KOMSCO JK72 V1.0

Security Target Lite V1.2

August 7, 2024

KOMSCO ICT Research Center

The evaluated Korean version (Security Target) has been translated into English version.

This page left blank on purpose for double-side printing.

[REVISION STATUS]

Revision	Description of Change	Date
1.0	Initial ST	2024.7.30.
1.1	Update document version information	2024.8.2.
1.2	Update document version information	2024.8.7.

This page left blank on purpose for double-side printing.

[List of Contents]

[List of Figures]

[List of Tables]

1. Security Target Introduction

This document is the Security Target (shortly, ST) of KOMSCO JK72 V1.0 product developed by the KOMSCO (Korea Minting, Security Printing & ID Card Operating Corporation). The evaluation assurance level of the Security Target is EAL5+.

This section provides the label and description to control and identify the ST and the TOE that the ST refers to. And this section briefly describes the structure of document, the TOE usage, and primary security features.

1.1 Security Target Reference

Security Target is completely identified by information located in the following table.

Title	KOMSCO JK72 V1.0 Security Target
Identifier	[JK72-TR-0001] Security Target
Version	V1.5
Evaluation criteria	Korea IT Security Evaluation and Certification Scheme (Ministry of Science, ICT and Future Planning Notice NO.2016-73)
CC version	v3.1r5
Evaluation assurance level	EAL5+(ALC_DVS.2, AVA_VAN.5)
Author	ICT Research Center, Technology Research Institute, KOMSCO
keyword	Smart Card, Javacard, IC Chip, Smart Card Terminal, Open Platform COS

1.2 TOE Reference

TOE is completely identified by information located in the following table.

Developer	IT Research Center, Technology Research Institute, KOMSCO
TOE Name	KOMSCO JK72 V1.0
TOE Version	V1.0
TOE Identifier	JK72-D38C02-R1
TOE Component	• IC Chip * IC Chip Certificate number : ANSSI-CC-2023/40 * Samsung Chip model : S3D384C • TOE Identifier * IC Fabricator: 4250 (Samsung) * IC Type: 0D0308040C (S3D384C) • OS software : KOMSCO JK72 COS V1.0 * OS Identifier: 0x4A4B (JK) * OS Level: 7201 (JK72_R1) * File : JK72-D38C02-R1.hex • Guidance : [JK72-MA-0002] Operational User Guidance-v1.3.pdf, [JK72-MA-0001] Preparation Procedure-v1.4.pdf

1.3 TOE Overview

In this section it identifies the TOE type. It also describes the uses and key security characteristics of TOE and identifies major hardware and software of TOE. The TOE is composed of the Open Platform Chip Operating System (COS) and security controller and model(S3D384C) of Samsung including the hardware component of IC Chip. The TOE is composite TOE based on the certified IC Chip.

1.3.1 TOE Type

The TOE type is a COB(Chip On board) type that a Javacard platform developed by KOMSCO is embedded in IC Chips, S3D384C. The IC Chips are CC EAL6+ certified smart card IC Chips of Samsung.

The open platform operating system of TOE is composed of Javacard Platform V3.0.5 and Global Platform V2.3.1 ID Configuration & Mapping Guidelines and Chip OS.

The Javacard Platform provides the firewall, memory management, transaction handling and Cryptographic operation for safe interaction of multi-application in a Chip. The Javacard Platform is composed of Javacard Runtime Environment 3.0.5[JCRE], Javacard Virtual Machine 3.0.5[JCVM], Javacard Application Programming Interfaces 3.0.5[JCAPI]). GP 2.3.1 provides the operating system management like administrator authority authentication, application load/install/delete, and life cycle management for the operating system and application. GP 2.3.1 is composed of the Card Manager and GP APIs 2.3.1. The Chip OS provides memory management, I/O function, low level transaction and Cryptographic algorithms based on software. The hardware of TOE is IC Chips that composed of CPU, co-processor, I/O port, memory(RAM, FLASH) and contact/contactless interfaces.

This security target defines security functional and assurance requirements for open platform card operating system—embedded in the IC Chip as part of TOE's sub-hardware—and the interface between the open platform card operating system and applications to be used there. The interface between the open platform card operating system and applications used consists of JCAPIs V3.0.5 of Javacard Platform V3.0.5 and ID Configuration V1.0.2 and Mapping Guideline V1.0.1 of Global Platform V2.3.1.

The IC Chips and Cryptographic libraries of TOE are completely identified by information located in the following table.

[Table 1] TOE IC Chips and Cryptographic libraries

Contents	Description
IC Chips	The Chips used in the TOE are S3D384C of Samsung certified CC EAL6+ augmented with' AES_TSS.2' . - PP : BSI-PP-0084-2014 - Certification Number : ANSSI-CC-2023/40
	The key security characteristic of IC Chip is as follows. - various detection circuits • ReverseEngineering/Voltage/Power/glitches/Temperature/Laser attack - countermeasures/defense • Memory encryption/Bus scrambling/Random branch/Variable Clock - Digital True random number generator (DTRNG FRO-M)

	- Triple DES cryptographic coprocessor with 112 or 168bits key size - AES cryptographic coprocessor with 128 bits, 192bits and 256bits key size - TORNADOTM-T supporting modular multiplications for the operand size up to 4128-bit and modular additions/subtractions for the operand size up to 544-bit
	The IC Chip hardware specifications are as follows. - Communication support : ISO 7816, ISO 14443 Type A - Memory : RAM(12KB), FLASH(384K) - Cryptographic module : DES/TDES, AES, RSA, ECC, DTRNG
Cryptographic libraries	The Cryptographic library Secure TORNADOTM-T Coprocessor is followings. - An optional modular arithmetic library for the support of RSA and ECC (with SHA) cryptographic operations - A DTRNG FRO M library built around Hardware DTRNG FRO M. This library meets some of ANSSI requirements (French scheme) as well as PTG.2 class of BSI-AIS31 (German scheme) • PKA_Lib_AT1_v4.03.lib • S3D384C_PTG2_DTRNG_library_v3.2.lib

1.3.2 TOE Usage

TOE can run all Java applets developed in accordance with the Javacard v3.0.5 standard. The applets run on the TOE include: public ID card applications such as electronic resident registration card application, financial applications (e.g. cash/credit, electronic wallet, e-commerce), and electronic signature applications (e.g. digital signature). Applications available on the TOE and their uses are outlined in [Table 2].

[Table 2] TOE Usage and Application

Application Type		Usage	Transaction Type
ID	Electronic resident registration card	IC Chip-embedded smart card-type electronic resident registration card that is used to address the weaknesses of conventional resident registration card in the prevention of falsification and privacy protection (The Chip contains private authentication certificate for online banking, PIN, health insurance and disability/elderly information)	Identification
	Driver's license	IC Chip-embedded smart card-type electronic driver's license that is used to better prevent falsification and improve online utilization	Identification
Finance & Payment	Cash card	Designed for direct deposit/withdrawal of bank savings using private information and bank account information saved in the TOE at ATMs or other facilities	Deposit & withdrawal of savings
	Credit card	Credit card merchants access the main computer of the credit card company online via the credit authorization terminal (CAT) to check a credit card's credit limit and	Payment

		validity and permit post-payment. Bank CDs are designed to read credit card information, check the status of the credit card owners' bank accounts and pay cash.	
	Electronic wallet	A certain level of value is saved in a semiconductor (IC) Chip electronically to make payments in the same way as in cash. Unlike in the case of a pre-paid card, a certain amount of money can be redeposited to the bank and be used repeatedly.	Payment
	E-commerce	Designed to trade products on a real-time basis via stores open on the Internet	Payment
Electronic Signature	Digital signature	Used as a sort of electronic signature in the open key cryptographic format (i.e. asymmetric cryptographic system); electronic data attached to or logically combined with data messages that are used to identify signers and represent their authorization on the content of data messages	Identification, prevention of document falsification & denial
Public Transport Card	Public transport card	Designed to read basic user information (i.e. the first six digits of the number displayed on the resident registration card) via the public transport terminal or other devices and exempt people with disabilities and senior citizens from public transport fares (gate opening/closing)	Payment

1.3.3 TOE Security Features

Security Features of TOE are the followings.

[Table 3] TOE Security Features

Security Features	Description
Data confidentiality	The Cryptographic Keys and TSF data are protected from unauthorized disclosure.
User identification and authentication	The TOE is protected from modification and use of resources by unauthorized user.
Data integrity	The Cryptographic Keys and TSF data are protected from unauthorized modification.
atomistic rollback and optimistic backup	The TOE safely protects stored data and provides automated recovery function when power is lost.
firewall access control	By isolating a single applet within the given space through the mechanism of firewall between applets, it prevents data from being leaked out by other applets and provides protection against hacking.
TDES signature – MAC computation	The TOE ensures that it prevents some data modification (delete, adding or data rearrangement) using MAC computation during data transaction.
integrity check of checksummed data	The TOE checks if data are modified by using a checksum function(summed value according as a specific computation rule)
secure state of information	The primary information of TOE is safely stored. The TOE ensures a secure state of information and secure state of

	TOE when abnormal operation, Power-off or Card Tearing is occured by external entity.
non-observability of operations on sensitive information	The TOE ensures non-observability by encrypting the primary TSF data (cryptographic keys and PIN, etc.) and verifying integrity using CRC32 or Hash.
unavailability of previous information content	The TOE performs the Zerorization mechanism to prevent reuse of information after it handles the primary TSF data for authentication and identification.
Data Access Control	The TOE checks the authentication by using PIN or other mechanism and checks the verification of authorization request. And the TOE performs data access control through data access about only specific data and specific area.
Secure Channel	When working together with an external system, the TOE performs authentication to identify and authenticate the external system's nodes for the mutual safety of paths and channels and ensures safe channel.

1.3.4 Non-TOE hardware/software/firmware required by the TOE

The IC Chip as its sub-hardware and the crypto library that supports cryptographic computation are included in the TOE. Applets installed at the issuance phase are excluded from the TOE.

- Applet

Non-evaluation elements in TOE configuration are illustrated in [Table 4].

[Table 4] Identification of non-evaluation elements

Non-evaluation elements	Description
Applet	Applets are applications installed in FLASH of sub-hardware where the TOE is embedded to use TOE resources and run through the TOE. Applets that can be installed in the TOE are Java Applet execution files compatible with the Javacard v3.0.5 standard.

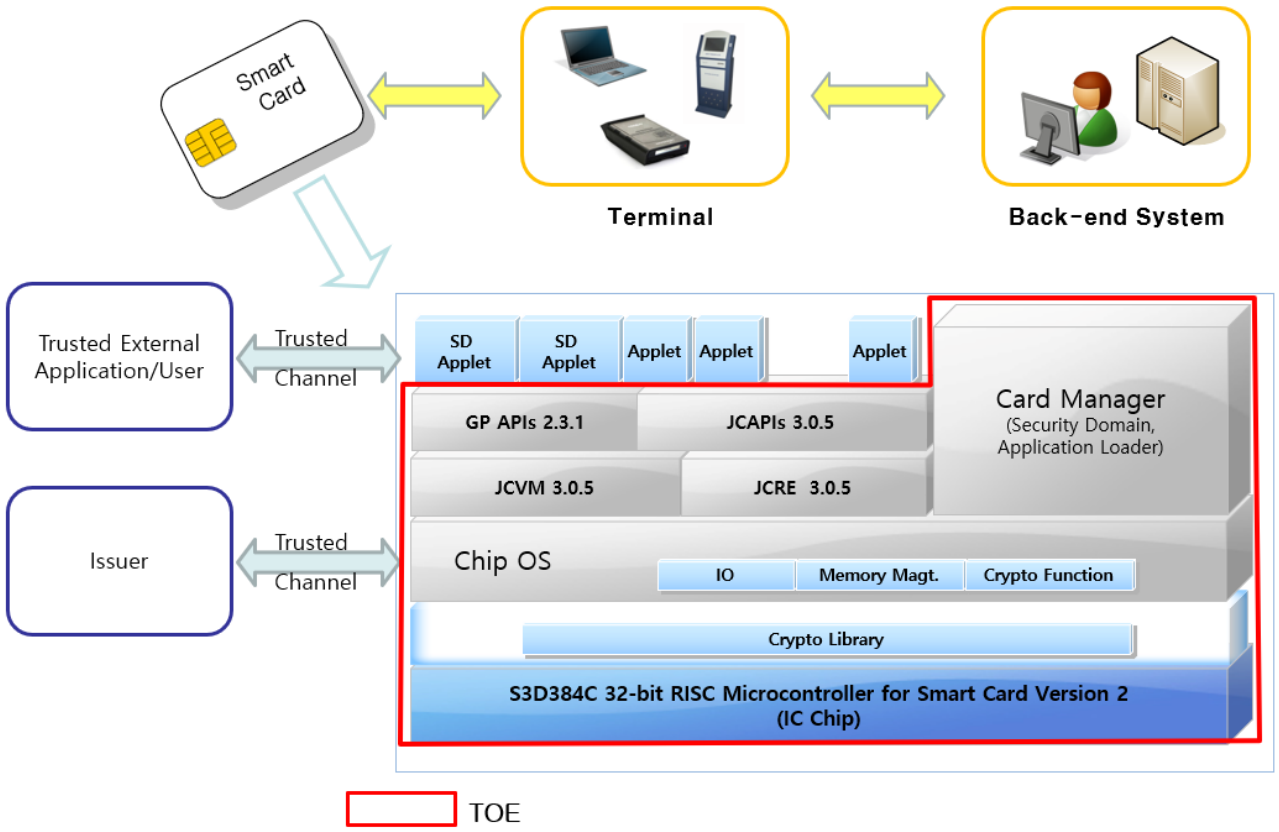
1.4 TOE Description

1.4.1 TOE Operational Environment

[Figure 1] visualizes the relationship between the TOE and the service system (i.e. terminal and servers), briefly illustrating the hierarchy and TOE scope of a multi-functional smart card. A smart card exchanges information needed for the service system (i.e. terminal and servers) through contact/contactless communication. As shown in [Figure 1], the IC hardware (i.e. micro-controller), crypto library is included in the composite TOE evaluation elements. Application layers of a TOE-embedded smart card and test software implemented on memory for testing hardware functions are excluded from the composite TOE evaluation elements. Also the TOE uses IC security

countermeasures to carry out its own functions.

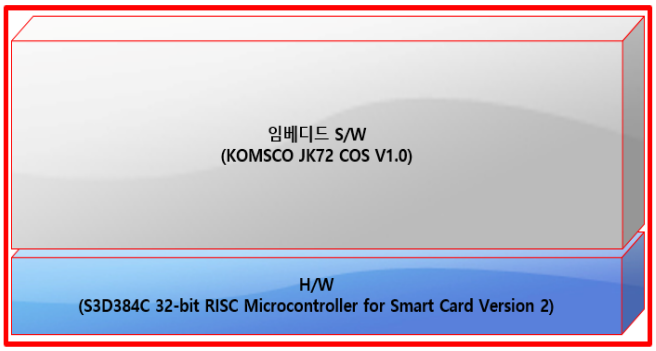
In other words, the TOE is the Javacard that includes a smart card operating system and the IC Chip and excludes applications installed. Smart card owners and issuers generally work through communication with system via the smart card terminal. The issuers carry out administrative tasks such as application installation, issuance and repair by using the issuance system and the smart card terminal; the owners use smart card functions through communication with operational system via the terminal. Here the smart card terminal, operation servers and application constitute the TOE operational environment.



