

Certification Report

Secure Chip CIU9872B_01 V1.0 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-2400053-01-CR**

Report version: **1**

Project number: **NSCIB-2400053-01**

Author(s): **Haico Haak**

Date: **09 May 2025**

Number of pages: **12**

Number of appendices: **0**

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

CONTENTS

Foreword	3
Recognition of the Certificate	4
International recognition	4
European recognition	4
1 Executive Summary	5
2 Certification Results	6
2.1 Identification of Target of Evaluation	6
2.2 Security Policy	6
2.3 Assumptions and Clarification of Scope	6
2.3.1 Assumptions	6
2.3.2 Clarification of scope	7
2.4 Architectural Information	8
2.5 Documentation	8
2.6 IT Product Testing	8
2.6.1 Testing approach and depth	8
2.6.2 Independent penetration testing	9
2.6.3 Test configuration	9
2.6.4 Test results	9
2.7 Reused Evaluation Results	9
2.8 Evaluated Configuration	9
2.9 Evaluation Results	9
2.10 Comments/Recommendations	10
3 Security Target	11
4 Definitions	11
5 Bibliography	12

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

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

Recognition of the Certificate

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

International recognition

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

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

European recognition

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

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

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Secure Chip CIU9872B_01 V1.0 with IC Dedicated Software V1.0. The developer of the Secure Chip CIU9872B_01 V1.0 with IC Dedicated Software V1.0 is CEC Huada Electronic Design Co., Ltd. located in Beijing, P.R. 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 the IC hardware with IC Dedicated Software which is stored in ROM and Non-user FLASH and related documentations which describes the instruction set and the TOE usage. It is intended for use as a security IC as described in [PP].

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 09-05-2025 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security [NSCIB].

The scope of the evaluation is defined by the security target [ST], which identifies assumptions made during the evaluation, the intended environment for the Secure Chip CIU9872B_01 V1.0 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 V1.0 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.

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 V1.0 with IC Dedicated Software V1.0 from CEC Huada Electronic Design Co., Ltd. located in Beijing, P.R. China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	CIU9872B_01	V1.0
Software	CMS	V1.0
	Cryptographic and functional library	V1.01
	Lib file API library	V1.0

To ensure secure usage a set of guidance documents is provided, together with the Secure Chip CIU9872B_01 V1.0 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 TOE is available in one configuration with IC Dedicated Software. The IC hardware is a microcontroller incorporating a central processing unit (ARM SC 000 CPU), 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 TOE controls the access to memory areas and resources in different chip modes.

The TOE is a Security Integrated Circuit Platform for various operating systems and applications, mainly banking and finance.

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 evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

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

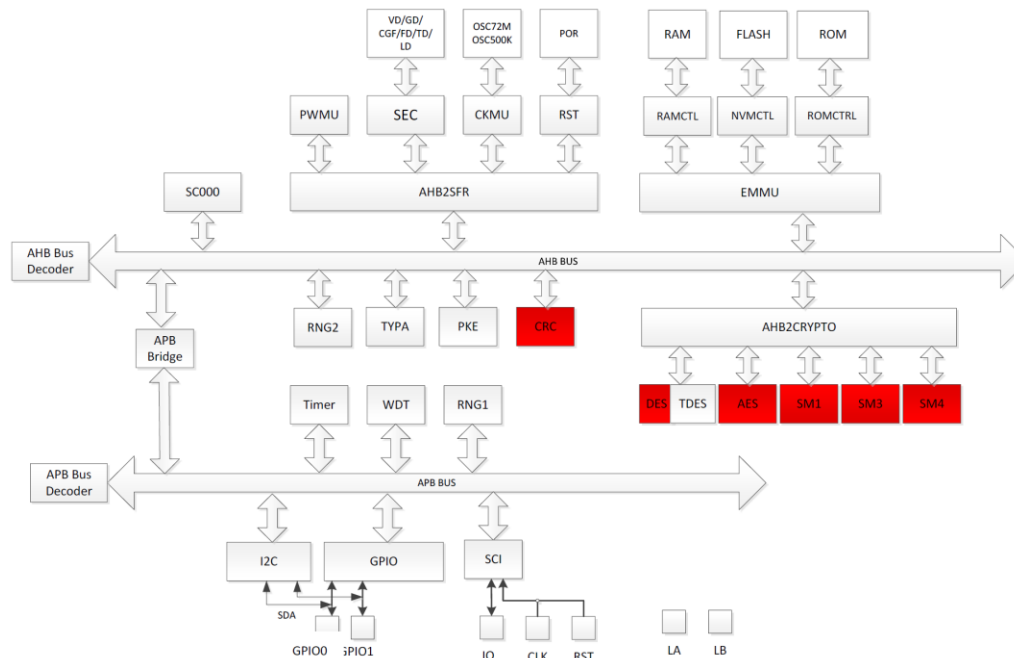
- Chinese domestic cryptographic coprocessors: SM1, SM3 and SM4
- CRC coprocessors (CRC16)
- TDES/DES coprocessor (DES mode) with countermeasures against SCA
- AES coprocessor with countermeasures against SCA

