REF: 2014-40-INF-2261 v3	Created by: CERT9
Target: P	Revised by: CALIDAD
Date: 20.03.2018	Approved by: TECNICO

CERTIFICATION REPORT

File: 2014-40 KASPERSKY ENDPOINT SECURITY

Applicant: 03654151A

References:

[EXT-2592] Certification request of KASPERSKY ENDPOINT SECURITY

[EXT-3775] Evaluation Technical Report of KASPERSKY ENDPOINT SECURITY.

The product documentation referenced in the above documents.

Certification report of the product “Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0 version 10.3.0.6294 AES256”, as requested in [EXT-2592] dated 11-08-2014, and evaluated by the laboratory “Epoche & Espri S.L.U.”, as detailed in the Evaluation Technical Report [EXT-3775] received on 14/02/2018.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product “Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0 version 10.3.0.6294 AES256”.

The TOE is a software product, which provides the encryption of device data (user data, operation system data), anti-virus and access control functionality. Together with the Kaspersky Security Center (KSC), which is used for management functions, both parts build a security suite for protection of personal computer systems (work stations, laptops and other devices) using Windows as operating system.

Developer/manufacturer:	Kaspersky Lab AO 39A/2 Leningradskoe Shosse, Moscow, 125212, Russia.
Sponsor:	Kaspersky Lab UK Ltd.
Certification Body:	Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).
ITSEF:	“Epoche & Espri S.L.U.”
Protection Profile:	None.
Evaluation Level:	EAL2+ALC_FLR.1.
Evaluation end date:	14/02/2018.

All the assurance components required by the evaluation level EAL2 (augmented with ALC_FLR.1) have been assigned a “PASS” verdict. Consequently, the laboratory “Epoche & Espri S.L.U.” assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2 (augmented with ALC_FLR.1), as defined by Common Criteria v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product “Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0 version 10.3.0.6294 AES256”, a positive resolution is proposed.

TOE SUMMARY

Kaspersky Endpoint Security for Windows combines world-class anti-malware with application start-up control, device access control, and web access control, plus data encryption in a single application.
Full Disk Encryption as part of Kaspersky Endpoint Security for Windows functionality helps to protect valuable business data from accidental loss due to lost or stolen devices. Kaspersky understands that data loss can result in devastating consequences. Kaspersky Endpoint Security for Windows Encryption functionality provides a strong encryption algorithm integrated in the endpoint protection suite that can be easily managed with a centralised management console.
Kaspersky Endpoint Security consists of components, each of which is responsible for protection against a particular type of threat. They can be organised into three groups covering main product functionality:

1. Anti-Virus protection:
   - File system protection
   - Network protection and traffic scanning
   - IM Antivirus
   - Proactive Defense
2. Control:
   - Application Startup Control
   - Device Access Control
   - Web Access Control
3. Encryption:
   - Full Disk Encryption
   - Removable Device Encryption (not a part of evaluation)
   - File Level Encryption (not a part of evaluation)
4. Management of all above.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 and the evidences required by the additional component ALC_FLR.1, according to Common Criteria v3.1 R5 and the CEM v3.1 R5.

Class	Family/Component
ASE: Security Target Evaluation	ASE_INT.1. ST Introduction ASE.CCL.1. Conformance claims ASE_SPD.1. Security problem definition ASE_OBJ.2. Security objectives ASE_ECD.1. Extended component definition ASE_REQ.2. Derived security requirements ASE_TSS.1. TOE summary specification
ADV: Development	ADV_ARC.1. Security architecture ADV_FSP.2. Functional specification ADV_TDS.1. TOE design
AGD: Guidance documents	AGD_OPE.1. Operational user guidance AGD_PRE.1. Preparative procedures
ALC: Life cycle support	ALC_CMC.2. CM capabilities ALC_CMS.2. CM Scope ALC_DEL.1. Delivery ALC_FLR.2. Flaw remediation
ATE: Tests	ATE_COV.1. Coverage ATE_FUN.1. Functional tests ATE_IND.2. Independent testing
AVA: Vulnerability assessment	AVA_VAN.2. Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

