Reference: 2024-10-INF-4699- v1
Target: Limitada al expediente
Date: 03.02.2026

Created by: I003
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2024-10**
TOE	**GEOP02 on GSE20 Security Chip, version 1.0**
Applicant	**9144030073882572XH - Shenzhen Goodix Technology Co., Ltd.**
References	

[EXT-8989] Certification Request

[EXT-9920] Evaluation Technical Report

Certification report of the product GEOP02 on GSE20 Security Chip, version 1.0, as requested in [EXT-8989] dated 07/03/2024, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-9920] received on 25/10/2025.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product GEOP02 on GSE20 Security Chip, version 1.0.

The TOE is a Java Card System comprising the JCOS and the IC. It is a composite TOE with the Security Card Operating System (COS) running on the Goodix GSE20 Security Chip with IC Dedicated Software.

Developer/manufacturer: Shenzhen Goodix Technology Co., Ltd.

Sponsor: Shenzhen Goodix Technology Co., Ltd..

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Nombre Laboratorio.

Protection Profile: Java Card System – Open Configuration Protection Profile, 3.1, April 2020.

Evaluation Level: Common Criteria 3.1 R5 EAL5 + ALC_DVS.2 + AVA_VAN.5.

Evaluation end date: 19/12/2025.

Expiration Date[1]: 18/01/2031

All the assurance components required by the evaluation level EAL5 (augmented with ALC_DVS.2 + AVA_VAN.5) have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL5 + ALC_DVS.2 + AVA_VAN.5, as defined by the Common Criteria 3.1 R5 and the CEM 3.1 R5.

Considering the obtained evidence during the instruction of the certification request of the product GEOP02 on GSE20 Security Chip, version 1.0, a positive resolution is proposed.

TOE SUMMARY

The TOE is a Java Card System comprising the JCOS and the IC. It is a composite TOE with the Security Card Operating System (COS) running on the Goodix GSE20 Security Chip with IC Dedicated Software.

The COS provides the following functionality:

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

- Virtual Machine Software and a Runtime Environment
- Common Application Programming Interface Software
- Application Programming Interface for HCI
- seRoot, implements OS Patch Update/Config Software. This component ensures that only Goodix Authorized updates may be applied
- EDA (Event Driven Architecture) for task management
- Kernel for managing system resources and communication between the IC and OS
- Limited Mode, provide functions to defend against continuous attacks
- Exception Handler, preserve TOE into secure state when physical attacks are detected

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL5 and the evidence required by the additional component ALC_DVS.2 + AVA_VAN.5 to the table, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE.TSS.1
ADV	ADV_ARC.1
	ADV_FSP.5
	ADV_IMP.1
	ADV_INT.2
	ADV_TDS.4
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.4
	ALC_CMS.5
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.2
ATE	ATE_COV.2
	ATE_DPT.3
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.5

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

SECURITY FUNCTIONAL REQUIREMENTS
FDP_ACC.2/FIREWALL
FDP_ACF.1/FIREWALL
FDP_IFC.1/JCVM
FDP_IFF.1/JCVM
FDP_RIP.1/OBJECTS
FMT_MSA.1/JCRE
FMT_MSA.1/JCVM
FMT_MSA.2/FIREWALL_JCVM
FMT_MSA.3/FIREWALL
FMT_MSA.3/JCVM
FMT_SMF.1
FMT_SMR.1
FCS_CKM.1
FCS_CKM.4
FCS_CKM.5
FCS_COP.1
FDP_RIP.1/ABORT
FDP_RIP.1/APDU
FDP_RIP.1/GlobalArray
FDP_RIP.1/bArray
FDP_RIP.1/KEYS
FDP_RIP.1/TRANSIENT
FDP_ROL.1/FIREWALL
FAU_ARP.1
FDP_SDI.2/DATA
FDP_SDI.2/ARRAY
FDP_SDI.2/RESULT
FPR_UNO.1
FPT_FLS.1
FPT_TDC.1
FIA_ATD.1/AID
FIA_UID.2/AID
FIA_USB.1/AID
FMT_MTD.1/JCRE
FMT_MTD.3/JCRE
FPT_RCV.3/Installer
FDP_ACC.2/ADEL
FDP_ACF.1/ADEL
FDP_RIP.1/ADEL

