LG CNS

XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/S3CT9K9 Security Target Lite V1.1

문서 ID: XSMART Openplatform V1.1_ASE_Lite_V1.1

[Revised history]

Version	Revised item	Revised contents	Date of issue	Approval
1.0	All	Initial Version	2014.08.21	LMH
1.1	Partial	OR apply	2014.09.16	LMH

[List of Contents]

References

[CC]	Common Criteria for Evaluation of IT Security, Version 3.1r4, CCBM-2012-09-001
[CEM]	Common Criteria Methodology for Evaluation of IT Security, Version 3.1r4, CCBM-2012-09-004,
[OSCPP]	Smart Card Open Platform Protection Profile V2.2, 2010.12.20
[GPCS]	GlobalPlatform Card Specification, Version 2.1.1, GlobalPlatform Inc., March 2003.
[GPST]	GlobalPlatform Smart Card Security Target Guidelines, Version 1.0, GlobalPlatform Inc., October 2005.
[GPSR]	GlobalPlatform Card Security Requirements Specification, Version 1.0, May 2003.
[VGP]	VISA GlobalPlatform 2.1.1 Card Implementation Requirements, Version 2.0, VISA, July 2007.
[VGPG]	VISA GlobalPlatform 2.1.1 Card Production Guide, Version 1.0, VISA, February 2004.
[JCVM]	Java Card Platform 2.2.2, Virtual Machine Specification, Sun Microsystems, October 2005.
[JCRE]	Java Card Platform 2.2.2, Runtime Environment Specification, Sun Microsystems, October 2005.
[JCAPI]	Java Card Platform 2.2.2, Application Programming Interface, Sun Microsystems, October 2005.
[ICST]	Security Target Lite of Samsung S3CT9KW/S3CT9KC/S3CT9K9 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software, Version 2.2, 2012. 09. 26
[JCSPP]	Java Card Protection Profile – Open Configuration ANSSI-CC-PP-2010/03-M01

Terms and Definition

Terms that are used in this document follow the meaning defined in the CC if they also defined in the CC.

EEPROM(Electrically Erasable Programmable Read-Only Memory)

This is non-volatile memory device that stably remembers memory over a long period of time without requiring power. As a modified version of EPROM (Electrically Programmable Read-only Memory), EEPROM can electrically erase and re-record data.

IC Chip(Integrated Circuit Chip)

As an important semiconductor to process the functions of Smart Card, IC chip is a processing device that includes the four functional units of mask ROM, EEPROM, RAM and I/O port.

RAM(Random Access Memory)

RAM is a storage that maintains operating system application program and the currently used data in order to enable quick access by computer processor

ROM(Read-Only Memory)

As a semiconductor memory device, ROM can read, but cannot change contents.

Applet

The name given to any Java Card technology-based application

Application Protocol Data Unit(APDU)

Application Protocol Data Unit, an ISO 7816-4 defined communication format between the card and the off-card applications

Card Manager

A generic term that refers to the entity that performs the card from the card management function

Card Production Life Cycle(CPLC) Data

Data to identify the manufacturer and the smart card issuer information

Cardholder Verification Method(CVM)

Method for proving that the person issuing the card is the person who presents the card

GlobalPlatform(GP) Registry

Storage for managing the applications installed in the card and information

Issuer Security Domain(ISD)

Substance on the card that performs the management, security and communication on behalf of the Issuer

Open Platform Environment(OPEN)

Software entity that manages the card GlobalPlatform Registry

Secure Channel

Communication mechanisms to ensure the security on the card to communicate with entities outside of the card process,

Personalization

The process of mounting the platform and the application data for the user

Personalization Agent

Authority to issue and collect personal information with your application and personal data

MAC Key (Key for Message Authentic Code)

Key for the symmetric key encryption algorithm in accordance with ISO 9797 in order to generate a message authentication code for the data to prevent forgery

RMI (Remote Method Invocation)

Technique of calling the remote object on the card in the terminal

1. Security Target Introduction

This section provides the information necessary for identifying and controlling security target and TOE.

1.1. Security Target Reference

Subject	XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/S3CT9K9 Security Target Lite
Version	V1.1
Author	LG CNS
Evaluation Assurance Level	EAL4+ (ATE_DPT.2, AVA_VAN.4)
Date	2014.09.16
IC Chip	S3CT9KW/S3CT9KC/S3CT9K9
Keywords	Smartcard, cos, ic chip, smartcard acceptance device, openplatform, javacard
ST Identification	XSMART Openplatform V1.1_ASE_LITE_V1.1

1.2. TOE Reference

Subject	XSmart OpenPlatform V1.1 on S3CT9KW/S3CT9KC/S3CT9K9
Version	V1.1
Author	LG CNS
Component of TOE	-Embedded Software(Operating System): XSmart OpenPlatform V1.1 -User's Guide for managent (XSmart OpenPlatform V1.1_AGD_V1.0) -Platform TOE: Samsung S3CT9KW/S3CT9KC/S3CT9K9 16bit RISC Microcontroller for Smart Card, Revision 2 with optional Secure RSA/ECC V2.2 Library including specific IC Dedicated Software
TOE code identification	- ROM CODE identification: XSMART_OPEN110_KW_m01.rom XSMART_OPEN110_KC_m01.rom XSMART_OPEN110_K9_m01.rom

	- EEPROM CODE identification: XSMART_OPEN110_KW_m01.eep XSMART_OPEN110_KC_m01.eep XSMART_OPEN110_K9_m01.eep
IC Chip	S3CT9KW/S3CT9KC/S3CT9K9
Reference of IC Chip Authentication	ANSSI-CC-2012/70

1.3. TOE Overview

The type of TOE is a smartcard consisting of embedded S/W(Open Platform COS) and IC Chip, and is composite TOE.

The TOE is complaint with JavaCard Specification(Java Card 2.2.2 Runtime Environment Specification[JCRE], Java Card 2.2.2 Virtual Machine Specification[JCVM], Java Card 2.2.2 Application Programming Interfaces[JCAPI], referred to as 'JavaCard Spec' hereafter), GlobalPlatform Specification(GlobalPlatform Card Specification 2.1.1[GPCS], referred to as 'GP Spec' hereafter), and Visa GlobalPlatform - Configuration 3 Specification(Visa GlobalPlatform 2.1.1 Card Implementation Requirements[VGP] - Configuration 3, referred to as 'VGP Spec' hereafter). TOE does not support the Multiple Security Domain of VGP Configuration 3

In order to make TOE to be operated correctly as a product, non only the physical interface of IC chip, which is the scope of the composite TOE, is required, but also the contact and the contactless interfaces are required in the case of manufactured as a smartcard type. However, this feature is not included in the TOE scope.

S3CT9KW/S3CT9KC/S3CT9K9 is a contact/contactless IC chip of Samsung Electronics and it is certified by CC from BSI.

- Protection Profile : Security IC Platform Protection Profile, Version 1.0, June 2007, BSI-PP-0035
- TOE identity : Samsung S3CT9KW/S3CT9KC/S3CT9K9 16bit RISC Microcontroller for Smart Card, Revision 2 with optional Secure RSA/ECC V2.2 Library including specific IC Dedicated Software
- Certification Number : ANSSI-CC-2012/70

- Assurance Level : CC EAL 5+ (AVA_VAN.5, ALC_DVS.2)
- Certified cryptography library : TORNADO 2MX2 Secure RSA/ECC library v2.2

To protect TOE itself, TOE data and important user data from unauthorized access and exposure, TOE provides smart card platform functions related with Managemet of application, Separation execution area between applications, Life cycle management of smart cards and applications, user identification and authentication., etc

TOE conforms to EAL 4+ and provides a function to install/delete a variety of applications through the secured communication channel. Depending on applications installed and issued, TOE is used as a credit card, a transportation card, and identity card., etc.

1.4. TOE description

1.4.1. TOE operational environment

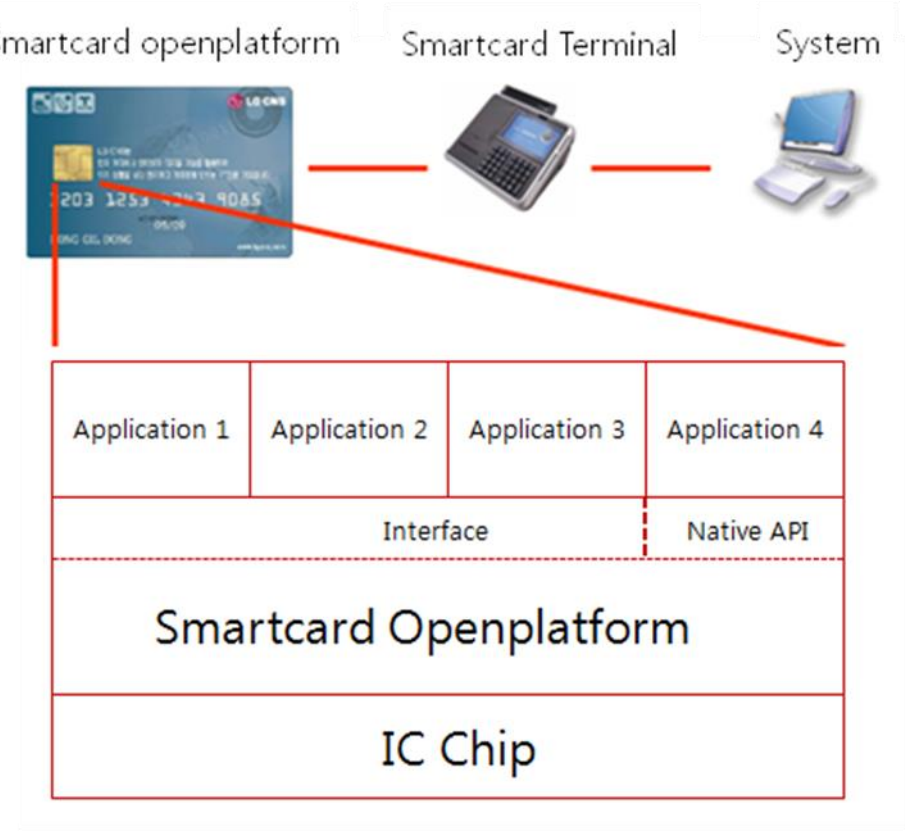


Figure 1 Smart Card Operational Environment

The Figure1 shows the structure of the open platform smart cards in which the TOE is included and the smart card operational environment.
Smart card holder and issuer do the task through the communication with the smartcard terminal.
The card issuer performs the TOE management tasks such as the application installation and the card holder uses the function of the application installed in TOE by using a smartcard terminal.

In order to run an application installed on the TOE, first of all select must be executed from terminal commands. The selected application to be executed, receives the command from a smartcard terminal and performs its function.
Card issuer can perform the management tasks such as the installation or deletion of applications, the personalization of applications and changing the life cycle of the application by using a smartcard terminal.
Even if the card holder or application provider, without explicit authentication they can not

install or delete application in TOE. And Authentication is necessary for card holder to use application's service installed by the card issuer.

Because a card holder's PIN(Personal Identification Number) is saved, it is impossible for others to use TOE, the card issuer's encryption key and the algorithm embedded in smartcard prevent attacks from outer environment. Also since the encryption algorithm is performed by the unique number of the smart card, it is impossible to clone and The high security system can be designed based on the International Standard security architecture

1.4.2. TOE Scope

TOE is composed of Smart Card Platform based on Open Platform and Global Platform, OS embedded in IC chip, IC chip H/W, Firmware, RSA/ECC crypto library.

The Open Platform based on Java Card is masked in ROM area of IC chip, is complaint with Java Card 2.2.2 and Visa GlobalPlatform 2.1.1-Configuration 3, and includes API interface for Java Card applications.
For extending functions of Open Platform based on Java Card, all application is not in TOE scope but user data.

