# Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

| | |
|---|---|
| Application date/ID | 2008-01-25 (ITC-8194) |
| Certification No. | C0229 |
| Sponsor | SC Square LTD. |
| Name of TOE | Apollo OS e-Passport |
| Version of TOE | V1.0 |
| PP Conformance | Common Criteria Protection Profile, Machine Readable Travel Document with "ICAO Application", Basic Access Control, version: 1.0, 18 August 2005, BSI, BSI-PP-0017 |
| Conformed Claim | EAL4 Augmented with ADV_IMP.2, ALC_DVS.2 |
| Developer | SC Square LTD. |
| Evaluation Facility | TÜV Informationstechnik GmbH, Evaluation Body for IT-Security |

This is to report that the evaluation result for the above TOE is certified as follows.
2009-07-27

Takumi Yamasato, Technical Manager
Information Security Certification Office
IT Security Center

**Evaluation Criteria, etc.:** This TOE is evaluated in accordance with the following criteria prescribed in the "IT Security Evaluation and Certification Scheme".

- Common Criteria for Information Technology Security Evaluation Version 2.3 (ISO/IEC 15408:2005)
- Common Methodology for Information Technology Security Evaluation Version 2.3 (ISO/IEC 18045:2005)

**Evaluation Result: Pass**

"Apollo OS e-Passport" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

## Table of Contents

# 1. Executive Summary

## 1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Apollo OS e-Passport" (hereinafter referred to as "the TOE") conducted by TÜV Informationstechnik GmbH, Evaluation Body for IT-Security (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, SC Square LTD.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to "1.5.9 Documents Attached to Product" for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

## 1.2 Evaluated Product

### 1.2.1 Name of Product

The target product by this Certificate is as follows:

|  |  |
|---|---|
| Name of Product: | Apollo OS e-Passport |
| Version: | 1.0 |
| Developer: | SC Square LTD. |

### 1.2.2 Product Overview

The Target of Evaluation (TOE) is the contactless integrated circuit chip （including software on the chip） implemented in MRTD （Machine readable travel document: For instance, public document required for travel abroad like a passport.）.

MRTD is issued to the holder to travel abroad. The holder presents a MRTD to the inspection system to prove his or her identity with reference to personal data kept in MRTD at the immigration/exit examination

MRZ （Machine Readable Zone） data and the digitized portraits like a facial portrait are kept in IC chip implemented in MRTD according to LDS（Logical Data Structure） specified by ICAO（International Civil Aviation Organization）.

The issuing State or Organization ensures the authenticity of the data of genuine MRTD's and those data will be protected by TOE security function since it has been issued.

ICAO specifies not only the specification of LDS but also the specification of Passive Authentication to assure the integrity of data and the specification of Basic Access Control to prevent skimming.

MRTD has to implement the functions in conformity with the specification.

### 1.2.3 Scope of TOE and Overview of Operation

TOE is the IC chip in the passport book and the software in it. This is the composite evaluation of the TOE together with a smart card. The chip itself has already evaluated and certified according to EAL 5 augmented with components ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.　In this evaluation, MRTD V1.0 Application in the following figure 1-1 and the software of Operating System Apollo OS V3.17 and Keys were evaluated according to CC/CEM and the consistency of evaluation result between IC chip and the software is also evaluated according to CC support document [19].

