



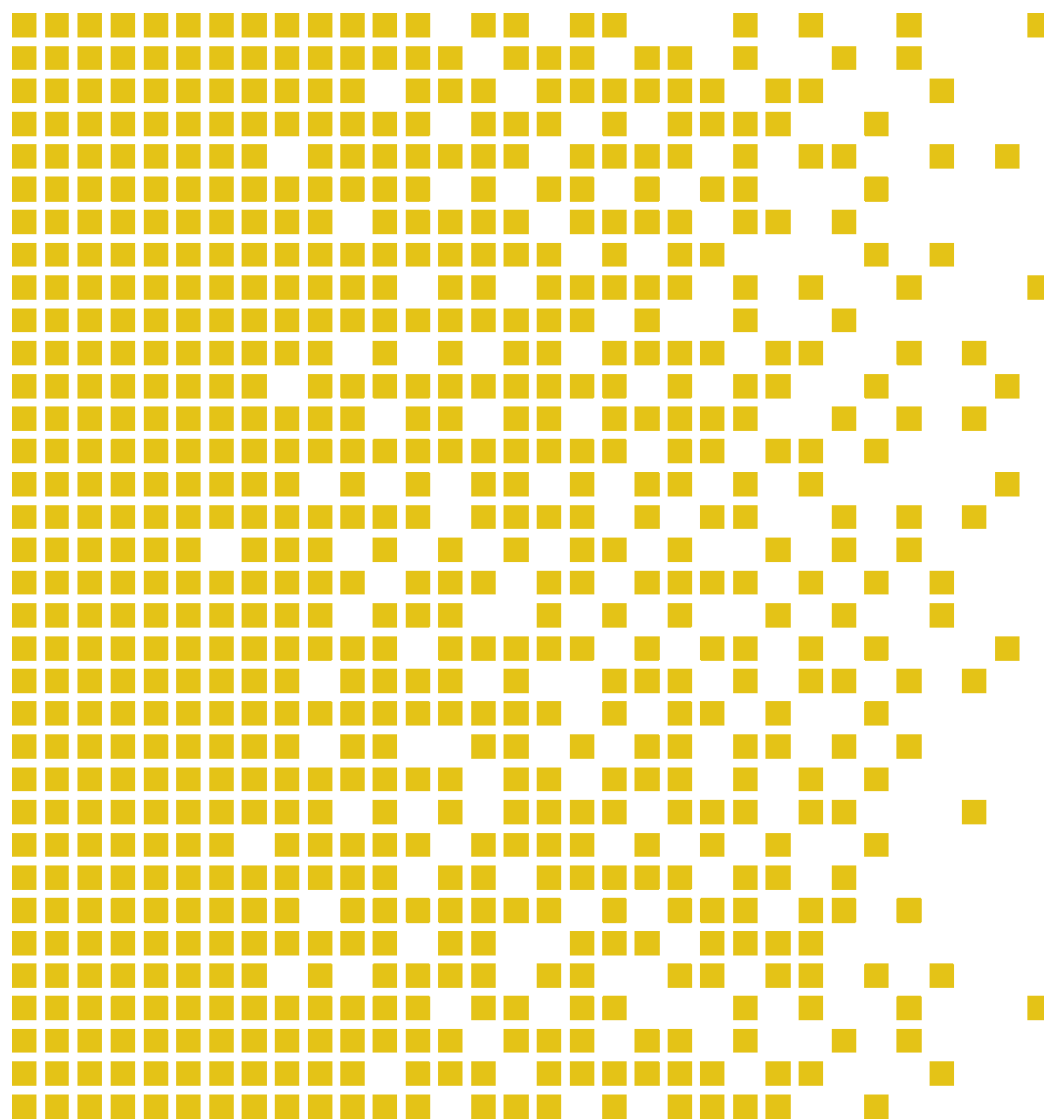
SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet Norwegian Certification Authority for IT Security

SERTIT-090 CR Certification Report

Issue 1.0 25 November 2016

HED Secure Smart Card Chip CIU9872B_01 C11 with IC Dedicated Software



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 Dutch 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

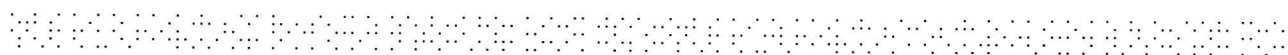
The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Dutch evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements 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

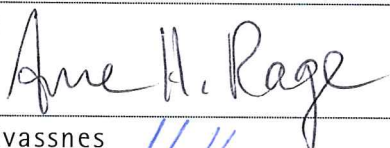


1	Certification Statement.....	4
2	Abbreviations	5
3	References.....	7
4	Executive Summary	8
4.1	Introduction	8
4.2	Evaluated Product	8
4.3	TOE scope	8
4.4	Protection Profile Conformance	8
4.5	Assurance Level	8
4.6	Security Policy	9
4.7	Security Claims	9
4.8	Threats Countered	9
4.9	Threats Countered 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	10
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	18



1 Certification Statement

CEC Huada Electronic Design Co, Ltd HED Secure Smart Card Chip CIU9872B_01 C11 with IC Dedicated Software is a high-end dual-interface secure smart card integrated circuit suitable for ID cards, Banking cards, e-Passport applications and the like.