Physical scope of TOE

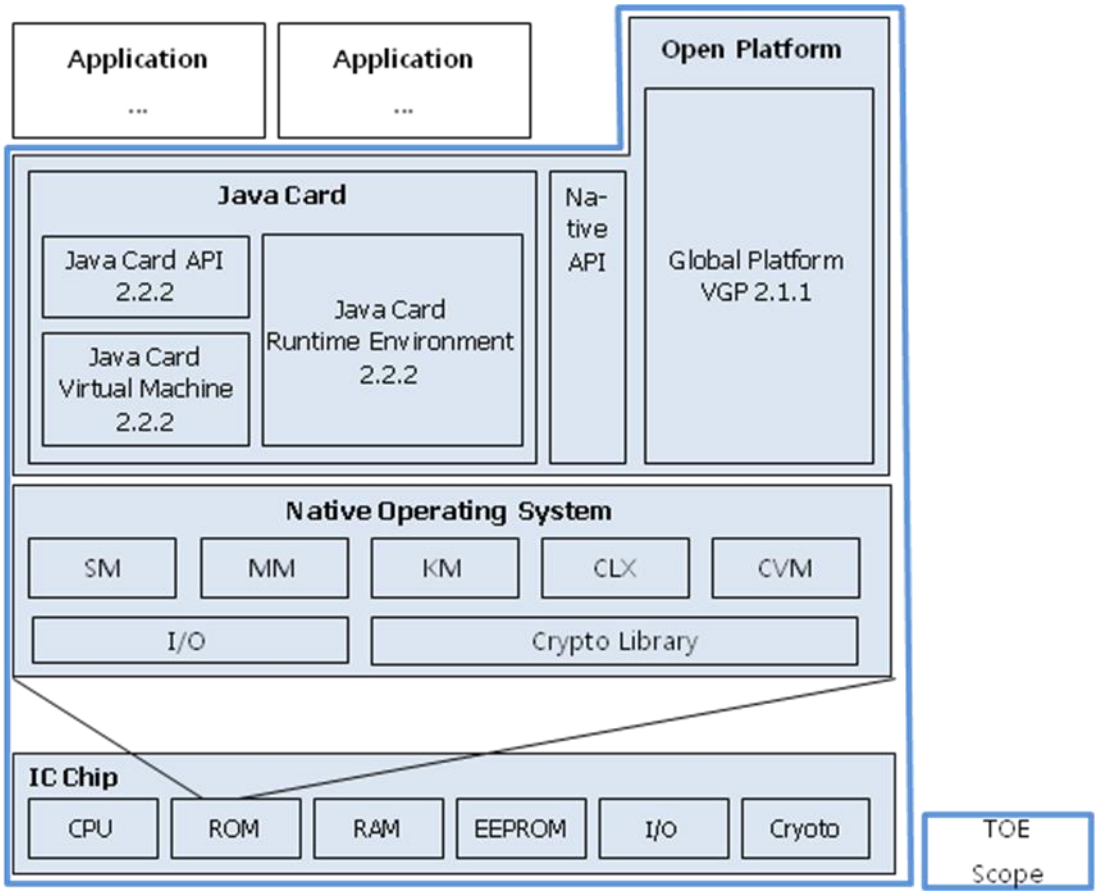


Figure 2 Scope and boundary of TOE

The TOE code, which is .rom file is masked in ROM area and .eep file is used for manufacture's initialization during chip manufacturing.

The IC chip, SAMSUNG's S3CT9KW/S3CT9KC/S3CT9K9 has a CCRA EAL5+ assurance level, and consists of IC chip H/W, firmware in ROM, crypto S/W library with certificate scope.

IC chip H/W

- 16 bit micro processor(CPU)
- 6KB RAM(RAM), 2.5KB Crypto RAM, 384KB ROM, 144/80/36KB EEPROM (S3CT9KW/S3CT9KC/S3CT9K9)
- Memory protection unit(MPU), random generator(RNG), timer(TIM), DES calculation engine(DES), method calculation engine (TORNADO 2Mx2)
- RF interface, address and data bus(ADBUS)

S/W library for crypto calculation

- RSA/ECC library
  ECDSA key generation
  ECDSA sign/verify
  ECDH key sharing
  RSA key generation
  RSA sign/verify
  Hash function(SHA-1,SHA-224, SHA-256, SHA-384, SHA-512)
- True random generator (TRNG)

IC chip H/W design is below.

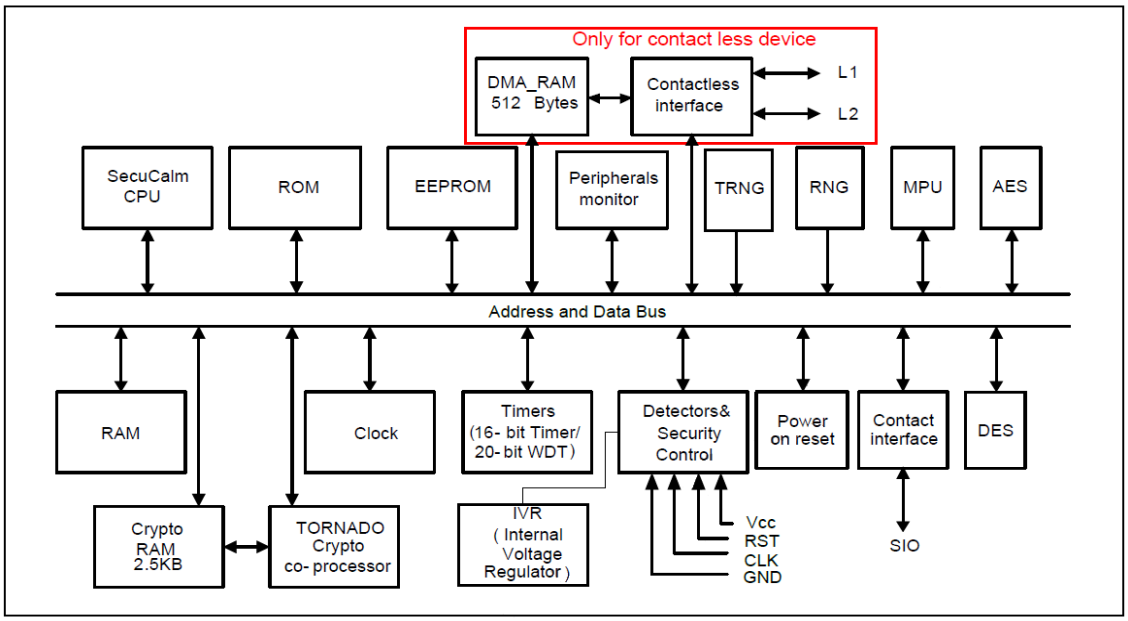


Figure 3 IC chip H/W design

The IC chip hardware among the IC chip composition elements provides DES module used in the symmetric key encryption according to DES and TDES standards, Tornado 2MX2 Crypto module used in the asymmetric key encryption, physical security measures such as shield, temperature sensor, voltage sensor, and filter, and non-determinant hardware random number generator. The firmware provides IC chip hardware management function such as EEPROM recording and the function for hardware testing, and the cryptographic calculation software library provides calculations such as digital signature generation/verification for hash value, ECDH key exchange, ECC/RSA key pair generation, and ECC/RSA public key verification

RSA/ECC Library V2.2

The ECC/RSA library certified with CCRA EAL5+ assurance level is a part of IC chip composition elements and the IT environment of TOE are not included in TOE scope.

ECC Library

The ECC library provides functions such as ECDSA digital signature generation and verification, ECDH key exchange, ECC key pair generation, and ECC public key verification. In TOE, however, only the functions of ECDSA digital signature generation and verification and ECDH key exchange are used. The ECC library includes countermeasures against SPA, DPA, EMA, DFA and such

RSA Library

The RSA library provides functions such as RSA digital signature generation, verification, and key pair generation. The RSA library also includes countermeasures against SPA, DPA, EMA, DFA and so on.

In addition, this library includes functions of SHA-224, SHA-256, SHA-384, SHA-512.

The final distributions of TOE are same below,

Classification		TOE	Name
TOE	SW	ROM code	XSMART_OPEN110_XX_m01.rom (XX means KW, KC, K9)
		EEPROM code	XSMART_ OPEN110_XX_m01.eep (XX means KW, KC, K9)
	HW	Chip identity	S3CT9KW/S3CT9KC/S3CT9K9
manual(file)		manual	User manual (XSmart OpenPlatform V1.1_AGD_V1.2)

Logical scope of TOE

The card manager provides management functions of open platform described in 'GP Spec' and 'VGP Spec'. The card manager provides load, installation, deletion, management of issued data and authentication information, management life cycle of application and OS by issuer authentication using SCP02 security mechanism.

Runtime Environment

The runtime environment provides Java Card platform's JCRE, JCVM, JCAPI functions described in 'Java Card Spec'. For normal execution of application on smart card, the

runtime environment provides TSF protection function like firewall, transaction, deletion residual information and crypto calculation to application on smart card.

Operational Environment

Operational Environment includes development as to a part of the Java Card platform-dependent hardware and ic chip operation, H/W resource management, native OS for high performance.

Logically, TOE is composed of card manager to perform smartcard's management functions, runtime environment to provide application's runtime environment, operating system to support access to H/W resource and asset.

As the card manager is a component to perform smartcard's manager function, it forces security policy of card issuer and provides functions like management of card and application's life cycle, of logical channel between terminal, of secure channel between card manager, of APDU command delivery to applications (currently active applet), of PIN for holder authentication shared by all applications**.**

- Administration Command Control
  The only card command specified in [VGP] is processed, for commands that do not conform to the specifications it returns the appropriate error message. Also It controls whether the card management commands can be processed according to the state of card.
- Card Content Management
  Is Charge of load, installation, deletition an application.
- Life Cycle Management
  Controls the life cycle of an application installed on the card and the card defined on the GlobalPlatform
- Open Platform Enviironment(OPEN)
  Enable and select a application, transmit received command. For developing card management service, it initializes internal data structure and manages them.
- Host Authentication (SCP02)
  Using host authentication by secure channel, it provides card manager's authentication function. This function guarantees message integrity exchanged over a secure channel and message security by message encryption for secure data. When secure channel is

closed, this function deletes session key used and initialize security level.

Runtime Environment interpretes application's execution code and provides execution area to each application for executing application. it does support functions related to application load, installation, deletion and supports transaction, application's PIN management, encryption, communication, remote method invocation.

- Resource Quotas
  Manage the limitations of the use of resources granted to the application
- Java Card Firewall
  Controls the sharing of Java objects between different applications or between applications and runtime environment.
- Remote Access Control
  Controls remote terminal access to Java objects over RMI
- Clearing Sensitive Information
  At the time of resource allocation and return, the remaining data do not exist.
- Atomic Transactions
  Supports to allow only return to the previous state of the execution of all operations or succeeds of all operations on a sequential task related to allocation and modification to EEPROM.

Operating System supports management functions for underlying H/W resource. Also, it provides low level crypto calculation using crypto co-processor like memory allocation and free RAM/EEPROM, access to IO device, low level transaction.

- CVM
  Provides PIN validation and management for security property of Global PIN shared by all applications in the platform. This function supports management of Owner PIN defined in application's itself.
- Crypto function
  Supports for the signature generation and verification, encryption and decryption, the hash value generation, the random number generation .
- Native API
  The TOE provides native APIs for data group creation and access (supporting development of e-Passport in accordance with "ICAO Doc 9303" and Driving License in accordance with "ISO/IEC 18013"), and the TOE provides native APIs for data integrity verification of secure transaction.

