認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙押印済

評価対象

申請受付日（受付番号）	**平成**20**年**1**月**25**日** (IT**認証**8194)
認証番号	C0229
認証申請者	SC Square LTD.
TOE**の名称**	Apollo OS e-Passport
TOE**のバージョン**	1.0
PP**適合**	**あり**
適合する保証パッケージ	EAL4**及び追加の保証コンポーネント**ADV_IMP.2**、**ALC_DVS.2
開発者	SC Square LTD.
評価機関の名称	TÜV Informationstechnik GmbH, Evaluation Body for IT-Security

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成21年7月27日

セキュリティセンター 情報セキュリティ認証室
技術管理者　山里 拓己

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「Apollo OS e-Passport」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「Apollo OS e-Passport」（以下「本TOE」という。）についてTÜV Informationstechnik GmbH, Evaluation Body for IT-Security（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者であるSC Square LTD.に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称：	Apollo OS e-Passport
バージョン：	1.0
開発者：	SC Square LTD.

1.2.2 製品概要

TOEは、MRTD（Machine readable travel document：例えばパスポート等を海外旅行に必要な公式文書）に埋め込まれた非接触型ICチップ（チップ上のソフトウェアも含む）である。MRTDは海外旅行のために所有者に発行され、所有者は入出国審査時にMRTDを提示し審査を受ける。審査時にはInspection SystemはMRTDに保持された本人データを参照し、本人確認を実施することができる。

MRTDのICチップには、ICAO（International Civil Aviation Organization）により規定されたLDS（Logical Data Structure）に従い、MRZ（Machine Readable Zone）データや顔写真などの情報が保存される。それらデータの真正性はMRTDの発行主体が保証するが、発行以降はTOEのセキュリティ機能により保護される。

ICAOはLDSの仕様を規定するほか、データの完全性を保証するPassive Authentication、スキミングを防止するBasic Access Control等の仕様も決定しており、MRTDはその仕様に準拠した機能を実装する必要がある。

1.2.3 TOEの範囲と動作概要

TOEはパスポート内のICチップ本体とその中に含まれるソフトウェアである。本評価はスマートカードコンポジット評価であり、ICチップ自体（下図1-1のIC Infineon Smart SLE66CLX800PE）は既にEAL5及び追加保証コンポーネントALC_DVS.2、AVA_MSU.3、AVA_VLA.4により評価認証済みである。本評価においては下図1-1のMRTD V1.0 ApplicationとOperating System Apollo OS V3.17 and Keysのソフトウェア部分とCC/CEMに従い評価するとともに、CCサポート文書[19]によりICチップとソフトウェア部分の評価結果の整合性も鑑みた評価も併せて実施している。

