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

Prodotto gestionale per il Controllo Accessi Palazzo Esercito, v. 2.33

OCSI/CERT/003/2007/RC

Versione 1.1

23/09/2009

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	Giacinto Dammicco Federico Filipponi	Prima emissione	10/09/09
1.1	Giacinto Dammicco Federico Filipponi	Riferimenti bibliografici (pagg. 7, 8, 13, 16, 20, 23). Capoversi [10], [27], [31], [32], [40], [41], [49], [53], [55]. Modifiche editoriali.	23/09/09

2 Indice

3 Elenco degli acronimi

ACL Access Control List

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CMD Carta Multiservizi della Difesa

EAL Evaluation Assurance Level

IT Information Technology

LVS Laboratorio per la Valutazione della Sicurezza

OCSI Organismo di Certificazione della Sicurezza Informatica

ODV Oggetto della Valutazione

PDV Piano di Valutazione

PP Profilo di Protezione (Protection Profile)

RFS Requisito Funzionale di Sicurezza

RFV Rapporto Finale di Valutazione

SOF Strength of Function

SW Software

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 “Prodotto gestionale per il Controllo Accessi Palazzo Esercito”, versione 3.0, Siemens SIS, 11/03/2009, cod. 9344-TDS-03.00

[MADM] Manuale Amministratore del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito, versione 3.0, Siemens SIS, 11/03/2009, cod. 9344-ADM-03.00

[MUSR] Manuale Utente del Prodotto Gestionale per il Controllo Accessi Palazzo

Esercito, versione 3.0, Siemens SIS, 11/03/2009, cod. 9344-USR-03.00

[MINST] Procedure di installazione, generazione e start-up del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito, versione 3.0, Siemens SIS, 11/03/2009, cod. 9344-IGS-03.00

[RFV] Rapporto Finale di Valutazione del “Prodotto gestionale per il Controllo Accessi Palazzo Esercito”, versione 1.1, LVS Eutelia, giugno 2009, cod. VAL-R01/07/RFV-1/15

5 Dichiarazione di certificazione

[1] L'oggetto della valutazione (ODV) è il prodotto software denominato "Prodotto gestionale per il Controllo Accessi Palazzo Esercito", v. 2.33, un'applicazione web che fornisce in remoto ai propri utenti, secondo la classica architettura client-server, le interfacce per controllare le funzionalità che realizzano la gestione di un'infrastruttura adibita al controllo degli ingressi ad aree riservate e per controllare le funzionalità per la gestione dei dati delle funzioni di sicurezza dell'ODV stesso.

[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) [CEM].

[4] L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 2.3 per il livello di garanzia EAL4, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B di questo Rapporto.

[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 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 "Prodotto gestionale per il Controllo Accessi Palazzo Esercito" 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 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	Prodotto gestionale per il Controllo Accessi Palazzo Esercito, versione 2.33
Traguardo di Sicurezza	9344-TDS-03.00, Traguardo di Sicurezza, versione 3.0, 11 marzo 2009
Livello di garanzia	EAL4
Robustezza delle funzioni di sicurezza	SOF-medium
Fornitore	Siemens IT Solutions & Services S.p.A.
Committente	Siemens IT Solutions & Services S.p.A.
LVS	Eutelia S.p.A.
Versione dei CC	2.3
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	13-11-2007
Data di fine della valutazione	17-06-2009

[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 un'applicazione web che fornisce in remoto ai propri utenti, secondo la classica architettura client-server, le interfacce per controllare sia la gestione del

controllo accessi all'infrastruttura di aree riservate, sia la gestione dei dati delle funzioni di sicurezza dell'ODV stesso.

[10] L'infrastruttura gestita dall'ODV è costituita da diversi tornelli (o porte carraie per il passaggio degli autoveicoli), presenti in ogni punto di accesso, dotati di un dispositivo denominato terminale orologio, dotato di un *display*, di un lettore di *smart card* e di un rilevatore di impronte digitali.

