Reference: 2021-41-INF-4381- v1
Target: Limitada al expediente
Date: 29.08.2024

Created by: CERT10
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2021-41**
TOE	**DefensePro and APSolute Vision Attack Mitigation System (APSolute Vision 4.85.00, DefensePro 8.26.1.0)**
Applicant	**520044371 - Radware, LTD.**
References	
	[EXT-7297] Certification request
	[EXT-9066] Evaluation technical report

Certification report of the product DefensePro and APSolute Vision Attack Mitigation System (APSolute Vision 4.85.00, DefensePro 8.26.1.0), as requested in [EXT-7297] dated 06/08/2024, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-7297] received on 03/05/2024.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product DefensePro and APSolute Vision Attack Mitigation System (APSolute Vision 4.85.00, DefensePro 8.26.1.0).

This document constitutes the Certification Report for the certification file of the product DefensePro and APSolute Vision Attack Mitigation System (APSolute Vision 4.85.00, DefensePro 8.26.1.0).

The TOE is a series of products which themselves are composed of two independent components: the DefensePro 8.26.1.0 and the APSolute Vision 4.85.00. Either of them can be running directly on a hardware appliance, or on a virtualized environment (Virtual Appliance).

The TOE is designed to act as a real-time perimeter attack mitigation system, securing organizations against emerging network attacks, Denial of Service (DoS) and Distributed-DoS (DDoS).

Developer/manufacturer: Radware, LTD.

Sponsor: Radware, LTD..

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

ITSEF: Applus Laboratories.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL2.

Evaluation end date: 18/07/2024

Expiration Date[1]: 13/08/2029

All the assurance components required by the evaluation level EAL2 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 EAL2, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

[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.

Considering the obtained evidences during the instruction of the certification request of the product DefensePro and APSolute Vision Attack Mitigation System (APSolute Vision 4.85.00, DefensePro 8.26.1.0), a positive resolution is proposed.

TOE SUMMARY

The TOE is composed of the **DefensePro 8.26.1.0** (running on DefensePro appliances or in a Virtual Appliance) and **APSolute Vision 4.85.00** (running on APSolute Vision appliances or in a Virtual Appliance). If the TOE is configured on bare-metal hardware, using the appliances defined in [ST] section 2.2.3, the following diagram relates the evaluated elements.

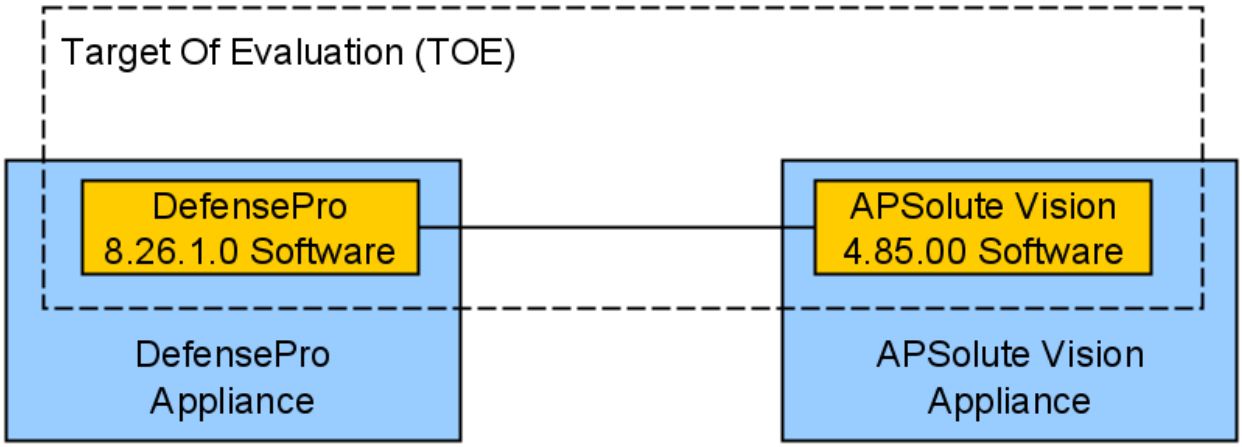

FIGURE 1 - PHYSICAL SCOPE ON APPLIANCES

In case the TOE is running on a Virtual Appliance (VA), the TOE evaluated elements behave under a logically equivalent diagram:

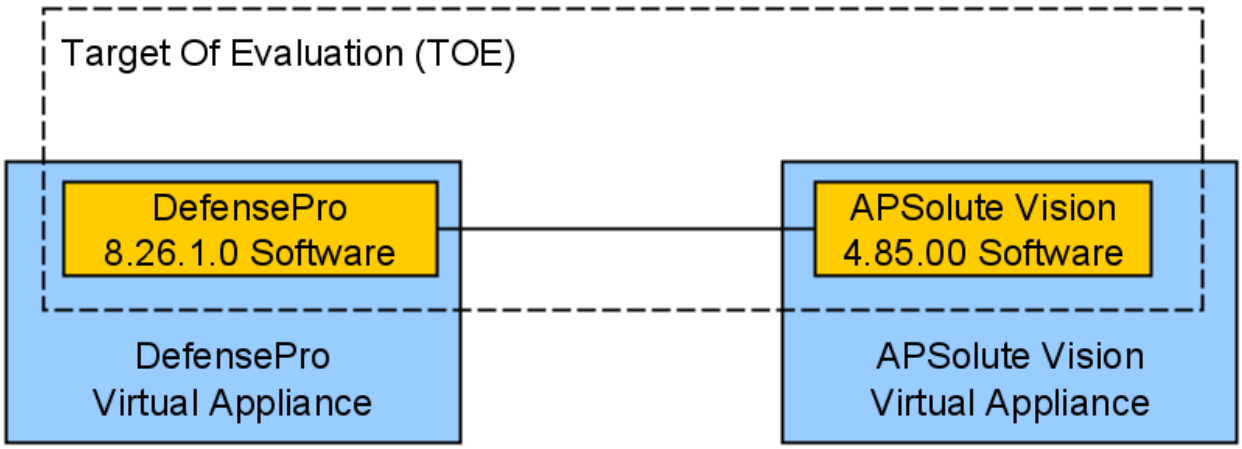

FIGURE 2 - PHYSICAL SCOPE ON VA

The differences between the bare-metal and the Virtual Appliance configurations of the TOE are only related to the throughput capacity, as the bare-metal system has specifically-selected hardware that executes the filtering at a Layer 2/3 level, whereas the Virtual Appliances perform the full filtering on the virtual NICs. In both cases the filtering results and the algorithms, which determine whether the traffic is benign or not, are functionally equivalent. The hardware acceleration is just performed on a specialized ASIC instead of the CPU to ensure a high-performance throughput can be achieved, for carrier grade solutions. Therefore, even mixed deployments, hardware AP and virtual DP, or vice versa, are equivalent and can be considered another instance of the series of products.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2, 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.2
	ADV_TDS.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
ATE	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

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

SECURITY FUNCTIONAL REQUIREMENT
FAU_GEN.1
FAU_GEN.2
FAU_STG.1
FAU_STG.4
FIA_AFL.1
FIA_UAU.2
FIA_UID.2
FDP_IFC.1
FDP_IFF.1
FMT_MSA.1
FMT_MSA.3
FMT_SMF.1
FMT_SMR.2
FTA_SSL.4

IDENTIFICATION

Product: DefensePro and APSolute Vision Attack Mitigation System (APSolute Vision 4.85.00, DefensePro 8.26.1.0)

Security Target: DefensePro and APSolute Vision Security Target (v2.0, 16/04/2024)

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL2.

SECURITY POLICIES

The use of the product DefensePro and APSolute Vision Attack Mitigation System (APSolute Vision 4.85.00, DefensePro 8.26.1.0) 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 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 DefensePro and APSolute Vision Attack Mitigation System (APSolute Vision 4.85.00, DefensePro 8.26.1.0), although the agents implementing attacks have the attack potential according to the Basic attack potential of EAL2 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 ("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

This section summarizes the logical scope of the TOE.

SECURITY AUDIT

The TOE generates audit records for security-related events which are stored in the APSolute Vision 4.85.00 and DefensePro 8.26.1.0. In addition, the security-related logs generated in the DefensePro 8.26.1.0 are sent to the APSolute Vision 4.85.00.

The audit logs are protected from unauthorized modification and deletion.

USER DATA PROTECTION

The TOE achieves information flow control applying different policies and rules to the traffic that passes through its interfaces. Information flow control is used by the TOE to mitigate denial of service attacks.

IDENTIFICATION AND AUTHENTICATION

The different parts of the TOE present a different set of roles. The TOE requires that the users associated with those roles must be identified and authenticated before granting them access to the TOE and its security functions. Users can authenticate through the different management interfaces using their username and password, but in the evaluated configuration all access and management will be done through the AP.

SECURITY MANAGEMENT

The APSolute Vision 4.85.00 provides remote management capabilities of the TOE via the management interfaces (HTTPS-AP). The security management functionality allows to configure users, roles and all of the other configuration objects (policies and profiles) needed to manage the data flow control.

TOE ACCESS

The TOE allows user-initiated session termination for its management interfaces (HTTPS-AP).

PHYSICAL SCOPE

This section outlines the physical scope of the TOE and all of the complementary parts needed for the proper usage of the TOE.

