DATASONIC

DCOS SECURITY TARGET

DOCUMENT VERSION	1.0
DOCUMENT DATE	09 APRIL 2019

Document management

Document identification

Document ID	DCOS_EAL4+_ST
Document title	DCOS Security Target
Document Version	Version 1.0
Document Date	09 April 2019

Document history

Version	Date	Description
0.1	10-JAN-17	Released for internal review.
0.2	18 Feb 2017	Document updates based on new updates from Developer.
0.3	29 March 2017	Document updates after internal review.
0.4	14 April 2017	Document updates section 1.4
0.5	12 Dec 2017	Document updates.
0.6	12 Mar 2018	Document updates.
0.7	11 Nov 2018	Content updates based on Developer new info.
0.8	20 Mar 2019	Content updates based on Developer new info.
1.0	09 Apr 2019	Final Released

Table of Contents

1 Security Target Introduction

1.1 ST Reference

Table 1: Security Target Reference

ST Title	DCOS Security Target
ST Identifier	DCOS_EAL4+_ST
ST Version	Version 1.0
ST Date	09 April 2019

1.2 TOE Reference

Table 2: Target of Evaluation (TOE) Reference

TOE Title	Datasonic Chip Operating System (DCOS)
TOE Version	Version 1.0

1.3 Document Organization

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).
- Section 2 provides the conformance claims for the evaluation (ASE_CCL.1).
- Section 3 provides the definition of the security problem that the TOE has been designed to address (ASE_SPD.1).
- Section 4 defines the security objectives for the TOE and the environment (ASE_OBJ.2).
- Section 5 contains the security functional and assurance requirements derived from the Common Criteria Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.2).
- Section 6 contains the security assurance requirements derived from the Common Criteria, Part 3 (ASE_REQ.2).
- Section 7 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 TOE Overview

1.4.1 TOE Usage and Major Security Functions

The Target of Evaluation (TOE) is Datasonic Chip Operating System (DCOS). The TOE is a smart card operating system purpose-designed for national identity card applications which also serves as a platform for national e-passport, precisely meeting individual needs of countries adopting the latest ID and e-passport standards.

The TOE simultaneously supports multiple applications with custom instruction sets and custom data structures define by the authorized agencies within a single smart card, limited only by the IC specifications. Consider a national ID card with the capabilities of hosting of other applet functions like a driver's license, e-purse, and bank card credentials, in which simplifies its cardholder's in dealing with various public and private agencies.

The main features are:

- Provide secured data accessibility and storage for identity card purpose;
- Provide cryptographic processing (e.g. encryption, decryption, key signing and relevant functions).;
- Store identity information of the cardholder;
- Support financial trading authentication and record; and
- Complies to BAC and EAC of ICAO 9303 standard for e-passport.

The following major security functions are implemented by the TOE:

Table 3: Major Security Functions of the TOE

Security functions	Descriptions
File Management	The TOE can protect confidential data and sensitive operations between generic applications.
Application and Platform Management	The TOE provides dynamic application loading, post-issuance application and application deletion.
Cryptographic Management	The TOE provides utilisation of cryptographic mechanisms with the capabilities of enforcing the TOE security functions (TSF).
Self-Protection and Testing	The TOE provides resistance through detection capabilities towards relevant smart card attacks, such as physical attacks on the IC Chip and Side Channel Analysis Attacks.

1.4.2 TOE Type

The TOE is Multi-Application Smart Card IC Operating Systems that provides a portable interfaces for smart card applications known as generic applications. Datasonic Chip Operating System (also will be known as DCOS, in this document) provides several libraries as a portable interfaces for generic application. Additionally, DCOS provides several libraries that initiate hardware level IC functions, such as cryptographic processing to those defined authorized generic applications.

The TOE can be categorised as **ICs, Smart Cards and Smart Card-Related Devices and Systems** in accordance with the categories identified on the Common Criteria Portal (www.commoncriteriaportal.org) that lists all the certified products.

1.4.3 TOE Scope (Non-TOE Requirements of Firmware/Hardware/Software)

In this section, shall describes the list of components of the TOE that covers under the scope of the TOE and define those non-dependencies TOE components that is define as not part of the TOE in its operational environment.

The Scope of this TOE only covers the Operating System of the Smart Card Chip and generic applications. The following table list the compatible evaluated IC hardware platforms applicable to the TOE. Note that, the list of IC hardware platforms are not part of the scope of the TOE, and shall not be re-evaluate in this scope of the TOE.

Table 4: List of IC Model Supported by the TOE

Manufacturer	Model	Certification
Infineon	SLE78CFX2000P SLE78CLFX2000P	281 June 2013
NXP	P60CC080 P60CD080	11 October 2016

In the TOE operational environment, the following is the list of components consist of hardware and software that composing the TOE, in which defined as non-dependencies to the TOE.

i. IC Hardware (as define in Table 4);

ii. Dedicated Software;

iii. Operating System (which is as part of TOE);

iv. Generic applications System Interface (which is as part of TOE); and

v. Generic applications.

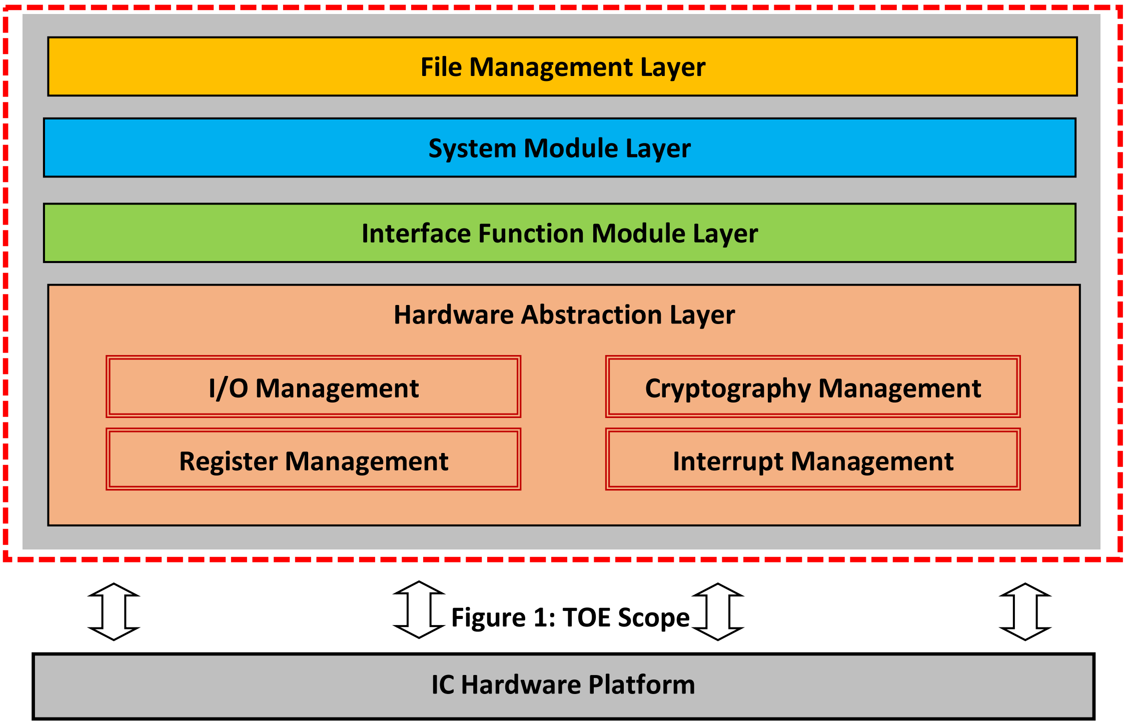
1.5 TOE Description

The TOE is a Multi-Application Smart Card Operating System is composed of hardware and software components as stated in Section 1.4.3. The TOE operates as a platform that store cardholder credentials as definitive electronic national identity card in which serves as national e-passport. The operating system is a native design platform that is using proprietary set of programming structures, in serving as national identity card.