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

Class	Component
FCS: Cryptographic Support	FCS_CKM.1(1) Cryptographic key generation (DEK/MK) FCS_CKM.1(2) Cryptographic key generation (User key) FCS_CKM.4 Cryptographic key destruction FCS_COP.1(1) Cryptographic operation (Data Encryption /Decryption) FCS_COP.1(2) Cryptographic operation (Key Encryption /Decryption) FCS_COP.1(3) Cryptographic operation (HMAC calculation) FCS_COP.1(4) Cryptographic operation (RSA Key Encryption)
FDP: User Data Protection	FDP_ACC.1(1) Subset access control (FDE) FDP_ACC.1(2) Subset access control (ASC) FDP_ACC.1(3) Subset access control (DAC) FDP_IFC.1 Subset information flow control (WAC) FDP_ACF.1(1) Security attribute based access control (FDE) FDP_ACF.1(2) Security attribute based access control (ASC) FDP_ACF.1(3) Security attribute based access control (DAC) FDP_IFF.1 Simple security attributes (WAC)
FIA: Identification and Authentication	FIA_UAU.2 User authentication before any action FIA_UID.2 User identification before any action
FMT: Security Management	FMT_MSA.1(1) Management of security attributes (FDE) FMT_MSA.1(2) Management of security attributes (ASC) FMT_MSA.1(3) Management of security attributes (DAC) FMT_MSA.1(4) Management of security attributes (WAC) FMT_MSA.3(1) Static attribute initialisation (FDE) FMT_MSA.3(2) Static attribute initialisation (ASC) FMT_MSA.3(3) Static attribute initialisation (DAC) FMT_MSA.3(4) Static attribute initialisation (WAC) FMT_MTD.1 Management of TSF data FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FAV: Anti-Virus	FAV_ACT.1 Anti-virus actions FAV_ALR.1 Anti-virus alerts FAV_SCN.1 Anti-virus scanning

IDENTIFICATION

Product: "Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0 version 10.3.0.6294 AES256"
Security Target: Security Target for Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0, version 1.01, January 2018.
Protection Profile: None.
Evaluation Level: Common Criteria v 3.1 R5 EAL2+ALC_FLR.1

SECURITY POLICIES

The use of the product "Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0 version 10.3.0.6294 AES256" 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.

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 3.4.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product "Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0 version 10.3.0.6294 AES256", 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 categorized below.

The detail of these threats is documented in the Security Target, section 3.2.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

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

The detail of these security objectives for the TOE operational environment is documented in the Security Target, section 4.2.

