Certification Report

TOSMART-GP1 v01.01.00 (Supporting PACE and BAC PP-0500)

Sponsor and developer:	***Toshiba Infrastructure Systems & Solutions Corporation*** **1 Komukai Toshiba-cho** **Saiwai-ku, Kawasaki** **212-8583, Japan**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2300105-01-CR**
Report version:	**1**
Project number:	NSCIB-**2300105-01**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**01 August 2025**
Number of pages:	**12**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

CONTENTS

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, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site 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 TrustCB 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 TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence 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, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, 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 or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the TOSMART-GP1 v01.01.00 (Supporting PACE and BAC PP-0500). The developer of the TOSMART-GP1 v01.01.00 (Supporting PACE and BAC PP-0500) is Toshiba Infrastructure Systems & Solutions Corporation located in Kawasaki, 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 which is used as the evaluated underlying platform and the ePassport (OS and application) software, which is built on the hardware platform. The HW is a secure single chip microcontroller with a RF type communication interface compliant to ISO-14443 type B. The software that is incorporated in the memory element is capable of providing security functions for the ePassport.

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

The ePassport application provides Active Authentication, Password Authenticated Connection Establishment, and facilitates Passive Authentication.

The TOE has been evaluated by SGS Brightsight B.V located in Delft, The Netherlands. The evaluation was completed on 01 August 2025 with the approval 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 scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the TOSMART-GP1 v01.01.00 (Supporting PACE and BAC PP-0500), 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-GP1 v01.01.00 (Supporting PACE and BAC PP-0500) 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 the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the 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. Note that the certification results apply only to the specific version of the product as evaluated.

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the TOSMART-GP1 v01.01.00 (Supporting PACE and BAC PP-0500) from Toshiba Infrastructure Systems & Solutions Corporation located in Kawasaki, Japan.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	IFX_CCI_000005H (Common criteria certification identifier) 0013H 0016H 0000H (Chip Type)	FW-Identifier 80.100.17.0
	CL52 Asymmetric Crypto Library for Crypto@2304T Cl52-LIB-base-XSMALL- HUGE.lib	v2.06.003
	CL52 Asymmetric Crypto Library for Crypto@2304T Cl52-LIB-ecc-XSMALL- HUGE.lib	v2.06.003
	CL52 Asymmetric Crypto Library for Crypto@2304T Cl52-LIB-toolbox- XSMALL-HUGE.lib	v2.06.003
	Hardware Support Library for SLCx2 HSL-01.22.4346-SLCx2_C65.lib	v1.22.4346
Software	ePassport application +OS	Ver.01.01.02

To ensure secure usage a set of guidance documents is provided, together with the TOSMART-GP1 v01.01.00 (Supporting PACE and BAC PP-0500). For details, see section 2.5 "Documentation" of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 2.3.4.

2.2 Security Policy

The main security functions of the TOE are to protect data stored in the TOE from unauthorized reading or writing. The operation of the security functions applied to contactless communication with the terminal shall comply with the BAC, PACE, and Active Authentication Standards specifications defined in Part 11 of Doc 9303.

The TOE provides the main security functions

- BAC function (mutual authentication and Secure Messaging)
- PACE function (mutual authentication and Secure Messaging)
- Active Authentication support function (prevention of copying the IC chip)
- Disabling function of BAC function(prohibition of operating BAC after issuing a passport)
- Write protection function (protection of writing data after issuing a passport)
- Protection function in transport (protection against attacks during transport before issuing the TOE(i.e. transport key lock))
- Tamper resistance (protection against confidential information leak due to physical attacks)

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 5.2 of the *[ST]*.

2.3.2 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.

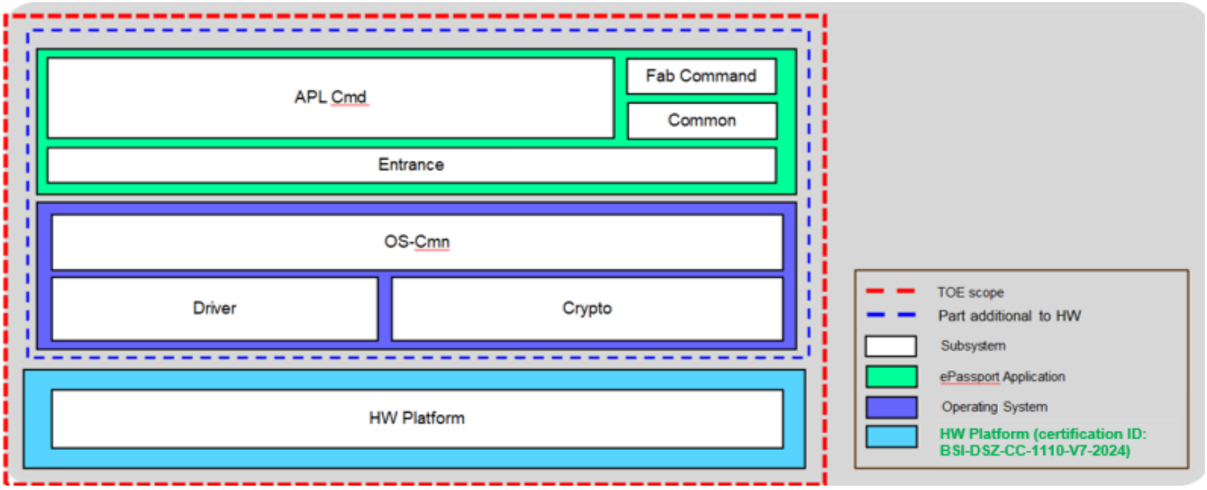
Note that the ICAO MRTD infrastructure critically depends on the objectives for the environment to be met. These are not weaknesses of this particular TOE, but aspects of the ICAO MRTD infrastructure as a whole.

