Ministero dello Sviluppo Economico

Dipartimento per le Comunicazioni

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

Software "Backoffice v. 5.0" incluso nella scheda di gioco ELSY J0E001 BLACK KILLER

OCSI/CERT/TEC/05/2009/RC

Versione 1.0

10/06/2010

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	Giacinto Dammicco Federico Filipponi	Prima emissione	10/06/10

2 Indice

3 Elenco degli acronimi

AAMS Azienda Autonoma dei Monopoli di Stato

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

EAL Evaluation Assurance Level

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 (Protection Profile)

RFV Rapporto Finale di Valutazione

SFR Security Functional Requirement (Requisito Funzionale di Sicurezza)

SAR Security Assurance Requirement (Requisito di Garanzia)

TDS Traguardo di Sicurezza (Security Target)

4 Riferimenti

[CC1] CCMB-2006-09-001, “Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model”, versione 3.1, Rev. 1, settembre 2006.

[CC2] CCMB-2007-09-002, “Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components”, versione 3.1, Rev. 2, settembre 2007.

[CC3] CCMB-2007-09-003, “Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components”, versione 3.1, Rev. 2, settembre 2007.

[CEM] CCMB-2007-09-004, “Common Methodology for Information Technology Security Evaluation - Evaluation Methodology”, versione 3.1, Rev. 2, settembre 2007.

[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. 1/07 – Modifiche alla LGP1, versione 1.0, Marzo 2007

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/07 – Modifiche alla LGP2, versione 1.0, Marzo 2007

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/07 – Modifiche alla LGP3, versione 1.0, Marzo 2007

[TDS] Traguardo di sicurezza per il software “Backoffice v. 5.0” incluso nella scheda di gioco ELSY J0E001 BLACK KILLER, versione 5.0, Rev. 2, 25 gennaio 2010

[MAN] Esercizio e manutenzione degli apparecchi elettronici di intrattenimento con a bordo la scheda J0E001, (Manuale di impiego), rev. 1 del 15/7/09

[RFV] Rapporto Finale di Valutazione del software “Backoffice v. 5.0” incluso nella scheda di gioco ELSY J0E001 BLACK KILLER, versione 2, 12 aprile 2010

5 Dichiarazione di certificazione

[1] L'oggetto della valutazione (ODV) è il software "Backoffice v. 5.0" incluso nella scheda di gioco J0E001 BLACK KILLER, progettata e prodotta dalla società Electro System S.p.A. (ELSY).

[2] 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 per la Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G. U. n.98 del 27 aprile 2004).

[3] 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].

[4] L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL1, con l'aggiunta di ALC_DEL.1, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B di questo Rapporto di Certificazione.

[5] 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 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.

6 Riepilogo della valutazione

6.1 Introduzione

[6] Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del software "Backoffice v. 5.0" incluso nella scheda di gioco J0E001 BLACK KILLER 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.

[7] 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.

6.2 Identificazione sintetica della certificazione

Nome dell'ODV	Software "Backoffice v. 5.0" incluso nella scheda di gioco J0E001 BLACK KILLER
Traguardo di Sicurezza	Traguardo di Sicurezza per il software "Backoffice v. 5.0" incluso nella scheda di gioco ELSY J0E001 BLACK KILLER, versione 5.0, Rev. 2, 25 gennaio 2010
Livello di garanzia	EAL1 con aggiunta di ALC_DEL.1
Fornitore	Electro System S.p.A. (ELSY)
Committente	Electro System S.p.A. (ELSY)
LVS	Technis Blu S.r.l.
Versione dei CC	3.1
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	11 febbraio 2010
Data di fine della valutazione	12 aprile 2010

[8] 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].

6.3 Prodotto valutato

[9] L'ODV è la procedura software denominata "Backoffice v. 5.0" integrata, come elemento chiaramente delimitato, nella scheda di gioco J0E001 BLACK KILLER, progettata e prodotta dalla società Electro System S.p.A. (ELSY).

