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. 1/20

(Certification No.)

Prodotto: **BooleBox On Premises V 4.2**
(Product)

Sviluppato da: **Boole Server S.r.l.**
(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.2)

Il Direttore
(Dott.ssa Eva Spina)
Firmato digitalmente da:Eva Spina
Organizzazione:MISE/80230390587
Data:23/04/2020 18:59:45

Roma, 23 aprile 2020

Common Criteria

SOGIS IT SECURITY CERTIFIED

Questa pagina è lasciata intenzionalmente vuota

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

Rapporto di Certificazione

BooleBox On Premises V 4.2

OCSI/CERT/IMQ/06/2018/RC

Versione 1.0

23 aprile 2020

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	23/04/2020

2 Indice

3 Elenco degli acronimi

AES Advanced Encryption Standard

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

COTS Commercial Off-The-Shelf

CPU Central Processing Unit

DBMS Database Management System

DPCM Decreto del Presidente del Consiglio dei Ministri

EAL Evaluation Assurance Level

HA High Availability

HTML HyperText Markup Language

HTTPS HyperText Transfer Protocol Secure

HW Hardware

IT Information Technology

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

OS Operating System

OTP One Time Password

OWASP Open Web Application Security Project

PC Personal Computer

PP Profilo di Protezione

RAM Random Access Memory

RFV	Rapporto Finale di Valutazione
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SMS	Short Message Service
SW	Software
TDS	Traguardo di Sicurezza
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface

4 Riferimenti

4.1 Criteri e normative

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2012-09-003, “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-2012-09-004, “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

[GADM] BooleBox online administrator guide, Version 1, Boole Server S.r.l., 18 February 2020

[GUSR] BooleBox online end user guide, Version 1, Boole Server S.r.l., 18 February 2020

[RFV] Rapporto Finale di Valutazione dell'ODV BooleBox on Premises V. 4.2, LVS IMQ/LPS, versione 1.0, 12 marzo 2020

[TDS] "BOOLEBOX ON PREMISES V. 4.2 Security Target", Version 1.5, Boole Server S.r.l., 21 febbraio 2020

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 http://www.sogisportal.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 fino a EAL4.

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 http://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 fino a EAL2.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "BooleBox On Premises V 4.2", sviluppato dalla società Boole Server S.r.l., nel seguito del documento anche indicato come "BooleBox" o "BBOP".

La valutazione è stata successiva allo sviluppo dell'ODV ed 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. 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.2, 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 "BooleBox On Premises V 4.2" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti 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	BooleBox On Premises V 4.2
Traguardo di Sicurezza	"BOOLEBOX ON PREMISES V. 4.2 Security Target", Version 1.5, 21 febbraio 2020
Livello di garanzia	EAL2 con l'aggiunta di ALC_FLR.2
Fornitore	Boole Server S.r.l.
Committente	Boole Server S.r.l.
LVS	IMQ/LPS
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	25 luglio 2018
Data di fine della valutazione	12 marzo 2020

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 "BooleBox On Premises V 4.2" offre un sistema di protezione completo per impedire l'utilizzo improprio di file da parte di utenti non autorizzati e le funzionalità di sicurezza da esso offerte possono complessivamente essere ricondotte alle categorie di prodotti indicate in Figura 1.

Figura 1 - Categorie di prodotti a cui BooleBox è riconducibile

BooleBox On Premises (BBOP) è una soluzione di sincronizzazione e condivisione file sicura, appositamente progettata per le persone e le aziende che dispongono di dati sensibili da proteggere. A differenza dei servizi di condivisione di file tipici, BBOP offre privacy e controllo completi sui propri dati mediante cifratura con chiavi personali e controlli dei dati, senza comprometterne l'usabilità.

L'ODV garantisce che i dati non possano essere persi o rubati durante il trasferimento o la memorizzazione. BBOP può proteggere qualsiasi tipo di file di dati, comprese presentazioni, documenti, immagini, fogli di calcolo, ecc. Esso consente al proprietario di controllare il modo in cui altri possono utilizzare le informazioni. Con BBOP è possibile stabilire quali utenti sono autorizzati ad accedere ai dati e controllare come, quando e per quanto tempo possono farlo. Tramite BBOP un'organizzazione può archiviare dati e informazioni sensibili all'interno della propria azienda, applicando i più severi standard di sicurezza.

