Version 2022-02

Certification Report

GEOP01 on GSEA01 Security Chip version 1.0

Sponsor and developer:	***Shenzhen Goodix Technology Co., Ltd.*** **Floor 13, Phase B, Tengfei Industrial Building** **Futian Freetrade Zone, Shenzhen** **China**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0583946-CR**
Report version:	**1**
Project number:	**0583946**
Author(s):	**Wim Ton**
Date:	**2 June 2023**
Number of pages:	**13**
Number of appendices:	**0**

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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, TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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, TÜV Rheinland Nederland 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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Recognition of the Certificate

The 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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the GEOP01 on GSEA01 Security Chip version 1.0. The developer of the GEOP01 on GSEA01 Security Chip version 1.0 is Shenzhen Goodix Technology Co., Ltd. located in Shenzhen, 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 Smart Card Platform (IC and OS) along with the native applications, a cryptographic library, and the Java Card System.

The Security Card Operating System (COS) implements GlobalPlatform functionality allowing the installation of various applications, including but not limited to access control, mobile transaction, digital ID and digital car key, etc. The TOE can load, install, instantiate and execute the off-card verified Java Card applets.

The TOE has been evaluated by SGS Brightsight B.V located in Delft. The evaluation was completed on 13 May 2023 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 GEOP01 on GSEA01 Security Chip version 1.0, 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 GEOP01 on GSEA01 Security Chip version 1.0 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 EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

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).

TÜV Rheinland Nederland 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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the GEOP01 on GSEA01 Security Chip version 1.0 from Shenzhen Goodix Technology Co., Ltd. located in Shenzhen, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier			Version
Hardware	GSEA01 Security IC			A0
	IC Dedicated Software			0101
Software	Card Operating System	COS Framework	RTE	1.0
			VM	1.0
			Common API	1.0
			HCI API	1.0
		Global Platform	GP API	1.0
			GP APDU	1.0
		Proprietary software	Yula NFC Tag application	1.0
			EDA framework	1.0
			Kernel	1.0
	Root2	Proprietary Sub OS	OS Update, OS Configuration	1.0

To ensure secure usage a set of guidance documents is provided, together with the GEOP01 on GSEA01 Security Chip version 1.0. For details, see section 2.5 “Documentation” of this report.

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

2.2 Security Policy

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

- DES/TDES for encryption/decryption (CBC and ECB) and MAC generation and verification (2-key/3-key 3DES, Retail-MAC, CMAC). (single DES security not claimed)
- AES (Advanced Encryption Standard) for encryption/decryption (GCM, CBC, ECB, OFB, CFB, CTR) and MAC generation and verification (CMAC)
- RSA and RSA CRT for encryption/decryption and signature generation and verification
- RSA and RSA CRT key generation
- ECC over GF(p) for signature generation and verification (ECDSA)
- ECC over GF(p) key generation for key agreement
- Random number generation conforming to class PTG.2 and DRG.3 of AIS 20/31
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithm. (security not claimed)
- HMAC (security not claimed)
- OSCCA Algorithms (SM2, SM3, SM4 and SM9) (security not claimed)

The following Java Card 3.1.0 functionality is supported:

- Java Card Virtual Machine for bytecode execution.
- Transient and persistent memory management for applets
- Applet firewall protection
- Access control rules between applets and the JCRE
- Javacard wrapper layer for native implementations

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

- Garbage Collection
- Support for Extended Length APDUs.
- Sensitive result, Sensitive array, array view
- Oneshot object.

The following GlobalPlatform 2.3.1 functionality is supported:

- Loading and installation of Java Card packages
- Java CAP file deletion
- Java applet deletion
- Supplementary Security Domains (APSD and CASD) creation
- Applet and Security Domain association
- Key installation
- Applet signature verification
- CVM (PIN) Management
- SCP 02 and SCP 03 secure channels
- Delegated Management, DAP (RSA up to 4096 bits and ECC up to 512 bit).
- Compliance to Secure Element configuration. (security not claimed)

HCI communication functionality

- HCI APIs for HCI communication

Goodix proprietary functionality

- EDA framework for task management
- Root2 OS for OS update and OS configuration over SCP 90 secure channel (only available for Goodix authorized entities)
- Yula NFC Tag application (security not claimed)
- API for proprietary stream cipher functionality (security not claimed)

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

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 5.2 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

2.4 Architectural Information

The TOE is a composite TOE with the Security Card Operating System (COS) running on the Goodix GSEA01 Security Chip. 40nm technology with IC Dedicated Software. The GSEA01 Security Chip and associated IC Dedicated Software are Common Criteria certified to EAL5+ [CC3], comparable to a smart card controller.

