Ministero dello Sviluppo Economico

Comunicazioni - Istituto Superiore C.T.I.

Rapporto di Certificazione

Gestione dei dati sanitari, infermerie e CMD

Versione 1.1

Ottobre 2008

Questa pagina è lasciata intenzionalmente vuota

1 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "Gestione dei dati Sanitari, infermerie e CMD", un'applicazione Web, installata su Oracle Application Server 10g, di supporto per la gestione dei dati sanitari del personale della Difesa e consente l'accesso ai dati sanitari dei pazienti da parte del personale medico autorizzato.
Il prodotto "Gestione dei dati Sanitari Infermerie e CMD" è stato valutato secondo lo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed è risultato conforme ai requisiti della Parte 3 dei Common Criteria v 2.3 per il livello di garanzia EAL3, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B di questo rapporto.

Committente: Blustaff S.p.A.
Fornitore: Blustaff S.p.A.
Prodotto e Versione: Gestione dei dati Sanitari, infermerie e CMD versione 3.2.4
Descrizione: il prodotto "Gestione dei dati Sanitari, infermerie e CMD", è un'applicazione Web composta da servlet, pagine JSP, JavaBeans e file XML che creano il punto di accesso ai dati sanitari per il personale medico della Difesa.
CC Parte 2: Conformant
CC Parte 3: Conformant
Livello di garanzia: EAL3
LVS: Eutelia S.p.A.
Data: Ottobre 2008

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).
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 CC [CC3] e alla Common Evaluation Methodology (CEM) [CEM].

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di
35 valutazione è stato condotto in modo conforme a quanto richiesto dai criteri e dalle procedure indicate dal 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.

2 Indice

1 Dichiarazione di certificazione 3
2 Indice 5
3 Elenco degli acronimi 6
4 Riferimenti 7
5 Riepilogo della valutazione 9
5.1 Introduzione 9
5.2 Identificazione sintetica della certificazione 9
5.3 Prodotto valutato 10
5.4 Ambito di valutazione dell'ODV 10
5.5 Dichiarazioni sulla robustezza delle funzioni 11
5.6 Politica di sicurezza dell'ODV 11
5.7 Requisiti funzionali e di garanzia 11
5.8 Conduzione della valutazione 12
5.9 Considerazioni generali sulla validità della certificazione 12
6 Esito della valutazione 14
6.1 Risultato della valutazione 14
6.2 Raccomandazioni 14
7 Appendice A – Indicazioni per l'uso sicuro del prodotto 16
7.1 Consegna 16
7.2 Installazione 16
7.3 Documentazione per l'utilizzo sicuro dell'ODV 16
8 Appendice B - Configurazione valutata 18
8.1 Configurazione dell'ODV 18
8.2 Configurazione dell'ambiente IT 18
9 Appendice C - Attività di Test 19
9.1 Configurazione per i Test 19
9.2 Test funzionali svolti dal Fornitore 19
9.3 Test funzionali ed indipendenti svolti dai valutatori 20
9.4 Analisi delle vulnerabilità e test di intrusione 20

3 Elenco degli acronimi

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CMD	Carta Multiservizi della Difesa
EAL	Evaluation Assurance Level
LVS	Laboratorio di Valutazione
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
PDV	Piano di Valutazione
PIN	Personal Identification Number
PP	Protection Profile
RFS	Requisito Funzionale di Sicurezza
RFV	Rapporto Finale di Valutazione
SMD	Stato Maggiore della Difesa
SOF	Strength of Function
SSL	Secure Socket Layer
TDS	Traguardo di Sicurezza

4 Riferimenti

[CC1] CCMB-2005-08-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, versione 2.3, Agosto 2005.

[CC2] CCMB-2005-08-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional requirements”, versione 2.3, Agosto 2005.

[CC3] CCMB-2005-08-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance requirements”, versione 2.3, Agosto 2005.

[CEM] CCMB-2005-08-004, “Common Methodology for Information Technology Security Evaluation – Evaluation Methodology”, versione 2.3, Agosto 2005.

[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 del software interforze “Gestione dei dati Sanitari, infermerie e CMD”, versione 4.1, 16 maggio 2008

[RFV] Rapporto Finale di Valutazione del software interforze “Gestione dei dati Sanitari, infermerie e CMD”, versione 1.1, settembre 2008

[GUIDE] Manuale di amministrazione del Software Interforze “Gestione dei dati Sanitari, infermerie e CMD”, versione 2.2, 16 maggio 2008 ; Manuale utente del Software Interforze “Gestione dei dati Sanitari, infermerie e CMD”, versione 2.1, 18 gennaio 2008; Installazione, generazione e start-up del Software Interforze “Gestione dei dati Sanitari, infermerie e CMD”, versione 2.1, 16 maggio 2008

[AIT] Rapporto Ambiente di Test, versione 1.0, maggio 2008

5 Riepilogo della valutazione

5.1 Introduzione

130 Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "Gestione dei dati Sanitari, infermerie e CMD" 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 deve essere consultato congiuntamente al Traguardo di 135 Sicurezza [TDS] che specifica i requisiti funzionali e di garanzia, e l'ambiente di utilizzo previsto.