[Figure 1] Operational Environment of TOE

1.4.2 Physical Scope of TOE

The physical scope of TOE is composed of a software that constitutes the Javacard platform as an open platform card operating system developed by KOMSCO, S3D384C, which are CC EAL6+-certified smart card IC Chips, and Cryptographic libraries of Samsung. The TOE software is converted into a binary image. And then the TOE is loaded in the FLASH area of an IC Chip and run with data in FLASH and RAM. The physical scope of TOE also includes “operational user guidance” and “preparative procedures” that are distributed to end users in the form of electronic document to ensure safe TOE operation.



[Figure 2] Physical Scope of TOE

The physical scope of TOE is conceptually composed of the following six parts:

- HW(S3D384C 32-bit RISC Microcontroller for Smart Card Version 2)
- Embedded SW(KOMSCO JK72 COS V1.0)

For the safe management of TOE, the user manual is offered to the end user in the form of electronic document format). The user manual distributed to the end user is also included in the physical scope of TOE and is identified as follows:

- [JK72-MA-0002] Operational user guidance -v1.3
- [JK72-MA-0001] Preparative procedures -v1.4

TOE and TOE components are completely identified by information located in the following table.

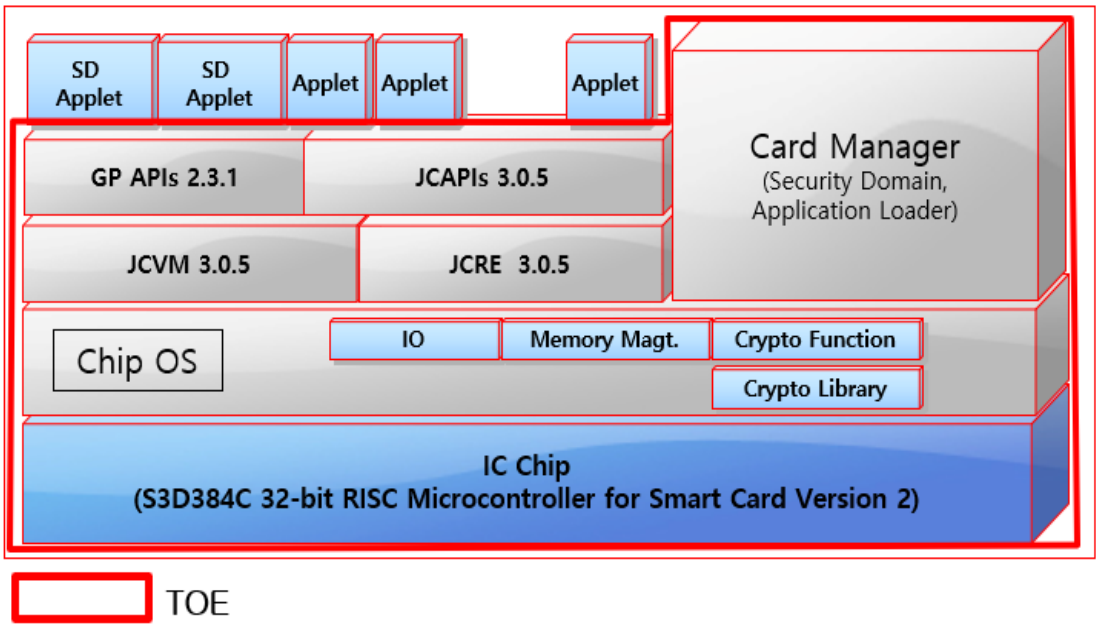
[Table 5] TOE and TOE component identification, delivery

content	Name	Version	Delivery
TOE	KOMSCO JK72 V1.0 (JK72-D38C02-R1)	V1.0	COB / direct delivery
HW	S3D384C 32-bit RISC Microcontroller for Smart Card	Version 2	COB / direct delivery
Embedded SW	KOMSCO JK72 COS V1.0 (PKA_Lib_AT1_v4.03.lib, S3D384C_PTG2_DTRNG_library_v3.2.lib) (JK72-D38C02-R1.hex)	V1.0	Flash code / PGP email
Guidance	[JK72-MA-0002] Operational user guidance-v1.3 - Operational user guidance- v1.3.pdf - Operational user guidance -v1.3.pgp	v1.3	Document / PGP email
	[JK72-MA-0001] Preparative procedures-v1.4 - Preparative procedures-v1.4.pdf - Preparative procedures -v1.4.pgp	v1.4	

Note: The composite evaluation components include CC EAL6+-certified IC Chip and cryptographic library. The TOE does not include the application although it is possible to load the application on the FLASH of IC Chip. That is out of scope in the ST.

1.4.3 Logical Scope of TOE

The TOE is the Javacard Platform that supports the analysis of security violation, the cryptographic operation, the access Control, the identification and authentication, the security management, and TSF protection function. The TOE is composed of the following logical scope that described in “Smart Card Open Platform Protection Profile V2.2, 2010.12.20, Korea Internet & Security Agency.”



[Figure 3] Logical Scope of TOE

- Card Manger(CM)
- Javacard Runtime Environment (JCRE) 3.0.5
- Javacard Virtual Machine (JCVM) 3.0.5
- Javacard Application Programming Interfaces(JCAPIs) 3.0.5
- Global Platform Application Programming Interfaces(GP APIs) 2.3.1
- Chip Operating System (Chip OS) with Cryptographic library
  - PKA_Lib_AT1_v4.03.lib
  - S3D384C_PTG2_DTRNG_Library_v3.2.lib

Crypto	Crypto library/Implementation	Remark
RSA 2048bit	- PKA_Lib_AT1_v4.03.lib - Implementation(SW): PKCS#1 V1.5, V2.1(PSS), OAEP	Platform library & Implementation(SW)
ECDSA 192,224,256,384,512bit	PKA_Lib_AT1_v4.03.lib	Platform library
ECDH 192,224,256,384,512bit		
SHA-2		

TDES 112,168bit AES 128,192,256bit	Implementation + Use chip HW	TOE
SEED 128bit ARIA 128,192,256bit SHA-3 CRC16/CRC32	Implementation(SW)	TOE
DTRNG	S3D384C_PTG2_DTRNG_Library_v3.2.li	Platform library

1.4.3.1 Card Manager

The Card Manager controls the TOE and applets Life Cycles and provides Key and applet management functions of TOE with administrator authority in the TOE user mode.
The TOE manages applets through applet's load, install and delete functions and life cycle management function of Card Manager. The TOE enforces the security policy of the card issuer, and provides the security services as the secure channel management during data transaction and data access and PIN management for Card holder authentication.

Notes: The Card Manager controls the identification and authentication of TOE, security functions, security attributions, TSF data, and secure roles. And it has the administrator authority in the TOE user mode.
Notes: The TOE provides SCP02/SCP03 authentication, DAP authentication, and DM authentication in the user mode. When working together with an external system, the TOE performs SCP02/SCP03 authentication to identify and authenticate the external system's nodes for the mutual safety of paths and channels and checks if the card issuer is an authorized one and guarantees the safety of channel. It ensures the integrity of messages through secure channels and their confidentiality through message encryption. When authentication protocol is closed, the TOE deletes TSF data and initializes the security level so that the information is not reused. The TOE verifies the integrity of applets and authorizes application providers through DAP authentication based on the public keys of authorized application providers. When the issuer wants to charge the issuance authority to a second issuer, the TOE carries out DM authentication that a second issuer delivers information of given applets to the issuer, receives tokens of these applets, submits them to the TOE and obtaining the issuance authority. This second issuer (commissioned issuer) issues cards through SCP02/SCP03 authentication or DAP authentication.

1.4.3.2 JCRE (Javacard Runtime Environment)

The JCRE, that is Javacard System Component running in the TOE, is responsible for the resource management during java applet running, the selected applet management, the communication with CAD and the security of applet. And the JCRE performs running applets using JCVM. The JCRE includes the frameworks related to the APDU routing, ISO communication protocol, JCVM and the classes for handling.
The TOE provides the firewall access control through JCRE. By isolating a single applet within the given space through the mechanism of firewall between applets, it prevents data from being leaked out by other applets and provides protection against hacking. In other words, it prevents that the object generated by applet is used by other applet without explicit sharing. And it prevents unauthorized access about field or method of an instance of a class, as well as length or the contents of an array.
Applet Firewall is considered the primary security feature. If necessary, it performs additional

mechanisms sharing objects using the concept of the static public variables and the SIO (shareable interface objects).

1.4.3.3 JCVM (Javacard Virtual Machine)

The JCVM has organic relationship with JCVM and executes the CAP file as entity of the applet. It performs byte-code execution, memory allocation management, object management, security features, etc., The JCVM is byte code interpreter based on Javacard Specification 3.0.5 appropriately designed for the smart card system and the Java language subset.
The Javacard applet's methods are converted to byte code can be performed on the JCVM. The process that converts it into machine code that can be understood by the hardware referred to as interpreting. TOE can run the applet independent from the hardware through JCVM.
Notes: Because JCRE use JCVM to run the applet, so JCVM may be considered as part of JCRE. JCVM make through the JCRE or JCAPI so that the applet access to resources.

Note : JCVM can be a part of JCRE because JCRE executes any applet using JCVM. JCVM allows any applet to access any resource via JCAPI or JCRE.

1.4.3.4 JCAPIs (Javacard Application Programming Interfaces)

JCAPI is the set of classes provided for development of application according to Java Specification. JCAPI provides primary APIs and extended APIs packages according to Javacard Application Programming Interfaces (JCAPIs) 3.0.5. JCAPI is the upper layer of JCRE, provides the interface for cryptographic functions and basic functions of application.
TOE performs cryptographic computation such as cryptographic key generation/destruction, encryption, decryption, and electronic signature generation and verification. It also supports hash value generation and random number generation. The TOE provides these functions for applications through the interface of JCAPI 3.0.5. Below is a list of algorithms supported by the TOE:

1.4.3.5 GP APIs (Global Platform Application Programming Interfaces)

Global Platform APIs is Javacard Interfaces of Global Platform function. It provides access to the OPEN, services for the application such as cardholder verification, personalization, security services and Card Content Management service such as card locking, application life cycle state update.

1.4.3.6 Chip Operating System

The Chip Operating System is hardware abstraction layer. It is responsible for operating system to run JCVM and JCRE and include low level I/O function, memory management function, low level transaction and crypto functions.
The TOE provides the administrator mode and user mode. The TOE provides initialization authentication in the administrator mode and SCP02/SCP03 authentication, DAP authentication and DM authentication in the user mode. Through initialization authentication in the administrator mode, it confirms the authorized administrator and initializes the TOE.
The Crypto functions provide algorithms supported by IC Chip using hardware accelerator. TDES and AES are implemented with both IC Chip hardware accelerator and software, and RSA and ECC are provided through cryptographic libraries implemented using modular multiplication accelerator. CRC is supported in IC Chip hardware itself. Also Crypto functions provide software cryptographic algorithm such as SEED, ARIA and SHA.

1.4.3.7 Cryptographic Library

Cryptographic Library belongs to the TOE hardware, certified as CC EAL6+ by IC Chip Manufacturer. The cryptographic library supports following functions.

- RSA, ECC, SHA

The primary functions are implemented in the Crypto Functions of the Chip Operating System through cryptographic libraries implemented using modular multiplication accelerator. And they are supported through JCAPIs.

The following summarizes the functions supported by IC chip that is used by composite TOE,

the functions supported by IC chip		TOE usage
Security Related Features	・TDES (scope : 112, 168 bits) (provided in S3D384C IC hardware)	Use (112, 168 bits)
	AES (scope : 128, 192, 256 bits) (provided in S3D384C IC hardware))	Use (128, 192, 256 bits)
	RSA (scope : 2048 ~ 4096 bits) (provided in Cryptographic library)	Use (2048 bits)
	ECC (scpoe : 192 ~ 521 bits) (provided in Cryptographic library)	Use (192 ~ 521 bits)
	Hash (scope : SHA 224 ~ 512 bits) (provided in software)	Use (224 ~ 512 bits)
	DTRNG(Digital True Random Number Generator)	Use
	Detectors & Security Logic	Use
	Memory management (MPU)	Use
	Timer	Use
Communication Features	ISO7816 Contact Interface	Use
	ISO14443 TypeA RF Interface	Use

And usage and the encryption algorithm are supported by the TOE as follows.

[Table 6] Support algorithm and usage

	Algorithm	Usage
TSF	TDES (112, 168 bits) in ECB/CBC mode	Data Encryption/Decryption, Generation and Verification of MAC (provided in IC hardware)
	AES(128, 192, 256 bits) in ECB/CBC mode	Data Encryption/Decryption, Generation and Verification of MAC (provided in IC hardware)
	RSA (2048 bits)	Data Encryption/Decryption, Generation and Verification of signature (provided in IC hardware and Cryptographic library)
	ECC (192, 224, 256, 384, 512 bits)	Generation and Verification of signature (provided in IC hardware and Cryptographic library)
	ECDH (192, 224, 256, 384, 512 bits)	Key agreement protocol (provided in IC hardware and Cryptographic library)
	SEED (128 bits) in ECB/CBC mode	Data Encryption/Decryption, Generation and Verification of MAC (provided in software)
	ARIA (128, 192, 256 bits) in ECB/CBC mode	Data Encryption/Decryption, Generation and Verification of MAC (provided in software)
	CRC32	Integrity of TSF execution code stored in FLASH of IC
	SHA-224/256/384/512	Hash generation for signature, integrity check for execution code of TSF (provided in software)
	PKCS #1 v2.1	Data Encryption/Decryption, Generation and Verification of Signature
Non-TSF	SHA-1, Single DES, RSA 512/768 bits, PKCS #1 v1.5/ISO 9796 padding, etc.	Include in TOE : For compatibility with DAP/DM authentication Security strength is not enough to deal with the possibility of attack corresponding to AVA_VAN.5, so it should not be used except for compatibility with standards.

Notes: Key features of cryptographic algorithm supported by TOE through JCAPIs are implemented in Crypto Functions in Chip Operating System.

1.4.4 TOE Life Cycle

The lifecycle of the TOE is illustrated in [Table 7].

[Table 7] TOE Life Cycle

Phase	Administrator	Description	Remarks
Development	Developer	① TOE design & development (COS, embedded S/W)	Necessary standards may be designed in the “initialization & issuance” phase
Manufacturing	Manufacturer	② IC Chip design/development IC Chip manufacturing IC Chip package IC card manufacturing (IC Chip package embedded in the card)	IC Chip design/development, IC Chip manufacturing are done by a single manufacturer, while IC Chip package and IC card manufacturing may be conducted by different manufacturers It is possible to COS loading at , ,
Initialization & issuance	Developer or issuer	⑥ Initialization ⑦ Card issuance ⑧ Application installation & issuance	The issuer performs , , .
Usage	Owner	⑨ After card issuance, the owner uses the card normally in line with intended purpose	
	Issuer	Application installation & issuance	
Termination of usage	Issuer	⑪ After the owner’s termination of card use, the issuer discontinues the use of the card or collects it for disposal	

The TOE as composite product is generated through the download process at the manufacturing stage. Delivery process in issuer and owner is not included in the evaluation.
In the TOE, developers are directly involved from ① Development through ⑤ IC card manufacturing. Among the internal phases, ②, ③, ④, ⑤ which are the areas of manufacturers alone are not directly correlated with the developers(It is possible to COS loading). After ① Development is completed, developers should distribute the TOE to manufacturers for ③, ④, ⑤. TOE becomes a product after being initialized by data generated by developers in Phase ⑥, ⑦, ⑧ and becomes available for issuers or for users via issuers.

