*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. 4/22

*(Certification No.)*

**Prodotto:** **Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)**
*(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
09:22:20 +01'00'

Roma, 26 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 Endpoint Security for Windows (version 11.6.0.394 AES256)

OCSI/CERT/CCL/02/2021/RC

Versione 1.1

31 gennaio 2022

## Nota editoriale

Il presente documento sostituisce la versione 1.0 del Rapporto di Certificazione OCSI/CERT/CCL/02/2021/RC associato al Certificato n. 4/22 del 26 gennaio 2022.

La versione corrente di questo Rapporto di Certificazione include unicamente correzioni di carattere editoriale (refusi, errori di formattazione, ecc.) e non modifica in alcun modo il contenuto informativo del testo.

Il Certificato mantiene la sua validità a partire dalla data di prima emissione.

# 1 Revisioni del documento

| Versione | Autori | Modifiche | Data |
|---|---|---|---|
| 1.0 | OCSI | Prima emissione | 26/01/2022 |
| 1.1 | OCSI | Correzioni editoriali | 31/01/2022 |
| | | | |

# 2 Indice

# 3 Elenco degli acronimi

| | |
|---|---|
| **AES** | Advanced Encryption Standard |
| **AV** | Anti-Virus |
| **CC** | Common Criteria |
| **CCRA** | Common Criteria Recognition Arrangement |
| **CEM** | Common Evaluation Methodology |
| **CPU** | Central Processing Unit |
| **DLL** | Dynamic-link library |
| **DPCM** | Decreto del Presidente del Consiglio dei Ministri |
| **DRBG** | Deterministic Random Bit Generator |
| **EAL** | Evaluation Assurance Level |
| **ETR** | Evaluation Technical Report |
| **FDE** | Full Disk Encryption |
| **GB** | Gigabyte |
| **GHz** | Gigahertz |
| **HMAC** | Keyed-Hash Message Authentication Code |
| **IT** | Information Technology |
| **KES** | Kaspersky Endpoint Security |
| **KSC** | Kaspersky Security Center |
| **LAN** | Local Area Network |
| **LGP** | Linea Guida Provvisoria |
| **LVS** | Laboratorio per la Valutazione della Sicurezza |
| **NIS** | Nota Informativa dello Schema |
| **NIST** | National Institute of Standards and Technology |
| **OCSI** | Organismo di Certificazione della Sicurezza Informatica |
| **ODV** | Oggetto della Valutazione |

| | |
|---|---|
| **PBKDF2** | Password-Based Key Derivation Function 2 |
| **PP** | Protection Profile |
| **RAM** | Random Access Memory |
| **RFV** | Rapporto Finale di Valutazione |
| **RSA** | Rivest, Shamir, Adleman |
| **SAR** | Security Assurance Requirement |
| **SFR** | Security Functional Requirement |
| **SIMD** | Single Instruction stream, Multiple Data stream |
| **SO** | Sistema Operativo |
| **SOGIS-MRA** | Senior Officials Group Information Systems Security – Mutual Recognition Arrangement |
| **SSE** | Streaming SIMD Extensions |
| **ST** | Security Target |
| **TDS** | Traguardo di Sicurezza |
| **TLS** | Transport Layer Security |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functionality |
| **TSFI** | TSF Interface |
| **XML** | Extensible Markup Language |
| **XXE** | XML External Entity |

# 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

[CC-STL] CCDB-2006-04-004, “ST sanitising for publication”, April 2006

[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

[KESUM] “Kaspersky Endpoint Security for Windows. User Manual”, Version 2.01, AO Kaspersky Lab

[KESUMA] “Kaspersky Endpoint Security for Windows. User Manual. Addendum A”, Version 2.04, AO Kaspersky Lab, 26 November 2021

[KESPP] “Kaspersky Endpoint Security for Windows. Preparative Procedures”, Version 2.03, AO Kaspersky Lab, 26 November 2021

[RFV] “Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)” Evaluation Technical Report, v1, CCLab Software Laboratory, 6 December 2021

[TDS] “Kaspersky Endpoint Security for Windows. Security Target”, Version 2.04, AO Kaspersky Lab, 26 November 2021

[ST-LITE] “Kaspersky Endpoint Security for Windows. Security Target Lite”, Version 2.04, AO Kaspersky Lab, 26 November 2021 (sanitised public document)

# 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 Endpoint Security for Windows (version 11.6.0.394 AES256)", nel seguito del documento anche indicato come "KES", sviluppato da AO Kaspersky Lab.

