Certification Report

Secure Chip CIU9872B_01 V1.1 with IC Dedicated Software V1.0

Sponsor and developer:	***CEC Huada Electronic Design Co., Ltd.*** **Building C, CEC Network Security and Information Technology Base, South Region of Future Science Park, Beiqijia County, Changping District** **Beijing, 102209** **P. R. China**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2400082-01-CR**
Report version:	**1.1**
Project number:	NSCIB-**2400082-01**
Author(s):	**Haico Haak**
Date:	**06-01-2026**
Number of pages:	**13**
Number of appendices:	**0**

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.

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 Secure Chip CIU9872B_01 V1.1 with IC Dedicated Software V1.0. The developer of the Secure Chip CIU9872B_01 V1.1 with IC Dedicated Software V1.0 is CEC Huada Electronic Design Co., Ltd. located in Beijing, China 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 single chip microcontroller with IC Dedicated Software stored in Non-user Flash intended for use as a Security IC.

The IC hardware is a microcontroller incorporating a central processing unit, cryptographic coprocessors, sensors, test protection circuits, clock/reset/power management units and communication interfaces. The IC Dedicated Software consists of Chip Management System (CMS), Cryptographic and functional library and Lib file API library.

The main usage of the TOE is for financial cards, health cards, transportation cards, automotive and eUICC applications.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 06-01-2026 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 Secure Chip CIU9872B_01 V1.1 with IC Dedicated Software V1.0, 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 Secure Chip CIU9872B_01 V1.1 with IC Dedicated Software V1.0 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 EAL6 augmented (EAL6+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.1 (Basic flaw remediation).

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.

This document was re-issued on 06 January 2025 as version 1.1 to correct the versions of the AGD_OPE and AGD_PRE in section 2.5.

[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 Secure Chip CIU9872B_01 V1.1 with IC Dedicated Software V1.0 from CEC Huada Electronic Design Co., Ltd. located in Beijing, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	CIU9872B_01	V1.1
Software	CMS	V1.0
	Cryptographic and functional library	V1.0
	Lib file API library • Random Number API • Enhancing Chip Stability Solution API • Chip Unique Serial Number API • Chip Firmware Total Version API	V1.0

To ensure secure usage a set of guidance documents is provided, together with the Secure Chip CIU9872B_01 V1.1 with IC Dedicated Software V1.0. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.3.3.

2.2 Security Policy

The TOE is a single chip microcontroller with IC Dedicated Software stored in Non-user Flash intended for use as a Security IC.
The IC hardware is a microcontroller incorporating a central processing unit, cryptographic coprocessors, sensors, test protection circuits, clock/reset/power management units and communication interfaces. The IC Dedicated Software consists of Chip Management System (CMS), Cryptographic and functional library and Lib file API library.

The main usage of the TOE is for financial cards, health cards, transportation cards, automotive and eUICC applications.

Hence the TOE shall maintain：

- the integrity and the confidentiality of code and data stored in its memories and while processed in the device
- the memory access controlled by memory address and different chip modes
- the integrity, the correct operation and the confidentiality of security functionality provided by the TOE

This is ensured by the construction of the TOE and its security functionalities. The user of the TOE is the developer of the Embedded Software.

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 4.2 of the *[ST]*.

2.3.2 Clarification of scope

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the *[ST]*

2.4 Architectural Information

The TOE is a single chip microcontroller with IC Dedicated Software stored in Non-user Flash and documentation (see chapter 2.5) which describes the instruction set and the usage.

The TOE provides hardware for implementations of secure applications with:

- 32-bit microprocessor CPU with security mechanisms
- Security detectors including high and low temperature detectors, internal and external frequency detectors, internal and external voltage detectors, internal and external glitch detectors, electromagnetism detectors and light detectors
- Active shielding against physical attacks
- TDES/DES coprocessor (2 keys TDES mode) with countermeasures against SCA
- AES coprocessor (with 128 bits, 192 bits and 256 bits key size) with countermeasures against SCA
- Hardware coprocessor PKE which facilitated the RSA and ECC (with ECDH/ECDSA/BDH/EC-SDSA) implementations supporting large integer
- arithmetic operations of modular multiplication, modular addition, modular subtraction, modular exponentiation with countermeasures against SCA, point addition with countermeasures against SCA, point doubling and scalar multiplication with countermeasures against SCA. (These operations are used by software to implement the RSA and ECC (with ECDH/ECDSA/BDH/EC-SDSA) functions. Based on the RSA/ECC (with ECDH/ECDSA/BDH/EC-SDSA) function, the countermeasures for RSA/ECC (with ECDH/ECDSA/BDH/EC-SDSA) against attacks of SCA, DFA and FA are implemented by software.)
- Memory access control enabled by chip modes, EMMU and MGU
- Memory data encryption and address scrambling
- Data integrity check for RAM and FLASH
- Security-sensitive registers protection
- Bus mask
- RNG1 module serves with a highly reliable true random number generator, which is compliant with PTG.2 class of AIS20/31[2013] [20]
- RNG2 module serves with internal random numbers, which is only used for security mechanism (e.g. masking)
- Test mode protection
- Debug mode protection
- Self-test function
- SDL

The TOE contains the following hardware, but they are not claimed as security

functions.

- Chinese domestic cryptographic coprocessors
- CRC coprocessors
- TDES/DES coprocessor (DES mode) with countermeasures against SCA

The TOE provides software for implementations of secure applications with:

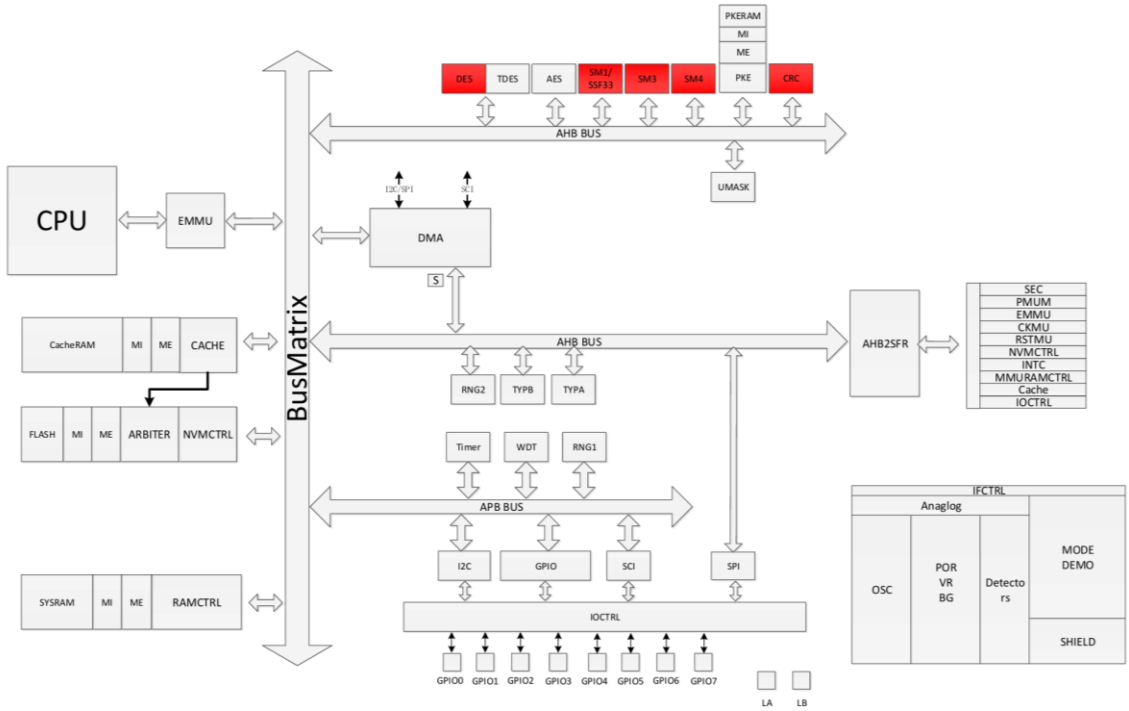
- CMS is for booting process controlling
- Cryptographic and functional library for the functions of 2 key TDES, AES (with 128 bits, 192 bits and 256bits key size), ECC (with ECDH/ECDSA/BDH/EC-SDSA) and private key functions of RSA (with key length from 512 bits to 4096 bits) in non-user Flash
- Lib file API library for the functions of a highly reliable true random number generation API interface with FA countermeasures cooperating with hardware which is compliant with PTG.2 class of AIS20/31[2013], a deterministic random number generation API with FA countermeasures which is compliant with DRG.3

The TOE contains the following cryptographic algorithms and functions, but they are

not claimed as security functions.