Radware maintains a single code base where all of the product features (TSF included) are implemented. The code base is then compiled and packaged specifically for each of the supported underlying platforms, resulting in multiple images. Thus, any change to the code base is observable

and applicable to all platforms, guaranteeing the complete equivalency at the functional and security level.

DEFENSEPRO 8.26.1.0 PHYSICAL APPLIANCES

The physical appliances may not include the correct version of the TOE, hence when the appliance is received the end user must perform an upgrade process in order to upgrade the TOE to its correct version.

File Name	Hardware Platform	SHA-256
DefensePro_6-20-60-110-220-200-400_v8-26-1-0-b93.tgz	DefensePro 6 DefensePro 20 DefensePro 60 DefensePro 110 DefensePro 200 DefensePro 220 DefensePro 400	47F14F430F662E7416AC999CFB1AB9E4B61B01146B11105F1D0690BE19800BD2

APSOLUTE VISION 4.85.00 PHYSICAL APPLIANCES

The physical appliances may not include the correct version of the TOE hence when the appliance is received, the end user must perform a re-installation process in order to setup the TOE to its correct version.

File Name	Hardware Platform	SHA-256
APSoluteVision-USB-4-85-00-40-x86_64.iso	APSolute Vision Server ODS-VL2	ECBA902692528E3995693B385C5BC8649021BC09FEAE1EBFA45E760835EB3922

DEFENSEPRO 8.26.1.0 VIRTUAL APPLIANCES

The virtual appliances (VA) correspond to images used to deploy virtual machines containing the DefensePro 8.26.1.0. The VAs always come as a complete DefensePro 8.26.1.0 instance for each supported platform and/or format:

File Name	Virtualization Platform	SHA-256
DefensePro_VA_v8-26-1-0-b93_ISO_KVM.iso	KVM (ISO Format)	193F3E67CC56F7A6A2A880F74E2F452395A3308271C8B703491EF0F84FD26A24
DefensePro_VA_v8-26-1-0-b93_Full_Install_KVM.tgz	KVM (tgz Format)	B8D0D68695159AF3AFCE304295C78D9D6223E9C0C6E8767A

		81AB7E3B8498CA33
DefensePro_VA_v8-26-1-0-b93_Full_Install_VMware.ova	VMWare	E1546ED74372058425AFC8D674AA741CF3D77E93E071BB9386742CA7E6458034

APSOLUTE VISION 4.85.00 VIRTUAL APPLIANCES

The virtual appliances (VA) correspond to images used to deploy virtual machines containing the APSolute Vision 4.85.00. The VAs always come as a complete APSolute Vision 4.85.00 instance for each supported platform and/or format:

File Name	Virtualization Platform	SHA-256
APSoluteVision-4-85-00-43-x86_64.iso	Generic	AB37D4EC44A998BB3976851AE543FE9933A303EC2CDE97591158CE0E65412256
Vision-4-85-00-KVM_43_prod.qcow2	KVM (OpenStack)	4AB4579C0BA21C8AF7E0D6F9D54CADB96841FAFB1846E404FB403F03D58F9005
Vision-4-85-00-VMware_43_Basic.ova	VMWare (OVA Format)	2C251F27F8E5CBF0A12B0CAC043604FAD8A41268C776FA4541BC38BB974F0A44

SUPPORTING SOFTWARE FOR APSOLUTE VISION 4.85.00

The APSolute Vision 4.85.00 physical appliances need some software scripts to allow it to create a bootable USB.

File Name	Hardware Platform	SHA-256
Vision-4-85-00-usb-boot-ODSVL2-43.tar.gz	APSolute Vision Server ODS-VL2	CC929F1285C967BA9665FE27BF1E009C50DF02E95AF81E80612F47FF7FAF3403

DOCUMENTS

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

The main CC documentation that is provided as part of the TOE delivery is:

Document Name	Version	SHA-256

DefensePro and APSolute Vision Common Criteria Guide	1.8	393cad5378801691a3ec871d880792dc3b601dd960dadebd7041481adb10fdc1

Additionally, the following complementary documentation is also provided as part of the TOE delivery:

Document Name	Document ID	SHA-256
APSolute Vision Installation and Maintenance Guide	RDWR_APSV_V485_IG2203	FDCC14CEC98F7D073F0B57CF8D88099F4707F0D918FA583D4CC65B073DC0D597
APSolute Vision User Guide	RDWR-APSV-V048500_UG2203	C71F598A108EDAE18293288B0267FD39CFB28C38083EB09258E06AC2DCB67DEA
DefensePro Installation and Maintenance Guide	RDWR_DP_IG_2309	F3C37B7486942BF93B9BAFB7CB9E9681FC83A1CCF26237F8908B7D3356E17930
DefensePro User Guide	RDWR-DP-V082610_UG2112	53B45E7C5444589494CC87F260780276365B932535790169390D3CCE14EF6B1A
DefensePro VA Installation and Maintenance Guide	RDWR-DPVA_IG2112	A6EE6AFFD7CF0CCDCA03A7008E32774C8B9E53445A006858F839044272EAC419

Furthermore, the TOE includes via its Web Management Interface complementary information describing each parameter. This Online Help is delivered as part of the APSolute Vision 4.85.00 and can be accessed through its Web Management Interface by clicking on the “?” button.