BBOP è progettato per proteggere i dati riservati da visualizzazione, manipolazione o distribuzione non autorizzate: gestisce la protezione dei dati, la crittografia, tutte le informazioni relative ai profili utente e i loro diritti di accesso anche su file condivisi.

Tramite questo approccio completo e controllato, BBOP consente alle organizzazioni di concentrarsi su:

- controllo della riservatezza e dell'integrità dei dati;
- protezione della proprietà intellettuale;
- assegnazione di diritti per l'accesso differenziato alle informazioni;
- audit delle operazioni eseguite dagli utenti sui file.

All'interno del suo dominio di competenza, un utente può:

- archiviare e proteggere in modo centralizzato file e cartelle;
- condividere informazioni in modo temporaneo con diritti di autorizzazione granulari;

- creare e controllare il profilo di accesso ai dati (progetto di classificazione);
- monitorare le attività svolte dagli utenti su informazioni protette;
- inviare e ricevere messaggi Email cifrati;
- visualizzare i file in modalità protetta;
- inviare collegamenti diretti per accedere a informazioni protette centralizzate;
- visualizzare documenti direttamente nel *browser* Web o scaricarli.

7.3.1 Architettura dell'ODV

L'ODV è costituito dal software applicativo "BooleBox On Premises V 4.2" che realizza le funzioni di sicurezza descritte nel Traguardo di Sicurezza [TDS].

BooleBox può essere utilizzato in modalità "Standard (not redundant)" o in "High Availability (HA)", in cui i vari componenti SW (l'ODV, lo *storage* cifrato e il database) sono installati su server diversi.

In Figura 2 è illustrata l'architettura di BooleBox (HA) in un tipico ambiente operativo, ovvero l'infrastruttura di un'azienda.