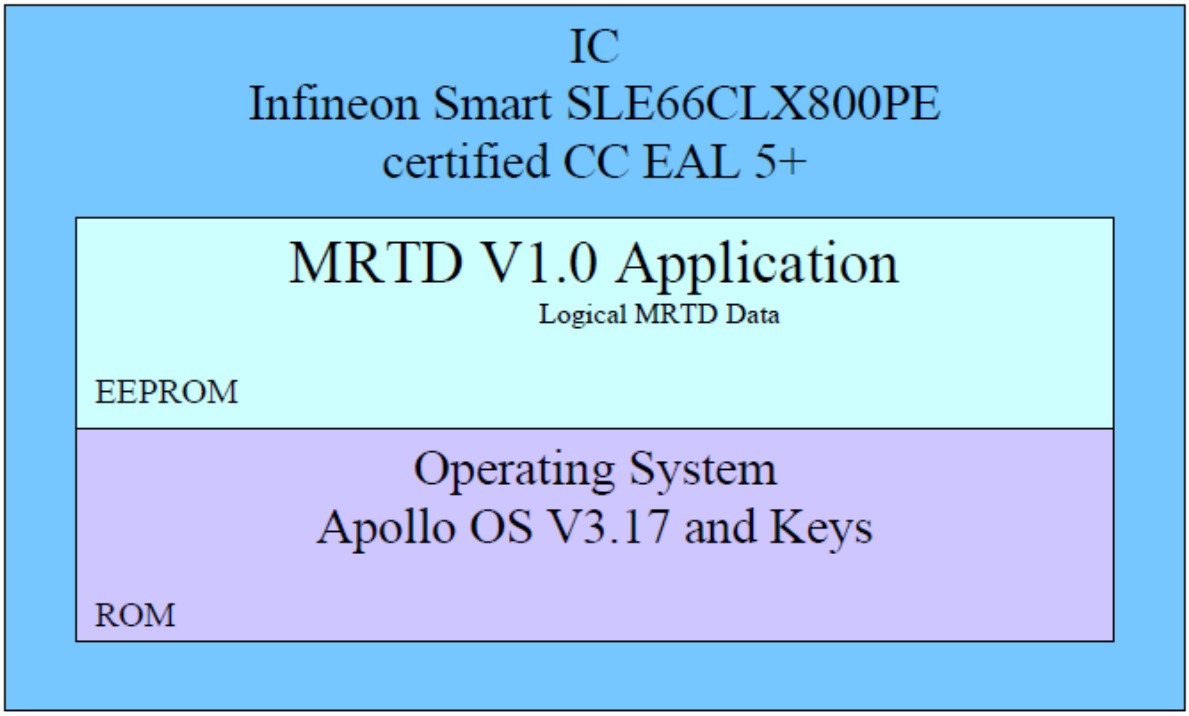

図1-1　TOE構成図

具体的には、TOEは上図のICチップ（Infineon Smart SLE66CLX800PE）と、その上で稼動するEEPROM上のMRTD V1.0 Application及びROMのOperating System Apollo OS V3.17により構成される。ICチップは2007年1月に、本案件担当評価機関（TÜV Informationstechnik GmbH, Evaluation Body for IT-Security）により評価済みである。

TOEは、Inspection Systemから発行されたコマンドに対し、所定の条件（認証

成功等）が満たされれば要求されたレスポンスを返す動作をするデバイスである。例えばInspection SystemがLDS内のデータを読み込む際は、Read Binaryコマンドをに対して発行し、は認証が既に成功していればLDS内のデータをそのレスポンスとして返す。本は非接触チップのため、コマンド及びレスポンスは無線データとしてとInspection System間でやり取りされる。

1.2.4 の機能

の主要機能は、LDS内のデータへのアクセス機能である。LDSにはPersonalizationの際には氏名、国籍、顔写真等の個人データが書き込まれ、審査時においてはそれらデータによる本人確認が実施される。また当然のことながらデータアクセスに付随するアクセス制御機能もの主要機能の一つといえる。

またMRTDという性質を鑑みれば、旅券の変造・偽造防止、或いは無線経由での許可ないデータ抜き取りやスキミングといった脅威に対抗する必要がある。従ってそれら脅威を防御するセキュリティ仕様がICAOで規定されており、一つはPassive Authenticationと呼ばれるLDSに保存されたデータの完全性を保証する仕組みであり、具体的にはLDSのデータのハッシュに電子署名したもの（Document Security Object）をチップ側に保存し、Inspection System側でそのハッシュを検証することによりデータの完全性を保証する仕組みである。従ってPassive Authenticationのうちハッシュによりデータの完全性を検証する部分はInspection System側で実装されるセキュリティ機能だが、Personalization時のハッシュ自体の書込み制御等はのセキュリティ機能である（上記アクセス制御機能に相当）。もう一つがスキミングを防止するBasic Access Controlであり、これはTOE側で実装されるメインのセキュリティ機能である。Basic Access Controlの詳細に関しては、「1.5.4 セキュリティ機能」を参照されたい。