L'ODV è un prodotto software che fornisce un'ampia gamma di funzionalità di sicurezza per i dispositivi *endpoint*, tra cui cifratura dei dati del dispositivo, antivirus e controllo degli accessi. Assieme al prodotto Kaspersky Security Center (KSC), una console di gestione centralizzata, KES realizza una suite di sicurezza informatica per la protezione di personal computer che utilizzano i sistemi operativi Windows.

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.

È stato fornito per la pubblicazione un Traguardo di Sicurezza "Lite" [ST-LITE]. Si tratta di una versione emendata del Traguardo di Sicurezza [TDS] utilizzato per la valutazione, da cui sono state rimosse informazioni tecniche riservate e proprietarie. La versione "Lite" del TDS è stata prodotta in conformità al documento di supporto del CCRA [CC-STL].

# 7 Riepilogo della valutazione

## 7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)" 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 Endpoint Security for Windows (version 11.6.0.394 AES256) |
| **Traguardo di Sicurezza** | "Kaspersky Endpoint Security for Windows. Security Target", Version 2.04 [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** | 6 dicembre 2021 |

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 Endpoint Security for Windows (version 11.6.0.394 AES256)" è un prodotto software che fornisce un'ampia gamma di funzionalità di sicurezza per i dispositivi *endpoint*, tra cui cifratura dei dati del dispositivo (dati utente e dati del sistema operativo),

antivirus e controllo degli accessi. Assieme al prodotto Kaspersky Security Center (KSC), una console di gestione centralizzata, KES realizza una suite di sicurezza informatica per la protezione di personal computer (workstation, laptop e altri dispositivi) che utilizzano i sistemi operativi Windows.

KES combina in un'unica applicazione le funzionalità di anti-malware, controllo dell'avvio delle applicazioni, controllo di accesso ai dispositivi, controllo di accesso al Web e cifratura dei dati.

La funzionalità Full Disk Encryption (FDE) aiuta a proteggere i dati aziendali importanti da perdite accidentali dovute allo smarrimento o al furto dei dispositivi.

Le principali funzionalità dell'ODV sono le seguenti:

- Protezione antivirus:
  - protezione del file system;
  - protezione della rete e scansione del traffico;
  - difesa proattiva.
- Controlli:
  - controllo dell'avvio delle applicazioni;
  - controllo degli accessi al dispositivo;
  - controllo degli accessi al Web.
- Cifratura completa del disco (FDE).
- Gestione delle funzioni sopra elencate, inclusa identificazione e autenticazione dell'utente.

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 è costituito dai seguenti sottosistemi:

- **Sottosistema FDE**: questo sottosistema fornisce meccanismi per negare l'accesso ai dati del dispositivo e alle chiavi crittografiche da parte di un individuo non autorizzato che ha accesso fisico al dispositivo spento. Questo sottosistema applica tutte le funzionalità relative alla crittografia e fornisce al sistema operativo la capacità di eseguire operazioni di lettura/scrittura su dischi cifrati. FDE richiede che ogni utente sia identificato e autenticato con successo prima di invocare la funzionalità di sicurezza responsabile della decifratura trasparente dei dischi cifrati. Questo sottosistema fornisce agli utenti autorizzati la possibilità di modificare la propria password.