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**.

1.6 Glossary

The terms used in the Security Target follow those of the Common Criteria in case they are same.

Development environment
Environment in which the TOE is developed

Object
A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations

Attack potential
Measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources, and motivation

Iteration
Use of the same component to express two or more distinct requirements

Security objective
Statement of intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions

ST, Security Target
Implementation-dependent statement of security needs for a specific identified TOE

ST Evaluation
Assessment of an ST against defined criteria

Security attribute
Property of subjects, users (including external IT products), objects, information, sessions and/or resources that are used in defining the SFRs and whose values are used in enforcing the SFRs

Assurance
Grounds for confidence that a TOE meets the SFRs

PP, Protection Profile
Implementation-independent statement of security needs for a TOE type

User
See "External Entity”

Selection
Specification of one or more items from a list in a component

Guidance documentation
Documentation that describes the delivery, preparation, operation, management and/or use of the TOE

Smartcard Terminal
A device which has a keypad, display, security module, and Smartcard read/write functions.

Identity
A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Trusted path
A means by which a user and a TSF can communicate with the necessary confidence

Secure state
State in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs

Trusted channel
A means by which a TSF (TOE Security Functionality) and another trusted IT product can communicate with necessary confidence

Element
Indivisible statement of a security need

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

Operation (on a component of the CC)
Modification or repetition of a component. Allowed operations on components are assignment, iteration, refinement, and selection.

Operation (on a subject)
A specific type of action performed by a subject on an object

Operational environment
Environment in which the TOE is operated

External Entity
Entity (human or IT entity) possibly interacting with the TOE from outside of the TOE boundary

Threat Agent
Unauthorized user or external IT entity that makes threat like illegal access, modification and deletion to the asset.

Authorized Issuer
Authorized User who safely operate and manage functions according to TOE Security Policy

Authorized User
TOE user who may, in accordance with the SFRs, perform an operation

Authentication Data
Information used to verify the claimed identity of a user

Assets
Entities that the owner of the TOE presumably places value upon

Refinement
specifies additional details to a component.

Organizational Security Policies
A set of security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

Dependency
Relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package

Subject
An active entity in the TOE that performs operations on objects

Augmentation
Addition of one or more requirement (s) to a package

Component
The smallest selectable set of elements on which requirements may be based

Class
A set of CC families that share a common focus

Evaluation
Assessment of a PP, an ST or a TOE, against defined criteria

TOE (Target of Evaluation)
A set of software, firmware and/or hardware possibly accompanied by guidance

EAL (Evaluation Assurance Level)
A set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

Family
A set of components that share a similar goal but differ in emphasis or rigour

Package
A named set of either security functional or security assurance requirements (ex: ‘EAL 4’)

Assignment
The specification of an identified parameter in a component (of the CC) or requirement

Applet
The name is given to a Javacard technology-based user application. An applet is the basic piece of code that can be selected for execution from outside the card. Each applet on the card is uniquely identified by its AID.

IC Chip (Integrated Circuit Chip)
A semiconductor for Smartcard functions, and it has FLASH, RAM and I/O port.

JCAPI (Javacard Application Programming Interface)
JCAPI is used to compose the application of Javacard, is the interface for functions defined java framework and extended java package. JCAPI is a subset of the Java™ programming language.

Package
A Package is a name space within the Java programming language that may contain classes and interfaces. A Package defines either a library or applet definitions and is divided in two sets of files: export files and CAP files.

RAM (Random Access Memory)
A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. There are two basic types of RAM: dynamic RAM (DRAM), static RAM (SRAM). The two types differ in the technology they use to hold data, dynamic RAM being the more common type. Dynamic RAM needs to be refreshed thousands of times per second. Static RAM does not need to be refreshed, which makes it faster; but it is also more expensive than dynamic RAM. Both types of RAM are volatile, meaning that they lose their contents when the power is turned off.

FLASH Memory
Flash memory is an electronic non-volatile computer storage medium that can be electrically erased and reprogrammed.

TSF, TOE Security Functionality
Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

TOE resource
Anything useable or consumable in the TOE

TOE evaluation
Assessment of a TOE against defined criteria

TSF Data
Data for the operation of the TOE upon which the enforcement of the SFR relies

TSF Executable Code
Binary image code as TOE SW

1.7 Security Target Organization

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 defines the references and abbreviations used in this ST

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.

2. Conformance claims

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

2.1 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 5, April 2017, CCMB-2017-04-001
  - Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002
  - Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003
- Conformance to Common Criteria
  - Extended to Conformance to Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5
  - Conformant to Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5

Note: To be specified in parallel as “Common Criteria” from below

2.2 PP Conformance Claim

This ST conforms to the following Protection Profile.

- Protection Profile Identification
- Smart Card Open Platform Protection Profile v2.2(KECS-PP-0097a-2008), December 20, 2010

The TOE includes an Integrated Circuit certified with CC EAL6+. The IC Chips conform to “Security IC Platform Protection Profile, Version 1.0, 13 January 2014” (BSI-CC-PP-0084-2014) (“ICPP” from below).

2.3 Package Conformance

This security target adds the following package of assurance requirements. This is added by the conformed Protection Profile.

- EAL5+ augmented with ALC_DVS.2, AVA_VAN.5

2.4 Rationale of Conformance Claim

This security target conforms to the Protection Profile, as required in Smart Card Open Platform Protection Profile v2.2 (to be specified as “SCOP-PP” from below; the specification of version omitted), as follows:

- Smart Card Open Platform Protection Profile v2.2 , “Demonstrable Conformance to Protection Profile”

The rationale of Conformance Claim for Protection Profile of this ST is based on the following.

2.4.1 Rationale of Protection Profile Conformance

The conformed Protection Profile is specified in line with “Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 3,” and this security target is prepared in line with “Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5.” However, the types of them remain consistent as no change has been made regarding the consistency of types and structures in the conformed Protection Profile and this security target.

TOE type of SCOP-PP is defined as an open platform that includes smart card operation system, execution environments, and management programs, except for IC chip and applications on board.

Composite TOE consists of IC chip(certified) and Java card based on open platform COS.

Thus, since TOE type (open platform) of SCOP-PP includes the TOE type of security target (Java card platform), it is consistent with the TOE type. TOE excluded IC chip from SCOP-PP. But, Security target includes certified IC chip.

2.4.2 Rationale of Conformance Claim for Security problem definition

This security target defines security problems relating to threats, organizational security policies and assumptions in the same way (or more limited way than) as SCOP-PP does. Therefore, the following tables show that this security target is consistent to SCOP-PP. It redefines added P.IC Chip in more limited way than SCOP-PP.

[Table 8] Rationale of Conformance Claim for Security problem definition-threats

Division	threats	Rationale
SCOP-PP ACCEPTANCE	T.Logical_Attack	This security target defines same operations allowed in SCOP-PP for threats on the left.
	T.Issuance_Misuse	
	T.Illegal_Terminal_Use	
	T.Illegal Program	
	T.Unintentional_Failure	
	T.Continuous_Authentication_Attempt	
	T.Intentional_Triggering_of_Failures	
	T.Residual_Information	
	T.Information Disclosure	

[Table 9] Rationale of Conformance Claim for Security problem definition –Organizaitonal Security policy

Division	Organizational security policy	Rationale
SCOP-PP ACCEPTANCE	P.Open_Platform	This security target defines restricted operations allowed in SCOP-PP for organizational security policy on the left.
	P.Role_Division	This security target defines same operations allowed in SCOP-PP for organizational security policy on the left.
	P.IC Chip	Because the Composite TOE includes EAL6+ certified IC Chip, It is added. Then the security problem definition of the Composite ST is more limited than SCOP-PP.

[Table 10] Rationale of Conformance Claim for Security problem definition -Assumptions

Division	Assumptions	Rationale
SCOP-PP ACCEPTANCE	A.Trusted_Path	This security target defines restricted operations allowed in SCOP-PP for assumptions on the left.
	A.Application_Program	This security target defines same operations allowed in SCOP-PP for assumptions on the left.
	A.TOE_Management	
	A.TSF_Data	
EXCEPTION	A.Underlying_Hardware	Because the Composite TOE includes IC Chip, the security features of IC Chip is excluded from Assumptions. It is redefined as Organizational Security Policy.
ADDITION	A.Process-Sec-IC	Because the Composite TOE includes EAL6+ certified IC Chip, It is added. Then the security problem definition of the Composite ST is more limited than SCOP-PP.

2.4.3 Rationale of Conformance Claim for Security objectives

The following tables show that the security objectives of composite security target is consistent to SCOP-PP. This security target redefines O.Information Leakage and adds O.IC Chip in more limited way than SCOP-PP.

[Table 11] Rationale of Conformance Claim for Security objectives-TOE security objectives

Division	TOE Security Objectives	Rationale
SCOP-PP ACCEPTANCE	O.Identification	This security target defines same or restricted in SCOP-PP for TOE security objectives on the left.
	O.Authorized_Failure_Repair	
	O.Authentication	
	O.Residual_Information_Deletion	
	O.Information_Disclosure_Handling	

	O.Open_Platform	By changing 'application' to 'authorized application' and specifying more restrictively than SCOP-PP, it satisfies provable Protection Profile compliance.
	O.Data_Protection	By adding data protection and specifying more restrictively than SCOP-PP, it satisfies provable Protection Profile compliance.
	O.Issuance and Management	By changing personalization and management for smart card and specifying more restrictively than SCOP-PP, it satisfies provable Protection Profile compliance.
	O. Automated_Recovery/ Correspondence failure	By adding actions for potential security violation detection and specifying more restrictively than SCOP-PP, it satisfies provable Protection Profile compliance.
	O.IC Chip	Since the TOE is a composite product and the IC chip is included in the TOE scope, the security characteristics of the IC chip have been changed from the security objectives for the operating environment (OE. Sub-hardware) to the TOE security objectives. Proved to be more restrictive than its security objectives

[Table 12] Rationale of Conformance Claim for Security objectives - operational environment

Division	Security objectives for operational environment	Rationale
SCOP-PP ACCEPTANCE	OE.Training	This security target defines same or restricted in SCOP-PP for TOE security objectives for operational environment on the left.
	OE.TSF_Data	
	OE.Application_Program	Because installing any application in TOE complies with authorized processes, ST's security objective is more restrictive than compliant SCOP-PP's one.
	OE.Trusted_Communication	Because any application installed in TOE communicates by smart card readers, ST's security objective is more restrictive than compliant SCOP-PP's one.
EXCEPTION	OE.Underlying hardware	Because the Composite TOE includes IC Chip, the security features of IC Chip is excluded from security objectives for operational environment.
ADDITION	OE.Process-Sec-IC	This security target defines restricted in SCOP-PP for TOE security objectives for operational environment on the left.

Note: TOE is a composite product that includes an IC chip, and has changed the security objective OE. underlying-hardware for the operating environment to the security objective O.IC chip of the TOE.

2.4.4 Rationale of Conformance Claim for Security functional requirements

The rationale of conformance claims for security functional requirements is provided in [Table 13], which demonstrates that the extended security functional requirements of this security target are equal to (or more limited than) those of SCOP-PP.

[Table 13] Rationale of Conformance Claim for Security functional requirements

Division	Component	Rationale
SCOP-PP ACCEPTANCE	FAU_ARP.1	This security target performs operations allowed in SCOP-PP for functional components suggested on the left.
	FAU_SAA.1	
SCOP-PP ACCEPTANCE	FCS_CKM.1(1)	This security target performs operations allowed in SCOP-PP for FCS_CKM.4 among the functional components on the left and is thus equal to SCOP-PP. It is more limited than SCOP-PP as it carries out “Iteration” operations allowed in the Common Criteria for FCS_CKM.1(1)~(3) and FCS_COP.1(1) ~(7) and specifies additional cryptographic computation. Also this composite security target additionally defines FCS_CKM.2 for cryptographic key distribution provided by cryptographic library. And this composite security target additionally defines FCS_RNG.1 based on IC-PP.
	FCS_CKM.1(2)	
	FCS_CKM.1(3)	
	FCS_CKM.4	
	FCS_COP.1(1)	
	FCS_COP.1(2)	
	FCS_COP.1(3)	
	FCS_COP.1(4)	
	FCS_COP.1(5)	
	FCS_COP.1(6)	
	FCS_COP.1(7)	
ADDITION	FCS_CKM.2	
ADDITION	FCS_RNG.1	
SCOP-PP ACCEPTANCE	FDP_ACC.2(1)	This security target performs operations allowed in SCOP-PP for FDP_ RIP.1 among the functional components suggested on the left and is thus equal to SCOP-PP. It is more limited than SCOP-PP as it carries out “Iteration” operations allowed in the Common Criteria for FDP_ACC.2(1) ~ (2) and FDP_ACF.1(1) ~ (2) and specifies additional requirements for user data protection.
	FDP_ACC.2(2)	
	FDP_ACF.1(1)	
	FDP_ACF.1(2)	
	FDP_RIP.1	
ADDITION	FDP_SDI.2	This security target additionally defines SFRs for the integrity test of saved data, response behaviors and the integrity of transmitted data. It is more limited than SCOP-PP as it defines additional security functional requirements for TSF protection.
	FDP_UCT.1	
	FDP_UIT.1	
SCOP-PP ACCEPTANCE	FIA_AFL.1	This security target carries out operations allowed in SCOP-PP for FIA_AFL.1, FIA_SOS.1, FIA_UAU.4, FIA_UAU.6 and FIA_UID.1 among the functional components suggested on the left and is thus equal to SCOP-PP. It is more limited than SCOP-PP as it carries out “Iteration” operations allowed in the Common Criteria for FIA_ATD.1(1) ~ (2) and FIA_UAU.1(1) ~ (5) among the functional components on the left to specify additional authentication.
	FIA_ATD.1(1)	
	FIA_ATD.1(2)	
	FIA_SOS.1	
	FIA_UAU.1(1)	
	FIA_UAU.1(2)	
	FIA_UAU.1(3)	
	FIA_UAU.1(4)	

	FIA_UAU.1(5)	
	FIA_UAU.4	
	FIA_UAU.6	
	FIA_UID.1	
ADDITION	FIA_USB.1	This security target additionally defines SFRs for user-subject binding. It is more limited than SCOP-PP as it defines additional security functional requirements for identification and authentication.
SCOP-PP ACCEPTANCE	FMT_MOF.1	This security target performs operations allowed in SCOP-PP for FMT_MOF.1, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_SMF.1 and FMT_SMR.1 among the functional components suggested on the left.It is more limited than SCOP-PP as it carries out “Iteration” operations allowed in the Common Criteria for FMT_MSA.1(1) ~ (2) among the functional components on the left to specify additional security management requirements.
	FMT_MSA.1(1)	
	FMT_MSA.1(2)	
	FMT_MSA.3	
	FMT_MTD.1	
	FMT_MTD.2	
	FMT_SMF.1	
	FMT_SMR.1	
SCOP-PP ACCEPTANCE	FPR_UNO.1	This security target performs operations allowed in SCOP-PP for functional components suggested on the left.
SCOP-PP ACCEPTANCE	FPT_FLS.1	This security target performs operations allowed in SCOP-PP for functional components suggested on the left. Also this composite security target additionally defines FPT_PHP.3 for resistance to physical attack and is limited than SCOP-PP.
	FPT_RCV.3	
	FPT_RCV.4	
	FPT_TST.1	
ADDITION	FPT_ITC.1	It is more restrictive than SCOP-PP because it defines additional requirements for inter-TSF transfer data protection.