- Crypto algorithms
  The supported algorithms are table below

Table 1 TOE algorithm and usage

Algorithm	Usage
AES (128,192,256 bits) in ECB/CBC	DATA En/Decryption, MAC generation/verification
ARIA (128,192,256 bits) in ECB/CBC	DATA En/Decryption, MAC generation/verification
SEED (128 bits) in ECB/CBC	DATA En/Decryption, MAC generation/verification
TDES (128, 192 bits) in ECB/CBC	DATA En/Decryption, MAC generation/verification
RSA(1408, 1984, 2048 bit)	DATA En/Decryption, digital signature generation and verification
ECDSA (192, 224, 256 bit)	digital signature generation and verification
ECDH (192, 224, 256 bit)	Key Agreement protocol
SHA 224/256/384/512	HASH value generation

In composite TOE, SHA1 is implemented separatly by S/W. SHA1 performing alone is NON-TSF but RSA with SHA1 and ECDSA with SHA1 required in Javacard specification are included in TSF.

Functions excluded from the TOE

Crypto functions which IC Chip provides are not certified range of IC Chip, are excluded from the scope of the composite TOE.

Table 2 Functions excluded from the TOE

Division	Details
Crypto	DES 64bit RSA 512,640,768,1024,1152 bit
HASH	SHA-1
Digital Signature	RSA(ISO9796) 512,640,768,1024,1152 bit
	RSA(PKCS#1) 512,640,768,1024,1152 bit

NON-TSF

Functions below are scope of TOE, but excluded in TSF

Division	Details
Crypto	RSA-CRT, SHA-1 used alone DES 64bit, RSA 512,640,768,1024,1152 bit
[VGP]	DAP Verification

	*In VGP specification, DAP Verifcation uses RSA-1024 during signature verification operation, But RSA-1024 is not certification scope, this is non-TSF. *It is not signature creation but signature verification using public key, so dap verication doesn't effect TSF's secure operation.
Native API	**<eID>** • native public short CipherQuick(byte mode, byte[] inBuff, short inOffset, short inLength, byte[] outBuff, short outOffset); • native public short SignQuick(byte[] inBuff, short inOffset, short inLength, byte[] sigBuff, short sigOffset); • native public boolean VerifyQuick(byte[] inBuff, short inOffset, short inLength, byte[] sigBuff, short sigOffset, short sigLength); • native public short unprotectedCAPDUQuick(byte[] ssc, short sscOffset, short apduLength); • native public short protectedRAPDUQuick(byte[] ssc, short sscOffset, short apduLength, short sw12) **<Patch Code, Get Patch Code>** For setting I/O protocol, it does not affect the safe operation TSF because it does not modify the information related to security functions of IC chip.

Functions that are not available

In Java Card and VGP Spec, Functions below are not supported by TOE.

Division	Details
[JCAPI]	<API> javacard.biometry javacard.framework.util.intx

	<Security Constants : javacardx.crypto.Cipher> ALG_DES_CBC_PKCS5, ALG_DES_ECB_PKCS5, ALG_RSA_ISO14888, ALG_RSA_PKCS1_OAEP <Security Constants : javacard.security.MessageDigest > ALG_MD5, ALG_RIPEMD160 <Security Constants : javacard.security.Signature> ALG_DES_MAC4_ISO9797_1_M2_ALG3, ALG_DES_MAC4_PKCS5, ALG_DSA_SHA, ALG_HMAC_MD5, ALG_HMAC_RIPEMD160, ALG_HMAC_SHA_256, ALG_HMAC_SHA_384, ALG_HMAC_SHA_512, ALG_HMAC_SHA1, ALG_RSA_MD5_PKCS1, ALG_RSA_MD5_PKCS1_PSS, ALG_RSA_MD5_RFC2409, ALG_RSA_RIPEMD160_ISO9796, ALG_RSA_RIPEMD160_ISO9796_MR, ALG_RSA_RIPEMD160_PKCS1, ALG_RSA_RIPEMD160_PKCS1_PSS, ALG_RSA_SHA_ISO9796_MR, ALG_RSA_SHA_PKCS1_PSS, ALG_RSA_SHA_RFC2409 <Security Constants : javacard.security.KeyBuilder> LENGTH_DSA_1024, LENGTH_DSA_512, LENGTH_DSA_768, LENGTH_EC_F2M_113, LENGTH_EC_F2M_163, LENGTH_EC_F2M_193, LENGTH_HMAC_SHA_1_BLOCK_64, LENGTH_HMAC_SHA_256_BLOCK_64, LENGTH_HMAC_SHA_384_BLOCK_128, LENGTH_HMAC_SHA_512_BLOCK_128 <Security Constants : javacard.security.KeyPair> ALG_DSA, ALG_EC_F2M, ALG_RSA, ALG_RSA_CRT
[VGP]	Delegated Management

1.4.3. TOE life cycle

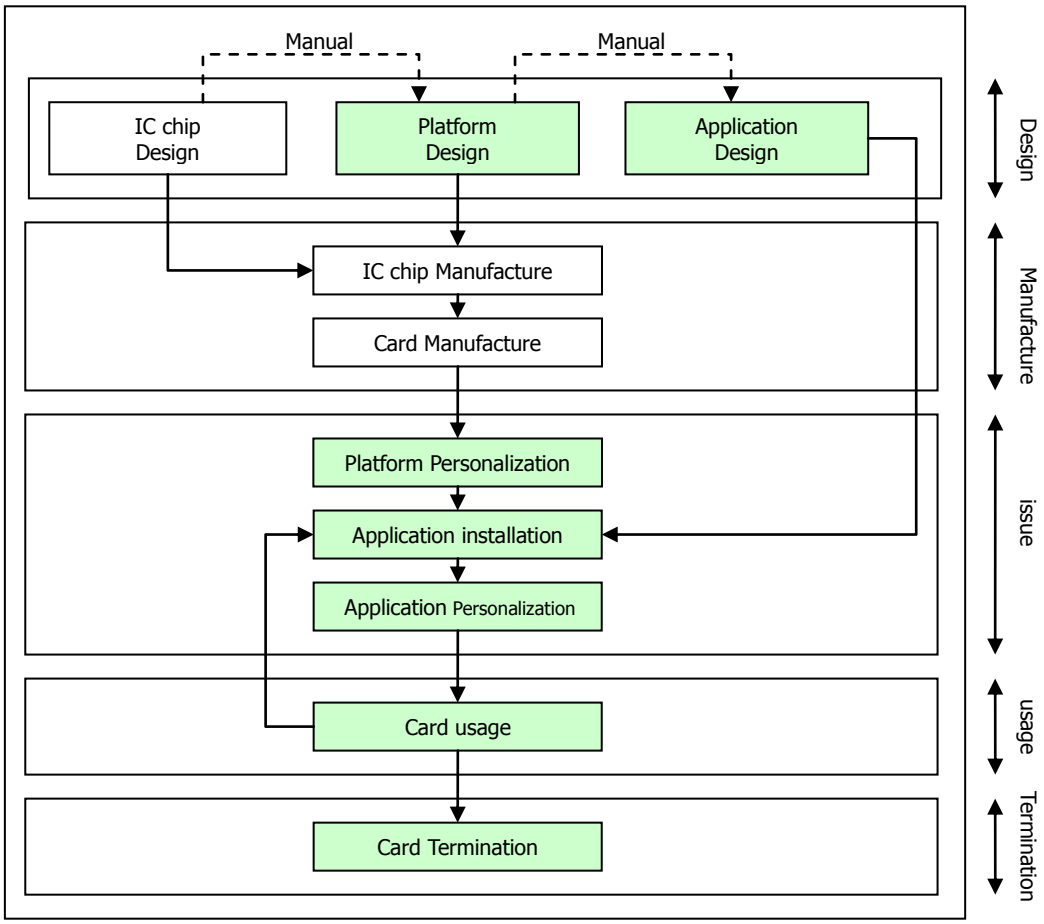


Figure 4 Life Cycle of TOE

The Life Cycle of TOE is consisting of 5 steps, which is design, manufacture, issue, usage and termination defined in Open Platform smartcard Protect Profile. At each life cycle various users are involved with different roles. Figure 4 show TOE's Life Cycle.

Step 1: Design

This step is S/W and IC Chip design step like card operation, interface between application and OS, application.

- IC chip Manufacturer

  Normally IC chip Manufacturer has a IC chip developed and designed by itself, and provides IC chip manual , interface library, manual with platform developer.
- Platform Developer

Develops platform using manual by IC chip manufacturer. And provides manual for platform interface with application developer.

- Application Provider
  develops an application that performs a particular function, using manual by platform developer.

Step 2: Manufacture

It consist of ROM masking with designed platform, IC chip manufacturing, packaging, card manufacturing using packaged IC chip. In case contactless smartcard it embed antenna to smartcard and complete it.

- IC chip Manufacturer
  Platform is masked in ROM and manufacture IC chip , it is packed to module or COB type for card or chip manufacture.
- Card Manufacturer
  The Packaged module or COB type is manufactured to a card or a passport type. in case of contactless smartcard, antenna is embedded on it.

Step 3: Issue

The manufactured card is delivered to issuer, for final usage issuer installs an application on the card and writes user data, and then delivers it.

- Card Issuer
  Modifies a manufactured card to the status can be used over specified process, application is installed to card depending on the purpose of card.
- Card Enabler
  After getting authority from card issuer, Card Enabler modifies card status to the status can be used over platform personalization.
- Application Loader
  After getting authority from card issuer, Card Enabler installs a application depending on the purpose of card.
- Personalization Agent
  After getting authority from card issuer, Personalization Agent writes user data in installed application.

Step 4: Usage

Card Holder, After getting personalized card, uses it correctly depending on the purpose

of card. In case expanding the function of the smart card, Card Issuer installs additional application.

- Card User.
  Card user requests the identification of the card owner.
- Card Holder
  Attempts to use the card properly.
- Card Issuer
  During use, If further extension of the functionality of the smart card is necessary, card issuer organizes the post issuance like application loading, personalization
- Terminal
  Terminal is an IT system that communicates with the TOE.

Step 5: Termination

Holder, card use is finished, can return the card to the issuer and, the issuer processes cards completely useless .

- Card Issuer
  Card Issuer makes the card completely useless.

1.5. Writing Rules

The notation, formatting and conventions used in this ST are consistent with the Common Criteria for Information Technology Security Evaluation (hereafter referred to as "CC"). In addition to this, additional writing rules are defined and used to prevent any confusion with operations that are already performed in the Protection Profile conformed to by this security target.
The Common Criteria allows selection, assignment, refinement, and iteration operations which can be executed in the Security Functional requirement. Each operation is used in the ST by the following types.

Iteration
This is used when a component is repeated with varying operations. The result of iteration operation is represented by iteration number with round bracketed, that is, (Iteration number).
Assignment

This is used to assign specific values to unspecified parameters (e.g., password length). The result of an assignment is represented by square brackets, that is, [Assignment Value].

Selection

This is used to select one or more options provided by the CC in stating a requirement. The result of selection operation is represented by *underlined italics*.

Refinement

This is used that a requirement to be "stricter" than the original by adding detail to a requirement. It therefore restricts a requirement further. The result of a refinement is represented by **bold text**.

2. Security target organization

References provide information on data that this document has referred to for users interested in this security target wishing to obtain further background or relevant information above what is specified here. The list of abbreviations is offered for better understanding of frequently used terms or abbreviations.

