part is presented below.

Threats and Objectives Sufficiency

T.P_Probe Physical Probing of the IC deals with mechanical attacks on the structure of the TOE itself. It is countered directly by *O.Phys_Prot Physical Protection* which ensures that the TOE is constructed using such elements as protective layering, special rules regarding integrated circuit layout, and removal of test pads after initial (wafer) testing is complete. These actions are intended to make deriving information from the IC difficult and, if such information is derived, to make it difficult to interpret and apply such information to attempts to compromise.

T.P_Modify Physical Modification of the IC deals with attempts to physically modify the TOE such that information relating to the secure operation of the TOE is revealed. This is an extension of *T.P_Probe Physical Probing of the IC* since it may involve physical changes to the IC such as rerouting connections or repairing fuses. This threat is also countered by *O.Phys_Prot Physical Protection,* which ensures that the TOE is constructed using such elements as protective layering, special rules regarding integrated circuit layout, and removal of test pads after initial (wafer) testing is complete. These actions are intended to make deriving information from the IC difficult and, if such information is derived, to make it difficult to interpret and apply such information to attempts to compromise.

T.E_Manip Electrical Manipulation of the IC addresses attempts in which the TOE is modified so that it can be directly fraudulently used. This differs from *T.P_Modify Physical Modification of the IC* in that the goal of the former threat is to derive information and not to reuse the TOE. This threat is also countered by *O.Phys_Prot Physical Protection*, which ensures that the TOE is constructed using such elements as protective layering, special rules regarding integrated circuit lay-

out, and removal of test pads after initial (wafer) testing is complete. These actions are intended to make deriving information from the IC difficult and, if such information is derived, to make it difficult to interpret and apply such information to attempts to compromise. The threat is also countered through *O.HW_Test Hardware testing* allowing the verification of the correct hardware operation.

T.Power Power Supply Failure Data Protection establishes that the power loss may lead to corruption of data stored on the card when such loss occurs during a transaction. *O.Power Power Loss Recovery* counters the possibility of data loss due to the interruptions n the power supply delivery.

T.Forced_Rst Forced Reset addresses the situations in which the TOE is reset during an operation. This may occur at any time including during the reset operation itself. This threat is countered directly by *O.Init Initialization*, which ensures that the TOE always enters its defined initial state upon reset.

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

T.Reuse Replay Attack addresses the attempts by an attacker to utilize the information available from a partially or fully completed operation to repeat the operation in a fraudulent fashion. This is countered through *O.Reuse Replay*, which ensures that no assets can be compromised in the event of a replay.

T.Access Invalid Access addresses the need for protection from unauthorized access to information or resources. This threat is distinguished by the emphasis on access of users to information. This is related to *P.Data_Acc Data Access*. This threat is countered directly by *O.Data_Acc Data Access Control*, which establishes the access control policies.

T.First_Use Fraud on First Use deals with fraud perpetrated through the use of a TOE which has not been officially issued. This threat is countered directly by

O.Data_Acc Data Access Control and *O.Set_Up Set-Up Sequence* which ensure that a defined and controlled sequence of events is completed before the TOE is enabled for use.

T.LC_Ftn Use of Unallowed Life Cycle Functions deals with the exploitation of inappropriate interaction of functions between various life cycle operations. *O.Life_Cycle Life Cycle Functions* ensures that such interactions do not compromise security through unauthorized availability of information between elements used in different parts of the life cycle.

T.Crypt_Atk Cryptographic Attack addresses direct attacks on the cryptographic mechanisms employed in the TOE. This threat is countered by *O.Crypt Cryptography*, which ensures that any cryptographic functions available are performed in a secure manner.

T.I_Leak Information Leakage deals with the exploitation of information inadvertently available from emanations or variations in power consumption or other operating parameters as a function of the operation being performed. SPA and DPA are examples of such information leakage. This threat is countered by *O.I_Leak Information Leakage*, which ensures that such information is not exposed. This threat is also partially countered by *O.Env_Strs Environmental Stress*, which ensures that the TOE performs in an acceptable fashion (i.e. does not reveal secure information) when exposed to out-of-design-specification conditions. This threat is also partially covered by *O.HW_Test Hardware testing* that allows verification of the correct operation of the hardware.