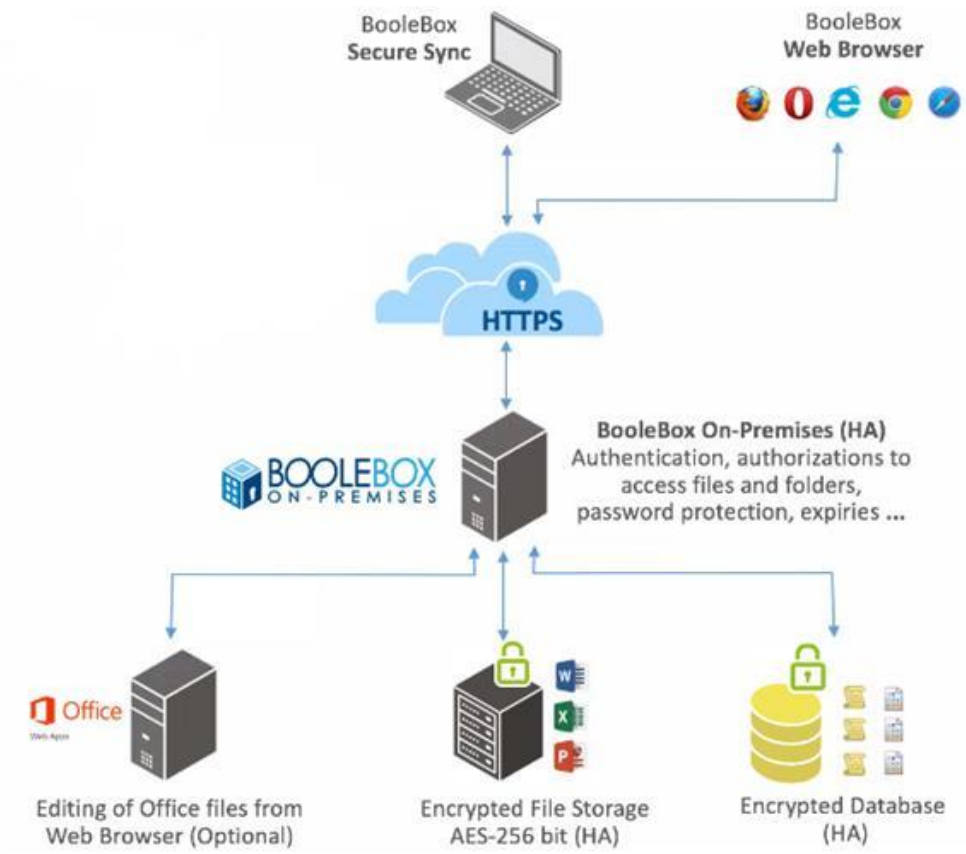

Figura 2 – Architettura dell'ODV all'interno di un'infrastruttura aziendale

L'utilizzo dell'ODV prevede che l'utente finale tramite un *browser* Web instauri una connessione TLS (realizzata dall'ambiente operativo) con la macchina in cui è installato l'ODV.

Gli amministratori autorizzati dell'ODV gestiscono l'ODV in locale mediante il Control Panel e da remoto, previa identificazione e autenticazione, utilizzando la Dashboard attraverso un *browser* Web.

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 nei cap. 3 e 4 del Traguardo di Sicurezza [TDS].

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consultino i cap. 1.5.2 e 1.6.3 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Identificazione e Autenticazione**: la funzione di identificazione e autenticazione assicura che gli utenti dell'ODV accedono alle funzioni dell'ODV solo dopo essere stati identificati ed autenticati con username, password e OTP. Solo per gli utenti GUEST l'autenticazione avviene con sola password, senza l'ausilio di OTP, per l'accesso a file condivisi.
  Dopo tre tentativi falliti di digitazione della password è richiesta la digitazione di un *captcha* che a sua volta, in caso digitazione errata, è sottoposto ad un ritardo crescente per ciascun tentativo di inserimento.

- **Audit**: le funzioni di audit effettuano la registrazione degli eventi di audit e ne consentono la visualizzazione da parte degli amministratori autorizzati. Vengono registrati sia gli eventi relativi alle attività di amministrazione dell'ODV, sia eventi relativi alle attività degli utenti. Gli utenti senza diritti amministrativi possono accedere solo alla visualizzazione degli eventi che li riguardano. Gli eventi sottoposti ad audit vengono archiviati cifrati nel DBMS.

- **Protezione dei dati degli utenti e del TSF**: l'ODV effettua la cifratura sia di dati utente sia di dati del TSF. La cifratura dei dati utente può avvenire, a scelta dell'utente, con Personal Key o con Master Key, mentre i dati generati dall'ODV sono cifrati con Master Key.
  La cifratura avviene sulla base dell'algoritmo AES-256.

- **Gestione della sicurezza**: l'ODV permette di modificare in tempo reale i diritti di accesso degli utenti. È possibile revocare i diritti di accesso ai file anche dopo che sono stati condivisi.
  La gestione dell'ODV è effettuata mediante la Dashboard ed il Control Panel.

- **Controllo di accesso**: l'ODV permette di controllare l'accesso alle sue funzioni sulla base del ruolo degli utenti. In particolare, l'accesso alle funzioni di configurazione della Dashboard è consentito solo ai ruoli di tipo amministrativo (SAM, ADM, ADR).
  Il sistema operativo su cui è installato l'ODV è configurato per essere accessibile solo agli amministratori autorizzati dell'ODV che di conseguenza hanno accesso esclusivo al Control Panel.

Gli utenti hanno pieno controllo dei propri file e, se li condividono, ne stabiliscono i diritti di accesso da parte di altri utenti.

- **Privacy**: l'ODV associa a ciascun utente un alias che non permette ad utenti non autorizzati di conoscere il nome utente effettivo che ha eseguito specifiche operazioni.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto viene fornita all'utente finale insieme al prodotto. Questa documentazione contiene le informazioni richieste per l'installazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguiti gli ulteriori obblighi o note per l'utilizzo sicuro dell'ODV contenuti nel par. 9.3 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 Funzionali (SFR) sono stati derivati direttamente dai CC Parte 2 [CC2].

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

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, i Requisiti Funzionali di Sicurezza (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 IMQ/LPS.