Section 1 provides security target references, TOE references, overview, and descriptions of TOE.
Section 2 provides the conformance claims that declare conformance for Common Criteria, Protection Profile, and Package and describes rationale of the conformance claims and methodology for conformance to the Protection Profile.
Section 3 describes the security problems and includes security problems of TOE and its operational environment in terms of threat, organizational security policy, and assumption.
Section 4 describes TOE security objectives and security objectives for the operational environment to counter to threats identified in the security problem definition, perform organizational security policies, and supporting assumptions.
Section 5 defines extended components, explaining components extended in Part 2 or Part 3 of the Common Criteria.
Section 6 describes the IT security requirements including the security functional and assurance requirements and rationale of security requirements intended to satisfy security objectives.

Section 7 summarizes TOE specification and explains security functionality implemented in the TOE.
Section 8 compares compatibility between Composite ST and Platform ST.
Section 9 defines the references and abbreviations used in this ST.

3. Conformance claims

This section provides a description of the Common Criteria, Protection Profile and Package that conform to Security Target..

3.1. CC Conformance Claim

This ST conforms to the following Common Criteria.

- Common Criteria Identification
  - Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012, CCMB-2012-09-001
  - Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002
  - Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003

- Conformance to Common Criteria
  - Extended to Conformance to Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 4
  - Conformant to Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 4

3.2. PP Conformance Claim

This ST conforms to the following Protection Profile.

- Smart Card Open Platform Protection Profile V2.2 [OSCPP](KECS-PP-0097a-2008), June 10, 2010
- Assuanrace Level: EAL4+ (ATE_DPT.2, AVA_VAN.4)

The IC chip of TOE is conforming to Protection Profile as follows

- Protection Profile Identification : Security IC Platform Protection Profile, Version 1.0, June 2007, BSI-PP-0035
- Evaluation Assurance Level : ANSSI-CC-2012/70
- Assurance Package : CC EAL 4+ (AVA_VAN.5, ALC_DVS.2)

3.2.1. Protection Profile Re-establishment

The following are the items of security target which re-established the protection profile.

Operational Environment

- [None]

Security Objective

- [None]

Security Functional Requirement

- FAU_ARP.1, FAU_SAA.1
- FCS_CKM.1, FCS_CKM.4, FCS_COP.1
- FDP_ACC.2, FDP_ACF.1, FDP_RIP.1
- FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.4, FIA_UAU.6, FIA_UID.1
- FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_SMF.1, FMT_SMR.1
- FPT_FLS.1, FPT_RCV.3, FPT_RCV.4, FPT_TST.1

Security objectives for operational environment

- FPR_UNO.1

3.2.2. Protection Profile Additions

The items described below are additional to the protection profile for this security target.

Security Environment

- [NONE]

Security Objective

- **[NONE]**

Security Function Requirement

- FCS_CKM.3, FCS_RNG.1
- FDP_UCT.1, FDP_UIT.1
- FPT_PHP.3

3.3. Package Claim

This Security Target is conforming to assurance package as follows

.

- Assurance Package : EAL4+ (ATE_DPT.2, AVA_VAN.4)

Addiontional assuarance packages:

- ATE_DPT.2 (Testing: modules)
- AVA_VAN.4 (methodical vulnerability analysis)

This Security Target's IC Chip is conforming to assurance package as follows

- Assurance Package : EAL5+ (ALC_DVS.2, AVA_VAN.5)

Addiontional assuarance packages:

- ALC_DVS.2 (Sufficiency of security measures)
- AVA_VAN.5 (methodical vulnerability analysis)

3.4. Rationale of Conformance Claim

- The Security Target meet includes all assurance requirements of OSCPP

3.4.1. Rationale of Conformance Claim for Security problem definition

The following tables show that the security objectives of composite security target is consistent to [OCSPP]. This security target redefines [A.UNDERLYING_HARDWARE]

Protection Profile	Security Target	Rationale
A.TRUSTED_PATH	A.TRUSTED_PATH	

A.APPLICATION_PROGRAM	A.APPLICATION_PROGRAM	Conformance
A.TOE_MANAGEMENT	A.TOE_MANAGEMENT	Conformance
A.TSF_DATA	A.TSF_DATA	Conformance
A.UNDERLYING_HARDWARE	-	Refinement Because composite TOE includes IC Chip, Assume of IC chip is excluded and is refined as O.UNDERLYING_HARDWARE
T.LOGICAL_ATTCK	T.LOGICAL_ATTCK	Conformance
T.ISSUANCE_MISUSE	T.ISSUANCE_MISUSE	Conformance
T.ILLEGAL_TERMINAL_USE	T.ILLEGAL_TERMINAL_USE	Conformance
T.ILLEGAL PROGRAM	T.ILLEGAL PROGRAM	Conformance
T.UNINTENTIONAL_FAILURE	T.UNINTENTIONAL_FAILURE	Conformance
T.CONTINUOUS_AUTHENTICATION_ATTEMPT	T.CONTINUOUS_AUTHENTICATION_ATTEMPT	Conformance
T.INTENTIONAL_TRIGGERING_OF_FAILURES	T.INTENTIONAL_TRIGGERING_OF_FAILURES	Conformance
T.RESIDUAL_INFORMATION	T.RESIDUAL_INFORMATION	Conformance
T.INFORMATION_DISCLOSURE	T.INFORMATION_DISCLOSURE	Conformance
P.Open platform	P.Open platform	Conformance
P.Duty separation	P.Duty separation	Conformance
-	T.SID.1	Addition the changes made to [JCSPP] is added
-	T.SID.2	
-	T.RESOURCES	
-	P.Verivication	

3.4.2. Rationale of Conformance Claim for Security Objective

This Security Target claims for all security objects provided in [OSCPP]

Protection Profile	Security Target	Rationale
O.DATA_PROTECTION	O.DATA_PROTECTION	Conformance
O.ISSUANCE	O.ISSUANCE_DELETION	Modification Deletion function is added
O.IDENTIFICATION	O.IDENTIFICATION	Conformance
O.AUTHORIZED_FAILURE_REPAIR	O.AUTHORIZED_FAILURE_REPAIR	Deletion Duplication with O.ISSUANCE, O.IDENTIFICATION, O. AUTHENTICATION
O.AUTHENTICATION	O.AUTHENTICATION	Conformance
O.AUTOMATED_RECOVERY	O.AUTOMATED_RECOVERY	Conformance
O.RESIDUAL_INFORMATION_DELETION	O.RESIDUAL_INFORMATION_DELETION	Conformance
O.INFORMATION_DISCLOSURE_HANDLIN	O.INFORMATION_DISCLOSURE_HANDLIN	Conformance
O.OPEN_PLATFORM	O.OPEN_PLATFORM	Conformance
-	O.HARDWARE	Addition Due to composite TOE, Underlying hardware in external environment is re-established as security objectives
-	O.AUDIT	Addition Due to Deletion O.Authorized_Failure_Repair , new security related audit objectives is added
OE.TRUSTED_COMMUNICATION	OE.TRUSTED_COMMUNICATION	Conformance
OE.TSF_DATA	OE.TSF_DATA	Conformance
OE.TRAINING	OE.TRAINING	Conformance
OE.UNDERLYING_HARDWARE	-	Deletion Due to composite TOE, Underlying hardware in external environment is re-established as security

		objectives
OE.APPLICATION_PROGRAM	OE.APPLICATION_PROGRAM	Conformance

3.4.3. Rationale of Conformance Claim for Security Funcational Requirement

This Security Target claims for all security objects provided in [OSCPP]

Protection Profile	Security Target	Rationale
FAU_ARP.1	FAU_ARP.1	Assignment
FAU_SAA.1	FAU_SAA.1	Assignment
FCS_CKM.1	FCS_CKM.1	Assignment
FCS_CKM.4	FCS_CKM.4	Assignment
FCS_COP.1	FCS_COP.1	Assignment
FDP_ACC.2	FDP_ACC.2	Assignment
FDP_ACF.1	FDP_ACF.1	Assignment
FDP_RIP.1	FDP_RIP.1	Assignment and Selection
FIA_AFL.1	FIA_AFL.1	Assignment and Selection
FIA_ATD.1	FIA_ATD.1	Conformance
FIA_SOS.1	FIA_SOS.1	Assignment
FIA_UAU.1	FIA_UAU.1	Assignment
FIA_UAU.4	FIA_UAU.4	Assignment
FIA_UAU.6	FIA_UAU.6	Assignment
FIA_UID.1	FIA_UID.1	Assignment
FMT_MOF.1	FMT_MOF.1	Assignment
FMT_MSA.1	FMT_MSA.1	Assignment and Selection
FMT_MSA.3	FMT_MSA.3	Assignment and Selection
FMT_MTD.1	FMT_MTD.1	Assignment and Selection
FMT_MTD.2	FMT_MTD.2	Assignment
FMT_SMF.1	FMT_SMF.1	Assignment
FMT_SMR.1	FMT_SMR.1	Refinement
FPR_UNO.1	FPR_UNO.1	Assignment

FPT_FLS.1	FPT_FLS.1	Assignment
FPT_RCV.3	FPT_RCV.3	Assignment
FPT_RCV.4	FPT_RCV.4	Assignment
FPT_TST.1	FPT_TST.1	Assignment and Selection

Added Security Functional Requirements

Security Functional Requirement	Rationale
FCS_CKM.2	Definition of cryptographic key distribution
FCS_CKM.3	Definition of cryptographic key Access
FCS_RNG.1	Due to composite TOE, Definition of SFR used by O.UNDERLYING_HARDWARE
FDP_UCT.1	Definition of data exchange
FDP_UIT.1	The Verification SFR for data exchange integrity is added
FDP_SDI.2	Verification for saved data integrity and actions for protection
FPT_PHP.3	Due to composite TOE, Definition of SFR used by O.UNDERLYING_HARDWARE
FIA_USB.1	Definition of User-subject binding

In SFR of IT environment, as ECC algorithms for application is proveded by IC chip and crypto library of TOE's IT environment, which is added to SFR

3.4.4. Rationale for Conformance of Assurance Requirements

This security target confroms to all assurance requirements of EAL4+ (ATE_DPT.2, AVA_VAN.4) assurance level required by [OCSPP], and there are no additional defined assurance requirements.

Table 3 Rationale of Conformance Claim for Assurance Requirements

Protection Profile	Security Target	Rationale
ASE_INT.1	ASE_INT.1	Acceptance
ASE_CCL.1	ASE_CCL.1	Acceptance
ASE_SPD.1	ASE_SPD.1	Acceptance

ASE_OBJ.2	ASE_OBJ.2	Acceptance
ASE_ECD.1	ASE_ECD.1	Acceptance
ASE_REQ.2	ASE_REQ.2	Acceptance
ASE_TSS.1	ASE_TSS.1	Acceptance
ADV_ARC.1	ADV_ARC.1	Acceptance
ADV_FSP.4	ADV_FSP.4	Acceptance
ADV_IMP.1	ADV_IMP.1	Acceptance
ADV_TDS.3	ADV_TDS.3	Acceptance
AGD_OPE.1	AGD_OPE.1	Acceptance
AGD_PRE.1	AGD_PRE.1	Acceptance
ALC_CMC.4	ALC_CMC.4	Acceptance
ALC_CMS.4	ALC_CMS.4	Acceptance
ALC_DEL.1	ALC_DEL.1	Acceptance
ALC_DVS.1	ALC_DVS.1	Acceptance
ALC_LCD.1	ALC_LCD.1	Acceptance
ALC_TAT.1	ALC_TAT.1	Acceptance
ATE_COV.2	ATE_COV.2	Acceptance
ATE_DPT.2	ATE_DPT.2	Acceptance
ATE_FUN.1	ATE_FUN.1	Acceptance
ATE_IND.2	ATE_IND.2	Acceptance
AVA_VAN.4	AVA_VAN.4	Acceptance

4. Security Problem Definition

Security Problem Definition defines threats, organizational policy and assumptions that intended to be processed by TOE and TOE environment.
Smart card, without the physical access control devices, are used freely under the control of the respective owners and physical security threats as well as a threat via logical interfaces, are exposed to malicious environment .
TOE is a Java Card platform that is run on the IC chip to manage information and resources.
In this ST, main assets is the data that is managed by the card.
There are TSF data and user data.
The document to be produced on the production of the TOE is an additional asset to be protected. Because it affects the integrity and confidentiality of the TOE.