T.Env_Strs Environmental Stress deals with the imposition of environmental extremes on the TOE with the intent to cause a direct or indirect failure in the security mechanisms. This threat is countered by *O.Env_Strs Environmental Stress*, which ensures that the TOE performs in an acceptable fashion (i.e. does not reveal secure information) when exposed to out-of-design-specification conditions.

T.Clon Cloning represents the threat that an attacker may manufacture all or a usable portion of the TOE which is then used for fraudulent purposes. This threat is countered by *O.Phys_Prot Physical Protection* through a construction that makes it difficult to understand any information derived from physical attacks on the TOE. The *OE.Data_Store Off-TOE Data Storage* also helps to counter the threat by preventing the illicit appropriation of design information.

T.Delivery Attacks during delivery represents the threat that an attacker may gain access to the whole TOE or a part of it during the delivery outside the secure facili-

ties used for development and manufacturing. This threat is countered by *OE.Delivery Delivery procedures* which ensures secure procedures are used for delivery that will prevent and detect such attempts.

Policies and Objectives Sufficiency

P.Crypt_Std Cryptographic Standards establishes that accepted cryptographic standards and operations shall be used in the design of the TOE. This is addressed by *O.Crypt Cryptography*, which ensures that such standards are used.

P.Data_Acc Data Access establishes that there must be a stated policy for access to data and data objects. This policy is addressed directly by *O.Data_Acc Data Access Control*, which establishes the access control policies.

P.Ident Identification establishes that there must be a clear, complete, and unique identification for the TOE. This is addressed through the *O.Ident TOE Identification*, which ensures that such identification is available.

P.Sec_Com Secure Communications establishes that there is a secure communication channel between the TOE and card reader/writer device. This is addressed in *O.Sec_Com Secure Communications*, which ensures that the TOE is capable of establishing and using such a link.

Assumptions and Objectives Sufficiency

A.Sec_Com Card Reader / Writer Secure establishes that there is assumed to be a secure communication capability in the card reader/writer device. This is addressed in *OE.Data_Store Off-TOE Data Storage*, which ensures that the reader/writer device is capable of establishing and using such a link.

A.Carrier Tamper detecting carrier establishes that the TOE is packaged in a carrier that facilitates detection of tampering. *OE.Tamper Tamper Indication* provides for this capability in the environment.

A.Data_Store Off-TOE Data Storage establishes that TOE information, when separate from the TOE, needs to be handled and stored in a secure fashion. *OE.Data_Store Off-TOE Data Storage* provides for that secure capability in the environment.

A.Key_Supp Cryptographic Key Support establishes that the generation, maintenance, distribution and destruction of keys for proper use of the TOE needs to be

supported external to the TOE. *OE.Pers Personnel* provides for that key support in the environment.

A.Power Power Supply establishes that the TOE is internally unpowered and therefore power supply must be delivered from the card reader/writer device. *OE.Power Power Supply* provides for that delivery.

A.Priv Abuse by Privileged Users establishes the need for properly trained and trustworthy personnel in the privileged positions. *OE.Pers Personnel* provides for such capability in the environment.

CHAPTER 8

Removed

This chapter will demonstrate the suitability of the choice of security requirements, demonstrating that each of the security objectives is addressed by at least one security requirement, and that every security requirement is directed toward solving at least one objective.

Security Requirements Coverage

The following tables provide a mapping of the relationships of security requirements to objectives, illustrating that each security requirement covers at least one objective and that each objective is covered by at least one security requirement.

TABLE 10. Removed

Security Objective	Is Addressed By:
O.Crypt	FCS_CKM.1, FCS_CKM.4, FCS_COP.1
O.Data_Acc	FDP_ACC.1, FDP_ACF.1, FDP_ETC.1, FDP_ITC.1, FDP_IFC.1, FDP_IFF.1