2.4.5 Rationale of Conformance Claim for Assurance Requirements

The rationale of conformance claims for assurance requirements is specified in [Table 14], which shows that the assurance requirements of this security target are equal to (or more limited than) those of SCOP-PP. The assurance requirements security target meet includes all assurance requirements of SCOP-PP and is added these of EAL5+(augmented ALC_DVS.2, AVA_VAN.5) based on Common Criteria. The added assurance requirements are followings.

- ADV_FSP.5 Complete semi-formal functional specification with additional error information
- ADV_INT.2 Well-structured internals
- ADV_TDS.4 Semiformal modular design
- ALC_DVS.2 Sufficiency of security measures
- ALC_CMS.5 Development tools CM coverage
- ALC_TAT.2 Compliance with implementation standards
- ATE_DPT.3 Testing: modules design
- AVA_VAN.5 Advanced methodical vulnerability analysis

[Table 14] Rationale of Conformance Claim for Assurance requirements

Assurance Class	Assurance Components	Rationale

ASE: Security Target	ASE_INT.1 ST introduction	This security target provides assurance requirements equivalent to EAL 5+. This security target includes all assurance requirements of SCOP-PP and is added ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_DVS.2 , ALC_CMS.5, ALC_TAT.2, ATE_DPT.3, AVA_VAN.5. Then the assurance requirements of Composite TOE is more limited than SCOP-PP.
	ASE_CCL.1 Conformance claims	
	ASE_SPD.1 Security problem definition	
	ASE_OBJ.2 Security objectives	
	ASE_ECD.1 Extended components definition	
	ASE_REQ.2 Derived security requirements	
	ASE_TSS.1 TOE summary specification	
ADV: Development	ADV_ARC.1 Security architecture description	
	ADV_FSP.5 Complete semi-formal functional specification with additional error information	
	ADV_IMP.1 Implementation representation of the TSF	
	ADV_INT.2 Well-structured internals	
	ADV_TDS.4 Semiformal modular design	
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	
	AGD_PRE.1 Preparative procedures	
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation	
	ALC_CMS.5 Development tools CM coverage	
	ALC_DEL.1 Delivery procedures	
	ALC_DVS.2 Sufficiency of security measures	
	ALC_LCD.1 Developer defined life-cycle model	
	ALC_TAT.2 Compliance with implementation standards	
ATE: Tests	ATE_COV.2 Analysis of coverage	
	ATE_DPT.3 Testing: modules design	
	ATE_FUN.1 Functional testing	
	ATE_IND.2 Independent testing - sample	
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis	

3. Security problem definition

The security problem definition defines the threats, the organizational security policies and the assumptions to be addressed by the TOE and the operational environment of the TOE.

3.1 Assets

TOE is a Javacard platform that is run on the IC Chip to manage information and resources. Its assets are divided into “primary assets” and “secondary assets.”

The security objective of the TOE is to protect primary assets during the usage phase. The information and tools used in the manufacturing and development of smart cards need to be protected to defend these primary assets, and these information and tools are called secondary assets. In other words, the information generated or utilized in the process of TOE production does not constitute assets that are directly protected by the TOE, but it significantly affects the integrity or confidentiality of the TOE itself. This information is called secondary assets, and the safety of secondary assets is satisfied by EAL5+ assurance requirements.

The primary assets that the TOE needs to protect are data managed in the smart card; they are divided into user data and TSF data. The former refers to data generated for or by the users, while the latter is data generated for or by the TOE. Smart cards are carried and used by users, so they are the subjects that the attackers seek to steal. Therefore, the IC Chips themselves are assets that need to be protected from physical threats.

These assets have to do with TOE threats and can be classified as follows:

- User data
- TSF data

The next section describes in detail the user data and TSF data among primary assets that the TOE needs to protect.

3.1.1 User Data

User data include certain PINs, authentication data, application codes and sensitive application values of applications that need to be protected from unauthorized exposure and modification.

D.APP_CODE
This is the code of the applets and libraries loaded on the TOE and shall be protected from unauthorized modification.

D.APP_DATA
This is sensitive data of the applications, like the data contained in an object, a static field of a package, a local variable of the currently executed method, or a position of the operand stack and shall be protected from unauthorized modification.

D.PIN
This is user PIN and shall be protected from unauthorized disclosure and modification.

D.APP_KEYs
This is cryptographic keys owned by the applets and shall be protected from unauthorized disclosure and modification.

3.1.2 TSF Data

TSF data include the initialization data, the configuration data, the cryptographic keys, random for

key generation that shall be protected from unauthorized disclosure and modification and all data using by TOE for the security feature of TOE.

D.TS_CODE
This is TOE system code and shall be protected from unauthorized disclosure and modification.

D.TS_KEYs
This is TOE system key, that is, the cryptographic key used when loading a file into the card and IK, TK for the card initialization

D.TS_DATA
This is TOE system data, the internal runtime data areas necessary for the execution of the JCVM and shall be protected from monopolization and unauthorized disclosure or modification

D.SEC_DATA
This is the runtime security data of the JCRE of TOE and shall be protected from unauthorized disclosure and Modification

D.CRYPTO
This is cryptographic data used in runtime cryptographic computations, like a seed used to generate a key and shall be protected from unauthorized disclosure and modification.

3.2 Threats

Threat agents are generally IT entity or users that illegally accesses and abnormally damage TOE and security target system. Threat agents hold medium level of professional knowledge, resources and motives

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

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

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.

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.

T.Unintentional_Failure
User 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.

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

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.

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

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

3.3 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 open platform that can be loaded with authorized application programs

P.Role_Division
The role is divided per each responsible person from the stage of the Smart Card manufacturing to the stage of use. The TOE must be manufactured and managed with secure method according to the role.

P.IC Chip
The TOE must ensure secure operation on a tamper-resistant IC Chip, and the Underlying hardware of the TOE shall provide means to counter various tampering attacks.

3.4 Assumptions

It is assumed that the following terms exist in the TOE operation environment accepting this Security Target.

A.Trusted_Path
There is trusted path between the Application which is installed in the TOE and the Smart Card terminal, the communication target of the TOE.

A.Application_Program
When installing the application program in the TOE, the approved procedures must be followed. Also, the legitimately installed the application program does not contain malicious code.

A.TOE_Management
The stage from the TOE manufacturing to use is divided of the roles, such as the manufacturer, the issuer and the holder. Appropriate training is necessary according to the regulations prescribed per each role. Also, repair and replacement due to defect of the TOE or the Smart Card are processed with secure method.

A.TSF_Data
The TSF data exported to the outside of the TOE, therefore handled in the course of the TOE

operation are securely managed.

Application note : TSF data processed outside the TOE are the Implementor Key (IK) and Transport Key (TK) used in the process of initializing the TOE. Since it is used only in the process of initializing the TOE, it is assumed that it is safely managed with out being leaked outside the developer and the issuer (administrator), and it is also safely managed between the TOE and the terminal.

<IC chip ST assumptions>

The following are assumptions included in the ST [R18] of the IC chip.

A.Process-Sec-IC Protection during Packaging, Finishing and Personalization

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

This means that the Phases after TOE Delivery are assumed to be protected appropriately

Application note :

This means that the Phases after TOE Delivery are assumed to be protected appropriately

4. Security objectives

This security target defines security objectives by categorizing them into the TOE and the environment. The security objectives for the TOE are directly handled by the TOE. The security objectives for the environment are handled by technical/process-related means so that TOE exactly provides its security functionality.

4.1 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. Also, the TOE shall be protected transmitted user data and TSF data.

O.Issue and Management

The TOE must ensure that the authorized issuer can issue the Smart Card according to the prescribed procedures.

O.Identification

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

O.Authorized_Failure Repair

The TOE must ensure that only the authorized user can repair a breakdown.

O.Authentication

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

O.Automated_Recovery/Correspondence failure

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.

Also, the TOE shall take actions upon detection of a potential security violation.

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_Handling

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

O.Open_Platform

The TOE must support open platform to which authorized application programs can be loaded.

O.IC Chip

The IC Chip, the underlying platform of the TOE, provides the random number generation and cryptographic operation to support security functions of the TOE. It also detects malfunctions of the TOE outside the normal operating conditions and provides the function of physical protection to protect the TOE from physical attacks using the probing and reverse engineering analyses.

4.2 Security objectives for the operational environment

Below are security objectives that need to be handled with technical/procedural means supported in the operational environment in order for the TOE to accurately provide its security functionality:

OE.Training

Operation training must be administered according to the roles of each administrator in the course of the TOE manufacturing, issuance and use.

OE.Trusted_Communication

The trusted path must be provided between the Application which is installed in the TOE and the Smart Card terminal as the communication target of the TOE

OE.Application_Program

The application installation must follow approved procedure, and adequately loaded applications shall not contain malicious code.

OE.TSF_Data

When installing the application program in the TOE, the approved procedures must be followed. Also, the legitimately installed the application program must not contain malicious code.

< Security objective for IC chip ST operating environment >

The following is a security objective for the operating environment included in the ST [R18] of the IC chip.

OE.Process-Sec-IC Protection during composite product manufacturing

Security procedures shall be used after TOE delivery up to delivery to the " consumer" to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

Application Note: This means that Phases after TOE Delivery up to the end of Phase 6 must be protected appropriately. The protection during packaging, finishing and personalization includes also the personalization process (Flash Loader) and the personalization data (TOE software components) during Phase 4, Phase 5 and Phase 6.

4.3 Security Objectives Rationale

The 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 15] Relation between security objectives and the security problem definition

	TOE security objectives Security objectives for the operational environment										Security objectives for the operational environment			
Security objectives / Definition of security problems	O.Data_Protection	O.Issuance and Management	O.Identification	O.Authorized_Failure_Repair	O.Authentication	O.Automated_Recovery/Correspondence failure	O.Residual_Information_Deletion	O.Information_Disclosure_Handling	O.Open_Platform	O.IC Chip	OE.Training	OE.Trusted_Communication	OE.Application_Program	OE.TSF_Data
T.Logical_Attack	X	X	X	X	X									
T.Issuance_Misuse		X											X	
T.Illegal_Terminal_Use	X	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							
T.Information Disclosure								X		X				
P.Open_Platform									X					
P.Role_Division		X	X	X	X						X			
P.IC Chip								X		X				
A.Trusted_Path												X		
A.Application_Program													X	
A.TOE_Management											X			
A.TSF_Data														X

Relation between security objectives and the security problem definition(2)

Security objectives	TOE security objectives Security objectives for the operational environment

Definition of security problems	OE.Process_Sec_IC
A.Process-Sec-IC	X

5. Extended Components Definition

This section describes the components extended from CC Part 2. The components extended from CC Part 3 do not exist.

5.1 Definition of the Family FCS_RNG

To define the IT security functional requirements of the TOE an additional Family (FCS_RNG) of the Class FCS(cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RNG is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.1 is intended for non-cryptographic use.

5.1.1 Generation of random numbers (FCS_RNG)

Family behavior :

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

Component levelling :

FCS_RNG Generation of random numbers	1

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 [selection: *physical, non-physical true, deterministic, hybrid physical*] 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*].

6. Security Requirements

Security requirements specify functional and assurance 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[1]

[Table 16] Subject and Object, related security attribute, operation definition

Subject (user)	Subject (user) security attribute	Object (information)	Object (information) security attribute	Operation
S.APP	Context, Active, Selected	OB.JAVAOBJECT	Sharing, Context, LifeTime	-OP.ARRAY_ACCESS -OP.INSTANCE_FIELD -OP.INVK_VIRTUAL -OP.INVK_INTERFACE -OP.THROW -OP.TYPE_ACCESS -OP.JAVA -OP.CREATE (Sharing, LifeTime)
S.JCRE	None			
S.CM	Lifecycle, Security Level, Privilege	OB.APP	Signature, Context	-OP.LOAD -OP.INSTALL -OP.DELETE
Issuer (Administrator)	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

Note: In [Table 16], the subjects of an active entity within the TOE during TOE operation are S.APP, S.JCRE and S.CM, and the entity as TOE administrator is the issuer.

[Table 17] Subject and Object

Subject/Object	Description
S.APP	It is the application and the subject that provide services to user using APIs of Javacard Platform or GP. It is selected and executed from the external entity and is identified by unique AID. This subject is S.PACKAGE in the [R6]

[1] Subjects (prefixed with an "*S*"), objects (prefixed with an "*OB*") and operations (prefixed with an "*OP*") are used in this document

	and accesses the object of Javacard according to Javacard Firewall access control.
OB.APP	It is the application based on Javacard Platform and Loaded, Installed, Deleted by Card Manager according to CARD CONTENT MANAGEMENT access control.
S.CM	It is the subject of CARD CONTENT MANAGEMENT access control and performs Load, Install, Delete of applet and access control for lifecycle. It is a special S.APP implemented the Card Issuer Policy based on GP or VGP. In this ST, S.CM is administrator or Card Issuer.
S.JCRE	S.JCRE provides the Javacard runtime environment to select an applet, transmit external command and run an applet. Also it is the subject of Javacard Firewall access control and it performs access control to the object of Javacard.
OB.JAVAOBJECT	It is the object of Javacard and the data belongs to S.APP including initialization data, personalization data, KEY, PIN, array and applet. Also it is accessed by applets according to Javacard Firewall access control.

b) External entities

- Smartcard Terminal

6.1 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. [Table 18] summarizes security functional components used in this security target.

[Table 18] Security functional requirements

Security Functional Class	Security Functional Component		Remarks
Security Audit	FAU_ARP.1	Security alarms	SCOPP
	FAU_SAA.1	Potential violation analysis	
Cryptographic Support	FCS_CKM.1(1)	Cryptographic key generation	
	FCS_CKM.1(2)	Cryptographic key generation	
	FCS_CKM.1(3)	Cryptographic key generation	Added (Iteration)
	FCS_CKM.1(4)	Cryptographic key generation	Added (Iteration)
	FCS_CKM.2	Cryptographic key distribution	Added
	FCS_CKM.4	Cryptographic key destruction	SCOPP
	FCS_COP.1(1)	Cryptographic operation	
	FCS_COP.1(2)	Cryptographic operation	Added (Iteration)
	FCS_COP.1(3)	Cryptographic operation	Added (Iteration)
	FCS_COP.1(4)	Cryptographic operation	Added (Iteration)
	FCS_COP.1(5)	Cryptographic operation	Added (Iteration)
	FCS_COP.1(6)	Cryptographic operation	Added (Iteration)
	FCS_COP.1(7)	Cryptographic operation	Added (Iteration)

	FCS_RNG.1	Random number generation	Added
User Data Protection	FDP_ACC.2(1)	Complete access control	SCOPPP
	FDP_ACC.2(2)	Complete access control	Added (Iteration)
	FDP_ACF.1(1)	Security attribute based access control	SCOPPP
	FDP_ACF.1(2)	Security attribute based access control	Added (Iteration)
	FDP_RIP.1	Subset residual information protection	SCOPPP
	FDP_SDI.2	Stored data integrity monitoring and action	Added
	FDP_UCT.1	Basic data exchange confidentiality	Added
	FDP_UIT.1	Data exchange integrity	Added
Identification and Authenticatio n	FIA_AFL.1	Authentication failure handling	SCOPPP
	FIA_ATD.1(1)	User attribute definition	
	FIA_ATD.1(2)	User attribute definition	Added (Iteration)
	FIA_SOS.1	Verification of secrets	SCOPPP
	FIA_UAU.1(1)	Timing of Authentication	
	FIA_UAU.1(2)	Timing of Authentication	Added (Iteration)
	FIA_UAU.1(3)	Timing of Authentication	Added (Iteration)
	FIA_UAU.1(4)	Timing of Authentication	Added (Iteration)
	FIA_UAU.1(5)	Timing of Authentication	Added (Iteration)
	FIA_UAU.4	Single-use authentication mechanisms	SCOPPP
	FIA_UAU.6	Re-authenticating	
	FIA_UID.1	Timing of Identification	
	FIA_USB.1	User-subject binding	Added
Security Management	FMT_MOF.1	Management of security functions behavior	SCOPPP
	FMT_MSA.1(1)	Management of security attributes	
	FMT_MSA.1(2)	Management of security attributes	Added (Iteration)
	FMT_MSA.3	Static attribute initialization	SCOPPP
	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_RCV.3	Automated recovery without undue loss	SCOPPP
	FPT_RCV.4	Function recovery	
	FPT_TST.1	TSF testing	
Trusted path/channel s	FTP_ITC.1	Inter-TSF trusted channel	Added

6.1.1 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.

