Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

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. 5/15

(Certification No.)

Prodotto: **Boole Server v3.2**
(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 Rita Forsi)

Roma, 29 ottobre 2015

Common Criteria

SOGIS IT SECURITY CERTIFIED

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

Boole Server v3.2

OCSI/CERT/IMQ/05/2014/RC

Versione 1.0

29 ottobre 2015

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	29/10/2015

2 Indice

3 Elenco degli acronimi

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CD-ROM	Compact Disk - Read-Only Memory
CEM	Common Evaluation Methodology
COTS	Commercial Off The Shelf
DBMS	Database Management System
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
HW	Hardware
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	Profilo di Protezione
RFV	Rapporto Finale di Valutazione
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SW	Software
TDS	Traguardo di Sicurezza
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface

4 Riferimenti

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012

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

[CCRA-2000] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, May 2000

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012

[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

[ALC] Supporto al ciclo di vita “Boole Server”, versione 1.3, 5 ottobre 2015, Boole Server S.r.l.

[OPE] Documentazione Operativa “Boole Server”, versione 1.3, 5 ottobre 2015, Boole Server S.r.l.

[RFV] Rapporto Finale di Valutazione “Boole Server”, versione 1.1, 12 ottobre 2015, LVS IMQ/LPS

[TDS] “Boole Server” Traguardo di Sicurezza, versione 1.5, 5 ottobre 2015, Boole Server S.r.l.

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 assurance indicati.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La nuova versione 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 EAL 2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

I certificati rilasciati prima dell'8 settembre 2014 sono ancora riconosciuti secondo le regole del precedente accordo [CCRA-2000], cioè fino al livello EAL 4 (e ALC_FLR). Queste stesse regole del CCRA-2000 si applicano ai processi di certificazione in corso alla data dell'8 settembre 2014, come pure al mantenimento e alla ri-certificazione di vecchi certificati, per un periodo di transizione fino all'8 settembre 2017.

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.

Poiché il prodotto certificato è stato accettato nel processo di certificazione prima dell'8 settembre 2014 il presente certificato è riconosciuto secondo le regole del precedente accordo [CCRA-2000], cioè per tutti i componenti di assurance indicati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "Boole Server v3.2", sviluppato dalla società Boole Server S.r.l.

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 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 "Boole Server v3.2" 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	Boole Server v3.2
Traguardo di Sicurezza	"Boole Server" Traguardo di Sicurezza, v1.5, 5 ottobre 2015
Livello di garanzia	EAL2 con 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. 4
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	4 giugno 2014
Data di fine della valutazione	12 ottobre 2015

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 "Boole Server v3.2" (nel seguito anche indicato semplicemente come Boole Server) 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.

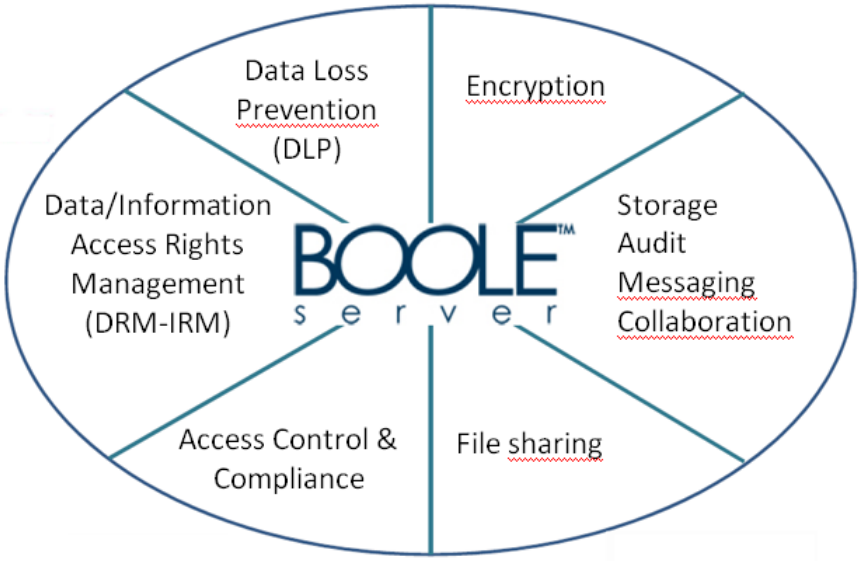


Figura 1 – Categorie di prodotti a cui Boole Server è riconducibile

L'ODV è composto da 3 componenti software:

- *Server*
- *Agent*
- *Web Client*

Il componente *Server* costituisce il fulcro di tutto il sistema di protezione dei file in quanto è responsabile di tutte le operazioni che garantiscono la protezione e la cifratura dei dati, le informazioni relative ai profili e alle loro autorizzazioni ad accedere ed utilizzare i singoli file. Di seguito le principali funzionalità implementate dal componente Server:

- creazione di policy di sicurezza centralizzate;
- gestione utenti e gruppi;
- gestione della configurazione in alta affidabilità;
- gestione delle chiavi di cifratura del database;
- gestione delle operazioni di recovery e ripristino in caso di disastro;
- gestione dei log di sistema.

Il componente *Web Client* dell'ODV è lo strumento attraverso cui gli utenti possono collegarsi a Boole Server utilizzando un qualunque browser e disporre di funzionalità come:

- download/upload di file e cartelle dal proprio spazio riservato in Boole Server;
- centralizzazione protetta di file e cartelle;

- condivisione di file in modo selettivo, granulare e temporaneo;
- creazione e controllo dei profili di accesso;
- monitoraggio delle attività svolte dagli utenti sui file protetti;
- invio e ricezione di messaggi in modalità cifrata;
- visualizzazione dei file in modalità protetta;
- cifratura di testi e file;
- modifica di file online senza necessità di effettuarne il download.

Il componente *Agent* può essere installato sulla macchina dell'utente in aggiunta al classico web browser e offrire una serie di funzionalità di sicurezza aggiuntive, di seguito sintetizzate:

- disporre della funzionalità Top Secret per bloccare attività non autorizzate come lo "screen capture", ed impedire la copia a video dei documenti condivisi in visualizzazione;
- lavorare sui file in modalità protetta;
- cifrare file e cartelle in locale;
- condividere le risorse cifrate in locale in modo selettivo, granulare e temporaneo;
- creare archivi di file cifrati in locale sotto forma di dischi virtuali;
- sincronizzare cartelle locali con risorse centralizzate accessibili da *Web Client*;
- generare certificati per consentire l'accesso ai documenti cifrati anche in modalità off-line.

L'utilizzo dell'ODV in un tipico ambiente operativo, ovvero l'infrastruttura di un cliente, prevede che l'End User tramite un web browser instauri una connessione SSL (realizzata dall'ambiente operativo) con la macchina di Front End in cui è installata la componente *Web Client* dell'ODV.

Esistono due categorie di utenti che sono autorizzate ad operare sull'ODV: quelli che si interfacciano con il componente *Web Client* dell'ODV, installato sulla macchina di Front End, e quelli che si interfacciano con il componente *Server* dell'ODV, installato sulla macchina server.

Gli utenti lato Server sono creati in fase di installazione dell'ODV e possono essere gestiti solo localmente dall' amministratore del sistema mentre gli utenti lato *Web Client* possono essere gestiti da remoto tramite l'interfaccia Web dell'ODV.

7.3.1 Architettura dell'ODV

L'ODV è un software costituito dalle seguenti tre componenti che realizzano le funzionalità di sicurezza offerte:

- Boole Server Version 3.2;
- Boole Server Agent Version 3.2;
- Boole Server Web Client Version 3.2.

Le caratteristiche SW delle macchine su cui può essere installato l'ODV e delle altre macchine costituenti l'ambiente operativo dell'ODV sono riportate in [TDS], par.1.5.3.

