



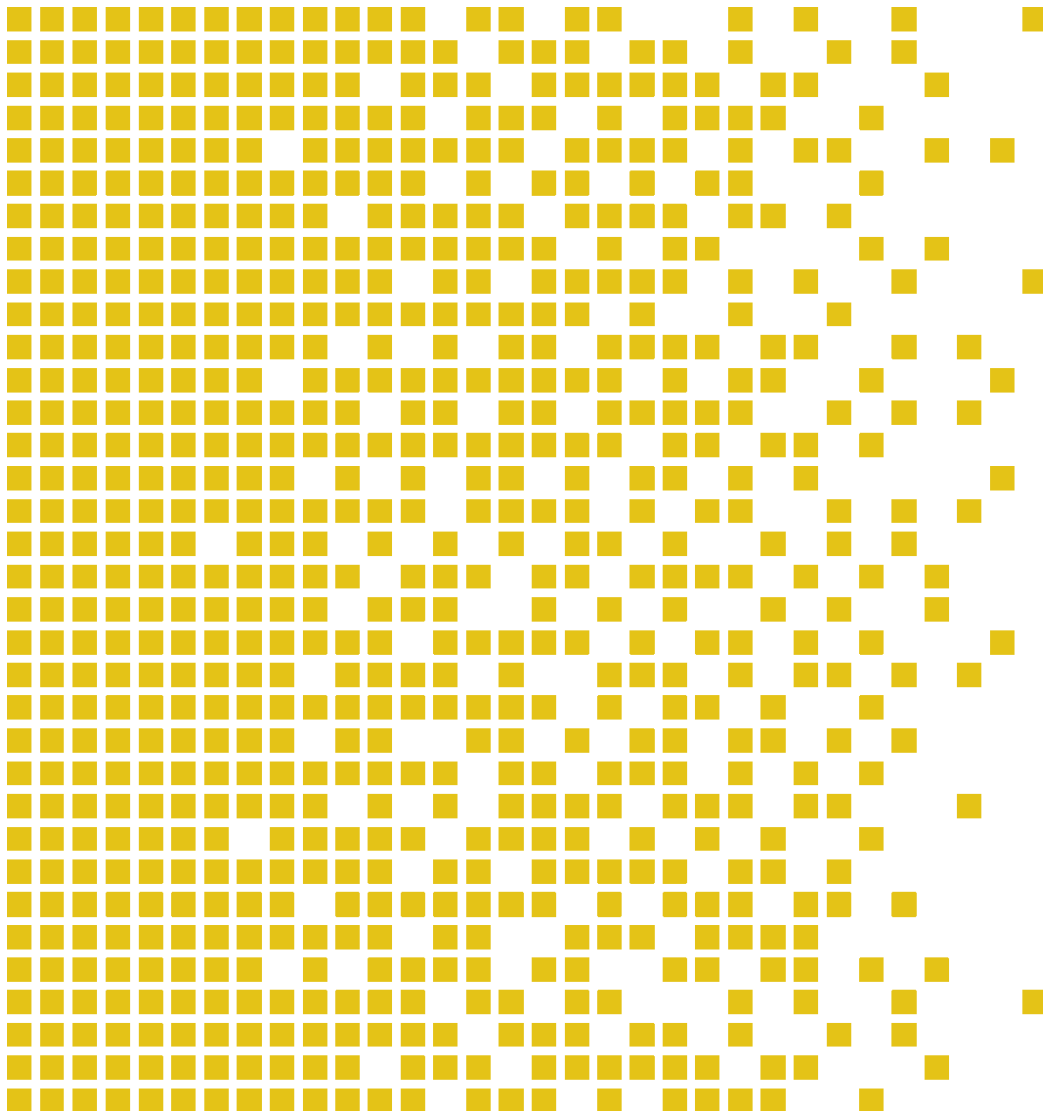
**SERTIT**

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

# SERTIT-097 CR Certification Report

Issue 1.0 28 February 2018

TOSMART-GP1 V01.00.00 (Supporting PACE PP-0499)



CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.1 11.11.2011

### **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. The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognized under the terms of the CCRA July 2nd 2014.