- **Sottosistema KES**: questo sottosistema applica la politica di accesso ai dispositivi e di controllo delle applicazioni utilizzando regole configurabili in modo sicuro. KES gestisce i ruoli KLUser e KLAdmin ed è in grado di associare ad essi utenti paticolari. KES richiede che ogni utente sia identificato e autenticato con successo prima di invocare le funzionalità di sicurezza.

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

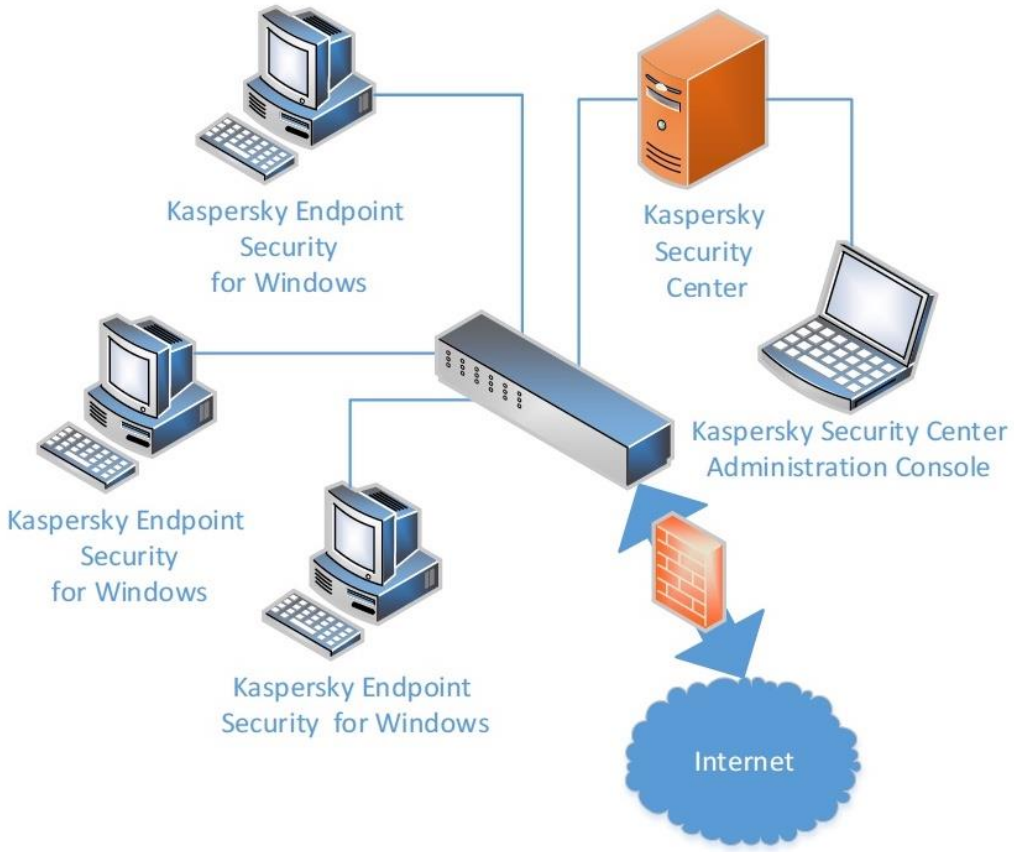


Figura 1 - Architettura fisica dell'ODV

### 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:

- **Funzionalità Full Disk Encryption**:

    1. Cifratura dati/generazione chiave master: durante l'installazione dell'ODV e la cifratura iniziale dei dati dei dispositivi (inizializzazione), viene utilizzato un generatore di numeri casuali deterministico per la generazione delle chiavi crittografiche AES necessarie. Le chiavi sono generate da una libreria

crittografica dell'ODV utilizzando l'algoritmo Hash_DRBG, in accordo a NIST SP 800-90A con SHA-256.

