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

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)

Firmato digitalmente
da Eva Spina
Data: 2022.01.31
09:21:37 +01'00'

Roma, 31 gennaio 2022

Common Criteria

SOGIS IT SECURITY CERTIFIED

Questa pagina è lasciata intenzionalmente vuota

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

Rapporto di Certificazione

Kaspersky Security Center (version 13.0.0.11247)

OCSI/CERT/CCL/03/2021/RC

Versione 1.0

31 gennaio 2022

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	31/01/2022

2 Indice

3 Elenco degli acronimi

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
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
ODV	Oggetto della Valutazione
PP	Protection Profile
RAM	Random Access Memory
RFV	Rapporto Finale di Valutazione
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SO	Sistema Operativo
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Arrangement

ST	Security Target
TDS	Traguardo di Sicurezza
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

4 Riferimenti

4.1 Criteri e normative

[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 Documenti tecnici

[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

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

[TDS] “Kaspersky Security Center. Security Target”, Version 2.02, AO Kaspersky Lab, 8 November 2021

5 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA)

L'accordo di mutuo riconoscimento in ambito europeo (SOGIS-MRA, versione 3, [SOGIS]) è entrato in vigore nel mese di aprile 2010 e prevede il riconoscimento reciproco dei certificati rilasciati in base ai Common Criteria (CC) per livelli di valutazione fino a EAL4 incluso per tutti i prodotti IT. Per i soli prodotti relativi a specifici domini tecnici è previsto il riconoscimento anche per livelli di valutazione superiori a EAL4.

L'elenco aggiornato delle nazioni firmatarie e dei domini tecnici per i quali si applica il riconoscimento più elevato e altri dettagli sono disponibili su https://www.sogis.eu/.

Il logo SOGIS-MRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito SOGIS-MRA per tutti i componenti di garanzia dichiarati.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su https://www.commoncriteriaportal.org/.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA per tutti i componenti di garanzia dichiarati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "Kaspersky Security Center (version 13.0.0.11247)", nel seguito del documento anche indicato come "KSC", sviluppato da AO Kaspersky Lab.

L'ODV è un'applicazione software progettata per la gestione centralizzata di altre applicazioni di sicurezza prodotte da Kaspersky Lab (principalmente antivirus) installate su dispositivi *endpoint* separati (ad esempio, Kaspersky Endpoint Security for Windows) e, in una certa misura, per la gestione centralizzata dei dispositivi *endpoint* stessi.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti e/o utilizzatori. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.1, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "Kaspersky Security Center (version 13.0.0.11247)" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

Il presente Rapporto di Certificazione deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	Kaspersky Security Center (version 13.0.0.11247)
Traguardo di Sicurezza	"Kaspersky Security Center. Security Target", Version 2.02 [TDS]
Livello di garanzia	EAL2 con l'aggiunta di ALC_FLR.1
Fornitore	AO Kaspersky Lab
Committente	AO Kaspersky Lab
LVS	CCLab Software Laboratory
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	11 maggio 2021
Data di fine della valutazione	7 gennaio 2022

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo paragrafo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV "Kaspersky Security Center (version 13.0.0.11247)" è un'applicazione software progettata per la gestione centralizzata di altre applicazioni di sicurezza prodotte da Kaspersky Lab (principalmente antivirus) installate su dispositivi *endpoint* separati (ad esempio, Kaspersky Endpoint Security for Windows) e, in una certa misura, per la gestione centralizzata dei dispositivi *endpoint* stessi.

Le principali funzionalità dell'ODV sono le seguenti:

- Audit
- Amministrazione
- Protezione delle comunicazioni

Per una descrizione dettagliata dell'ODV, si consulti il par. 1.3 e il par. 1.4 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito.

7.3.1 Architettura dell'ODV

L'ODV può essere suddiviso nei seguenti due sottosistemi:

- Administration Server
- Network Agent (installato su un dispositivo *endpoint* gestito)

L'ODV può comprendere un'istanza del sottosistema Administration Server e più istanze dei sottosistemi Network Agent su diverse macchine *endpoint* gestite. Un Administration Server può gestire più Network Agent, mentre un Network Agent può funzionare solo in presenza di un Administration Server.