The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC\_FLR CC part 3 components.



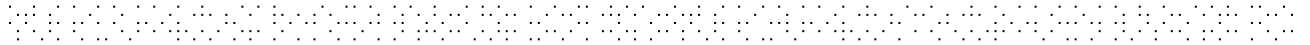
### **MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)**

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

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 SOGIS MRA applies to components up to EAL 4.

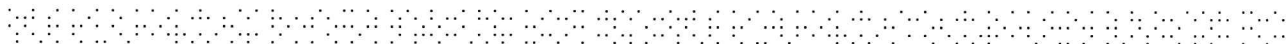




## Contents

1	Certification Statement	5
2	Abbreviations	6
3	References	7
4	Executive Summary	8
4.1	Introduction	8
4.2	Evaluated Product	8
4.3	TOE scope	8
4.4	Protection Profile Conformance	8
4.5	Assurance Level	8
4.6	Security Policy	9
4.7	Security Claims	9
4.8	Threats Countered	9
4.9	Threats Countered by the TOE's environment	9
4.10	Threats and Attacks not Countered	9
4.11	Environmental Assumptions and Dependencies	9
4.12	IT Security Objectives	9
4.13	Non-IT Security Objectives	9
4.14	Security Functional Requirements	9
4.15	Security Function Policy	11
4.16	Evaluation Conduct	11
4.17	General Points	11
5	Evaluation Findings	13
5.1	Introduction	14
5.2	Delivery	14
5.3	Installation and Guidance Documentation	14
5.4	Misuse	14
5.5	Vulnerability Analysis	14
5.6	Developer's Tests	15
5.7	Evaluators' Tests	15
6	Evaluation Outcome	17
6.1	Certification Result	17
6.2	Recommendations	17
	Annex A: Evaluated Configuration	18
	TOE Identification	18
	TOE Documentation	18
	TOE Configuration	19






## 1 Certification Statement

Toshiba TOSMART-GP1 is an e-passport secure IC consisting of the hardware IFX\_CCI\_000005H, which is used as the evaluated underlying platform and the ePassport (OS and application) software on implementing PACE

TOSMART-GP1 version V01.00.00 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the specified Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 4+ ALC\_DVS.2 and AVA\_VAN.5 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended with FCS\_RND.1 It has also met the requirements of Protection Profile PP 0499 PACE.

Author	Arne Høye Rage Certifier 
Quality Assurance	Kjartan Jæger Kvassnes Quality Assurance 
Approved	Jørn Arnesen Head of SERTIT 
Date approved	28 February 2018



## 2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
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
EWP	Evaluation Work Plan
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



### 3 References

- [1] TOSMART-GP1with Supplemental Access Control (PACE) and Active Authentication Security Target, 11 January 2018, version 01.00.05
- [2] TOSMART-GP1with Supplemental Access Control (PACE) and Active Authentication Security Target lite, 11 January 2018, version 01.00.05
- [3] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.
- [4] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.
- [5] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.
- [6] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.
- [7] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.
- [8] JIL Application of Application Attack Potential to Smart Cards, Version 2.9, May 2013
- [9] MSSR, Minimum site security requirements, v1.1, July 2013
- [10] ICAO. Doc 9303 - Machine Readable Travel Documents, seventh edition, 2015
- [11] Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 3 – Common Specifications, Version 2.10,20. March 2012.
- [12] 18-RPT-017 Evaluation Technical Report Sertit-097 version 2.0 .
- [13] Guidance Document for Personalization agent (USR) MC-SM1911/ Version 01.00.06
- [14] Preparative guidance (PRE) MC-SM1905/ Version 01.00.04
- [15] Application Specification MC-SM1917 / Version 1.0.6
- [16] Authentication Manual using VERIFY command MC-SJ0131 / Version 01.00.03
- [17] Personalization Specification MC-SM1895 / Version 1.0.5
- [18] Procedural Request of Security Products Delivery and Receipt MB-ICCARD-W471-03 / Version 01.00.03
- [19] Protection Profile for ePassport IC with SAC (PACE) and Active Authentication,, version 1.00, March 8, 2016 (English translation).



