Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

DCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 5/22

(Certification No.)

Prodotto: **Kaspersky Security Center (version 13.0.0.11247)**
(Product)

Sviluppato da: **AO Kaspersky Lab**
(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard
ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard
ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL2+
(ALC_FLR.1)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 31 gennaio 2022

This page is intentionally left blank

Organismo di Certificazione della Sicurezza Informatica

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Kaspersky Security Center
(version 13.0.0.11247)

OCSI/CERT/CCL/03/2021/RC

Version 1.0

31 January 2022

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	31/01/2022

2 Table of contents

3 Acronyms

AES   Advanced Encryption Standard

CC   Common Criteria

CCRA   Common Criteria Recognition Arrangement

CEM   Common Evaluation Methodology

CPU   Central Processing Unit

DBMS   Database Management System

DPCM   Decreto del Presidente del Consiglio dei Ministri

EAL   Evaluation Assurance Level

ETR   Evaluation Technical Report

GB   Gigabyte

GHz   Gigahertz

IT   Information Technology

KSC   Kaspersky Security Center

LAN   Local Area Network

LGP   Linea Guida Provvisoria

LVS   Laboratorio per la Valutazione della Sicurezza

NIS   Nota Informativa dello Schema

OCSI   Organismo di Certificazione della Sicurezza Informatica

OS   Operating System

PP   Protection Profile

RAM   Random Access Memory

SAR   Security Assurance Requirement

SFR   Security Functional Requirement

SOGIS-MRA Senior Officials Group Information Systems Security – Mutual Recognition Arrangement

ST   Security Target

TLS   Transport Layer Security

TOE   Target of Evaluation

TSF   TOE Security Functionality

TSFI   TSF Interface

4   References

4.1   Criteria and regulations

[CC1]   CCMB-2017-04-001, "Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model", Version 3.1, Revision 5, April 2017

[CC2]   CCMB-2017-04-002, "Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components", Version 3.1, Revision 5, April 2017

[CC3]   CCMB-2017-04-003, "Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components", Version 3.1, Revision 5, April 2017

[CCRA]   "Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security", July 2014

[CEM]   CCMB-2017-04-004, "Common Methodology for Information Technology Security Evaluation – Evaluation methodology", Version 3.1, Revision 5, April 2017

[LGP1]   Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2]   Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3]   Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1]   Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2]   Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3]   Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS]   "Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", Version 3, January 2010

4.2 Technical documents

[ETR]   "Kaspersky Security Center (version 13.0.0.11247)" Evaluation Technical Report, v1, CCLab Software Laboratory, 7 January 2022

[KSCUM]   "Kaspersky Security Center (version 13.0.0.11247). User Manual", Version 2.00, AO Kaspersky Lab

[KSCUMA]   "Kaspersky Security Center (version 13.0.0.11247). User Manual. Addendum A", Version 2.02, AO Kaspersky Lab

[KSCPP]   "Kaspersky Security Center (version 13.0.0.11247). Preparative Procedures", Version 2.02, AO Kaspersky Lab, 8 November 2021

[ST]   "Kaspersky Security Center. Security Target", Version 2.02, AO Kaspersky Lab, 8 November 2021

5 Recognition of the certificate

5.1 European Recognition of CC Certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

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

This certificate is recognized under SOGIS-MRA for all declared assurance components.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all declared assurance components.

6   Statement of certification

The Target of Evaluation (TOE) is the product "Kaspersky Security Center (version 13.0.0.11247)", also referred to in the following as "KSC", developed by AO Kaspersky Lab.

The TOE is a software application designed for centralised management of other Kaspersky Lab security software applications (primarily anti-virus) installed on separate endpoint devices (for example, Kaspersky Endpoint Security for Windows), and, to some extent, for centralised management of those endpoint devices themselves.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL2, augmented with ALC_FLR.1, according to the information provided in the Security Target [ST] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product "Kaspersky Security Center (version 13.0.0.11247)" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Kaspersky Security Center (version 13.0.0.11247)
Security Target	"Kaspersky Security Center. Security Target", Version 2.02 [ST]
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.1
Developer	AO Kaspersky Lab
Sponsor	AO Kaspersky Lab
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	No compliance declared
Evaluation starting date	11 May 2021
Evaluation ending date	7 January 2022

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description, please refer to the Security Target [ST].

