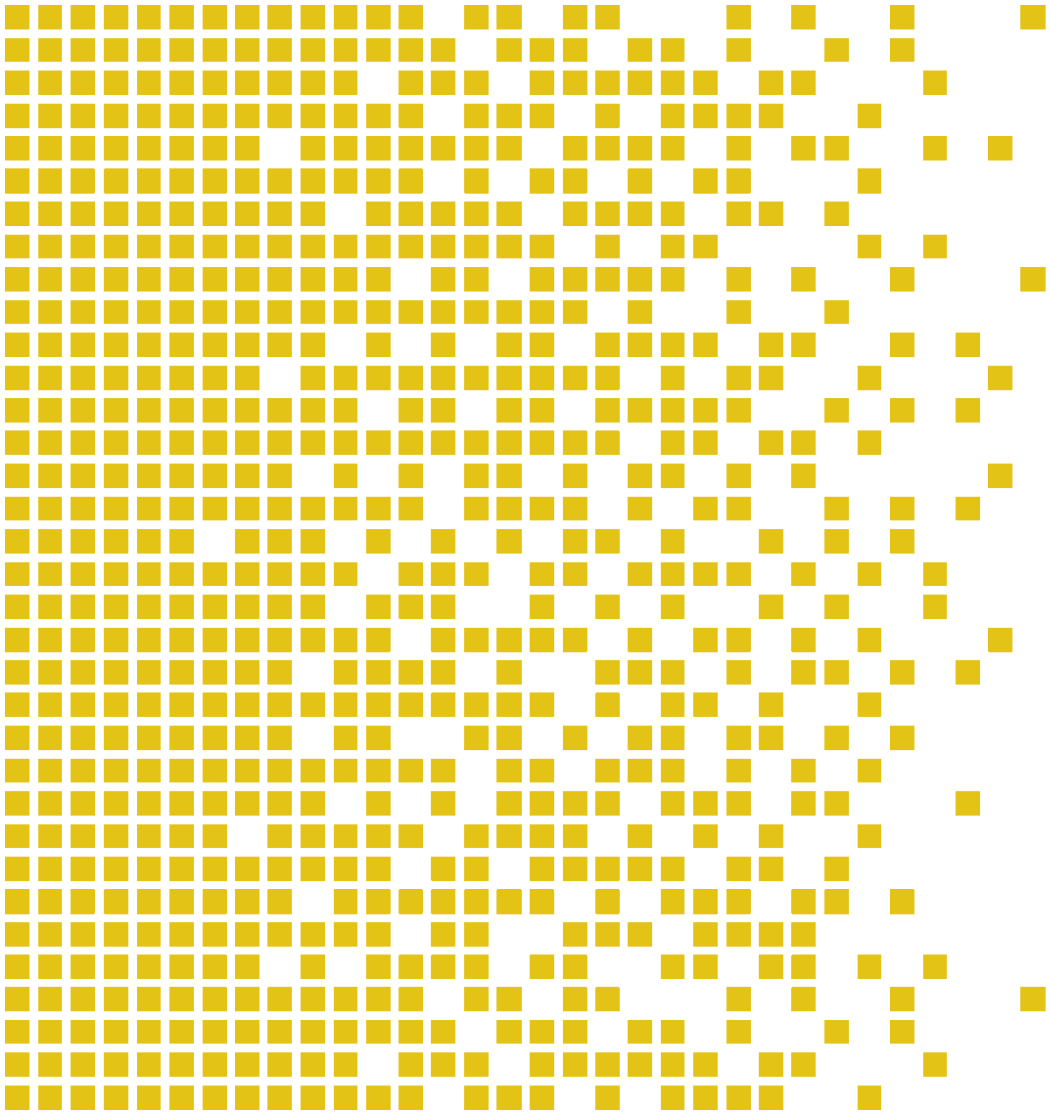
SERTIT-021 CR Certification Report

Issue 1.0 23.05.2011

Toshiba TOSMART-P080-AAJePassport version 01.06.04 + NVM Ver.01.00.00



SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. [*]

[* Mutual Recognition under the CC recognition arrangement applies to EAL 4 but not to AVA_VAN.5, ALC_DVS.2 and ASE_TSS.2.]

Contents

1 Certification Statement

TOSHIBA CORPORATION Social Infrastructure Systems Company Toshiba TOSMART-P080-AAJePassport is a The TOE is a Machine Readable Travel Document (MRTD), consisting of the hardware T6ND1, which is used as the evaluated underlying platform and the MRTD (OS and application) software, which is built on this hardware platform.

Toshiba TOSMART-P080-AAJePassport version 01.06.04 + NVM Ver.01.00.00 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 augmented with AVA_VAN.5, ALC_DVS.2 and ASE_TSS.2 for the specified Common Criteria Part 2 conformant functionality in the specified environment when running on the platforms specified in Annex A. It has also met the requirements of Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247].