In Figura 1 è illustrata una panoramica dell'architettura fisica dell'ODV.

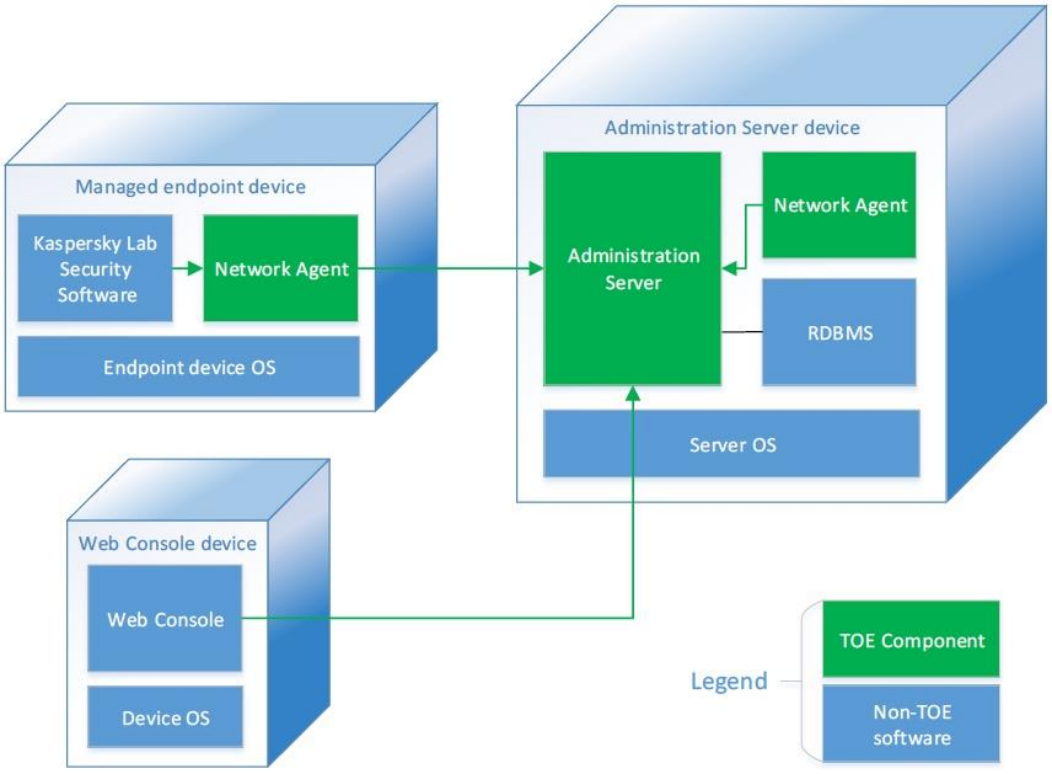

Figura 1 - Architettura fisica dell'ODV

La Web Console è un'applicazione che utilizza un'interfaccia Web fornita da KSC per la propria gestione. La Web Console non fa parte dell'ODV.

7.3.2 Caratteristiche di sicurezza dell'ODV

Il problema di sicurezza dell'ODV, comprendente obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza dell'organizzazione, è definito nel cap. 3 del Traguardo di Sicurezza [TDS].

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il cap. 7 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Audit**: l'ODV genera record di audit relativi ai propri eventi auditabili e raccoglie i record di audit dal software di sicurezza di Kaspersky Lab installato sui dispositivi *endpoint* gestiti, fornendo inoltre strumenti per la verifica dei record di audit.

- **Amministrazione**: l'ODV è in grado di raccogliere da remoto i dati dal software di sicurezza di Kaspersky Lab installato su dispositivi *endpoint* nella LAN di un'organizzazione e di gestire questi applicativi. L'ODV garantisce che solo gli utenti autorizzati possano accedere alle funzionalità di amministrazione. Per le proprie funzioni di amministrazione l'ODV fornisce identificazione e autenticazione e controllo di accesso basato sui ruoli.