L'attività di valutazione è terminata in data 12 marzo 2020 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 6 aprile 2020. 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 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 "BooleBox On Premises V 4.2" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.2, 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.2.

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
Flaw reporting procedures	*ALC_FLR.2*	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 6 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "BooleBox On Premises V 4.2" 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 capitolo 4.2 del Traguardo di Sicurezza [TDS]. Si consiglia ai potenziali acquirenti di verificare la rispondenza ai requisiti identificati e di prestare attenzione alle raccomandazioni contenute in questo Rapporto.

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata, le cui modalità di installazione e configurazione sono descritte nelle Guide per l'amministratore [GADM] e per l'utente [GUSR], fornite insieme all'ODV.

Si raccomanda l'utilizzo dell'ODV in accordo con quanto descritto nella documentazione citata. In particolare, l'Appendice A – Indicazioni per l'uso sicuro del prodotto del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'installazione e all'utilizzo sicuro del prodotto.

Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le Politiche di sicurezza organizzative e le ipotesi descritte in [TDS], par. 3.2 e 3.3, in particolare quelle relative al personale ed ai locali all'interno dei quali andrà ad operare l'ODV.

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

La distribuzione dell'eseguibile necessario per installare BooleBox On Premises avviene via Internet mediante una connessione HTTPS ad un indirizzo creato *ad hoc* da Boole Server S.r.l. per il cliente.

Il cliente, una volta identificato e autenticato con le credenziali di accesso ricevute da Boole Server S.r.l. via Email o telefono, accede ad una cartella condivisa da cui deve scaricare il file di installazione dell'ODV "BBSetup.exe".

La distribuzione dei componenti software sviluppati da Boole Server S.r.l., non facenti parte dell'ODV ma necessari per il suo corretto funzionamento (BooleBox Storage Service, BooleBox Server Service, BooleBox Document Service), avviene con procedura analoga a quella per la distribuzione dell'ODV.

9.2 Identificazione dell'ODV

Prima dell'installazione è possibile verificare il nome del prodotto, la *major release* (BooleBox On Premises 4.2) e la *minor release* (ad. es., 4.2.1.3), cliccando con il tasto destro del mouse sul file di installazione e scegliendo la voce di menu "Proprietà".

Una volta che l'ODV è installato e in stato operativo, è possibile identificarne la versione partendo dal pannello di controllo principale, cliccando sulla sezione "License Info" della System Bar.

9.3 Installazione, inizializzazione ed 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 la preparazione dell'ambiente operativo dell'ODV, l'inizializzazione sicura dell'ODV e il funzionamento sicuro dell'ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS]:

- BooleBox online administrator guide, Version 1, Boole Server S.r.l., 18 February 2020 [GADM]
- BooleBox online end user guide, Version 1, Boole Server S.r.l., 18 February 2020 [GUSR]

10 Appendice B – Configurazione valutata

L'ODV è il prodotto software "BooleBox On Premises V 4.2". Il nome e il numero di versione identificano univocamente l'ODV e i suoi componenti, costituenti la configurazione valutata dell'ODV a cui si applicano i risultati della valutazione.

È prevista una sola configurazione dell'ODV, illustrata in Figura 3, dove l'ODV è evidenziato in grassetto su sfondo giallo, nel suo ambiente operativo.

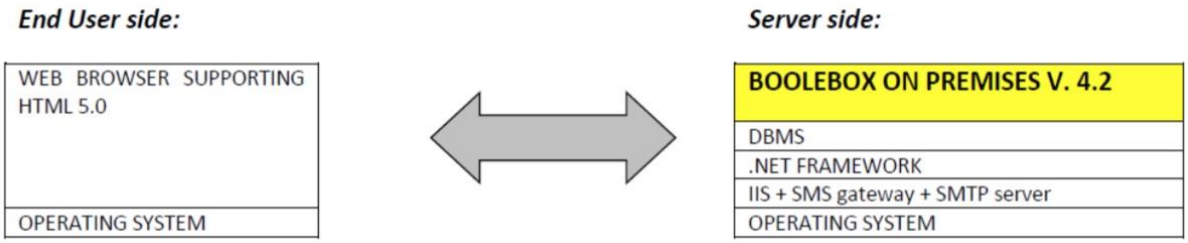

Figura 3 – Configurazione valutata dell'ODV

Gli elementi indicati in Tabella 2 costituiscono la configurazione valutata dell'ODV.