The TOE "Kaspersky Security Center (version 13.0.0.11247)" is a software application designed for centralised management of other Kaspersky Lab security software applications (primarily anti-virus) installed on separate endpoint devices (for example, Kaspersky Endpoint Security for Windows), and, to some extent, for centralised management of those endpoint devices themselves.

The main functionalities of the evaluated TOE are the following:

- Audit

- Administration

- Protected communication

For a detailed description of the TOE, consult sects. 1.3 and 1.4 of the Security Target [ST]. The most significant aspects are summarized below.

7.3.1 TOE architecture

The TOE can be divided into two subsystems:

- Administration Server

- Network Agent (on a managed endpoint device)

The TOE can comprise one instance of the Administration Server subsystem and multiple instances of the Network Agent subsystems on different managed endpoint machines. One Administration Server can manage multiple Network Agents, while one Network Agent can work only with one Administration Server.

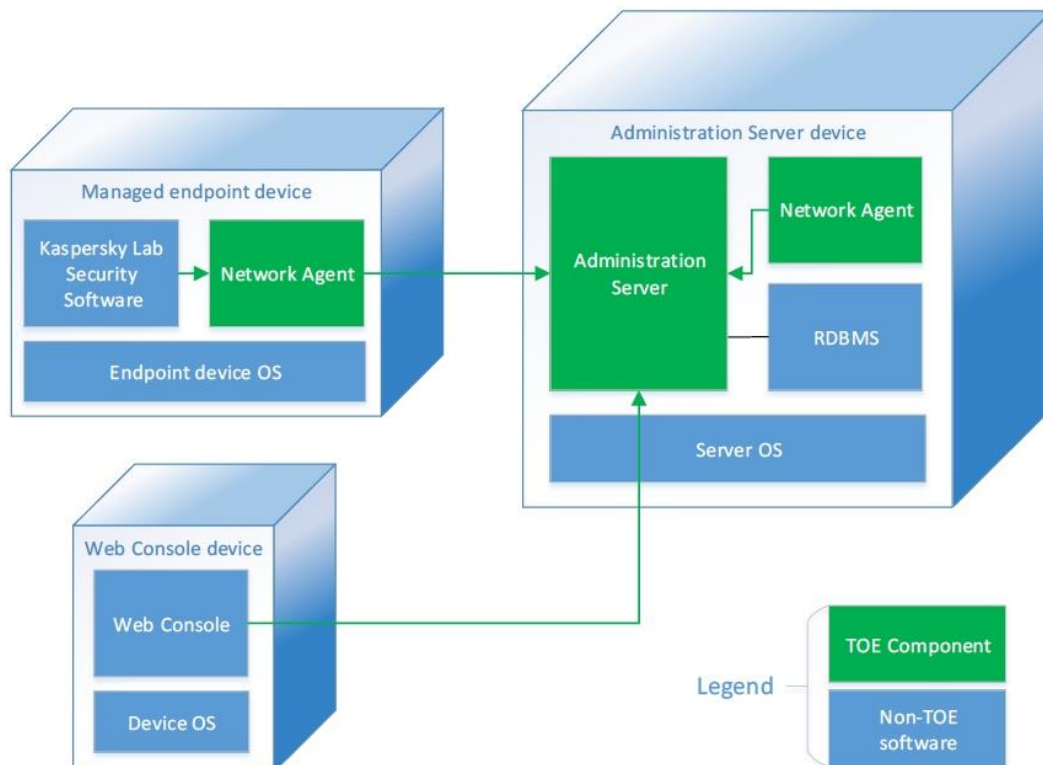The overview of the TOE physical architecture is given in Figure 1.

Figure 1 - TOE physical architecture

The Web Console is an application that uses a web interface provided by KSC for its management. The Web Console is not part of the TOE.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in sect. 3 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult sect. 7 of the Security Target [ST]. The most significant aspects are summarized below:

- **Audit**: the TOE generates audit records for its own audible events, and collects audit records from Kaspersky Lab security software installed on the managed endpoint devices, and provides means for audit reviewing.

- **Administration**: the TOE is able to remotely collect data from Kaspersky Lab security software installed on endpoint devices in an organization's LAN, and manage this software. Providing these administration capabilities, the TOE ensures that only authorised users are able to access this functionality. The TOE provides identification/authentication and role-based access control for the TOE administration.