The environment in which the TOE is personalised must perform proper and safe personalisation according to the guidance and referred ICAO guidelines.

The environment in which the TOE is used must ensure that the inspection system protects the confidentiality and integrity of the data send and read from the TOE.

2.4 Architectural Information

The TOE architecture can be depicted as follows:



The TOE is an ePassport formed of a composite security IC, the underlying hardware platform, and the ePassport software.

The underlying hardware platform 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 (RAM, Flash memory), and circuitry for the RF external interface that have been integrated with consideration given to tamper resistance.

The ePassport software consists of a secure operating system and an application on top of the underlying hardware platform. The operating system contains the embedded software functions used by the ePassport application.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Guidance Document for Personalization agent (USR), dated September 27, 2023	MC-SM1911 / Version 01.01.01
Preparative guidance, dated 29 March, 2023	MC-SM1905 / Version 01.01.00
Application Specification, dated 07 January 2025	MC-SM1917 / Version 1.1.3

Authentication Manual using VERIFY command, dated 07 January 2025	MC-SJ0131 / Version 01.01.03
Personalization Specification), dated 07 January 2025	MC-SM1895 / Version 1.1.2
Procedural Request of Security Product Delivery and Receipt, 07 January 2025	MB-ICCARD-W471 / Version 1.0.4

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

The developer performed extensive testing on functional specification, subsystem and module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

The methodical analysis approach was as follows:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack oriented analysis the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this analysis will be performed according to the attack methods in [JIL-AP]. An important source for assurance in this step is the technical report [ETRfC-HW] of the underlying platform.
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

Following the JIL attack methods *[JIL_AM]*, in case that attack scenarios are identified, then a hypothetical rating of minimum attack effort would have been made for the identified attack scenarios.

The total test effort expended by the evaluators was 4 weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The TOE used for testing was:

- TOSMART-GP1 version 01.01.00

2.6.4 Test 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.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.7 Reused Evaluation Results

Sites involved in the development and production of the hardware platform were reused by composition.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number TOSMART-GP1 v01.01.00 (Supporting PACE and BAC PP-0500).

2.9 claims 'strict' Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the TOSMART-GP1 v01.01.00 (Supporting PACE and BAC PP-0500), to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_DVS.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target conformance to the Protection Profile *[PP*_c500*]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <none>.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 "high attack potential". To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The TOSMART-GP1with Supplemental Access Control (BAC+PACE) and Active Authentication Security Target v01.01.11, Dated July 09, 2025 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

BAC	Basic Access Control
CA	Chip Authentication
eMRTD	electronic MRTD
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
JIL	Joint Interpretation Library
MRTD	Machine Readable Travel Document
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
TA	Terminal Authentication
TOE	Target of Evaluation

5 Bibliography

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

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017

[COMP] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[Doc 9303] Machine Readable Travel Documents Seventh Edition — 2015 Doc 9303, Part 11, Security Mechanisms for MRTDs, Seventh edition, 2015

[ETR] Evaluation Technical Report “TOSMART-GP1 v01.01.00” – EAL4+, R4-RPT-074, Version 11.0, Dated 14 July 2025

[HW-CERT] BSI-DSZ-CC-1110-V7-2024 for Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 from Infineon Technologies AG, 30 September 2024.

[HW-ETRfC] Evaluation Technical Report For Composite Evaluation (ETR COMP) for the IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h H13. Cert-ID BSI-DSZ-CC-1110-V6, Version 3, 2023-12-01, TÜV Informationstechnik GmbH.

[ETRfC_ADD] Evaluation Technical Report for Composite Evaluation Addendum (ETR COMP_ADD) for the IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h H13. Cert-ID BSI-DSZ-CC-1110-V7, Version 3, 2024-09-20, TÜV Informationstechnik GmbH.

[HW-ST] Public Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h H13, Including optional Software Libraries Flash Loader – 4x ACL – 4x HSL – 3x SCL – HCL -NRG – CCL, Revision: 5.1, 2024-09-11, Infineon Technologies AG.

[JIL-AAPS] JIL Application of Attack Potential to Smartcards, Version 3.2.1, February 2024

[JIL-AM] Attack Methods for Smartcards and Similar Devices, Version 2.5, May 2022 (sensitive with controlled distribution)

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022

[PP_c500] Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication, version 1.0, registered under the JISEC reference C0500

[ST] TOSMART-GP1with Supplemental Access Control (BAC+PACE) and Active Authentication Security Target v01.01.11, Dated July 09, 2025

(This is the end of this report.)