The TOE as smart card operating system uses customize command sets (APDU) in communication with the smart card reader (also known as terminal reader or card acceptance device (CAD)), that enables layers of security protection in reading protected data inside the smart card chip memory.

Within the design of the smart card chip (IC), the following is the high level structure of the DCOS illustrate in the figure below, with the highlight of the TOE scope of evaluation. Note that the highlight **dotted RED line (DCOS Operating System)** is the scope of the TOE.

Figure 1: TOE Scope



The TOE implements the following logical components that reside upon the hardware platform IC. Note that the IC hardware platform are not part of the TOE scope of evaluation.

Table 5: List of Components in the TOE Scope

Component	Descriptions
File Management Layer	The File Management Layer holds the data and operations of generic applications by providing those generic applications to load via the virtual machine interfaces platform. Thus, allowing certain runtime API calls by those generic applications using such functions: cryptographic processing, input/output and other programming interfaces.
System Module Layer	The System Module Layer managed the process flow of the TOE by managing the initialization of the TOE and relevant generic applications when being calls in retrieving relevant data related to the generic application management.
Interface Function Module Layer	The Interface Function Module Layer is the TOE component that handles the processing requests between Application Layers and Hardware Abstraction Layer (HAL). Whilst, managing the security functions between layers of data transacted, such as between HAL and the Application Layers.
Hardware Abstraction Layer (HAL)	The hardware Abstraction layer provides access to low level IC routines provided by the certified IC and IC libraries. i. I/O Management; ii. Register Management; iii. RNG & DES Management; and **iv.** Interrupt Service.

1.5.1 Logical scope of the TOE

The TOE is an operating system design to serve the smart card chip and managing data securely stored in the memory of smart card chip (IC). Furthermore, the TOE shall operate through the interfaces of generic application that managed the data through segregation of logical data structures. Thus, the following is the scope of TOE covers in the evaluations defined as the logical boundary of the TOE that is consists of the security functionalities, is summarized below.

A. File Management

The TOE has the capabilities of preventing generic application from interfering with the other generic applications in the aspects of applet execution and accessing private data and operation of the TOE itself.

B. Generic Application and Platform Management

The TOE provides functions of secure installation and secure removal process flow of the generic application by ensuring the data management and processing of the smart card applications are allocated accordingly inside the memory of the smart card chip.

Nonetheless, the platform itself allows the owner of the card lifecycle manage the smart card through its operating system (TOE) in ensuring the continuous of the smart card usage throughout its lifecycle by the cardholder via card services management/revocation. Additionally, the platform allows the smart card owner to initiate any data/generic application accessibility through secure channel via cryptographic processing.

C. Cryptographic Management

As the smart card chip (IC) has cryptographic functions, this allows the TOE to initiate cryptographic processes on the relevant generic applications, in which these generic applications implement specific security mechanism on top of the evaluated TOE platform. Note that, the generic applications are not part of the TOE scope of evaluation.

D. TOE Self Protection and Testing

As the platform that manage those generic applications, the TOE requires to provide secure operational environment for those generic applications. Thus, set of triggers that able to react and response to any external events related to smart card chip are required to detects any failure or attempts of bypass any security measures that may compromise the TOE.

1.5.2 Physical scope of the TOE

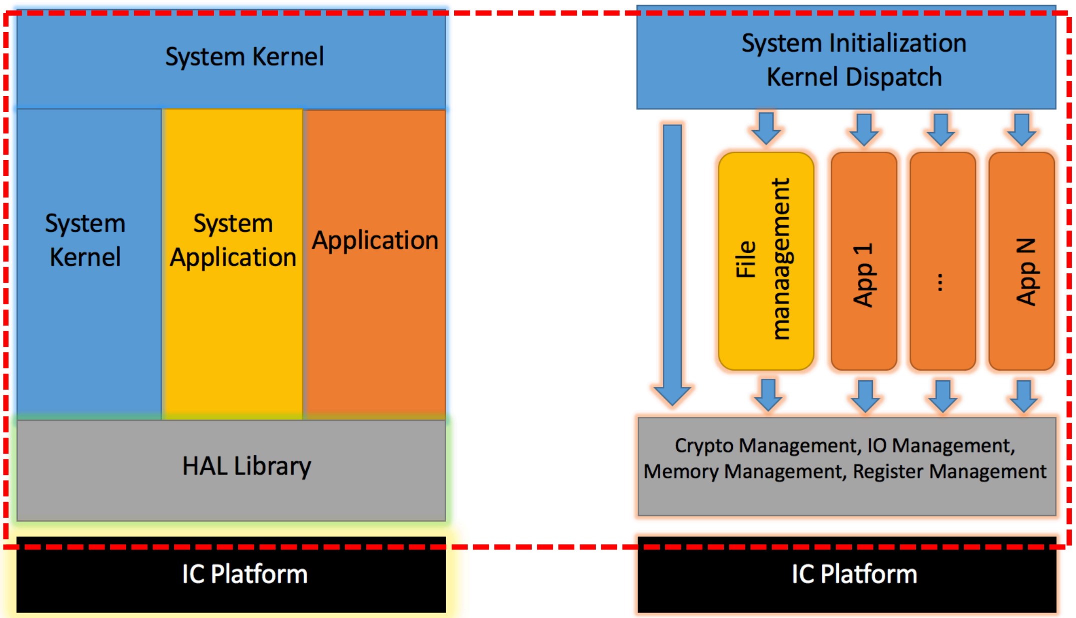
As per describe that the TOE is a multi-purpose smart card operating system that runs/execute within the hardware operational environment of certified Common Criteria IC hardware platform. Thus, it is been known that the IC hardware platform provides the physical interfaces of the TOE between cardholder with authorized terminal/smart card reader and the data resided in the management of the TOE. Note that the IC hardware platform of the certified Common Criteria, is not included inside the scope of the TOE.

In accessing the data or card holder credentials inside the smart card memory, an authorized smart card reader/terminal reader (also known as Card Acceptance Device, CAD) are require to initiate the request as in between platform of accessibility between card holder and smart card. Thus, note that the smart card reader/terminal reader (also known as CAD) are not part of the scope of the TOE.

Furthermore, the data reside in the smart card memory are under management of the TOE, based on the smart card application access control through certain addressing of the data structures. Thus, it is require to have authorized access control commands known as Application Protocol Data Unit (APDU). The TOE uses APDU commands based on ISO/IEC 7816 and ISO/IEC 14443 requirements as well as there are additional APDU commands design only for specific data structure in the management of the TOE towards the generic applications, known as proprietary APDU commands. On that note, the APDU commands are not part of the TOE.

