Reference: 2020-44-INF-3867- v1
Target: Pública
Date: 16.06.2023

Created by: CERT9
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2020-44**
TOE	**Huawei CloudEngine S Series Switches running VRP software Version V200R020C00SPC300 Patch V200R020SPH507T**
Applicant	**B84136464 - Huawei Technologies España, S.L.**
References	
	[EXT-7494] 2021-12-24_2020-44_ETR_V1

Certification report of the product Huawei CloudEngine S Series Switches running VRP software Version V200R020C00SPC300 Patch V200R020SPH507T, as requested in [EXT-6186] dated 01/06/2020, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-7494] received on 24/12/2021.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei CloudEngine S Series Switches running VRP software Version V200R020C00SPC300 Patch V200R020SPH507T.

The Huawei CloudEngine S Series Switches TOE are used to satisfy the requirements for networks of various scales. They are deployed at the edge of IP backbone networks, IP metropolitan area networks (MANs), and other large-scale IP networks, also can be used to access, aggregate, and transmit carrier-class Ethernet services on Fixed-Mobile Convergence (FMC) Metropolitan Area Networks (MANs).

The TOE is comprised of several security features as identified below:

- Security audit
- Cryptographic support
- Identification and authentication
- Secure Management
- Protection of the TSF
- TOE access through user authentication
- Trusted path and channels for device authentication.

Developer/manufacturer: Huawei Technologies España, S.L.

Sponsor: Huawei Technologies España, S.L..

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories.

Protection Profile: [CPP_ND] Collaborative Protection Profile for Network Devices, Version 2.1, 24-Sep-2018[1].

Evaluation Level: Common Criteria version 3.1 release 5 (assurance packages according to the [CPP_ND]

Evaluation end date: 19/01/2023.

Expiration Date[2]: 17/06/2028.

[1] This cPP version is CCRA archived at the time of issuing this certificate.

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

All the assurance components required by the evaluation level of the [CPP_ND] 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 [CPP_ND], as defined by the Common Criteria version 3.1 release 5, the [CPP_ND], and Common Criteria Evaluation Methodology version 3.1 release 5.

Considering the obtained evidences during the instruction of the certification request of the product Huawei CloudEngine S Series Switches running VRP software Version V200R020C00SPC300 Patch V200R020SPH507T, a positive resolution is proposed.

TOE SUMMARY

The TOE is CloudEngine S Series Switches comprised of both software and hardware. The software is comprised of Versatile Routing Platform (VRP) software, VRP is a network OS incorporating Huawei's proprietary intellectual properties and capable of supporting various network systems of Huawei. The hardware is comprised of the following: CloudEngine S6730-H, CloudEngine S6730-S, CloudEngine S5731-H, CloudEngine S5732-H, CloudEngine S5731-S, CloudEngine S5735-S, CloudEngine S5735-L, CloudEngine S6330-H, CloudEngine S5331-H, CloudEngine S5335-L, CloudEngine S5332-H, CloudEngine S5335-S, CloudEngine S12700E.

The Huawei CloudEngine S Series Switches use the same VRP version. TSF relevant functions depend on software implementation.

The physical scope comprises the following hardware appliances and the TOE software:

CloudEngine S6730-H, CloudEngine S6730-S, CloudEngine S5731-H, CloudEngine S5732-H, CloudEngine S5731-S, CloudEngine S5735-S, CloudEngine S5735-L, CloudEngine S6330-H, CloudEngine S5331-H, CloudEngine S5335-L, CloudEngine S5332-H, CloudEngine S5335-S, CloudEngine S12700E.

There are only hardware differences between different devices. All the switches share the same platform so the SFRs are the same. Network management server, local console and syslog server are supported by all TOE evaluated configurations. The TOE only has one configuration.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level of the [CPP_ND] to the table, according to Common Criteria version 3.1 release 5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_FSP.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.1

	ALC_CMS.1
ASE	ASE_CCL.1
	ASE_SPD.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.1
	ASE_REQ.1
	ASE_TSS.1
ATE	ATE_IND.1
AVA	AVA_VAN.1

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to Common Criteria version 3.1 release 5 assurance packages according to the Collaborative Protection Profile for Network Devices, Version 2.1, 24-Sep-2018.

The detail of these security functional requirements is documented in the Security Target, section 6 ("Security Functional Requirements").

