Version 20101101

Certification Report

TOSMART-P080 Version 01.06.04 + NVM Ver.01.00.01

Sponsor and developer: ***TOSHIBA CORPORATION***
Social Infrastructure Systems Company
1-1, Shibaura 1-Chome, Minato-Ku,
Tokyo 105-8001
Japan

Evaluation facility: ***Brightsight***
Delftechpark 1
2628 XJ Delft
The Netherlands

Report number: **NSCIB-CC-10-26681-CR**

Report version: **1**

Project number: **NSCIB-CC-10-26681**

Authors(s): **NLNCSA**

Date: **June 16, 2011**

Number of pages: **16**

Number of appendices: **0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Head office Apeldoorn:
Boogschutterstraat 11A
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Eindhoven:
De Rondom 1
P.O. Box 6235
5600 HE Eindhoven
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)40 265 0 302

Location Enschede:
Josink Esweg 10
P.O. Box 337
7500 AH Enschede
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a registered company with the Amsterdam Chamber of Commerce under number 27288788
info@nl.tuv.com
www.tuv.com/nl

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 3 (ISO/IEC 15408)
Certificate number	**C11-26681**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**TOSHIBA CORPORATION Social Infrastructure Systems Company** **Located in Tokyo, Japan**
Product and assurance level	**TOSMART-P80,Version 01.06.04 + NVM Ver.01.00.01** Assurance Package: ▪ EAL4 augmented with ALC_DVS.2, ASE_TSS.2 and AVA_VAN.5 except for the Basic Access Control Mechanism. ▪ EAL4 augmented with ALC_DVS.2, ASE_TSS.2 and AVA_VAN.3 for the Basic Access Control Mechanism.
Project number	**NSCIB-CC-10-26681-CR**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 3 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 3 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 3. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity	Date of issue : **29-06-2011** Certificate expiry : **29-06-2021**

Registration number
Notified Body 0336
PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

Managing Director
TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

CONTENTS:

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products.

A part of the procedure is the technical examination (evaluation) of the product according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Recognition of the certificate

The Common Criteria Recognition Arrangement and SOG-IS logos are printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products in the technical domain of Smart cards and similar Devices. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the TOSMART-P080 Version 01.06.04 + NVM Ver.01.00.01. The developer of the TOSMART-P080 is TOSHIBA CORPORATION Social Infrastructure Systems Company located in Tokyo, Japan and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a composite security IC, consisting of the hardware T6ND1, a Toshiba Integrated Circuit with Crypto Library 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 evaluation of the TOE was therefore conducted as a composite evaluation and uses the results of the CC evaluation of the underlying Toshiba T6ND1 integrated circuit certified by NSCIB on 11 March 2011 (*[HW CERT]*). The chip is under surveillance by NSCIB and the certificate validity has been confirmed.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on June 14th 2011 with the delivery of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*. The certification was completed on June 17th 2011 with the preparation of this Certification Report. It should be noted that the certification results only apply to the specific version of the product as evaluated.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the TOSMART-P080 , the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the TOSMART-P080 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provide sufficient evidence that it meets the claimed assurance requirements for the evaluated security functionality.

The claimed assurance requirements are:

- **EAL 4 augmented by ALC_DVS.2, ASE_TSS.2 and AVA_VAN.5 for all operations except the Basic Access Control Mechanism**.
- **EAL 4 augmented by ALC_DVS.2, ASE_TSS.2 and AVA_VAN.3 for the Basic Access Control Mechanism**.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 3 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the TOSMART-P080 Version 01.06.04 + NVM Ver.01.00.01 evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the TOSMART-P080 Version 01.06.04 + NVM Version 01.00.01 from TOSHIBA CORPORATION Social Infrastructure Systems Company located in Tokyo, Japan.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Toshiba T6ND1	5
Software	MRTD + OS Version 01.06.04 + NVM Version 01.00.01	

To ensure secure usage a set of guidance documents is provided together with the TOSMART-P080. Details can be found in section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 2.3.4.

2.2 Security Policy

The TOE is a composite security IC, consisting of the hardware T6ND1, a Toshiba Integrated Circuit with Crypto Library 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 T6ND1 provide secure cryptographic services - triple DES, RSA, ECDSA signature verification, EC-Diffie-Hellman key exchange and Diffie-Hellman.

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

I. Basic Access Control

II. Active Authentication

III. Extended Access Control

and facilitates Passive Authentication.

In the personalization phase, the TOE provides four mechanisms for authentication of the personalization agent. These are

I. Authentication using the Mutual Authenticate command

II. Basic Access Control

III. Terminal Authentication

IV. Authentication

When personalizing the TOE as an EAC passport, only the Terminal Authentication protocol shall be used for authentication of the personalization agent.