7.3.2 Caratteristiche di Sicurezza dell'ODV

7.3.2.1 Ipotesi

Le ipotesi definite nel Traguardo di Sicurezza [TDS] ed alcuni aspetti delle minacce e delle politiche di sicurezza organizzative non sono coperte direttamente dall'ODV stesso; ciò implica che specifici obiettivi di sicurezza debbano essere soddisfatti dall'ambiente operativo. In particolare in tale ambito i seguenti aspetti sono da considerare di rilievo:

- Si assume che l'ODV sia installato, configurato e gestito in modo conforme alla configurazione valutata.
- Si assume che tutti gli utenti dell'ODV siano sufficientemente addestrati per gestire l'ODV in modo sicuro e non compromettano, attivamente o per negligenza, la sicurezza del computer su cui è installato l'ODV, ad es. non installando software contenenti virus o cavalli di Troia, né modificando il programma dell'ODV o i file di dati. Si assume inoltre che gli amministratori dell'ODV siano fidati e osservino scrupolosamente le indicazioni fornite dalla documentazione.
- Si assume che il database e lo Storage siano installati nell'ambiente operativo dell'ODV, e che siano usati dall'ODV tramite meccanismi al di fuori del suo confine; l'accesso fisico e logico ad essi è consentito solo a utenti amministrativi coordinati dall'amministratore dell'ODV.
- Si assume che sia effettuato regolarmente il backup di BS server, DBMS e Storage nell'ambiente operativo dell'ODV, in modo da garantire che i backup siano tenuti allineati.
- Si assume che la chiave utilizzata per la cifratura del database sia conservata in un luogo sicuro sotto il controllo del General Administrator Master.
- Si assume che l'ambiente operativo fornisca un riferimento temporale affidabile.
- Si assume che l'ambiente operativo fornisca una linea di comunicazione sicura tra le diverse parti distribuite dell'ODV e tra questo e gli amministratori remoti.
- Si assume che l'ambiente operativo assicuri la protezione dell'integrità dei file eseguibili che costituiscono l'ODV.

- Si assume che Il sistema operativo su cui risiede l'ODV venga configurato in modo da consentire di modificare gli eseguibili dell'ODV, il sistema operativo stesso, i file di configurazione, database e chiavi crittografiche ai soli amministratori autorizzati.

- Si assume che l'amministratore dell'ambiente operativo assicuri che la piattaforma su cui è in esecuzione l'ODV consenta il funzionamento sicuro dell'ODV. Qualora venisse individuata una vulnerabilità di tale piattaforma, che sia rilevante per il funzionamento dell'ODV, tale vulnerabilità deve essere rimossa o protetta da adeguate misure di sicurezza esterne.

7.3.2.2 Funzioni di sicurezza

Le funzioni di sicurezza implementate dall'ODV sono descritte in [TDS], par. 7.1.

- **Identification and Authentication**: tale funzione assicura che solo gli amministratori autorizzati possano accedere alle impostazioni di configurazione e gestione dell'ODV. Gli utenti finali (End User) devono fornire uno user name e un PIN validi e il Gruppo di appartenenza prima che il server permetta loro di accedere all'ODV. Gli utenti lato server devono accedere con un nome utente ed una password validi prima che il server permetta agli amministratori di gestire l'ODV.

- **Audit**: l'ODV realizza un sistema di auditing che consente la traccia completa e dettagliata delle operazioni effettuate sui file protetti, mantenendo gli utenti autorizzati al corrente di chi visualizza, modifica o condivide tali file.

- **Encryption**: l'ODV implementa l'algoritmo di cifratura RC6 con lunghezza della chiave 2040 bit. Questo assicura che i dati sensibili possono essere visualizzati e utilizzati solo da utenti autorizzati, evitando che informazioni critiche vengano indebitamente intercettate.

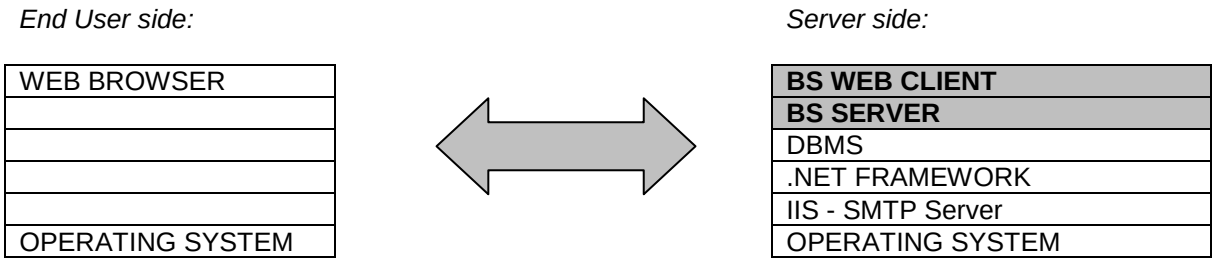
- **Management**: l'ODV fornisce una serie di comandi per gli utenti autorizzati a gestire le funzioni di sicurezza, la configurazione e altre caratteristiche di Boole Server. La funzione di Security Management consente di specificare i ruoli utente con permessi di accesso definiti per la gestione dei componenti dell'ODV. In generale, la funzione di gestione della sicurezza dei dati è resa disponibile ai proprietari dei dati che vogliono condividere queste informazioni con altri utenti.