IDENTIFICATION

Product: Huawei CloudEngine S Series Switches running VRP software Version V200R020C00SPC300 Patch V200R020SPH507T

Security Target: Security Target of Huawei CloudEngine S Series Switches Running VRP Software version 4.9, 2021-11-29

Protection Profile: [CPP_ND] Collaborative Protection Profile for Network Devices, Version 2.1, 24-Sep-2018[3].

SECURITY POLICIES

The use of the product Huawei CloudEngine S Series Switches running VRP software Version V200R020C00SPC300 Patch V200R020SPH507T 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 3.3 ("Organizational Security Policies").

[3] This cPP version is CCRA archived at the time of issuing this certificate.

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 3.2 (“Assumptions”).

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Huawei CloudEngine S Series Switches running VRP software Version V200R020C00SPC300 Patch V200R020SPH507T, although the agents implementing attacks have the attack potential according to the attack potential of the [CPP_ND] 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 3.1 (“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 4.1 (“Security Objectives for the operational Environment”).

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

(1) Security audit

The log module of the host software records operations on a device and events that occur to a device. The recorded operations and events are log messages. Log messages provide evidence for diagnosing and maintaining a system. Log messages reflect the operating status of a device and are used to analyze the conditions of a

network and to find out the causes of network failure or faults.

Key elements of log messages include timestamp, host name, Huawei identity, version, module name, severity, brief description, etc.

IC component are the module processing, outputting log records. Information hierarchy is designed

to help the user roughly differentiate between information about normal operation and information about faults. Since the information center needs to output information to the terminal, console, log buffer, and log file.

(2) Cryptographic support

The TOE provides cryptography in support of secure connections that includes remote administrative management.

The cryptographic services provided by the TOE are described in Table below.

TABLE 1: CRYPTOGRAPHY PROVIDED BY TOE

Cryptography Function	Use in the TOE
DRBG	Used in session establishment of TLS and SSH
RSA	Used in session establishment of TLS
SHA	Used to provide cryptographic hashing services
HMAC-SHA	Used to provide integrity and authentication verification
AES	Used to encrypt traffic transmitted through TLS and SSH
ECDSA	Used in the authentication of SSH
DH	Used in session establishment of SSH
DHE	Used in session establishment of TLS

(3) Identification and authentication

The authentication functionality provides validation by user's account name and password. Public key authentication is supported for SSH users. Detailed functionalities, for example max idle-timeout period, max log-in attempts, UI lock, user kick out, can be applies by administrator according to networking environment, customized security considerations, differential user role on TOE, and/or other operational concerns.

(4) Secure Management

The TOE restricts the ability to determine the behavior of and modify the behavior of the function's transmission of audit data to the security administrator. Only the security administrator can manage the cryptographic keys. Only the security administrator has the right of opening/closing the security services and creation/deletion/modification of the user accounts.

(5) Protection of the TSF

The TOE protects the pre-shared keys, symmetric keys, and private keys from reading them by an unauthorized entity. The TOE stores the users or administrator passwords in non-plaintext form preventing them from reading. The TOE verifies the packet before their installation and uses the digital signature.

(6) TOE access through user authentication

The TOE provides communication security by implementing SSH protocol.

To protect the TOE from eavesdrop and to ensure data transmission security and confidentiality, SSH implements:

- authentication by password or by public-key;
- AES encryption algorithms;
- secure cryptographic key exchange;
- Besides default TCP port 22, manually specifying a listening port is also implemented since it can effectively reduce attack.

(7) Trusted path and channels for device authentication

The TOE supports the trusted connections using TLS for the communication with the audit server.

PHYSICAL ARCHITECTURE

This section will define the physical scope (Table 3) of the Huawei CloudEngine S Series Switches running VRP Software to be evaluated.

TABLE 2: PHYSICAL SCOPE

Type	Delivery Item	Version
Hardware	CloudEngine S6730-H, CloudEngine S6730-S, CloudEngine S5731-H, CloudEngine S5732-H, CloudEngine S5731-S, CloudEngine S5735-S, CloudEngine S5735-L, CloudEngine S6330-H, CloudEngine S5331-H, CloudEngine S5335-L, CloudEngine S5332-H, CloudEngine S5335-S, CloudEngine S12700E The Hardware will be delivered by air, ship, train or automobile.	NA
Software	S12700E-4/S12700E-8/S12700E-12: S12700E-V200R020C00SPC300-MPUE.CC Info： Users can login the HUAWEI support website to download the	V200R020C00SPC300