PRODUCT TESTING

The developer has executed tests for all the TOE TSFIs and a subset of the TOE SFRs. 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 executed 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 match the expected results. To verify the results of the developer tests, the evaluator has repeated all the developer functional tests.

In addition, the lab has devised independent test cases to complement the testing performed by the developer. The devised independent test cases aimed to test the SFRs that were not covered by the developer testing effort. The evaluators verified that the obtained results conform to the expected results. Through the tests performed by the Laboratory it is concluded that 92.85% of the SFRs and all the TSFIs defined in the Functional Specification has been tested.

Based on the vulnerability analysis activities performed as part of the AVA class activities, the evaluation team defined a list of potential vulnerabilities applicable to the TOE in its operational environment, and subsequently devised attack scenarios for penetration tests according to the potential vulnerabilities detected. The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with attack potential Basic has been successful in the TOE's operational environment as defined in the security target, when all security measures required by the developer security guidance documentation [AGD] are applied.

EVALUATED CONFIGURATION

For the operation of the DefensePro 8.26.1.0 the disposition of the following software and hardware components is required:

- For bare-metal installations, at least one of the following appliances is required:
  - DefensePro 6
  - DefensePro 20
  - DefensePro 60
  - DefensePro 110
  - DefensePro 200
  - DefensePro 220
  - DefensePro 400
- For Virtual Appliance (VA) installations, the following minimum specs apply:
  - Supported Virtualization Platforms:
    - KVM
    - VMWare
  - System Requirements:
    - vCPU: 2

- Recommended Intel server-grade processors: Westmere, Sandy-bridge, Ivy-bridge, Haswell, Broadwell, Skylake

- RAM: 4 GB per vCPU + 5 GB (16 GB minimum recommended)
- Disk space: 10 GB
- Network Interfaces: 3

For the operation of the APSolute Vision 4.85.00 the disposition of the following software and hardware components is required:

- For bare-metal installations, the following appliance is required:
  - APSolute Vision Server ODS-VL2
- For Virtual Appliance (VA) installations, the following minimum specs apply:
  - Virtualization platform:
    - VMWare
    - KVM
    - KVM (OpenStack)
    - Hyper-V
  - System Requirements:
    - vCPU: 8
    - RAM: 32 GB
    - Disk space: 500 GB
    - NICs: 3

The TOE configuration used for the testing is the same configuration obtained after performing the TOE installation steps according to the guidance documentation [AGD]. The TOE was installed both in a virtualized environment and in a physical platform environment, both of which have been used during the testing.

The TOE version and specific platform used for testing are the following:

<u>Virtual platform installation:</u>

- APSolute Vision 4.85.00, virtualized in Proxmox platform
- DefensePro 8.26.1.0, virtualized in eSXi platform

Physical platform installation:

- APSolute Vision 4.85.00, running in appliance APSolute Vision Server ODS-VL2
- DefensePro 8.26.1.0, running in appliance DefensePro 6

The evaluators used the TOE installed in a virtual environment as the base TOE for testing, and also repeated all the tests using the TOE installed in a physical platform environment to verify the consistency of the test results for both the virtual and physical installations.

EVALUATION RESULTS

The product DefensePro and APSolute Vision Attack Mitigation System (APSolute Vision 4.85.00, DefensePro 8.26.1.0) has been evaluated against the Security Target DefensePro and APSolute Vision Security Target (v2.0, 16/04/2024).

All the assurance components required by the evaluation level EAL2 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 EAL2, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 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 keep the administrators properly trained.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product DefensePro and APSolute Vision Attack Mitigation System (APSolute Vision 4.85.00, DefensePro 8.26.1.0), a positive resolution is proposed.

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:

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.

[JIL-PROD-SERIE] Joint Interpretation Library, Evaluation methodology for product series, V.1.0, April 2017.

[ST] DefensePro and APSolute Vision Security Target, v2.0, 16/04/2024.

[AGD] DefensePro & APSolute Vision Common Criteria Guide, v1.8, 16/04/2024.

SECURITY TARGET

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

- DefensePro and APSolute Vision Security Target (v2.0, 16/04/2024).

RECOGNITION AGREEMENTS

In order to avoid multiple certification 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 selected.