1.3 評価の実施

認証機関が運営するITセキュリティ評価･認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本のセキュリティ設計が適切であること。
② 本のセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
③ 本がセキュリティ設計に基づいて開発されていること。
④ 上記①、②、③を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「Security Targets For Apollo OS e-Passport V1.0」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発･製造･出荷の現場を調査し、本TOEがCCパート1 ([5][8][11]のいずれか) 附属書B、CCパート2（[6][9][12]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「EVALUATION TECHNICAL REPORT(ETR)」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。また、コンポジット評価やスマートカード特有の評価に関する規定、或いはCEMを規定されていない保証コンポーネントに関する評価手法に関しては、サポート文書群（[19][20][21][22][23][24][25][26][27][28][29][30][31]のいずれか）に準拠する。

1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成21年7月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

1.5 報告概要

1.5.1 PP適合

適合するPPは[32]を参照の事。

1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL4追加である。
追加の保証コンポーネントは、ADV_IMP.2、ALC_DVS.2である。

1.5.3 セキュリティ機能強度

STは、最小機能強度として、“ SOF-高位 ” を主張する。
本TOEは、偽造される危険性の高い旅券に組み込まれることを考慮すれば、セキュリティ機能強度は攻撃者の能力を考えSOF-高位である必要がある。

1.5.4 セキュリティ機能

本TOEの主要なセキュリティ機能は、前述した通りデータへのアクセス制御機能とBasic Access Controlである。

Basic Access Controlとは、まずMRZをベースにシードを生成後セッション鍵及び認証鍵を生成し、セッション鍵による通信の暗号化・認証鍵による通信の完全性の保証を行う、所謂スマートカードにおけるセキュアメッセージング機能である。従ってBasic Access Controlは下記のSF.Cryptographic Support機能やSF.Identification and Authentication機能により実現される。またInspection System側の機能に応じBasic Access ControlをEnable/Disableすることが出来るが、そのような管理を提供するSF.Security Management機能もTOEセキュリティ機能である。またデータアクセス制御機能は下記のSF.User Data Protection機能に相当し、それ以外にもTOEは物理的な攻撃を検知してリセットするなどの自己保護をSF.Protection機能により実現している。

表1-1　TOEセキュリティ機能

TOEセキュリティ機能	概要
SF.Cryptographic Support	暗号鍵生成・破棄やTriple DESによる暗号化、乱数生成等の暗号化機能。
SF.Identification and Authentication	Basic Access Controlを利用した端末認証やBasic Access Control時でReplay防止、Personalization Agentの認証等の識別認証に関わる機能。
SF.User Data Protection	Personalization AgentにのみLDSデータ書込みを許可し、それ以外は読込みのみ許可する等LDSデータの保護機能。
SF.Security Management	Basic Access Controlの Enable/Disable を Personalization Agentにのみ許可する等のセキュリティ管理機能。
SF.Protection	電圧や温度センターによる物理攻撃の検知等の保護機能やバイパス防止機能等のTSF保護機能。

1.5.5 脅威

本TOEは、表1-2に示す脅威を想定し、これに対抗する機能を備える。

表1-2　想定する脅威

識別子	脅　威
T.Chip_ID	**Identification of MRTD's chip**

	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** 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** 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. 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** 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** An attacker may use functions of the TOE which shall not be used in TOE operational phase in order i. to manipulate User Data, ii. to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or iii. to disclose or to manipulate TSF Data. 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** 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** An attacker may perform physical probing of the MRTD's chip in order i. to disclose TSF Data, or ii. to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to i. modify security features or functions of the MRTD's chip, ii. modify security functions of the MRTD's chip Embedded Software, iii. to modify User Data or iv. to modify TSF data. 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. 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** An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying

	environmental stress in order to i. deactivate or modify security features or functions of the TOE or ii. Circumvent or deactivate or modify security functions of the MRTD's chip Embedded Software. 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 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表1-3に示す。

