Certification Report

Goodix Security Chip GSE20 Series with IC Dedicated Software, version A1.1 D0

Sponsor and developer: ***Shenzhen Goodix Technology Co., Ltd.*****, P.R. China**
F13, Phase B, Tengfei Industrial Building, Futian Free Trade Zone
Shenzhen
P.R. China

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-2300076-01-CR**
Report version:	**1**
Project number:	NSCIB-**2300076-01**
Author(s):	**Jordi Mujal**
Date:	**24 June 2024**
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 Goodix Security Chip GSE20 Series with IC Dedicated Software, version A1.1 D0. The developer of the Goodix Security Chip GSE20 Series with IC Dedicated Software, version A1.1 D0 is Shenzhen Goodix Technology Co., Ltd. located in Shenzhen, 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 an Embedded-Flash-based secure microcontroller platform with IC Dedicated Software. The applications can be executed securely and with good performance in this platform.

The TOE has been evaluated by SGS Brightsight B.V located in Delft, The Netherlands. The evaluation was completed on 24 June 2024 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 Goodix Security Chip GSE20 Series with IC Dedicated Software, version A1.1 D0, 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 Goodix Security Chip GSE20 Series with IC Dedicated Software, version A1.1 D0 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 Goodix Security Chip GSE20 Series with IC Dedicated Software, version A1.1 D0 from Shenzhen Goodix Technology Co., Ltd. located in Shenzhen, P.R. China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	IC	A1
Software	Boot OS	v1 0100
	Root0	
	Analysis OS	
	HAL	
	Crypto Library	v1 0101

To ensure secure usage a set of guidance documents is provided, together with the Goodix Security Chip GSE20 Series with IC Dedicated Software, version A1.1 D0. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.3.4.

2.2 Security Policy

The TOE provides the following major security functionalities:

- CPU supporting unprivileged and privileged modes for access control
- CPU Monitor ensuring the correct execution of the programs
- SAHB with bus protection
- MMU supporting access control to memories and SFRs of the hardware components
- Memory encrypted and integrity protection for all embedded memories (Flash and its
- cache, ROM, SYSRAM, PKCRAM)
- Register integrity protection for critical registers
- AES with countermeasures against SCA and DFA attacks
- Galois/Counter Mode (GCM) mode for AES
- TDES with countermeasures against SCA and DFA attacks
- RSA cryptography, including key generation, with countermeasures against SCA and DFA
- ECC cryptography, including key generation, with countermeasures against SCA and DFA
- Diffie-Hellman functions with X25519, including key generation, with countermeasures against SCA and DFA attacks
- KDF functions
- TRNG conforming to class PTG.2 of AIS-20/31
- DRNG conforming to class DRG.3 of AIS-20/31
- CRC calculation with hardware acceleration
- Secure SHA-256 calculation
- HMAC functions
- Active Shielding resisting physical attacks
- Physical Sensors: Light Sensor, Low/High Voltage Sensor, Spike Sensor, Low/High
- Frequency Sensor, Low/High Temperature Sensor
- Test Mode and Analysis Mode protection

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]*.

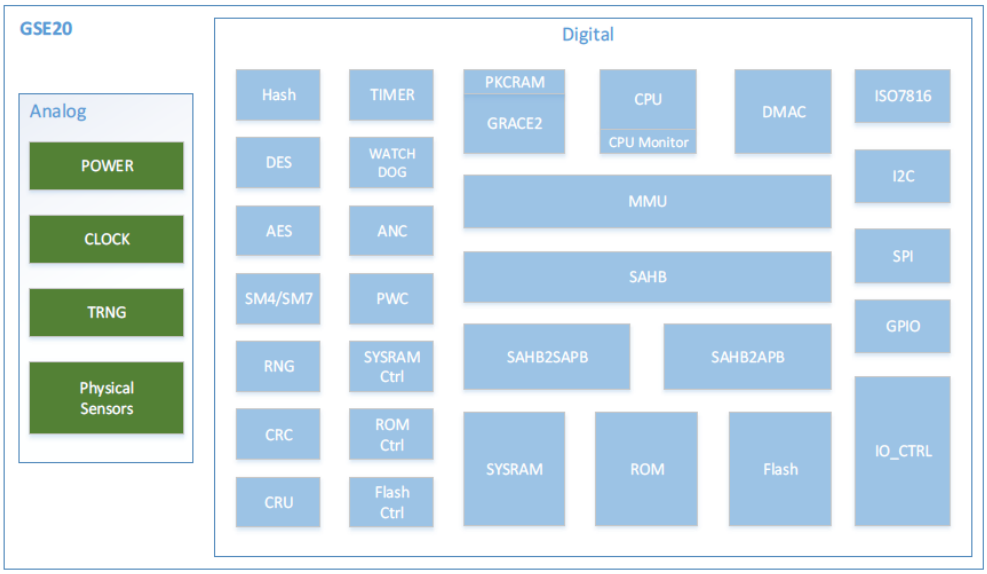
2.3.2 Clarification of scope

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

Please note that the TOE contains additional HW accelerators, HAL and CL APIs not explicitly claimed in the *[ST]*. The functionality and security of these features have not explicitly been addressed in this certification. Therefore, if these features are required by the composite product the developer/evaluator should do their own security analysis and/or testing.