[10] Esemplari di un medesimo tipo di scheda sono impiegati come componenti di controllo di apparecchi da divertimento ed intrattenimento denominati Newslot, di seguito riferiti come apparecchi di gioco. Schede e apparecchi debbono essere conformi alle prescrizioni normative emesse dall'Azienda Autonoma dei Monopoli di Stato (AAMS).

[11] Uno schema logico dell'ODV e del suo ambiente operativo è illustrato in Figura 1.

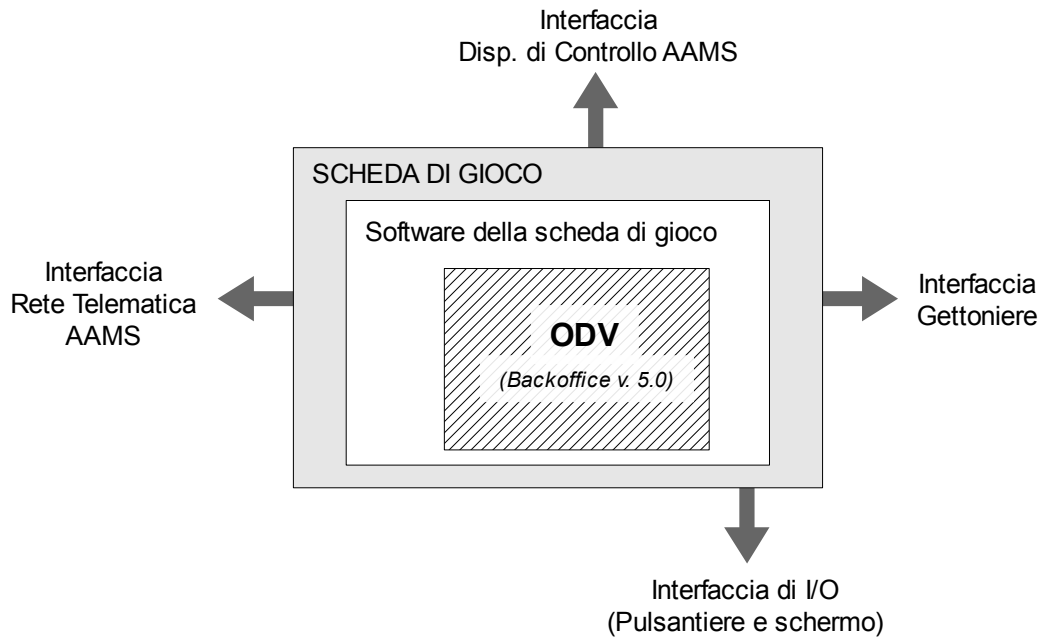

Figura 1 – Schema logico dell'ODV e del suo ambiente operativo

[12] Ogni apparecchio di gioco è installato presso locali, aperti al pubblico e di competenza di un esercente, e consente lo svolgimento di suoi giochi peculiari, implementati dalla scheda di gioco, conformi alle norme AAMS. È collegato a una rete telematica AAMS, per il cui tramite uno specifico sistema informatico AAMS provvede a supervisionare i modi di funzionamento degli apparecchi di gioco.

[13] Ogni apparecchio di gioco è dotato delle strumentazioni di visualizzazione e di intervento manuale necessarie per lo svolgimento dei giochi e include:

- un dispositivo di accettazione di monete, in cui il giocatore inserisce gli importi richiesti per le partite;
- dispositivi di erogazione monete, impiegati per il pagamento al giocatore delle vincite delle partite;
- un esemplare di una scheda di gioco, che implementa le operatività

funzionali dell'apparecchio;

- un cavo di trasferimento dati su cui hanno luogo le comunicazioni informatiche tra la scheda di gioco e la rete telematica AAMS.