The TOE Software, other than the IC Dedicated Software, is composed of the following components:

- Java Card Virtual Machine Software and Runtime Environment,
- Common Application Programming Interface Software,
- Application Programming Interface for HCI,
- GlobalPlatform (GP) Software,
- OS Update/Config Software (Root2). This component ensures that only Goodix Authorized updates may be applied,

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

- Proprietary Application Programming Interface Software (Extension API), including OSCCA algorithms (no security claimed),
- Proprietary Native Application, Yula, an NFC Tag application. (no security claimed)
- EDA (Event Driven Architecture) for task management.
- Kernel, a basic native functional set that provide functions such as non-volatile memory management, key management, cryptographic API, etc.

2.5 Documentation

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

Identifier	Version
GEOP ROOT2 User Manual	1.0
GEOP User Manual	1.6
GEOP01 Security Guidance	1.4
GEOP01 Preparative Procedures	1.7
GEOP01 Operational User Guidance	1.4

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.

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.

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 independent vulnerability analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considered whether potential vulnerabilities could 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 was performed on the TOE. During this attack-oriented analysis the protection of the TOE was analysed using the knowledge gained from all evaluation classes. This resulted in the identification of (additional) potential vulnerabilities. This analysis used the attack methods in *[JIL-AM]* and *[JIL-AAPS]*.
- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

these potential vulnerabilities are not exploitable. The potential vulnerabilities were addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 117 days. During that test campaign, 60% of the total time was spent on Perturbation attacks, 28% on side-channel testing, and 12% on logical tests.

2.6.3 Test configuration

The evaluator used special applets for the logical tests of the JCVM.

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

The evaluator testing and penetration testing was performed on the TOE in the operational life-cycle state with applet instance configurations specified in the Security Target *[ST]*.

The TOE was tested in the following configurations:

- The TOE in an exposed QFP100 package on a developer provided carrier board.
- Using T=0, T=1 (ISO/IEC 7816), SPI, and T=CL (ISO/IEC 14443)

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.

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 Site Technical Audit Reports.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number GEOP01 on GSEA01 Security Chip version 1.0. The user can use the command in chapter 3.3 of the GEOP User Manual to read the TOE version.

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 a Site Technical Audit Report(s) for the Wuhan site *[STAR]* [2]. To support composite evaluations according to *[COMP]* a derived document

[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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

[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 GEOP01 on GSEA01 Security Chip version 1.0, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims ‘demonstrable’ 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.

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in the GEOP01 Security Guidance sections RSA_4, and GNRL_10. 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: OSCCA Algorithms SM2, SM3, SM4 and SM9, 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).

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

3 Security Target

The Security Target of GEOP01 on GSEA01 Security Chip, v1.8, 2023-03-17 *[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:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation
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
EDA	Event Driven Architecture
EMA	Electromagnetic Analysis
HCI	Host Controller Interface
IC	Integrated Circuit
JIL	Joint Interpretation Library
MAC	Message Authentication Code
NFC	Neat Field Communication
OSCCA	Office of the State Commercial Cryptographic Administration
PKI	Public Key Infrastructure
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SCP	Secure Channel Protocol
SHA	Secure Hash Algorithm
SM	Secure Messaging
SPA/DPA	Simple/Differential Power Analysis
SPI	Serial Protocol Interface

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

SSH	Secure Shell
TRNG	True Random Number Generator
VLAN	Virtual LAN

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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 GEOP01 on GSEA01 Security Chip – EAL5+, 21-RPT-273,4.0, 27 April 2023

[ETRfC] Evaluation Technical Report for Composition GEOP01 on GSEA01 Security Chip – EAL5+, 23-RPT-311,2.0, 27 April 2023

[HW-CERT] Certification Report – Security Chip GSEA01.x.D00 with IC Dedicated Software, v.1, 24-02-22

[HW-ETRfC] Evaluation Technical Report for Composition "Security Chip GSEA01.x.D00 with IC Dedicated Software” – EAL5+, v5.0, 2022-02-24

[HW-ST] Security Target Lite of Security Chip GSEA01.x.D00 with IC Dedicated Software, v1.31, 2022-01-21

[JIL-AAPS] JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020

[JIL-AM] 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 2.5, 28 March 2019

[PP] Java Card Protection Profile - Open Configuration, version 3.1.0, April 2020 registered under the reference BSI-CC-PP-0099-V2-2020

[ST] Security Target of GEOP01 on GSEA01 Security Chip, v1.8, 2023-03-17

[ST-lite] Security Target Lite of GEOP01 on GSEA01 Security Chip, v1.0, 2023-04-27

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

[STAR] Site Technical Audit Report GEOP01 on GSEA01 Security Chip version 1.0Wuhan Site, 22-RPT-403, 2.0, 27 April 2023

(This is the end of this report.)

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.