## 4 Executive Summary

### 4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of TOSMART-GP1 version V01.00.00 to the Sponsor, Toshiba, 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][2] which specifies the functional, environmental and assurance evaluation requirements.

### 4.2 Evaluated Product

The version of the product evaluated was TOSMART-GP1 version V01.00.00.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Toshiba.

The TOE is an secure IC consisting of hardware and software (OS and application) for machine readable travel documents (MRTDs) based on the requirements of the International Civil Aviation Organization, as defined in ICAO Doc 9303 [10]. The TOE is composited product where the hardware (and crypto library) is developed and certified by developed and produced by Infineon IFX\_CCI\_000005H certified under and the software is developed by Toshiba. Toshiba is responsible for the form factor and delivers an inlay (sheet) to be embedded in a booklet to the personalization agent.

The TOE implements and supports PACE. An authenticated Personalization agent is able to perform the personalization for a specific e-passport holder. Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

### 4.3 TOE scope

The TOE Scope is described in the Security Target[1][2], section 1.

### 4.4 Protection Profile Conformance

The Security Target[1] claimed conformance to the following protection profile PP 0499 PACE

### 4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 4+, augmented by ALC\_DVS.2 and AVA\_VAN.5 and extended by FCS\_RND.1. Common Criteria Part 3 [5] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[3].





#### 4.6 Security Policy

The TOE security policies are detailed in ST[1] section 4.5.

#### 4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats and OSP's which these objectives counter or meet and security functional requirements and security functions to elaborate the objectives. Most of the SFR's are taken from CC Part 2[4]; use of this standard facilitates comparison with other evaluated products.

The following extended SFR is defined in the protection profile [19] FCS\_RND.1.

#### 4.8 Threats Countered

All threats that are countered are described in the Security Target[1] section 4.4.

#### 4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

#### 4.10 Threats and Attacks not Countered

There are no threats and attacks not countered

#### 4.11 Environmental Assumptions and Dependencies

The assumptions that apply to this TOE are described in the Security Target [1] *section 4.2*

#### 4.12 IT Security Objectives

The security objectives that apply to this TOE are described in the Security Target [1] section 5.1

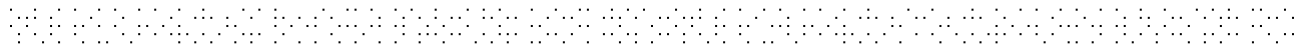
#### 4.13 Non-IT Security Objectives

The security objectives for the environment that apply to this TOE are described in the Security Target [1] section 5.2

#### 4.14 Security Functional Requirements

The security objectives that apply to this TOE are described in the Security Target [1] section 7.2.1

Security functional requirements		
FCS_CKM.1p	Cryptographic key generation	
FCS_CKM.1e		
FCS_CKM.4	Cryptographic key destruction	
FCS_COP.1a	Cryptographic operation	
FCS_COP.1h		
FCS_COP.1n		
FCS_COP.1e		
FCS_COP.1hp		
FCS_COP.1mp		
FCS_COP.1sp		
FCS_RND.1		Quality standards for random numbers
FDP_ACC.1a		Subset access control
FDP_ACC.1p		
FDP_ACF.1a	Security attribute based access control	
FDP_ACF.1p		
FDP_ITC.1	Import of user data without security attributes	
FDP_UCT.1p	Basic data exchange confidentiality	
FDP_UIT.1p	Data exchange integrity	
FIA_AFL.1a	Authentication failure handling	
FIA_AFL.1d		
FIA_AFL.1r		
FIA_UAU.1	Timing of authentication	
FIA_UAU.4	Single-use authentication mechanism	
FIA_UAU.5	Multiple authentication mechanisms	
FIA_UID.1	Timing of identification	
FMT_MTD.1	Management of TSF data	
FMT_SMF.1	Specification of management functions	
FMT_SMR.1	Security roles	
FPT_PHP.3	Resistance to physical attack	



FTP_ITC.1	Inter-TSF trusted channel
-----------	---------------------------

#### 4.15 Security Function Policy

The PACE access control policy will enforce that only Subjects, namely the Inspection System being properly authenticated read content of files during operational use of the TOE.