The following is the operations of the TOE illustrated in the figure below. The **dotted RED** define the boundary of the TOE operations.

Figure 2: TOE Physical Scope



1.5.2.1 TOE Life Cycle

The following describes in the table of the TOE lifecycle and its relationship with the underlying IC lifecycle.

Table 6: TOE Lifecycle through IC Hardware Platform

Stage	Stage Title	Stage Description
Stage 1	Integrated Circuit Development Stage	• Design of IC • Development of IDE, Integrated Development Environment for IC • Provide integration document and guideline to Chip OS developer • To build the IDE IC library for the deliverable required for ROM masking/ tape out process.
Stage 2	Embedded Firmware Development Stage	• Chip OS development • Defining chip OS specification including initialization, personalization and operation process.
Stage 3	IC Manufacturing and Testing Stage	• IC manufacturing • IC testing • IC initialization
Stage 4	IC Packaging and Testing Stage	• IC Packaging and testing
Stage 5	IC card production Stage	• Embedding of chip onto card • Smart card testing • Initialization could be initiated with file creation and key injection process
Stage 6	Smart Card Personalization Stage	• Personalization of smart card • Verification of personalized data
Stage 7	Smart Card in the Field stage	• Issuance of smart card to end user • Smart card user determines the end of card life cycle.

1.5.2.2 TOE Generic Applications Life Cycle

The following describes in the table of the TOE generic applications lifecycle and its relationship towards the TOE.

Table 7: TOE Generic applications Lifecycle

Stage	Stage Title	Stage Description
A	Development of Generic Application	This stage allows any developer of the generic applications either internally or externally from the TOE developer to conduct their development of the TOE generic applications. Consideration made upon that the generic applications are met the requirements set by the TOE based on the data structures and accessibility of the data reside by the generic applications compliance with the security features of the TOE.
B	Loading the Generic Applications to the TOE	Related to the operations in stage 6 and stage 7.
C	Removal of the Generic Application from the TOE	Related to the operations in stage 7, where it can be performed before the initiation of the stage 7 or concurrent with the stage 7.

1.5.3 TOE Environment

The TOE environment is defined as following descriptions:

i. TOE Development environment corresponding to stage 1 and 2. Which is not part of the TOE scope.

ii. Production environment of the TOE consist of the stage 3 including integration of the Embedded Software (ES) in the IC and the test operations.

iii. TOE Packaging and finishing operation consist of the stage 4 and 5.

iv. Personalisation of the TOE environment consist of the personalisation and testing of the smart card with the user define data (executed in the stage 6 and stage 7).

v. The TOE User environment consist of downloading/loading/installing the generic applications software and related data (stage7) or vice versa (removal/unloading/uninstalling the generic applications) with the respect of the smart card lifecycle ended.

1.5.4 TOE Development Environment

The TOE Development Environment is defined as following descriptions:

i. With respect of the secure operational environment of the TOE, the operational development environment of the TOE must be securely managed with controllable accesses that allows traceability functions (minimum of tracking via audit logs). Furthermore, all personnel or staffs that involved in the TOE operational development environment shall follows all security mechanisms and procedures accordingly in maintaining the secure development environment.

ii. The development of the TOE defined specifically from its design during initial stage. All parties involved in the loop of communications shall abide to the Non-Disclosure Agreement either as company representatives of as individually defined.

iii. In the process of design and development of the TOE itself and its generic applications, the programmers or personnel involved shall uses secure and protection applied devices such as desktop/laptops/etc. and also within the secure operational physical environment with limited accessibility from any external access.

iv. All relevant documentations and procedures (either hardcopy or softcopy) related to the TOE shall be safely managed in a secure environment with proper protection implementations. Furthermore, in the events of documentation require disposal, proper removal of the those documentation shall be initiated with the objectives of unable to retrace the removal (such as using shredding method).

v. All types of activities such as programming, testing and delivering of the TOE shall be take place in a proper secure environment with protection mechanism are being implemented with traceability. It shall allow accountability and traceability of the TOE in its condition either good or bad as a product.

vi. Any initiation of data transfer via electronic platform, secure procedures shall established accordingly in ensuring the data arrive to the defined recipients and will not have temporary logical storage that allow any redundancy copies of the data.

1.5.5 TOE User Environment

The TOE User Environment is defined as following descriptions:

i. Within Stage 4 and 5:

Within the stage 4 and 5, the TOE is define in a form of IC Packing, involve in the smart card finishing process and the TOE test environments. All parties involved in these process flows shall abide to all security procedures and secure protection mechanism applied.

Moreover, the operational environment must be secured and protection. Any sensitive information (hard disk, tapes and etc.) are stores in appropriately locked cupboard/safe. In the events of documentation require disposal, proper removal of the those documentation shall be initiated with the objectives of unable to retrace the removal (such as using shredding method).

ii. Within Stage 6:

In the area of smart card manufacturing that involve product high volumes of smartcards quantities, adequate control procedures are necessary to account for all products at all stages.

Those smartcards should be transported and managed in a secure environment and shall allow accountability and traceability of the TOE in its condition either good or bad as a product. In this stage also, process of loading the smart card generic applications are allows to be executed within a secure environment.

iii. Within Stage 7:

During this phase, generic application can be loaded on the platform in an insecure environment. Nonetheless, it is recommended that the process of loading or unloading the generic application goes in a proper secure environment that allows protections to the TOE even though in this level of operations did not involve TOE development environment.

2 Conformance Claim

The ST and TOE are conformant to version **3.1 (revision 5)** of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- **Part 2 conformant.** Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1 (revision 5), September 2012
- **Part 3 conformant, EAL4+.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1 (revision 5), September 2012. The Evaluation is EAL4 Augmented with ALC_DVS.2 and ALC_FLR.2.

3 Security Problem Definition

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a series of ***threats*** that the TOE has been designed to mitigate;

b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate; and

c) any relevant ***organisational security policies*** are any statements made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

The following is the list of threats that is applicable for the TOE.

Table 8: Threats of the TOE

Identifier	Threat statements	Applicability
T.CLONE	An unauthorized individual with the understanding of smart card operational and logical knowledge may attempt to duplicate/cloning the data reside inside the smart card chips, in which may compromise the confidential data, generic application and TSF data in the smart card chip storage/memory.	All Stages

T.TSF_DATA	An unauthorized individual may attempt to access the confidential data transmitted/delivered/communicated in between IC designer and Loaded Applet Developers.
	Such confidential information/data can be compromise or disclosed, as the following:
	i. IC Specification;
	ii. Design documentations;
	iii. Technical Information/Specification;
	iv. Software Information uses for Testing and Development;
	v. Generic Application design and specification;
	vi. Data specification reside in the Generic Application;
	vii. IC personalization requirements/specifications;
	viii. TSF Data;
	ix. Implementation Codes and Commands;
	x. Security mechanisms in the TOE or IC (parameters, commands and etc.); and
	xi. Test data and Test Software uses by the TOE.
		Stage 1