2. Generazione chiave crittografica dell'utente: durante l'installazione dell'ODV e la cifratura iniziale dei dati dei dispositivi (inizializzazione), viene utilizzato un generatore di numeri casuali deterministico per la generazione delle chiavi crittografiche AES necessarie (Chiavi utente). Le chiavi vengono generate dalla libreria crittografica dell'ODV mediante la Password-Based Key Derivation Function 2 (PBKDF2) con HMAC-SHA256, valore di iterazione 10.000, *salt* a 256 bit e password come input, in accordo a NIST SP 800-132, opzione 2a. Questa chiave viene successivamente utilizzata durante l'autenticazione dell'utente con il metodo nome utente/password.

3. Distruzione chiavi crittografiche: l'ODV sovrascrive le chiavi crittografiche in memoria con zeri quando non sono più necessarie.

4. Operazioni crittografiche: le seguenti operazioni crittografiche vengono eseguite dalla libreria crittografica dell'ODV in accordo agli standard pertinenti: cifratura/decifratura dati, cifratura/decifratura chiavi, calcolo HMAC, cifratura chiavi RSA.

5. Cifratura completa del disco: la protezione dei dati dell'utente non si basa sui meccanismi del sistema operativo, che possono essere aggirati se si ottiene l'accesso fisico al disco, ma cifratura forte e sui dati di autenticazione dell'utente.

- **Controllo dell'avvio delle applicazioni**: questa funzionalità dell'ODV si basa sui meccanismi di intercettazione del driver filtro, mediante i quali l'ODV intercetta tutti i processi avviati nel sistema operativo a livello del *kernel*. Quando il sistema operativo o un'applicazione esegue una nuova applicazione (processo), l'ODV esegue la scansione dell'applicazione o dello script in esecuzione per ottenere le proprietà e i metadati del processo.

- **Controllo degli accessi al dispositivo**: questa funzionalità dell'ODV si basa sui meccanismi di intercettazione del driver filtro, mediante i quali l'ODV intercetta tutte le operazioni sui file di dati nel sistema operativo a livello del *kernel*. Quando il sistema operativo avvia una trasmissione di dati da o verso il dispositivo collegato, l'ODV raccoglie le proprietà e i metadati dell'operazione. Questi possono essere il tipo di dispositivo, il bus o il numero di serie univoco del dispositivo, il tipo di operazione (lettura o scrittura), l'utente attivo, la durata dell'operazione.

- **Controllo degli accessi al Web**: questa funzionalità dell'ODV si basa sui meccanismi di intercettazione del driver filtro, mediante i quali l'ODV intercetta tutte le operazioni sui dati nel sistema operativo livello del *kernel*. Quando il sistema operativo avvia una trasmissione di dati da o verso la rete, l'ODV raccoglie le proprietà e i metadati dell'operazione. Questi possono essere il tipo di indirizzo di destinazione, la durata dell'operazione, l'utente attivo.

- **Identificazione e autenticazione**: l'ODV esegue l'identificazione e l'autenticazione dell'utente durante il pre-avvio. Le credenziali dell'utente vengono verificate rispetto

ai valori archiviati e le operazioni di decifratura del disco sono disponibili per gli utenti autenticati.

- **Gestione della sicurezza**:

    1. Ruoli di sicurezza: l'ODV fornisce servizi a tutti gli utenti nel suo ambiente. L'ODV fornisce due ruoli distinti: KLUser e KLAdmin. Gli utenti vengono associati al ruolo KLUser quando eseguono l'autenticazione durante la fase di pre-avvio. Gli utenti vengono associati al ruolo KLAdmin quando forniscono credenziali valide (nome utente e password) su richiesta dell'ODV quando viene avviata un'azione ristretta al ruolo KLAdmin.

    2. Gestione degli attributi di sicurezza delle policy: l'ODV opera in base a regole, policy di accesso e altri parametri dell'ODV, quali la password di KLAdmin, le chiavi di cifratura, le impostazioni delle attività, le azioni predefinite e valori per le policy di controllo degli accessi. Tutte le policy e le regole dell'ODV vengono memorizzate nel file di registro di Windows e vengono lette dall'ODV quando necessario.