- **Protezione delle comunicazioni**: l'ODV implementa meccanismi di sicurezza per la protezione delle comunicazioni tra parti fisicamente separate dell'ODV stesso, garantendo la sicurezza dei dati sensibili inviati da e verso i dispositivi gestiti. Le comunicazioni utilizzate per l'amministrazione remota dell'ODV sono inoltre protette mediante un canale attendibile instaurato con la Web Console, che non fa parte dell'ODV.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita al cliente insieme al prodotto.

La documentazione indicata contiene le informazioni richieste per l'inizializzazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] non dichiara conformità ad alcun Profilo di Protezione.

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3].

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati derivati direttamente dai CC Parte 2 [CC2].

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, gli SFR e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS CCLab Software Laboratory.

L'attività di valutazione è terminata in data 7 gennaio 2022 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 19 gennaio 2022. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS CCLab Software Laboratory e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "Kaspersky Security Center (version 13.0.0.11247)" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.1, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL2, con l'aggiunta di ALC_FLR.1.

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

Classi e componenti di garanzia		Verdetto
Test	**Classe ATE**	Positivo
Evidence of coverage	ATE_COV.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Vulnerability analysis	AVA_VAN.2	Positivo

Tabella 1 - Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 5.1 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "Kaspersky Security Center (version 13.0.0.11247)" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel par. 4.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le Politiche di Sicurezza dell'Organizzazione e le ipotesi descritte rispettivamente nel par. 3.3 e nel par. 3.4 del Traguardo di Sicurezza [TDS].

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella sua configurazione valutata. In particolare, l'Appendice A – Indicazioni per l'uso sicuro del prodotto del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'inizializzazione, all'installazione e all'utilizzo sicuro del prodotto, in accordo con la documentazione di guida fornita con l'ODV ([KSCUM], [KSCUMA], [KSCPP]).

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

9.1 Consegna dell'ODV

L'ODV è costituito dai seguenti elementi:

1. Il codice eseguibile del programma KSC consegnato in forma di pacchetto di installazione binario:
   `ksc_13_13.0.0.11247_full_en.exe`
   SHA256 checksum: 42210DB5E9F5EFE9A18E9B8F3C4BC7CF71433BBB844C1F6170586243B8370B27

2. Il manuale d'utente per l'amministrazione e la manutenzione dell'ODV "Kaspersky Security Center. User Manual", versione 2.00, distribuito in forma di file PDF
   SHA256 checksum 27C4FCD9C24EA8835C964F18C43DC03D491F711B2F5B0A7F34C6E11FD0BE968B

3. L'appendice al manuale utente "Kaspersky Security Center. User Manual. Addendum A", versione 2.02, distribuito in forma di file PDF
   SHA256 checksum 5667972B31C2F58537B584478F201FF1E97FA6BCCA99FDEC001B097F31412E6C

4. La guida per la preparazione e l'installazione dell'ODV "Kaspersky Security Center. Preparative procedures", versione 2.02, distribuita in forma di file PDF
   SHA256 checksum DFBB230939D34B6667CEE67D7F75B7F9DE32BE59B00391218CCB46D0A84D0A11

La consegna dell'ODV è effettuata in maniera sicura, in modo tale da consentire all'utente di determinare l'autenticità del pacchetto software ricevuto. Il pacchetto di consegna, che include l'ODV e la documentazione associata, viene scaricato dal sito Web di Kaspersky Lab.

Tutti i file eseguibili dell'ODV, incluso il pacchetto di installazione, sono firmati digitalmente con un certificato di firma del codice con una marca temporale. Ciò consente ai clienti di verificare l'origine, l'integrità e l'autenticità dell'ODV. Inoltre, vengono forniti ai clienti i valori di *checksum* SHA256 dei file binari dell'ODV che consentono di verificare che i file ricevuti sono quelli previsti.