[11] Chiunque voglia attraversare un tornello deve essere in possesso di una *smart card* valida (una Carta Multiservizi Difesa CMD, nel caso di un dipendente civile o militare, o un *badge* temporaneo nel caso di un visitatore), inserirla nel lettore di *smart card* del terminale orologio e permettere al rilevatore la lettura della propria impronta digitale. Il terminale orologio permetterà l'ingresso al possessore della *smart card*, sbloccando il tornello o aprendo la porta carraia, se l'identificazione e autenticazione hanno avuto esito positivo e se il numero identificativo (ID) della *smart card* è presente nella lista di controllo degli accessi (ACL), che il terminale orologio stesso possiede al proprio interno.

[12] L'utente dell'ODV è un possessore di una *smart card* CMD, quindi un dipendente civile o militare dell'organizzazione, che è stato abilitato ad avere accesso alle funzionalità ed alle informazioni gestite dall'ODV.

[13] L'accesso è subordinato ad una politica di controllo degli accessi basata sul ruolo dell'utente. Sono previsti quattro ruoli differenti, ad ognuno dei quali sono associate le funzionalità che l'utente con tale ruolo può svolgere ed i dati a cui può accedere.

[14] I ruoli utente previsti dall'ODV sono:

1. Ufficio sicurezza;
2. Ufficio Pass;
3. Acquisitore CMD;
4. Amministratore.

[15] Le funzionalità dell'ODV per la gestione dell'infrastruttura sono qui riportate in forma sintetica (per una descrizione completa si rimanda a [TDS]):

- Gestione varchi. Il software permette di creare o eliminare varchi, di modificare l'insieme dei terminali orologio che formano il varco, ecc.
- Gestione ACL. Il software permette di ricercare una *smart card* per verificare in quali ACL è presente il suo ID e di aggiungere o eliminare l'ID di una *smart card* nell'ACL associata ad un varco.

- Gestione dei pass temporanei. Il software permette di assegnare ad un visitatore una *smart card* (*badge* temporaneo) con validità limitata nel tempo.

- Acquisizione delle CMD. Il software permette di acquisire la *smart card* (CMD) di un militare o dipendente civile, permettendone l'accesso ad uno o più varchi.

- Ricerca accessi. Il software permette di conoscere quali terminali orologio hanno consentito l'accesso ad una determinata *smart card*.

- Ricerca anagrafica. Il software permette la ricerca e la modifica dei dati anagrafici dei possessori delle CMD.

- Gestione autorizzazioni. Il software permette di gestire la possibilità di negare o consentire l'assegnazione dei *pass* temporanei.

[16] Le funzionalità per la ricerca nel file di *log* sono:

- Ricerca nel file di Log. Il software permette di ricercare nel file di *log* gli eventi rilevanti per la sicurezza.

[17] Le funzionalità per la gestione dei dati delle funzioni di sicurezza sono:

- Gestione dei ruoli degli utenti dell'ODV. Il software permette di assegnare, revocare o modificare i ruoli associati agli utenti dell'ODV.

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

- Identificazione: l'ODV identifica gli utenti verificando se gli stessi hanno un ruolo assegnato.

- Controllo degli accessi: l'ODV permette di accedere ai propri dati e funzioni in base al ruolo dell'utente.

- Audit e Accountability: l'ODV permette di mantenere traccia delle operazioni rilevanti per la sicurezza svolte dagli utenti autorizzati, associando alle stesse l'identità di chi le ha effettuate; l'ODV fornisce inoltre agli Amministratori la possibilità di esaminare i dati di *audit*. L'ODV registra infine le eccezioni inviategli dall'ambiente IT riguardanti l'integrità dei dati, ma non ne permette la lettura ad alcun utente dell'ODV. Le informazioni relative alle eccezioni saranno accessibili e utilizzabili soltanto da parte dell'amministratore dell'ambiente IT.

6.4 Ambito di valutazione dell'ODV

[19] L'ODV è un'applicazione web sviluppata su piattaforma Microsoft .NET, installata su un server denominato Server di controllo degli accessi e le cui funzionalità sono rese disponibili in remoto dal web server Microsoft IIS v. 6.0. Tutte le tabelle che organizzano e raggruppano i dati utente e i dati delle funzioni di sicurezza dell'ODV sono contenute nel Database di controllo accessi.