FMT_MSA.1/ADEL
FMT_MSA.3/ADEL
FMT_SMF.1/ADEL
FMT_SMR.1/ADEL
FPT_FLS.1/ADEL
FDP_RIP.1/ODEL
FPT_FLS.1/ODEL
FDP_IFC.2/GP-ELF
FDP_IFF.1/GP-ELF
FDP_ITC.2/GP-ELF
FDP_IFC.2/GP-KL
FDP_IFF.1/GP-KL
FDP_ITC.2/GP-KL
FCO_NRO.2/GP
FDP_UIT.1/GP
FMT_SMR.1/GP
FPT_FLS.1/GP
FPT_TDC.1/GP
FIA_UID.1/GP
FIA_UAU.1/GP
FIA_UAU.4/GP
FMT_MSA.1/GP
FMT_MSA.3/GP
FMT_SMF.1/GP
FTP_ITC.1/GP
FDP_ACC.2/OSM
FDP_ACF.1/OSM
FDP_UIT.1/OSM
FMT_MSA.3/OSM
FMT_SMF.1/OSM
FTP_ITC.1/OSM
FPT_FLS.1/OSM
FCS_RNG.1/PTG.2
FCS_RNG.1/DRG.3
FPT_EMSEC.1
FPT_PHP.3
FDP_ACF.1/LM
FDP_ACC.2/LM
FMT_MSA.1/LM
FMT_MSA.3/LM
FMT_SMF.1/LM
FIA_UID.1/LM
FIA_UAU.1/LM

IDENTIFICATION

Product: GEOP02 on GSE20 Security Chip, version 1.0.

Security Target: Security Target of GEOP02 on GSE20 Security Chip v1.9 (10 October 2025).

Protection Profile: Java Card System – Open Configuration Protection Profile, 3.1, April 2020.

Evaluation Level: Common Criteria 3.1 R5 EAL5 + ALC_DVS.2 + AVA_VAN.5.

SECURITY POLICIES

The use of the product GEOP02 on GSE20 Security Chip, version 1.0 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 4.3 ("Organizational Security Policies").

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 4.4 ("Assumptions").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product GEOP02 on GSE20 Security Chip, version 1.0, although the agents implementing attacks have the attack potential according to the High of EAL5 + ALC_DVS.2 + AVA_VAN.5 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 4.2 ("Description of Threats").

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 5.2 ("Security Objectives for the operational Environment").

ARCHITECTURE

LOGICAL ARCHITECTURE

The certification of this TOE is a composite certification. The certificate of the underlying hardware platform GSE20, which is part of this TOE, is re-used. In the following sections more detailed descriptions of the TOE components are provided.

Security IC

The security IC, GSE20, is a high-security C040 System on Chip with ARM SC300 processor, AES, (T)DES cryptographic engines and a GRACE2 co-processor for RSA, ECC and OSCCA crypto operations. It contains RAM, ROM and Flash which protect the confidentiality and integrity of the stored data, MMU for memory protection, DRNG and TRNG for random number generation and other peripherals like DMA, I2C, ISO7816 and SPI. It also has an active shield and sensors for the detecting physical or environmental attacks. The security IC is certified according to Common Criteria.

IC Dedicated Software

The IC Dedicated Software is certified in the scope of the security IC.

Security OS and GlobalPlatform Software

Security OS consists of Native OS, JCVM, JCRE, JCAPI and GP framework. JCVM, JCRE, JCAPI and GP Software are implemented according to the Java Card Specification Version 3.1.0 and Global Platform Specification v2.3.1.

Global Platform Software consists of GP framework and Amendment A v1.2, C v1.3, D v1.2, E v1.1. The following GP components are excluded from the certification:

- Secure Element configuration.
- Common Implementation Configuration.

Proprietary Software

The TOE implements the proprietary software: Kernel, EDA, seRoot.

- Kernel manages system resources and communication between the IC and OS.

- EDA, provides a task scheduler and task management functionalities, and it also separates resources from different tasks.
- seRoot mainly provides OS Patch Update and OS Config. OS Patch Update is used to update TOE securely. And OS Config provides a method to set up the initial states, pre-personalization data, features configurations of the TOE securely.

The TOE provides a Limited Mode to prevent continuous physical attacks.

The TOE uses SCP90, a proprietary Secure Channel Protocol designed for GSE20, which ensures the security of information transmission between the terminal and the chip.

Non-evaluated features

Yula NFC Tag Application and its Javacard API & Extension API are excluded from evaluation. Yula NFC Tag Application is not directly responsible for security. It primarily serves as an interface for communication between the NFC-enabled device and the tag. The actual security mechanisms are implemented at a lower level.