- **Protected communication**: the implemented security mechanisms are oriented to protect the communications between physically divided parts of the TOE, ensuring the security of the sensitive data being sent from/to the managed devices. The communication used for the remote administration of the TOE is also protected by establishing a trusted channel to Web Console, which is not a part of the TOE.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All Security Functional Requirements (SFR) have been selected from CC Part 2 [CC2].

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7   Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab Software Laboratory.

The evaluation was completed on 7 January 2022 with the issuance by LVS of the Evaluation Technical Report [ETR] that has been approved by the Certification Body on 19 January 2022. Then, the Certification Body issued this Certification Report.

7.8   General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS CCLab Software Laboratory and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "Kaspersky Security Center (version 13.0.0.11247)" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2 augmented with ALC_FLR.1, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL2 augmented with ALC_FLR.1.

Assurance classes and components		Verdict
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.1	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Use of a CM system	ALC_CMC.2	Pass
Parts of the TOE CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass
Basic flaw remediation	*ALC_FLR.1*	Pass
Tests	**Class ATE**	Pass

Assurance classes and components		Verdict
Evidence of coverage	ATE_COV.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 - Final verdicts for assurance requirements

8.2   Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 (Statement of Certification).

Potential customers of the product "Kaspersky Security Center (version 13.0.0.11247)" are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Organizational Security Policies and the Assumptions described, respectively, in sect. 3.3 and 3.4 of the Security Target [ST] are respected.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, Annex A – Guidelines for the secure usage of the product includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([KSCUM], [KSCUMA], [KSCPP]).

9   Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1   TOE delivery

The TOE consists of the following items:

1. The program code of the KSC delivered as a binary installation package:
   `ksc_13_13.0.0.11247_full_en.exe`
   SHA256 checksum: 42210DB5E9F5EFE9A18E9B8F3C4BC7CF71433BBB844C1F6170586243B8370B27

2. The User Manual for administering and maintaining the TOE "Kaspersky Security Center. User Manual", version 2.00, distributed as PDF file
   SHA256 checksum 27C4FCD9C24EA8835C964F18C43DC03D491F711B2F5B0A7F34C6E11FD0BE968B

3. The User Manual addendum "Kaspersky Security Center. User Manual. Addendum A", version 2.02, distributed as PDF file
   SHA256 checksum 5667972B31C2F58537B584478F201FF1E97FA6BCCA99FDEC001B097F31412E6C

4. The Guide for preparing for installation and installing KSC "Kaspersky Security Center. Preparative procedures", version 2.02, distributed as PDF file
   SHA256 checksum DFBB230939D34B6667CEE67D7F75B7F9DE32BE59B00391218CCB46D0A84D0A11

The delivery of the TOE is secured in a manner that any user is able to determine the authenticity of the software package received. The delivery package, including the TOE and associated documentation is downloaded from Kaspersky Lab website

All executable files of the TOE, including installation package, are digitally signed with a Code Signing Certificate with a timestamp. This allows customers to verify the origin, integrity and authenticity of the TOE. Also, the SHA256 checksums of the TOE binary files are provided to the customers to confirm that the received TOE files are the expected ones.

9.2   Installation, initialization and secure usage of the TOE

TOE installation, configuration and operation should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the following documents contain detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST]:

- Kaspersky Security Center. Preparative Procedures [KSCPP]

- Kaspersky Security Center. User Manual [KSCUM]

- Kaspersky Security Center. User Manual. Addendum A [KSCUMA]

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product "Kaspersky Security Center (version 13.0.0.11247)", developed by AO Kaspersky Lab.

The name and version number uniquely identify the TOE and the set of its subsystems, constituting the evaluated configuration of the TOE, verified by the Evaluators at the time the tests are carried out and to which the results of the evaluation are applied.

The evaluated TOE deployment configuration includes the following elements:

- The Administration Server component (part of the TOE) installed on a device (server) running Windows Server OS. The DBMS is installed on the same device.

- The Web Console (not part of the TOE) installed on a device running Windows OS.

- The Network Agent (part of the TOE) installed on a managed endpoint device running Windows OS.

- All devices connected to a LAN.

