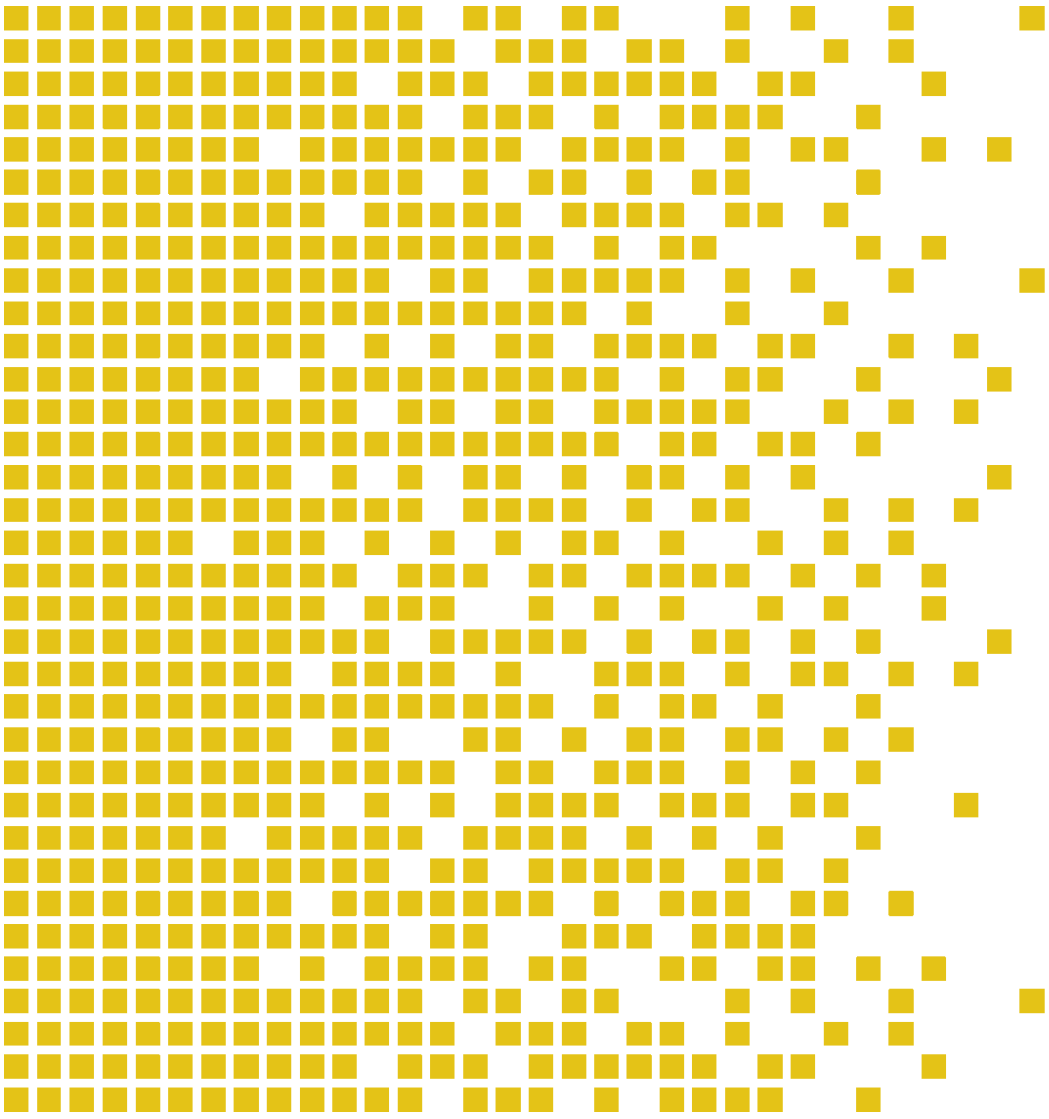
SERTIT-080 CR Certification Report

Issue 1.0 17 January 2017

CEITEC ePassport Module, CTC21001, v1.0 (supporting EAC)



SERTIT, Postboks 814, 1306 Sandvika, 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.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised 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.

The recognition under SOGIS MRA is for components up to EAL 4.