[

List of actions:

a) blocks the action that produces the security violation and throws an exception;

b) locks the card session (to become mute);

c) reinitializes the Javacard System and its data (reset);

d) temporarily disables the services of the card until a privileged roles performs a special action;

e) definitely disables all the services of the card;

f) deletion of memory data

]

Application Notes: This functional requirement may define a variety of response functions to protect data in the smart card if TOE detects any potential external security violation event. When an external attack is detected, the response could be the suspension of card functions or the deletion of memory data.

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 **specified** 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 **specified** events.

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

[

[Table 19] Security violation events

Security violation events
Abnormal environmental conditions (frequency, voltage, temperature)
Physical tampering
Memory failure audited through exceptions in the read/write operations and inconsistency check
Card Manger life cycle inconsistency audited through the life cycle checks in all administrative operations
Corruption of check-summed objects
Applet life cycle inconsistency
Card tearing (unexpected removal of the Card out of the CAD) and power failure
Abortion of a transaction in an unexpected context
Violation of the Firewall or JCVM security policies
Unavailability of resources
Array overflow
Access uninitialized key
Security exception limit excess
Abort Transaction limit excess
Other runtime errors related to applet's failure, like uncaught exceptions
Randomness test for the random number generator is failed

Authentication failed
Cryptography operation failed

]

b) [none]

Application Notes: Refinement operations are undertaken as TOE does not conduct potential violation analysis and auditing record using audited events but utilizes the handling progress of internal events to carry out potential security violation analysis. TSF may perform security alert functions in FAU_ARP.1 through security violation analysis on the check sum values of internal data, errors in resource allocation and authentication failure events.

6.1.2 Cryptographic Support

FCS_CKM.1(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 [TDES] and specified cryptographic key sizes [112bits, 168bits] that meet the following: [[R9], *8. Secure Communication,* [*R10*], *5. Secure Channel*, [R15]*, KeyBuilder*].

FCS_CKM.1(2) 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 [AES] and specified cryptographic key sizes [128bits, 192bits, 256bits] that meet the following: [[R9], *8. Secure Communication,* [*R11*], *4. Specification Amendments*, [R15]*, KeyBuilder*].

FCS_CKM.1(3) 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 [RSA] and specified cryptographic key sizes [RSA 2048bits] that meet the following: [RFC3447 PKCS v2.1-section 3.2, [R15]-*KeyPair , KeyBuilde*],.

Application Note: The key for this security function requirement can be generated or created based on Classes Key Builder of [R15] and Key Pair, and the dedicated crypto processor for the smart

card IC chip included in the TOE or crypto library installed in the IC chip can support the encryption key generation function. For related matters, refer to [R18] of hardware Security Target.

FCS_CKM.1(4) 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 [ECC] and specified cryptographic key sizes [ECC 192, 224, 256, 384, 512bits] that meet the following: [[R28]-A.4.3 Elliptic Curve Key Generation, ISO/IEC 15946-1:2002-section 6.1, [R15]- KeyPair, KeyBuilder].

Application Note: The key for this security function requirement can be generated or created based on Classes Key Builder of [R15] and Key Pair, and the dedicated crypto processor for the smart card IC chip included in the TOE or crypto library installed in the IC chip can support the encryption key generation function. For related matters, refer to [R18] of hardware Security Target.

Note: ECC cryptographic key generation supports crypto function from TOE hardware-like smart card IC chip dedicated crypto processor and crypto library based on [R18] FCS_CKM.1/EC-2. The security is satisfied with the CC EAL6+ assurance requirements of the TOE hardware..

Category	TOE H/W	TOE S/W
Specification	ANSI X9.62-2005,A.4.3 ISO/IEC 15946-1:2002, section 6.1	Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., June 2015, Oracle[R15], KeyPair, KeyBuilder

FCS_CKM.2 Cryptographic key distribution

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 [Elliptic curve Diffie-Hellman key agreement] that meets the following: [the below list of key distribution standards]

[

- ANSI X9.63-2001: Key Agreement and Key Transport Using Elliptic Curve Cryptography, approved November 20, 2001

]

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].

FCS_COP.1 (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 [data encryption and decryption and data signature generation/verification] in accordance with a specified cryptographic algorithm [SEED in ECB/CBC mode] and cryptographic key sizes [128 bits] that meet the following: [the below list of SEED standards].

[

- TTAS.KO-12.0004: 128-bit Symmetric Block Cipher (SEED)

]

FCS_COP.1 (2) 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 [data encryption and decryption and data signature generation/verification] in accordance with a specified cryptographic algorithm [ARIA in ECB/CBC mode] and cryptographic key sizes [128, 192 or 256 bits] that meet the following: [the below list of ARIA standards].

[

- KSX1213 -1 128-bit Symmetric Block Cipher ARIA Part 1, 2014
- KSX1213 -2 128-bit Symmetric Block Cipher ARIA Part 2, 2014

]

FCS_COP.1 (3) 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 [data encryption/decryption and data signature generation/verification] in accordance with a specified cryptographic algorithm [TDES in ECB/CBC mode] and cryptographic key sizes [112, 168 bits] that meet the following: [the below list of TDES standards and].

[

- Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., June 2015, Oracle
- FIPS PUB 46-3, Data Encryption Standard(ANSI X3.92)
- ISO/IEC 9797-1:2011: Information technology Security techniques-Message Authentication Codes(MACs)-Part1:Mechanisms using a block cipher
- NIST SP 800-67, Version 2

]

Note: TDES crypto operation supports crypto functions in the Smartcard IC chip cryptographic processor, which is TOE hardware, in accordance with FCS_COP.1/TDES of [R18], and is software expanded an d implemented in accordance with [R15], and safety is satisfied with the CC EAL6+ assurance requirements of TOE hardware.

Note : NIST SP 800-67 standard allows encryption with 168 bit keys only

Category	TOE H/W	TOE S/W
Crypto algorithm	TDES	TDES in ECB/CBC mode
Crypto operation	encryption and decryption * NIST SP 800-67 standard allows encryption with 168 bit keys only	Data encryption and decryption and MAC generation and verification
Specification	[FIPS SP800-67],	Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., June 2015, Oracle FIPS PUB 46-3, Data Encryption Standard(ANSI X3.92) ISO/IEC 9797-1:2011: Information technology Security techniques-Message Authentication Codes(MACs)-Part1:Mechanisms using a block cipher

FCS_COP.1 (4) 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 [data encryption/decryption and data signature generation/verification] in accordance with a specified cryptographic algorithm [AES in ECB/CBC mode] and cryptographic key sizes [112, 192, 256 bits] that meet the following: [the below list of AES standards and [R12]].

[

- Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., June 2015, Oracle
- FIPS PUB 197(FIPS 197),Advanced Encryption Standard
- NIST SP 800-38A
- ISO/IEC 18033-3
- ISO/IEC 9797-1 Mac Algorithm 1 and 2 respectively

]

Note: AES crypto operation supports crypto functions in the Smartcard IC chip cryptographic processor, which is TOE hardware, in accordance with FCS_COP.1/AES of [R18], and is software expanded and implemented in accordance with [R15], and safety is satisfied with the CC EAL6+ assurance requirements of TOE hardware.

Category	TOE H/W	TOE S/W
Crypto algorithm	AES	AES in ECB/CBC mode
Crypto operation	encryption and decryption	Data encryption and decryption and MAC generation and verification
Specification	[FIPS 197]	Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0. 5., June 2015, Oracle FIPS PUB 197(FIPS 197), Advanced Encryption Standard

FCS_COP.1 (5) 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 [data encryption/decryption and data signature generation/verification] in accordance with a specified cryptographic algorithm [RSA Cipher /Signature] and cryptographic key sizes [2048 bits] that meet the following: [the below list of RSA standards and [R12]].

[

- Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., June 2015, Oracle
- PKCS#1 v2.1 : RSA Cryptography Standard, RSA Laboratories, June 14, 2002
- ANSI X9.31, PKCS#2 and IEEE-P13-63
- ISO/IEC 9796-2:2002: Information technology – Security techniques-Digital signature schemes giving message recovery-Part 2: Integer factorization based mechanism

]

Note: RSA crypto operation supports crypto functions in the Smartcard IC chip cryptographic processor, which is TOE hardware, in accordance with FCS_COP.1/RSA -2 of [R18], and is software expanded and implemented in accordance with [R15], and safety is satisfied with the CC EAL6+ assurance requirements of TOE hardware.

Category	TOE H/W	TOE S/W
Crypto algorithm	RSA:standard RSA and RSA-CRT	RSA Cipher&Signature
Crypto operation	Encryption/Decryption, Signature generation and verification	Data encryption and decryption and data signature generation and verification
Specification	[RFC3447] PKCS v2.1, section 5	Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., June 2015, Oracle PKCS#1 v2.1 : RSA Cryptog raphy Standard, RSA Laboratories, June 14, 2002. ANSI X9.31, PKCS#2 and IEEE-P1363 ISO/IEC 9796-2:2002: Information technology – Security techniques-Digital signature schemes giving message recovery-Part 2: Integer factorization based mechanism

FCS_COP.1 (6) 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 [data signature generation and verification] in accordance with a specified cryptographic algorithm [ECC Signature] and cryptographic key sizes [192, 224, 256, 384, 512 bits] that meet the following: [the below list of ECC standards and [R12]].

[

- Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., June 2015, Oracle
- ANSI X9.62-2005: The Elliptic Curve Digital Signature Algorithm(ECDSA), approved November 16, 2005
- ISO/IEC 15946-2:2002

]

Note: ECC crypto operation supports crypto functions in the Smartcard IC chip cryptographic processor, which is TOE hardware, in accordance with FCS_COP.1/ECDSA -2 of [R18], and is software expanded and implemented in accordance with [R15], and safety is satisfied with the CC EAL6+ assurance requirements of TOE hardware.

Category	TOE hardware	TOE software
Crypto algorithm	ECDSA	ECC Signature
Crypto operation	signature generation and signature verification	data signature generation and verification
Specification	[ANSI X9.62], section 7.3 Singing Process and section 7.4 Verifying Process [ISO/IEC 15946-2:2002], section 6.2, 6.4	Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., June 2015, Oracle ANSI X9.62 -2005: The Elliptic Curve Digital Signature Algorithm(ECDSA), approved November 16, 2005

FCS_COP.1 (7) 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 [secure hashing] in accordance with a specified cryptographic algorithm [SHA -224, SHA-256, SHA-384, SHA-512] and cryptographic key sizes [none] that meet the following: [the below list of SHA standards and [R12]].

[

- Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., June 2015, Oracle

- NIST FIPS180-4: Secure Hash Standard, August, 2015

]

Note: The FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(7)/SHA-1 defines software cryptographic computation functions provided by TOE(S/W). The FCS_COP.1(3),FCS_COP.1(4), FCS_COP.1(5), FCS_COP.1(6) defines hardware cryptographic computation and crypto library functions provided by TOE(IC Chip).

Due to the IC chip certification scpoe, signature generation and verification using SHA-1 in ECDSA are not included in the TOE evaluation scope, so SHA-224, SHA-256, SHA-384, and SHA-512 must be used for ECDSA signature generation and verification.

Note: AES and TDES cryptography algorithms support cryptographic functions in Smart Card IC chip cryptographic processors, which are TOE hardware.

Note: RSA and ECC cryptography algorithms support cryptographic functions in Smart Card IC chip cryptographic processors and crypto library, which are TOE hardware.

Note: Other than cryptographic processors and library usage, cryptographic functions are implemented in software.

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 that meet [*AIS 31 version 1 Functional Classes and Evaluation Methodology for Physical Random Number Generators, 25 September 2001, Class PTG.2 and PTG.3*]

Application Note : You can refer to the [15],[16] for details of this requirement.

6.1.3 User Data Protection

FDP_ACC.2 (1) 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 [CARD CONTENT MANAGEMENT access control SFP] on [list of subjects and objects specified in [Table 20] in relation to CARDMANAGER] and all operations among subjects and objects covered by the SFP.

[

[Table 20] List of subjects and objects

Subject and Object	Description

S.CM	Card Manager, which is the security policy of [R9]
OB.APP	This represents the Javacard Package and is the object of S.CM.

[Table 21] List of Operation

Operation	Description
OP.LOAD	Load Package under the card Lifecycle, Security Level, Privilege, Package AID and Signature [R9]
OP.INSTALL	Install Package under the card Lifecycle, Security Level, Privilege, Package AID and Signature [R9]
OP.DELETE	Delete Package under the card Lifecycle, Security Level, Privilege, Package AID and Signature [R9]

]

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_ACC.2(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 [FIREWALL access control SFP] on [list of subjects and objects specified in [Table 22] in relation to FIREWALL] and all operations among subjects and objects covered by the SFP.

[

[Table 22] List of subjects and objects

Subject and Object	Description
S.APP	Any package, which is the security unit of the firewall policy
S.JCRE	The JCRE. This is the process that manages applet selection and deselection, along with the delivery of APDUs from and to the smart card device. This subject is unique.
OB.JAVAOBJECT	Any Object. Note that KEYS, PIN, arrays and applet instances are specific objects in the Java programming language.