Componente SW	Descrizione	Versione
BBSetup.exe	Installer dell'ODV	*Major release* 4.2 *Minor release* 1.3

Tabella 2 – Elementi della configurazione valutata dell'ODV

L'ODV non comprende componenti di tipo HW né COTS.

10.1 Ambiente operativo dell'ODV

Di seguito si riportano i requisiti minimi HW e SW dell'ambiente operativo dell'ODV lato server e lato client (utente finale) ([TDS], cap. 1.5.4):

Sistema Operativo	Microsoft Windows Server 2012 Microsoft Windows Server 2008R2
Requisiti minimi software	Versioni seguenti di DBMS Microsoft: • SQL Server 2012 • SQL Server 2008R2 .NET Framework 4.0 IIS (Internet Information Server) 6 Microsoft Office 2007
Requisiti minimi hardware	RAM: 4 GB Spazio su disco: 1 GB Scheda di rete: 10/100 Mbit CPU: Dual Core Processor

Tabella 3 – Requisiti minimi HW e SW lato server

Sistema Operativo (richiesto per le funzionalità Anti-Capture e Deter Photo Shots)	Versioni seguenti di Microsoft Windows: • Microsoft Windows 10 • Microsoft Windows 8 e 8.1 • Windows 7
Requisiti software	Microsoft Internet Explorer 10 o successive. Tutti gli altri *browser* Web più diffusi (Chrome, Safari, Opera, Firefox). Nota: si raccomanda l'uso di *browser* Web compatibili con HTML5 aggiornati all'ultima versione disponibile.
Requisiti hardware	PC con hardware minimo richiesto dal Sistema Operativo o, nel caso in cui le funzionalità Anti-Capture e Deter Photo Shots non siano richieste, qualsiasi dispositivo fisso o mobile su cui è installato un *browser* Web compatibile con HTML5.

Tabella 4 – Requisiti HW e SW lato client

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.2, tali attività prevedono tre passi successivi:

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

11.1 Configurazione per i Test

Per l'esecuzione dei test il Fornitore ha messo a disposizione dell'LVS un insieme di risorse equivalente a quelle utilizzate per effettuare i suoi test. In particolare, è stata messa a disposizione una macchina virtuale per l'installazione dell'ODV e dei componenti dell'ambiente operativo previsti (database, *storage*, *document manager*) oltre che dei server necessari al funzionamento dell'ODV (*SMS gateway*, *Email server*).

I Valutatori hanno configurato l'ODV ed il suo ambiente operativo seguendo le istruzioni contenute nella documentazione operativa fornita, come indicato nel cap. 9.3. Pertanto, l'ODV utilizzato per i test è risultato installato in modo corretto ed in uno stato noto.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Copertura dei test

I Valutatori hanno verificato che la documentazione di test presentata dal Fornitore comprende:

- il piano di test, i risultati attesi e i risultati ottenuti per ogni test;
- le evidenze di copertura dei test che dimostrano la corrispondenza tra i test identificati nella documentazione di test e le TSFI descritte nelle specifiche funzionali;
- l'ordine di esecuzione dei test e gli scenari per l'esecuzione di ogni test, inclusa ogni dipendenza rispetto ai risultati degli altri test.

11.2.2 Risultati dei test

Per lo svolgimento dell'attività di esecuzione dei test funzionali proposti dal Fornitore non è stato usato nessuno strumento specifico in quanto per i test sono state utilizzate le interfacce messe a disposizione dall'ODV.

In una prima fase, i Valutatori hanno effettuato un campione dei test presenti nel piano di test e nelle procedure di test del Fornitore e hanno verificato positivamente il corretto comportamento delle TSFI e la corrispondenza tra risultati attesi e risultati ottenuti per ogni test.

Al termine delle sessioni di test effettuate dai Valutatori, tutti questi test hanno dato esito positivo.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

Successivamente, i Valutatori hanno progettato dei test indipendenti per la verifica della correttezza delle TSFI.