[14] L'apparecchio di gioco appare come un telaio strutturato, inclusivo di sportelli e chiavistelli metallici. Lo stato di apertura-chiusura dei vani è riportato sotto forma di segnalazioni informatiche sui connettori della scheda di gioco. La custodia e l'impiego dei chiavistelli è di pertinenza delle parti coinvolte nell'impiego degli apparecchi di gioco (esercenti e gestori).

[15] Nella scheda di gioco risiedono i componenti informatici necessari al funzionamento dell'apparecchio di gioco. La scheda è costituita da unità fisiche interconnesse in cui sono realizzate:

- le funzioni (logico-informatiche) di gioco, inclusive delle interazioni con i dispositivi di pagamento delle partite e di erogazione delle vincite;

- le interfacce verso la rete telematica AAMS e verso un dispositivo di controllo AAMS;

- il protocollo di comunicazione tra scheda di gioco e rete telematica e dispositivo di controllo AAMS.

[16] La scheda di gioco è chiusa all'interno di un suo contenitore ermetico munito di sigilli ed etichette antieffrazione, sensori in grado di rilevare tentativi di manomissione del contenitore, aperture per i collegamenti alla rete telematica AAMS e agli altri dispositivi dell'apparecchio di gioco.

[17] I confini della scheda sono costituiti dai suoi connettori elettrici verso gli ulteriori dispositivi presenti nell'apparecchio di gioco e verso il dispositivo di controllo AAMS.

[18] Oltre all'esecuzione degli algoritmi di elaborazione associati alle partite di gioco, la scheda implementa flussi informatici bidirezionali di interazione tra la scheda da una parte e il dispositivo di controllo AAMS e la rete telematica AAMS dall'altra.

[19] Con riferimento a quanto fino a qui esposto, l'ODV è costituito da una ben delimitata procedura software, denominata "Backoffice", inclusa nella scheda di gioco e dedicata al suo governo. I requisiti di sicurezza sottoposti alla certificazione sono riferiti solo al software "Backoffice v. 5.0" integrato nella scheda di gioco J0E001 BLACK KILLER.

[20] L'accesso all'ODV è subordinato ad un insieme di politiche di controllo degli accessi basata sul ruolo degli utenti. Sono previsti due ruoli differenti, ad ognuno dei quali sono associate le funzionalità che l'utente con tale ruolo può svolgere:

- ELSY (Fornitore);
- Produttore.

[21] Le funzionalità dell'ODV sono divise in due categorie, qui riportate in forma sintetica (per una descrizione completa si rimanda a [TDS]):

- Funzionalità ordinarie: Contabilità, Musiche, Gettoniere, Rabbocco, Visure e Statistiche;
- Funzionalità straordinarie: Apparecchio di gioco, Manutenzione apparecchio, Manutenzione scheda, Registrazione e Cambio parola.

[22] Le funzionalità ordinarie sono eseguibili da chiunque disponga di chiavistelli meccanici con cui accedere ai vani riservati dell'apparecchio di gioco.

[23] L'esecuzione delle funzionalità straordinarie, invece, è consentita solo agli utenti che si siano preventivamente identificati e autenticati; in particolare, la funzionalità "Manutenzione scheda" è riservata ai soli utenti appartenenti al ruolo ELSY.

[24] Tra le funzionalità indicate, le sole che realizzano funzionalità di sicurezza sono:

- Registrazione: abilitazione/rimozione di una parola chiave di accesso di pertinenza da parte del produttore di apparecchi di gioco;
- Cambio parola: modifica da parte di un addetto della parola chiave di accesso in suo possesso.

[25] Le funzioni di sicurezza dell'ODV sono quindi le seguenti:

- Identificazione e autenticazione, mediante parola chiave, degli addetti che vogliono accedere alle funzioni straordinarie dell'ODV.
- Controllo sugli accessi degli addetti che intendono svolgere le funzioni straordinarie di esercizio e manutenzione incluse nell'ODV.
- Gestione dei ruoli di abilitazione dell'ODV.
- Gestione degli attributi di sicurezza utilizzati dalle funzionalità di sicurezza dell'ODV.
- Gestione delle sessioni concorrenti.