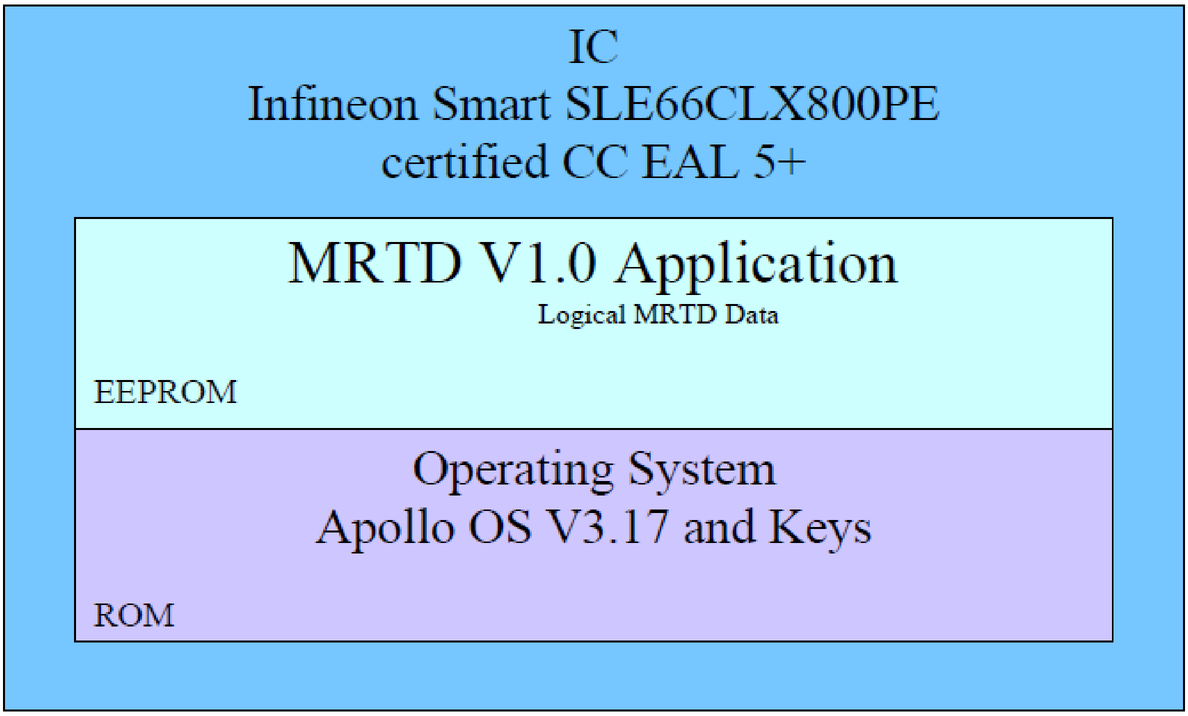

Figure 1-1 TOE Configuration

To be more precise, TOE is composed of the IC chip（Infineon Smart SLE66CLX800PE）in the above figure, MRTD V1.0 Application on EEPROM which is operated on the chip and Operating System Apollo OS V3.17 on the ROM.

IC chip has evaluated on January 2007 by the evaluation facility（TÜV Informationstechnik GmbH, Evaluation Body for IT-Security）in charge of this case.

TOE is the device to reply the required response when the prescribed conditions（success of authentication and so on）are satisfied. For instance, when the inspection system read the data in LDS, Read Binary command is issued to TOE and if the TOE is succeeded the certification, the data in LDS is sent back as the response.

This TOE is contactless chip so that command and response are exchanged as the wireless data between TOE and Inspection System.

### 1.2.4 TOE Functionality

The TOE provides the following service functions.

The main function of TOE is access function to the data in LDS.

When personalize the holder, the personal data like name, nationality and face portrait is written in LDS and at a inspection, the identity is confirmed using those data.

As a matter of course, Access control function that is associated with the data access is one of the main functions of TOE.

In considering with the characteristic of MRTD, forgery preventions of passport or countermeasures for threats like unauthorized data extraction and skimming is necessary.

Accordingly, the security specification to protect from the threats is specified by ICAO. One is the mechanism called Passive Authentication that assure the data integrity of stored data in LDS

To be more precise, it is the mechanism to assure the integrity by storing the digital signature in the hash of LDS data (Document Security Object) in the chip side and verifying the hash in the inspection system side. Accordingly, the passive authentication can be said the security function implemented in the inspection system side.

The other is Basic Access Control which prevent the skimming. It is the main security function implemented in TOE side. Regarding the detail of Basic Access Control, refer to the "1.5.4 Security Function".

## 1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Procedure"[3] and "Evaluation Facility Approval Procedure"[4].

Scope of the evaluation is as follow.