表1-3 組織のセキュリティ方針

識別子	組織のセキュリティ方針
P.Manufact	**Manufacturing of the MRTD's chip** 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. * TOEのLifecycleはPhase1のDevelopment（ICチップ及びソフトウェアを個別に作成）、Phase2のManufacturing（ICチップへソフトウェアをロード)、Phase3のPersonalization（所有者の本人情報の書込み)、Phase4のOperational Use（所有者へMRTDを受け渡し）にフェーズわけされる。
P.Personalization	**Personalization of the MRTD by issuing State or Organization only** 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** 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 i. to enable the Basic Access Control for the protection of the MRTD holder personal data or 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 構成条件

TOEと通信するInspection Systemには、Basic Access Controlに対応していないPrimary Inspection SystemとBasic Access Control対応のBasic Inspection Systemが存在する。TOEをPrimary Inspection System環境で使用するためにはBasic Access ControlをDisableに構成する必要があり、Basic Inspection System環境ではBasic Access ControlをEnableに構成する必要がある。

1.5.8 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-4に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

表1-4　TOE使用の前提条件

識別子	前提条件
A.PERS_AGENT	PERSONALIZATION OF THE MRTD'S CHIP The Personalization Agent ensures the correctness of i. the logical MRTD with respect to the MRTD holder, ii. the Document Basic Access Keys, iii. the Active Authentication Public Key Info (DG15) if stored on the MRTD's chip, and iv. The Document Signer Public Key Certificate (if stored on the MRTD's chip). 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 The Inspection System is used by the border control officer of the receiving State i. examining an MRTD presented by the traveller and verifying its authenticity and 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. The TOE allows the Personalization agent to disable the Basic Access Control for use with Primary Inspection Systems.

1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す（ICチップ付属の添付ドキュメントはICチップ（Infineon Smart SLE66CLX800PE）の認証書[32]参照の事）。

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 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成20年3月に始まり、平成21年7月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成20年6月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付と運用・ライフサイクルの各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成21年3月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストの環境は以下の通りである。

- Personal PC with windows XP, 2000.

- PC card readers

o Contactless reader ACG – Dual 2.2

o Contactless reader Microprоss- 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) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a. テスト構成

開発者が実施したテストの構成は上記1)の通り。開発者テストはTOEとコンタクトレスリーダ、或いはデバッガを用い実施された。

b. テスト手法

テストには、以下の手法が使用された。

①コンタクトレスリーダから自動スクリプトにより一連のコマンド実行し、そのレスポンスをログファイルに記録後、期待される結果と比較する

②デバッガを用い逐次メモリの内容を参照し、期待される結果と比較しながらテストを実施

c. 実施テストの範囲

テストは開発者によって53項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。深さ分析が実施され、上位レベル設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証されている。

d. 結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成は、2.3.1 1)に示した開発者テストと同様の構成である。但し1つの侵入テスト（Alpha fault injection test）においては開発者テストで使用されていないAlpha radiatorを用いた以下の構成においてテストを実施している。

・Personal Computer with Windows XP

・Contactless reader SCM SDI 010

・Alpha radiator

o Ra-226-isotope

o activity 3,3 kBq

o isotope-holder: aluminium bar (ø 10 mm)

o exhaust port ø 3 mm

o installation depth 3 mm

・DPA_FI (Software)

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a. テスト構成

評価者テストは開発者同様TOEとコンタクトレスリーダ、或いはデバッガを用い実施された。上記1)で示したAlpha radiatorも使用し一部のテストを実施している。

b. テスト手法

テストには、以下の手法が使用された。

①コンタクトレスリーダから自動スクリプトにより一連のコマンド実行し、そのレスポンスをログファイルに記録後、期待される結果と比較する

②デバッガを用い逐次メモリの内容を参照し、期待される結果と比較しながらテストを実施

③Alpha radiatorを使用しAlpha粒子を放射したFault Injectionテスト

c. 実施テストの範囲

評価者が独自に考案したテストを30項目（評価者独立テスト17項目、侵入テスト13項目）、開発者テストのサンプリングによるテストを53項目、計83項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① 開発者が実施した全テスト（53項目）の追試