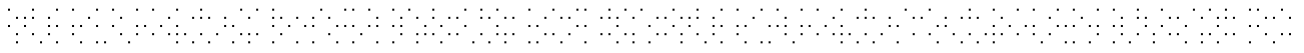
HED Secure Smart Card Chip CIU9872B_01 C11 with IC Dedicated Software has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 5+ augmented with AVA_VAN.5 and ALC_DVS.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended functionality in the specified environment when running on the platforms specified in Annex A. It has also met the requirements of Protection Profile BSI-CC-PP-0084-2014 V1.0.

Author	Arne Høye Rage Certifier 
Quality Assurance	Kjartan Jæger Kvassnes Quality Assurance 
Approved	Kristian Bae Head of SERTIT 
Date approved	25 November 2016



2 Abbreviations

API	Application Programming Interface
CC	Common Criteria for Information 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
CMS	Chip Management System
DEMA	Differential Electro Magnetic Analysis
DES	Data Encryption Standard
DPA	Differential Fault Analysis
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
EMFI	Electro-Magnetic Fault Injection
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
FBBI	Forward-Body Bias Injection
IC	Integrated Circuit
OSP	Organizational Security Policy
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir, Adleman Public Key Encryption
SERTIT	Norwegian Certification Authority for IT Security
SEMA	Simple Electro Magnetic Analysis
SFR	Security Functional Requirements
SPA	Simple Power Analysis
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

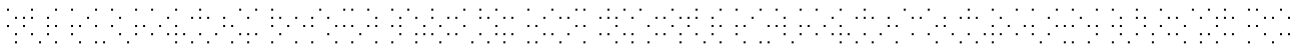


VM Voltage Manipulation



3 References

- [1] Security Target Lite of CIU9872B_01 C11 Secure Smart Card Chip, CEC Huada Electronic Design Co, Ltd, Version 1.1, 2 November 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 Attack Methods for Smartcards and Similar Devices, Version 2.2, January 2013.
- [8] JIL Application of Application Attack Potential to Smart Cards, Version 2.9, May 2013.
- [9] AIS20/31 A proposal for Functionality classes for random number generators, Version 2.0, 18 September 2011.
- [10] Evaluation Technical Report (ETR) Common Criteria EAL5+ Evaluation of the HED Secure Smart Card Chip CIU9872B_01 C11 with IC Dedicated Software, 16-RPT-444 Version 2.0, 2 Nov, 2016 (Brightsight).
- [11] CIU9872B_01 C11 Operational User Guidance, Version 1.0, 20 Oct 2016.
- [12] CIU9872B_01 C11 Preparative Procedures, Version 1.0, 20 Oct 2016
- [13] CIU9872B_01 C11 Crypto Library User Guide, Version 1.0, 20 Oct 2016
- [14] CIU9872B_01 C11 Product Datasheet, Version 1.0, 20 Oct 2016
- [15] Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, Version 1.0, January 2014.



4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of HED Secure Smart Card Chip CIU9872B_01 C11 with IC Dedicated Software to the Sponsor, CEC Huada Electronic Design Co, Ltd, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their 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 HED Secure Smart Card Chip CIU9872B_01 C11 with IC Dedicated Software.

This product is also described in this report as the Target of Evaluation (TOE). The developer was CEC Huada Electronic Design Co, Ltd.

The TOE is a secure smart card integrated circuit with dedicated software mainly for banking and finance market, electronic commerce or governmental applications. The scope of the TOE includes a dual-interface IC hardware and IC dedicated software for DES and RSA. The IC has a DES coprocessor, a RSA coprocessor, a True Random Number Generator (AIS20/31 [9] PTG.2 class) and a Deterministic Random Number Generator (AIS 20/31 [9] DRG.3 class).

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], chapter 1.3.

4.4 Protection Profile Conformance

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

BSI-CC-PP-0084-2014 V1.0

4.5 Assurance Level

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



4.6 Security Policy

The TOE security policies are detailed in Security Target [1], chapter 3.3.