- **Centralized Access Control**: con tale funzione solo gli utenti autorizzati possono lavorare direttamente sui file protetti, ed essere in grado di condividere con altri utenti specificando politiche di controllo accessi con granularità molto fine. Gli utenti autorizzati possono lavorare direttamente sui file protetti, essere in grado di condividerli con altri utenti secondo policy altamente controllate: ad es., un utente può essere autorizzato a leggere il contenuto di alcuni file, ma senza la possibilità di modificarli o di salvarli, anche a livello locale, mentre un altro utente può avere il diritto di leggere e scrivere, ma per un tempo limitato.

7.3.3 Configurazioni valutate dell'ODV

Il Traguardo di Sicurezza di Boole Server descrive le due diverse possibili configurazioni dell'ODV sottoposte a valutazione, di seguito riportate in Figura 2. I componenti dell'ODV sono evidenziati in grassetto su sfondo grigio.

CONFIGURAZIONE 1:



CONFIGURAZIONE 2:

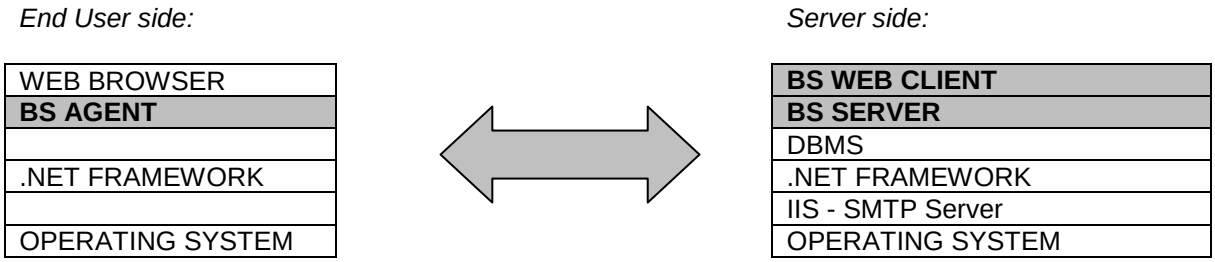


Figura 2 – Configurazioni valutate dell'ODV

La differenza tra le due configurazioni è la presenza o l'assenza di Boole Server Agent rappresentato nella configurazione n° 2. Questa configurazione fornisce un maggior livello di controllo e di protezione rispetto alla configurazione n° 1. Gli utenti di BS Agent sono in grado di cifrare file e cartelle memorizzati in locale, creare dischi locali criptati, bloccare le attività di cattura dello schermo, crittografare risorse locali rendendoli accessibili anche senza connessione a Boole Server e molto altro ancora. Quando l'utente non ha la possibilità di connettersi a BS Server, BS Agent consente di accedere ed utilizzare i file o archivi protetti utilizzando un certificato off-line generato precedentemente.

Per ulteriori dettagli si rimanda al [TDS], par. 1.5 e 1.6.

7.4 Documentazione

La documentazione specificata in Appendice A viene fornita al cliente 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. 9.2 di questo rapporto.

7.5 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3] e tutti i Requisiti Funzionali di Sicurezza (SFR) 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.

7.6 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 ottobre 2015 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 22 ottobre 2015. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.7 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. 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 "Boole Server v3.2" 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.

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

Classi e componenti di garanzia		Verdetto
Flaw reporting procedures	ALC_FLR.2	Positivo
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 "Boole Server v3.2" 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 all'ambiente di sicurezza specificato nel capitolo 3 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 nella Documentazione Operativa [OPE] fornita insieme all'ODV.

