EUCC Certification Report

CIU98N70 Secure Element 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:	***Serma Safety and Security*** **14, rue Galilée – CS10071** **33608 Pessac** **France**
Report number:	**EUCC-3110-2026-2500106-01 Certification Report**
Report version:	**1.5**
Project number:	**EUCC-2500106-01**
Author(s):	**Wim Ton, TrustCB B.V.** **contact: eucc@trustcb.com**
Date:	**18 August 2026**
Number of pages:	**20**
Number of appendices:	**0**

CONTENTS

Foreword

The Common Criteria-based European Cybersecurity Certification Scheme (EUCC) is a certification scheme created under the Cybersecurity Act (CSA), Regulation (EU) 2019/881 of 17 April 2019.

The EUCC is described by Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

The Dutch implementation of the CSA is regulated in Dutch law in the 'Uitvoeringswet cyberbeveiligingsverordening' (UITVW). In this law the role of NCCA is assigned to the Dutch Authority for Digital Infrastructure (RDI), which is part of the Ministry of Economic Affairs.

TrustCB B.V. has been licensed by the RDI as a Certification Body (CB) for the task of ISO/IEC 17065 Certification Activities up to and including CSA assurance level high for ICT security products, as well as for protection profiles. Part of the procedure is the technical examination (evaluation) of the product, protection profile according to the NP002 EUCC processes published by the Dutch NCCA.

Evaluations of ICT products are performed by an IT Security Evaluation Facility (ITSEF) licensed by the Dutch NCCA as a CAB for ISO/IEC 17025 Evaluation Activities, with scope aligning to the requested Evaluation Assurance Level of the Object for the evaluation, referred to as the Target of Evaluation (TOE) in this report.

By awarding an EUCC certificate as a Common Criteria certificate, TrustCB B.V. asserts that the ICT product complies with the security requirements specified in the associated 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 security target is a requirements specification document that defines the scope of the evaluation activities.

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

.

Recognition of the Certificate

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of published 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.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the CIU98N70 Secure Element V1.0, identified in this document as either the ICT Product or as the Target of Evaluation (TOE).

The developer of the ICT Product is CEC Huada Electronic Design Co., Ltd. located in Beijing, China and they also act as the sponsor of the evaluation and certification.

This Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the ICT product for their particular requirements. The TOE is a Security Integrated Circuit Platform for operating systems and applications with high security requirements.

The TOE incorporates an ARM Cortex M35P processor augmented with dedicated coprocessors for symmetric cryptography, public-key cryptography, and random number generation.

On-chip memories are Flash memory, ROM and RAMs. The ROM contains the IC dedicated software for factory testing, program upload, and the flash memory drivers. The flash memory contains a cryptographic library

In addition, the hardware embeds sensors which ensure the proper operating conditions of the device such as EMFI detector, light sensing and other security functionality.

Memory encryption, checksum, and masking mechanisms are implemented to preserve the confidentiality and the integrity of the stored data. The IC hardware is shielded against physical attacks.

The TOE claims conformance to the following Protection Profile *[PP]*:

- Security IC Platform Protection Profile, Version 1.0, 13.01.2014 registered under the reference BSI-CC-PP-0084-2014

A certification procedure has been conducted on the TOE by TrustCB B.V., in accordance with the provisions of the EUCC as described in Commission implementing regulation (EU) 2024/482 of 31 January 2024, amended by (EU) 2024/3144 of 18 December 2024 and (EU) 2025/2462 of 8 December 2025.

The successful completion of the certification procedure resulted in TrustCB issuing an EUCC certificate. The certificate identifier is **EUCC-3110-2026-2500106-01**, dated 18-08-2026 and with a 5-year validity.

The evaluation of the TOE was performed by Serma Safety & Security located in Pessac, France. The evaluation was completed on 2026-06-08 with the issuance of the evaluation technical report *[ETR*]. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CC:2022, R1 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 R1 *[CC]* (Parts 1, 2, 3, 4, 5).

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ICT Product, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the a multi assurance package as follows:

Global conformance: EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5 and ALC_FLR.2.