The TOE consists of the security functions: Memory access control, Sensitive data with CRC checksum, encrypted key data on NVM.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

The memory access control provides functionality to protect the memory against illegal access during response data transmitting and sensitive data transporting. It uses the HW memory firewall function and it protects the TOE against fault injection attacks.

The Sensitive data with CRC checksum function provides the data integrity.

The encrypted key data on NVM is one of the file management functions and useful to store the data confidentiality.

Other security features of the TOE are:

- The sensitive flag is verified by CRC
- The special comparison time-constant function
- The double processing (for the sensitive process)
- Write the data with atomic transaction for the sensitive process
- The Software random wait
- Checking the ROM CRC
- The Self-diagnose for HW (Coprocessor, HW-DES, RNG) before using it
- Clear or randomize the temporary data after cryptographic processes
- Protection of integrity by write only once access control

And there are security features of the HW below, these are direct copy from [ST-HW].

Detection for:

- *trap latch (light sensor)*
- *power supply glitch*
- *clock frequency, out of the range*
- *internal/rectified supply and current, out of the range*
- *temperature, out of the range*
- *signal line error*
- *illegal access to the memories*
- *illegal configuration on test mode*
- *undefined instruction to CPU or co-processor*
- *access to vacant addresses*
- *active shield error*

Countermeasures for physical probing to the TSF:

- *bus scrambling*
- *memory address scrambling*
- *memory ciphering*
- *active shield*

For cryptographic functions, the TOE provides only cryptographic operational mechanisms. Key management shall be performed by "the security IC Embedded software" (an application program on the TOE).

The TOE is designed for use as MRTD. The issuing State or Organization has issued the MRTD to the holder to be used for international travel. The intended environment is at inspection systems where the

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

holder presents the MRTD to prove his or her identity. Therefore limited control can be applied to the MRTD and the card operational environment.

The TOE does not require non-TOE hardware, software or firmware to operate. However, it is noted that the TOE needs proper set up public key infrastructure to operate. The issuing and receiving States and Organizations are responsible for setting up this infrastructure.

2.3 Assumptions and Clarification of Scope

2.3.1 Usage assumptions

There are no usage assumptions identified in the Security Target that are of relevance to the TOE.

2.3.2 Environmental assumptions

The Security Target claims conformance to *[PP-0055]* and *[PP-0056]*. Therefore the assumptions defined in section 3.2 of the Protection Profiles are valid. The following table lists the assumptions of both Protection Profiles.

Assumptions	Titles
A.MRTD_Manufact	MRTD manufacturing on steps 4 to 6
A.MRTD_Delivery	MRTD delivery during steps 4 to 6
A.Pers_Agent	Personalization of the MRTD's chip
A.Insp_Sys	Inspection System for Global Interoperability
A.BAC_Keys	Cryptographic quality of Basic Access Control Keys
A.Signature_PKI	PKI for Passive Authentication
A.Auth_PKI	PKI for Inspection Systems

The Organisational Security Policies defined in section 3.4 of *[PP-0055]* and *[PP-0056]* are valid for the Security Target. The following table lists the Organisational Security Policies of the Protection Profiles.

OSP	Titles
P.BAC-PP ([PP-0056] only)	Fulfilment of the Basic Access Control Protection Profile
P.Sensitive_data ([PP-0056] only)	Privacy of sensitive biometric reference data
P.Manufact	Manufacturing of the MRTD's chip
P.Personalization	Personalization of the MRTD by issuing State or Organization only
P.Personal_data ([PP-0055] only)	Personal data protection policy

The additional Organisation Security Policies because of optional active authentication are:

P.Pers_Agent_Active_Authentication - Personalization of the MRTD's chip including Active Authentication

The Personalization Agent ensures the correctness of the Active Authentication Public Key if stored on the MRTD's chip. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by using the Personalization keys.

P.Insp_Sys_Active_Auth - Inspection systems for global interoperability supporting Active Authentication.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

The Extended Inspection Systems in addition may also support the terminal part of the Active Authentication protocol. Active authentication is optional and can be enabled or disabled by the manufacturer.