9.2 Installazione, inizializzazione e utilizzo sicuro dell'ODV

L'installazione, la configurazione e l'operatività dell'ODV devono essere eseguite secondo le istruzioni riportate nelle sezioni appropriate della documentazione di guida fornita con il prodotto al cliente.

In particolare, i seguenti documenti contengono informazioni dettagliate per l'inizializzazione sicura dell'ODV, la preparazione del suo ambiente operativo e il funzionamento sicuro dell'ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS]:

- Kaspersky Security Center. Preparative Procedures [KSCPP]
- Kaspersky Security Center. User Manual [KSCUM]

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

10 Appendice B – Configurazione valutata

L'oggetto della valutazione (ODV) è il prodotto "Kaspersky Security Center (version 13.0.0.11247)", sviluppato dalla società AO Kaspersky Lab.

Il nome e il numero di versione identificano in modo univoco l'ODV e l'insieme dei suoi sottosistemi, che costituiscono la configurazione valutata dell'ODV verificata dai Valutatori al momento dell'effettuazione dei test e alla quale si applicano i risultati della valutazione.

La configurazione valutata della distribuzione dell'ODV include i seguenti elementi:

- Il componente Administration Server (compreso nell'ODV) installato su un dispositivo (server) con sistema operativo Windows Server. Su questo dispositivo è installato anche il DBMS.
- La Web Console (non facente parte dell'ODV) installata su un dispositivo con sistema operativo Windows.
- Il componente Network Agent (compreso nell'ODV) installato su un dispositivo *endpoint* gestito con sistema operativo Windows.
- Tutti i dispositivi connessi ad una LAN.

Per maggiori dettagli, incluse le liste dei sistemi operativi e dei DBMS supportati, si consulti il par. 1.3.3 del Traguardo di Sicurezza [TDS].

10.1 Ambiente operativo dell'ODV

Per garantire il corretto funzionamento dell'ODV, il dispositivo (workstation o server) deve soddisfare i seguenti requisiti minimi generali:

- CPU con frequenza operativa di 1 GHz o superiore. Per i sistemi a 64-bit è richiesta una CPU con frequenza minima di 1.4 GHz.
- RAM: 4 GB per l'Administration Server, 512 MB per il Network Agent.
- Spazio disponibile su disco: 10 GB per l'Administration Server, 1 GB per il Network Agent.

Per maggiori dettagli si consulti il par. 1.3.3 del Traguardo di Sicurezza [TDS].

11 Appendice C – Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.1, tali attività tali attività prevedono tre passi successivi:

- valutazione dei test eseguiti dal Fornitore in termini di copertura;
- esecuzione di test funzionali indipendenti da parte dei Valutatori;
- esecuzione di test di intrusione da parte dei Valutatori.

11.1 Configurazione per i Test

I Valutatori hanno eseguito tutti i casi di test sull'ambiente di test messo a disposizione dal Fornitore.

L'ambiente di test dell'ODV è stato predisposto e configurato secondo quanto descritto nel piano di test del Fornitore. L'ambiente di test è costituito da tre macchine virtuali situate nella stessa LAN e include i seguenti elementi:

- Dispositivo Server 1 con il seguente software installato:
  - Windows Server 2016 Standard 64-bit (version 1607)
  - Administration Server
  - MySQL 5.7
  - Wireshark
- Dispositivo Host 1 con il seguente software installato:
  - Windows 10 Education (20H2) 64-bit
  - Web Console 13.0.10286
  - OpenSSL
  - Nmap
- Dispositivo Host 2 con il seguente software installato:
  - Windows 10 Education (20H2) 64-bit
  - Network Agent
  - Kaspersky Endpoint Security for Windows (11.6.0.394 AES 256)

I Valutatori hanno installato l'ODV seguendo le procedure preparatorie fornite nel documento [KSCPP].

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

La documentazione di test del Fornitore include un totale di 16 casi di test mappati sulle TSFI elencate nel documento di specifiche funzionali. Il Fornitore ha incluso anche casi di test aggiuntivi associati agli SFR relativi al supporto crittografico.