② 評価者独立テストにおいては全てのセキュリティ機能をカバーするようテスト項目を選択

③ 侵入テストにおいては、CCサポート文書[27]、[28]及びCEMの記述より、攻撃シナリオを特定しテスト項目を選択

d. 結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

2.4 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

3 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 当該所見報告書でなされた指摘内容が妥当であること。
② 当該所見報告書でなされた指摘内容が正しく反映されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、ST及び評価報告書において、所見報告書及び認証レビューで指摘された問題点が解決されていることを確認した。

4 結論

4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL4及び保証コンポーネントADV_IMP.2、ALC_DVS.2に対する保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1 評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE識別、境界の記述が明瞭であることを確認している。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。

ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件のいずれかへ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、STにおいてPPが識別されSFRの操作がPPと適合していることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張がPPを正確に具象化したものであることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、STに定義された拡張機能要件が曖昧なく定義されていることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、STに定義された拡張機能要件の依存性が全て識別されていることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。

ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された**
ACM_AUT.1.1E	評価はワークユニットに沿って行われ、CMシステムが人為的誤りまたは怠慢による影響を受けないように、実装表現に対する変更が自動化ツールのサポートにより制御されていることを確認している。
ACM_AUT.1.1D	評価はワークユニットに沿って行われ、CM計画に記述されている自動化ツールと手順が使用されていることを確認している。
ACM_CAP.4.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
ACM_SCP.2.1E	評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んでいることを確認している。
配付と運用	**適切な評価が実施された**
ADO_DEL.2.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
ADO_DEL.2.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
開発	**適切な評価が実施された**

ADV_FSP.2.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。
ADV_FSP.2.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。
ADV_HLD.2.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのハードウェア、ソフトウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。
ADV_HLD.2.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_IMP.2.1E	評価はワークユニットに沿って行われ、実装表現がTSFを作成できる詳細レベルでTSFを明確に定義していること、開発者の提供した実装表現が十分足るものであること、それが内部的に一貫していることを確認している。
ADV_IMP.2.2E	評価はワークユニットに沿って行われ、実装表現がその関連するTOEセキュリティ機能要件を正しく具体化したものであることを確認している。
ADV_LLD.1.1E	評価はワークユニットに沿って行われ、下位レベル設計が必要な説明情報を含み、内部的に一貫していること、モジュールの観点から記述されており、各モジュールの目的を記述していること、提供されるセキュリティ機能という観点でモジュール間の相互関係と依存性を定義していること、TSP実施機能の提供方法を記述していること、TSFモジュールのインタフェースと外部インタフェースを識別していること、各モジュールの使用法と目的を記述していること、そしてTSP実施モジュールとその他に区別できることを確認している。

ADV_LLD.1.2E	評価はワークユニットに沿って行われ、下位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であり、下位レベル設計が上位レベル設計の正しく完全な表現であることを、それらの対応分析により確認している。
ADV_SPM.1.1E	評価はワークユニットに沿って行われ、セキュリティ方針モデルが非形式的でありSTにおいて明示的方針をもたないこと、ST中のセキュリティ機能要件で表されたすべてのセキュリティ方針がモデル化されていること、セキュリティ方針モデルの規則や特性がモデル化されたTOEのセキュリティふるまいを明確に表していること、モデル化されたふるまいがセキュリティ方針と一貫し完全であること、セキュリティ方針を実装している機能仕様にてすべてのセキュリティ機能を識別していること、機能仕様の内容とセキュリティ方針モデルの実装として識別された機能の内容が一貫していることを確認している。
ガイダンス文書	**適切な評価が実施された**
AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
ライフサイクルサポート	**適切な評価が実施された**