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined "Security Target For Apollo OS e-Passport V1.0" (hereinafter referred to as "the ST")[1] as the basic design of security functions for the TOE, the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex B of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7], [10] or [13]) as its rationale. Such evaluation procedure and its result are presented in "EVALUATION TECHNICAL REPORT(ETR)"(hereinafter referred to as "the Evaluation Technical Report" [17]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]). Regarding Composite evaluation, smartcard specific prescription for evaluation and evaluation approach for assurance components which are not prescribed in CEM, they are based on the supporting documents (either of [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29]or[30]).

## 1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated 2009-7-16 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

## 1.5 Overview of Report

### 1.5.1 PP Conformance

Refer to [31] regarding conformable PP.

### 1.5.2 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL4 augmented with ADV_IMP.2 and ALC_DVS.2.

### 1.5.3 SOF

ST claimed the minimum strength of function level of the TOE security functions to be SOF-high.

Considering that this TOE is implemented in the passport that has a high-risk of forgery and attackers with high attack potential, the strength of security function level is needed to be SOF-high.

### 1.5.4 Security Functions

Security functions of the TOE are as follows.

Main security function of this TOE is Access Control Function to Data and Basic Access Control as stated previously.

Basic Access Control is so-called "Secure Messaging Function in Smart Cards" that generates Session key and Authentication keys after generating the seed based on MRZ, encrypts the communication by Session key and assures the integrity of the communication by Certification key.

Accordingly, Basic Access Control is implemented in the following **F.Cryptographic Support** function and **SF.Identification and Authentication** function.

Depending on the functions in Inspection System side, Basic Access Control can be set whether Enable/Disable. **SF.Security Management** function that provides such management is also TOE security function.

Data access control function is equivalent to **SF.User Data Protection** function.

Beside this, TOE implements Self protection functions such as to reset itself when detect the physical attack by **SF.Protection** function.

Table 1-1 TOE Security Functions

| TOE Security Functions | Description |
|---|---|
| SF.Cryptographic Support | Cryptographic functions like cryptographic key generation /destroying, encryption using Triple DES and random number generation. |
| SF.Identification and Authentication | Identification and Authentication related functions like Terminal Authentication using Basic Access Control, Replay Prevention at Basic Access Control and Certification of Personalization Agent and so on. |
| SF.User Data Protection | LDS data protection function to allow only for personalization agents to write LDS data and to allow read only for others. |
| SF.Security Management | Security management function to allow only for personalization agents to enable /disable Basic Access Control. |
| SF.Protection | TSF protection function to detect physical attack by electrical voltage and heat sensor and bypassing prevention function. |

### 1.5.5 Threat

This TOE assumes such threats presented in Table 1-2 and provides functions for countermeasure to them.

Table 1-2 Assumed Threats

| Identifier | Threat |
|---|---|
| T.Chip_ID | **Identification of MRTD's chip**<br>An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening a communication through the contactless communication interface. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page. |
| T.Skimming | **Skimming the logical MRTD**<br>An attacker imitates the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page. |
| T.Eavesdropping | **Eavesdropping to the communication between TOE and inspection system**<br>An attacker is listening to the communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know this data in advance.<br>Note in case of T.Skimming the attacker is establishing a communication with the MRTD's chip not knowing the MRZ data printed on the MRTD data page and without a help of the inspection system which knows these data. In case of T.Eavesdropping the attacker uses the communication of the inspection system. |
| T.Forgery | **Forgery of data on MRTD's chip**<br>An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to impose on an inspection system by means of the changed MRTD holders identity or biometric reference data. This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveller. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTD's to create a new forged MRTD, e.g. the attacker write the digitized portrait and optional biometric reference data of finger read from the logical MRTD of a traveller into an other MTRD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the |