User Data

- Application(AS.Applet)

the application includes executing code associated with the applications running in the execution environment (Runtime Environment), the library, the amount of memory Quota available in the applet. It is information that is not exposed and can not access from outside

- Application Data(AS.Applet_Data)

It is all the data that you are managing for the application to provide services specific to the user. It is the information that can be exposed based on the user's privileges in the application.
It is Application data that must ensure confidentiality and integrity, cryptographic key owned by applet, user pin.

TSF DATA

- Embedded Software (AS.Embedded Software)
  It is the Openplatform smartcard platforms' code and library loaded on the TOE and shall be protected from unauthorized disclosure.

- Embedded Software Data(AS.Embedded Software_Data)
  It is the data like instance, frame stack, program counter, object class, assigned length, when operation of java Card VM. shall be protected from unauthorized disclosure and modification.

- Global Platform Registry(AS.GP_Registry)
  It is the data for the management of TOE itself and the loaded applet. It includes the applet identifier, administration, lifecycle status, card life cycle. It can be exposed in accordance with rights.

- Global PIN (AS.Global_PIN)
  This is Global PIN and can be sharable by all applets on the card.
  Global Pin includes PIN number, Retry Count, try-limt. It shall be protected from unauthorized disclosure and modification from external.

- Issuer Key(AS.Issuer_Key)
  This is TOE system key, that is, the cryptographic key used when generating secure channel. It can be input from the outside, but isn't accessible by.

- Secure Channel Session Key(AS.SCS_Key)
  It is the symmetric key when establishing a secure channel and is used for the exchange of secure messages between the terminal and the card. It is not accessible from the outside.

- Cryptographic Data(AS.Cryptographic_Data)
  It is the encryption-related data of all types produced in the password calculation. It includes seed, hash function data, result of the cryptographic operation. It is not accessible from the outside.

- AS.API_DATA
  Private data of the API, like the contents of its private fields.
  To be protected from unauthorized disclosure and modification.

- AS.SEC_DATA
  The runtime security data of the Java Card RE, like, for instance, the AIDs used to

identify the installed applets, the currently selected applet, the current context of execution and the owner of each object.
To be protected from unauthorized disclosure and modification.

4.1. Threats

The threat agent is user and external IT entity that attempts illegal access to assets protected by the TOE using physical or logical methods outside the TOE and harm using abnormal method. The threat agent to the TOE requires the middle level of expertise, resources and motivation.

T.LOGICAL_ATTACK
The threat agent may change or disclose the user data or the TSF data by exploiting logical interface

Application Notes:

The logical interface is the data exchange interface between the TOE and the Smart Card terminal. It mainly implies the instructions and the responses between the Smart Card and terminal. For the instruction and the response syntaxes, there are the international standards, the local standards, the company standards and the independent standards. The attacker may attack by exploiting syntaxes that exploit logical interface or interpretational difference, or by exploiting instructions for specific use.

Directly threatened user data(s): AS.Applet_Data, AS.Applet
Changeable/exposable asset(s): AS.GP_Registry, AS.API_DATA,AS.SEC_DATAi
Changeable asset(s): AS.Issuer_Key

T.ISSUANCE_MISUSE
The threat agents may exploit the TOE in the process issuing the Smart Card that includes the TOE.

Application Notes:
Directly threatened asset(s): AS.SEC_DATA

T.ILLEGAL_TERMINAL_USE

The threat agent may change and disclose the user data or the TSF data by using unauthorized the Smart Card terminal.

Application Notes:

Directly threatened user data(s): AS.Applet_Data,
Changeable/exposable TSF asset(s): AS.GP_Registry
Changeable asset(s): AS.Issuer_Key

T.ILLEGAL PROGRAM

The threat agent may change and disclose the user data or the TSF data by illegally installing the application program that includes malicious code in the TOE.

Application Notes:

Applet can bypass the TOE security functions by performing piecemeal method, unauthorized method, native methods. And It may perform a remote method that is not authenticated by the card.

Directly threatened user data(s): AS.Applet_Data,
Changeable/exposable TSF asset(s): AS.GP_Registry
Changeable asset(s): AS.Issuer_Key

T.UNINTENTIONAL_FAILURE

The threat agent may exploit disclosure of and damage to the user data and the TSF data caused by suspension of the power supply during the card use or incomplete ending of the TSF service due to impact, etc.

Application Notes:

Directly threatened user data(s): AS.Applet_Data,
Changeable/exposable TSF asset(s): AS.GP_Registry
Changeable asset(s): AS.Issuer_Key

T.CONTINUOUS_AUTHENTICATION_ATTEMPT

Threat agent can obtain the rights by the subsequent attempts to access the TOE.

The threat agent may access the TOE by continuously attempting authorization.

Application Notes:
Changeable/exposable user data(s): AS.Applet_Data, AS.Applet
Changeable/exposable TOE data(s): AS.SCS_Key

T.INTENTIONAL_TRIGGERING_OF_FAILURES
The threat agent may change and disclose the user data or the TSF data by incompletely ending the TSF service with attack using physical stress to the Smart Card.

Application Notes:
Changeable/exposable user data(s): AS.Applet_data
Changeable/exposable TSF data(s): AS.GP_Registry, AS.Cryptographic_Data

T.RESIDUAL_INFORMATION
In case the TOE reuses resources, the threat agent may illegally access information as information of the object is not properly removed.

Application Notes:
Changeable/exposable user data(s): AS.SEC_DATA , AS.Embedded_Software, AS.Applet_Data

T.INFORMATION_DISCLOSURE
The threat agent may exploit the information disclosed from the TOE during normal use of the TOE.

Application Notes:
Information disclosed during normal use of the TOE refers to the electrical signals, such as the electrical power, the voltage and the current, etc. emitted from the IC circuit of the Smart Card. This threat implies the attack by the attacker to obtain cryptographic key or important the TSF data by analyzing electrical signals generated from the Smart Card with analysis devices. Types of this attack include the electric power analysis attack, the electric power difference analysis attack and the timing attack, etc.

T.SID.1

An applet impersonates another application in order to gain illegal access to some resources of the card or with respect to the end user or the terminal

Application Notes:
Directly threatened asset(s): AS.SEC_DATA,AS.Global_PIN, AS.Applet_Data

T.SID.2
The attacker modifies the TOE's attribution of a privileged role (e.g. default applet and currently selected applet), which allows illegal impersonation of this role.

Application Notes:
Directly threatened asset(s): AS.GP_Registry , AS.SEC_DATA

T.RESOURCE
An attacker prevents correct operation of the Java Card System through consumption of some resources of the card: RAM or NVRAM.

Application Notes:
Directly threatened asset(s): AS.Embedded Software, AS.Applet_Data, AS.Embedded Software_Data

4.2. Organizational Security Policies

Organizational security policies described this section must be observed in the TOE following this Security Target.

P. Open platform
The TOE must be developed as an open platform which can load and use multiple applications in an interoperable manner.

P. Duty separation
Role must be assigned to the responsible personnel of each step from manufacturing to using the smartcard and the TOE must be created and managed according to each role in a secure manner.

P.VERIFICATION

This policy shall ensure the consistency between the export files used in the verification and those used for installing the verified file.

4.3. Assumptions

Following conditions are assumed to exist in the TOE security environment that conforms to this Protection Profile

A.TRUSTED_PATH
There shall be a secure channel between the TOE and the IFD.

A.APPLICATION_PROGRAM
If the application program is installed adequately, it shall not contain malicious code.

Application Notes:
When loading, installing, executing the application program in the TOE, the approved procedures must be Followed.

A.TOE_MANAGEMENT
In the steps from manufacturing to using the TOE, there are roles of manufacturers, issuers and holders and training to each role shall be conducted in accordance with defined provisions. And the TOE is handled in a secure manner when repaired or replaced due to breakdown of the TOE or the smartcard.

Application Notes:
Confidentiality and integrity of the TOE shall be maintained in the entire process from manufacturing to delivery, and providing security-related processes.

A.TSF_DATA
TSF data that are exposed to be processed in the course of TOE operation are managed securely.

5. Security Objectives

This Security target defines security objectives by categorizing them into the TOE security purpose and security purpose for the environment. The TOE security objective is directly handled by the TOE. Security objective for the environment is handled in relation to the IT fields or by the technical/process-related means.

5.1. Security Objectives for the TOE

The followings are security objectives directly handling by the TOE:

O.DATA_PROTECTION

The TOE must protect the TSF data stored in TOE against unauthorized disclosure, modification and deletion.

Application Notes :
TOE has to be able to clearly identify the assets and user to be connected with the asset that allows each user to access a logical interface,
TOE must provide a way to securely encrypt your sensitive data, such as the API TOE, which must comply with each of the standard algorithm
TOE must provide a secure management method of generation / distribution / access / destruction of encryption key.
The need to provide confidentiality and integrity, such as PIN and PIN value attempts, conditions with regard to the PIN.
The TOE must provide a series of methods to support the Atomic transaction.
The TOE need to provide the separation function and controlled share between JCRE context and package or between packages, and other applet.

O.ISSUANCE_DELETION
The TOE shall ensure that both applet and package installation/deletion perform as expected and, guarantee that the integrity of the data sent to the issuing process is not impaired.

O.IDENTIFICATION

The TOE must clarify users capable of the using logical interface and the assets to be used according to the role.

Application Notes :

The TOE must be able to clearly identity user and asset so that each user is connected to the asset that can be accessed with the logical interface.

O.AUTHENTICATION

User must complete authentication process when attempting to access the TOE user data and the TSF data.

O.AUTOMATED_RECOVERY

The TOE must be recovered to secure state when failure in the TSF occurs. Also, the TOE, by detecting failure in the TSF, must recommence the TSF service under the state prior to failure.

O.RESIDUAL_INFORMATION_DELETION

The TOE must ensure that the user data or the TSF data are not remaining when ending operation domain used by the TSF.

O.INFORMATION_DISCLOSURE_HANDLIN

The TOE must implement countermeasures to prevent misuse of the information disclosed during normal use of the TOE

Application Notes :

In normal operation the password function provided by the TOE state, a countermeasure must be implemented from exposure through a sub-channel or a perturbation attack of critical information. The TOE activates the countermeasures provided by the IC chip.

O.OPEN_PLATFORM

The TOE must support open platform to which a variety of the application programs can be loaded.

O.UNDERLYING_HARDWARE

The underlying hardware of the TOE, in order to support the security features of the TOE, need to provide a cryptographic operation and countermeasures to various physical attacks.

O.AUDIT

If it detects a potential security breaches, TOE will have to provide feedback and corresponding action.

O.RESOURCE

The TOE shall control the availability of resources for the applications

5.2. Security objectives for the operational environment

The followings are security objectives directly handling by the TOE:

OE.TRUSTED_COMMUNICATION

The trusted path must be provided between the TOE and the Smart Card terminal as the communication target of the TOE.

OE.TSF_DATA

The TSF data exported to the outside of the TOE, therefore handled in the course of the TOE operation must be securely managed.

OE.TRAINING

It must be done the operating education, depending on the role of each administrator of the process.

OE.APPLICATION_PROGRAM

The legitimately installed the application program must not contain malicious code.

OE.VERIFICATION

All the byte codes shall be verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time.