Si raccomanda l'utilizzo dell'ODV in accordo con quanto descritto nella documentazione citata. In particolare, l'Appendice A 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

L'ODV viene distribuito all'utente mediante il file Setup.exe che contiene i componenti BS Server, BS Web Client e BS Agent. La distribuzione avviene via internet mediante una connessione https oppure mediante CD-ROM, nel caso in cui il cliente non fosse fornito di connessione internet.

Terminata l'installazione dei componenti BS Server e BS Web Client (ODV in configurazione 1), l'End User può portare l'ODV in configurazione 2 connettendosi ad un indirizzo web https creato ad hoc sul Server, salvare sul proprio desktop il file BSAgent.exe ed eseguirlo per avviare il wizard di installazione.

L'integrità dei file d'installazione e dei componenti applicativi dell'ODV è garantita dal certificato digitale apposto dallo strumento di sviluppo Microsoft .Net e verificato dal Sistema Operativo Windows, sia nella versione Server sia Client.

9.2 Installazione e utilizzo sicuro dell'ODV

L'installazione sicura dell'ODV e la preparazione sicura del suo ambiente operativo in accordo agli obiettivi di sicurezza indicati nel [TDS], devono avvenire seguendo le istruzioni contenute nella Documentazione Operativa Boole Server [OPE].

10 Appendice B – Configurazione valutata

Il nome e il numero di versione identificano univocamente l'ODV e i suoi componenti SW, costituenti la configurazione valutata dell'ODV, come riportato in [ALC], a cui si applicano i risultati della valutazione.

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

10.1 Ambiente operativo dell'ODV

Di seguito si riportano gli elementi HW e SW che devono essere presenti nell'ambiente operativo dell'ODV (TDS], par. 1.5.3):

Operating System	Microsoft Windows Server 2012 Microsoft Windows Server 2008R2
Minimum Software Prerequisites	Following versions of Microsoft DBMS: • SQL Server 2012 • SQL Server 2008R2
	.NET Framework 4.0
	IIS (Internet Information Server) 6
	Microsoft Office 2007
Minimum Hardware Prerequisites	**Ram**: 4 GB
	Disk Space: 1 GB
	Network Card: 10/100 Mbit
	CPU: Dual Core Processor

Tabella 2 – Prerequisiti della macchina che ospita i componenti Server e Web Client

Operating System	Following versions of Microsoft Windows OS: • Microsoft Windows 8 e 8.1 • Microsoft Windows Server 2008 (all versions) • Windows 7 • Windows Vista
Software Prerequisites	Microsoft Internet Explorer (from version 7 and up) All other major internet browser (Chrome, Safari, Opera, Firefox) *Note*: Browsers HTML 5 compliant in their most updated version recommended
	.NET FRAMEWORK V 3.5 (*Note*: only with TOE configuration n. 2)
Hardware Prerequisites	PC with at least the minimum hardware required by the operating system

Tabella 3 – Prerequisiti della macchina End User che ospita il componente Agent

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 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 è stato predisposto un apposito ambiente di test presso la sede del Committente/Fornitore, che ha fornito le risorse necessarie e il supporto del proprio personale.

Prima dell'esecuzione dei test il software è stato installato e configurato seguendo le istruzioni contenute nella Documentazione Operativa [OPE], come indicato nel par. 9.2.

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 con la descrizione degli scenari per l'esecuzione di ogni test, i risultati attesi e i risultati ottenuti per ogni test, incluse le informazioni relative all'ordine di esecuzione e alle eventuali priorità di esecuzione di ciascun test;
- le evidenze di copertura dei test, espresse tramite una tabella che dimostra la corrispondenza tra i test descritti nella documentazione di test e le TSFI descritte nelle specifiche funzionali.

11.2.2 Risultati dei test

Per l'esecuzione dei test funzionali proposti dal Fornitore, e per la riesecuzione degli stessi da parte dei Valutatori, non è stato utilizzato nessuno strumento specifico.

In una prima fase, i Valutatori hanno eseguito una serie di test, scelti a campione tra quelli del Fornitore: per alcuni test i risultati non sono risultati conformi a quelli attesi e sono emersi alcuni comportamenti incoerenti rispetto alla documentazione dell'ODV.