[20] L'ODV include solamente l'applicazione web che fornisce le interfacce utente attraverso il web *browser* della postazione remota. Nella configurazione di valutazione l'ODV e il database di controllo degli accessi sono installati sulla stessa macchina.

[21] L'utente autorizzato può accedere all'ODV attraverso una postazione remota, collegata alla rete intranet dell'organizzazione, utilizzando il web *browser* Internet Explorer dopo aver instaurato una connessione con il server attraverso il protocollo HTTPS.

[22] Per accedere all'ODV, l'utente deve essere in possesso di una CMD, inserirla nel lettore di *smart card* collegato alla postazione remota, e digitare l'indirizzo che l'Amministratore dell'ambiente IT ha stabilito, nella barra degli indirizzi del *browser*. Dopo aver digitato l'indirizzo, con la *smart card* CMD inserita nell'apposito lettore, si avvia il processo di identificazione e autenticazione del possessore di quest'ultima, con le modalità descritte nel Traguardo di Sicurezza [TDS].

[23] Il processo di identificazione e autenticazione è affidato all'ambiente IT; l'ODV si limita a identificare l'utente, verificando se possiede uno dei ruoli previsti.

6.5 Dichiarazioni sulla robustezza delle funzioni

[24] Per l'ODV viene dichiarata una robustezza dei meccanismi "medium" (SOF-medium) per la funzione di sicurezza di identificazione, come indicato nel Traguardo di Sicurezza ([TDS], par. 5.2).

6.6 Politiche di sicurezza dell'organizzazione

[25] Per l'ODV non è richiesta alcuna conformità ad una politica di sicurezza dell'organizzazione ([TDS], par. 3.3).

6.7 Requisiti funzionali e di garanzia

[26] 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.

[27] Tutti gli RFS sono stati presi o ricavati per estensione dai CC Parte 2 [CC2].

6.8 Conduzione della valutazione

[28] 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).

[29] 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].

[30] L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS Eutelia S.p.A.

[31] La valutazione è terminata in data 17 giugno 2009 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 27 luglio 2009. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

6.9 Considerazioni generali sulla validità della certificazione

[32] 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 installazione, generazione e start-up [MINST]. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto.

[33] 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.

7 Esito della valutazione

7.1 Risultato della valutazione

[34] 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 ("Prodotto gestionale per il Controllo Accessi Palazzo Esercito") soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, 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 [MINST]).

[35] 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 EAL4, con l'aggiunta della classe ASE per la valutazione del TDS.

Classi e componenti di garanzia		**Verdetto**
Security Target evaluation	**Classe ASE**	Positivo
TOE description	ASE_DES.1	Positivo
Security environment	ASE_ENV.1	Positivo
ST introduction	ASE_INT.1	Positivo
Security objectives	ASE_OBJ.1	Positivo
PP claims	ASE_PPC.1	Positivo
IT security requirements	ASE_REQ.1	Positivo
Explicitly stated IT security requirements	ASE_SRE.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Configuration Management	**Classe ACM**	Positivo
Partial CM automation	ACM_AUT.1	Positivo
Generation support and acceptance procedures	ACM_CAP.4	Positivo
Problem tracking CM coverage	ACM_SCP.2	Positivo
Delivery and operation	**Classe ADO**	Positivo
Detection of modification	ADO_DEL.2	Positivo
Installation, generation, and start-up procedures	ADO_IGS.1	Positivo
Development	**Classe ADV**	Positivo
Fully defined external interfaces	ADV_FSP.2	Positivo