5.2 Identificazione sintetica della certificazione

Nome dell'ODV	Gestione dei dati Sanitari, infermerie e CMD Versione 3.2.4
Traguardo di Sicurezza	SMD06_Traguardo_Di_Sicurezza_v4.1_16mag08.doc Versione 4.1
Livello di garanzia	EAL 3
Robustezza delle funzioni di sicurezza	SOF-high
Fornitore	Blustaff S.p.A.
Committente	Blustaff S.p.A.
LVS	Eutelia S.p.A.
Versione dei CC	2.3
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	06-02-2007
Data di fine della valutazione	04-09-2008

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

5.3 Prodotto valutato

L'ODV è una applicazione Web per la gestione dei dati sanitari del personale della Difesa. Quando accede al sistema un utente con profilo medico o super amministratore, questo può servirsi dei dati sanitari del personale della Difesa per effettuare visite mediche ai propri pazienti. L'applicazione web mette inoltre a disposizione funzioni di gestione, quali ad esempio la gestione degli utenti e funzioni di visualizzazione dei dati di audit, ad un amministratore o ad un super amministratore dell'ODV.

L'ODV identifica e autentica l'utente mediante nome utente e password richiesti all'atto della connessione.

In alternativa l'ODV può limitarsi solamente ad identificare l'utente se questo è stato autenticato dalla propria CMD mediante l'inserimento del PIN.

Dopo che l'utente è stato correttamente autenticato, in base al profilo dell'utente, l'ODV consente o meno l'accesso ad alcune funzionalità piuttosto che ad altre.

L'applicazione Web costituisce quindi il sistema per accesso delle postazioni client, dove opera il personale medico, alla Base Dati Sanitaria, che contiene i dati sanitari dei pazienti.

L'ODV registra le operazioni eseguite dagli utenti in un archivio che può essere consultato tramite l'ODV solamente da utenti con profilo di tipo amministratore.

5.4 Ambito di valutazione dell'ODV

L'ODV è installato su un server Microsoft ed essendo costituito da pagine JSP, servlet, JavaBeans e controlli JavaScript, è in esecuzione nel contesto di un application server (prodotto da Oracle).

Per funzionare correttamente l'applicazione Web si appoggia su due DB (Base Dati Sanitaria e Base Dati del Personale) ospitati da un DBMS Oracle installato su un altro server Microsoft collegato sulla stessa LAN del primo server. Sulla medesima LAN viene anche collegato il client utilizzato per la fruizione dei servizi dell'ODV.

Tutte le macchine sopra elencate sono alloggiate in un unico bunker schermato ad accesso controllato.

L'applicazione Web viene attivata da un browser Web in esecuzione sul client dopo l'instaurazione di una connessione SSL tra browser Web ed application server. All'atto della connessione viene scaricata ed eseguita sul client un'applet per la gestione della CMD. L'utente può scegliere di autenticarsi mediante l'inserimento del nome utente e della password oppure può utilizzare la propria CMD inserendola nel lettore di smart card, digitando il pin della carta. Nel caso di inserimento del nome utente e password l'autenticazione viene effettuata dall'ODV verificando le credenziali inserite rispetto a quelle memorizzate sulla Base Dati Sanitaria. Nel caso di utilizzo della CMD l'autenticazione viene effettuata dalla CMD stessa; successivamente allo sblocco della CMD l'applet invia all'ODV i dati utilizzati per identificare l'utente e caricare il corretto profilo.

5.5 Dichiarazioni sulla robustezza delle funzioni

Per l'ODV viene dichiarata una robustezza dei meccanismi “high” (SOF-high) per la funzione di identificazione/autenticazione limitatamente all'utilizzo del nome utente e della password per l'autenticazione come indicato nel Traguardo di Sicurezza, par. 8.4.2 [TDS].

5.6 Politica di sicurezza dell’ODV

Il Traguardo di Sicurezza [TDS] identifica le seguenti politiche di sicurezza dell’organizzazione a cui l’ODV deve essere conforme:

- P.ACCOUNTABILITY Le azioni che gli utenti dell'ODV svolgono all'interno dell'ODV saranno registrate e ad essi ricondotte.
- P.GESTIONE I ruoli degli utenti all'interno dell'ODV potranno essere modificati solo da utenti con privilegi amministrativi

5.7 Requisiti funzionali e di garanzia

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 (RFS) e le funzioni di sicurezza che realizzano gli obiettivi stessi.