ALC_DVS.2.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。
ALC_DVS.2.2E	評価はワークユニットに沿って行われ、ALC_DVS.2.1Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。
ALC_LCD.1.1E	評価はワークユニットに沿って行われ、使用されたライフサイクルモデルが開発者と保守手続きをカバーしており、その記述にある手続き、ツール、技法の使用が開発と保守に貢献していることを確認している。
ALC_TAT.1.1E	評価はワークユニットに沿って行われ、開発ツール証拠資料が明確であり、実装に用いられた開発ツールのステートメント及び実装依存オプションの意図を明確に定義していることを確認している。
テスト	**適切な評価が実施された**
ATE_COV.2.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_DPT.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。

ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_MSU.2.1E	評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。
AVA_MSU.2.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.2.3E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを確認している。

AVA_MSU.2.4E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEの全ての操作モードにおいてのセキュアな操作を提供していることを確認している。
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。
AVA_VLA.2.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。
AVA_VLA.2.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。
AVA_VLA.2.3E	評価はワークユニットに沿って行われ、開発者がまだ扱っていない脆弱性の可能性を検査している。
AVA_VLA.2.4E	評価はワークユニットに沿って行われ、独立脆弱性分析に基づく侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテストの概要について報告がなされている。
AVA_VLA.2.5E	評価はワークユニットに沿って行われ、意図する環境においてTOEが低い攻撃力に対抗できることを侵入テストと脆弱性分析の結果から検査し、悪用され得る脆弱性及び残存脆弱性が存在しないことが報告されている。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

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

本報告書で使用されたTOE特有の略語を以下に示す。

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

本報告書で使用された用語を以下に示す。

Active Authentication	ICAOにより規定された、MRTDのチップが真正であることをInspection Systemが検証するメカニズム。
Alpha fault injection	Alpha粒子を放射することにより故障を発生させ、セキュリティ上の不具合が発生しないか検査するテスト。
Basic Access Control	ICAOにより規定された、スキミングを防止するためのセキュアメッセージング機能。
Basic Inspection System	Basic Access Controlに対応したInspection System。Basic Inspection SystemとTOE間の通信はセキュアメッセージングで保護される。
Country Signing Public Key	Document Signer Public Key Certificateの検証のために使用される公開鍵。
DEMA	Differential Electromagnetic Analysisの略称。チップから放射される電磁波を複数回測定し分析することにより、鍵等の秘密情報を推定する攻撃。

Differential Fault Analysis	電波の放射等によりチップに故障を発生させ、その故障時の振る舞いよりチップ内のロジック等を推定する攻撃。
Document Basic Access Key	Basic Access Controlのセキュアメッセージングの際に使用される鍵。MRZをシードとして生成される。
DG	Data Groupの略称。LDS内のデータ構成要素の1単位。例えばDG1にはMRZデータが、DG2には顔写真等、各DGにおいてどのようなデータが保存されるか規定されている。
Document Signer Public Key	署名されたDocument Security Objectを検証するために使用される公開鍵。
Document Signer Public Key Certificate	署名されたDocument Security Objectを検証するために使用される証明書。
DPA	Differential Power Analysisの略称。チップで消費される電流を複数回測定し分析することにより、鍵等の秘密情報を推定する攻撃。
Document Security Object	LDS内のデータのハッシュを秘密鍵により署名されたもの。ICチップ内に保存される。
ICAO	International Civil Aviation Organizationの略称。日本名称は国際民間航空機関であり、国際民間航空に関する原則と技術を開発・制定し、その健全な発達を目的とする機関であり、パスポートに関する諸規定も規定する。
Inspection System	所有者から提示されたMRTDを調査し、その内容の真正性及びそれに基づく本人確認を実施するための機器を指す。
LDS	Logical Data Structureの略称。チップ内の論理データ構造を規定。
MRTD	Machine readable travel documentの略称。公的な機関から発行され海外旅行のためにしようされる文書（所謂パスポートやビザをさす）。
MRZ	Machine Readable Zoneの略称。発行国、所有者氏名、国籍等の所有者に関する基本情報。パスポートの所定の場所に印字されるほか、チップにも同じデータが保存される。
Passive Authentication	電子署名を利用しLDS内に保存されたデータの完全性を保証するメカニズム。
Personalization	MRTD（TOE含む）に本人データが記載されることを指す。
Personalization Agent	Personalizationの作業を実行する主体。
Personalization Agent Key	Personalizationの作業者を認証するために使用される鍵。
Pre-personalization	MRTD製造者により、ICチップの不揮発性メモリに書き込ま