Identifier	Threat statements	Applicability
T.THEFT	An unauthorized individual may attempt to stole/theft and/or relevant components of the TOE that may compromise the TOE design, operations and information of security mechanism of the TOE. The following is the list of relevant components of the TOE: i. Generic Application; ii. Data types and structures related to Generic Application; iii. Test Data uses by Generic Application Developer or IC Designer; iv. Development Tools and Test Tools of the TOE; and v. TOE Samples or TOE IC Samples.	Stage 1
T.MODIFY	An unauthorized individual may attempt to modify/made changes without authorization to the generic applications data during delivery of the TOE or in between communication of Developer and IC Designer. Additionally, modification can also be applied to Embedded Software or TSF Data that may compromise the TOE operations and/or TOE security features due to the changes made on the TOE specification.	Stage 1
T.DELIVERY	An unauthorized individual may attempt to have access and/or modification to relevant data (as define below) during the delivery process in between Manufacturer IC Packaging and Finalizing process by the Personaliser (Finalizer). The following is the list of relevant data, as such: i. Embedded Software Data; and ii. Generic Applications Data.	Stage 4 to Stage 6
T.DISCLOSE	An unauthorized individual may attempt to access to the following security mechanism of the TOE and its relevant components (as such: Embedded Software, Generic Application, TSF Data and etc.) that may compromise the security functionality of the TOE and its components. The TSF data that may in danger: data protection system, memory directory structure (partitions), cryptographic process flow, cryptographic functions and cryptographic keys).	Stage 4 to Stage 7
T.USAGE	An unauthorized individual may attempt to misuse the TOE with irrelevant components (unstable) that mays compromise the TOE security functions and IC security functions. Example of attempts: bond-out chips with embedded software, execute commands or any set of instructions that was not authorized for the usage of the TOE and etc.	Stage 4 to Stage 7

Identifier	Threat statements	Applicability
T.ATTACK	An unauthorized individual may attempt to perform specialized from of attack vector on the TOE that may modify, destruct and destroy relevant TSF data, which may lead to compromise the TOE or disclose TSF data or bypassing relevant security measures of the TOE. Example of attack vector, as the following: i. Probing; ii. Electronic Perturbation; iii. Circumvent TSF Protections; iv. Installing native generic application that is not authorized by the TOE usage; v. Execute unauthorized software that can modify data in the generic application or the TOE; and vi. Overwrite generic application with irrelevant data that leads to compromise the data integrity managed the generic applications.	Stage 4 to Stage 7
T.APP_LOAD	An unauthorized individual may attempt to load unauthorized generic application on the platform of the TOE that may leads to bypassing the ownership and lifecycle model defined by the card issuer. In which, the unauthorized generic application will lead to compromising any existing generic application through actions such as: bypassing file management, modify data of the existing loaded applet, altering the generic application codes, gaining access to other generic application data and etc.	Stage 6 to Stage 7
T.APP_REMOVE	An unauthorized individual may attempt to load unauthorized generic application on the platform of the TOE that may leads to removing the existing generic applications or rewriting the data inside the generic applications, making the data or generic applications unavailable. Thus, the threat may lead to disclosure of data, unavailability of access to the original generic application, removing/deleting data of the generic applications that are sensitive/confidential, destroying data that uses by the TOE in between the generic application and etc.	Stage 6 to Stage 7

3.3 Organisational Security Policies

No organisational security policies have been defined regarding the use of the TOE.

3.4 Assumptions

The following is the list of assumptions that is applicable for the TOE.

Table 9: Assumptions made for the TOE

Identifier	Assumption statements:	Applicability
A.HW_IC	It is assumed that the TOE shall be execute under the platform of certified common criteria hardware platform with the minimum requirements of EAL4 evaluated configurations. Additionally, the security functions of the evaluated hardware IC shall be utilized by the TOE in terms of cryptographic implementations and side channel attack preventions/detections. Furthermore, the evaluated hardware IC shall provide evaluated cryptographic libraries and interfaces for the usage of the TOE and its generic application.	All Stages
A.USE_TEST	It is assumed that the TOE and its relevant components are being tested on the scope of functionality test using a proper process and procedures applied in Stage 4, Stage 5 and Stage 6.	Stage 4 to Stage 6
A.USE_PROC	It is assumed that there are proper implementations of process and procedures in stage 4 to stage 6 in ensuring the confidentiality, integrity and availability of the TOE and its relevant components are in place. Preventing from any lost or being copied or being modified and etc.	Stage 4 to Stage 6
A.SEC_DEV	It is assumed that the Loaded Applet Developers and Embedded Software Developer shall design the relevant components related to the TOE operations by using authorize software development tools (compliers assemblers, linkers, simulators, etc.) and software hardware integration testing tools (emulators) that will ensure the integrity of the program and data. Note that, only authorized personnel shall handle the management of data and data confidentiality.	Stage 4 to Stage 7
A.DEL_PROC	It is assumed that the TOE components, TOE materials and TOE relevant information shall be delivered using secure platform and protected by certain measures of secure packaging.	Stage 4 to Stage 7
A.DEL_TRACK	It is assumed that there is certain measurement of actions taken into consideration if there were detection of improper operations during the delivery of the TOE and its components.	Stage 4 to Stage 7
A.DEL_STAFF	It is assumed all the handling of the TOE delivery and its component shall be executed by knowledgeable and trained competent personnel/staff.	Stage 4 to Stage 7
A.READER	It is assumed that there are secure communications protocols and procedures are used between smart card reader/terminal (CAD) and smart card.	Stage 7

Identifier	Assumption statements:	Applicability
A.LOAD_APP	It is assumed that all relevant generic application shall be loaded to the TOE management are approved and authorized by the card issuer with follow the endorsed administrator guidance.	Stage 7
A.DEL_APP	It is assumed that all relevant generic application shall be removed from the TOE management via the approval and authorization by the card issuer with follow the endorsed administrator guidance.	Stage 7

4 Security Objectives

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. There are security objectives for the TOE to address and additional objectives that provide specific direction for the intended in environment in which the TOE is to operate.

4.2 Security Objectives for the TOE

Table 10: Security Objectives of the TOE

Identifier	Objective statements
O.CLONE	The TOE shall able to protect itself from being clone and also provides protection on all sensitive data reside under TOE management relates back to the generic applications.
O.TAMPER	The TOE must prevent from any attempts of tampering with the enforce security functions. TOE able to enforce security functions with certain mechanism in place in preventing any unauthorized changes made on the TOE and its relevant components (including TSF data).
O.SIDE_CHANNEL	The TOE and Embedded Software are designed to avoid any interpretations of electrical signals manipulation from the TOE hardware components.
O.OPERATION	The TOE must ensure proper operations and continuously maintain its security protection mechanism.
O.DESIGN	The TOE design must not contain any flaws in design, operations and its implementations (process and procedures).
O.PROTECT	The TOE shall ensure that the Embedded Software with it security mechanisms are protected from any unauthorized disclosure. Protecting the TSF data and card holder data in the IC memory and preventing modification of data from unauthorized attempts/actions through the security features of the TOE.
O.RESTORE	The TOE shall operate in a secure state of operations that well defined valid state before loading relevant generic applications or removing generic application, in ensuring the processes are been validated and monitored. Restoration of the previous stated are applicable for the TOE are applicable in the events of failure processes in the TOE with certain commands or automatically performed by the TOE.
O.CONTROL	The TOE shall provide the ability of controlling the relevant components of the TOE and those relevant generic applications, in preventing any misuse or unauthorized access that leads to denial of services.