2.3.3 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The physical TOE is considered to be the IC with embedded software without the antenna. The following figure describes the physical scope of the IC and software of the TOE:

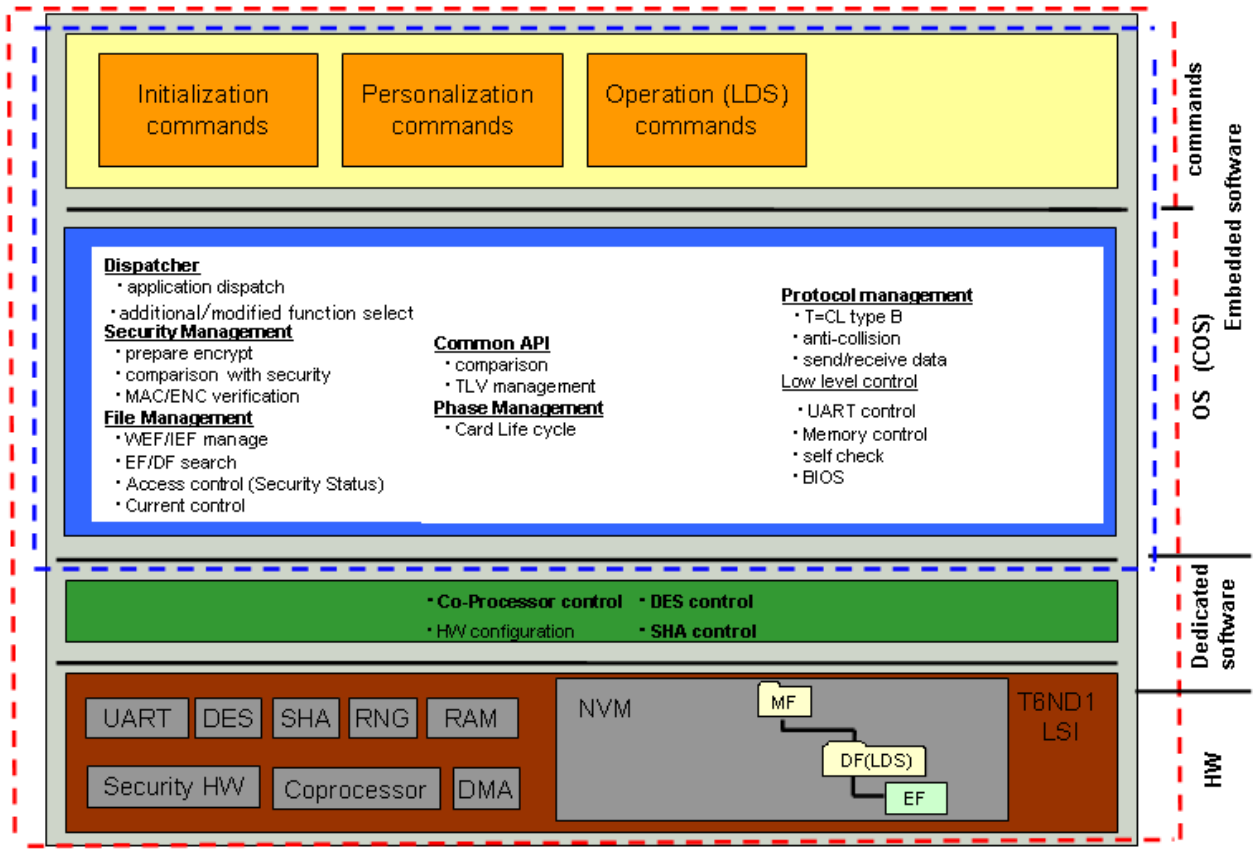

Figure 1 TOE scope (marked by red dashed line) and part additional to hardware (marked by blue dashed line)

The MRTD (OS and ePassport application) consists of a binary package that is implemented in the User ROM of the T6ND1. It can be divided in two layers, namely the OS providing a number of services to the other layer the application with commands.

The T6ND1 provides the computing platform and cryptographic support by means of co-processors and crypto library for the ePassport (OS and application) dedicated software. The T6ND1 Security Target describes the features as detectors, sensors and circuitry to protect the TOE of this hardware platform. These also apply to the composite TOE.

The antenna and capacitors for the RF interface are not part of the T6ND1 hardware. Paragraph 34 of the PP *[PP-0056]* states the following with respect to these items:

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete MRTD, nevertheless these parts are not inevitable for the secure operation of the TOE.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer (the personalization agent):

Identifier	Version
Guidance Document for Personalization agent	MC-SJ0046-06
Preparative guidance	MC-SJ0045-02
Application Specification	MC-SM0914-05
Personalization Manual	MC-SJ0047-05
AA Personalization Manual	MC-SJ0048-05
Authentication Manual using asymmetric command	MC-SJ0049-05
Authentication Manual using MUTUAL AUTHENTICATE command	MC-SJ0050-05
Authentication Manual using BAC	MC-SJ0051-05
Authentication Manual using TA	MC-SJ0100-02
Personalization Specification	MC-SM0812-04
Procedural Request of Security Products Delivery and Receipt	MB-ICCARD-W471

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

Developer Testing approach

Tests are defined for each of the Manufacturing, Personalization and Operational phases. For each TSFI (APDU) a test is defined consisting of a series of subtests. Tests on the TOE are categorized in four categories namely unit tests, integration tests and system tests. In addition TOE tests, a combination of integration test and system test are performed by the developer. The tests are performed in this order.