TABLE 10. Removed

Security Objective	Is Addressed By:
O.Env_Strs	FPT_FLS.1, FPT_RCV.4, FDP_SDI.1, FTP_ITC.1, AVA_VLA.2
O.HW_Test	FPT_AMT.1
O.I_Leak	AVA_VLA.2
O.Ident	ACM_CAP.4, ACM_SCP.2
O.Init	FDP_SDI.1, FPT_FLS.1, FPT_RCV.4
O.Life_Cycle	FDP_ACC.1, FDP_ACF.1, AVA_VLA.2
O.Log_Prot	FDP_ACC.1, FDP_ACF.1, FDP_DAU.1, FDP_SDI.1, FPT_FLS.1, FPT_ITI.1, FPT_RCV.4
O.Phys_Prot	FDP_SDI.1, AVA_VLA.2
O.Power	FDP_SDI.1, FPT_FLS.1, FPT_RCV.4
O.Reuse	FPT_RPL.1
O.Sec_Com	FTP_ITC.1
O.Set_Up	FDP_ACC.1, FDP_ACF.1, ADO_DEL.2, ADO_IGS.1

TABLE 11. Removed

Security Requirement	Is Necessitated By:
FCS_CKM.1	O.Crypt
FCS_CKM.4	O.Crypt
FCS_COP.1	O.Crypt
FDP_ACC.1	O.Data_Acc, O.Life_Cycle, O.Log_Prot, O.Set_Up
FDP_ACF.1	O.Data_Acc, O.Life_Cycle, O.Log_Prot, O.Set_Up
FDP_DAU.1	O.Log_Prot
FDP_ETC.1	O.Data_Acc
FDP_IFC.1	O.Data_Acc
FDP_IFF.1	O.Data_Acc
FDP_ITC.1	O.Data_Acc
FDP_SDI.1	O.Env_Strs, O.Init, O.Log_Prot, O.Phys_Prot, O.Power

TABLE 11. Removed

Security Requirement	Is Necessitated By:
FPT_AMT.1	O.HW_Test
FPT_FLS.1	O.Env_Strs, O.Init, O.Log_Prot, O.Power
FPT_ITC.1	O.Sec_Com
FPT_ITI.1	O.Log_Prot, O.Sec_Com
FPT_RCV.4	O.Env_Strs, O.Init, O.Log_Prot, O.Power
FPT_RPL.1	O.Reuse
FTP_ITC.1	O.Sec_Com

TABLE 12. Removed

Security Requirement	Is Necessitated By:
ACM_AUT.1	Selection of EAL4
ACM_CAP.4	Selection of EAL4
ACM_SCP.2	Selection of EAL4
ADO_DEL.2	Selection of EAL4
ADO_IGS.1	Selection of EAL4
ADV_FSP.2	Selection of EAL4
ADV_HLD.2	Selection of EAL4
ADV_IMP.1	Selection of EAL4
ADV_LLD.1	Selection of EAL4
ADV_RCR.1	Selection of EAL4
ADV_SPM.1	Selection of EAL4
AGD_ADM.1	Selection of EAL4
AGD_USR.1	Selection of EAL4
ALC_DVS.1	Selection of EAL4
ALC_LCD.1	Selection of EAL4
ALC_TAT.1	Selection of EAL4
ATE_COV.2	Selection of EAL4
ATE_DPT.1	Selection of EAL4
ATE_FUN.1	Selection of EAL4

TABLE 12. Removed

Security Requirement	Is Necessitated By:
ATE_IND.2	Selection of EAL4
AVA_MSU.2	Selection of EAL4
AVA_SOF.1	Selection of EAL4
AVA_VLA.2	Selection of EAL4

TABLE 13. Removed

Security Objective	Is Addressed By:
OE.Sec_Com	FTP_ITC.1, FCS_COP.1
OE.Key_Supp	FCS_CKM.1, FCS_CKM.2, FCS_CKM.4

TABLE 14. Removed

Security Objective
OE.Data_Store
OE.Pers
OE.Power
OE.Tamper

Security Functional Requirements suitable to achieve the security objectives

This chapter discusses why the identified SFRs and SARs are sufficient to satisfy the given objectives.

O.Crypt Cryptography is provided by *FCS_COP.1 Cryptographic operation*. This is supported through *FCS_CKM.1 Cryptographic key generation* and *FCS_CKM.4 Cryptographic key destruction* for the generation and validation of the associated secret information.