Tutti gli RFS sono stati presi dai CC Parte 2 [CC2].

5.8 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.

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 Eutelia S.p.A..

La valutazione è terminata in data 4 settembre 2008 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV]. Tale rapporto è stato ricevuto l'11 settembre 2008 dall'Organismo di Certificazione che, dopo averlo analizzato, lo ha approvato il 18 settembre 2008. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

5.9 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS] e con riferimento all'ambiente operativo ivi specificato. La configurazione valutata è quella riassunta nel documento di installazione, generazione e start-up [GUIDE]. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti, e a prestare attenzione alle raccomandazioni contenute in questo Rapporto.

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 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.

6 Esito della valutazione

6.1 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 ("Gestione dei dati Sanitari, infermerie e CMD") soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL3, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS], se configurato secondo la configurazione valutata (documento di installazione generazione e start-up [GUIDE]).L'LVS ha inoltre verificato che l'analisi prodotta dal Fornitore sulla robustezza del meccanismo che realizza la funzione di autenticazione mediante password è corretta e che il meccanismo di autenticazione è in grado di resistere ad attacchi diretti con un potenziale di attacco elevato.

6.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nella dichiarazione di Certificazione a pagina 3.

Si raccomanda ai potenziali acquirenti del prodotto "Gestione dei dati Sanitari, infermerie e CMD" versione 3.2.4 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 nella sezione 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 valutato, la cui configurazione è specificata nel documento di installazione generazione e start-up [GUIDE].

Si raccomanda l'utilizzo dell'ODV in accordo con quanto descritto nella documentazione di guida [GUIDE] fornita con la configurazione valutata. In

particolare l'Appendice A include una serie di raccomandazioni relative alla consegna, all'installazione e all'utilizzo del prodotto.

Si suppone che gli operatori dell'ODV siano soggetti fidati, e che siano opportunamente addestrati all'uso sicuro dell'ODV. L'ODV non è realizzato per contrastare minacce provenienti da operatori inesperti, malfidati o negligenti.

Occorre inoltre notare che la sicurezza dell'operatività dell'ODV è condizionata al corretto funzionamento dei sistemi operativi, delle Basi di Dati e dell'application server su cui è installato l'ODV. Le specifiche dell'ambiente IT sono descritte nel documento [AIT].

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

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

7.1 Consegna

Il Fornitore adotta sistemi per il Controllo della Configurazione e di assicurazione della qualità del prodotto per garantire l'autenticità delle componenti dell'ODV realizzate durante il processo di sviluppo e produzione e per garantire la correttezza e la completezza delle consegne al cliente finale. Il processo di sviluppo dell'ODV è quindi sottoposto ad un processo di verifica e validazione finale tramite procedure di test, al termine del quale l'ODV e la relativa documentazione a corredo possono essere formalmente consegnati al cliente finale, attraverso corrieri abilitati.

Il pacco per la consegna dell'ODV al cliente finale è costituito da 2 CD contenenti:

- i file di generazione e start-up della Base Dati Sanitaria;
- le componenti software dell'applicazione Web che costituisce l'ODV;
- la documentazione di installazione, di amministrazione e di utente [GUIDE].

Il Fornitore, al fine di verificare la correttezza e completezza del contenuto dei CD, predispone un opportuno ambiente di test, in grado di simulare l'ambiente d'installazione presso il cliente finale e un relativo piano di test, di cui controlla e verifica l'esecuzione.

7.2 Installazione

La fase di installazione è svolta da apposito personale incaricato che si assume essere fidato ed opportunamente istruito a seguire le procedure descritte nella manualistica a corredo dell'ODV stesso.

I documenti di Guida [GUIDE] contengono le informazioni necessarie sull'uso dell'ODV e su tutti gli aspetti di sicurezza che dovrebbero essere considerati.

7.3 Documentazione per l'utilizzo sicuro dell'ODV

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 del software interforze “Gestione dei dati Sanitari, infermerie e CMD” [TDS];
- Manuale di amministrazione del Software Interforze “Gestione dei dati Sanitari, infermerie e CMD” [GUIDE];
- Manuale utente del Software Interforze “Gestione dei dati Sanitari, infermerie e CMD” [GUIDE];
- Installazione, generazione e start-up del Software Interforze “Gestione dei dati Sanitari, infermerie e CMD” [GUIDE];
- Rapporto Ambiente di Test [AIT].

8 Appendice B - Configurazione valutata

La configurazione valutata per l'ODV è descritta nel documento di installazione, generazione e start-up [GUIDE]. L'ambiente operativo dell'ODV è riassunto nel documento sopra indicato ed è completamente descritto nel rapporto dell'ambiente di test [AIT].