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Lars Borgos Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT
Date approved	23.05.2011

2 Abbreviations

AA	Active Authentication
APDU	Application Data Unit
BAC	Basic Access Control
CC	Common Criteria for Information Technology Security Evaluation
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
ICAO	International Civil Aviation Organization
MRTD	Machine Readable Travel Document
NVM	Non Volatile Memory (=EEPROM)
PA	Passive Authentication
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
IC	Integrated Circuit

3 References

[1] TOSMART-P080-AAJePassport Security Target February 24, 2011 Public ST Version 01.00.00.

[2] Common Criteria Part 1, CCMB-2009-07-001, Version 3.1 R3, July 2009.

[3] Common Criteria Part 2, CCMB-2009-07-002, Version 3.1 R3, July 2009.

[4] Common Criteria Part 3, CCMB-2009-07-003, Version 3.1 R3, July 2009.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1 R3, July 2009.

[7] Evaluation Technical Report Common Criteria EAL4+ Evaluation of Toshiba TOSMART-P080-AAJePassport, v1.0, 22/04/2011

[8] Guidance Document for Personalization agent, v. MC-SJ0046-02

[9] Preparative guidance, v. MC-SJ0045-01

[10] Application Specification, v. MC-SM0914-02

[11] Personalization Manual, v. MC-SJ0047-03

[12] AA Personalization Manual, v. MC-SJ0048-03

[13] Authentication Manual, v. MC-SJ0049-03

[14] Authentication Manual using MUTUAL AUTHENTICATE command, v. MC-SJ0050-03

[15] Authentication Manual using BAC, v. MC-SJ0051-03

[16] Personalization Specification, v. MC-SM0812-03

[17] Procedural Request of Security Products Delivery and Receipt, v. MB-ICCARD-W471

[18] Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247]

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Toshiba TOSMART-P080-AAJePassport version 01.06.04 + NVM Ver.01.00.00 to the Sponsor, TOSHIBA CORPORATION Social Infrastructure Systems Company, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was Toshiba TOSMART-P080-AAJePassport and version 01.06.04 + NVM Ver.01.00.00.

This product is also described in this report as the Target of Evaluation (TOE). The developer was TOSHIBA CORPORATION Social Infrastructure Systems Company.

The TOE is a composite security IC, consisting of the hardware T6ND1, which is used as the evaluated underlying platform and the Machine Readable Travel Document (OS and application) software, which is built on this hardware platform. The T6ND1 is a secure single chip microcontroller with a RF type communication interface compliant to ISO-14443 type B. It consists of a central processing unit (CPU), memory elements (ROM, RAM, NV memory), and circuitry for the RF external interface that have been integrated with consideration given to tamper resistance. The software that is incorporated in the memory element is capable of providing security functions for the Machine Readable Travel Document (MRTD)

The MRTD consists of a secure operating system and application on top of the T6ND1. The operating system contains the embedded software functions used by the MRTD application.

The MRTD application provides Active Authentication, Basic Access Control, and facilitates Passive Authentication. The TOE consists of the security functions: Memory access control, Sensitive data with CRC checksum, encrypted key data on NVM.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

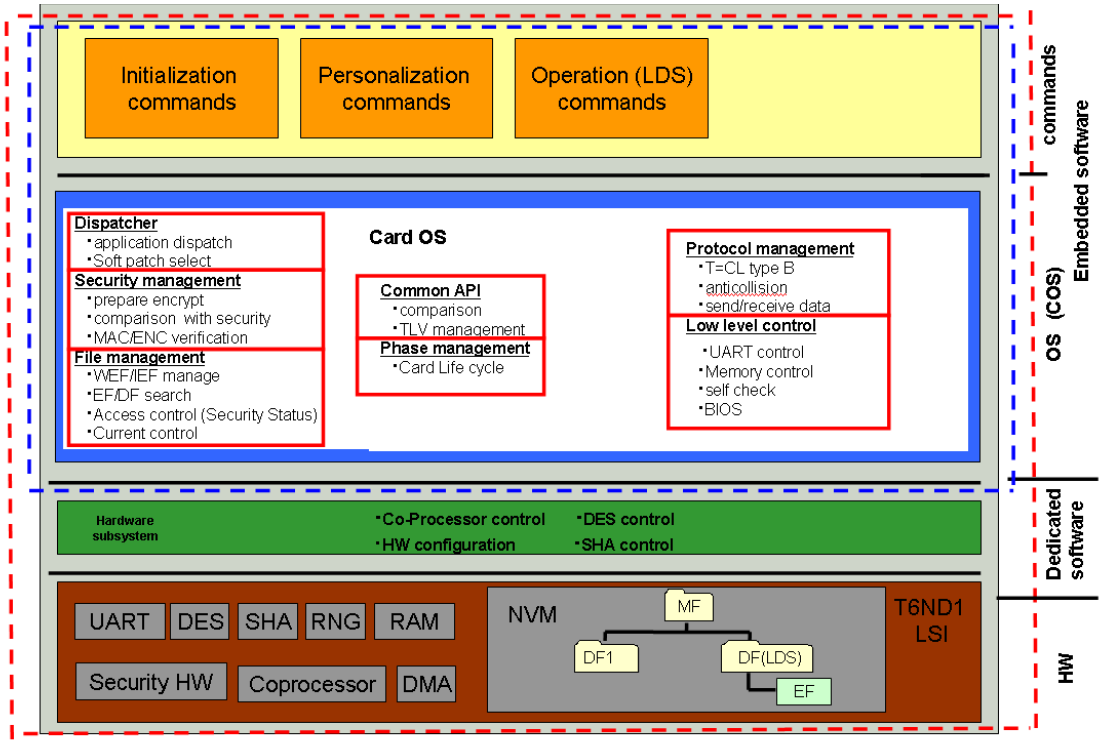
The TOE is a composite product comprising an integrated circuit (IC) and an ePassport application with a card operating system.