O.Data_Acc Data Access Control is provided by a combination of requirements. *FDP_ACF.1 Security attribute based access control* sets the basic rules through the access control SFPs named in *FDP_ACC.1 Subset access control* based on the named security attributes. Export and import of user data are controlled through *FDP_ETC.1 Export of user data without security attributes* and *FDP_ITC.1 Import of user data without security attributes.* When a complete isolation of information between service providers is desired the *FDP_IFF.1 Simple security attributes* sets the rules through the information flow control SFP named in *FDP_IFC.1 Subset information flow control* for using the optional card separation function.

O.Env_Strs Environmental Stress is provided by *FPT_FLS.1 Failure with preservation of secure state*. The correct operation of TOE is ensured by *FTP_ITC.1 Inter-TSF trusted channel.* The recovery of the TOE is provided for by *FPT_RCV.4 Function recovery*. The objective is ensured by *AVA_VLA.2 Low Resistant* which provides for a review of obvious vulnerabilities, including those dealing with manipulations outside defined operational boundaries. *FDP_SDI.1 Stored data integrity monitoring* ensure the integrity of the user data.

O.HW_Test Hardware testing is provided by *FPT_AMT.1 Abstract machine testing* that allows to verify the correct operation of the hardware that comprises part of this TOE.

O.I_Leak Information Leakage is provided by *AVA_VLA.2 Low Resistant.* This requirement reviews obvious vulnerabilities, including those dealing with the leakage of information from the TOE.

O.Ident TOE Identification is provided through the assurance requirements *Security Requirements for TOE Environment.* and *ACM_SCP.2 Problem tracking CM coverage,* which require the developer to uniquely identify the configuration items that constitute the TOE.

O.Init Initialization is provided through the following requirements. *FDP_SDI.1 Stored data integrity monitoring* provides for the protection of information that occupies an allocated resource. *FPT_FLS.1 Failure with preservation of secure state* and *FPT_RCV.4 Function recovery* provide for acceptably secure operation in the event of failures. The instance of power failure is of particular concern because of the stated unreliability of the power supply.

O.Life_Cycle Life Cycle Functions is provided by *FDP_ACF.1 Security attribute based access control* with the specification of the access control SFPs named in *FDP_ACC.1 Subset access control.* The implementation of these requirements in

the TOE is ensured by *AVA_VLA.2 Low Resistant* in the review of obvious vulnerabilities, including those dealing with manipulations outside defined boundaries and the assurance of secure responses to all logical commands.

O.Log_Prot Logical Protection is provided by the following requirements. The access control SFPs named in *FDP_ACC.1 Subset access control* and detailed in *FDP_ACF.1 Security attribute based access control* set the rules for accessing the data. *FDP_DAU.1 Basic data authentication* provides for the verification of the firmware stored on the TOE and *FDP_SDI.1 Stored data integrity monitoring* provides for the protection of the logical functions from the use of corrupted data. *FPT_ITI.1 Inter-TSF detection of modification* provide for protection of the logical functions from the input of corrupted data. *FPT_FLS.1 Failure with preservation of secure state* and *FPT_RCV.4 Function recovery* provide for acceptably secure operation in the event of failures. The instance of power failure is of particular concern due to the stated unreliability of the power supply.

O.Phys_Prot Physical Protection is provided by the requirement *AVA_VLA.2 Low Resistant*. *AVA_VLA.2 Low Resistant* provides the review of obvious vulnerabilities, including those involving the deconstruction and manipulation of the IC. The *FDP_SDI.1 Stored data integrity monitoring* requirement supports this objective through monitoring the stored data for integrity errors.

O.Power Power Loss Recovery is provided by a number of requirements. *FDP_SDI.1 Stored data integrity monitoring* provides for the detection of the stored user data corruption. *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 a power loss.

O.Reuse Replay is provided by *FPT_RPL.1 Replay detection* directly.

O.Sec_Com Secure Communications is provided by a variety of requirements. *FTP_ITC.1 Inter-TSF trusted channel* provides the establishment of a trusted channel. *FDP_ETC.1 Export of user data without security attributes* and *FDP_ITC.1 Import of user data without security attributes* provide the means of controlling the information which can be exchanged through imposition of the access control SFPs. *FPT_ITC.1 Inter-TSF confidentiality during transmission* provides for confidentiality of the TSF data traffic. *FPT_ITI.1 Inter-TSF detection of modification* provides for the TSF data exchange without modification.