Application Notes :

All the byte codes shall be verified CAP file grammar rules, constraints, at least once, before the loading and installation,

In organizations that are operational TOE, it must be ensured that for the applet to be installed to maintain separation attributes of the platform, it is in compliance with all recommendations of the Application Development Guide "

5.3. Security Objectives Rationale

theoretical rationale of security objectives proves that the specified security objectives are adequate, sufficient to deal with security problems, and not excessive but essential.

The theoretical rationale of security objectives demonstrates the followings:

Each assumption, threat or organizational security policy is handled by at least one security objective.

Each security objective handles at least one assumption, threat or organizational security policy.

Table 4 Relation between security objectives and the security problem definition

Security objectives / Definition of security environment	TOE security objectives											Security objectives for the operational environment				
	O.DATA_PROTECTION	O.ISSUANCE_DELETION	O.IDENTIFICATION	O.AUTHENTICATION	O.RESIDUAL_INFORMATION_DELETION	O.RESIDUAL_INFORMATION_DELETION	O.INFORMATION_DISCLOSURE_HANDLIN	O.OPEN_PLATFORM	O.UNDERLYING_HARDWARE	O.AUDIT	O.RESOURCE	OE.TRAINING	OE.TRUSTED_COMMUNICATION	OE.TSF_DATA	OE.APPLICATION_PROGRAM	OE.VERIFICATION
T.LOGICAL_ATTCK	x	x	x	x						x						
T.ISSUANCE_MISUSE		x														
T.ILLEGAL_TERMINAL_USE	x	x	x	x												
T.ILLEGAL PROGRAM	x		x	x												x
T.UNINTENTIONAL_FAILURE					x	x				x						
T.CONTINUOUS_AUTHENTICATION_ATTEMPT				x												
T.INTENTIONAL_TRIGGERING_OF_FAILURES									x	x						
T.RESIDUAL_INFORMATION						x			X							
T.INFORMATION_DISCLOSURE							x									
T.SID.1			x							x						
T.SID.2			x							x						
T.RESOURCE										x	x					
P.Open platform								x								
P.Duty separation		x	x									x				
P.VERIFICATION		x										x				x
A.TRUSTED_PATH													x			
A.APPLICATION_PR															x	

OGRAM																
A.TOE_MANAGEMEN												x				
A.TSF_DATA														x		

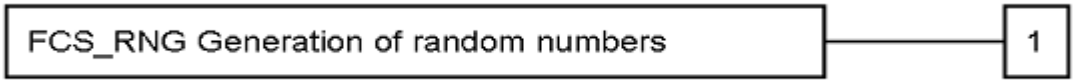
6. Extended Components Definition

This chapter identifies the extended security requirement of this Security Target and provides the explanation about them.

This Security Target defines FCS_RNG that is claimed in the Security Target of the IC Chip.

FCS_RNG Generation of random numbers

Family behaviour
This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purpose.
Component levelling:



FCS_RNG.1 Generation of random numbers requires that random numbers meet a defined quality metric.

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

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

FCS_RNG.1 Random number generation
Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid] random number generator that implements: [assignment: list of security capabilities].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: a defined

quality metric].

7. Security Requirements

Security requirements specify function and warranty requirements that are accepted by this security target and should be met on the TOE.
This security target defines all the subjects, objects, operations, security attributes and external entities used in security requirements as follows:

a) Subjects, objects and related security attributes and operations

표 5 Subject and Object, related security attribute, operation definition

Subject (user)	Subject (user) security attribute	Object (information)	Object (information) security attribute	Operation
S.ISD S.APPLET S.RE	-	O.ISD O.APPLET O.GLOBAL_PIN O.ISSUER_KEY O.JAVA_OBJECT O.REMOTE_OBJECT	-	-All Operation
Administrator, Holder	User identifier, authentication data, role	TSF data	-	Modification, deletion -Specification of limits -Verification of integrity
		security attribute	-	-Modification, deletion -Specification of initial values to replace defaults

b) External entities
- Smartcard Terminal

- Smartcard IC Chip

7.1. Security Functional requirements

Security functional requirements defined in this security target are expressed by selecting relevant security functional components from Part 2 of the Common Criteria to meet the security objectives identified in the previous section. Below tables summarizes security functional components used in this security target.

표 6 Security functional requirements

Security Functional Class	Security Functional Component	
Security Audit	FAU_ARP.1	Security alarms
	FAU_SAA.1	Potential violation analysis
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.3	Cryptographic key access
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FCS_RNG.1	Random number generation
User Data Protection	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute based access control
	FDP_RIP.1	Subset residual information protection
	FDP_UCT.1	Basic data exchange confidentiality
	FDP_UIT.1	Data exchange integrity
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Authentication
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.6	Re-authenticating
	FIA_UID.1	Identification
	FIA_USB.1	User-subject binding

Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF Data
	FMT_MTD.2	Management of limits on tsf data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Privacy	FPR_UNO.1	Unobservability
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
	FPT_PHP.3	Resistance to physical attack
	FPT_RCV.3	Automated recovery without undue loss
	FPT_RCV.4	Function recovery
	FPT_TST.1	TSF testing
Inter-TSF trusted channel	FTP_ITC.1	Inter-TSF trusted channel

7.1.1. Security Audit

FAU_ARP.1 Security alarms

Hierarchical to: No other components

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [one of the below list of actions] upon detection of a potential security violation.

Lists of actions

- blocks the action that produce the security violation and throws an exception
- terminates the card session

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events.

a) Accumulation or combination of the following known [security violation events] representing potential security violations

Security violation events

- Integrity corruption of authentication data
- Unavailability of resources
- Failure of EEPROM programming
- Violation of the access policy for java object
- Violation of the access policy for remote object
- Array overflow
- card tearing
- transaction error
- Failure of TRNG test

b) [none]

7.1.2. Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [cryptographic key generation algorithm] and specified cryptographic key sizes [cryptographic key sizes] that meet the following: [list of standards].

Algorithm	key sizes	standards
E.4.1 DES Session Keys(for C-MAC, encryption, data encryption)	128 bits	[GPCS]

A.4.3 Elliptic Curve Key Pair Generation	192/224/256 bits	ANSI X9.62-2005

Application note :

External entity is able to exploit the crypto-related information (current, voltage, and electromagnetic change) from the physical phenomenon that occurs when the TSF to perform cryptographic operations.

TSF provides the countermeasures like DPA, SPA.

TOE executes symmetric crypto operation, MAC, signature verification using an authenticated co-processor on IC Chip or cryptography library mounted on IC Chip.

TOE performs the electronic signature verification according to the ECDSA algorithm and the encryption key length using a library of the IC chip ECC crypto library.

The evaluation range of the IC chip contains means to countermeasure against DPA, SPA attack response, and IC Chip can not be observed, such as the cryptographic operation by the IC Chip, MAC, digital signature verification, digital signature.

Applications installed TOE can be called a command to generate a key based on the following standards.

Specification	Generation method	Type of cryptographic key generation
[JCAPI]	genKeyPair	ECC cryptographic key

FCS_CKM.2 Cryptographic key destribution

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [cryptographic key distribution method] that meets the following: [specification].

Specification	Distribution method	Type of cryptographic key distribution
[JCAPI]	setKey	DES,AES,SEED,ARIA Key set
	setS, setW	ECPrivateKey, ECPublicKey set

	setExponent, setModulus	RSAPrivateKey, RSAPublicKey set
	KeyAgreement	ECDH key distribution

Application note :
ECDH conforms to ANSI X9.63-2001 standard.

FCS_CKM.3 Cryptographic key accesses
Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.3.1 The TSF shall perform [none] in accordance with a specified cryptographic key access method [cryptographic key access method] that meets the following: [specification].

Application note :

Specification	Key access method	Type of key access
[JCAPI]	getKey	DES,AES, SEED, ARIA key read
	getS	ECPrivateKey read
	getW	ECPublicKey read
	getExponent	RSAPrivateKey read
	getModulus	RSAPrivateKey read

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [physical deletion by overwriting the memory data with zero value] that meets the following: [none].

Application note:

Specification	Key destruction method	Type of key destruction
[JCAPI]	clearKey	TDES,AES,SEED,ARIA,RSA, ECC key destruction

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [list of cryptographic operations] in accordance with a specified cryptographic algorithm [cryptographic algorithm] and cryptographic key sizes [cryptographic key sizes] that meet the following: [list of standards].

standard	algorithm	key size	cryptography operation
TTAS.KO-12.0004	SEED in ECB/CBC	128 bits	data encryption and decryption , mac generation
KSX 1213	ARIA in ECB/CBC	128/192/256 bits	data encryption and decryption , mac generation
FIPS PUB 46-3 ISO/IEC 9797-1]	TDES in ECB/CBC	128/192 bits	data encryption and decryption , mac generation
FIPS PUB 197	AES in ECB/CBC	128/192/256 bits	data encryption and decryption , mac generation
PKCS#1 ISO 9796-2	RSA encryption	1408/1984/2048 bits	data encryption and decryption , mac generation
PKCS#1 ISO 9796-2	RSA sign	1408/1984/2048 bits	data signature generation and verification(

ANSI X9.62-2005	ECDSA	192/224/256 bits	data signature generation and verification(
NIST FIPS 180-3	SHA 224/256/384/512	none	Secure hash

FCS_RNG.1 Random number generation
Hierarchical to : No other components
Dependencies : No dependencies

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

FCS_RNG.1.2 The TSF shall provide random numbers together with a post processing described in TRNG application note and TRNG library that meet the "standard" level of ANSSI requirements (French metric). In addtition, The TSF shall provide random numbers that meet AIS 31 version 1 Functional Classes and Evaluation Methodology for Physical Random Number Generators, 25 September 2001 , Class P2

Application Notes : The SFR provided by IC chip is applied as it is.

7.1.3. User data Protection

FDP_ACC.2 Complete access control
Hierarchical to: FDP_ACC.1
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the [access control SFP] on [list of subject and object] and all operations among subjects and objects covered by the SFP.

access control SFP	subject	object

Card Manager	S.ISD S.APPLET	O.ISD O.APPLET O.GLOBAL_PIN O.ISSUER_KEY
Java Object	S.APPLET S.RE	O.JAVA_OBJECT
Remote Method	S.RE S.APPLET	O.REMOTE_OBJECT

subject/object	description
S.APPLET	Entity that performs the functions of Java card applications that are installed on the TOE
S.ISD	Entity to perform the type of application, the function of the administrator
S.RE	Principal that provides an environment for the execution of the application
O.ISD	Entity to perform the type of application, the function of the administrator
O.APPLET	Java card applications that are installed on the TOE
O.GLOBAL_PIN	PIN in the card specific for owner authentication
O.ISSUER_KEY	Secret key for authentication of the issuer
O.JAVA_OBJECT	Java data generated by the application
O.REMOTE_OBJECT	remote accessible object

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP .

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [access control SFP] to objects based on the following: [list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

Access control SFP	Subject and Object	Security Attribute
Card Manager	S.ISD	Admin_Auth_Status Card_Life_Cycle_State
	S.APPLET	Applet_Life_Cycle_State Privilege
	O.GLOBAL_PIN	PIN_State
	O.ISSUER_KEY	-
Java Object	S.APPLET	Context Quota
	S.RE	Currently_Active_Context
	O.JAVA_OBJECT	Context Life_Time
Remote Method	O.REMOTE_OBJECT	Context

Security attributes	description
Admin_Auth_Status	Status that indicates whether or not to keep the administrator authentication
Card_Life_Cycle_State	Card life cycle status
Applet_Life_Cycle_State	S.APPLET's life cycle
Privilege	Privileges granted to S.APPLET by administrator
PIN_State	O.GLOBAL_PIN's status
Context	Security zone O.APPLET, O.JAVA_OBJECT, O.REMOTE_OBJECT belong
Quota	The amount of memory that can be used by S.APPLET
Currently_Active_Context	Security zones O.APPLET currently active
Life_Time	O.JAVA_OBJECT life state

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

access control SFP	rules	description
Card Manager	CM-1	Loading, installation, removal of O.APPLET are permitted only S.ISD's Admin_Auth_Status is valid.
	CM-2	. If Applet_Life_Cycle_State of O.APPLET is valid, the selection of S.APPLET is permitted to all entities.
	CM-3	Changes O.GLOBAL_PIN is acceptable to S.APPLET to own a consistent privilege and S.ISD 's Admin_Auth_Status is valid.
	CM-4	If PIN_State is enabled, verification of O.GLOBAL_PIN are permitted to all entities.
	CM-5	Changes O.ISSUER_KEY are authorized only to S.ISD which Admin_Auth_Status is valid.
	CM-6	Change of Card_Life_Cycle_State of O.ISD is acceptable to S.APPLET to own a consistent privilege or S.ISD which Admin_Auth_Status is valid.
Java Object	JO-1	Access to O.JAVA_OBJECT, are permitted only in the case of Context of S.APPLET and O.JAVA_OBJECT is convertible or identical
Remote Method	RM-1	Remote access to O.REMOTE_OBJECT is permitted only if it is the same as Currently_Active_Context of S.RE and the Context of O.REMOTE_OBJECT

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [rules].

SFP	rules	description
Card Manager	CM-7	All entities are possible to query card management information of O.ISD.
Java Object	JO-3	S.RE is accessible to all O.JAVA_OBJECT which Life_Time is valid.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [rules].

SFP	rules	description

Card Manager	CM-8	If Card_Life_Cycle_State of O.ISD is not valid, the operation for the object of the subject is not allowed
	CM-9	Searching of O.GLOBAL_PIN is not permitted in any subject.
	CM-10	Searching of O.ISSUER_KEY is not permitted in any subject.
Java Object	JO-4	S.APPLET does not allow the generation of O.JAVA_OBJECT exceeding the Quota.
	JO-5	Access to the disabled O.JAVA_OBJECT is impossible.

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* the [list of objects]:

objects
O.ISD
O.APPLET
O.GLOBAL_PIN
O.ISSUER_KEY
O.JAVA_OBJECT
O.REMOTE_OBJECT

Application note :

In addition, the package and the instance of the applet, APDU buffer, bArray object, Key, encryption buffer, such as Java card trainsient object corresponds.

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the [access control SFP] to *transmit, receive* user data in a manner protected from unauthorized disclosure.

Application note :
The TSF maintains the confidentiality by encrypting the transmitted data

FDP_UIT.1 Data exchange integrity
Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1 The TSF shall enforce the [access control SFP] to *transmit, receive* user data in a manner protected from *modification, deletion, insertion,replay* errors

Application note:
By using the MAC key of the session, TSF protects the integrity of the transmitted data. This provides the method of protection against the insertion,deletion, change of the user data. It is intended to provide a method that is protected from re-use by using the SendSequenceCounter.

FDP_SDI.2 Stored data integrity monitoring and action
Hierarchical to: FDP_SDI.1 Stored data integrity monitoring
Dependencies: No dependencies

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [integrity errors] on all objects, based on the [integrity of sensitive data]:
FDP_SDI.2.2 Upon detection of integrity error, the TSF shall run [the exception occurrence].

Application note :
At the time of saving, Integrity information of the encryption key, PIN, the package is stored.

7.1.4. Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Authentication

FIA_AFL.1.1 The TSF shall detect when *thresholds* unsuccessful authentication attempts occur related to [authentication events].

authentication events	thresholds
Authentication of Administrator	[1]

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *reached or surpassed,* the TSF shall [actions].

authentication events	actions
Authentication of Administrator	Terminate the card session

FIA_ATD.1 User attribute definition

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

[

a) Identity of user ;

b) Authentication data ;

c) Role ;

]

Application note:

When user is Applet, It must maintain a list of security attributes list such as Package AID, Applet's version number,Registered applet AID, Applet Selection Status.

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [List of metric].

Secrets information	List of metric
PIN of administrator	At least 1 digit up to 16 digits, number and letter
PIN of user	At least 1 digit up to 127 digits, number and letter
KEY of S.CM on behalf of administrator	112 bit TDES key

FIA_UAU.1 Authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Identification

FIA_UAU.1.1 The TSF shall allow [list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

- Logical communication channel generation with card
- Request issuer and the card issuer information
- Select the applications installed on the card
- The attempt to create a secure channel with card

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user in addition to FIA_UAU.1.1.

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.4.1 The TSF shall prevent the reuse of authentication data related to [authentication mechanism of the security of the channel administrator].

FIA_UAU.6 Re-authenticating

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [list of re-authentication is required].

- All commands can be passed to the TOE only through the administrator security channel mechanism
- Card session termination
- Card reset

FIA_UID.1 Identification

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow [list of TSF-mediated actions specified] on behalf of the user to be performed before the user is identified.

- Generation of logical communication channel with card
- Request of issuer and card issuing information

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user in addition to FIA_UID.1.1.

FIA_USB.1 User-subject binding

Hierarchical to: No other components

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:[user - security attribute]

User - Security Attribute	Subject - Security Attribute
Issuer - PACKAGE AID - Registerd APPLET AID - Privilege	S.APPLET - Context
Issuer - Card_Life_Cycle_State	S.ISD - Card_Life_Cycle_State

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [rules defined in FDP_ACF.1(1)]

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [rules defined in FMT_MSA.1].

7.1.5. Security Management

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to *disable, enable* the behavior of the functions [Function].

Function	Role
Card lock by Application	S.ISD
Card termination by Application	S.ISD
Global pin initiation by Application	S.ISD
Package Load/Install/Delete	S.ISD
Context Management	S.RE

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [Access control SFP] to restrict the ability to *modify,change,create* the security attributes [security attributes] to [Role].

Access control SFP	Security attributes	Operation	Role
Card Manager	Card_Life_Cycle_State	modify	S.ISD
	Privilege	create	S.ISD
	PIN_State	change	S.ISD
Java Object	Context	change	S.RE
Remote Methods	Context	change	S.APPLET

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [access control SFP] to provide *Attributes* default values for security attributes that are used to enforce the SFP.

Access control SFP	Attributes
Card Manager	Restrictive
Java Object	Restrictive
Remote Methos	Restrictive

FMT_MSA.3.2 The TSF shall allow the [S.ISD, S.RE] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 TSF MANAGEMENT of TSF Data

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to *modify* the [TSF data] to [Role].

TSF data	Operation	Role
AS.GP Registry	Modification	S.ISD
AS.Global PIN	Value modification	S.ISD
	Resume use	S.ISD

AS.Issuer Key	Modification	S.ISD

FMT_MTD.2 TSF Management of limits on TSF data

Hierarchical to: No other components
Dependencies: FMT_MTD.1 MANAGEMENT OF TSF Data
FMT_SMR.1 Security roles

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [TSF data] to [role].

TSF data	role
AS.Global PIN's Retry Counter	S.ISD
AS.Applet의 Quota	S.ISD
As.Issuer_Key's number of use	S.ISD

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

TSF data	action
AS.Global PIN's Retry Counter	stop using the Global PIN until issuer's restarting the Global PIN service
AS.Applet's Quota	To stop the generation of Java Object of Applet, and raises an exception
As.Issuer_Key's number of use	By generating an error code, additional authentication becomes impossible.

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components
Dependencies: No dependencies

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

- The application of rights management

- cardholder authentication
- Card Life Cycle management
- Applet Context management
- Key management
- PIN management
- Signature generation
- Object sharing management
- Package AID register and applet AID change

FMT_SMR.1 Security roles

Hierarchical to: No other components

Dependencies: FIA_UID.1 Identification

FMT_SMR.1.1 The TSF shall maintain the roles [Role].

Role	Description
S.APPLET: represents the card user	Application to perform the functions of the card
S.ISD: represents the card issuer	Management program that the role of the issuer
S.RE	Context Management Object Sharing Management

FMT_SMR.1.2 The TSF shall be able to associate users with roles defined in FMT_SMR.1.1

7.1.6. Privacy

FPR_UNO.1 Unobservability

Hierarchical to: No other components

Dependencies: No dependencies

FPR_UNO.1.1 TSF shall ensure that [external entities] are unable to observe the operation [

a) "FCS_CKM.1 Cryptographic key generation"

b) "FCS_CKM.2 Cryptographic key distribution"
c) O.ISSUER_KEY
d) O.GLOBAL_PIN

] on [

a) FCS_COP.1 Cryptographic key operation
b) PIN verification operation]

By [TSF].

Application note :
An external entity may obtain and abuse cryptographic information from physical phenomena that take place during the cryptographic computation of TOE (e.g. change in current, voltage and electromagnetism). TSF may provide means to counter attacks like DPA, SPA.

7.1.7. Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components
Dependencies: No dependencies

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur : [

a) Potential security violation events defined in FAU_SAA.
b) Failure of self test defined in FPT_TST.1
c) Condition beyond the normal operating range of the TSF which an IC chip is detected
d) Load/install/delete failure of package and applet

]

FPT_PHP.3 Resistance to physical attack
Hierarchical to: No other components.
Dependencies: No dependencies

FPT_PHP.3.1 The TSF shall resist [physical manipulation and physical probing] to [TSF] by re-sponding automatically such as that the SFRs are always enforced.

Application Notes :
The SFR provided by the IC chip is applied as it is.

FPT_RCV.3 Automated recovery without undue loss
Hierarchical to: FPT_RCV.2 Automated recovery
Dependencies: AGD_OPE.1 Operational user guidance

FPT_RCV.3.1 When automated recovery from [list of failures/services continuities in FPT_FLS.1] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.3.2 For [list of failures/services continuities in FPT_FLS.1], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.3.3 The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [quantification of TSF data or objects during failures event] for loss of TSF data or objects under the control of the TSF.

FPT_RCV.3.4 The TSF shall provide the capability to determine the objects that were or were not capable of being recovered.

FPT_RCV.4 Function recovery
Hierarchical to: No other components
Dependencies: No dependencies

FPT_RCV.4.1 The TSF shall ensure that [list of failures/services continuities in FPT_FLS.1] have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

FPT_TST.1 TSF self test
Hierarchical to: No other components
Dependencies: No dependencies

FPT_TST.1.1 The TSF shall run a suite of self tests during *initial start-up, at the conditions [random number generation, crypto operation, administrator authentication, At the user's request that has been approved]* to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorized issuer with the capability to verify the integrity of [*IC Chip's value of enabled security function, random number, cryptographic key and crypto operation's result value, authentication data, TSF execution code*]

FPT_TST.1.3 The TSF shall provide authorized issuer with the capability to verify the integrity of [stored TSF executable code, random number generation function]

7.1.8. Inter-TSF trusted channel

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components
Dependencies: No dependencies

The TSF shall provide a communication channel between itself and another 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

The TSF shall permit [another trusted IT product] to initiate communication via the trusted channel

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [new application package's load and install to card].

7.2. Security Assurance Requirements

The security assurance requirement level is EAL5 augmented with ATE_DPT.2 and . AVA_VAN.4.

8. TOE Summary

8.1. TOE Security Functions

This section explains TOE security functions (TSF) that meets the security requirements described in the previous chapter. Each security functions are described as the name of the function and a simple description. FSP document provides description in detail

Table 7 TOE Security Function

Security Function	Description
SF_CARD_MANAGEMENT	Card Data Management
SF_AUTHENTICATION	Identity and Authentication
SF_COUNTER_MEASURE	Counter Measure
SF_OBJECT_ACCESS	Access Control for Java Object
SF_RESOURCE_MANAGEMENT	Resource Management
SF_TRANSACTION	Transaction Management
SF_CRYPTOGRAPHY	Crypto Support

8.1.1. SF_CARD_MANAGEMENT

Management functions for the card provides command processing, application/life cycle management and sub system of card management.