Identifier	Objective statements
	Such events of misuse or unauthorized generic applications that can access another data from other generic applications. These events must be prevented by the TOE through its management.
O.LOAD_APP	All relevant generic applications shall be load to the platform through management of the TOE with the permission of the authorised personnel (Administrator). Additionally, all generic applications shall be verified its integrity, confidentiality, and known origin by Administrator through its codes and data management process flow.
O.UNLOAD_APP	All relevant generic applications can be unloaded securely from the TOE management and its platform without any effect of operations of other generic applications in the aspects of data, codes and process flow.
O.PARTITION	All generic applications are segregated on its own data structure/directory in the platform memory through the management of TOE (File Management). TOE shall prevent any loaded applet/s from read/write on another loaded applet either codes or data without any authorization.
O.CRYPTO	The TOE shall provide sufficient cryptographic functions to the request of generic applications in order of preventing attacks against the TSF data or card holder data.

4.3 Security Objectives for the Environment

Table 11: Security Objectives of the TOE Operational Environment

Identifier	Objective statements
OE.HW_IC	The TOE and Embedded Software shall be deployed onto a certified Common Criteria IC platform that was evaluated and certified with the minimum requirements of EAL4.
OE.SEC_DEV	The Loaded Applet Developers and Embedded Software Developers shall design the relevant components related to the TOE operations using authorized software development tools (compliers assemblers, linkers, simulators, etc.) and software hardware integration testing tools (emulators) that will ensure the integrity of the program and data. Note that, only authorized personnel shall handle the management of data and data confidentiality.
OE.DEL_APP	Process and procedures of all relevant components of the TOE specifically on the generic applications shall be followed accordingly through upholding secure delivery mechanism in ensuring the availability, integrity and confidentiality are not being compromised.
OE.INITIALIZE	Process data initialization are shall only accessible to authorized personnel.

Identifier	Objective statements
OE.TEST	Sample for the testing shall be accessible only by authorized personnel.
OE.PROC	Process flow and procedures shall ensure protection of the materials/information upon delivery of the TOE and also require traceability (tracking). Process and procedures as follow: i. Established non-disclosure agreement arrangement of any security details and information; ii. Clear define identification of materials to be deliver; iii. Enforce confidentiality requirement that been approved by all parties in the delivery process; iv. Enforce physical security implementation on packaging the materials in preventing from physical damage with define procedures of handling; v. Traceability (tracking) of the packaging travel shall be labelled with details of origin info (address and name), shipment details, acknowledgement details, receipt acceptance, procedures handling and materials info.
OE.TRACK	Process flow and procedures shall ensure relevant corrective actions are taken into consideration when improper handling of the TOE in delivery and proper procedures are in place for corrective and preventive action taken. Additionally, process flow and procedures shall in place in ensuring the delivery of the TOE are successfully, secured and manageable by knowledge, skill and competent personnel; whilst acceptable by both parties (sender and recipient).
OE.USE_TEST	Any type of testing shall be certain process flow and procedures that been authorized by the card issuer and agreed by relevant parties involved in the TOE development and TOE implementations. Likewise, all measures of security mechanism shall be in place in ensuring the confidentiality, integrity and availability of TSF data are intact during the testing being performed without modifying or compromising the TOE.
OE.READER	Communication between smart card reader/terminal (CAD) shall be in a secure protocol of communications and follow specific approved procedures.
OE.LOAD_APP	All relevant Generic applications shall follow defined and approved process flow and procedures, whilst authorized by card issuer by following endorsed administrator guidance.

5 Security Functional Requirements

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (revision 5) of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].
- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].
- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.
- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

5.2 List of Security Functional Requirements (SFRs)

The following is the list of defined Security Functional Requirements (SFRs) relates to the TOE security functions, covers in the scope of evaluation.

5.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**the cryptographic key generation algorithm as stated in table below**] and specified cryptographic key sizes [**the key sizes as stated in table below**] that meet the following: [**the standards as stated in table below**].

Note: Cryptographic functions and libraries are defined based on the provided functionality of the TOE IC hardware platform.

Table 12: Cryptographic Functions Detail

Cryptographic Algorithms	Key sizes	Standards
AES	128-bit	FIPS PUB 197
DES	8-bit	FIPS PUB 46
3DES	24-bit	FIPS PUB 46-3
ECC	256-bit	SEC 1
RSA	2048-bit	PKCS#1

5.2.2 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

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

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [**encryption and decryption**] In accordance with a specified cryptographic algorithm [**the cryptographic algorithm as stated in table below**] and cryptographic key sizes [**the key sizes as stated in table below**] that meet the following: [**the standards as stated in table below**].

Note: Table 13: Cryptographic Functions Detail

Cryptographic Algorithms	Key sizes	Standards
AES	128-bit	FIPS PUB 197
DES	8-bit	FIPS PUB 46
3DES	24-bit	FIPS PUB 46-3
ECC	256-bit	SEC 1
RSA	2048-bit	PKCS#1

5.2.3 FDP_ACC.2 Complete Access Control

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the [**Lifecycle Management SFP**] on [**User attempting to retire the card from an initialised state**] and all operations among subjects and objects covered by the SFP.

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.

Note: Kindly take note:

i. User is the Subject;

ii. Retire the card is the Operation; and

iii. The Card is the Object.

5.2.4 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [**Lifecycle Management SFP**] to objects based on the following: [**initialised card**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**Card Issuer must authenticate using cryptographic function in order to change security attributes of an initialised card**].

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

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

Note: None.

5.2.5 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_RIP.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] on the [**Generic Applications**]

Note: None.

5.2.6 FDP_ROL.1 Basic rollback

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_ROL.1.1 The TSF shall enforce [**Generic Applications Installation SFP**] to permit the rollback of the [**installation of those generic applications**] on the [**TOE NVRAM**].

FDP_ROL.1.2 The TSF shall permit operations to be rolled back within the [**memory boundary limit of the task being performed when operation is prematurely terminated**].

Note: None.

5.2.7 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**symmetric and asymmetric cryptographic keys**].

Note: None.

5.2.8 FIA_UAU.1 Timing of Authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [

i. **Selection of a file;**

ii. **Selection of an application;**

iii. **Record reading;**

iv. **Opening a channel;**

v. **Closing of a channel;**

vi. **Request challenge material; and**

vii. **Check command status**] 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.

Note: None.

5.2.9 FIA_UID.1 Timing of Identification

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow [

i. **Selection of a file;**

ii. **Selection of an application;**

iii. **Record reading;**

iv. **Opening a channel;**

v. **Closing of a channel;**

vi. **Request challenge material; and**

vii. **Check command status**] on behalf of the user to be performed before the user is authenticated.

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.

Note: None.

5.2.10 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [**Generic File Management SFP**] to restrict the ability to [***modify***] the security attributes [**memory access control attributes**] to [**nobody**].

Note: None.

5.2.11 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 [**Generic File Management 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 [**nobody**] to specify alternative initial values to override the default values when an object or information is created.

Note: None.

5.2.12 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**loading and the installing, removal, and operation of generic applications]**.

Note: None.

5.2.13 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 [**authorised administrator, card holder (user) and generic application subjects**].

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

Note: None.

5.2.14 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: [**unexpected interference with TSF (FAU_ARP), IC hardware failure (unresponsive)**].

Note: None.