Contents

1	**Certification Statement**	**4**
2	**Abbreviations**	**5**
3	**References**	**6**
4	**Executive Summary**	**7**
4.1	Introduction	7
4.2	Evaluated Product	7
4.3	TOE scope	7
4.4	Protection Profile Conformance	7
4.5	Assurance Level	7
4.6	Security Policy	8
4.7	Security Claims	8
4.8	Threats Countered	8
4.9	Threats Countered by the TOE's environment	8
4.10	Threats and Attacks not Countered	8
4.11	Environmental Assumptions and Dependencies	8
4.12	IT Security Objectives	8
4.13	Non-IT Security Objectives	8
4.14	Security Functional Requirements	9
4.15	Security Function Policy	10
4.16	Evaluation Conduct	10
4.17	General Points	11
5	**Evaluation Findings**	**12**
5.1	Introduction	13
5.2	Delivery	13
5.3	Installation and Guidance Documentation	13
5.4	Misuse	13
5.5	Vulnerability Analysis	13
5.6	Developer's Tests	14
5.7	Evaluators' Tests	15
6	**Evaluation Outcome**	**16**
6.1	Certification Result	16
6.2	Recommendations	16
Annex A: Evaluated Configuration		**17**
TOE Identification		17
TOE Documentation		17
TOE Configuration		17
Annex B: TOE's security architecture		**19**

1 Certification Statement

Ceitec S.A. CEITEC ePassport Module, CTC21001 is an electronic micro module for machine readable travel documents based on the requirements of the International Civil Aviation Organization, as defined in ICAO Doc 9303 implementing BAC and EAC.

CEITEC ePassport Module, CTC21001 version v1.0 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 4+ augmented with ALC_DVS.2 and AVA_VAN.5 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended by FAU_SAS.1, FCS_RND.1, FIA_API.1, FMT_LIM.1, FMT_LIM.2 and FPT_EMSEC.1. It has also met the requirements of Protection Profile PP-0056.

Author	Arne Høye Rage Certifier
Quality Assurance	Kjartan Jæger Kvassnes Quality Assurance
Approved	Kristian Bae Head of SERTIT
Date approved	17 January 2017

2 Abbreviations

BAC	Basic Access control
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
EAC	Extended Access control
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
SERTIT	Norwegian Certification Authority for IT Security
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] CEITECSA 5.410.052, Security Target Lite for CEITEC ePassport Module CTC21001 with EAC, Version 1.0 – 07/Nov/2016

[2] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.

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

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[7] JIL Application of Application Attack Potential to Smart Cards, Version 2.9, May 2013t

[8] A proposal for Functionality classes for random number generators, version 2.0, 18 September 2011

[9] Minimum site security requirements, v1.1, July 2013

[10] ICAO. Doc 9303 - Machine Readable Travel Documents, version 6, 2006

[11] RF PROTOCOL AND APPLICATION TEST STANDARD FOR EMRTD - PART 3 TESTS FOR APPLICATION PROTOCOL AND LOGICAL DATA STRUCTURE Version: V2.06, Date – March 10, 2014

[12] Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 3 – Common Specifications, Version 2.10,20. March 2012

[13] 16-RPT-533 Evaluation technical report Sertit-080, v1.1, 15-12-2016

[14] CEITECSA 5-410-022 - Personalization Protocol v5.0

[15] CEITECSA 5-410-031 - CTC21001 User Guidance v4.0

[16] CEITECSA 5.420.014, Micromodule CTC21001 MM, R00, 16-12-2014

[17] [PP-0056] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control BSI-CC-PP-0056, version 1.10, 25th March 2009 Evaluation Technical Report

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of CEITEC ePassport Module, CTC21001 version v1.0 to the Sponsor, Ceitec S.A., 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 CEITEC ePassport Module, CTC21001 and version v1.0.

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

The TOE is an electronic module 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 developed and produced by Ceitec S.A. and delivered to the Passport Manufacturer as micro modules.

The TOE implements and supports BAC and EAC. A Personalization agent needs the EAC functionality for authentication during 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.

An overview of the TOE's security architecture can be found in Annex B.

4.3 TOE scope

The TOE scope is described in the Security Target[1], chapter 1

4.4 Protection Profile Conformance

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

PP-0056

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 FAU_SAS.1, FCS_RND.1, FIA_API.1,

FMT_LIM.1, FMT_LIM.2 and FPT_EMSEC.1. 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 ST[1] section 3.4.

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[3]; use of this standard facilitates comparison with other evaluated products.

The following SFRs are defined in the protection profile [17]: FAU_SAS.1, FCS_RND.1, FIA_API.1, FMT_LIM.1, FMT_LIM.2 and FPT_EMSEC.1.