Classi e componenti di garanzia		Verdetto
Security enforcing high-level design	ADV_HLD.2	Positivo
Subset of the implementation of the TSF	ADV_IMP.1	Positivo
Descriptive low-level design	ADV_LLD.1	Positivo
Informal correspondence demonstration	ADV_RCR.1	Positivo
Informal TOE security policy model	ADV_SPM.1	Positivo
Guidance documents	**Classe AGD**	Positivo
Administrator guidance	AGD_ADM.1	Positivo
User guidance	AGD_USR.1	Positivo
Life cycle support	**Classe ALC**	Positivo
Identification of security measures	ALC_DVS.1	Positivo
Developer defined life-cycle model	ALC_LCD.1	Positivo
Well-defined development tools	ALC_TAT.1	Positivo
Tests	**Classe ATE**	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing high-level design	ATE_DPT.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Validation of analysis	AVA_MSU.2	Positivo
Strength of TOE security function evaluation	AVA_SOF.1	Positivo
Independent vulnerability analysis	AVA_VLA.2	Positivo

Tabella 1 - Verdetti finali per i requisiti di garanzia

[36] L'LVS ha inoltre verificato che l'analisi prodotta dal Fornitore sulla robustezza del meccanismo che realizza la funzione di identificazione, mediante l'utilizzo dell'algoritmo SHA-1 per calcolare l'impronta del certificato associato a ciascun utente, è corretta e che tale meccanismo è in grado di resistere ad attacchi diretti con un potenziale di attacco medio.

7.2 Raccomandazioni

[37] Le conclusioni dell'Organismo di Certificazione sono riassunte nella Dichiarazione di certificazione a pagina 9.

[38] **Si raccomanda ai potenziali acquirenti del prodotto "Prodotto gestionale per il Controllo Accessi Palazzo Esercito", versione 2.33, di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS]**.

[39] 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.

[40] **Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV valutato**, le cui modalità di configurazione sono specificate nel documento di installazione generazione e start-up [MINST].

[41] Si raccomanda l'utilizzo dell'ODV in accordo con quanto descritto nella documentazione di guida per l'amministratore [MADM] e per l'utente [MUSR] fornita con la configurazione valutata. In particolare, l'Appendice A del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'installazione e all'utilizzo del prodotto.

[42] Si assume che gli amministratori dell'ODV siano adeguatamente addestrati al corretto utilizzo dell'ODV e scelti tra il personale fidato dell'organizzazione. L'ODV non è realizzato per contrastare minacce provenienti da amministratori inesperti, malfidati o negligenti.

[43] Occorre inoltre notare che la sicurezza dell'operatività dell'ODV è condizionata al corretto funzionamento del sistema operativo, delle basi di dati e del server web installati sulla macchina su cui è installato l'ODV e delle cui funzionalità questo si serve. Le specifiche dell'ambiente IT sono descritte nel documento [TDS].

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

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

8.1 Consegna

[45] 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 soggetto a continuo monitoraggio da parte della figura preposta al controllo della qualità del prodotto affinché tale processo venga svolto nel rispetto dei requisiti imposti dal Sistema di Gestione della Qualità aziendale.

[46] La consegna del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 2.33 al Cliente viene effettuata sulla base di una "Packing List" a fronte di un ordine di spedizione originato dal Project Manager di Siemens IT Solutions and Services.

[47] Nella "Packing List" sono riportati tutti gli elementi che verranno consegnati al Cliente:

- il CD-ROM contenente il prodotto software che costituisce l'ODV e tutti gli altri componenti SW necessari al funzionamento e all'installazione dell'ODV stesso;
- la documentazione di guida all'uso dell'ODV ed alla sua installazione.

[48] Le procedure di consegna del prodotto sono rispondenti alle normative ISO9000.

[49] In particolare tutto il materiale elencato all'interno della "Packing List" viene inserito all'interno di una medesima busta/pacco secondo le modalità previste dal contratto con il Cliente a garanzia dell'integrità fisica dei materiali spediti (supporti magnetici e documentazione).

[50] Il materiale viene consegnato al Cliente da parte del Project Manager oppure tramite raccomandata A/R.

8.2 Installazione

[51] L'installazione può essere eseguita solamente dal CD-ROM indicato nella "Packing List" che riporta tutti gli elementi dell'ODV consegnati al Cliente.

[52] Il personale con il compito di installare l'ODV deve seguire scrupolosamente le procedure indicate nel documento di installazione generazione e start-up [MINST] fornito a corredo dell'ODV stesso.