O.Set_Up Set-Up Sequence is provided by the access control SFPs named in *FDP_ACC.1 Subset access control* and detailed in *FDP_ACF.1 Security attribute based access control.* The objective is also supported through *ADO_DEL.2 Detection of modification* and *ADO_IGS.1 Installation, generation, and start-up procedures.*

Rationale for refinements of Security Functional Requirements

FCS_CKM.1 Cryptographic key generation was refined to improve the readability of the resulting statement.

FCS_CKM.4 Cryptographic key destruction was refined to improve the readability of the resulting statement.

FCS_COP.1 Cryptographic operation was refined to improve the readability of the resulting statement.

FDP_IFF.1 Simple security attributes was refined to omit the unnecessary details and improve readability.

Security Assurance Requirements appropriate

The assurance level for this Security Target is EAL 4.

Security Requirements mutually supportive

This chapter addresses mutual support and dependencies between the Security Requirements.

Consistency and mutual support

The choice of the security requirements is justified as was shown above in “Security Functional Requirements suitable to achieve the security objectives” on page 78 and “Security Assurance Requirements appropriate” on page 81. The choice of SFRs and SARs was made based on the assumptions about, the objectives for, and the threats to the TOE and the security environment.

The SARs are appropriate for the level of assurance EAL4 that provides a low level of independently assured security. The identified metrics and SOF claim are commensurate with the EAL4 level of assurance.

Security Functional Requirements dependencies

The following table summarizes the dependencies of the Security Functional requirements and shows how they are satisfied.

TABLE 15. Removed

Security Functional Requirement	Depends on:	Satisfied by:
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	FCS_COP.1 included
	FCS_CKM.4	included
	FMT_MSA.2	See “Unsatisfied dependencies for FMT_MSA.2 and FMT_MSA.3” on page 85.
FCS_CKM.4	FDP_ITC.1 or FCS_CKM.1	both included
	FMT_MSA.2	See “Unsatisfied dependencies for FMT_MSA.2 and FMT_MSA.3” on page 85.
FCS_COP.1	FDP_ITC.1 or FCS_CKM.1	both included
	FCS_CKM.4	included
	FMT_MSA.2	See “Unsatisfied dependencies for FMT_MSA.2 and FMT_MSA.3” on page 85.
FDP_ACC.1	FDP_ACF.1	included
FDP_ACF.1	FDP_ACC.1	included
	FMT_MSA.3	See “Unsatisfied dependencies for FMT_MSA.2 and FMT_MSA.3” on page 85.
FDP_DAU.1	none	n/a
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1 included
FDP_IFC.1	FDP_IFF.1	inculded
FDP_IFF.1	FDP_IFC.1	included
	FMT_MSA.3	See “Unsatisfied dependencies for FMT_MSA.2 and FMT_MSA.3” on page 85.

TABLE 15. Removed

Security Functional Requirement	Depends on:	Satisfied by:
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1 included
	FMT_MSA.3	See "Unsatisfied dependencies for FMT_MSA.2 and FMT_MSA.3" on page 85.
FDP_SDI.1	none	n/a
FPT_AMT.1	none	n/a
FPT_FLS.1	ADV_SPM.1	included (see Chapter "TOE Security Assurance Requirements," on page 50)
FPT_ITC.1	none	n/a
FPT_ITI.1	none	n/a
FPT_RCV.4	ADV_SPM.1	included (see Chapter "TOE Security Assurance Requirements," on page 50)
FPT_RPL.1	none	n/a
FTP_ITC.1	none	n/a

Security Assurance Requirements dependencies

EAL4 is a self-contained package. Therefore the following table summarizes the dependencies of the Security Assurance Requirements resulting from EAL4 and shows how they are satisfied.