I Valutatori hanno riscontrato che le funzionalità corrispondenti alle interfacce TSFI-CMD-S e TSFI-CMD-N (interfacce a riga di comando per lo svolgimento di attività amministrative sull'ODV, principalmente per manutenzione) sono state testate solo marginalmente, e si sono quindi concentrati su queste interfacce durante i test indipendenti per compensare la copertura insufficiente. È stato inoltre previsto un solo test case che copre l'interfaccia TSFI-CONN (un'interfaccia di programma utilizzata per trasportare i dati tra l'ODV e le applicazioni gestite), ma tale interfaccia non è pensata per l'accesso diretto da parte di qualsiasi tipo d'utente.

11.2.2 Risultati dei test

Nella documentazione di test del Fornitore, ad ogni caso di test sono associati un numero e un titolo univoci. Per ogni test sono inclusi i prerequisiti necessari per la sua configurazione, le istruzioni dettagliate per la sua esecuzione, il risultato previsto e il risultato effettivo.

I risultati effettivi ottenuti da tutti i test del Fornitore sono risultati conformi a quelli previsti.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

11.3.1 Approccio adottato per i test

I Valutatori hanno selezionato un sottoinsieme dei test del Fornitore che copre tutte le TSFI.

I Valutatori hanno selezionato i test del Fornitore con l'obiettivo di verificare l'ODV in profondità e hanno progettato casi di test aggiuntivi per aumentare ulteriormente le funzionalità dell'ODV testate, ottenendo una copertura più rigorosa.

In particolare, i Valutatori hanno eseguito test specifici per le seguenti funzionalità dell'ODV:

- verifica che un backup non possa essere ripristinato senza conoscere la password corretta;
- specifica dell'indirizzo per la connessione del server di amministrazione eseguendo uno strumento a riga di comando come amministratore.

11.3.2 Risultati dei test

I Valutatori hanno eseguito tutti i test sull'ambiente di test messo a disposizione dal Fornitore. L'ambiente di test dell'ODV è stato predisposto e configurato secondo quanto descritto nel piano di test del Fornitore e nelle procedure preparatorie fornite nel documento [KSCPP].

Tutti i test del Fornitore sono stati eseguiti con successo. I Valutatori hanno verificato il corretto comportamento delle TSFI e la corrispondenza tra risultati attesi e risultati ottenuti per ogni test.

Tutti i casi di test progettati dai Valutatori hanno avuto esito positivo, ovvero tutti i risultati dei test sono risultati conformi a quelli previsti.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività i Valutatori hanno lavorato sullo stesso ambiente di test dell'ODV già utilizzato per le attività dei test funzionali, verificando che la configurazione di test fosse congruente con la versione dell'ODV in valutazione.

In una prima fase, i Valutatori hanno condotto ricerche su fonti pubbliche per identificare potenziali vulnerabilità dell'ODV. Come risultato di questa attività, sono state identificate le seguenti vulnerabilità potenziali nell'implementazione del protocollo TLS 1.2:

- Attacco "Logjam" (CVE-2015-4000)
- Attacco "Raccoon" (https://raccoon-attack.com/)

Tuttavia, la complessità molto elevata di questi attacchi richiede un potenziale di attacco superiore al livello Basic; di conseguenza, le vulnerabilità sopra elencate sono da considerare residue.

I Valutatori hanno altresì eseguito test specifici per i seguenti scenari di attacco:

- Distribuzione dei pacchetti di installazione tramite canali non cifrati.
- Esecuzione di codice da remoto come utente System.
- Esecuzione di codice da remoto come utente non privilegiato.
- Attacco a forza bruta alle password.
- Enumerazione dei pacchetti di installazione.

Questi test non hanno evidenziato nessuna vulnerabilità sfruttabile.

Sulla base dell'analisi di vulnerabilità e dei risultati dei test di intrusione, i Valutatori hanno quindi concluso che l'ODV, nel suo ambiente operativo, è in grado di resistere ad un attaccante che possiede un potenziale di attacco di livello Basic. Non sono state identificate vulnerabilità sfruttabili.