Sub-TSF for memory access control policy: EAL6 augmented with ALC_FLR.2

The AVA_VAN level applied during the evaluation was AVA_VAN.5 This assurance level is recognised by article 52 of [CSA] as ‘high’.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

Consumers of this ICT Product 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.

TrustCB B.V., as the Certification Assessment Body licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC high certification activities, declares that the product will be listed on the ENISA EU Cybersecurity Certificates list and that the evaluation meets all the conditions for international recognition of Common Criteria Certificates.

Note that the certification results apply only to the specific version of the product as evaluated.

2 ICT Product details

2.1 Identification of the ICT Product

The Target of Evaluation (TOE) for this evaluation is the ICT product CIU98N70 Secure Element 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	CIU98N70_SE	V1.0
Security IC Dedicated Software	Chip Management System	V1.0
	Cryptographic and functional library	V1.0
	Lib file API library (NVM, RNG, version)	V1.0

Additional requirements for the operational environment of the certified ICT product are described in section 4.2 of the *[ST]*.

To ensure secure usage, a set of guidance documents is provided with the ICT Product. For details, see section 2.6 of this report, “Supplementary Cybersecurity Information.

2.2 Contact information related to the evaluation of the ICT Product

Holder of the EUCC Certificate

The name and contact information provided for the holder of the issued Certificate associated with this Certification Report are as follows:

Organisation name:	CEC Huada Electronic Design Co., Ltd.
Address:	Building C, CEC Network Security and Information Technology Base, South Region of Future Science Park Beiqijia County, Changping District, Beijing, 102209 PR China
Certified product contact details	zhouyc@hed.com.cn

Developer of the certified ICT Product

ICT product developer	CEC Huada Electronic Design Co., Ltd.

Identification of CAB

The Certification Assessment Body for this ICT Product is TrustCB B.V located in Hoofddorp, The Netherlands.

Identification of ITSEF

Evaluation and testing for this ICT Product was performed by following ITSEF:

Serma Safety & Security, in Pessac, France

Responsible national cybersecurity certification authority

Dutch Authority for Digital Infrastructure (RDI)

2.3 Security Policy and Services

2.3.1 Security services

IC with crypto library

The following cryptographic primitives are supported and included within the TSF:

- 3DES for encryption/decryption (CBC and ECB)
- AES for encryption/decryption (CBC, ECB, GCM and Counter Mode)
- RSA and RSA-CRT for decryption and signature generation and key generation
- Elliptic curve cryptography (ECC)
- X25519 cryptography
- TRNG
- DRNG

The IC also supports SHA-1, SHA-2, and the Chinese domestic algorithms: SM2, SM3, SM4, SM9 and ZUC, but these are not subject of this certification.

The TOE maintains:

- the integrity and confidentiality of code and data stored in its memories;
- the different CPU modes with the related capabilities for configuration and memory access;
- the integrity, the correct operation and the confidentiality of security functionality provided by the TOE.
- Different functionality determined by the TOE life cycle state.

This is ensured by the construction of the TOE and its security functionality.

- memory management control using a “Trustzone” and an EMMU.
- an ISO/IEC 7816 contact interface with UART.
- An interface to an NFC controller

In addition, several security mechanisms are implemented to ensure proper operation as well as integrity and confidentiality of stored data.

2.3.2 Vulnerability management

The following vulnerability policy has been identified as applicable to the CIU98N70 Secure Element V1.0

Document reference: Product Security Vulnerability Management Procedure, version A02, 2025-10-23, summarized:

Prior to mass production, HED implements a Bug Management Process using URTracker to document, track, resolve, and archive issues.

For vulnerabilities identified during production, the Product Security Incident Response Team (PSIRT) will promptly notify the product manager of the ongoing project.

The sources of vulnerability discovery fall into three categories:

• Built in test: the vulnerabilities were identified by the HED's internal R&D department during product business testing.

• External submission: to receive vulnerabilities submitted by external entities or individuals, including customers and security research organizations.

• Public disclosure: the vulnerabilities were disclosed through public channels such as social media, standards organizations, cryptographic research associations, and academic conferences.

After receiving a vulnerability report, the following steps will be taken:

• PSIRT first verifies the completeness of vulnerability report content. If information is missing or descriptions are unclear, a request for supplementation must be submitted within 24 hours to the reporter for content revision. The request should specify information requirements and clearly highlight both confirmed and ambiguous details.