2.4 Architectural Information

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



2.5 Documentation

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

Identifier	Version
GSE20 Datasheet	1.0
GSE20 Preparative Procedures	1.3
GSE20 User Manual	0.4
GSE20 Security User Guidance Manual	1.4
HAL and Crypto Library Header File	0101

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 following test approaches are used:

- Factory testing: The purpose of Factory test is to assure the chips meet the design specification and reduce earlier failure in mass production flow.
- Simulation testing: It is done in Linux system with EDA tool and Scripts to realized simulation Test. Simulation test is used in chip development for digital function the logic, analog function, chip level verification to make sure design meet our target.
- Emulator testing: Emulator tests are performed with FPGA emulator during development for IC dedicated software. They guarantee the functionality of TOE software functions and mechanisms. The software coverage test is done as part of the FPGA testing.
- Engineering sample testing: It is done in lab for OS/HAL/CL validation, execute all emulator tests, and analog IP validation and characteristic testing which not covered by Factory test.
- Quality testing: Quality testing contains chip level ESD, system level ESD, OLT, NVM cycling for endurance to ensure the overall quality of the chip.

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 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. This analysis was performed according to the attack methods in *[JIL- AAPS]* and *[JIL-AM]*.
- 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 September 2023 and February 2024,

with 55 man-weeks in total for testing and reporting. During that test campaign, 2% of the total time was spent on physical attacks, 29% on perturbation attacks, 7% on retrieving keys with FA, 58% on side-channel attacks and 4% on attacks on RNG.

2.6.3 Test configuration

Part of the independent evaluator testing and penetration testing was performed on an earlier revision of the TOE. The assurance gained from testing on an earlier revision has been assessed to be valid for the final TOE version, because the changes introduced were minimal and did not have an impact on the TSF.

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. These activities revealed that for some cryptographic functionality the security level could be reduced from an algorithmic security level above 100 bits to a practical remaining security level lower than 100 bits. The remaining security level still exceeds 80 bits, so this is considered sufficient. Therefore, no exploitable vulnerabilities were found with the independent penetration tests.

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 3 Site Technical Audit Reports.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Goodix Security Chip GSE20 Series with IC Dedicated Software, version A1.1 D0 with the specific configuration GSE20 A1.1.0 D0 and GSE20 A1.1.1 D0

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 Reports for the sites *[STAR_JSCC]*[2]*, [STAR_GHQ], [STAR_GZJ], [STAR_GSZ], [STAR_SJSemi].* 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 Goodix Security Chip GSE20 Series with IC Dedicated Software, version A1.1 D0, 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.

[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.

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: none.

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 Security Chip GSE20 Series with IC Dedicated Software, version 1.10, 19 June 2024 *[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
MAC	Message Authentication Code
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
RMI	Remote Method Invocation
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 “Goodix Security Chip GSE20” – EAL6+, Version 5.0, 19 June 2024
[ETRfC]	Evaluation Technical Report for Composition “Goodix Security Chip GSE20” – EAL6+, Version 3.0, 19 June 2024
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022
[JIL-AMS]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[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
[ST]	Security Target of Security Chip GSE20 Series with IC Dedicated Software, version 1.10, 19 June 2024
[ST-lite]	Security Target Lite of Security Chip GSE20 Series with IC Dedicated Software, version 1.10, 19 June 2024
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
[STAR_JSCC]	STAR JSCC Site, 23-RPT-919, v3.0, 17 June 2024
[STAR_GHQ]	STAR Goodix Shanghai Hongqiao Site, 23-RPT-921, v3.0, 17 June 2024
[STAR_GZJ]	STAR Goodix Shanghai Zhangjiang Site, 23-RPT-921, v3.0, 17 June 2024
[STAR_GSZ]	STAR Goodix Shenzhen Site, 23-RPT-922, v3.0, 17 June 2024
[STAR_SJSemi]	STAR SJSemi site 23-RPT-923, v3.0, 17 June 2024

(This is the end of this report.)