Type	Delivery Item	Version
	software packet in accordance to the version of the TOE. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website). S6730-H48X6C/S6730-H24X6C/S6730-H28Y4C/S6730-H24X4Y4C: S6730-H-V200R020C00SPC300.CC Info：Users can login the HUAWEI support website to download the software packet in accordance to the version of the TOE. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website). S6730-S24X6Q: S6730-S-V200R020C00SPC300.CC Info：Users can login the HUAWEI support website to download the software packet in accordance to the version of the TOE. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website). S5731-H24T4XC/S5731-H48T4XC/S5731-H24P4XC/S5731-H48P4XC: S5731-H-V200R020C00SPC300.CC Info：Users can login the HUAWEI support website to download the software packet in accordance to the version of the TOE. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website). S5732-H24S6Q/S5732-H48S6Q/S5732-H24UM2CC/S5732-H48UM2CC/S5732-H48XUM2CC/S5732-H24S4Y4Q: S5732-H-V200R020C00SPC300.CC Info：Users can login the HUAWEI support website to download the software packet in accordance to the version of the TOE. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website). S5731-S24T4X/S5731-S24P4X/S5731-S48T4X/S5731-S48P4X: S5731-S-V200R020C00SPC300.CC Info：Users can login the HUAWEI support website to download the software packet in accordance to the version of the TOE. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website). V200R020C00SPC300 S5735-S24T4X/S5735-S24P4X/S5735-S48T4X/S5735-S48P4X/S5735-	

Type	Delivery Item	Version
	S32ST4X/S5735-S48S4X/S5735-S24T4X-I: S5735-S-V200R020C00SPC300.CC Info：Users can login the HUAWEI support website to download the software packet in accordance to the version of the TOE. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website). S5735-L12T4S-A/S5735-L12P4S-A/S5735-L24T4S-A/S5735-L24T4X-A/S5735-L24P4S-A/S5735-L24P4X-A/S5735-L48T4S-A/S5735-L48T4X-A/S5735-L48P4X-A/S5735-L32ST4X-A/S5735-L24T4X-D/S5735-L12T4S-D/S5735-L32ST4X-D: S5735-L-V200R020C00SPC300.CC Info：Users can login the HUAWEI support website to download the software packet in accordance to the version of the TOE. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website). S6330-H48X6C/S6330-H24X6C/S6330-H28Y4C/S6330-H24X4Y4C: S6330-H-V200R020C00SPC300.CC Info：Users can login the HUAWEI support website to download the software packet in accordance to the version of the TOE. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website). S5331-H24T4XC/S5331-H24P4XC/S5331-H48T4XC/S5331-H48P4XC: S5331-H-V200R020C00SPC300.CC Info：Users can login the HUAWEI support website to download the software packet in accordance to the version of the TOE. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website). S5335-L12T4S-A/S5335-L48T4X-A/S5335-L12P4S-A: S5335-L-V200R020C00SPC300.CC Info：Users can login the HUAWEI support website to download the software packet in accordance to the version of the TOE. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website). S5332-H24S6Q/ S5332-H48S6Q/ S5332-H24S4Y4Q: S5332-H-V200R020C00SPC300.CC Info：Users can login the HUAWEI support website to download the software packet in accordance to the version of the TOE.	

Type	Delivery Item	Version
	Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website). S5335-S24T4X/ S5335-S24P4X/ S5335-S48T4X/ S5335-S48P4X/ S5335-S32ST4X/ S5335-S48S4X: S5335-S-V200R020C00SPC300.CC Info：Users can login the HUAWEI support website to download the software packet in accordance to the version of the TOE. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website).	
Patch	Patch for the TOE Name: patch_all_pack.pat Info: The patch can be download from HUAWEI support website. The patch is verify using digital signature when it's loaded for the TOE.	V200R020SPH507T
Product guidance	Huawei CloudEngine S Series Switches V200R020C00 Operational user Guidance.pdf Info: The documentation is delivered by email.	1.6
	Huawei CloudEngine S Series Switches V200R020C00 Preparative Procedures .pdf Info: The documentation is delivered by email.	1.9
	S2720, S5700, and S6700 Series Ethernet Switches Product Documentation 03 Related TOE: CloudEngine S6730-H, CloudEngine S6730-S, CloudEngine S5732-H, CloudEngine S5731-S, CloudEngine S5735-S, CloudEngine S5735-L S5300 and S6300 Series Ethernet Switches Product Documentation 03 Related TOE: CloudEngine S6330-H, CloudEngine S5331-H, CloudEngine S5335-L, CloudEngine S5332-H, CloudEngine S5335-S S12700 and S12700E Series Agile Switches Product Documentation 03 Related TOE: CloudEngine S12700E	refers to the last number of document name shown in the left column

Type	Delivery Item	Version
	Info: Users can login the HUAWEI support website to read the document directly or download the product documentation in accordance to the version of the TOE. The download file format is *.chm or *.hdx, user can download the *.hdx reader from the same website. At least a registered user is required. If a customer who does not have the permission clicks the product name, the registration page is redirected.	