[Table 23] List of Operation

Operation	Description
OP.ARRAY_ACCESS	Read/Write an array component under the Firewall Access Control
OP.INSTANCE_FIELD	Read/Write a field of an instance of a class in the Java programming language under the Firewall Access Control

OP.INVK_VIRTUAL	Invoke a virtual method(either on a class instance or an array object) under the Firewall Access Control
OP.INVK_INTERFACE	Invoke an interface method under the Firewall Access Control
OP.THROW	Throwing of an object under the Firewall Access Control
OP.TYPE_ACCESS	Invoke checkcast or instance of on an object under the Firewall Access Control
OP.JAVA	Any access in the sense of [R16], §6.2.8. In our Information, this is one of the preceding operations under the Firewall Access Control
OP.CREATE (Sharing, LifeTime)	Creation of an object(new or make transient call) under the Firewall Access Control

]

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(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 [CARD CONTENT MANAGEMENT access control SFP based Security attribute of Subject and Object specified in the [Table 24]] to objects based on the [Security attribute of Subject and Object specified in the [Table 25] in relation to CARDMANAGER]:

[

[Table 24] Security attribute of Subject and Object

Subject and Object	Security Attribute
S.CM	Lifecycle, Security Level, Privilege
OB.APP	Signature, Package AID

[Table 25] Values of Security attribute

Name	Description
Lifecycle	Card lifecycle - OP_READY, INITIALIZED, SECURED, CARD_LOCKED, TERMINATED
Security Level	Secure Channel Protocol- SCP02 or SCP03 authentication of [R9] [R11] operates according to the Security Level that is established. The Security level is one of AUTHENTICATED, NO_SECURITY, C_MAC, etc.
Privilege	Privilege - SECURITY_DOMAIN, DAP_VERIFICATION, DELEGATED_MANAGEMENT, CARD_LOCK, CARD_TERMINATE, DEFAULT_SELECTED, CVM_MANAGEMENT, MANDATED_DAP_VERIFICATION

Signature	C_MAC - Signature for each command which includes Package AID, Code and Data by SCP02 or SCP03 authentication of [R9] [R11] [R14]
	DM_TOKEN - Signature on Package AID and Information for DM authentication of [R9] [R11] [R13]
	DAP block - Signature on Package AID, Code and Data for DAP authentication of [R9] [R11] [R13]
Package AID	Unique identifier for the Package - 5~16bytes value

]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [Authorizing access rules specified in the [Table 26] and A.Added rules]

[

A.Added rules

If the Security Level sets C_MAC is successfully verified by the key issued by S.CM, then OP.LOAD, OP.INSTALL and OP.DELETE continues.

If the SECURITY_DOMAIN and DELEGATED_MANAGEMENT Privilege are granted, the DM_TOKEN is presented and it is successfully verified by the key issued by S.CM, then OP.LOAD, OP.INSTALL and OP.DELETE continues.

If the SECURITY_DOMAIN and DAP_VERIFICATION or MANDATED_DAP_VERIFICATION Privilege is granted, the DAP block is presented and it is successfully verified by the key issued by S.CM, then OP.LOAD, OP.INSTALL and OP.DELETE continues.

]

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [Denying access rules specified in the [Table 26]]:

[

[Table 26] Security attribute based access control rules

Security attributes	Governing access rules	Authorizing access rules	Denying access rules
Lifecycle	Verify the card lifecycle is OP_READY, INITIALIZED, SECURED, CARD_LOCKED or TERMINATED	If the card lifecycle is OP_READY, INITIALIZED or SECURED. OP.LOAD, OP.INSTALL and OP.DELETE continues.	If the card lifecycle is CARD_LOCKED or TERMINATED. OP.LOAD, OP.INSTALL and OP.DELETE is aborted.
Security Level	Verify the SCP02 or SCP03 authentication of [R9] [R11] is successful and the Security Level is AUTHENTICATED or NO_SECURITY	If the SCP02 or SCP03 authentication of [R9] [R11] is successful and the Security Level is AUTHENTICATED. OP.LOAD, OP.INSTALL and	If the SCP02 or SCP03 authentication of [R9] [R11] is fail and the Security Level is NO_SECURITY. OP.LOAD, OP.INSTALL and

		OP.DELETE continues.	OP.DELETE is aborted.
Package AID	Verify there is other application currently loaded on this TOE with the same AID	If there is no other application currently loaded on this TOE with the same AID. OP.LOAD and OP.INSTALL continues. OP.DELETE is aborted.	If there is another application currently loaded on this TOE with the same AID. OP.LOAD and OP.INSTALL is aborted. OP.DELETE continues.

FDP_ACF.1(2) 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 [FIREWALL access control SFP based Security attribute of Subject and Object specified in the [Table 28]] to objects based on the [Security attribute of Subject and Object specified in the [Table 27] in relation to FIREWALL]

[

[Table 27] Security attribute of Subject and Object

Subject and Object	Security Attribute
S.APP	Context, Active, Selected
S.JCRE	Context
OB.JAVAOBJECT	Sharing, Context, LifeTime

[Table 28] Values of Security attribute

Name	Description
Context	Package context or JCRE context
Active	Context of any package is currently active context
Selected	Context of any package is currently selected applet context
Sharing	Standard, SIO, Javacard RE entry point, or global array
LifeTime	CLEAR_ON_DESELECT (below, COD) or PERSISTENT

]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [Authorizing access rules specified in the [Table 29]

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

[

A.Added rules

The S.JCRE can freely perform all operations which includes OP.JAVA and OP.CREATE with the exception given in the Denying access rules of the LifeTime (COD) at the below table, provided it is the currently active context.

]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [Denying access rules specified in the[Table 29]]:

[

A.Added rules

S.APP explicitly deny access to OB.JAVAOBJECT with JCRE Context.

[Table 29] Security attribute based access control rules

Security attributes	Governing access rules	Authorizing access rules	Denying access rules
Context with Sharing(Standard) and LifeTime(PERSISTENT)	Verify the Context of OB.JAVAOBJECT to be accessed by S.APP is the same as the Active Context.	If the Context of OB.JAVAOBJECT to be accessed by S.APP is the same as the Active Context. OP.ARRAY_ACCESS, OP.INSTANCE_FIELD, OP.INVK_VIRTUAL, OP.INVK_INTERFACE, OP.THROW or OP.TYPE_ACCESS continues.	If the Context of OB.JAVAOBJECT which is to be accessed by S.APP is not the same as the Active Context. OP.ARRAY_ACCESS, OP.INSTANCE_FIELD, OP.INVK_VIRTUAL, OP.INVK_INTERFACE, OP.THROW or OP.TYPE_ACCESS is aborted.
Sharing(JCRE entry point or global array)	Verify the Sharing attribute of OB.JAVAOBJECT to be accessed by S.APP is JCRE entry point or Global Array	If the Sharing attribute of OB.JAVAOBJECT to be accessed by S.APP is JCRE entry point or Global Array. OP.ARRAY_ACCESS, OP.INSTANCE_FIELD, OP.INVK_VIRTUAL, OP.INVK_INTERFACE, OP.THROW or OP.TYPE_ACCESS continues.	-

Sharing(SIO)	Verify the Sharing attribute of OB.JAVAOBJECT to be accessed by S.APP is SIO	If the Sharing attribute of OB.JAVAOBJECT to be accessed by S.APP is SIO and the OB.JAVAOBJECT's interface is verified as and extends the Shareable interface. OP.TYPE_ACCESS or OP.INVK_INTERFACE continue.	If the Sharing attribute of OB.JAVAOBJECT to be accessed by S.APP is SIO and the OB.JAVAOBJECT's interface is not verified as or does not extend the Shareable interface. OP.TYPE_ACCESS or OP.INVK_INTERFACE is aborted.
LifeTime(COD)	Verify the LifeTime attribute of OB.JAVAOBJECT to be accessed by S.APP is COD	If the LifeTime attribute of OB.JAVAOBJECT to be accessed by S.APP is COD and its Context is the same as the Selected applet Context. OP.ARRAY_ACCESS, OP.INSTANCE_FIELD, OP.INVK_VIRTUAL, OP.INVK_INTERFACE, OP.THROW or OP.TYPE_ACCESS continues.	If the LifeTime attribute of OB.JAVAOBJECT to be accessed by Any subject is COD and its Context is not the same as the Selected applet Context. OP.JAVA, OP.CREATE is aborted.

]

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 *allocation of the resource to, deallocation of the resource from* the [list of objects specified in the [Table 30]]:

[

[Table 30] List of Objects

Objects
Applet instances and package
APDU buffer
Array object
Keys
PIN
Any Javacard transient object

Cryptographic buffer
Any reference to an object instance created during an aborted transaction

]

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 [user data attributes specified in the [Table 31]]:

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [action specified in the [Table 31]].

[

[Table 31] Data integrity monitoring and action

Data	Attribute	Action
Package	CRC32	definitely disables all the services of the card
Privilege	CRC32	definitely disables all the services of the card
Card LifeCycle	CRC32	definitely disables all the services of the card
PIN	CRC32	definitely disables all the services of the card
Key	CRC32	definitely disables all the services of the card

]

Note: The data defined in [Table 31] belongs to objects of OB.JAVAOBJECT. Patch Table is not the objects of OB.JAVAOBJECT and they are described as user data because TSF data used in administrator mode or issuer can be an administrator or user

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 [CARD CONTENT MANAGEMENT access control SFP for the SCP02 and DM authentication] to be able to *transmit and receive* user data in a manner protected from unauthorized disclosure.

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 [CARD CONTENT MANAGEMENT access control SFP for the SCP02 and DM authentication] to be able to *receive* user data in a manner protected from *modification, deletion, insertion, replay* errors.

FDP_UIT.1.1 The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion, replay* has occurred.

6.1.4 Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of Authentication

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within range of values specified in the [Table 32]* unsuccessful authentication attempts occur related to [*list of authentication events specified in the* [Table 32]].

[

[Table 32] List of authentication events

List of authentication events	List of thresholds
Authentication of any user of S.APP	An administrator configurable positive integer within 1 and 127 (default value : 3)
Authentication of S.CM on behalf of card issuer	255
Initial Authentication	5

]

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *surpassed*, the TSF shall [list of actions specified in the [Table 33]].

[

[Table 33] List of TSF actions

List of authentication events	List of actions
Authentication of any user of S.APP	Temporarily lock the cardholder authentication service, until an unlocking action has been successfully undertaken by a privileged user
Authentication of S.CM on behalf of card issuer	definitely disables all the services of the card
Initial Authentication	Relate failure message transfer, Configure_Card command doesn't permitted

]

FIA_ATD.1(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.

[

[Table 34] List of user security attributes

User	Security Attribute
Administrator	User Identifier
	Authentication Data
	Role

]

FIA_ATD.1(2) 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.

[

[Table 35] List of user security attributes

User	Security Attribute
Any user of S.APP	The AID and version number of each package
	The AID of each registered applet
	Whether a registered applet is currently selected for execution
Card issuer of S.CM	The Card Lifecycle for card content management
	The Security Level for card content management
	The Privilege for card content management

]

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 [a defined quality metric specified in the [Table 36]].

[

[Table 36] List of verification of secrets

secret	List of metric
PIN of any user of S.APP	maximum length (<= 8bytes) of PIN
	PIN value and retry counter is encrypted by an applet specific key
KEY of S.CM on behalf of card issuer	A maximum length (112bits) of TDES and maximum length (1024bits) of RSA, maximum length(256bits) of ECC
	KEY value is encrypted by an applet specific key

]

Application Notes: In the case of a password authentication mechanism, the defined allowable criteria can be the minimum length, combination rule, and change cycle.

FIA_UAU.1(1) Timing of Authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 I Timing of Identification

FIA_UAU.1.1 The TSF shall allow [list of TSF mediated actions specified in the [Table 37] in relation to SCP02/SCP03] on behalf of the user to be performed before the user is authenticated.

[

[Table 37] List of TSF mediated action

Command	Action
Get Data	reads data that identifies the card or the Card Issuer
Manage Channel	opens a logical channel with the card
Select Applet	selects an application on the card
Initialize Update	opens a secure communication channel with the card
External Authenticate	opens a secure communication channel with the card

[Table 38] SCP Authentication

Mechanism	Description
SCP02	Secure Channel Protocol 02 according to [R9]
SCP03	Secure Channel Protocol 02 according to [R11]

]

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.

Application Notes: This security functional requirement is authentication performed by S.CM with an aim of compelling CARD CONTENT MANAGEMENT access control SFP.S.CM authenticates external entities through the authentication of this security functional requirement.

FIA_UAU.1(2) Timing of Authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of Identification

FIA_UAU.1.1 The TSF shall allow [list of TSF mediated actions specified in the [Table 39] in relation to DAP] on behalf of the user to be performed before the user is authenticated.

[

[Table 39] List of TSF mediated action

Command	Action
Get Data	reads data that identifies the card or the Card Issuer
Manage Channel	opens a logical channel with the card
Select Applet	selects an application on the card
Initialize Update	opens a secure communication channel with the card
External Authenticate	opens a secure communication channel with the card
Load	Loads DAP Blocks for DAP Verification

[Table 40] DAP Authentication

Mechanism	Description
DAP	Data Authentication Pattern according to [R9][R11][R13]

]

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.

Application Notes: This security functional requirement is authentication performed by S.CM with an aim of compelling CARD CONTENT MANAGEMENT access control SFP. S.CM examines and authenticates the integrity of S.APP.

FIA_UAU.1(3) Timing of Authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of Identification

FIA_UAU.1.1 The TSF shall allow [list of TSF mediated actions specified in the [Table 41] in relation to DM] on behalf of the user to be performed before the user is authenticated.

[

[Table 41] List of TSF mediated action

Command	Action

Get Data	reads data that identifies the card or the Card Issuer
Manage Channel	opens a logical channel with the card
Select Applet	selects an application on the card
Initialize Update	opens a secure communication channel with the card
External Authenticate	opens a secure communication channel with the card
Load	Loads Package
Install	Installs Package & Token Verification

[Table 42] DM Authentication

Mechanism	Description
DM	Delegated management according to [R9][R11][R13]

]

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.

Application Notes: This security functional requirement is authentication performed by S.CM with an aim of compelling CARD CONTENT MANAGEMENT access control SFP. S.CM authenticates special S.APP serving the role of S.CM.

FIA_UAU.1(4) Timing of Authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of Identification

FIA_UAU.1.1. The TSF shall allow [list of TSF mediated actions specified in the [Table 43] in relation to CVM] on behalf of the user to be performed before the user is authenticated.

[

[Table 43] List of TSF mediated action

Command	Action
Get Data	reads data that identifies the card or the Card Issuer
Manage Channel	opens a logical channel with the card
Select Applet	selects an application on the card
Verify	invokes GPAPI_CVM_Verify according to [R9]

]

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

Application Notes: This security feature requirement is authentication performed by S.CM.

FIA_UAU.1(5) Timing of Authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of Identification

FIA_UAU.1.1. The TSF shall allow [establishment of logical communication channel] on behalf of the user to be performed before the user is authenticated.

[]

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

Application Notes: This security functional requirement is initial authentication performed by S.CM.

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [authentication mechanisms specified in the [Table 44]].

[

[Table 44] List of authentication mechanism

List of authentication mechanism	Action
SCP02 authentication mechanism	uses random number and clear crypto buffer
SCP03 authentication mechanism	uses random number and clear crypto buffer
DAP authentication mechanism	uses applet AID and clear crypto buffer
DM authentication mechanism	uses applet AID and clear crypto buffer
CVM authentication mechanism	verifies the PIN encrypted by the key specific to an applet and clear crypto buffer
Initial authentication mechanism	clear crypto buffer

]

Application Notes: Single-use authentication mechanisms can be applied to all users including authorized administrator and may not be used in services available within the range that does not violate the security policy.

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 [under which re-authentication is required specified in the [Table 45]].

[

[Table 45] Condition of Re-authenticating

List	Condition
SCP02	after Card Manager is deselected after card session is closed(after card reset) SCP02 authentication mechanism is failed
SCP03	after Card Manager is deselected after card session is closed(after card reset) SCP03 authentication mechanism is failed
DAP	when any Package is loaded DAP authentication mechanism is failed
DM	when any Package is installed DM authentication mechanism is failed
CVM	after applet is deselected after card session is closed(after card reset) CVM authentication mechanism is failed
Initial authentication	When Initial authentication mechanism is failed

]

Application Notes: Initialization authentication occurs when TOE is first driven. At the time of successful authentication, the administrator mode is changed to the user mode, and initialization authentication cannot be performed any more.

FIA_UID.1 Timing of Identification

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow [list of TSF-mediated actions specified in the [Table 46]] on behalf of the user to be performed before the user is identified.