• For reports with complete information and clear descriptions, the R&D department conducts a preliminary evaluation of the vulnerability content to determine if it is a valid vulnerability. If the evaluation

is negative, a closure notice must be sent, including the technical assessment results and the basis for the vulnerability determination.

• For valid vulnerability reports, a confirmation notice will be sent to the reporter within 3 working days. The notice includes the unique vulnerability report number, next steps, security communication guidelines, and other important notes.

Vulnerabilities requiring further investigation or deemed valid should be validated, while those considered invalid will still have their analysis process and conclusions documented.

Nature and effect of the vulnerability is verified as follows:

For vulnerabilities requiring further investigation or deemed valid, the PSIRT's technical experts conduct verification.

• Verification personnel must employ technical means to confirm the authenticity and existence of vulnerabilities. If a vulnerability is identified, they must specify its exact module, trigger conditions, exploitation methods, and other relevant details.

The verification process will be thoroughly documented. Simultaneously, the PSIRT must immediately complete the Information Security Incident Report Form and notify the product manager of the HED"s ongoing project regarding the vulnerability.

After preliminary evaluation, the PSIRT assigns a unique number to each vulnerability report requiring further investigation or identified as a valid vulnerability, ensuring traceability in its collection and processing. The numbering format is as follows:

• VULN is a fixed prefix for vulnerability numbering, used to distinguish it from other types of numbering.

• The product model is the target model for vulnerability reporting, used to distinguish vulnerabilities across different products.

• Version is the target product version number for vulnerability reports, used to distinguish vulnerabilities across different versions.

• The date is when the vulnerability report was submitted

• The two-digit serial number is a supplementary vulnerability report number to distinguish reports submitted on the same date, version, and product.

The PSIRT should identify the numbered vulnerability report, create vulnerability database entries according to the 8-vulnerability database management requirements, and update the Product Security Vulnerability database.

Then, the vulnerability is released after PSIRT review and approval by the Chief Information Security Officer, and the recipients include customers and regulatory authorities. The technical support department delivers it to customers, and PSIRT delivers it to regulatory authorities (e.g. Certification Bodies).

The vulnerability release must notify customers at least 72 hours prior to public disclosure, with full efforts made to mitigate their risks.

The PSIRT monitors the entire vulnerability remediation process to track progress in real time. The focus is on monitoring within one week after vulnerability patching to observe the product's operational status and check for any recurrence of vulnerabilities or new anomalies.

A statistical analysis of vulnerability Handling will be carried out regularly to summarize experience and lessons.

2.3.3 Assurance Continuity policies

This is a new product certification. An assurance continuity policy was not provided.