4.8 Threats Countered

All threats that are countered are described in the Security Target[1], section 3.3

4.9 Threats Countered by the TOE's environment

Threats that are covered by the TOE's environment are identified in the Security Target[1], section 4.3

4.10 Threats and Attacks not Countered

No threats or attacks are described that are not countered

4.11 Environmental Assumptions and Dependencies

The assumptions that apply to this TOE are described in the Security Target[1], section 3.2

4.12 IT Security Objectives

The security objectives for the TOE that apply to this TOE are described in the Security Target[1], section 4.1

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 4.2

4.14 Security Functional Requirements

The security functional requirements that apply to this TOE are described in the Security Target[1], section 6.1

Security Functional Requirements	
FAU_SAS.1	Audit storage
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1/SHA	Cryptographic operation
FCS_COP.1/SYM	
FCS_COP.1/MAC	
FCS_COP.1/SIG_VER	
FCS_RND.1	Quality metric for random numbers
FIA_UID.1	Timing of identification
FIA_UAU.1	Timing of authentication
FIA_UAU.4	Single-use authentication mechanisms
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.6	Re-authenticating
FIA_API.1	Authentication Proof of Identity
FDP_ACC.1	Subset access control
FDP_ACF.1	Basic Security attribute based access control
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FMT_MTD.1/INI_ENA	Management of TSF data
FMT_MTD.1/INI_DIS	
FMT_MTD.1/CVCA_INI	

FMT_MTD.1/CVCA_UPD	
FMT_MTD.1/DATA	
FMT_MTD.1/KEY_WRITE	
FMT_MTD.1/CAPK	
FMT_MTD.1/KEY_READ	
FMT_MTD.3	Secure TSF data
FPT_EMSEC.1	TOE Emanation
FPT_FLS.1	Failure with preservation of secure state
FPT_TST.1	TSF testing
FPT_PHP.3	Resistance to physical attack

4.15 Security Function Policy

The Basic access control policy will enforce that only Subjects, namely the Personalization Agent, Basic Inspection System and Terminal, being properly authenticated can write content of files during personalization or read content of files during operational use of the TOE, except for the biometric user data

Biometric user data shall only be accessible when Subjects are authenticated with the Enhanced Access Control authentication.

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 itself evaluated. 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].Interpretation [7] is used as input for the vulnerability analysis

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

submitted the final Evaluation Technical Report (ETR) [13]to SERTIT on 15 December 2016. 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 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	Focused 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 [13] 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 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[15].

5.3 Installation and Guidance Documentation

Installation procedures are described in supporting document [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 [14][15] 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 design review and a code review were 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). The design review on the IC and the code review on the software was clearly separated by using secure programmer guidelines created by the IC development team. The goal of the design and 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 secure programmer guidelines were validated. The combined 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 finalizing the vulnerability analysis the evaluation project was stopped for a while. A year later during the restart one penetration test was redone and the vulnerability analysis was revisited while finalizing the vulnerability analysis.

5.6 Developer's Tests

The developer tests consist of different parts, focused on the different core components as described in Annex B.

Testing is performed using engineering samples, samples implementing a debug version and the finalized design.

The tests were performed on the hardware separately and on the software combined with the hardware in the following test suites.

Hardware tests:

- Simulation tests on the design under verification
- Physical tests on engineering samples in the lab and on the wafer during production
- Conformance tests on the ISO-14443 interface

Software tests:

- Profile BAC and ICAO Layer 6 (BAC functionality according ICAO standard [11])
- Standard Chip Layer 6 (including M and N) (EAC functionality according to BSI standard [12])
- Proprietary test suites for (pre)-personalization
- Proprietary test suites for Inspections
- Proprietary test suites for lifecycle testing, implemented self-test functionality and sensor testing.

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 on the hardware at the developer's premises and repetition of 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 as the other test suites are commercial tools, widely accepted within the industry:

- Proprietary test suites for (pre)-personalization
- Proprietary test suite for inspection

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 focused on error behavior and blocking of the TOE.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR [13], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that CEITEC ePassport Module, CTC21001 version v1.0 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4+ augmented with ALD_DVS.2 and AVA_VAN.5 for the specified Common Criteria Part 2 extended by FAU_SAS.1, FCS_RND.1, FIA_API.1, FMT_LIM.1, FMT_LIM.2 and FPT_EMSEC.1.functionality as in the Protection Profile PP-0056, in the specified environment described in the Security target[1].

6.2 Recommendations

Prospective consumers of CEITEC ePassport Module, CTC21001 version v1.0 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.

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

These guidance documents include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Component	Version	Package
Silicon Integrated Circuit	COP V1R0 R	Micro Module
IC Software	1.0.0.719	Embedded in the hardware
CEITECSA 5.410.031 -CTC21001 User Guidance	4.0	Document
CEITECSA 5.410.022 - Personalization Protocol	5.0	Document
CEITECSA 5.420.014 -Micromodule CTC21001 MM	R00	Document

TOE Documentation

The supporting guidance documents evaluated were:

[a] CEITECSA 5.410.031 -CTC21001 User Guidance, version 4.0

[b] CEITECSA 5.410.022 -Personalization Protocol . version 5.0

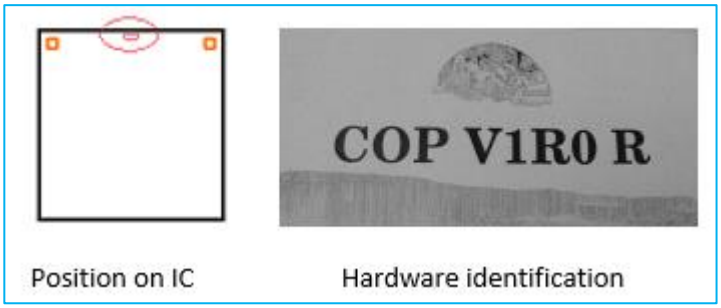
[c] CEITECSA 5.420.014 -Micromodule CTC21001 MM , R00

[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 Hardware configuration has been described in [15] and can be read from the IC surface V1R0



The TOE Software configuration has been described in [15] and can be read before personalisation by the Get Data command as described in [14] .

The software version has been identified conform [14] by:

COMMAND NAME	*COMMAND APDU*	*APDU RESPONSE*	*RESULT OF VERIFICATION*
READ_SOFTWARE_VERSION	*0C CA 01 01 0D 97 01 0A 8E 08 21 52 78 CE 8B B7 AA E1 00*	*37 31 39 90 00*	*As expected*

Annex B: TOE's security architecture

In this ST the physical TOE comprises the chip with the MRTD application, encapsulated on a micro module, which provides the contacts for an external antenna (see[1]). The TOE is intended to be embedded in an inlay with an antenna as part of a booklet. Together they represent a complete MRTD (e-passport).

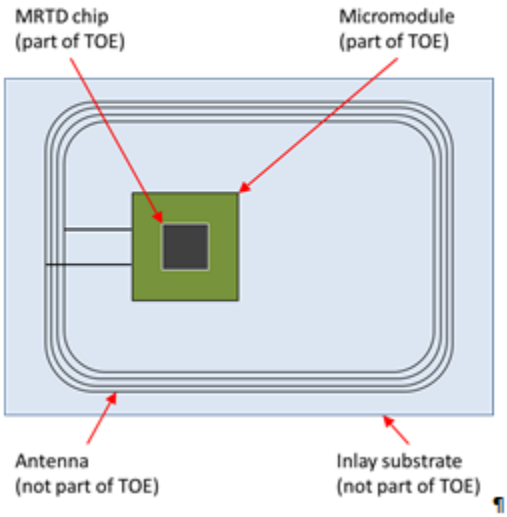


Figure 1: Physical scope of the TOE

From a logical perspective the TOE provides the following:

- identification and authentication;
- access control for personalization;
- protection of integrity of personal data;
- protection of confidentiality of personal data;
- protection against abuse of functionality;
- protection against information leakage;
- protection against physical tampering; and
- protection against malfunctions.

A Personalization Agent is granted access to the personalization function of the TOE after a successful BAC and EAC authentication (where EAC comprise both the Chip Authentication and Terminal Authentication). The personalization is performed within a secure session that is established during the authentication.

At the operational stage, the Inspection System must authenticate himself using a BAC mechanism with keys derived from the MRZ information in order to read the biographical data of the MRTD Holder and TSF data.

The optional biometric data can only be read after the Inspection System successfully performs a Chip Authentication and a Terminal Authentication procedure (i.e. EAC).

Integrity of the personal data is protected via control of the TOE life-cycle stage. The life-cycle management checks the result of the Personalization Agent authentication and decides whether the TOE can be switched to the personalization state, kept in the pre-personalized state (awaiting a new agent authentication attempt) or be permanently disabled (if a potentially unsecure condition has been detected).

The TOE will only transition to the "Operational Use" phase if the personalization is complete. Any interrupted personalization (e.g. due to power loss) will be discarded and the personalization process will have to be executed from scratch on the next attempt. Changes and additions to data on a personalized TOE are prevented.

Confidentiality of personal data is protected by a secure communication mechanism between the TOE and external systems and via access control to regulate access to the assets stored on the TOE.

A secure communication session is established between the TOE and the Personalization or the Inspection System once the BAC and EAC procedures are successfully executed. The secure communication uses data encryption and message authentication according to [10] in order to protect the MRTD Holder's data from eavesdropping and unauthorized access. If the communication session is finished or interrupted, the session keys are destroyed and the TOE requires that the Personalization or Inspection System be re-authenticated by the BAC and EAC in order to resume the message exchange.

Assets stored in the TOE are protected by measures that enforce their confidentiality and/or integrity. The TOE private key for Chip Authentication and the code memory are not accessible externally after the "Manufacturing" phase of the TOE. Also, integrity of TSF data objects is checked before their use, e.g. by redundancy checks.

Correct software execution is enforced by the use of logical constructs and techniques designed to detect perturbations in the program flow.

The integrated circuit of the TOE provides a number of hardware security features aimed at protecting the stored information against leakage or disclosure.