- *Unit tests test* software modules using a symbolic debugger. The Unit tests execute on a breadboard emulator connected to a debugger. The Debugger consists of a hardware emulation pod, controller and Integrated Development Environment (IDE) software on PC.
- *Integration tests* test TOE functionality from tests for APDU commands and focus on combination of groups of modules. The tests are for simple protocol functions (called 'scenarios'). During development the integration tests are performed on an emulator not connected to a debugger in which the ROM image can be loaded into IRAM and executed.
- *System tests* are focused on the correct operation of the software w.r.t. ISO 14443, i.e. the contactless communication protocol and anti-collision sequences are tested..
- *TOE test.* This is same test as combine of integration test and system test. The Integration and System test specification are reused for all tests except debugger test. The certified TOE is tested by APDU command and response.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

The TOE is tested in total in 5 configuration types in 15 test configurations.

The developer tests are performed from TSFI up to module level. Tests relate to the top module of a module call graph and SFR-enforcing module.

Evaluator Testing approach

The testing effort focused on the complete set of APDUs as expressed by [ICAO_9303].

The testing approach consisted of the following:

1. Repeat part of the developer's tests in such way that each of the TSFI available in the personalization and operational phases was tested.
2. The tests were performed in different configurations: five configurations for the personalization phase and nine configurations for the operation phase.
3. In addition to the developer's tests, the correct handling of the Chip Authentication, Active Authentication, and Terminal Authentication protocols by the TOSMART-P080 were tested.

Testing samples in different configurations were used. For the operational phase, nine different configurations and five different configurations for the personalization phase. For each configuration, personalisation details are provided as well to be used for correct authentication.

2.6.2 Independent Penetration Testing

The evaluators performed tests to determine whether the TOE's authentication and access control mechanism could be circumvented by light manipulation. The evaluators also created an attack rating table that represented the minimum number of points that the evaluator viewed for this attack. In total more than 10 samples were used.

2.6.3 Test Configuration

The test configuration for the independent evaluator testing consisted of a PC with test software, connected to a contactless reader. The following are details of the set-up:

- A PC running Windows 2000;
- A Java tool developed within Brightsight that allows for scriptable communication with cards;
- A Contactless card reader, developed by Brightsight, with identification HH-RF-CARDREADER 1.

The penetration testing configuration consisted of a dedicated Light manipulation set-up for contactless cards consisting of a function generator (laser trigger, clock, cold reset), power supply, oscilloscope, XY-stage and contactless reader. The evaluators used both samples in the personalisation mode and operational mode.

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its ST and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number as the TOSMART-P080 Version 01.06.04 + NVM Ver.01.00.01 and can be identified by following the instructions in the user guidance.

The TOE is tested by the developer during the Manufacturing, Personalization and Operational life-cycle phases. The TOE was tested by the evaluator in the Personalization and Operational life-cycle phases.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references several Intermediate Reports and other evaluator documents. The verdict of each claimed assurance requirement is given in the following tables:

Development		**Pass**
Security architecture	ADV_ARC.1	Pass
Functional specification	ADV_FSP.4	Pass
Implementation representation	ADV_IMP.1	Pass
TOE design	ADV_TDS.3	Pass

Guidance documents		**Pass**
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass

Life-cycle support		**Pass**
Configuration Management capabilities	ALC_CMC.4	Pass
Configuration Management scope	ALC_CMS.4	Pass
Delivery	ALC_DEL.1	Pass
Development security	ALC_DVS.2	Pass
Life-cycle definition	ALC_LCD.1	Pass
Tools and techniques	ALC_TAT.1	Pass

Security Target		**Pass**
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.2	Pass

Tests		**Pass**
Coverage	ATE_COV.2	Pass
Depth	ATE_DPT.1	Pass
Functional tests	ATE_FUN.1	Pass
Independent testing	ATE_IND.2	Pass

Vulnerability assessment		**Pass**
Vulnerability analysis	AVA_VAN.5	Pass
Vulnerability Analysis (BAC mechanism)	AVA_VAN.3	Pass

[2] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Based on the above evaluation results the evaluation lab concluded the TOSMART-P080 Version 01.06.04 + NVM Ver.01.00.01, to be **CC Part 2 extended**[3]**, CC Part 3 conformant**, and to meet the requirements of:

- **EAL 4 augmented by ALC_DVS.2, ASE_TSS.2 and AVA_VAN.5 for all operations except the Basic Access Control Mechanism**.
- **EAL 4 augmented by ALC_DVS.2, ASE_TSS.2 and AVA_VAN.3 for the Basic Access Control Mechanism**.