2.3.4 Lifecycle management processes and production facilities

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

2.3.5 Patch management process

Not applicable to this evaluation

2.4 Assumptions and Clarification of Scope

2.4.1 Assumptions

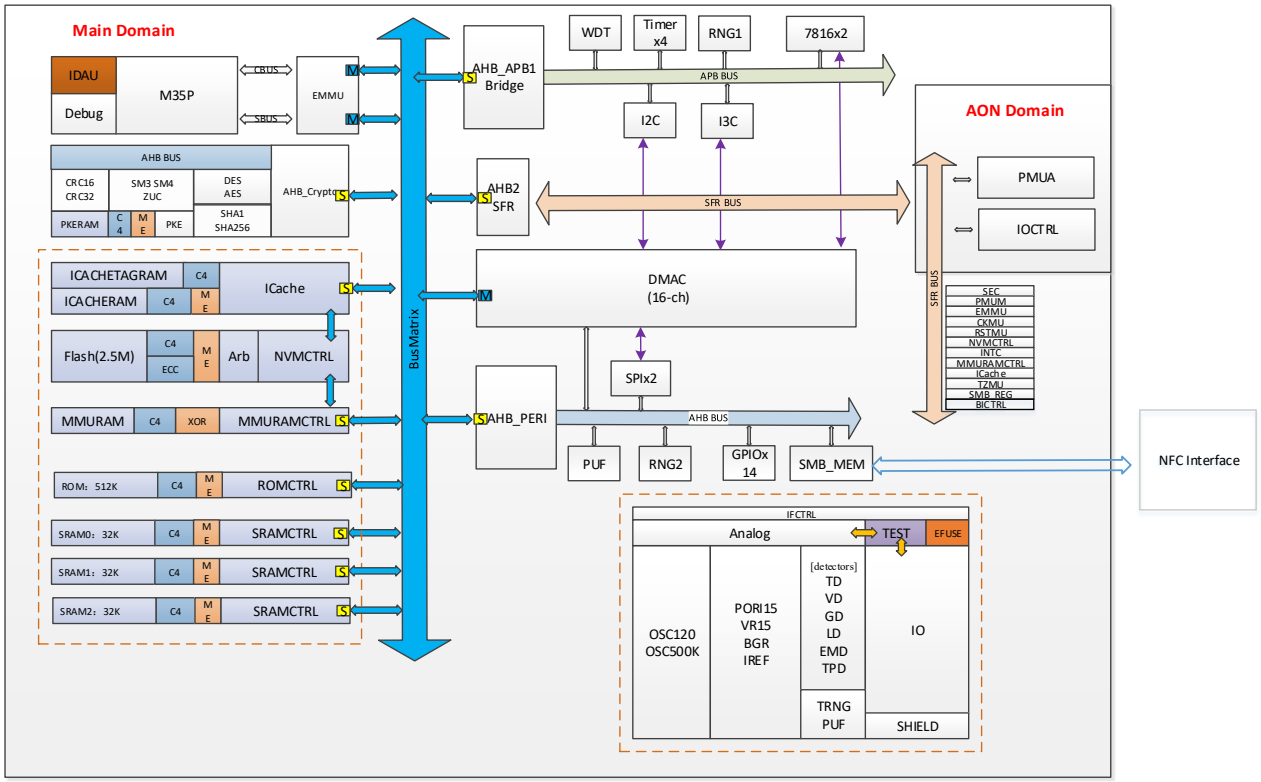
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.4.2 Clarification of scope

Considering all Assumptions above, the evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Organisational Security Policies for the ICT Product are stated to be the same as in [PP_0084], with one additional OSP as detailed in section 3.3 of the [ST]. Threats are presented in Section 3.2 of [ST] and are the threats as presented in the [PP_0084], due to the strict conformance of the TOE to [PP_0084]

2.5 Architectural Information



2.6 Supplementary Cybersecurity Information

The following website link was provided for the CIU98N70 Secure Element V1.0 supplementary cybersecurity information as referred to in Article 55 of Regulation (EU) 2019/881: https://www.hed.com.cn/en/nfcxp

This link provides further details on

- Guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the CIU98N70 Secure Element V1.0.
- The period during which the CIU98N70 Secure Element V1.0 security support will be offered to end users, in particular as regards the availability of cybersecurity related updates, is stated as 5 years aligned with the validity of the issued EUCC certificate.

- Contact information and accepted method for receiving vulnerability information from end users and security researchers for the CIU98N70 Secure Element V1.0, including the public key for confidential mail exchange A vulnerability report should contain:
    - Product and version information.
    - A technical description of the operation and results being performed, as detailed as possible.
    - Example code for testing or demonstrating vulnerabilities.
    - Identified risk assessment details, including the risk level of the assessment results (critical, high, medium, low).
    - The time and date of discovery.
    - Contact information for the vulnerability reporter.
- An online repository listing publicly disclosed vulnerabilities related to the CIU98N70 Secure Element V1.0 and to any relevant cybersecurity advisories.

Note: The following documentation, guidance and recommendations, is provided with the product by the developer to the customer to assist end users with the secure configuration, installation, deployment, operation and maintenance of the CIU98N70 Secure Element V1.0:

Identifier	**Version**
CIU98N70 Secure Element V1.0 Product Datasheet	V1.2
CIU98N70 Secure Element V1.0 Crypto and Function Library User Guide	V1.2
CIU98N70 Secure Element V1.0 Operational User Guidance	V1.3
CIU98N70 Secure Element V1.0 Preparative Procedures	V1.2

3 Evaluation summary

3.1 Identification of used assurance components

This was a multi-assurance evaluation. The multi assurance components used in the product testing were applied as follows:

- **Global conformance: EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5 and ALC_FLR.2,**
- **Sub-TSF for memory access control policy: EAL6 augmented with ALC_FLR.2**

as defined by, and detailed in, [CC] and [CEM].