The IC, Toshiba T6ND1 is a secure single chip micro controller with a RF type communication interface compliant to ISO-14443 type B. It consists of a central processing unit (CPU), memory elements (ROM, RAM, NVM), and circuitry for the RF

external interface. The IC enables that embedded software can run securely. The T6ND1 is compliant to the IC platform protection profile [PP-0035].

The ePassport application with the operating system form the Machine Readable Travel Document (MRTD). The MRTD application provides Active Authentication (AA), Basic Access Control (BAC), and facilitates Passive Authentication (PA). The TOE consists of the security functions: Memory access control, Sensitive data with CRC checksum, encrypted key data on Non Volatile Memory (=EEPROM). The TOE follows the international guidelines of ICAO for MRTD as defined in [ICAO_9303].

The figure below presents the TOE. The red line denotes the composite TOE boundary. The blue line denotes the part that was added on the T6ND1.



Architectural view on the TOE

Logically the TOE consists of the following subsystems:

1. The Card OS, providing services to the applications with the subsystems:
    a. Protocol management, which handles the ISO14443 type B T=CL protocol, sends the REQB, sets up the communication protocol as defined in ISO14443, and contains the functionality to send/receive APDUs handling management;
    b. Dispatcher, which transfers the control to the application and provides soft patching functionality to that application;
    c. Low level control, a set of modules that directly control hardware registers.

   d. File management, which provides ISO file system primitives (MF, DFs, EFs with write and read operations) to applications;
   e. Phase management, which checks the card life cycle management data in NV memory and sets a phase flag in RAM;
   f. Security management, consisting of general routines with security services, such as comparison with security flags;
   g. Common API, containing general routines (without specific security services);
2. The Initialisation commands subsystem, containing the APDU commands only used in the manufacturing phase;
3. The Personalization commands subsystem, containing the ADPU commands only used in the personalization phase;
4. The Operation (LDS) commands subsystem, containing the remaining APDU commands.

4.4 Protection Profile Conformance

The Security Target[1] claimed conformance to the protection profile:

Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247]

4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL4 augmented with AVA_VAN.5, ALC_DVS.2 and ASE_TSS.2. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

The TOE security policies are detailed in Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247], the Organisational Security Policies defined in section 3.2 of the Protection Profile are valid for this TOE.

4.7 Security Claims

The Security Target[1] and the PP [18] fully specifies the TOE's security objectives, the threats, Organisational security Policies which these objectives meet and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

The threats countered by the TOE are detailed in Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247].

4.9 Threats Countered by the TOE's environment

The threats countered by the TOE's environment are detailed in Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247].

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

The environmental assumptions and dependencies are detailed in Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247].

4.12 IT Security Objectives

The TOE security objectives are detailed in Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247], the Security Objectives for the TOE defined in section 4.1 of the Protection Profile are valid for this TOE.

4.13 Non-IT Security Objectives

The Non-IT TOE security objectives are detailed in Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247], the Security Objectives for the operational environment defined in section 4.2 of the Protection Profile are valid for this TOE.

4.14 Security Functional Requirements

The security functional requirements are detailed in Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247], Security Functional Requirements in section 6.1 of the Protection Profile are valid for this TOE.

4.15 Security Function Policy

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical MRTD, Active Authentication of the MRTD's chip to and the Data Encryption of sensitive biometrics as optional security measure in the ICAO DOC 9303[ICAO_9303]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently of the TOE by the TOE environment.