6.4 Ambito di valutazione dell'ODV

[26] L'accesso alle funzionalità straordinarie dell'ODV (elencate nel par. 6.3) è subordinato ad una procedura di identificazione ed autenticazione degli addetti basata sull'impiego di parole chiave di accesso. Le parole chiave sono distribuite ai loro incaricati dal Fornitore, ossia il produttore della scheda di gioco su cui è installato l'ODV (ELSY), e dal produttore dell'apparecchio di gioco.

[27] Il Fornitore assegna a ciascun produttore di apparecchi di gioco suo cliente una parola chiave di accesso capostipite (differente per ciascun apparecchio), per consentirgli lo svolgimento protetto delle operazioni di esercizio e manutenzione del suo apparecchio di gioco.

[28] Una parola chiave (differente per ciascuna scheda) è riservata dal Fornitore a se stesso, per l'accesso protetto alle funzioni di governo della scheda di gioco.

[29] Un produttore di apparecchi di gioco, tramite suoi addetti che impiegano la funzionalità di sicurezza "Registrazione", introdotta nel par. 6.3, può creare e cancellare sull'ODV parole chiave secondarie.

[30] Ogni addetto in possesso di una parola chiave, capostipite o secondaria, la può cambiare tramite la funzione di sicurezza "Cambio parola" (vedi par. 6.3).

[31] Accanto alle parole chiave capostipite e secondarie, per coprire condizioni di emergenza, è prevista, da parte del produttore degli apparecchi di gioco, l'emissione di parole chiave temporanee, del tipo usa e getta, da utilizzare una sola volta e su una sola scheda di gioco, nell'ambito di una singola sessione di manutenzione.

[32] Gli addetti si autenticano, ove richiesto, sull'ODV inserendo nell'apposita schermata ("Autenticazioni") una parola chiave tra quelle che, al momento, l'ODV riconosce in quanto memorizzate al suo interno.

[33] La procedura di identificazione e autenticazione degli addetti viene svolta dall'ODV sulla base della sola parola chiave inserita. La struttura sintattica di ciascuna parola chiave, descritta nel dettaglio in [TDS], è definita in modo tale da consentire all'ODV di discriminare la tipologia di addetto e di assegnargli il giusto ruolo tra quelli gestiti dall'ODV stesso (ELSY o Produttore), consentendo quindi la differenziazione delle autorizzazioni concesse al possessore della parola chiave.

[34] Su ogni apparecchio di gioco può essere operativa al più una sessione di esercizio e manutenzione, assegnabile a un solo operatore. Ciò mentre non è in corso una partita di gioco.

[35] Durante una sessione di esercizio e manutenzione non possono essere avviate partite di gioco.

[36] Per avviare una sessione di esercizio/manutenzione occorre premere il pulsante TEST dell'apparecchio. Per terminarla, l'addetto utilizzerà uno dei bottoni software presenti nella sequenza di schermate navigate.

6.5 Politiche di sicurezza dell'organizzazione

[37] Per l'ODV non è richiesta alcuna conformità ad una politica di sicurezza dell'organizzazione.

6.6 Requisiti funzionali e di garanzia

[38] Trattandosi di una valutazione a livello di garanzia EAL1, nel Traguardo di Sicurezza [TDS] non viene descritto completamente il problema di sicurezza, ma ci si limita a definire gli obiettivi di sicurezza per l'ambiente operativo e a fornire i Requisiti Funzionali di Sicurezza (SFR).

[39] Tutti gli SFR sono stati selezionati dai CC Parte 2 [CC2].

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

6.7 Conduzione della valutazione

[41] 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).

[42] 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].