3.2 EUCC State of the Art documents and Protect Profiles

EUCC state-of-the-art documents *[SotA Documents]* were applied as referenced in the Bibliography.

The following Protection Profiles was applied:

Security IC Platform Protection Profile with Augmentation Packages, as certified under the reference BSI-CC-PP-0084-2014 by CAB Bundesamt für Sicherheit in der Informationstechnik (BSI) ICT Product Testing

3.3 EUCC State of the Art documents and Protect Profiles

The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

3.3.1 Testing approach and depth

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

The evaluators witnessed a selection of the developer tests.

The evaluators conducted a conformance test for the cryptographic algorithms.

The evaluators tested the statistical properties of the TRNG and the DRNG,

3.3.2 Independent penetration testing

By analysis of the code and the documentation, the evaluator defined 29 testcases to verify that vulnerabilities are not exploitable with an attack potential of "beyond high".

The evaluator used an IR laser to the backside of the TOE for fault injection.

The evaluator used an EM probe for side channel analysis.

The total test effort expended by the evaluators was 142 weeks. During that test campaign, 59% of the total time was spent on Perturbation attacks, 37% on side-channel testing, and 4% on physical tests.

3.3.3 Test configuration

The tests used the TOE in a WLCSP mounted on a special PCB. For laser fault injection, the epoxy was removed from the backside of the chip.

The chips were loaded with a special operation system that allowed the evaluators to load test programs and to manipulate all special function registers.

3.3.4 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.

3.4 ICT Product evaluation

The evaluation was performed referencing ISO/IEC 18045, Common Evaluation Methodology, and the EUCC State of the Art documents listed in section 6 of this report,*[SotA_XXX].*

Further security evaluation criteria were not applied in this evaluation

3.4.1 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 5 Site Technical Audit Reports.

No sites have been visited as part of this evaluation.

3.4.2 Evaluated Configuration

The TOE is defined uniquely by its name and version number CIU98N70 Secure Element V1.0.

The detailed version of the chip and software can be found the "Factory Code Region" as described in in table 2 of the [*ST*]. Chapter 3.2 of the "Operational User Guidance" gives the address of these data.

3.4.3 Assessment against each assurance requirement

ASE

Security Target evaluation	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.1
Extended components definition	ASE_ECD.1
Security requirements	ASE_REQ.1
TOE summary specification	ASE_TSS.1

The findings are well-documented and internally consistent, demonstrating a thorough understanding of the Security Target [ST] and its components. The TOE introduction, conformance claim, security problems, security objectives, security requirements, TOE summary specification are appropriately addressed, and the TOE description is accurate and adequate for the evaluation level. Consequently, the ASE activities fulfil the assurance requirements for EAL5 and EAL6 . No issues or deviations were identified.

ADV

Development	
Architecture	ADV_ARC.1
Functional specification	ADV_FSP.1
Implementation representation	ADV_IMP.2
TSF Internals	ADV_INT.3

Security Policy Model (for memory access control)	ADV_SPM.1
TOE Design Specification	ADV_TDS.5

The evaluation has demonstrated that the developer's evidence meets ADV specified requirements. The TOE model is complete, clearly showing all interfaces (TSFI/non-TSFI), user roles, and relations, with explanations on completeness and tracing requirements met. The subsystem/module level model is sensible, useful, and shows TSFIs and subsystem/module decomposition. The security architecture is thoroughly explained, design compliance rationale is complete and coherent, and necessary evidence is extracted per alternative approach. The evaluator confirmed why the TSF is well structured. SFRs were inspected, with findings mapped to the implementation representation in the evaluation meetings. The internal structure has a high level of cohesion, and low levels of coupling and complexity. Accordingly, the ADV activities meet the assurance requirements for EAL6 for memory access control and EAL5 augmented with ADV_IMP.2, ADV_INT.3, and ADV_TDS.5 for the other TSFs, with no issues or deviations identified.