For more details, including lists of supported OSes and DBMSs, please refer to sect. 1.3.3 of the Security Target [ST].

10.1 TOE operational environment

To ensure proper operation of the TOE, the device (workstation or server) must meet the following minimum hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For 64-bit operating systems, the minimum CPU frequency is 1.4 GHz.

- RAM: 4 GB for Administration Server, 512 MB for Network Agent.

- Available disk space: 10 GB for Administration Server, 1 GB for Network Agent.

For more details please refer to sect. 1.3.3 of the Security Target [ST].

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level EAL2, augmented with ALC_FLR.1, such activities include the following three steps:

- evaluation of the tests performed by the Developer in terms of coverage;

- execution of independent functional tests by the Evaluators;

- execution of penetration tests by the Evaluators.

11.1 Test configuration

The Evaluators executed all the test cases on the test environment which was provided by the Developer.

The TOE test setup was prepared according to the Developer's test plan. The test environment consists of three virtual machines, which need to be in the same LAN. The test environment includes the following items:

- Server 1 device with the following software installed:

  o Windows Server 2016 Standard 64-bit (version 1607)

  o Administration Server

  o MySQL 5.7

  o Wireshark

- Host 1 device with the following software installed:

  o Windows 10 Education (20H2) 64-bit

  o Web Console 13.0.10286

  o OpenSSL

  o Nmap

- Host 2 device with the following software installed:

  o Windows 10 Education (20H2) 64-bit

  o Network Agent

  o Kaspersky Endpoint Security for Windows (11.6.0.394 AES 256)

The Evaluators installed the TOE following the preparative procedures supplied in the document [KSCPP].

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer's test documentation includes a total of 16 test cases mapping the TSFIs listed in the functional specification document. The Developer also included additional test cases associated to cryptographic support SFRs.

The Evaluators found that functionalities corresponding to the TSFI-CMD-S and TSFI-CMD-N (command-line interfaces for conducting administrative tasks with the TOE, mainly as a maintenance) were only marginally tested, so they focused on these interfaces during the independent testing to compensate for the incomplete coverage. There is also only one test case that covers TSFI-CONN (a program interface used to transport data between the TOE and managed applications), but that interface is not meant to be accessed directly by any user.

11.2.2 Test results

In the Developer's test documentation every test case has a unique test case number and a title. For each test the pre-requisites required for the test setup are included, along with detailed step-by-step instructions for execution, the expected result and the actual result.

The actual test results of all Developer's tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Testing approach

The Evaluators selected a subset of the Developer's tests that covers all of the TSFIs of the TOE.

The Evaluators selected the Developer's tests aiming to test the TOE in depth and created own test cases to further increase the tested functionalities of the TOE resulting in a more rigorous coverage.

In particular, the Evaluators performed specific tests for the following TOE functionalities:

- verify that the backup cannot be restored without knowing the correct password;

- specify the address of the administration server for connection running a command line tool as administrator.

11.3.2 Test results

The Evaluators ran all tests on the test environment provided by the Developer. The TOE test setup was prepared according to the Developer's test plan and the preparative procedures supplied in the document [KSCPP].

All Developer's tests were run successfully. The Evaluators verified the correct behavior of the TSFIs and correspondence between expected results and achieved results for each test.

All test cases devised by the Evaluators passed, i.e., all the actual test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the same TOE test setup already used for the functional test activities, verifying that the test configuration was consistent with the version of the TOE under evaluation.

The Evaluators first performed a search of public domain sources to identify potential vulnerabilities in the TOE. This activity revealed the following potential vulnerabilities in the TLS 1.2 protocol implementation:

- The "Logjam" attack (CVE-2015-4000)

- The "Raccoon" attack (https://raccoon-attack.com/)

However, the very high complexity of these attacks would require a greater attack potential than Basic, so the above vulnerabilities are considered residual.

The Evaluator also executed the following attack scenarios:

- Distributing installation packages through cleartext channels.

- Remote code execution with System user.

- Remote code execution with unprivileged user.

- Password brute force.

- Enumeration of Installation packages.

They did not result in any exploitable vulnerability.

Based on the vulnerability analysis and the penetration testing results, the Evaluators could then conclude that the TOE is resistant to an attack potential of Basic in its intended operational environment. No exploitable vulnerabilities have been identified.