È stato quindi necessario produrre da parte del Fornitore una nuova versione del software dell'ODV, che è stato nuovamente installato e configurato per eseguire le attività di test.

Su tale versione aggiornata i Valutatori hanno eseguito ulteriori test, focalizzando l'attenzione, in modo particolare, su quelli che nella precedente sessione non avevano dato i risultati attesi e che stavolta hanno avuto invece 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 TSF.

Non sono stati utilizzati strumenti di test particolari oltre ai componenti dell'ODV che hanno permesso di sollecitare tutte le TSFI selezionate per i test indipendenti.

Per ogni test è stata predisposta una scheda apposita; tali schede sono state utilizzate sia come piano dei test dei Valutatori sia in seguito, opportunamente compilate con i risultati, anche come rapporto dei test stessi.

Nella progettazione dei test indipendenti, i Valutatori hanno considerato aspetti che nei test del Fornitore erano non presenti o ambigui o eseguiti con esito negativo o inseriti in test più complessi che interessavano più interfacce contemporaneamente ma con un livello di dettaglio non ritenuto adeguato.

Alcuni dei test sono stati progettati per avere conferma delle anomalie riscontrate durante l'esecuzione a campione dei test predisposti dal Fornitore.

I Valutatori, infine, hanno anche progettato ed eseguito alcuni test in modo indipendente da analoghi test del Fornitore, sulla base della sola documentazione di valutazione.

Questo approccio ha portato a rilevare delle anomalie, che sono state poi risolte dal Fornitore nella nuova versione del software rilasciato.

I Valutatori hanno quindi rieseguito i test su tale versione aggiornata, con particolare focalizzazione su quelli che avevano dato esito negativo nel precedente riciclo, che hanno dato conferma della risoluzione positiva da parte del Fornitore.

In questa fase finale di test, i Valutatori hanno verificato anche la corretta implementazione dell'algoritmo RC6, utilizzato dall'ODV per la cifratura dei file, utilizzando un'apposita interfaccia predisposta dal Fornitore nel componente BS Server, sollecitata con i vettori di test specificati nella documentazione disponibile relativa all'algoritmo.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività sono stati utilizzati lo stesso ambiente di test predisposto per le attività dei test funzionali e la versione aggiornata del software dell'ODV, come risultato dalle attività stesse (cfr. par. 11.2.2).

I Valutatori hanno innanzitutto verificato che la configurazione di test fosse congruente con la versione dell'ODV in valutazione, cioè quella indicata nel [TDS], par. 1.5.

In una prima fase, i Valutatori hanno utilizzato alcuni strumenti software contenuti nella distribuzione Kali Linux, che contengono un database aggiornato delle vulnerabilità note, individuando alcune vulnerabilità potenziali.

I Valutatori hanno poi esaminato i documenti di valutazione (TDS, documentazione operativa, specifiche funzionali, progetto dell'ODV e architettura di sicurezza) al fine di evidenziare eventuali vulnerabilità potenziali dell'ODV. Da questa analisi i Valutatori hanno effettivamente determinato la presenza di nove vulnerabilità potenziali.

Sulla base di questi risultati, i Valutatori hanno progettato dei test di intrusione per verificare la sfruttabilità delle vulnerabilità potenziali individuate. I test di intrusione sono stati descritti con un dettaglio sufficiente per la loro ripetibilità avvalendosi a tal fine delle schede di test, utilizzate in seguito, opportunamente compilate con i risultati, anche come rapporto dei test stessi.

I test di intrusione sono stati condotti prevalentemente sul componente BS Web Client in quanto unico componente con potenziale accesso a internet e pertanto esposto a ogni tipologia di attaccante.

L'analisi e i test di intrusione sono stati condotti mediante strumenti prevalentemente automatici messi a disposizione dalla distribuzione Kali Linux. Tali strumenti non hanno messo in luce criticità di sicurezza.

Pertanto, i Valutatori hanno esaminato i risultati di tutti i test di intrusione e hanno determinato che l'ODV, nel suo ambiente operativo, è in grado di resistere ad un attaccante che possiede un potenziale di attacco di livello Basic, concludendo che l'ODV non presenta vulnerabilità sfruttabili né vulnerabilità residue.