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
- Chinese domestic cryptographic algorithms (SM1, SM2, SM3 and SM4)
- 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
- AES Algorithm API
- APIs in RSA library except the private key calculation APIs

2.4 Architectural Information

The TOE architecture, originating from the Security Target [ST], can be depicted as follows (for red parts see 2.3.2 Clarification of scope):



2.5 Documentation

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

Identifier	Version
CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Operational User Guidance (AGD_OPE)	V1.6
CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Preparative procedures (AGD_PRE)	V1.3
CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Product Datasheet	V1.3
CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Crypto and Function Library User Guide	V1.3

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

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

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

2.6.2 Independent penetration testing

The total test effort expended by the evaluators was 6 weeks. During that test campaign, 0% of the total time was spent on physical attacks, 0% overcoming sensors and filters, 24% perturbation attacks, 0% retrieving keys with FA, 66% side-channel attacks, 0% exploitation of test features, 10% attacks on RNG, 0% ill-formed Java Card application, 0% software attacks, and 0% application isolation penetration tests.

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 a number of Site Technical Audit Reports.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Secure Chip CIU9872B_01 V1.0 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, and Site Technical Audit Report for the site [STAR-HHGrace]². 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".

² The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

Based on the above evaluation results the evaluation lab concluded the Secure Chip CIU9872B_01 V1.0 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 and SM4, 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 V1.0 with IC Dedicated Software V1.0, Version 0.5, 2024-01-15 [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)
CBC-MAC	Cipher Block Chaining Message Authentication Code
DES	Data Encryption Standard
DFA	Differential Fault Analysis
ECB	Electronic Code Book (a block-cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMA	Electromagnetic Analysis
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
JIL	Joint Interpretation Library
MAC	Message Authentication Code
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash 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
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[ETR]	Evaluation Technical Report "Secure Chip CIU9872B_01 V1.0 with IC Dedicated Software V1.0" – EAL6+, 24-RPT-738, Version 4.0, 24-April 2025
[ETRFc]	Evaluation Technical Report for Composition "Secure Chip CIU9872B_01 V1.0 with IC Dedicated Software V1.0" – EAL6+, 24-RPT-1544, Version 2.0, 24-April 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 V1.0 with IC Dedicated Software V1.0, Version 0.5, 2024-01-15
[ST-lite]	Security target Lite of Secure Chip CIU9872B_01 V1.0 with IC Dedicated Software V1.0, Version 1.0, 2024-12-11
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
[STAR-HHGrace]	Site Technical Audit Report – HHGrace Shanghai Fab1, 24-RPT-1373, Version 1.0, 15 November 2024

(This is the end of this report.)