Data	れる情報。例えばPersonalization Agent Key等。
Primary Inspection System	Basic Access Controlに対応していないInspection System。Primary Inspection SystemとTOE間の通信はセキュアメッセージングで保護されず、平文での通信となる。
スマートカードコンポジット評価	ICチップを最初に評価し、次にその評価結果をインプットとしてチップ上で稼動するソフトウェアを評価することを指す。評価方法はCC/CEMとは別途提供されるCCサポート文書[19]に記載されている。

6 参照

[1] Security Targets For Apollo OS e-Passport V1.0 Version 1.03 14.07.2009

[2] ITセキュリティ評価及び認証制度の基本規程　平成19年5月　独立行政法人 情報処理推進機構　CCS-01

[3] ITセキュリティ認証申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン2.3 2005年8月 CCMB-2005-08-001　(平成17年12月翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能要件 バージョン2.3 2005年8月 CCMB-2005-08-002　(平成17年12月翻訳第1.0版)

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証要件 バージョン2.3 2005年8月 CCMB-2005-08-003　(平成17年12月翻訳第1.0版)

[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] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8月　(平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] EVALUATION TECHNICAL REPORT(ETR) Version 1 2009-07-16

[19] Composite product evaluation for Smart Cards and similar devices September

2007 Version 1.0 Revision 1 CCDB-2007-09-001

[20] Application Notes and Interpretation of the Scheme (AIS), AIS 1,Durchführung der Ortsbesichtigung in der Entwicklungsumgebungdes Herstellers, Version 13, 2008-08-14, Bundesamt für Sicherheit in der Informationstechnik.

[21] Application Notes and Interpretation of the Scheme (AIS), AIS 14, Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC, Version 1, 1998-11-24, Bundesamt für Sicherheit in der Informationstechnik.

[22] Application Notes and Interpretation of the Scheme (AIS), AIS 19, Gliederung des ETR, Version 1, 12.11.1998, Bundesamt für Sicherheit in der Informationstechnik.

[23] Application Notes and Interpretation of the Scheme (AIS), AIS 23, Zusammentragen von Nachweisen der Entwickler, Version 2, 2009-03-11, Bundesamt für Sicherheit in der Informationstechnik.

[24] Application Notes and Interpretation of the Scheme (AIS), AIS 31, Functionality classes and evaluation methodology for physical random number generators, Version 1, 2001-09-25, Bundesamt für Sicherheit in der Informationstechnik.

[25] Application Notes and Interpretation of the Scheme (AIS), AIS 32, Übernahme international abgestimmter CC Interpretationen ins deutsche Zertifizierungsschema, Version 1, 2001-07-02, Bundesamt für Sicherheit in der Informationstechnik.

[26] Application Notes and Interpretation of the Scheme (AIS), AIS 34, Evaluation Methodology for CC Assurance Classes for EAL5+, Version 1.4, 2008-08-14, Bundesamt für Sicherheit in der Informationstechnik.

[27] Joint Interpretation Library, Application of Attack Potential to Smartcards, Version 2.7, 2009-02, BSI, TÜViT, et. al.

[28] Joint Interpretation Library, Attack Methods for Smartcards and Similar Devices, confidential Version 1.5, 2009-02, BSI, TÜViT, et. al.

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

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

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

[32] Common Criteria Protection Profile, Machine Readable Travel Document with „ICAO Application", Basic Access Control, version: 1.0, 18 August 2005, BSI,

BSI-PP-0017

[33] 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