[43] L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS Technis Blu S.r.l.

[44] La valutazione è terminata in data 12 aprile 2010 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV]. Tale Rapporto è stato analizzato dall'Organismo di Certificazione e approvato il 7 giugno 2010. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

6.8 Considerazioni generali sulla validità della certificazione

[45] 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 nel documento di Esercizio e manutenzione degli apparecchi elettronici di intrattenimento con a bordo la scheda J0E001 [MAN]. 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.

[46] 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.

7 Esito della valutazione

7.1 Risultato della valutazione

[47] 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 (software "Backoffice v. 5.0" incluso nella scheda di gioco J0E001 BLACK KILLER) soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL1, con l'aggiunta di ALC_DEL.1, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS], se configurato secondo la configurazione valutata (Appendice B o [MAN]).

[48] 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 EAL1, con l'aggiunta di ALC_DEL.1, oltre a quelli della classe ASE per la valutazione del TDS.

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 for the operational environment	ASE_OBJ.1	Positivo
Stated security requirements	ASE_REQ.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Basic functional specification	ADV_FSP.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
Labelling of the TOE	ALC_CMC.1	Positivo
TOE CM coverage	ALC_CMS.1	Positivo
Delivery procedures	ALC_DEL.1	Positivo
Tests	**Classe ATE**	Positivo
Independent testing - conformance	ATE_IND.1	Positivo
Vulnerability assessment	**Classe AVA**	Positivo

Classi e componenti di garanzia		Verdetto
Vulnerability survey	AVA_VAN.1	Positivo

Tabella 1 - Verdetti finali per i requisiti di garanzia

7.2 Raccomandazioni

[49] Le conclusioni dell'Organismo di Certificazione sono riassunte nella Dichiarazione di Certificazione riportata nel par. 5.

[50] **Si raccomanda ai potenziali acquirenti del software "Backoffice v. 5.0" incluso nella scheda di gioco ELSY J0E001 BLACK KILLER, di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto di Certificazione in riferimento al Traguardo di Sicurezza [TDS]**.

[51] L'ODV deve essere utilizzato in accordo all'ambiente di sicurezza specificato nei capitoli 3 e 4 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 di Certificazione.

[52] **Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV valutato**, configurato come riportato in Appendice B o [MAN].

[53] L'inclusione nella presente certificazione delle attività previste dal componente ALC_DEL.1 garantisce che le caratteristiche di sicurezza dell'ODV sono mantenute durante la consegna dello stesso all'utente nel solo caso in cui tutti i soggetti coinvolti nel processo di consegna (Fornitore, Produttore, Gestore, Esercente) sono fidati e operano nel rispetto delle procedure esaminate. La presente certificazione non può dunque fornire garanzie circa la corrispondenza della scheda di gioco consegnata all'utente con un esemplare di riferimento, né in alcun modo fornisce garanzie di protezione da personale malintenzionato interessato a produrre e distribuire esemplari di schede di gioco (inclusive di ODV) alterate, in violazione delle prescrizioni normative emesse da AAMS.

[54] L'ODV, in quanto univocamente associato alla scheda di gioco "ELSY J0E001 BLACK KILLER", mutua e deriva dalla scheda in questione tutti i parametri identificativi. È pertanto dotato dell'identificativo univoco ritenuto da AAMS per poter omologare tale scheda. La società ELSY traccia, in una base dati aziendale, tutti gli esemplari delle sue schede di gioco approvati da AAMS. Ciascun esemplare è dotato di descrittori e identificativi che ne consentono il puntamento univoco. Si raccomanda quindi all'utente finale dell'ODV di:

- verificare con attenzione tale identificativo riportato sulla scheda di gioco interagendo con ELSY per avere certezza che tale identificativo rientra tra quelli contenenti l'ODV nella sua versione valutata e certificata;

- verificare che la scheda di gioco non presenti ulteriori informazioni (ad es. numero di versione o revisione). La presenza di tale informazione indicherebbe infatti una versione differente dell'ODV da quella valutata e certificata, cui non si applicano le conclusioni riportate nel presente Rapporto di Certificazione.