The TOE implements cryptographic mechanisms and proprietary interfaces for providing those mechanisms as a service (OSCCA algorithms). However, these mechanisms are out of the evaluation scope and their interfaces do not compromise the security of the TOE. Also, the hashing algorithms (SHA1, SHA-224, SHA-256, SHA-384, SHA-512) are out of the evaluation scope and their interfaces do not compromise the security of the TOE either.

The product includes cryptographic mechanisms that are not conformant with SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms v1.3 (the list is provided in [ST] section 1.4.2.5).

Interfaces of the TOE

Electrical and Physical interface

These interfaces are provided by the certified security IC.

Logical interface

The logical interface of the TOE is composed of the following:

- Javacard API interface
- GP API interface
- GP APDU command
- HCI API interface
- seRoot APDU command
- Bytecodes
- Yula NFC Tag API Interface (security not claimed)

- Yula NFC command (security not claimed)
- Extension API (security not claimed)

PHYSICAL ARCHITECTURE

The TOE consists of Security OS, IC hardware, IC Dedicated Software and guidance documentation.

Category	Component	Version	Delivery form
IC hardware	Security IC	A1	Module
IC Dedicated Software	IC Dedicated Software	v1	binary in ROM and Flash
IC Crypto Library	IC Crypto Library	v1.1	binary in ROM and Flash
COS framework	Runtime Environment Virtual Machine Common API HCI API	03.01.0000	binary in ROM and Flash
GlobalPlatform	GP API GP APDU		binary in ROM and Flash
Proprietary software	Yula NFC Tag application *		binary in ROM and Flash
	EDA framework		binary in ROM and Flash
	Kernel		binary in ROM and Flash
Proprietary Applet	seRoot (OS Patch Update, OS Configuration)		binary in ROM and Flash
User Manual	GEOP02 User Manual	1.9	.pdf file
	GEOP seRoot User Manual	0.7	.pdf file
	GEOP02 Preparative Procedures	1.8	.pdf file
	GEOP02 Operational User Guidance	1.7	.pdf file
	GEOP02 Security Guidance	1.5	.pdf file

* This is the only component from the table which is not part of the evaluation scope.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- Security Target of GEOP02 on GSE20 Security Chip v1.0 – Lite (14 October 2025).
- GEOP02 User Manual, version 1.9 (10 October 2025).

- GEOP seRoot User Manual, version 0.7 (10 October 2025).
- GEOP02 Preparative Procedures, version 1.8 (10 October 2025).
- GEOP02 Operational User Guidance, version 1.7 (10 October 2025).
- GEOP02 Security Guidance, version 1.5 (10 October 2025).

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result. During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test. All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results. To verify the results of the developer tests, the evaluator has repeated a sample of the developer tests through a remote test witnessing session.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer. It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

Through the tests performed by the Laboratory it is concluded that all the SFRs and TSFIs of the TOE have been tested through the developer testing effort and the evaluator's independent testing.

PENETRATION TESTING

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment, the evaluation team has devised attack scenarios for penetration tests according to JIL supporting documents [JILAAPS] and [JILADVARC]. Within these activities all aspects of the security architecture which were not covered by functional testing have been considered. The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential High has been successful in the TOE's operational environment as defined in the security target when all security measures required by the developer in the security guidance defined in DOCUMENTS section are applied.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product GEOP02 on GSE20 Security Chip, version 1.0 it is necessary the disposition of the following software components:

Category	Component	Version	Delivery form
IC hardware	Security IC	A1	Module
IC Dedicated Software	IC Dedicated Software	v1	binary in ROM and Flash
IC Crypto Library	IC Crypto Library	v1.1	binary in ROM and Flash
COS framework	Runtime Environment Virtual Machine Common API HCI API	03.01.0000	binary in ROM and Flash
GlobalPlatform	GP API GP APDU		binary in ROM and Flash
Proprietary software	Yula NFC Tag application *		binary in ROM and Flash
	EDA framework		binary in ROM and Flash
	Kernel		binary in ROM and Flash
Proprietary Applet	seRoot (OS Patch Update, OS Configuration)		binary in ROM and Flash

EVALUATION RESULTS

The product GEOP02 on GSE20 Security Chip, version 1.0 has been evaluated against the Security Target Security Target of GEOP02 on GSE20 Security Chip v1.9 (10 October 2025).