- **Protezione antivirus**:

    1. Scansione antivirus: la funzionalità antivirus protegge il sistema da software malevolo utilizzando un'ampia gamma di tecniche, incluso il monitoraggio in tempo reale degli accessi ai file, scansioni su richiesta e programmate delle aree critiche del sistema.

    2. Azioni antivirus: quando il motore AV restituisce una segnalazione di rilevamento, l'ODV confronta la segnalazione ricevuta con le impostazioni di scansione che definiscono le possibili esclusioni e le azioni (disinfetta, elimina, blocca, ignora) da intraprendere sugli oggetti rilevati.

    3. Avvisi antivirus: quando un oggetto malevolo viene rilevato ed elaborato, l'ODV genera i record di audit rilevanti; è altresì possibile configurare notifiche pop-up o avvisi via Email.

## 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 o ricavati per estensione dai CC Parte 2 [CC2].

Il Traguardo di Sicurezza [TDS] definisce la classe funzionale estesa FAV (Anti-Virus) con i seguenti componenti:

- FAV_ACT.1 (Famiglia: Anti-Virus Actions)
- FAV_ALR.1 (Famiglia: Anti-Virus Alerts)
- FAV_SCN.1 (Famiglia: Anti-Virus Scanning)

Per una descrizione dettagliata delle proprietà dei componenti estesi, si consulti il cap. 5 del Traguardo di Sicurezza [TDS].

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 6 dicembre 2021 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 23 dicembre 2021. 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 Endpoint Security for Windows (version 11.6.0.394 AES256)" 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 Endpoint Security for Windows (version 11.6.0.394 AES256)" 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 ([KESUM], [KESUMA], [KESPP]).

# 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 KES consegnato in forma di pacchetto di installazione binario:
   `keswin_11.6.0.394_en_aes256.exe`
   SHA256 checksum: 12DBDC9014EC71BC9EF1BE884343DD5C200A662026A7EB7FB9F82E766CC7156B

2. L'Application Control Plugin consegnato in forma di pacchetto ZIP:
   `keswin_web_plugin_11.6.0.394.zip`
   SHA256 checksum: 43A8D7377CDB6130BF14E923590D3EE9291C13AE57D46F01E25DA71807CE8E3E

3. Il manuale d'utente per l'amministrazione e la manutenzione dell'ODV "Kaspersky Endpoint Security for Windows. User Manual. Version 2.01", distribuito in forma di file PDF
   SHA256 checksum: 42D8BB9C86FF8062F7B459C4F87F1EB220691C48768DA460110C8231419FEF30

4. L'appendice al manuale utente con riferimento alle evidenze architetturali dell'ODV "Kaspersky Endpoint Security for Windows. User Manual. Addendum A. Version 2.04", distribuito in forma di file PDF
   SHA256 checksum: 12B67ADFD1B55554A375AA9170DAE3C3B76694BAC3AD4F872E593BF9EABA641D

5. La guida per la preparazione e l'installazione dell'ODV "Kaspersky Endpoint Security for Windows. Preparative Procedures. Version 2.03", distribuita in forma di file PDF
   SHA256 checksum: CAD0018F6279D26DD5B969C6429E85C2794D1C67EA34AFD82F75162A907DA8B0

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 Endpoint Security for Windows. Preparative Procedures [KESPP]
- Kaspersky Endpoint Security for Windows. User Manual [KESUM]
- Kaspersky Endpoint Security for Windows. User Manual. Addendum A [KESUMA]

# 10 Appendice B – Configurazione valutata

L'oggetto della valutazione (ODV) è il prodotto "Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)", 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:

- Kaspersky Endpoint Security for Windows (ODV) installato su un dispositivo *endpoint* gestito (workstation) con sistema operativo Windows. Su questo dispositivo è installato anche Kaspersky Security Center 13 (componente Network Agent).
- I componenti Administration Server e Network Agent di Kaspersky Security Center 13 installati su un dispositivo (server) con sistema operativo Windows Server.
- Kaspersky Security Center 13 Web Console installata su un dispositivo (workstation) con sistema operativo Windows. Su questo dispositivo è installato anche il plug-in di gestione di Kaspersky Endpoint Security for Windows.
- Tutti i dispositivi connessi ad una LAN.