[55] Per una futura rivalutazione di questo prodotto, o più in generale in caso di valutazione di ODV analoghi al presente, si raccomanda fortemente al Fornitore di inserire strumenti automatici per la verifica immediata della versione del software Backoffice introdotto nella scheda di gioco, in modo da semplificare all'utente le operazioni necessarie per l'esecuzione di tali verifiche.

[56] Si raccomanda l'utilizzo dell'ODV in accordo con quanto descritto in [MAN]. Inoltre, l'Appendice A del presente Rapporto di Certificazione include una serie di raccomandazioni relative alla consegna, all'installazione e all'utilizzo del prodotto.

[57] Le funzionalità di identificazione e autenticazione dell'ODV si basano sull'unico meccanismo della parola chiave che contiene un segreto di 7 caratteri alfanumerici. Si raccomanda agli utenti abilitati incaricati di registrare le parole chiave nell'ODV di selezionare parole chiave non banali.

[58] Si assume che le persone cui vengono assegnati i ruoli di ELSY e Produttore siano adeguatamente addestrate al corretto utilizzo dell'ODV e scelte tra il personale fidato dell'organizzazione. L'ODV non è realizzato per contrastare minacce provenienti da amministratori inesperti, malfidati o negligenti.

[59] Occorre inoltre notare, stante la scelta del committente di limitare l'oggetto della valutazione al solo software "Backoffice v. 5.0", che la sicurezza dell'operatività dell'ODV è condizionata al corretto funzionamento della scheda di gioco e al corretto comportamento dell'interfaccia esterna verso le connessioni provenienti dalla rete AAMS. La presente certificazione non fornisce dunque garanzie circa la protezione da attacchi intenzionali o malfunzionamenti casuali provenienti da tale interfaccia.

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

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

8.1 Predisposizione e Consegna delle macchine contenenti l'ODV

[61] Il Fornitore adotta sistemi per il controllo della qualità del processo di istallazione e messa in opera dell'ODV e per garantire la correttezza e la completezza dell'istanza di ODV valutata e certificata nella consegna al cliente finale.

[62] L'ODV, il software "Backoffice v. 5.0", in quanto univocamente associato alla scheda di gioco "ELSY J0E001 BLACK KILLER", mutua e deriva dalla scheda in questione tutti i parametri identificativi. È pertanto dotato dell'identificativo univoco ritenuto da AAMS per poter omologare tale scheda.

[63] La società ELSY traccia, in una base dati aziendale, tutti gli esemplari delle sue schede di gioco approvati da AAMS. Ciascun esemplare è dotato di descrittori e identificativi che ne consentono il puntamento univoco.

[64] Tutto il materiale viene predisposto, imballato e consegnato al Cliente mediante spedizione con corriere, secondo le procedure previste dal piano di qualità aziendale della società ELSY, rispondenti alle normative ISO9000.

8.2 Documentazione per l'utilizzo sicuro dell'ODV

[65] I documenti di guida rilevanti ai fini della valutazione o referenziati all'interno dei documenti prodotti e disponibili ai potenziali acquirenti, sono i seguenti:

- Traguardo di sicurezza per il software "Backoffice v. 5.0" incluso nella scheda di gioco ELSY J0E001 BLACK KILLER, versione 5.0, Rev. 2, 25 gennaio 2010 [TDS];

- Esercizio e manutenzione degli apparecchi elettronici di intrattenimento con a bordo la scheda J0E001, rev. 1 del 15/7/09 [MAN].