#### 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[6]. 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 itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[5] and the Common Evaluation Methodology (CEM)[7]. Interpretation [8] is used as input for the vulnerability analysis

SERTIT monitored the evaluation which was carried out by the Brightsight Commercial Evaluation Facility (ITSEF/EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR)[12] to SERTIT in 20 February 2018. 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[5]. These classes comprise the EAL4 assurance package augmented with ACL\_DVS.2 and AVA\_VAN.5

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 life-cycle model
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_TSS.1	TOE summary specification
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	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[12] under the CC Part 3[5] 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/evaluated versions of its constituent components have been supplied, and to check that the security of the TOE has not been compromised in delivery.

The delivery procedure is described in the supporting document [18]

## 5.3 Installation and Guidance Documentation

Installation procedures are described in supporting documents [16][17][14]

## 5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Security IC Embedded Software shall follow the guidance documentation [16][17][14] for the TOE in order to ensure that the TOE is operated in a secure manner.

The guidance documents adequately describe 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 use the TOE's security functions.

## 5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

An independent vulnerability analysis was done, consisting of the following steps:

- A code review was performed focusing on key security functionalities of the TOE (key functionalities are covering the SFRs claimed by the ST and Security Mechanisms claimed in ARC). As part of the code review the evaluators verified that the software has followed the security recommendations of the underlying platform. The goal of the code review is to identify potential vulnerabilities that are later taken into account during the vulnerability analysis.



- The vulnerability analysis is then performed using the findings of the design review and the code review. During the vulnerability analysis also the content of the ETR for Composition from the underlying certified platform was taken into account. The vulnerability analysis resulted in a penetration test plan. Other available information was also taken into consideration as input for the vulnerability analysis including Attack Methods for Smartcards and Similar Devices (controlled distribution) and internal knowledge on ePassport products.
- The penetration tests are performed according to the penetration test plan.
- Upon the vulnerability analysis was already finished in August 2017. Some open items remained and were closed in November 2017 and January 2018. The vulnerability analysis was revisited and considered the new attacks that have appeared since August 2018. The vulnerability analysis was finalized in January 2018.

## 5.6 Developer's Tests

Developer tests were performed using engineering samples and the TOE embedded on the emulator.

tests performed can be categorized as follows:

- Unit tests: all branches of modified modules (i.e., C functions) are tested. Unit test results for unmodified modules are reused.
- Integration tests: different combinations of groups of modules are tested. Most tests are performed through (short sequences of) APDU commands, but some are performed using a debugger. Batch files are used to process successive tests and take care of ordering dependencies.
- System tests: the overall system is tested. This is done by testing many aspects of the TOE, including but not limited to various valid and invalid CLA/INS combinations, command processing time, boundary and access conditions, the state transition table, and the customer requirements for passport issuance (e.g. changing of the keys, performing the whole personalisation flow, checking valid and invalid Short File Identifiers). Most tests are performed through (sequences of) APDU commands, but some are performed using a debugger.
- Protocol tests: both integration and system tests also contain protocol tests. These tests focus on ISO/IEC 10373-6 scenarios, but also on measuring the protocol processing time and checking other timing characteristics.

## 5.7 Evaluators' Tests

The evaluator's responsibility for performing independent testing is required by the ATE\_IND class.



Since developer's testing procedures have been found to be extensive and thorough the choice was made to perform the evaluator independent testing by witnessing of testing a portion of the developer's test cases, using the developer's tools, at the premises of the EVIT.