8.1.2. SF_AUTHENTICATION

For authentication and identity, this Security Function provides terminal authentication which manage security channel for administrator authenctation,message integrity, closing of secure channel.
For user authentication, Global PIN used in card and Owner PIN using its own function of the application via the API are provided.
In addition, installation/modification of administrator key and management of session key, and creation/deletion of key are provided.

8.1.3. SF_COUNTER_MEASURE

This security function enable H/W protection against various attacks(side attack, error injection, physical attack.. etc) from the outside and provides counter measure to maintain stable status when security problem is made from integrity error etc.

8.1.4. SF_RESOURCE_MANAGEMENT

This security function is responsible for resource management and provides deletion function of remaining information at the time creation or return resource.

8.1.5. SF_OBJECT_ACCESS

This security function controls the application access and the remote access for java object created by application

8.1.6. SF_TRANSACTION

If abnormal TSF service stops, etc.. the end of power during TOE operation, this security function detects error at the start of TOE and provides transaction function to start service at previous status before error status

8.1.7. SF_CRYPTOGRAPHY

This security function provides crypto function like creation/verification of electronic signature, encryption/decryption, creation hash/random value.

8.2. TSF of IC Chip used in TOE

TOE uses various security functions like table below at using TDES, RSA, ECDSA, and ECDH from IC chip

Table 8 IC chip security function

Security Function	Corresponding SFR	Description

TOE's Detectors	FPT_FLS.1	Voltage detector, Frequency detector, Active shield removal detector, Inner insulation removal detector, Light and laser detector, Temperature detector, Voltage glitch detector
Memory Encryption	FDP_IFC.1	Memory Encryption when sensitive data into the memory. Data will be encrypted before stored in memory so this will enhance the difficultly for an attacker to get useful information on data bytes hamming weight.
TRNG	FCS_RNG.1	TRNG is a hardware true random number generator compliant with AIS31 standard class P2 high.
TDES	FCS_COP.1	Hardware DES has several security countermeasures to prevent side channel attacks. - Secure Key & Data loading - DPA prevent : random mask - Variable clock - RWG automatic enable - High Order DPA prevent : Virtual DES
RSA	FCS_COP.1	The acceleration of modulo exponentiations required in the RSA encryption/decryption algorithm.
ECDSA	FCS_COP.1	ECDSA_sign_digest, ECDSA_verify_digest
SHA	FCS_COP.1	SHA224, SHA256, SHA384, SHA512

8.2.1. SFR of IC Chip

described in the following table compatible with the SFR of IC chips used in the TOE

SFR of IC Chip	SFR of Composite TOE	Compatibility
FAU_SAS.1	[none]	N/A
FCS_CKM.1/ECDSA	FCS_CKM.1	Composite TOE provide ECDSA Key generation using ECC key function provided by IC Chip
FCS_COP.1/3DES FCS_COP.1/AES FCS_COP.1/RSA FCS_COP.1/ECDS	FCS_COP.1	Composite TOE provides TDES, RSA, AES, ECDSA, SHA function using IC Chip

A FCS_COP.1/SHA		
FCS_COP.1/ECDH	FCS_CKM.2	Composite TOE provides ECDH calculation and crypto key distribution using IC chip
FCS_RNG.1	FCS_RNG.1	Composite TOE provides True Random generation using IC chip
FDP_ACC.1	[none]	N/A
FDP_ACF.1:	[none]	N/A
FPT_ITT.1	FPR_UNO.1	Composite TOE protects the exposure of inside information using various functions of IC chip -memory encryption -Random wait generator -Variable Clock 등
FDP_ITT.1	FPR_UNO.1	
FDP_IFC.1	FPR_UNO.1	Composite TOE treats confidential data to be managed by embedded S/W
FMT_LIM.1	[none]	N/A
FMT_LIM.2	[none]	N/A
FMT_MSA.1	[none]	N/A
FMT_MSA.3	[none]	N/A
FMT_SMF.1	[none]	N/A
FPT_FLS.1	FPT_FLS.1	Composite TOE maintains stable status in case of failure
FPT_PHP.3:	FPT_PHP.3:	When physical attack is detected , Composite TOE generates FIQ or reset for TSF protection
FRU_FLT.2	[none]	N/A

8.2.2. Security Objectives of IC Chip

The following table specifies compatibility between the security objectives of composite TOE and of the Chip

security objectives of IC chip	security objectives of composite TOE	Compatibility

O.Leak-Inherent	O.INFORMATION_DISCLOSURE_HANDLIN	O.Leak-Inherent is intended to protect the leakage of inherent data in IC, it is compatible with O.INFORMATION_DISCLOSURE_HANDLIN of composite TOE
O.Phys-Probing	O.UNDERLYING_HARDWARE	O.Phys-Probing is intended to protect the physical attack, it is compatible with O.UNDERLYING_HARDWARE of composite TOE
O.Malfunction	O.UNDERLYING_HARDWARE	O.Malfunction provides security objectives of correct operation of IC chip, it is compatible with O.UNDERLYING_HARDWARE of composite TOE
O.Phys-Manipulation	O.UNDERLYING_HARDWARE O.DATA_PROTECTION	O.Phys-Manipulation provides security objectives which protects embedded software and user data from Reverse Engineering., etc. it is compatible with O.UNDERLYING_HARDWARE and O.DATA_PROTECTION of composite TOE
O.Leak-Forced	O.INFORMATION_DISCLOSURE_HANDLIN O.UNDERLYING_HARDWARE	O.Leak-Forced provides security objectives which protects data leakage at environmental stress of IC Chip and incorrect operation. it is compatible with O.INFORMATION_DISCLOSURE_HANDLIN and O.UNDERLYING_HARDWARE of composite TOE
O.Abuse-Func	[none]	N/A
O.Identification	[none]	N/A
O.RND	O.AUTHENTICATION O.UNDERLYING_HAR	O.RND provides security objectives which generate IC Chip Random

	DWARE	number. it is compatible with O.AUTHENTICATION and O.UNDERLYING_HARDWARE of composite TOE
O.Add-Functions	O.UNDERLYING_HARDWARE	O.Add-Functions provides security objectives that embedded software provides security function like 3DES,AES,RSA,ECC using IC Chip it is compatible with O.UNDERLYING_HARDWARE of composite TOE
O.Mem-Access	[none]	N/A

8.2.3. Threats of IC Chip

The following table specifies compatibility between the threats of composite TOE and of the Chip

Threats of IC Chip	Threats of Composite TOE	Compatibility
T.Leak-Inherent	T.INFORMATION_DISCLOSURE T.INTENTIONAL_TRIGGERING_OF_FAILURES T.UNINTENTIONAL_FAILURE	Threat of IC Chip is compatible with threat of composite TOE
T.Phys-Probing	T.INFORMATION_DISCLOSURE T.INTENTIONAL_TRIGGERING_OF_FAILURES	Threat of IC Chip is compatible with threat of composite TOE
T.Malfunction	T.INFORMATION_DISCLOSURE T.INTENTIONAL_TRIGGERING_OF_FAILURES	Threat of IC Chip is compatible with threat of composite TOE
T.Phys-Manipulation	T.INFORMATION_DISCLOSURE	Threat of IC Chip is compatible with threat of composite TOE
T.Leak-Forced	T.INFORMATION_DISCLOSURE T.INTENTIONAL_TRIGGERING	IC Threat of IC Chip is compatible with threat of composite TOE

	_OF_FAILURES T.UNINTENTIONAL_FAILURE	
T.Abuse-Func	T.ISSUANCE_MISUSE T.ILLEGAL PROGRAM	Threat of IC Chip is compatible with threat of composite TOE
T.RND	T.LOGICAL ATTACK T.SID.1 T.SID.2 T.CONTINUOUS_AUTHENTICATION_ATTEMPT T.INFORMATION_DISCLOSURE T.INTENTIONAL_TRIGGERING_OF_FAILURES	Threat of IC Chip is compatible with threat of composite TOE
T.Mem-Access	[none]	N/A

8.2.4. Organizational Security Policies of the IC chip

The following table specifies compatibility between the Organizational Security Policies of the IC chip and Security Policies/Threats of composilte TOE

Organizational Security Policies of the IC chip	Security Policies/Threats of composilte TOE	Compatibility
P.Procss-TOE	P.ROLE_DIVISION	P.Process-TOE is security policy that IC manufacturer protects TOE by identifying correct TOE. It is compatible with P.ROLE_DIVISION of composite TOE 3DES, AES, RSA, ECC,SHA with embedded software.
P.Add-Functions	P.ROLE_DIVISION T.INFORMATION_DISCLOSURE T.INTENTIONAL_T	Organizational security policy provides security policy that IC manufacturer protects TOE by identifying correct TOE.

	RIGGERING_OF_FAILURES	It is not contradictory to P.ROLE_DIVISION,T.INFORMATION_DISCLOSURE,and T.INTENTIONAL_TRIGGERING_OF_FAILURE.

8.2.5. Assumptions of IC Chip

The following table specifies compatibility between the Assumptions of the IC chip and Assumptions/Security Objectives of composilte TOE

Assumptions of IC Chip	Assumptions/Security Objectives of composilte TOE	Compatibility
A.Process-Sec-IC	A.TOE_MANAGEMEN	A.Process-Sec-IC assumes that it observes security process for confidence and integrity from TOE manufacture to user delivery. It is compatible with A.TOE_MANAGEMEN of composite TOE
A.Plat-Appl	O.INFORMATION_DISCLOSURE_HANDLIN O.UNDERLYING_HARDWARE	A.Plat-Appl assumes that the requested contents by manual, certificate report, IC chip document related platform TOE should be applied to composite TOE. These request is mandatory at the time developing security functions, so it is compatible with O.INFORMATION_DISCLOSURE_HANDLIN and O.UNDERLYING_HARDWARE
A.Resp-Appl	A.TSF_DATA O.DATA_PROTECTION	A.Resp-Appl assumes that user data(crypto keys specially) is treated for the purposes of the application safely, user data(Issuer Key, PIN., etc) related security by managed composite TOE is compatible with DATA_PROTECTION.

		Application to be installed to composite TOE should manage user data safely, it is compatible with A.TSF_DATA which assumes that TSF data transferred out of TOE is managed safely.
A.Key-Function	O.INFORMATION_DISCLOSURE_HANDLIN	A.Key-Function assumes that it can protect leakage attack at the time developing Key-dependent function in Embedded software, Composite TOE applied all Counter Measure using IC chip's crypto function against leakage attack. In addition, software counter measure is applied to additonal SEED,ARIA crypto algorithms. it is compatible with O.INFORMATION_DISCLOSURE_HANDLIN

8.2.6. Operational Environment of IC Chip

The following table specifies compatibility between the operational environment of the IC chip and of composilte TOE

Operational Environment of IC Chip	Operational Environment of composite TOE	Compatibility
OE.Plat-Appl	OE.TRUSTED_COMMUNICATION OE.APPLICATION_PROGRAM OE.TSF_DATA	OE.Plat-Appl comply with IC Chip's specification and compatible with operational environment of composite TOE
OE.Resp-Appl	OE.TRUSTED_COMMUNICATION OE.APPLICATION_PROGRAM OE.TSF_DATA	OE.Resp-Appl is operational environment that user data is treated by composite TOE safely, it is compatible with operational environment of composite TOE
OE.Process-Sec-IC	OE.TSF_DATA	OE.Process-Sec-IC guarantees

		integrity during delivery, , it is compatible with operational environment of composite TOE