All the assurance components required by the evaluation level EAL5 + ALC_DVS.2 + AVA_VAN.5 have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL5 + ALC_DVS.2 + AVA_VAN.5, as defined by the Common Criteria 3.1 R5 and the CEM 3.1 R5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

- To follow the security guidance's of the TOE strictly.
- To keep the TOE under personal control and set all other security measures available from the environment.
- To periodically review the status of the certification of the underlying platform.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidence during the instruction of the certification request of the product GEOP02 on GSE20 Security Chip, version 1.0, a positive resolution is proposed.

The Certification Body strongly recommends to the TOE consumer to strictly follow the security recommendations that can be found on guidance documents, taking special care of those included in document GEOP02 Security Guidance, version 1.5, as well as to observe the operational environment requirements and assumptions defined in the applicable Security Target.

The TOE consumer should also observe the application notes defined in the applicable Security Target, especially those related to the cryptographic mechanisms.

GLOSSARY

CCN Centro Criptológico Nacional

CNI Centro Nacional de Inteligencia

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

OC Organismo de Certificación

TOE Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[JILAAPS] Application of Attack Potential to Smartcards. Joint Interpretation Library. Version 3.2.1. February 2024. Joint Interpretation Library.

[JILADVARC] Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices, version 2.1. July 2021. Joint Interpretation Library.

[START] Joint Interpretation Library. Site Technical Audit Report Template. Version 1.0. February 2018.

[CCDB-2006-04-004] ST sanitising for publication. CCMC. April 2006.

[ST] Security Target of GEOP02 on GSE20 Security Chip v1.9 (10 October 2025).

[ST Lite] Security Target of GEOP02 on GSE20 Security Chip v1.0 – Lite (14 October 2025).

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- Security Target of GEOP02 on GSE20 Security Chip v1.9 (10 October 2025).

The public version of this document constitutes the ST Lite. The ST Lite has also been reviewed for the needs of publication according to [CCDB-2006-04-004], and it is published along with this certification report in the Certification Body and CCRA websites. The ST Lite identifier is:

- Security Target of GEOP02 on GSE20 Security Chip v1.0 – Lite (14 October 2025).

ETR FOR COMPOSITION IDENTIFICATION

The evaluation activities carried out in this certification dossier have been summarized in an Evaluation Technical Report for composite evaluation (ETR_COMP). This ETR_COMP has been validated by this Certification Body. The reference of the ETR_COMP is:

- **Report name**: ETR for composite evaluation. GEOP02 on GSE20 Security Chip v1.0.
- **Report ID**: CCEGDX001-ETRfC-M1.
- **Version**: M1.
- **Issue Date**: 21/11/2025.
- **SHA256**: 3423ef8219dc4c9a7eb52a8454d6623ecd1d7b3b616386b191ce2163ae322961.
- **Issuing ITSEF**: Applus Laboratories.

The ETR_COMP report constitutes an evaluation evidence, therefore according to article 25 of Presidential Order PRE/2740/2007 which regulates the CCN Certification Body, written authorization must be requested by Applus Laboratories to the Certification Body to share any information of this certification dossier with third parties.

It is expected that if the applicant Shenzen Goodix Technology Co., Ltd. is willing to share the ETR_COMP report with any third party, they may contact Applus Laboratories to perform an authorization request to the CCN Certification Body to distribute this report.

SITE TECHNICAL AUDIT REPORT (STAR)

The site visit carried out within this dossier have been summarized in one Site Technical Audit Report (STAR). This STAR report has been validated by this Certification Body according to [START]. The reference of the STAR is:

- **Report name**: Site technical audit report (STAR). Goodix Wuhan Site.
- **Report ID**: CCEGDX001-STAR-M2.
- **Version**: M2.
- **Issue Date**: 21/11/2025.
- **Issuing ITSEF**: Applus Laboratories.
- **Site audit dates**: 13-14/05/25.

This STAR report constitute an evaluation evidence, therefore according to article 25 of Presidential Order PRE/2740/2007 which regulates the CCN Certification Body, written authorization must be requested by Applus Laboratories to the Certification Body to share any information of this certification dossier (including any of the STAR reports) with third parties.

It is expected that if the applicant Shenzen Goodix Technology Co., Ltd. is willing to share this STAR report with any third party, they may contact Applus Laboratories to perform an authorization request to the CCN Certification Body to distribute this report

RECOGNITION AGREEMENTS

In order to avoid multiple certifications of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.