The security target addresses the protection of the logical MRTD

- in integrity by write-only-once access control and by physical means, and
- in confidentiality by the Basic Access Control Mechanism

The Security Target addresses the optional Active Authentication stated in [ICAO_9303]

The TOE implements Basic Access Control. The inspection system

- reads optically the MTRD
- Authenticates itself as an inspection system by means of Document Access Keys.
- An access control by the TOE to allow reading data (except for the sensitive biometric data) only to successfully authenticated authorized inspection systems

The TOE also optionally implements Active Authentication (described in [ICAO_9303]). By means of a challenge-response protocol between the inspection system and the TOE, is ensured that the chip has not been cloned. For this purpose the TOE contains its own Active Authentication RSA key pair. A hash representation of Data Group 15 Public key is stored in the Document Security Object (SOD) and therefore authenticated by the issuer's digital signature. The corresponding Private Key is kept in the TOE's secure memory and never disclosed.

The following functionality is provided by the software building upon what was already provided by the hardware on which the software builds.

In addition to the T6ND1 hardware platform and crypto library, the TOE-Software implements a file system and the functionality as described in section4.14, furthermore it implements functionality that protects the data in files and uses the data stored in files.

The TOE Software satisfies the following requirements of the underlying certified hardware platform T6ND1 and crypto library.

- Destruction of the cryptographic keys after usage
- Implementation of the T6ND1 user guidance with respect to:
  - Enabling the hardware countermeasures
  - Anti-perturbation countermeasures

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first evaluated itself. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Brightsight B.V. Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the

EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT 22.04.2011. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 4 assurance package augmented with AVA_VAN.5, ALC_DVS.2 and ASE_TSS.2.

Assurance class	Assurance components	
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
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
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_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
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.2	TOE summary specification with architectural design summary
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

Following [PP-C0247], the TOE delivery occurs after phase 2 (or before phase 3), as an inlay and sheeted product transport key locked. The TOE is in its evaluated configuration after the card lifecycle state has been set to "Operation", i.e. after phase 3(or before phase 4).

5.3 Installation and Guidance Documentation

The Preparative guidance[9] gives the procedures necessary for the secure installation of the TOE and the secure preparation of the operational environment are in accordance with the ST.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Administrators should follow the guidance[8][9][11][12] for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively administer and use the TOE's security functions.

5.5 Vulnerability Analysis

The evaluators' assessment of potential exploitable vulnerabilities in the TOE has been addressed and shows that the vulnerability analysis is complete, and that the TOE in its intended environment is resistant to attackers with a high attack potential.

5.6 Developer's Tests

The evaluators' assessments of the developers' tests shows that the developer testing requirements is extensive and that the TSF satisfies the TOE security functional requirements. The testing performed on the TOE by both the developer and evaluator

showed that the EAL 4 assurance components augmented with AVA_VAN.5, ALC_DVS.2 and ASE_TSS.2 are fulfilled.

5.7 Evaluators' Tests

The evaluator have independently tested the TSFs and verified that the TOE behaves as specified in the design documentation and confidence in the developer's test results is gained by performing a sample of the developer's tests.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Toshiba TOSMART-P080-AAJePassport version 01.06.04 + NVM Ver.01.00.00 running on T6ND1 meet the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 augmented with AVA_VAN.5, ALC_DVS.2 and ASE_TSS.2 for the specified Common Criteria Part 2 conformant functionality and Protection Profile for IC for ePassport - Active Authentication Support - [PP-C0247], in the specified environment, when running on the T6ND1.

6.2 Recommendations

Prospective consumers of Toshiba TOSMART-P080-AAJePassport version 01.06.04 + NVM Ver.01.00.00 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 4.3 “TOE Scope” and Section 5 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Item	Identifier	Version
Hardware	T6ND1 Integrated Circuit	5.0
Software	TOSMART-P080-AAJePassport	Ver.01.06.04 with NVM Ver.01.00.00

TOE Documentation

The supporting guidance documents evaluated were:

Item	Identifier	Version
Manuals	Guidance Document for Personalization agent	MC-SJ0046-02
	Preparative guidance	MC-SJ0045-01
	Application Specification	MC-SM0914-02
	Personalization Manual	MC-SJ0047-03
	AA Personalization Manual	MC-SJ0048-03
	Authentication Manual	MC-SJ0049-03
	Authentication Manual using MUTUAL AUTHENTICATE command	MC-SJ0050-03
	Authentication Manual using BAC	MC-SJ0051-03
	Personalization Specification	MC-SM0812-03
	Procedural Request of Security Products Delivery and Receipt	MB-ICCARD-W471

TOE Configuration

The following configuration was used for testing:

The TOE is tested on a set-up with

- Contact less card reader
- PC with Brightsight ePassport test tool

The configuration of the TOE samples where as follows:

- Operational phase: BAC
- Operational phase and Personalization phase BAC + AA