La strategia utilizzata dai Valutatori è stata quella di effettuare dei test sulle interfacce più "sensibili" per l'utente, per le quali i test del Fornitore non hanno previsto alcuni casi d'uso o per le quali i Valutatori hanno previsto condizioni di utilizzo anomale (ad es., tentativi di uso improprio o insicuro dell'ODV da parte dell'utente, riconfigurazione del dispositivo per la ricezione dell'OTP, ecc.).

I test indipendenti predisposti dai Valutatori hanno avuto i seguenti principali obiettivi:

- verificare che l'utente non può effettuare il login se non mediante autenticazione in due passaggi (username/password + OTP via SMS);
- verificare che un utente non amministratore non possa disabilitare il meccanismo di autenticazione in due passaggi;
- verificare che dopo tre tentativi errati di login (ovvero al quarto tentativo) viene richiesta la digitazione di un *captcha*;
- verificare che dopo tre tentativi di login da parte di un utente non esistente viene richiesta la digitazione di un *captcha*;
- verificare che la Master Key sia gestita in modo corretto;
- verificare che l'accesso al Control Panel sia permesso solo previo login da parte dei soli amministratori autorizzati (SAM, ADM);
- verificare che un utente con ruolo ADM non può creare utenti con ruolo ADM di altre *company* e che un utente con ruolo ADR non può creare utenti con ruolo ADR di altre *company* o con diritti superiori ai suoi.

I Valutatori hanno svolto in tutto tre diverse sessioni di test. I risultati intermedi delle prove effettuate hanno portato alla luce alcune problematiche, segnalate dai Valutatori al Fornitore mediante Rapporti di Osservazione, che hanno richiesto aggiornamenti dell'ODV.

Al termine della sessione finale di test effettuata dai Valutatori, tutti i test hanno dato esito positivo.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività è stato utilizzato lo stesso ambiente di test già utilizzato per le attività dei test funzionali. I Valutatori hanno verificato che le configurazioni di test fossero congruenti con la versione dell'ODV in valutazione.

In una prima fase, i Valutatori hanno esaminato fonti di informazione pubbliche per la ricerca di potenziali vulnerabilità dell'ODV. Questa ricerca non ha prodotto risultati.

In una seconda fase, i Valutatori hanno esaminato i documenti di valutazione (Traguardo di Sicurezza, documentazione operativa, specifiche funzionali, progetto dell'ODV e architettura di sicurezza) al fine di identificare possibili vulnerabilità dell'ODV.

Da questa analisi i Valutatori hanno effettivamente individuato la presenza di alcune vulnerabilità potenziali dell'ODV e hanno progettato dei test di intrusione per verificarne l'effettiva sfruttabilità nell'ambiente operativo previsto.

L'approccio dei Valutatori ai test di intrusione può essere riassunto elencandone i principali obiettivi:

- cercare di leggere i file o le informazioni riservate degli utenti dell'ODV senza essere in possesso delle necessarie credenziali;
- cercare di individuare debolezze nei meccanismi di autenticazione e autorizzazione;
- cercare di aggirare i controlli di validazione degli input implementati dalle TSFI per ottenere esecuzione di codice, inserimento o lettura di dati ove non previsto dall'ODV.

I Valutatori hanno condotto i test di intrusione applicando la metodologia OWASP con l'ausilio dello strumento di analisi semi-automatica Burp Suite Pro.

In una prima fase, i Valutatori hanno esaminato i risultati di tutti i test di intrusione e hanno riscontrato la presenza di vulnerabilità sfruttabili, prontamente segnalate al Fornitore mediante un Rapporto di Osservazione. Il Fornitore ha recepito le osservazioni dei Valutatori e ha rilasciato un aggiornamento dell'ODV. I Valutatori hanno quindi analizzato le modifiche effettuate sull'ODV e hanno ripetuto i test di intrusione sulla nuova versione.

Al termine della seconda sessione di test di intrusione, i Valutatori hanno potuto verificare che la nuova versione dell'ODV ha risolto le vulnerabilità riscontrate in precedenza e hanno 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 individuate vulnerabilità residue.