| | |
|---|---|
| | complete unchanged logical MRTD in another contactless chip. The TOE shall avert the threat as specified below. |
| T.Abuse-Func | **Abuse of Functionality**<br>An attacker may use functions of the TOE which shall not be used in TOE operational phase in order<br>i. to manipulate User Data,<br>ii. to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or<br>iii. to disclose or to manipulate TSF Data.<br>This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder. |
| T.Information_Leakage | **Information Leakage from MRTD's chip**<br>An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis). |
| T.Phys-Tamper | **Physical Tampering**<br>An attacker may perform physical probing of the MRTD's chip in order<br>i. to disclose TSF Data, or<br>ii. to disclose/reconstruct the MRTD's chip Embedded Software.<br>An attacker may physically modify the MRTD's chip in order to<br>i. modify security features or functions of the MRTD's chip,<br>ii. modify security functions of the MRTD's chip Embedded Software,<br>iii. to modify User Data or<br>iv. to modify TSF data.<br>The physical tampering may be focused directly on the discloser or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct |

| | |
|---|---|
| | interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used.<br>Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary. |
| T.Malfunction | **Malfunction due to Environmental Stress**<br>An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to<br>i. deactivate or modify security features or functions of the TOE or<br>ii. Circumvent or deactivate or modify security functions of the MRTD's chip Embedded Software.<br>This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misuse of administration function. To exploit this attacker needs information about the functional operation |

### 1.5.6 Organisational Security Policy

Organizational security policy required in use of the TOE is presented in Table 1-3.

Table 1-3 Organisational Security Policies

| Identifier | Organisational Security Policies |
|---|---|
| **P.Manufact** | **Manufacturing of the MRTD's chip**<br>The IC Manufacturer and MRTD Manufacturer ensure the quality and the security of the manufacturing process and control the MRTD's material in the Phase 2 Manufacturing (*). The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.<br>*Lifecycle of TOE can be divided into four phases.<br>Phase 1: Development (Create IC chip and software individually.)<br>Phase 2: Manufacturing (Load the software to IC chip)<br>Phase 3: Personalization (Write the personal information of holder.)<br>Phase 4: Operational Use (Delivery and receipt of MRTD to holder) |
| **P.Personalization** | **Personalization of the MRTD by issuing** |

| | |
|---|---|
| | **State or Organization only**<br>The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical MRTD with respect to the MRTD holder. The personalization of the MRTD for the holder is performed by authorized agents of the issuing State or Organization only. |
| **P.Personal_Data** | **Personal data protection policy**<br>The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (DG1), the printed portrait and the digitized portrait (DG2), the biometric reference data of finger(s) (DG3), the biometric reference data of iris image(s) (DG4) and data according to LDS (DG5 to DG14, DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [PKI]. The issuing State or Organization decides<br>i. to enable the Basic Access Control for the protection of the MRTD holder personal data or<br>ii. to disable the Basic Access Control to allow Primary Inspection Systems of the receiving States and all other terminals to read the logical MRTD. |

### 1.5.7 Configuration Requirements

Primary Inspection System which is not corresponded to Basic Access Control and

Basic Inspection System which is corresponded to Basic Access Control are existed in Inspection System that communicates TOE.

To use TOE in Primary Inspection System environment, Basic Access Control must be set Disable. In Basic Inspection System environment, Basic Access Control must be set Enable.

### 1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-2.

The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-4 Assumptions in Use of the TOE

| Identifier | Assumptions |
|---|---|
| **A.PERS_AGENT** | **PERSONALIZATION OF THE MRTD'S CHIP**<br>The Personalization Agent ensures the correctness of<br><br>i. the logical MRTD with respect to the MRTD holder,<br>ii. the Document Basic Access Keys,<br>iii. the Active Authentication Public Key Info (DG15) if stored on the MRTD's chip, and<br>iv. The Document Signer Public Key Certificate (if stored on the MRTD's chip).<br>The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms. |
| **A.INSP_SYS** | **INSPECTION SYSTEMS FOR GLOBAL INTEROPERABILITY**<br>The Inspection System is used by the border control officer of the receiving State<br>i. examining an MRTD presented by the traveller and verifying its authenticity and<br>ii. verifying the traveller as MRTD holder. The Primary Inspection System for global interoperability contains the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization [PKI]. The Primary Inspection System performs the Passive Authentication to verify the logical MRTD if the logical MRTD is not protected by Basic Access Control. The Basic Inspection System in addition to the Primary Inspection System implements the terminal part of the Basic Access Control and reads the logical MRTD being under Basic access Control.<br>The TOE allows the Personalization agent to disable the Basic Access Control for use with Primary Inspection Systems. |

### 1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

Regarding the attached documents come with the IC chip, refer to [32] of certification of IC chip (Infineon Smart SLE66CLX800PE).