- Power Management API
- SHA Algorithm API
- Get Algorithm API Version API
- Flash Translation Layer API
- Enhancing Chip Stability Solution API
- Get Chip Unique Serial Number API
- Get Chip Firmware Total Version API
- APIs in ECC library except ECDH/ECDSA/BDH/EC-SDSA
- X25519 Algorithm API
- Chinese domestic cryptographic algorithms
- APIs in RNG library except the true/deterministic random number generation APIs
- 3key TDES algorithm API
- DES Algorithm API not claimed as security function but implemented SCA, DFA and FA countermeasures
- APIs in RSA library except the private key calculation APIs

The architecture, originating from the Security Target *[ST]* of the TOE can be depicted as follows:



2.5 Documentation

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

Identifier	Version
CIU9872B_01 V1.1 with IC Dedicated Software V1.0_Crypto and Function Library User Guide	1.0
CIU9872B_01 V1.1 with IC Dedicated Software V1.0_Product Datasheet	1.0
CIU9872B_01 V1.1 with IC Dedicated Software V1.0_Operational User Guidance (AGD_OPE)	1.1
CIU9872B_01 V1.1 with IC Dedicated Software V1.0_Preparative Procedures (AGD_PRE)	1.1

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 TOE is tested thoroughly by the developer. The testing is performed in four categories:

- Hardware: simulation tests, sample tests, wafer tests, qualification and characterization tests;
- CMS: simulation sample: simulation tests, emulation test, sample tests, wafer tests
- Cryptographic and functional library: simulation tests, emulation test, sample tests, wafer tests
- Lib File API library: simulation sample: simulation tests, emulation test, sample tests, wafer tests

All TSFIs, subsystems and modules are tested.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- 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-AAPS].
- 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.

The total test effort expended by the evaluators was spent between July 2025 and August 2025, with 29 man-weeks in total for testing and reporting. During that test campaign, 4% of the total time was spent on Physical Attacks, 0% of the total time was spent on Overcoming Sensors and Filters, 24% of the total time was spent on Perturbation Attacks, 10% on Retrieving Keys with FA, 58% on Side Channel Attacks – Non-invasive retrieving of secret data, 0% of the total time was spent on Exploitation of Test Features, 4% on Attacks on RNG, 0% of the total time was spent on Ill-formed Java Card Applications and 0% of the total time was spent on Software Attacks

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*.

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.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities.

For composite evaluations, please consult the *[ETRfC]* for details.

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of seven Site Technical Audit Reports.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Secure Chip CIU9872B_01 V1.1 with IC Dedicated Software V1.0.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. To support composite evaluations according to *[COMP]* a derived document *[ETRfC]* was provided and approved. 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 Secure Chip CIU9872B_01 V1.1 with IC Dedicated Software V1.0, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 6 augmented with ALC_FLR.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profile *[PP]*.

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: SM1, SM2, SM3, SM4 and SSF33, which are out of scope as there are no security claims relating to these.

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 Security target of Secure Chip CIU9872B_01 V1.1 with IC Dedicated Software V1.0 Version 1.2, 19 December 2025 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

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

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining (a block cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SPA/DPA	Simple/Differential Power Analysis
TOE	Target of Evaluation
TRNG	True Random Number Generator

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
[ETR]	Evaluation Technical Report “HED Secure Chip CIU9872B_01 V1.1 with IC Dedicated Software V1.0” – EAL6+, 24-RPT-1332, Version 5.0, 19 December 2025
[ETRfC]	Evaluation Technical Report for Composition “HED Secure Chip CIU9872B_01 V1.1 with IC Dedicated Software V1.0” – EAL6+, 25-RPT-1278, Version 3.0, 19 December 2025
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2.1, February 2024
[JIL-AMS]	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]	Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014
[ST]	Security target of Secure Chip CIU9872B_01 V1.1 with IC Dedicated Software V1.0 Version 1.2, 19 December 2025
[ST-lite]	Security target Lite of Secure Chip CIU9872B_01 V1.1 with IC Dedicated Software V1.0 Version 1.2, 19 December 2025
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)