5.2.15 FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_PHP.3.1 The TSF shall resist [**physical attacks detectable by the IC hardware platform and side channel attacks**] to the [**IC hardware platform and embedded software**] by responding automatically such that the SFRs are always enforced.

Note: None.

6 TOE Security Assurance Requirements

As the evaluation upon the TOE, it claims that the TOE conformance to the Common Criteria Part 3 EAL4 with augmented requirements of ALC_DVS.2 and ALC_FRL.2. Thus, the following is the details of EAL4+ requirements met by the TOE inclusive of the augmentations.

Table 14: Defined SARs

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV.IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic 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.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.2 Flaw reporting procedures
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design

Assurance class	Assurance components
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

7 TOE Summary Specification

7.1 Overview

This section provides the TOE summary specification in which, illustrates the mapping of justifications on the TOE security functions in achieving the consistency with the logical scope of the TOE. Thus, the following mapping that leads with the scope of TOE shall justify the requirements of SFRs defined.

7.2 Mapping of TOE Logical Scope towards the SFRs

The following the descriptions of mapping between TOE logical scope with the list of Security Functional Requirements (SFRs) defined in this document. Whilst, this mapping shall elaborate the components of the TOE defined in the Logical Scope are meeting the SFRs as per required by the CEM.

7.2.1 File Management

The TOE allows several generic applications to exist in the TOE operations, where TOE manage multiple data sectors stored and handle by the generic applications. In which, the TOE shall be able to manage all those relevant generic applications, in which the TOE able to segregate certain sectors of memory in terms of logical access control, where those generic applications able to operations, coexist in a secure manner.

Thus, the TOE requires to allows all those generic applications to operates securely in the TOE operational environment without compromising the TOE TSF data as well as other generic applications stored on the IC platform memory, managed by the TOE. Furthermore, the TOE requires to ensure and securely protects each memory allocation of each individual loaded applet, whilst preventing data from been access without authorization either by defined loaded applet or any external or other internal components without known by the TOE. Note that, the define generic applications are not part of the TOE.

SFRs Mapped:	FDP_ACC.2c, FDP_ACF.1, FMT_MSA.1 and FMT_MSA.3.

7.2.2 Application and Platform Management

The TOE existed in ensuring the TSF data as well as User data reside in the IC hardware platform memory are managed securely and protected from any unauthorized access either externally or internally (between generic applications). In which, the TOE and other components (inclusive of the generic applications) have certain lifecycle management scheme defined by the card issuer and/or card manufacturer.

The TOE has its own management lifecycle scheme in which managed by trusted parties either the card issuer as well and the card manufacturer. Furthermore, as for generic applications developers, has also define the lifecycle of the authorized generic applications managed by the TOE. Whilst, with the capabilities of the TOE in supporting multiple application loaded into the platform (coexist), the TOE allows trusted parties such as generic applications developers or generic applications owner shall loaded and unload their authorized generic applications to the TOE platform under the TOE management.

Accessibility in loading or removal of define trusted generic applications, the TOE allows those accessibility through define authorized cryptographic authentication mechanism that enforce security protections through exchange cryptographic keys. These processes are established in all initialization of loading and removal process flow of generic applications.

All data transacted between smart card memory, TOE, generic applications and smart card reader/terminal/CAD are through encrypted data format with all initial engagement through exchange of cryptographic keys. This is to ensure TOE provides security mechanism in preventing authorization accessibility and enforcing confidentiality, integrity and availability of TOE TSF data and User data.

SFRs Mapped:	FDP_ACC.2, FDP_ACF.1, FDP_RIP.1, FDP_ROL.1, FIA_UAU.1, FIA_UID.1, FIA_ATD.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1 and FMT_SMF.1.

7.2.3 Cryptographic Management

The TOE provides accessibility to the TOE TSF data and User data stored in the IC hardware platform through secure communications using cryptographic keys exchange process flow. Those defined secure communications shall be initiated through the request made by the APDU commands send by the smart card reader/terminal/CAD. The process of cryptographic keys exchange shall enforce security mechanism in accessing encrypted data in the IC hardware platform memory, manageable by the TOE.

The TOE enforces secure communications and data management as the interfaces between IC hardware platform (memory access) and the smart card reader/terminal/CAD. Operations of cryptographic that under the TOE operations such as Digital Signing, Secure Authentication, Secure Communication and others relevant security mechanism are being applied in ensuring the data access by the trusted entities are securely managed and through proper authorizations processes. This involved the process of data encryption and data decryption as part of the process flow.

Cryptographic process flow involves in the operations of the TOE such as: DES, AES, 3DES, RSA, ECC and SHA Hashing functions. Changes of cryptographic keys uses by the TOE and generic applications are allowed if there was a request made by the card issuer and/or loaded applet developer/user. In which, this process is performed through the agreement authority of the card holder, card issuer and generic applications developer, whilst with the objective of better security enforcement applied to the TOE operational environment.

SFRs Mapped:	FCS_CKM.1 and FCS_CKM.4.

7.2.4 TOE Self Protection and Testing

The TOE has security mechanism that protect itself from any internal or external threats relevant to smart card threats and attacks. As such, the TOE able to perform self-testing by its own to ensure the TOE are not been compromise or malfunctions through unauthorized modification made on the TOE operations.

In the events of the IC hardware platform are being compromise, that lead to the TOE unable to perform self-test, the TOE shall halt from its operations and did not continues to loaded the whole TOE operations, whilst stop immediately. This is the prevention mechanism made by the TOE functions in detection physical attack on the IC hardware platform and relevant side channel attacks.

Once the TOE fail the self-test or detects the IC hardware platform are being compromise through relevant attacks approaches, the TOE shall halt and prevent the continues operation of the TOE. Therefore, this security functions prevents from the TOE disclose relevant protected data to the external threats or any other internal threats such as allows generic applications to misbehave reading irrelevant (unauthorized access to other data section) data.

SFRs Mapped:	FPT_FLS.1 and FPT_PHP.3.

8 Rationale

8.1 Assurance Requirement Rationale

This ST claims compliance to the assurance requirements from the CC EAL4 assurance package. This EAL was chosen based on the security problem definition and the security objectives for the TOE. The TOE is intended to address the common authentication and authorization attacks on the web-based applications.

Thus, provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation, to understand the security behaviour.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, implementation representation, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential.

8.2 Rationale for not Addressing the Dependencies

FAU_GEN.1 is a dependency of FAU_SAA.1 that has not been included. The dependencies of the this SFR are not applicable due to the TOE did not generate audit logs, in which there are no storage for audit logs be stored. Thus, this SFR is to define that if there are asynchronous events capture through the operations of the TOE during the operational lifetime of the TOE. It is not defined that is any requirement of the audit logs storage.

8.3 Security Objectives Rationale

The following is the mapping between Security Objectives towards the Security Problem Definition define in this document.