Apollo OS - Smart Card Operating System Guide - Version 3.17 - User Guide V1.3 2009-04-01

Apollo OS - Smart Card Operating System Guide - Version 3.17 - Administrator Guide V1.5 2009-04-01

# 2. Conduct and Results of Evaluation by Evaluation Facility

## 2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are report in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM.

## 2.2 Overview of Evaluation Conducted

The history of evaluation conducted was present in the Evaluation Technical Report as follows.

Evaluation has started on 2008-03 and concluded by completion the Evaluation Technical Report dated 2009-07. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites on 2008-06 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on 2009-03.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to developer. These concerns were reviewed by developer and all problems were solved eventually.

As for concerns indicated during evaluation process by the Certification Body, the certification review was sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

## 2.3 Product Testing

Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

### 2.3.1 Developer Testing

1) Developer Test Environment

Test configuration performed by the evaluator is as follows:

- Personal Computers with Windows XP, 2000.

- PC card readers

  - Contactless reader ACG - Dual 2.2

- Contactless reader Micropross – class 185, part number 907-1056C

- IDE, TT$^2$, Golden Reader Tool, KMT, SCOUT

- ROM Monitor Infineon (KEIL) – RM66-II-P/PE version 2.62.

- Contactless Card adapter spy 06/41

2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follows:

a. Test configuration

Test configuration performed by the developer is shown above 1).
Developer testing was performed by means of TOE and Contactless readers, or debugger.

b. Testing Approach

For the testing, following approach was used.

1. Executing a sequence of commands by automatic scripts from Contactless reader, compare the response recorded on log file with the expected test results.
2. Referring contents of memory sequentially with debugger, compare them with the expected test results and perform testing.

c. Scope of Testing Performed

Testing is performed about 53 items by the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the high-level design and the subsystem interfaces.

d. Result

The evaluator confirmed consistency between the expected test results and the actual test results provided by the developer. The Evaluator confirmed the developer testing approach performed and legitimacy of items performed, and confirmed consistency between the testing approach described in the test plan and the actual test results.

### 2.3.2 Evaluator Testing

1) Evaluator Test Environment

Test configuration performed by the evaluator shall be the same configuration with developer testing described in section 2.3.1 1). Only a penetration test, i.e. Alpha fault injection test, is conducted in the following configuration using the Alpha radiator which is not used in Developer Testing.

- Personal Computer with Windows XP
- Contactless reader SCM SDI 010
- Alpha radiator
    - Ra-226-isotope
    - activity 3,3 kBq
    - isotope-holder: aluminium bar (φ10mm)
    - exhaust port φ3mm
    - installation depth 3mm
- DPA_FI (Software)

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

Evaluator testing was performed at the same TOE testing environment with the Contactless reader and Debugger. Alpha radiator mentioned above 1) was also used for a part of testing.

b. Testing Approach

For the testing, the following approach was used.

1. Perform a series of commands from the contactless reader by the automatic script. Record the response to the log file. Then, compare them to the expected results.
2. Refer the contents of sequential memory using Debugger and compare them to the expected results.
3. Perform the Fault Injection Test using Alpha radiator to emit

alpha-particles.

c. Scope of Testing Performed

Total of 83 items of testing; namely 30 items ( Independent Testing: 17 items, Penetration Testing:13 items) from testing devised by the evaluator and 53 items from testing from sampling of developer testing were conducted. As for selection of the test subset, the following factors are considered.

1. Additional testing of all tests performed by the developer. (53 items)
2. Select the test items to cover all security functions in the Evaluator independent testing.
3. Select the test items to specify the attack scenario followed by CC support documents [26] and [27] in the Penetration testing.

d. Result

All evaluator testing conducted is complete correctly and could confirm the behavior of the TOE. The evaluator also confirmed that all the test results are consistent with the behavior.