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 meet the objectives. Most of the SFR's are taken from CC Part 2 [3]. Others come from extended component definitions copied from the claimed PP [15]. Use of the standard and the standardized PP [15] facilitates comparison with other evaluated products

The following SFR's are defined in the Protection Profile [15]: FCS_RNG.1, FMT_LIM.1, FMT_LIM.2, FAU_SAS.1, FDP_SDC.1.

4.8 Threats Countered

All threats that are countered are described in the Security Target [1], chapter 3.2.

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

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], chapter 3.4.

4.12 IT Security Objectives

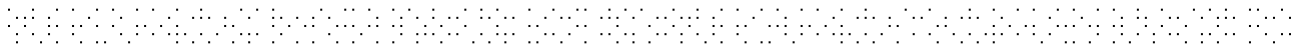
The security objectives that apply to this TOE are described in the Security Target [1], chapter 4.1.

4.13 Non-IT Security Objectives

The security objectives for the environment are described in the Security Target [1], chapter 4.2.

4.14 Security Functional Requirements

The following Security Functional Requirements are directly taken from the Protection Profile [15].



Security Functional Requirement	Title
FRU_FLT.2	"Limited fault tolerance"
FPT_FLS.1	"Failure with preservation of secure state"
FMT_LIM.1	"Limited capabilities"
FMT_LIM.2	"Limited availability"
FAU_SAS.1	"Audit storage"
FPT_PHP.3	"Resistance to physical attack"
FDP_ITT.1	"Basic internal transfer protection"
FDP_IFC.1	"Subset information flow control"
FPT_ITT.1	"Basic internal TSF data transfer protection"
FDP_SDC.1	"Stored data confidentiality"
FDP_SDI.2	"Stored data integrity monitoring and action"
FCS_RNG.1[PTG.2]	"Random Number Generation (Class PTG.2)"
FCS_RNG.1[DRG.2]	"Random number generation (Class DRG.3)"
FCS_COP.1[TDES]	"Cryptographic operation"
FCS_COP.1[RSA]	"Cryptographic operation"

Except for FAU_SAS.1, FDP_SDC.1, FDP_SDI.2, FCS_RNG.1 and FCS_COP.1 all assignments and selections are completely defined in the Protection Profile [15].

The following additional Security Functional Requirements are claimed in the Security Target [1]:

Security Functional Requirement	Title
FDP_ACC.1	"Subset access control"
FDP_ACF.1	"Security attribute based access control"

4.15 Security Function Policy

The TOE is a secure microcontroller with with IC dedicated support software intended for use as a smart card IC.



The TOE consists of hardware and IC dedicated software. The hardware is based on a 32-bit CPU with ROM (Non-Volatile Read-Only Memory), EEPROM (Non-volatile Programmable Memory) and RAM (Volatile Memory). The hardware of the TOE also incorporates communication peripherals and cryptographic coprocessors for execution and acceleration of symmetric and asymmetric cryptographic algorithms. The IC dedicated software consists of boot code and a library of cryptographic services.

The TOE supports the following communication interfaces:

- ISO/IEC 7816 contact interface
- ISO/IEC 14443 contactless interface.

The TOE is delivered to a composite product manufacturer. The security IC embedded software is developed by the composite product manufacturer. The security IC embedded software is sent to Huada Company to be implemented in ROM and delivered back to the composite product manufacturer together with the TOE. The security IC embedded software is not part of the TOE.

4.16 Evaluation Conduct

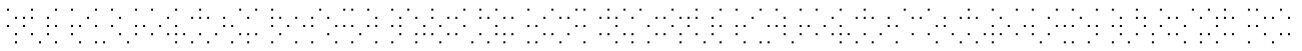
The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E [5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, 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]. Interpretations [7], [8], [9] are used.

SERTIT monitored the evaluation, which was carried out by Brightsight B.V. as Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR) [10] to SERTIT on 2 November 2016. As a result 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



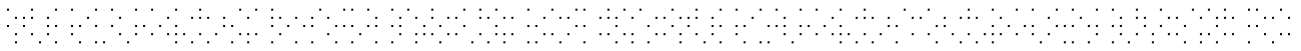
consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

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 EAL5 assurance package augmented with AVA_VAN.5 and ALC_DVS.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.5	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	TSF Internals
	ADV_TDS.4	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.5	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.2	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.3	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis



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

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target [1]. The results of this work were reported in the ETR [10] under the CC Part 3 [4] headings. The following sections note considerations that are of 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 [12].

5.3 Installation and Guidance Documentation

Installation procedures are described in detail in the supporting document [12].