9 Appendice B - Configurazione valutata

9.1 Software Backoffice v. 5.0

[66] L'ODV, il software “Backoffice v. 5.0”, in quanto univocamente associato alla scheda di gioco “ELSY J0E001 BLACK KILLER”, mutua e deriva dalla scheda in questione tutti i parametri identificativi. È pertanto dotato dell’identificativo univoco ritenuto da AAMS per poter omologare tale scheda.

[67] La società ELSY traccia, in una base dati aziendale, tutti gli esemplari delle sue schede di gioco approvati da AAMS. Ciascun esemplare è dotato di descrittori e identificativi che ne consentono il puntamento univoco.

[68] Il software applicativo della scheda, incluso il “Backoffice v. 5.0” oggetto della valutazione, è generato, configurato e caricato nella scheda, a partire dal binario eseguibile, tramite un sistema di lavoro denominato “Programmatore software”.

[69] Per la messa in esercizio, una volta caricato il binario eseguibile è sufficiente inserire le parole chiave necessarie per l'operatività dell'ODV. L'ODV non necessita quindi di altre configurazioni per l'esercizio.

9.2 Hardware

[70] L’ODV è costituito solo da componenti software. Richiede tuttavia specifiche componenti software (relative all'esercizio della scheda di gioco), firmware e hardware della scheda di gioco ELSY J0E001 BLACK KILLER in cui è indissolubilmente integrato. Tale legame con la scheda di gioco in questione limita l'utilizzo dell'ODV, con le garanzie della presente certificazione, alla sola versione della scheda di gioco ELSY J0E001 BLACK KILLER individuata senza alcun numero di versione o altro riferimento.

[71] La scheda è a sua volta inserita in un apparecchio di gioco della tipologia Newslot, conforme alle specifiche prescrizioni normative emesse da AAMS.

10 Appendice C - Attività di Test

[72] Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL1 tali attività non prevedono l'esecuzione di test funzionali da parte del Fornitore, ma soltanto test funzionali indipendenti da parte dei Valutatori.

10.1 Configurazione per i Test

[73] L'ODV è parte inscindibile di una scheda di gioco istallata su un apparecchio di gioco. Le procedure di prova sono state effettuate su un apparecchio di gioco completo, equipaggiato con due gettoniere, con a bordo la scheda J0E001 BLACK KILLER identificata dal codice CM000000000000020 e conforme alle prescrizioni normative emessa da AAMS.

10.2 Test funzionali ed indipendenti svolti dai Valutatori

[74] I Valutatori hanno dimostrato che l'ODV si comporta come descritto nella documentazione di progetto e che l'ODV realizza i requisiti funzionali di sicurezza.

[75] I test indipendenti sono stati eseguiti dai Valutatori dell'LVS presso la sede della Electro System S.p.A. (ELSY).

[76] Per l'esecuzione dei test indipendenti i valutatori hanno stimolato le TSFI *interfering* dell'ODV e utilizzato le stesse unitamente alle TSFI *non interfering* come strumento di riscontro dei risultati ottenuti.

[77] I test hanno dimostrato che l'ODV si comporta come atteso.

[78] L'ODV ha quindi superato con verdetto positivo la fase di test indipendenti.

10.3 Analisi delle vulnerabilità e test di intrusione

[79] I Valutatori non hanno identificato fonti specifiche sulle vulnerabilità note del software incluso nelle schede di gioco della tipologia Newslot.

[80] Inoltre, in considerazione della particolare tipologia dell'ODV e della presenza di obiettivi per l'ambiente operativo che contrastano eventuali minacce provenienti dalla rete telematica AAMS, i Valutatori hanno ritenuto di limitare le prove di intrusione al tentativo di aggirare la funzione di autenticazione utilizzando la pulsantiera dell'apparecchio di gioco. Tali test hanno dato un esito negativo.

[81] In conclusione, quindi, durante l'attività di analisi delle vulnerabilità note ed esecuzione delle prove di intrusione operata dai Valutatori, non sono state riscontrate vulnerabilità sfruttabili né vulnerabilità residue dell'ODV.