The evaluator employs a sampling strategy to select developer tests to validate the developer's test results. The sampling strategy is focused especially on the proprietary test suites used for integration and system tests

- Proprietary test suites for integration tests
- Proprietary test suite for system tests

In addition to this, the evaluator has defined additional test cases, prompted by study of the developer's documentation. Independent test suite developed by the EVIT and aimed at making sure that the guidance is reasonable and that the APDU necessary for AVA\_VAN.5 testing can be executed and show the expected behaviour.





## 6 Evaluation Outcome

### 6.1 Certification Result

After due consideration of the ETR[12], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that TOSMART-GP1 version V01.00.00 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4+ augmented with AVA\_VAN.5 and ALC\_DVS.2 for the specified Common Criteria Part 2 extended by FCS\_RND.1 as in the Protection Profile PP 0499 PACE

### 6.2 Recommendations

Prospective consumers of TOSMART-GP1 version V01.00.00 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

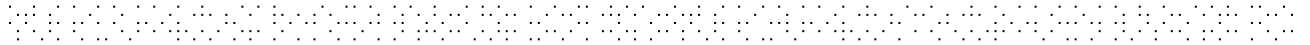
The TOE consists of:

Delivery item type	Identifier	Version	Medium
Hardware	IFX_CCI_000005H (Common criteria certification identifier)	FW-Identifier 80.100.17.0	Sheet
CL52 Asymmetric Crypto Library for Crypto@2304T	0013H 0016H 0000H (Chip Type)		
	CI52-LIB-base-XSMALL-HUGE.lib	v2.06.003	
CL52 Asymmetric Crypto Library for Crypto@2304T	CI52-LIB-ecc-XSMALL-HUGE.lib	v2.06.003	
CL52 Asymmetric Crypto Library for Crypto@2304T	CI52-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.01.00.14	Flash memory of hardware (user area)
Delivery item type	Identifier	Document No. / Version	Medium
Guidance (for personalization agent)	Guidance Document for Personalization agent (USR)	MC-SM1911/ Version 01.00.06	Document / pdf
	Preparative guidance (PRE)	MC-SM1905/ Version 01.00.04	Document / pdf
	Application Specification	MC-SM1917 / Version 1.0.6	Document / pdf
	Authentication Manual using VERIFY command	MC-SJ0131 / Version 01.00.03	Document / pdf
	Personalization Specification	MC-SM1895 / Version 1.0.5	Document / pdf
	Procedural Request of Security Products Delivery and Receipt	MB-ICCARD-W471-03 / Version 01.00.03	Document / pdf

### TOE Documentation

The supporting guidance documents evaluated were:

- [a] Guidance Document for Personalization agent (USR) MC-SM1911/ Version 01.00.06
- [b] Preparative guidance (PRE) MC-SM1905/ Version 01.00.04
- [c] Application Specification MC-SM1917 / Version 1.0.6
- [d] Authentication Manual using VERIFY command MC-SJ0131 / Version 01.00.03
- [e] Personalization Specification MC-SM1895/ Version 1.0.5



[f] Procedural Request of Security Products Delivery and Receipt MB-  
ICCARD-W471-03 / Version 01.00.03

Further discussion of the supporting guidance

material is given in Section 5.3 "Installation and Guidance Documentation".

### TOE Configuration

The following configuration was used for testing:

The TOE can be identified using the procedure as specified in [17]

Command	APDU command	APDU response
GET MASK VERSION	C0 F8 00 00 0A 42 00 36 73 90 00	E0 53 C1 05 42 00 36 73 90 C2 03 01 00 14 C4 03 01 00 00 C5 36 CD 16 33 63 01 00 13 00 16 00 00 07 0D 0A 06 AF C9 00 19 00 48 00 5F 74 6F 73 32 35 FF FF FF 80 10 01 70 82 03 03 01 92 03 21 02 0A 01 00 00 05 01 0B 0B 0B 03 02 C9 04 FF FF FF FF CA 02 00 00 90 00