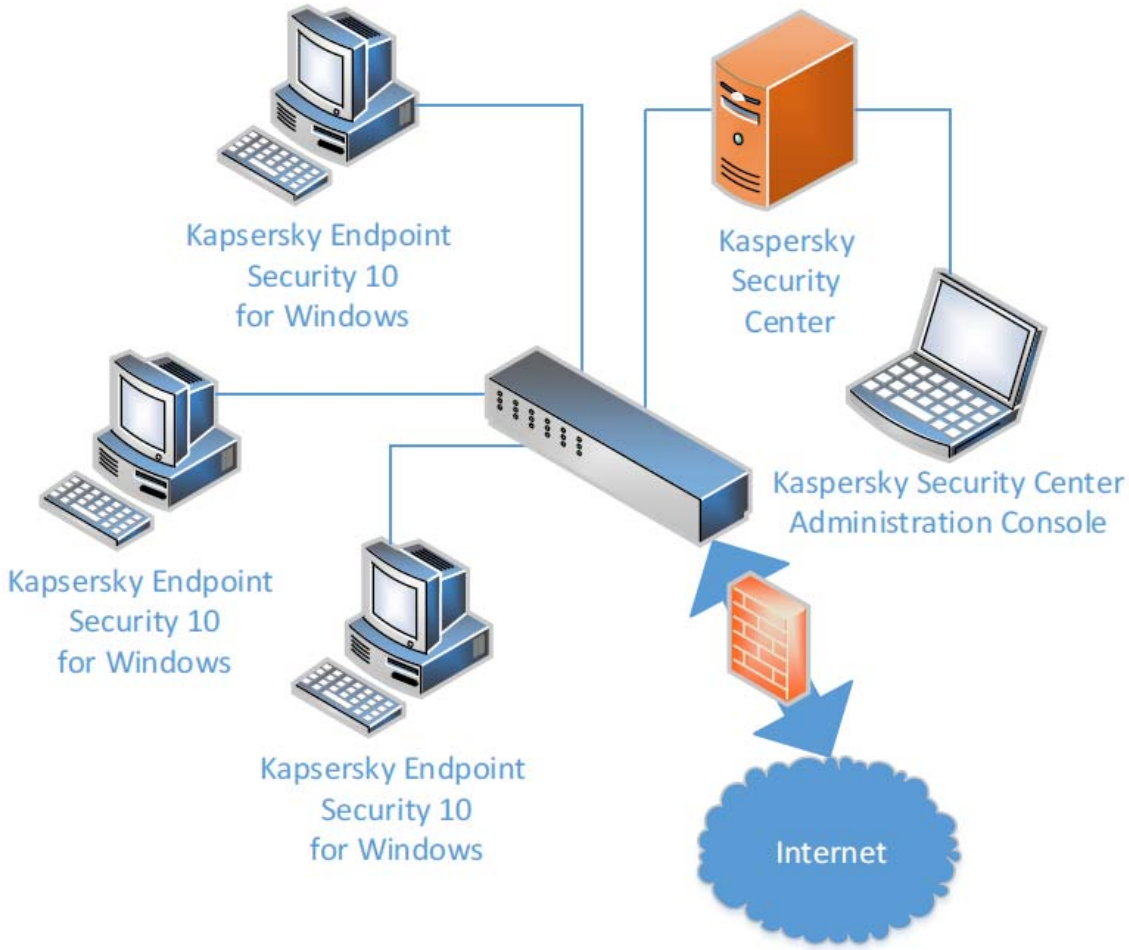
ARCHITECTURE

LOGICAL ARCHITECTURE

Kaspersky Endpoint Security consists of components, each of which is responsible for protection against a particular type of threat. They can be organised into three groups covering main product functionality:

1. Anti-Virus protection:
   - File system protection
   - Network protection and traffic scanning
   - IM Antivirus
   - Proactive Defense
2. Control:
   - Application Startup Control
   - Device Access Control
   - Web Access Control
3. Encryption:
   - Full Disk Encryption
   - Removable Device Encryption (not a part of evaluation)
   - File Level Encryption (not a part of evaluation)
4. Management of all above.

PHYSICAL ARCHITECTURE



DOCUMENTS

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

- Administration Guide for administering and maintaining Kaspersky Endpoint Security, and Full Disk Encryption ”Kaspersky Endpoint Security 10 for Windows. User Manual. Version 1.03”, distributed as PDF file with SHA256 checksum available on the ST.
- Addendum that references User Manual and TOE architectural evidences ”Kaspersky Endpoint Security 10 for Windows. User Manual. Addendum A. Version 1.03”, distributed as PDF file with SHA256 checksum available on the ST.
- Guide for preparing for installation and installing Kaspersky Endpoint Security, and Full Disk Encryption ”Preparative Procedures for Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0”. Version 1.04” distributed as PDF file with SHA256 checksum available on the ST.

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 all the developer functional tests in the developer premises. Likewise, he has selected and repeated all of the developer functional tests in the testing platform implemented in the evaluation laboratory.

In addition, the lab has devised a set of tests for each of the security functions 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.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product “Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0 version 10.3.0.6294 AES256” it is necessary the disposition of the following software components:

- Microsoft Windows 10 Professional x86 / x64
- Microsoft Windows 10 Enterprise x86 / x64
- Microsoft Windows 8.1 Enterprise x86 / x64
- Microsoft Windows 8.1 Pro x86 / x64
- Microsoft Windows 8 Pro x86 / x64
- Microsoft Windows 8 Enterprise x86 / x64
- Microsoft Windows 7 Professional x86 / x64 SP1
- Microsoft Windows 7 Enterprise x86 / x64 SP1

It works with the following file systems under Windows:

- FAT
- FAT32
- NTFS4

Regarding the hardware components, the TOE has to run on devices (usually personal computer systems) with the following minimum requirements:

- Processor: Intel Core i3 Duo 3.10GHz or equivalent
- RAM: 2GB of free RAM or more
- HDD: 2GB of available hard disk space
- Network connection peripherals

Among all the possibilities offered by these software and hardware requirements, the configuration selected for the evaluation is the following:

- PC with Intel Core i3 Duo 3.10GHz or equivalent with 4GB RAM or more, running Windows 10 enterprise 64 bits

EVALUATION RESULTS

The product “Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0 version 10.3.0.6294 AES256” has been evaluated against the Security Target for Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0.

All the assurance components required by the evaluation level EAL2 (augmented with ALC_FLR.1) have been assigned a “PASS” verdict. Consequently, the laboratory “Epoche & Espri S.L.U.” assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2 (augmented with ALC_FLR.1), as defined by 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.

Regarding the virus detection functionality, the TOE is able to detect a set of “Known malware” specified in Kaspersky Endpoint Security for Windows - User Manual. Addendum A version 1.03 [UMA103]. This document states the list of malware objects the TOE is able to detect.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product “Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0 version 10.3.0.6294 AES256”, 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:

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

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:

- Security Target for Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0, version 1.01, January 2018

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:

- Sanitized Security Target for Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0, version 1.02, 19-Feb-18

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 several national bodies. 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.sogisportal.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.

This certificate 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.