There are only hardware differences between different devices. All the switches share the same platform so the SFRs are the same. Network management server, local console and syslog server are supported by all TOE evaluated configurations. The TOE only has one configuration.

DOCUMENTS

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

- Huawei CloudEngine S Series Switches V200R020C00 Operational user Guidance version 1.6
- Huawei CloudEngine S Series Switches V200R020C00 Preparative Procedures version 1.9
- S2720, S5700, and S6700 Product Documentation, version 03.
- S2320, S5300, S6300 Product Documentation, version 03.
- S12700 and S12700E Product Documentation, version 03.

PRODUCT TESTING

The tests performed by both the evaluator and the developer are based on the TSFIs description included in the functional specification and the SFRs description included in the Security Target [ST].

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to the Security Target [ST].

The product series testing has followed the SOGIS supporting document Evaluation methodology for product series, version 1.0. The ITSEF analysed the Differential Analysis Report (DAR) and Testing Reuse Rationale (TRR) provided by the applicant to prepare the independent testing strategy.

The evaluator has repeated cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report. The test repetition performed by the evaluator has demonstrated that the test plan and report provided by the vendor contains information enough to make a reader able to repeat all tests included. Additionally, after the repetition, the evaluator has obtained the same results as the expected ones. The independent testing has covered SFRs of the [ST] and TSFIs defined in the functional specification for the TOE, sampling has not been performed. The test cases have taken into account critical parameters values, searching that the TOE behaves in a nonexpected manner. There has not been any deviation from the expected results under the environment defined in the Security Target [ST].

EVALUATED CONFIGURATION

The acceptance and installation procedures are given in section 2, 3, 4 and 5 (Secure Acceptance by Production, Secure Installation of TOE Software by Production, Secure Preparation for Delivery by Production and Secure Acceptance by User) of the preparative user guidance Huawei CloudEngine S Series Switches V200R020C00 Preparative Procedures version 1.9.

EVALUATION RESULTS

The product Huawei CloudEngine S Series Switches running VRP software Version V200R020C00SPC300 Patch V200R020SPH507T has been evaluated against the Security Target “Security Target of Huawei CloudEngine S Series Switches Running VRP Software version 4.9, 2021-11-29”.

All the assurance components required by the evaluation level of the [CPP_ND] 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 of the [CPP_ND], as defined by the [CC_P1], [CC_P2], [CC_P3] y [CEM].

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Each assurance class and evaluation activity from the [CPP_ND] has a Pass verdict.

During the evaluation process, the developer has provided evidences and resolutions to close the Observation Reports issued by the lab. The observation reports were related to the documentation evidences, no exploitable vulnerabilities have been found in any part of the TOE. Therefore, no

issue was detected according to the standard and evidences used for the evaluation. The product fulfilled the whole set of Security Functional Requirements established in the Security Target.

The evaluation team makes the following security recommendations:

- 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.

Finally, since all the classes of the evaluation have a PASS verdict and all the dependencies have been fulfilled, considering the evaluations results and verdict, the laboratory recommends the CB to take into account the certification of the product POSITIVELY for an assurance level of CPP_ND compliance.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Huawei CloudEngine S Series Switches running VRP software Version V200R020C00SPC300 Patch V200R020SPH507T, a positive resolution is proposed.

Considering that the CCRA status of the Protection Profile [CPP_ND] Collaborative Protection Profile for Network Devices, Version 2.1, 24-Sep-2018 is archived, consumers are advised to check if the TOE satisfies their security requirements.

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.

[CPP_ND] Collaborative Protection Profile for Network Devices, Version 2.1, 24-Sep-2018

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- [ST]: Security Target of Huawei CloudEngine S Series Switches Running VRP Software version 4.9, 2021-11-29.

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 recognized under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA up to EAL2 + ALC_FLR only due to the fact that the cPP is archived by CCRA at the time of issuing this certificate.