TABLE 16. Removed

Security Assurance Requirement	Depends on:	Satisfied by:
ADV_SPM.1	ADV_FSP.2	included in EAL4
	ADV_HLD.2	included in EAL4
	ADV_IMP.1	included in EAL4
	ADV_LLD.1	included in EAL4
	AGD_ADM.1	included in EAL4
	AGD_USR.1	included in EAL4

Unsatisfied dependencies for FMT_MSA.2 and FMT_MSA.3

The Security Functional Requirements listed here:

1. *FCS_CKM.1 Cryptographic key generation*
2. *FCS_CKM.4 Cryptographic key destruction*
3. *FCS_COP.1 Cryptographic operation*
4. *FDP_ACF.1 Security attribute based access control*
5. *FDP_IFF.1 Simple security attributes*
6. *FDP_ITC.1 Import of user data without security attributes*

depend on the Security Functional Requirements Family *FMT_MSA Management of security attributes.* The FMT_MSA family is intended to describe the behaviour of the system with respect to the control of security attributes by authorized users. Such control may include viewing and changing the security attributes, setting default values and specifying secure values for the security attributes of objects or subjects by the users assigned specifric roles.

The RC-S860 Contactless Smart Card does not support the notion of users or roles and cannot distinguish between authorized and unauthorized roles as long as conditions set forth in *FDP_ACC.1 Subset access control* and detailed in *FDP_ACF.1 Security attribute based access control* are met. The creation and management of subject attributes is, therefore, irrelevant.

The dependency of the FCS SFRs on FMT_MSA.2 relate to the need to ensure that any cryptographic key attributes are always assigned secure values. Since there are no cryptographic key attributes, this requirement is not relevant.

The dependency of FDP SFRs on FMT_MSA.3 relate to the need to ensure that when an object is created, the security attributes are initialized to appropriate default values. The only object attributes are the access key and the “insecure access” attributes, together with the authentication key stored in the card. The notion of assigning default values is not relevant for the cryptographic keys and there is no default value assigned to the “insecure access” attribute on creation of the object.

Security Functional Requirements are suitable to achieve the Security Objectives for TOE Environment.

OE.Sec_Com Reader/Writer Secure Communication is provided by *FTP_ITC.1 Inter-TSF trusted channel* which allows for establishment of a trusted channel between the environment and the TOE. *FCS_COP.1 Cryptographic operation* provides support for the necessary cryptographic operations in accordance with specified standards and guidelines

OE.Key_Supp Cryptographic Key Support is provided through a number of requirements. *FCS_CKM.1 Cryptographic key generation* provides for the secure cryptographic key generation, *FCS_CKM.2 Cryptographic key distribution* provides for the secure distribution of the cryptographic keys, and *FCS_CKM.4 Cryptographic key destruction* provides for the secure destruction of the cryptographic keys.

Rationale for not completing the assignment operations in Security Requirements for TOE Environment.

The following operations were not completed in the Chapter “Security Requirements for TOE Environment.,” on page 51:

Functional Requirement	Operation	Content of the operation
FCS_CKM.1	assignment	cryptographic key generation algorithm
FCS_CKM.2	assignment	cryptographic key distribution method
FCS_CKM.4	assignment	cryptographic key destruction method

These operations relate to the methods and algorithms that are performed by the environment of the TOE to support the cryptographic operations in that environment. Since there may exist different algorithms and methods satisfying the requirements, the choice of the particular algorithms and methods is left to the environment.

CHAPTER 9

Removed

As was demonstrated in the chapter “IT Security Functions” on page 56 the TOE Security Functions satisfy all Security Functional Requirements established in “TOE Security Functional Requirements” on page 44. The TOE assurance measures detailed in “Assurance Measures” on page 63 demonstrate that all Security Assurance Requirements described in “TOE Security Assurance Requirements” on page 50 are addressed. The choice of the SFRs and SARs was made based on the assumptions about, the objectives for, and the threats to the TOE and the security environment. Therefore the ST provides evidence that the Security Functions together with Assurance Measures counter all threats to the TOE.

Removed

CHAPTER 10

Version Information

This chapter provides the detailed version information for this Security Target document. The following table summarizes the changes applied to the document in chronological order.

TABLE 17. The version information for Security Target

Version	Release Date	Name	Summary of release
Ver1.0 Draft-01	24 June 2002	Koichiro Tokunaga	The first release.
Ver1.0 Draft-02	10 July 2002	Koichiro Tokunaga	Correction of Minor Error and Miss typo.
Ver1.0	20 August 2002	Albert Dorofeev Koichiro Tokunaga Hiroki Ebisawa	Release Ver1.0.