AGD

Guidance documents	
Operational user guidance	AGD_OPE.1
Preparative procedures	AGD_PRE.1

The evaluation has demonstrated that the guidance documentation is clear, complete, and sufficient to support the secure acceptance, installation, configuration, and operation of the TOE within its intended environment by its user roles. The guidance effectively helps prevent common misconfigurations and promotes correct usage. Therefore, the AGD activities fulfil the assurance requirements for EAL5 and EAL6, with no issues or deviations identified.

ALC

Life cycle support	
Labelling of the TOE	ALC_CMC.5
TOE CM coverage	ALC_CMS.5
Developer Security	ALC_DVS.2
Flaw Remediation	ALC_FLR.2
Lifecycle Definition	ALC_LCD.1
Tools and techniques	ALC_TAT.3

The evaluation has demonstrated that the developer's evidence meets ALC specified. The CI-list was comprehensive and uniquely identified all configuration items, with clear identification of the developer. The CM documentation effectively described unique identification methods, a CM plan for development, procedures for accepting modified or new CIs, and the CM system was operated in accordance with the CM plan to maintain all configuration items by automated means. Delivery procedures were well-documented, ensuring security during TOE distribution. The developer security is defined by the STARS. Flaw remediation procedures were comprehensive, including methods for receiving reports, tracking flaws, providing corrective actions, and updating users. Accordingly, the ALC activities satisfy the assurance requirements for EAL5 augmented with ALC_CMC.5 , ALC_DVS.2, ALC_FLR.2, and ALC_TAT.3 and for EAL6 augmented with ALC_FLR.2, with no issues or deviations identified.

ATE

Tests	
Test coverage	ATE_COV.3
Test Depth	ATE_DPT.3
Functional testing	ATE_FUN.2
Independent testing	ATE_IND.1

The evaluation has demonstrated that the developer's evidence for ATE requirements meets all specified requirements. The testing approach used by the developer effectively covered the TSFIs. The developer's

rationale for testing all TSFIs was presented and verified. The developer test results show that for all tests either the result was pass or a proper rationale was given why the test failed. For the evaluator's independent testing, the overall approach for test selection, goals for the witnessing session, and independent test plan were clearly outlined. The evaluator's testing results showed that all sampled tests were passed. Accordingly, the ATE activities satisfy the assurance requirements for EAL5 augmented with ATE_COV.3, ATE_DPT.3, and ATE_FUN.2 and for EAL6, with no issues or deviations identified.

AVA

Vulnerability assessment	
Vulnerability analysis	AVA_VAN.5

The evaluator conducted a vulnerability analysis based on the ADV documents. The results were checked which vulnerabilities could be exploited by an attacker with a beyond high attack potential. For the possibly exploitable vulnerabilities, the evaluator designed and conducted 66 tests. When adhering to the guidance, none of the identified vulnerabilities are exploitable

3.5 Results of the evaluation

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report, other evaluator documents, developer documentation *[DEV_DOCS]* and Site Technical Audit Report(s) for the site(s) *[STAR]* [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**".

Based on the above evaluation results the evaluation lab concluded the CIU98N70 Secure Element V1.0, to be **CC:2022 revision 1 Part 2 extended, CC:2022 revision 1 Part 3 conformant**, at an assurance level recognised by article 52 of [CSA] as 'high', with **AVA_VAN.5** and to meet the multi-assurance requirements as follows:

- **Global Conformance: EAL 5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, and AVA_VAN.5, ALC_FLR.2**.
- **Sub-TSF for memory access control policy: EAL6 augmented with ALC_FLR.2**

This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

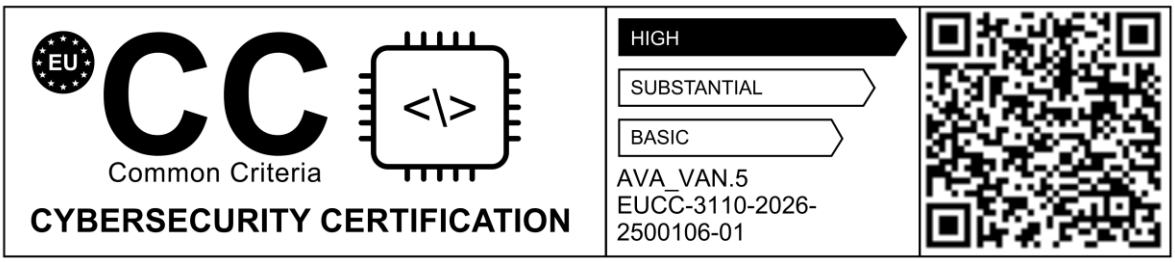
The Security Target claims 'strict' conformance to the Protection Profile *[PP]*.