L'ODV supporta l'operatività con le seguenti versioni di Kaspersky Security Center:

- Kaspersky Security Center 11
- Kaspersky Security Center 12
- Kaspersky Security Center 12 Patch A
- Kaspersky Security Center 12 Patch B
- Kaspersky Security Center 13

Per maggiori dettagli si consulti il par. 1.4.4 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:

- 2 GB di spazio libero sul disco
- CPU:
    - Workstation: 1 GHz
    - Server: 1.4 GHz

  - Supporto per il set di istruzioni SSE2

- RAM:
  - Workstation (x86): 1 GB
  - Workstation (x64): 2 GB
  - Server: 2 GB

- Microsoft .NET Framework 4.0 o successivo.

Un elenco dei sistemi operativi per workstation e server e delle piattaforme di virtualizzazione supportati dall'ODV è fornito nel par. 1.3.2 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.

La configurazione di test dell'ODV è stata preparata in accordo al piano di test del Fornitore, che descrive il seguente ambiente:

- Host 1:

| Hardware | Software |
|---|---|
| Processore: Intel Core i3 Duo 3.10GHz<br>RAM: 4 GB<br>Capacità disco: 40 GB | SO: Windows 10 Enterprise 20H2 x64<br>Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES 256)<br>Kaspersky Security Center (version 13.0.0.11247): Administration Server, Network Agent |

- Server 1:

| Hardware | Software |
|---|---|
| Processore: Intel Core i3 Duo 3.10GHz<br>RAM: 4 GB<br>Capacità disco: 40 GB | SO: Windows Server 2016 Standard x64<br>Kaspersky Security Center (version 13.0.0.11247): Administration Server, Network Agent, Administration Console<br>Kaspersky Endpoint Security for Windows management plug-in 11.6.0 |

Si noti che il par. 1.4.4 del Traguardo di Sicurezza [TDS] elenca un *host* aggiuntivo, ovvero Kaspersky Security Center (Web Console), anch'esso messo a disposizione dal Fornitore ai Valutatori. Questo *host* non è stato utilizzato durante l'esecuzione dei casi di test in quanto la Web Console serve per la connessione a KSC, che può essere utilizzato anche senza tale componente.

I Valutatori hanno installato l'ODV seguendo le procedure preparatorie fornite nel documento [KESPP]. L'ODV è stato installato su una macchina virtuale, anch'essa messa a disposizione dal Fornitore.

## 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 104 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 (interfaccia a riga di comando) e TSFI-XPL (scansione AV su richiesta tramite Windows Explorer) sono state testate solo marginalmente, e si sono quindi concentrati su queste interfacce durante i test indipendenti per compensare la copertura insufficiente.

### 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 test effettuati dai Valutatori hanno coperto l'intero TSF con due casi di test per porzione di TSF.

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 della presenza di virus in un file non malevolo;
- verifica della presenza di virus in un file malevolo;
- verifica della presenza di virus in un file malevolo mediante la linea di comando.

### 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 [KESPP].

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:

- presenza di condizioni di *buffer overflow* in operazioni sui file eseguite dall'interfaccia grafica;
- presenza di condizioni di *buffer overflow* in operazioni sui file eseguite dall'interfaccia a linea di comando;
- analisi di un *dump* della memoria per verificare l'eventuale diffusione di informazioni sensibili;
- analisi dei file DLL per verificare l'eventuale diffusione di informazioni sensibili;
- Invio di un vettore di attacco XXE come input per un'operazione di importazione.

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.