## 2.4 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM by submitting the Evaluation Technical Report.

## 3. Conduct of Certification

The following certification was conducted based on each materials submitted by evaluation facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The Evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in certification process were prepared as certification review, which were sent to evaluation facility.

The Certification Body confirmed such concerns pointed out in Observation Reports and certification reviews were solved in the ST and the Evaluation Technical Report.

# 4. Conclusion

## 4.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the EAL4 augmented with ADV_IMP.2 and ALC_DVS.2 assurance requirements prescribed in CC Part 3.

## 4.2 Recommendations

None

## 5. Glossary

The abbreviations used in this report are listed below.

| | |
|---|---|
| CC | Common Criteria for Information Technology Security Evaluation |
| CEM | Common Methodology for Information Technology Security Evaluation |
| EAL | Evaluation Assurance Level |
| PP | Protection Profile |
| SOF | Strength of Function |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |

The TOE specific abbreviations used in this report are listed below.

| | |
|---|---|
| DEMA | Differential Electromagnetic Analysis |
| DG | Data Group |
| DPA | Differential Power Analysis |
| ICAO | International Civil Aviation Organization |
| LDS | Logical Data Structure |
| MRTD | Machine Readable Travel Document |
| MRZ | Machine Readable Zone |

The glossaries used in this report are listed below.

Active Authentication
Mechanism specified by ICAO to verify that MRTD chip is genuine by Inspection System.

Alpha fault injection
Test whether security problems occurs or not by causing the malfunction by emitting Alpha-particles.

Basic Access Control
Secure messaging function specified by ICAO to prevent skimming.

Basic Inspection System
The Inspection System which enabled Basic Access Control. The communication between Basic Inspection System and TOE is protected by Secure Messaging.

Country Signing Public Key
Public key used to verify "Document Signer Public Key Certificate".

DEMA

Abbreviated expressions of "Differential Electromagnetic Analysis".
Attack to estimate the confidential information like keys by measuring the electromagnetic wave emitted from the chip several times and analyzing them.

Differential Fault Analysis

Attack to estimate the logic and the like in the chip from the behavior at a failure by causing the malfunction by emitting the electromagnetic wave and so on.

Document Basic Access Key

Key used for Secure Messaging of Basic Access Control. It is generated from MRZ as a seed.

DG

Abbreviated expressions of "Data Group".
A unit of data components in LDS.
For instance, MRZ data for DG1, Facial portrait and so on for DG2 and what kind of data is kept for each DG are specified.

Document Signer Public Key

Public key used to verify the signed Document Security Object.

Document Signer Public Key Certificate

Certificate used to verify the signed Document Security Object.

DPA

Abbreviated expressions of "Differential Power Analysis".
Attack to estimate the confidential information like keys by measuring the current of electricity consumed by the chip several times and analyzing them.

Document Security Object

Stored Data in LDS which is hashed and is signed with private key. It is kept in the IC chip.

ICAO

Abbreviated expressions of "International Civil Aviation Organization".
It is the organization to develop and establish the

general rule and technology regarding the international civil aviation and aimed to its sound development. It also specifies all kinds of rules about a passport.

Inspection System

Equipments to ensure the correctness of the contents of MRTD presented by the holder and to perform the personal identification based on it.

LDS

Abbreviated expressions of "Logical Data Structure".
It specifies the structure of logical data in the chip.

MRTD

Abbreviated expressions of "Machine readable travel document".
Documents used for the travel abroad issued form the public organization. (So- called passport and visa.)

MRZ

Abbreviated expressions of "Machine Readable Zone ".
Basic information about the holder's like issued country, holder's name and nationality.
Those information is printed in the designated area of passport and the same data is also kept in the chip.

Passive Authentication

Mechanism to ensure the integrity of data kept in LDS using digital sign.

Personalization

To be recorded the personal data to MRTD (including TOE).

Personalization Agent

Object to perform the operation of Personalization.

Personalization Agent Key

Key used to certificate the Personalization Agent.

Pre-personalization Data

Information to be written in nonvolatile memory of IC chip by MRTD manufacture.
For instance, Personalization Agent Key and so on.