Table 15: Mapping SO to Threats

Security Objectives	Threats	Rationale
O.CLONE	T.CLONE	The TOE security function able to ensure that the TOE TSF data and User data are protection from being access or duplicate or clone in enforcing data confidentiality.
O.PROTECT O.OPERATION	T.TSF_DATA	The TOE security functions able to ensure that the TOE TSF Data and User data are being protected from any unauthorized access on any relevant information that shall not be disclosed.
O.TAMPER O.OPERATION O.PROTECT O.DESIGN	T.THEFT T.MODIFY	The TOE security functions able to ensure that the TOE TSF data and User data are being protected from any unauthorised access and/or attempt of modification and/or loading unauthorized foreign generic applications to the TOE operations. Additionally, the TOE are being design with enforce security features and validate functions

Security Objectives	Threats	Rationale
		that able to protect itself from modifications and detecting any attempts of compromising the TOE through proper design functions of the TOE.
O.PROTECT O.CONTROL O.PARTITION	T.DISCLOSE	The TOE security functions able to ensure that the TOE TSF data and User data are being protected from any unauthorised disclosure of information or security functionality of the TOE that enforce the TOE security mechanism, whilst upholding the confidentiality, integrity and availability of data reside in the TOE management. The TOE management consist of cryptographic functions, management of data in generic applications reside in the IC hardware platform memory, memory management partitioning and relevant components under management of the TOE. This is to ensure the TOE security functions are being enforce and protecting the data reside in the TOE management.
O.OPERATION O.PROTECT O.CONTROL O.CRYPTO	T.USAGE	The TOE security functions able to ensure all relevant security mechanism are being enforce through the management of the TOE, by validating any operations of the TOE as well as controlling all access to the TOE through cryptographic operations.
O.SIDE_CHANNEL O.CRYPTO O.OPERATION	T.ATTACK	The TOE security functions able to ensure that any unauthorized attempts of attacking the TOE either through physical attacks or logical attacks, whilst, the TOE able to detects those attempts of compromising the TOE. Additionally, all operations of the TOE are enforce through cryptographic operations and if been compromise, TOE won't allow those operations to be executed or performed.
O.LOAD_APP O.RESTORE O.CRYPTO	T.APP_LOAD	The TOE security functions able to ensure that any unauthorized access on loading foreign generic applications are being block (prevent from loaded into the TOE management) and enforcing security mechanism if there's any event of forcing the TOE to accept foreign (unauthorized generic applications) to be installed. All process of loading generic applications are through secure cryptographic process flow. Furthermore, the TOE able to restore back to the condition that the TOE in the events of

Security Objectives	Threats	Rationale
		incomplete processes and all security mechanism are in place to protect the TOE accordingly.
O.UNLOAD_APP O.RESTORE O.CRYPTO	T.APP_REMOVE	The TOE security functions able to ensure that any process on loaded applet removal are being performed securely through proper engagement of cryptographic process flow. Residual data shall made unavailable upon removal of the selected loaded applet. Furthermore, the TOE able to restore back to the condition that the TOE in the events of incomplete processes and all security mechanism are in place to protect the TOE accordingly.

8.4 Security Objectives of the TOE Operational Environment Rationale

The following is the mapping between Security Objectives of the TOE Operational Environment towards the Security Problem Definition define in this document.

Table 16: Mapping SOOE to Assumptions

Security Objectives	Assumptions	Rationale
OE.HW_IC	A.HW_IC	The TOE operational environment shall ensure that the IC hardware platform of the TOE are certified and evaluated configuration using Common Criteria with the conformance of EAL4 as the minimum requirement.
OE.TEST OE.USE_TEST	A.USE_TEST	The TOE operational environment shall ensure the relevant test cases are being perform by authorized personnel and with approved data samples define with approval by trusted parties. Furthermore, the TOE shall be tested with the guidance of proper process flow and procedures.
OE.PROC	A.USE_PROC	The TOE operational environment shall provide proper process flow and procedures in ensuring the TOE are being protected through security mechanism defined by the trusted parties.
OE.TRACK OE.INITIALIZE	A.DEL_PROC A.DEL_TRACK A.DEL_STAFF	The TOE operational environment shall provide secure operating environment for the TOE by following proper process flow and procedures with support of preventive/corrective actions being applied. This is to ensure the process of the

Security Objectives	Assumptions	Rationale
		delivery of the TOE are securely been performed by authorized personnel.
OE.READER	A.READER	The TOE operational environment shall provide secure communication process and procedures in the aspects of communication protocol between smart card reader/terminal/CAD and the smart card IC hardware platform.
OE.LOAD_APP OE.INITIALIZE	A.LOAD_APP	The TOE operational environment shall provide guidance in managing the TOE Generic applications under the provision of authorized card issuer by following agreed process and procedures in the process of loading/installation.
OE.DEL_APP	A.DEL_APP	The TOE operational environment shall provide guidance in managing the TOE Generic applications under the provision of authorized card issuer by following agreed process and procedures in the process of unloading/removal.
OE.SEC_DEV	O.SEC_DEV	The TOE operational environment shall provide guidance and procedures to be follow by external parties in developing components of the TOE operations in ensuring the TOE security functions are enforce accordingly.

8.5 Security Functional Requirements (SFRs) Rationale

The following is the mapping between SFRs towards the Security Objectives of the TOE.

Table 17: Mapping SFRs to Security Objectives

Security Objectives	SFRs	Rationale
O.CLONE	FCS_CKM.4	The TOE will overwrite or regenerate new cryptographic keys if the existing keys are not being recovered.
	FPT_PHP.3	The TOE are able to prevent or mitigate the threats from physical attacks through its security functions/mechanism.
	FCS_COP.1	The TOE enforce authentication through cryptographic processes and procedures.
	FDP_ACC.2	The TOE enforce access control authentication process and procedures through cryptographic security functions that prevents any attempt to

Security Objectives	SFRs	Rationale
		clone/tamper/authorize access of TSF data and/or User data of the TOE operations.
	FDP_ACF.1	The TOE enforce access control authentication process and procedures through cryptographic security functions that prevents any attempt to clone/tamper/authorize access of TSF data and/or User data of the TOE operations.
	FIA_UAU.1	The TOE prevent and enforce security functions of cryptographic authentication and identification in preventing unauthorized access to the TOE data/operations.
	FIA_UID.1	The TOE prevent and enforce security functions of cryptographic authentication and identification in preventing unauthorized access to the TOE data/operations.
	FMT_MSA.1	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
	FMT_MSA.3	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
O.TAMPER	FPT_FLS.1	In the events of IC hardware platform failure of operations, the TOE shall revert into fail safe state, in which secure and prevent any access to the TOE.
	FPT_PHP.3	The TOE have the capabilities to prevent any attacks through the manipulations of power supply such as through side channel attacks or violation (fault analysis).
	FIA_ATD.1	The TOE prevent and enforce security functions of cryptographic authentication and identification in preventing unauthorized access to the TOE data/operations.
	FIA_UID.1	The TOE prevent and enforce security functions of cryptographic authentication and identification in preventing unauthorized access to the TOE data/operations.
	FIA_UAU.1	The TOE prevent and enforce security functions of cryptographic authentication and identification in preventing unauthorized access to the TOE data/operations.