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 [11], [12], [13], [14] for the TOE in order to ensure that the TOE is operated in a secure manner.

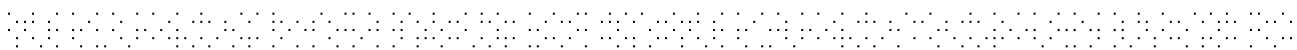
The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

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 design and implementation review on the TOE was done to identify weaknesses in the TOE that could potentially be exploited by attackers. A code review of the crypto library and boot code was also executed.
- Validation tests of security features performed in the ATE class are taken into account for the following vulnerability analysis.
- A vulnerability analysis based on the design and implementation review results and the validation test results of security features, was performed considering the well-known attacks from the "JIL Attack Methods for Smartcards and



Similar Devices" [7]. User guidance is also taken into consideration while analysing potential vulnerabilities.

- A penetration test plan is established based on the results of the vulnerability analysis.
- Practical penetration tests are performed according the penetration test plan.

5.6 Developer's Tests

The developer tests consist of four parts; 1) testing on engineering samples, 2) testing on wafers, 3) testing on simulation tools and 4) testing on an emulation board (FPGA).

- Testing on engineering samples:

Developer tests performed on engineering samples (cards or Dual-In-Line-Package ICs)

- Testing on wafers:

Developer tests performed on wafers

- Testing on simulation tools:

Developer tests were done on simulation tools in the chip development environment, which were used to verify the logical functions.

- Testing on the emulation board:

Developer tests were done on an emulation board (FPGA), mainly for the Crypto library.

5.7 Evaluators' Tests

The evaluator's responsibility for independent testing is required by the ATE_IND class. Since developer's testing procedures were found to be extensive and thorough, and developer's hardware testing tools are not generally available to allow reproduction of developer test cases in the evaluator's test lab, the choice was made to perform the evaluator independent testing by witnessing of the developer's test cases, using the developer's tools, at the premises of the developer. The evaluator used a sampling strategy to select developer tests to validate the developer's test results. The sampling strategy is as follows:

- At least one test is chosen for each SFR-enforcing subsystem
- If there are several tests mapped to a subsystem, the test(s) that verify security functions/mechanism will be preferred.

In addition to this, the evaluator has defined additional test cases, prompted by study of the developer's documentation. The test strategy is as shown below:

- Augmentation of developer testing for interfaces by varying parameters in order to more rigorously test the interface



- Performing positive and negative tests on selected Security Functions or Security Mechanisms.

These tests are also performed using the developer's tools at the premises of the developer. The evaluator witnessed the whole process of the tests.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR [10], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that the HED Secure Smart Card Chip CIU9872B_01 C11 with IC Dedicated Software meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 5+ augmented with AVA_VAN.5 and ALC_DVS.2 for the specified Common Criteria Part 2 extended functionality and Protection Profile BSI-CC-PP-0084-2014 V1.0, in the specified environment.

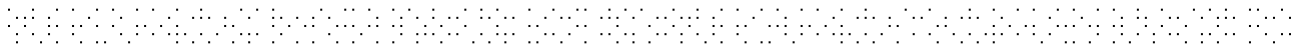
6.2 Recommendations

Prospective consumers of HED Secure Smart Card Chip CIU9872B_01 C11 with IC Dedicated Software 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 [11], [12], [13], [14] included in the evaluated configuration.

The above "Evaluation Findings" 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:

Type	Name	Version	Package
Hardware	CIU9872B_01	C11	module
Software	CMS	1.3	boot code in ROM
	Cryptographic library	1.2	Cryptographic library in ROM
	API library	1.1	API library binary file
Manuals	CIU9872B_01 C11 Operational User Guidance [11]	1.0	document
	CIU9872B_01 C11 Preparative Procedures [12]	1.0	document
	CIU9872B_01 C11 Crypto Library User Guide [13]	1.0	document
	CIU9872B_01 C11 Product Datasheet [14]	1.0	document

TOE Documentation

The supporting guidance documents evaluated were:

- [a] CIU9872B_01 C11 Operational User Guidance, Version 1.0, 20 Oct 2016 [11]
- [b] CIU9872B_01 C11 Preparative Procedures, Version 1.0, 20 Oct 2016 [12]
- [c] CIU9872B_01 C11 Crypto Library User Guide, Version 1.0, 20 Oct 2016 [13]
- [d] CIU9872B_01 C11 Product Datasheet, Version 1.0, 20 Oct 2016 [14]

Further discussion of the supporting guidance material is given in Section 5.3 "Installation and Guidance Documentation".

TOE Configuration

The TOE configuration used for testing was the same used for developer tests. This is described in chapter 5.6 of this report.