8.1 Configurazione dell'ODV

L'ODV deve essere configurato secondo quanto descritto nella documentazione di installazione, generazione e start-up [GUIDE]. I valutatori hanno ripetuto l'installazione dell'applicazione Web con la supervisione del Fornitore, verificando la presenza nella documentazione di tutti gli elementi necessari per una corretta installazione dell'ODV nel suo ambiente operativo.

8.2 Configurazione dell'ambiente IT

L'ODV è stato sottoposto ad attività di valutazione in presenza dell'ambiente IT riassunto nel par 5.4 e configurato in base a quanto riportato nella documentazione di supporto [GUIDE]. Questo documento parte da un ambiente operativo già installato e configurato e descrive in dettaglio solamente i passi relativi all'installazione dell'applicazione Web. Durante la fase di test del processo di valutazione, i valutatori hanno eseguito una serie di analisi sull'ambiente IT in modo da ottenere una ricostruzione fedele dello stato dell'ambiente IT riportata nel rapporto ambiente di test [AIT]. Per i valutatori e per il Fornitore non è stato possibile ripetere l'installazione dell'ambiente IT in quanto, durante il processo di valutazione, questo non era sotto il controllo del Fornitore dell'ODV.

9 Appendice C - Attività di Test

Questa appendice descrive l'impegno dei valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL3 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.

9.1 Configurazione per i Test

La piattaforma utilizzata per i test è stata configurata nel pieno rispetto di tutti i requisiti relativi all'ambiente di utilizzo su computer gestiti e amministrati dallo Stato Maggiore della Difesa. Conseguentemente, l'ambiente operativo dell'ODV non è stato installato dai valutatori e sono stati previsti degli appositi test per determinare gli elementi chiave dello stato. I risultati di questi test sono stati riportati nel documento [AIT].

Per l'esecuzione dei test funzionali e di intrusione non sono stati previsti strumenti particolari ma sono stati utilizzati direttamente i computer facenti parte dell'ambiente operativo dell'ODV. Per i test mirati a ricostruire lo stato dell'ambiente operativo sono stati utilizzati software per la scansione delle vulnerabilità che hanno ricostruito in parte lo stato dell'ambiente IT ed hanno inoltre anche evidenziato alcune vulnerabilità note nei prodotti commerciali utilizzati a supporto dell'ODV. Si raccomanda, infatti, ai potenziali acquirenti del prodotto di eseguire periodicamente attività di controllo delle vulnerabilità note per i software che fanno parte dell'ambiente IT.

9.2 Test funzionali svolti dal Fornitore

Il Fornitore ha effettuato test su tutte le interfacce identificate nelle specifiche funzionali ed ha provveduto ad associare i singoli test alle funzioni di sicurezza dichiarate. I test progettati hanno preso in considerazione tutte le funzioni di sicurezza e le relative interfacce. I valutatori hanno in seguito verificato la corrispondenza dei risultati effettivi ottenuti dal Fornitore con quelli attesi. La documentazione di test prodotta ha dimostrato che il Fornitore ha eseguito i test con

un livello di approfondimento adeguato al livello di garanzia EAL3 dichiarato per l'ODV.

Pertanto, in base al verdetto espresso dai valutatori nel Rapporto Finale di Valutazione [RFV], gli sforzi del Fornitore dimostrano che le funzionalità di sicurezza definite nel Traguardo di Sicurezza [TDS] sono state implementate correttamente.

9.3 Test funzionali ed indipendenti svolti dai valutatori

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.

L'LVS ha scelto di ripetere nella loro interezza i test progettati dal Fornitore, completandoli con test indipendenti progettati dai valutatori in base alla documentazione di guida e di progetto ed ai risultati ottenuti ripetendo i test del Fornitore.

I test hanno dimostrato che l'ODV si comporta come atteso. Il livello di profondità dei test è stato considerato adeguato in base al livello di garanzia dichiarato per l'ODV.

Tutti i test sono stati progettati e documentati ad un livello tale da permetterne la ripetibilità.

L'ODV ha quindi superato con verdetto positivo la fase di test indipendente.

9.4 Analisi delle vulnerabilità e test di intrusione

I valutatori hanno confermato che l'analisi di vulnerabilità svolta dal Fornitore è esauriente in termini di ricerca delle vulnerabilità note inserite in fonti pubbliche e di presa in esame delle prove.

I valutatori hanno svolto un'analisi indipendente delle vulnerabilità relative all'ODV e al suo ambiente IT, basata su fonti pubbliche, sulla documentazione fornita per la valutazione e sull'ODV stesso messo a disposizione per l'intero processo, tenendo in giusta considerazione le ipotesi formulate sull'ambiente di sicurezza. Hanno inoltre condotto una limitata sessione di test di intrusione dimostrando che, nel rispetto delle ipotesi, nessuna vulnerabilità dell'ODV è presente e quindi sfruttabile.