This implies that the product satisfies the security technical requirements specified in TOSMART-P080 Security Target, version 01.00.03, May 13th 2011.

The Security Target claims strict conformance to the following protection profiles:

- Bundesamt für Sicherheit in der Informationstechnik, Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-CC-PP-0055, Version 1.10, March 25, 2009
- Bundesamt für Sicherheit in der Informationstechnik, Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-CC-PP-0056, Version 1.10, March 25, 2009

The Security Target also refers to the T6ND1 security target [ST-HW], which is compliant to the IC platform protection profile [PP-0035]. In addition to [PP-0055] and [PP-0056] security objectives for both the TOE and the environment are defined in the Security Target for the implementation of the Active Authentication protocol. This protocol is used in life-cycle phase 4 and complements the Basic and Extended Access Control mechanisms. The additional security objectives do not conflict with the security objectives defined in the two Protection Profiles.

2.9 Evaluator Comments/Recommendations

2.9.1 Obligations and hints for the developer

None.

2.9.2 Recommendations and hints for the customer

The customer must/shall follow the provided guidance documentation and meet the requirements of the environmental assumptions.

[3] The extended Security Functional Requirements are defined in [PP-0055], Chapter 4, and in [PP-0056], Chapter 4.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

3 Security Target

The TOSMART-P080 Security Target, version 01.00.03, May 13th 2011 is included here by reference. Please note that for the need of publication a public version TOSMART-P080 Security Target, version 01.00.00, May 13th 2011 *[STP]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

AA	Active Authentication
APDU	Application Data Unit
BAC	Basic Access Control
CAP	Chip Authentication Protocol
CSCA	Country Signing CA Certificate
CVCA	Country Verifying Certification Authority
DF	Dedicated File
DES	Data Encryption Standard
EAC	Extended Access Control
ECDSA	Elliptic Curve Digital Signature Algorithm
IC	Integrated Circuit
IEF	Internal Elementary File
IR	Intermediate Report
IT	Information Technology
ITSEF	IT Security Evaluation Facility
LDS	Logical Data Structure
MF	Master File
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
NSCIB	Netherlands Scheme for Certification in the area of IT Security
NVM	Non Volatile Memory (=EEPROM)
PA	Passive Authentication
PP	Protection Profile
RSA	Rivest-Shamir-Adleman Algorithm
SCP	Smart Card Platform
SM	Secure Messaging
SOD	Document Security Object
TA	Terminal Authentication
TAP	Terminal Authentication Protocol
TOE	Target of Evaluation
WEF	Working Elementary File

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[PP-0035]	EUROSMART "Security IC Platform Protection Profile", Version 1.0, June 2007.
[PP-0055]	Bundesamt für Sicherheit in der Informationstechnik, Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-CC-PP-0055, Version 1.10, March 25, 2009.
[PP-0056]	Bundesamt für Sicherheit in der Informationstechnik, Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-CC-PP-0056, Version 1.10, March 25, 2009.
[CC]	Common Criteria for Information Technology Security Evaluation, Parts I version 3.1 revision 1, and Part II and III, version 3.1 revision 3.
[CEM]	Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 3, July 2009.
[ETR]	Brightsight, Evaluation Technical Report TOSMART-P080 - EAL4+, Version 2.0, June 14th, 2011.
[ETR-HW]	Evaluation Technical Report T6ND1 series Integrated Circuit with Crypto Library Version #6.0 (T6ND1), Version 2.0, February 21st 2011.
[ICAO_9303]	ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization
[JIL]	Attack methods for Smart cards and similar devices, JIL, version 1.4, April 2008.
[NSCIB]	Nederlands Schema for Certification in the Area of IT Security, Version 1.2, 9 December 2004.
[ST]	TOSMART-P080 Security Target, version 01.00.03, May 13th 2011.
[STP]	Public sanitized version of the TOSMART-P080 Security Target, version 01.00.00, May 13th 2011.
[ST-HW]	T6ND1 Integrated Circuit with Crypto Library Security Target, Version 2.11, 12 April 2010.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.