[

[Table 46] List of TSF mediated action

Command	Action
CheckChipData_Command	checks card integrity and gets Chip and OS data
Initialize_Card_Command	Injects Implementer data and installs FLASH package
Configure_Card_Command	Injects card issuer key and initializes Card Manger

Get Data	reads data that identifies the card or the Card Issuer
Manage Channel	opens a logical channel with the card
Select Applet	selects an application on the card

]

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.

Application Notes: Within the range of TOE, the user is confined to the issuer, who should undergo identification and authentication before accessing TOE and using its functions in a way befitting his/her role.

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: [list of user security attributes specified in the [Table 47]].

[

[Table 47] Security attributes of User-subject

User - Security Attribute	Subject - Security Attribute
Any user of S.APP - The AID and version number of each package - The AID of each registered applet - Whether a registered applet is currently selected for execution	S.APP - The Context security attribute
Card issuer of S.CM - The Card Lifecycle for card content management - The Security Level for card content management - The Privilege for card content management	S.CM - The Lifecycle and Security Level and Privilege security attribute

]

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).1, FDP_ACF.1(2).1/ and FMT_MSA.3.1].
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.1.1].

Application Notes: The user-subject binding is limited to descriptions on FIA_ATD.1(1) concerning the active entity within the TOE during TOE operation.

6.1.5 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, [management] the behavior of* the functions [list of functions of S.CM' operation specified in the [Table 48]] to [S.CM].

[

[Table 48] List of Security Functions

Role	Behavior	Functions
S.CM	Load/Install/Delete	Package Load/Install/Delete
S.CM	Enable/Disable	Card Lock
S.CM	Enable	Card Terminate

]

Application Notes: This security functional requirement should be implemented to activate the functions of a smart card always via the issuer when the use of the smart card begins. At the same time, it should make sure that the issuer suspends the functions of the smart card when discontinuing the use of its functions.

While using the smart card, the issuer may add, delete or modify applications. In this document, the term "package" includes application (or applet), and the modification of applications is confined to certain cases. In other words, it refers to the operation of installing, issuing and recording information on applications, which does not constitute the role of S.CM as it is performed by the issuer and is done using the functions of the given applications.

FMT_MSA.1 (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 [*CARD CONTENT MANAGEMENT access control SFP*] to restrict the ability to *modify, [creation]* the security attributes [list of security attributes of subjects defined in FDP_ACF.1(1)] to [S.CM roles defined in FMT_SMR.1.1].

FMT_MSA.1 (2) 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 [*FIREWALL access control SFP*] to restrict the ability to *modify* the security attributes [list of security attributes of subjects defined in FDP_ACF.1(2)] to [S.JCRE roles defined in FMT_SMR.1.1].

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 [*CARD CONTENT MANAGEMENT access control SFP and FIREWALL access control SFP*] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [S.CM role and S.JCRE role defined in FMT_SMR.1.1] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 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 *query, modify* the [list of TSF data specified in the [Table 49]] to [list of the authorized roles specified in the [Table 50]].

[

[Table 49] List of TSF data

TSF data	role
Card Life Cycle	S.CM
Privilege	S.CM
KEY (DES-SCP02, AES-SCP03, DAP)	S.CM
KEY (RSA-DAP, ECC-DAP, DM)	S.CM
GLOBAL_PIN	S.CM
AID	S.CM

]

FMT_MTD.2 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 [list of TSF data specified in the [Table 50]] to [list of the authorized roles specified in the [Table 50]].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [action specified in the [Table 50]].

[Table 50] List of limits for TSF data

TSF data	Limit	role	Action
Card Life Cycle	One of the following OP_READY, INITIALIZED, SECURED, CARD_LOCKED, TERMINATED	S.CM	Throw an error status word and terminate card
Privilege	One of the following SECURITY_DOMAIN, DAP_VERIFICATION, DELEGATED_MANAGEMENT, CARD_LOCK, CARD_TERMINATE, DEFAULT_SELECTED, CVM_MANAGEMENT, MANDATED_DAP_VERIFICATION	S.CM	Throw an error status word
KEY(TDES-SCP02, AES-SCP03, DAP)	Authentication Retry Counter	S.CM	Throw an error status word and close seucre communication channel
	Key Size		
KEY(RSA-DAP, ECC-DAP, DM)	Authentication Retry Counter	S.CM	Throw an error status word and close seucre communication channel
	Key Size		
GLOBAL_PIN	PIN retry counter	S.CM	Throw an error status word and block PIN
	PIN Size		

]

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 management functions: [list of security management functions to be provided by the TSF specified in the [Table 51]].

[

[Table 51] List of security management function of TSF

List of Security Management Functions
Package Load/Install/Delete
Card Life Cycle Management
Package AID Registration

Card Security Level Management
Privilege Management
Signature Generation Management
Key Management
PIN Management
Applet Life Cycle Management
Applet PIN Management
Context Management
Object Sharing Management
Object LifeTime Management
Other Security Management : IC Chip Register Management

]

FMT_SMR.1 Security roles

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of Identification

FMT_SMR.1.1 The TSF shall maintain the roles [**S.CM, S.APP, S.JCRE specified in the [Table 52**]].

[

[Table 52] List of Security roles

Role	Description
S.CM(Card Manager) represents the card issuer	Package Load/Install/Delete Card Life Cycle Management Package AID Registration Card Security Level Management Privilege Management Signature Generation Management Key Management PIN Management
S.APP represents the card user	Applet Life Cycle Management Applet PIN Management
S.JCRE	Context Management Object Sharing Management Object LifeTime Management

]

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

Application Notes: Described here are the security roles of TOE during operation; TOE's security role as administrator is the issuer, but such is not described in this security role. The smart card issuer plays the overall roles of an administrator for his/her smart card—by installing applications before using the smart card, receiving reports on failures during use and fixing the failures, and discarding the smart card upon the discontinuation of use. In this security target, the roles of the issuer may be transferred to another issuer through privilege management.

6.1.6 Privacy

FPR_UNO.1 Unobservability

Hierarchical to: No other components

Dependencies: No dependencies

FPR_UNO.1.1 The TSF shall ensure that [external entities] are unable to observe the operation [FCS_COP.1 Cryptographic operation, comparison of Keys and PIN] on [Keys and PIN] by [TSF].

Application Notes: 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). TOE encrypts keys and PINs and uses CRC32 and MAC to verify integrity and provide means to counter attacks like DFA. The TSF provides the means to handle attacks such as DPA and SPA.

6.1.7 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. The list of potential security violations in FAU_SAA.1
b. Failure detected during self-testing by FPT_TST.1
c. Conditions outside the normal operating conditions of the TSF detected by the IC Chip
d. Load/Install/Delete failure of Packages and applets

]

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 specified in the 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 specified in the 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 [Reading from and writing to static and objects' fields interrupted by Card tearing (unexpected removal of the Card out of the CAD) and power failure] 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 testing

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[before executing the TSF]* 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 *[TSF data(cryptographic key, etc.)]* .

FPT_TST.1.3 The TSF shall provide authorized **issuer** with the capability to verify the integrity of [*stored TSF executable code*].

Application Notes: The self-test of FPT_TST.1.1 consists of the following tests:

[

[Table 53] List of self-tests

List of Self Tests
Randomness test
Integrity Test

]

6.1.8 Trusted path/channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components

Dependencies: No dependencies

FTP_ITC.1.1 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.

FTP_ITC.1.2 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

[Package Load /Install/Delete, transmit of TSF data].

6.2 Assurance Requirements

The assurance requirements of this Security Target are composed of assurance component in the Common Criteria Part3 and added the following assurance components. [Table 54] shows the assurance components.

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

[Table 54] Assurance Requirements

Assurance Class	Assurance Components	
ASE: Security Target	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_ECD.1	Extended components definition
	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE summary specification
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.5	Complete semi-formal functional specification with additional error information
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-structured internals
	ADV_TDS.4	Semiformal modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.5	Development tools CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.2	Compliance with implementation standards
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Testing: modules design
	ATE_FUN.1	Functional testing

	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

6.2.1 Security Target

ASE_INT.1 ST introduction

Dependencies :

No dependencies

Developer action elements :

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements :

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements :

ASE_INT.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator *shall confirm* that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies :

ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Developer action elements :

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements :

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements :

ASE_CCL.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 Security problem definition

Dependencies :

No Dependencies

Developer action elements :

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements :

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements :

ASE_SPD.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.2 Security objectives

Dependencies :

ASE_SPD.1 Security problem definition

Developer action elements :

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements :

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements :

ASE_OBJ.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies :

No Dependencies

Developer action elements :

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements :

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements :

ASE_ECD.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator *shall confirm* that no extended component can be clearly expressed using existing components.

ASE_REQ.2 Derived security requirements

Dependencies :

ASE_OBJ.2 Security objectives

ASE_ECD.1 Extended components definition

Developer action elements :

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a rational for security requirements.

Content and presentation elements :

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements :

ASE_REQ.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE summary specification

Dependencies :

ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements :

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements :

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements :

ASE_TSS.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator *shall confirm* that the TOE summary specification is consistent with the TOE overview and the TOE description.

6.2.2 Development

ADV_ARC.1 Security architecture description

Dependencies :

ADV_FSP.1 Basic functional specification

ADV_TDS.1 Basic design

Developer action elements :

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements :

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements :

ADV_ARC.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.5 Complete semi-formal functional specification with additional error information

Dependencies :

ADV_TDS.1 Basic design

ADV_IMP.1 Implementation representation of the TSF

Developer action elements :

ADV_FSP.5.1D The developer shall provide a functional specification.

ADV_FSP.5.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements :

ADV_FSP.5.1C The functional specification shall completely represent the TSF.

ADV_FSP.5.2C The functional specification shall describe the TSFI using a semi-formal style.

ADV_FSP.5.3C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.5.4C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.5.5C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.5.6C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.5.7C The functional specification shall describe all error messages that do not result from an invocation of a TSFI.

ADV_FSP.5.8C The functional specification shall provide a rationale for each error message contained in the TSF implementation yet does not result from an invocation of a TSFI.

ADV_FSP.5.9C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements :

ADV_FSP.5.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.5.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_IMP.1 Implementation representation of the TSF

Dependencies :

ADV_TDS.3 Basic modular design

ALC_TAT.1 Well-defined development tools

Developer action elements :

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

Content and presentation elements :

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

Evaluator action elements :

ADV_IMP.1.1E The evaluator *shall confirm* that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

ADV_INT.2 Well-structured internals

Dependencies :

ADV_IMP.1 Implementation representation of the TSF

ADV_TDS.3 Basic modular design

ALC_TAT.1 Well-defined development tools

Developer action elements :

ADV_INT.2.1D The developer shall design and implement the entire TSF such that it has well-structured internals.

ADV_INT.2.2D The developer shall provide an internal description and justification.

Content and presentation elements :

ADV_INT.2.1C The justification shall describe the characteristics used to judge the meaning of “well-structured”.

ADV_INT.2.2C The TSF internals description shall demonstrate that the entire TSF is well-structured.

Evaluator action elements :

ADV_INT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_INT.2.2E The evaluator shall perform an internal analysis on the TSF.

ADV_TDS.4 Semiformal modular design

Dependencies :

ADV_FSP.5 Complete semi-formal functional specification with additional error information

Developer action elements :

ADV_TDS.4.1D The developer shall provide the design of the TOE.

ADV_TDS.4.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements :

ADV_TDS.4.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.4.2C The design shall describe the TSF in terms of modules, designating each module as SFR-enforcing, SFR-supporting, or SFR-non-interfering.

ADV_TDS.4.3C The design shall identify all subsystems of the TSF.

ADV_TDS.4.4C The design shall provide a semiformal description of each subsystem of the TSF, supported by informal, explanatory text where appropriate.

ADV_TDS.4.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.4.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.4.7C The design shall describe each SFR-enforcing and SFR-supporting module in terms of its purpose and relationship with other modules.

ADV_TDS.4.8C The design shall describe each SFR-enforcing and SFR-supporting module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing or SFR-supporting modules.

ADV_TDS.4.9C The design shall describe each SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.4.10C The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.

Evaluator action elements :

ADV_TDS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.4.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

6.2.3 Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies :

ADV_FSP.1 Basic functional specification

Developer action elements :

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements :

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements :

AGD_OPE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies :

No Dependencies

Developer action elements :

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements :

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements :

AGD_PRE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.2.4 Life-cycle support

ALC_CMC.4 Production support, acceptance procedures and automation

Dependencies :

ALC_CMS.1 TOE CM coverage

ALC_DVS.1 Identification of security measures

ALC_LCD.1 Developer defined life-cycle model

Developer action elements :

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

Content and presentation elements :

ALC_CMC.4.1C The TOE shall be labeled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements :

ALC_CMC.4.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.5 Development tools CM coverage

Dependencies :

No Dependencies

Developer action elements :

ALC_CMS.5.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements :

ALC_CMS.5.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation

representation; security flaw reports and resolution status; and development tools and related information.

ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.5.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements :

ALC_CMS.5.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 Delivery procedures

Dependencies :

No Dependencies

Developer action elements :

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements :

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements :

ALC_DEL.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.2 Sufficiency of security measures

Dependencies :

No Dependencies

Developer action elements :

ALC_DVS.2.1D The developer shall produce and provide development security documentation.

Content and presentation elements :

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

Evaluator action elements :

ALC_DVS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.2.2E The evaluator shall confirm that the security measures are being applied.

ALC_LCD.1 Developer defined life-cycle model

Dependencies :

No Dependencies

Developer action elements :

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation elements :

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements :

ALC_LCD.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.2 Compliance with implementation standards

Dependencies :

ADV_IMP.1 Implementation representation of the TSF

Developer action elements :

ALC_TAT.2.1D The developer shall provide the documentation identifying each development tool being used for the TOE.

ALC_TAT.2.2D The developer shall document and provide the selected implementation-dependent options of each development tool.

ALC_TAT.2.3D The developer shall describe and provide the implementation standards that are being applied by the developer.

Content and presentation elements :

ALC_TAT.2.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.2.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.2.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options..

Evaluator action elements :

ALC_TAT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.2.2E The evaluator shall confirm that the implementation standards have been applied.

6.2.5 Tests

ATE_COV.2 Analysis of coverage

Dependencies:

ADV_FSP.2 Security-enforcing functional specification

ATE_FUN.1 Functional testing

Developer action elements :

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation elements :

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements :

ATE_COV.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.3 Testing: modular design

Dependencies :

ADV_ARC.1 Security architecture description

ADV_TDS.4 Semiformal modular design

ATE_FUN.1 Functional testing

Developer action elements :

ATE_DPT.3.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements :

ATE_DPT.3.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and modules in the TOE design.

ATE_DPT.3.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.3.3C The analysis of the depth of testing shall demonstrate that all TSF modules in the TOE design have been tested.

Evaluator action elements :

ATE_DPT.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional tests

Dependencies

ATE_COV.1 Evidence of coverage

Developer action elements :

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements :

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements :

ATE_FUN.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing - sample

Dependencies:

ADV_FSP.2 Security-enforcing functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_COV.1 Evidence of coverage

ATE_FUN.1 Functional testing

Developer action elements :

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements :

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements :

ATE_IND.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator *shall execute* a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator *shall test* a subset of the TSF to confirm that the TSF operates as specified.