Primary Inspection System

Inspection System not corresponded to Basic Access Control.
Communication between Primary Inspection System

and TOE is not protected with Secure Messaging and it is plaintext.

Smart card Composite Evaluation

It means that to evaluate the IC chip first, then evaluate the software run on the chip by the evaluation result as a input.
Evaluation method is described on CC support document [18] which is supplied separately from CC/CEM.

## 6. Bibliography

[1] Security Targets For Apollo OS e-Passport V1.0 Version 1.03, 14 July 2009

[2] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[3] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[4] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3, August 2005, CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3, August 2005, CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3, August 2005, CCMB-2005-08-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3, August 2005, CCMB-2005-08-001
(Translation Version 1.0 December 2005)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3, August 2005, CCMB-2005-08-002 (Translation Version 1.0 December 2005)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3, August 2005, CCMB-2005-08-003
(Translation Version 1.0 December 2005)

[11] ISO/IEC 15408-1:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3, August 2005, CCMB-2005-08-004

[15] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3, August 2005, CCMB-2005-08-004
(Translation Version 1.0, December 2005)

[16] ISO/IEC 18045:2005 Information technology - Security techniques -

Methodology for IT security evaluation

[17] EVALUATION TECHNICAL REPORT(ETR) Version 1, 16 July 2009

[18] Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0 Revision 1 CCDB-2007-09-001

[19] Application Notes and Interpretation of the Scheme (AIS), AIS 1,Durchführung der Ortsbesichtigung in der Entwicklungsumgebungdes Herstellers, Version 13, 14 August 2008, Bundesamt für Sicherheit in der Informationstechnik.

[20] Application Notes and Interpretation of the Scheme (AIS), AIS 14, Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC, Version 1, 24 November 1998, Bundesamt für Sicherheit in der Informationstechnik.

[21] Application Notes and Interpretation of the Scheme (AIS), AIS 19, Gliederung des ETR, Version 1, 12 November 1998, Bundesamt für Sicherheit in der Informationstechnik.

[22] Application Notes and Interpretation of the Scheme (AIS), AIS 23, Zusammentragen von Nachweisen der Entwickler, Version 2, 11 March 2009, Bundesamt für Sicherheit in der Informationstechnik.

[23] Application Notes and Interpretation of the Scheme (AIS), AIS 31, Functionality classes and evaluation methodology for physical random number generators, Version 1, 25 September 2001, Bundesamt für Sicherheit in der Informationstechnik.

[24] Application Notes and Interpretation of the Scheme (AIS), AIS 32, Übernahme international abgestimmter CC Interpretationen ins deutsche Zertifizierungsschema, Version 1, 2 July 2001, Bundesamt für Sicherheit in der Informationstechnik.

[25] Application Notes and Interpretation of the Scheme (AIS), AIS 34, Evaluation Methodology for CC Assurance Classes for EAL5+, Version 1.4, 14 August 2008, Bundesamt für Sicherheit in der Informationstechnik.

[26] Joint Interpretation Library, Application of Attack Potential to Smartcards, Version 2.7, February 2009, BSI, TÜViT, et. al.

[27] Joint Interpretation Library, Attack Methods for Smartcards and Similar Devices, confidential Version 1.5, February 2009, BSI, TÜViT, et. al.

[28] CC Supporting Document Guidance, Smartcard Evaluation, Version 1.3, Revision 1, March 2006, CCDB-2006-04-001

[29] Joint Interpretation Library - The Application of CC to Integrated Circuits, Version 3.0, February 2009

[30] CC Supporting Document Guidance, Mandatory Technical Document, Application of Attack Potential to Smartcards, Version 2.7 Revision 1, March 2009, CCDB-2009-03-001

[31] Common Criteria Protection Profile, Machine Readable Travel Document with

„ICAO Application", Basic Access Control, version: 1.0, 18 August 2005, BSI, BSI-PP-0017

[32] BSI-DSZ-CC-0399-2007 for Infineon Smart Card IC (Security Controller) SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12 and SLE66CLX360PES / m1589-e12 with specific IC Dedicated Software from Infineon Technologies AG