Security Objectives	SFRs	Rationale
	FMT_MSA.1	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
	FMT_MSA.3	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
	FMT_SMR.1	The TOE only allows authorise personnel performed management of the TOE, embedded software and generic applications. The role of administrator for the TOE are allows to perform relevant authorise TOE management.
	FCS_CKM.4	The TOE will overwrite or regenerate new cryptographic keys if the existing keys are not being recovered.
	FCS_COP.1	The TOE enforce authentication through cryptographic processes and procedures.
	FDP_ACC.2	The TOE enforce access control authentication process and procedures through cryptographic security functions that prevents any attempt to clone/tamper/authorize access of TSF data and/or User data of the TOE operations.
	FDP_ACF.1	The TOE enforce access control authentication process and procedures through cryptographic security functions that prevents any attempt to clone/tamper/authorize access of TSF data and/or User data of the TOE operations.
O.SIDE_CHANNEL	FDP_ACF.1	The TOE perform monitoring and tracks the TOE operations through observations of TOE operational behaviours that prevent any unauthorized access in between generic applications.
O.OPERATION	FMT_SMR.1	The TOE maintain the role of TOE administrator that allows to manage the TOE and its components.
	FMT_SMF.1	The TOE ensure secure communication between IC hardware platform and the CAD/terminal/smart card reader in access the generic applications data.
	FPT_PHP.3	The TOE have the capabilities to prevent any attacks through the manipulations of power supply such as through side channel attacks or violation (fault analysis).

Security Objectives	SFRs	Rationale
	FAU_SAA.1	TOE detects any attempt of physical attacks and halt the TOE operations.
	FCS_CKM.1	The TOE shall generate unique cryptographic keys for each generic applications.
	FCS_CKM.4	The TOE will overwrite or regenerate new cryptographic keys if the existing keys are not being recovered.
	FDP_ACC.2	The TOE enforce access control authentication process and procedures through cryptographic security functions that prevents any attempt to clone/tamper/authorize access of TSF data and/or User data of the TOE operations.
	FDP_ACF.1	The TOE enforce access control authentication process and procedures through cryptographic security functions that prevents any attempt to clone/tamper/authorize access of TSF data and/or User data of the TOE operations.
	FIA_ATD.1	The TOE prevent and enforce security functions of cryptographic authentication and identification in preventing unauthorized access to the TOE data/operations.
	FMT_MSA.1	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
	FMT_MSA.3	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
O.DESIGN	FDP_ACF.1	The TOE enforce cryptographic operations (access control) during loading/removal of generic applications and prevent any interference of other generic applications operations.
	FDP_ACC.2	The TOE enforce cryptographic operations (access control) during loading/removal of generic applications and prevent any interference of other generic applications operations.
	FMT_MSA.1	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
	FMT_MSA.3	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.

Security Objectives	SFRs	Rationale
	FPT_FLS.1	In the events of IC hardware platform failure of operations, the TOE shall revert into fail safe state, in which secure and prevent any access to the TOE.
O.PROTECT	FDP_ITC.1	The TOE shall track and monitor any attempts of accessing the TOE management from outside its control and prevent this from happening. TOE shall not allow unauthorized access from unknown source.
	FCD_ACF.1	The TOE prevents any modification or tampering between generic applications.
	FDP_ACC.2	The TOE prevents any modification or tampering between generic applications.
	FIA_UID.1	The TOE prevent and enforce security functions of cryptographic authentication and identification in preventing unauthorized access to the TOE data/operations.
	FIA_UAU.1	The TOE prevent and enforce security functions of cryptographic authentication and identification in preventing unauthorized access to the TOE data/operations.
	FIA_ATD.1	The TOE prevent and enforce security functions of cryptographic authentication and identification in preventing unauthorized access to the TOE data/operations.
	FCS_COP.1	The TOE enforce authentication through cryptographic processes and procedures.
	FCS_CKM.4	The TOE will overwrite or regenerate new cryptographic keys if the existing keys are not being recovered.
	FMT_MSA.1	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
	FMT_MSA.3	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
	FPT_PHP.3	The TOE have the capabilities to prevent any attacks through the manipulations of power supply such as through side channel attacks or violation (fault analysis).

Security Objectives	SFRs	Rationale
O.RESTORE	FDP_ROL.1	If there any failure operations under the provision of the TOE, the TOE shall reverts to the secure state if those operations were minor issues.
O.CONTROL	FDP_ACC.2	The TOE response and fail safe mode upon physical attacks being applied.
	FMT_SMR.1	TOE detects any attempt of physical attacks and halt the TOE operations.
O.LOAD_APP	FIA_UID.1	The TOE prevent and enforce security functions of cryptographic authentication and identification in preventing unauthorized access to the TOE data/operations.
	FIA_UAU.1	The TOE prevent and enforce security functions of cryptographic authentication and identification in preventing unauthorized access to the TOE data/operations.
	FMT_MSA.1	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
	FMT_MSA.3	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
	FMT_SMR.1	The TOE maintain the role of TOE administrator that allows to manage the TOE and its components.
	FMT_SMF.1	The TOE ensure secure communication between IC hardware platform and the CAD/terminal/smart card reader in access the generic applications data.
	FDP_ACF.1	The TOE enforce cryptographic operations (access control) during loading/removal of generic applications and prevent any interference of other generic applications operations.
	FDP_ACC.2	The TOE enforce cryptographic operations (access control) during loading/removal of generic applications and prevent any interference of other generic applications operations.
	FCS_COP.1	The TOE enforce authentication through cryptographic processes and procedures.
O.UNLOAD_APP	FIA_UID.1	The TOE prevent and enforce security functions of cryptographic authentication and identification in

Security Objectives	SFRs	Rationale
		preventing unauthorized access to the TOE data/operations.
	FIA_UAU.1	The TOE prevent and enforce security functions of cryptographic authentication and identification in preventing unauthorized access to the TOE data/operations.
	FDP_ACF.1	The TOE enforce cryptographic operations (access control) during loading/removal of generic applications and prevent any interference of other generic applications operations.
	FDP_ACC.2	The TOE enforce cryptographic operations (access control) during loading/removal of generic applications and prevent any interference of other generic applications operations.
	FMT_MSA.1	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
	FMT_MSA.3	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
	FMT_SMR.1	The TOE maintain the role of TOE administrator that allows to manage the TOE and its components.
	FMT_SMF.1	The TOE ensure secure communication between IC hardware platform and the CAD/terminal/smart card reader in access the generic applications data.
	FCS_CKM.4	The TOE will overwrite or regenerate new cryptographic keys if the existing keys are not being recovered.
	FCS_COP.1	The TOE enforce authentication through cryptographic processes and procedures.
	FDP_RIP.1	The TOE ensure reallocation of allocated data previously will not be available for access.
O.PARTITION	FDP_ACF.1	The TOE enforce cryptographic operations (access control) during loading/removal of generic applications and prevent any interference of other generic applications operations.
	FDP_ACC.2	The TOE enforce cryptographic operations (access control) during loading/removal of generic applications and prevent any interference of other generic applications operations.

Security Objectives	SFRs	Rationale
	FMT_MSA.1	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
	FMT_MSA.3	Applied TOE controls of the security attributes defined in the FDP_ACC.2 and FDP_ACF.1.
O.CRYPTO	FCS_CKM.1	The TOE generates relevant cryptographic keys for each generic applications.
	FCS_COP.1	The TOE provides relevant cryptographic processes for all TOE operations, Embedded Software and Generic applications.

9 Acronyms and Abbreviations

CC	Common Criteria
DES	Data Encryption Standard
ECC	Elliptic Curve Cryptography
ES	Embedded Software
IC	Integrated Circuited
RSA	Rivest, Shamir & Adleman Cryptographic Algorithm
TSF	TOE Security Function
SFR	Security Functional Requirement
TOE	Target of Evaluation

--End of Document--