6.2.6 Vulnerability assessment

AVA_VAN.5 Advanced methodical vulnerability analysis

Dependencies :

ADV_ARC.1 Security architecture description

ADV_FSP.4 Complete functional specification

ADV_TDS.3 Basic modular design

ADV_IMP.1 Implementation representation of the TSF

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_DPT.1 Testing: basic design

Developer action elements :

AVA_VAN.5.1D The developer shall provide the TOE for testing.

Content and presentation elements :

AVA_VAN.5.1C The TOE shall be suitable for testing.

Evaluator action elements :

AVA_VAN.5.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.5.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.5.3E The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.5.4E The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing High attack potential.

6.3 Security Requirements Rationale

This section proves that security requirements are suited to fulfill the security objectives described in section 4 and adequate to handle the security problem.

6.3.1 Security Functional Requirements Rationale

The security requirements rationale proves the followings:

- Each TOE security objective has at least one TOE security functional requirement tracing to it.
- Each TOE security functional requirement traces back to at least one TOE security objectives.

[Table 55] Mapping of security functional requirements and security objectives

Security Objectives / Security Functional requirements	O.Data_Protection	O.Issuance and management	O.Identification	O.Authorized_Failure Repair	O.Authentication	O.Automated_Recovery	O.Residual_Information_Deletion	O.Information_Disclosure_Handling	O.Open_Platform	O.IC Chip
FAU_ARP.1				X	X					
FAU_SAA.1				X	X					
FCS_CKM.1(1)					X					X
FCS_CKM.1(2)					X					X
FCS_CKM.1(3)					X					X
FCS_CKM.1(4)					X					X
FCS_CKM.2					X				X	X
FCS_CKM.4					X		X			
FCS_COP.1(1)	X				X					
FCS_COP.1(2)	X				X					
FCS_COP.1(3)	X				X					X
FCS_COP.1(4)	X				X					X
FCS_COP.1(5)	X				X					X
FCS_COP.1(6)	X				X					X
FCS_COP.1(7)	X				X					X

FCS_RNG.1	X				X					X
FDP_ACC.2(1)	X	X							X	
FDP_ACC.2(2)	X								X	
FDP_ACF.1(1)	X	X							X	
FDP_ACF.1(2)	X		X						X	
FDP_RIP.1							X		X	
FDP_SDI.2	X				X			X		
FDP_UCT.1	X							X	X	X
FDP_UIT.1	X							X	X	X
FIA_AFL.1		X		X	X					
FIA_ATD.1(1)		X	X	X	X					
FIA_ATD.1(2)		X	X	X	X					
FIA_SOS.1					X					
FIA_UAU.1(1)	X	X		X	X					X
FIA_UAU.1(2)	X	X		X	X					X
FIA_UAU.1(3)	X	X		X	X					X
FIA_UAU.1(4)			X		X					
FIA_UAU.1(5)			X		X					
FIA_UAU.4		X		X	X					
FIA_UAU.6		X		X	X					
FIA_UID.1	X	X	X	X						
FIA_USB.1	X		X		X					
FMT_MOF.1	X	X							X	
FMT_MSA.1(1)	X	X							X	
FMT_MSA.1(2)	X		X						X	
FMT_MSA.3	X								X	
FMT_MTD.1		X								
FMT_MTD.2		X								
FMT_SMF.1		X								
FMT_SMR.1		X	X	X	X					
FPR_UNO.1								X		X
FPT_FLS.1						X				X
FPT_RCV.3						X				
FPT_RCV.4						X				
FPT_TST.1	X					X				X
FTP_ITC.1	X				X					

6.3.2 Assurance Requirements Rationale

The evaluation assurance level of this security target is EAL5+. Below are the assurance components added:

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

EAL5 assurance package requires semi-formal design and test. EAL5 allows a developer to gain maximum assurance from security engineering based on rigorous commercial development practices supported by moderate application of specialist security engineering techniques. The TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialized techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

To understand security behaviors, EAL5 assure the TOE through complete analysis of SFR in ST using functions, complete interface specification, design description of TOE, expressions on the implementation. EAL5 requires the TSF module design.

TOE is developed for multi- purpose such as public ID, finance, electronic signature etc. Specially, the public ID such as national ID requires a high level of independently assured security to protect the sensitive information such as personal bio-information. The evaluation assurance level of this security target is EAL5+ for this requirement.

The TOE is developed by using publicly available standard implementation specifications. Therefore, it is easy to obtain information related to design and operation of the TOE. Also, TOE is easily accessed as it is used in open environment and it is difficult to trace an attack. However, it is difficult to understand the hardware architecture of EAL6+ certified IC Chip with a high level security and the software including mechanism of the security countermeasures. It requires a high level of knowledge and advanced specialized equipment and a high level of independently assured security for the TOE.

Therefore, considering the resources, motivation and expertise, the TOE must counter attackers possessing high attack potential. In the EAL5 evaluation level, AVA_VAN.4 is augmented to SCOP-PP considering execution of systematic vulnerability analysis and resistant to attackers possessing moderate attack potential. So AVA_VAN.5 is added to perform the resistance analysis on attackers possessing high attack potential, the advanced methodical vulnerability analysis of the module design and the implementation expression of TOE.

The TOE is used as a primary security product in the high level secure infra-structure. Therefore, ALC_DVS.2 is augmented to assure high level development security in terms of physical, procedural, personal, and other security measures in the phase of development.

6.4 Dependencies Rationale

6.4.1 Dependencies of the Security Functional Requirements

[Table 56] Dependencies of the functional components

Num.	Functional Component	Dependencies	Num. of Ref.
1	FAU_ARP.1	FAU_SAA.1	2
2	FAU_SAA.1	FAU_GEN.1	None
3	FCS_CKM.1(1)~(4)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	[4 or 6] 5
4	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	[- or – or 3], 5

5	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1],	[- or - or 3]
6	FCS_COP.1(1)~(7)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	[- or - or 3], 5
7	FCS_RNG.1	-	-
8	FDP_ACC.2(1),(2)	FDP_ACF.1	9
9	FDP_ACF.1(1),(2)	FDP_ACC.1, FMT_MSA3	8, 24
10	FDP_RIP.1	-	-
11	FDP_SDI.2	-	
12	FDP_UCT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	[8 or -] [34 or -]
13	FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	[8 or -] [34 or -]
14	FIA_AFL.1	FIA_UAU.1	17
15	FIA_ATD.1(1),(2)	-	-
16	FIA_SOS1	-	-
17	FIA_UAU.1(1)~(5)	FIA_UID.1	20
18	FIA_UAU.4	-	-
19	FIA_UAU.6	-	-
20	FIA_UID.1	-	-
21	FIA_USB.1	FIA_ATD.1	15
22	FMT_MOF.1	FMT_SMF.1, FMT_SMR1	27, 28
23	FMT_MSA1(1),(2)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1, FMT_SMR1	[8 or -] 27, 28
24	FMT_MSA3	FMT_MSA1, FMT_SMR1	23, 28
25	FMT_MTD.1	FMT_SMF.1, FMT_SMR1	27, 28
26	FMT_MTD.2	FMT_MTD.1, FMT_SMR1	25, 28
27	FMT_SMF.1	-	-
28	FMT_SMR1	FIA_UID.1	20
29	FPR_UNO.1	-	-
30	FPT_FLS.1	-	-
31	FPT_RCV.3	AGD_OPE.1	EAL5
32	FPT_RCV.4	-	-
33	FPT_TST.1	-	-
34	FTP_ITC.1	-	-

Dependent upon FAU_SAA.1, FAU_GEN.1 is not satisfied. A smart card does not have enough space for recording security events. Excessive security auditing may put the safety of the card at risk, so security events are not recorded. Therefore, this ST does not define the requirements of FAU_GEN.1.

FDP_ACF.1, FMT_MSA.1 is dependent upon FDP_ACC.1, which is satisfied by FDP_ACC.2 in a hierarchical relationship with FDP_ACC.1.

FDP_UCT.1, FDP_UIT.1 is dependent upon FDP_ACC.1 or FDP_IFC.1, which is satisfied by FDP_ACC.2 in a hierarchical relationship with FDP_ACC.1.

6.4.2 Dependencies of the Assurance Requirements

All the dependencies of the EAL5 assurance package offered in the Common Criteria for the Information Protection System, so the theoretical rationale for this package is not specified here. The dependencies of added assurance requirements are outlined in [Table 57], and this security target meets the dependencies of all the assurance requirements.

[Table 57] Dependencies of the added assurance requirements

Num.	Assurance Component	Dependency	Reference Number
1	ALC_DVS.2	-	-
2	AVA_VAN.5	ADV_ARC.1 ADV_FSP.4 ADV_TDS.3 ADV_IMP.1 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1	EAL5 EAL4 EAL4 EAL5 EAL5 EAL5 EAL4

7. TOE Summary Specification

This section provides a description of the security functionality of the TOE that met the TOE security requirements.

7.1 TOE Security Functionality

This section describes the security functionality of TOE that meets the security requirements. The security functionality of TOE can be broadly divided into: [Security Audit, Cryptographic Support, User Data Protection, Identification and Authentication, Security Management, Privacy and TSF Protection]. This section describes how the TOE meets its security functionality.

The followings are the security functionality of TOE:

7.1.1 Security Audit

The TOE detects potential security violations such as the check sum values of internal data, errors in resource allocation and authentication failure events, resetting TOE operations or suspending TOE functions either temporarily or permanently.

7.1.2 Cryptographic Support

The TOE provides cryptographic computation such as cryptographic key generation/destruction, encryption, decryption, and electronic signature generation and verification through Cryptographic Function Subsystem and JCAPIs. It also supports hash value generation and random number generation.

7.1.3 User Data Protection

The TOE provides the user data protection through CM, JCRE and Secure Management. The CM provides card content manager and access control policies based on security attributes and management of security attribute. It met for requirement for the user data protection. The TOE provides firewall access control policies for all computations among the Javacard system, applets and data based on the security attribute “Context” with the user data protection.

7.1.4 Identification and Authentication

The TOE provides the identification and authentication through CM. The TOE performs card administrator authentication through Secure Channel Protocol (SCP 02, SCP 03). It also performs authentication of application providers and issuers through data authentication pattern (DAP) authentication and delegated management (DM) authentication. The TOE provides means to authenticate users with PIN and controls Card Manager’s operations related to global PIN/PIN management.

7.1.5 Security Management

The TOE provides the security management through CM and JCRE. The CM provides Card Content Management and Access Control based on security attributes and manages the security attributes. The TOE provides firewall access control policies for all computations among the Javacard system, applets and data based on the security attribute “Context” and manages the security attributes.

7.1.6 Privacy

The TOE provides secure management for resource. The TOE provides the mechanism of the integrity verification and encryption for the cryptographic keys and PIN. It ensure the un-observability against external attacks during operation

7.1.7 Protection of the TSF

The TOE provides TSF protection functions through secure management. It provides the self-test to verify the integrity of TSF data and execution code during power on, and check the integrity of internal sensitive data. Whenever applet is selected, it verifies the integrity of applet. When this verification of integrity is failed, the TOE is stopped through self-test and keeps the safe state from external attack and failure.

8. Annex

8.1 References

[R1] Korea IT Security Evaluation and Certification Scheme, Ministry of Science, ICT and Future Planning Notice NO.2017-7, 2017. 8. 24

[R2] Common Criteria for Information Technology Security Evaluation, Part 1, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[R3] Common Criteria for Information Technology Security Evaluation, Part 2, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[R4] Common Criteria for Information Technology Security Evaluation, Part 3, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

[R5] Smart Card Open Platform Protection Profile V2.2, 2010. 12. 20

[R6] Javacard™ System Protection Profile Collection Version 1.0b, Sun Microsystems, August 2003

[R7] Protection Profile Smart Card IC with Multi-Application Secure Platform Version 2.0, European Smart Card Industry Association, November 2000

[R8] Smart Card Protection Profile Version 3.0(SCSUG-SCPP), Smart Card Security User Group, September 2001

[R9] GlobalPlatform Card Specification 2.3.1, GPC_SPE_034, March 2018

[R10] GlobalPlatform Card Mapping Guidelines of Existing GP v2.1.1 Implementation on v2.2.1, Janunary 2011

[R11] GlobalPlatform Card Technology Secure Channel Protocol ‘03’ Card Specification v2.2, Amendment D, July 2014

[R12] GlobalPlatform ID configuration, December 2011

[R13] GlobalPlatform Card Technolog Security Upgrade for Card Content Management Card Specification v2.2, Amendment E, July 2014

[R14] GlobalPlatform Card Common Implementation Configuration v1.0, February 2014.

[R15] Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., September 2011, Oracle

[R16] Java Card 3 Platform, Runtime Environment Specification, Classic Edition, Version 3.0.5., September 2011, Oracle

[R17] Java Card 3 Platform, Virtual Machine Specification, Classic Edition, Version 3.0.5., September 2011, Oracle

[R18] Public Common Criteria Information Technology Security Evaluation S3D384C/S3D352C/ S3D300C/S3D264C/S3D232C/S3K384C Version 7.0 28th June 2023 ANSSI-CC-2023/40

[R19] FIPS PUB 180-1: FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SECURE HASH STANDARD, 1995 April 17

[R20] FIPS PUB 180-3: FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SECURE HASH STANDARD, October 2008

[R21] FIPS PUB 197: Federal Information Processing Standards Publication 197, Announcing the ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001

[R22] FIPS PUB 46-3: FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

[R23] PKCS #1: RSA Encryption Standard, An RSA Laboratories Technical Note, Version 2.1, June 14, 2002

[R24] ISO/IEC 9796-2:2002: Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms

[R25] ISO/IEC 9797-1:1999: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher

[R26] Bundesanzeiger Nr. 59, Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Regulierungsbehörde für Telekommunikation und Post, 2005-03-30

[R27] Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, ETSI TS 102 176-1 V1.2.1 (2005-07)

[R28] American National Standard X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm(ECDSA), November 16, 2005.

[R29] American National Standard X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, November 20, 2001.

[R30] ISO/IEC 9796-1: Information technology – Security techniques – Digital signature schemes giving message recovery – Part 1: Mechanisms using redundancy

[R31] Composite product evaluation for Smart Cards and similar devices, Version 1.5.1 May 2018

8.2 Abbreviated terms

AES	Advanced Encryption Standard
AID	Applet Identifier
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
API	Application Programming Interface
ARIA	Cryptographic Algorithm “Academy, Research Institute, Agency”
CBC	Cipher Block Chaining
CC	Common Criteria
CF	Cryptographic Function
CM	Card Manager
COS	Card Operating System
CPU	Central Processing Unit
DAP	Data Authentication Pattern
DES	Data Encryption Standard
DH	Diffie-Hellman
DM	Delegated Management
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
GP	Global Platform
IC	Integrated Circuit
IFD	Interface Device
IK	Implementor Key
ISO	International Organization for Standardization
JCAPI	Javacard Application Programming Interface
JCRE	Javacard Runtime Environment
JCVM	Javacard Virtual Machine
MAC	Message Authentication Code
OSP	Organizational Security Policy
PCD	Proximity Coupling Device
PICC	Proximity Card
PP	Protection Profile
RF	Radio Frequency
RAM	Random Access Memory
RNG	Random Number Generation
RSA	Cryptographic Algorithm “Rivest, Shamir, Adleman”

SCOP	Smart Card Open Platform
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TDES	Triple-DES
TK	Transport Key
TOE	Target of Evaluation
TSF	TOE Security Functionality