3.6 Certificate information and scheme label

A Certificate has been issued recognising this evaluation result as follows:

Unique identifier: EUCC-2110-2026-2500106-01

Date of issuance: 18-08-2026 and with a validity period of **5 years**.



[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.

3.7 Comments/Recommendations

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE.

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in chapter 5 of theCIU98N70 Secure Element V1.0 Operational User Guidance. Therefore, it is vital to maintain meticulous adherence to the user guidance of both the software and the hardware part of the TOE.

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: SM2, SM3, SM4, SM9, and ZUC

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).

4 Security Target

The Security target of CIU98N70 Secure Element V1.0, v1.4 *[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]*.

5 Glossary

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

IT	Information and communication technologies product as defined by [EUCC]
ITSEF	IT Security Evaluation Facility
EUCC	European Cybersecurity Certification Scheme [EU-EUCC], created under the Cybersecurity Act [EU-CSA] and detailed in Commission Implementing Regulation (EU) 2024/482
PP	Protection Profile
SotA	EUCC State-of-the-Art document
TOE	Target of Evaluation; the object of the certification activity described by this report
API	Application Program Interface
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
EMMU	Enhanced Memory Management Unit
IC	Integrated Circuit
JIL	Joint Interpretation Library
LAN	Local Area Network
MAC	Message Authentication Code
NFC	Near Field Communication
NVM	Non-Volatile Memory
DRNG	Deterministic Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SPA/DPA	Simple/Differential Power Analysis

TRNG	True Random Number Generator
WLCSP	Wafer Level Chip Scale Package

6 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, CC:2022 Parts 1, 2, 3, 4 and 4, Revision 1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022
[CC-ERRATA]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2
[CC2022_TP]	Transition Policy to CC:2022 and CEM:2022
[DEV_DOCS]	CIU98N70 Product Development Project Configuration Item List-v1.0.xlsx
	CIU98N70 Secure Element V1.0 Crypto and Function Library User Guide, v1.2, 21 May 2026
	CIU98N70 Secure Element V1.0 Product Datasheet, v1.2, 27 Feb 2026
	CIU98N70 Secure Element V1.0 Operational User Guidance, v1.3, 05 June 2026
	CIU98N70 Secure Element V1.0 Preparative Procedures, v1.2, 21 May 2026
[ETR]	Evaluation Technical Report IC-N70 Project, v1.2, 08 June 2026
[ETRfC]	Evaluation Technical Report Lite for composition IC-N70 Project, v1.2, 08 June 2026
[EU-CSA]	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[EU-EUCC]	COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
[EU-EUCC-amdt.1]	Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
[EU-EUCC-amdt.2]	Commission Implementing Regulation (EU) 2025/2462 of 08 December 2025 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
[PP_0084]	Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014
[SotA_AAPS]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of Attack Potential to Smartcards and Similar Devices, Version 2, February 2025
[SotA ADV_SPM]	EUCC STATE-OF-THE-ART DOCUMENT ADV_SPM.1 interpretation for CC:2022 transition Version 1.1, October 2025
[SotA_CC_IC]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of Common Criteria to integrated circuits Version 2.0, December 2024
[SotA_COMP]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Composite product evaluation and certification for CC: 2022 Version 1, February 2025

[AIS20/31]	A Proposal for: Functionality classes for random number generators, 2.0, 2011-09
[ST]	Security target of CIU98N70 Secure Element V1.0, v1.4, 5 June 2026
[ST-lite]	Security target Lite of CIU98N70 Secure Element V1.0, v1.4, 5 June 2026
[ST-SAN]	Sanitization of a security target for publication, [EUCC] Annex V section V.2
	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)