[53] Successivamente alla consegna e all'installazione dell'ODV, il Fornitore presta assistenza al Cliente (sotto forma di manutenzione e di addestramento all'utilizzo), verifica in esercizio le funzionalità del prodotto con il Cliente e rimane a sua disposizione per eventuali aggiornamenti derivanti da una modifica delle esigenze del Cliente e/o da problemi nell'utilizzo. Durante la fase di supporto il Project Manager rappresenta il punto di contatto tra il Cliente e il Fornitore.

8.3 Documentazione per l'utilizzo sicuro dell'ODV

[54] 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 "Prodotto gestionale per il Controllo Accessi Palazzo Esercito", versione 3.0, Siemens SIS, 11/03/2009, cod. 9344-TDS-03.00 [TDS];
- Manuale Amministratore del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito, versione 3.0, Siemens SIS, 11/03/2009, cod. 9344-ADM-03.00 [MADM];
- Manuale Utente del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito, versione 3.0, Siemens SIS, 11/03/2009, cod. 9344-USR-03.00 [MUSR];
- Procedure di installazione, generazione e start-up del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito, versione 3.0, Siemens SIS, 11/03/2009, cod. 9344-IGS-03.00 [MINST].

9 Appendice B - Configurazione valutata

9.1 Software

[55] Gli elementi della configurazione valutata del "Prodotto Gestionale per il Controllo Accessi Palazzo Esercito", versione 2.33, sono riportati in Tabella 2. Tali elementi includono, oltre all'ODV, anche componenti del suo ambiente IT. I file elencati sono quelli presenti sul CD di installazione dell'ODV; per facilitarne l'identificazione, per ognuno di essi è fornita l'impronta prodotta utilizzando l'algoritmo di *hash* SHA-1.

Nome File	Impronta SHA-1
CA_Ministero_della_Difesa_PKI_di_Firma_Qualificata.cer	F6DE4D6E7FD8ECE8E3DD8AD4C2399DA3A3AADCF2
CertMgr.Exe	5D50FC2611E617DAD6154D7974EC4D19DF09CAB3
INSTALLA_CERTIFICATI_DIFESA.bat	0BF2617010707E24CC4A5685A8719EF3ACBF2694
TSA_Time_Stamp_Authority_PKI_di_Firma_Qualificata.cer	E2F438D6A735ABB2BF4DBF1175244B7B133C69C0
aeronautica.cer	BCD0B89BD9940B25235FDE926E8734A6E01A09CF
difesa.cer	C24B8B8DBC3D81A22C2728902721F693E4293D61
esercito.cer	E23BFA9939AE252DEFB821E62F6BECC22DEFAA0A
iis.pfx	9EEAB1FEC82BE90C8D2274EA067B6F32710B7E5A
marina.cer	E49E1A2F5D192D9D14BC196C9CDAC4D5569F2A51
persociv.cer	39D0C139B4C9A5A633DB253650377A0F9F96DBFC
Acrobat Reader.exe	8FAABD08289B9A88023F71136F13FC4BD3290EF0
CardOS CMD.reg	24C864036AB5250FC40E60919E6E1EE5187F44D1
Microsoft .net Framework 1_1.exe	16A354A2207C4C8846B617CBC78F7B7C1856340E
Siemens .net Card Control.msi	C55E24B3089448E086C7CA8AC3B10C4D11EB16B5
Siemens .net Framework.msi	C18FAD18E2C3DC4A747B2BBC5D244DCD4CC197AE
Siemens CardOS API 2_0_4_14.exe	8BE9AB322DC5C621F6FCEF5FC1B7373E5D3CA85F
Athena ASEDrive Setup 1_4.exe	6E6837B9905CA8A64CC24063F530A9DECBBB627B
Bludrive 2.exe	C5A2174C941F8A7A0CC489CB991A870BD0215979
Gemplus_readers_on_32_bits_platform.msi	8F18168023E3D4184DE09163568147589AEC6C94
Italdata ET10 - FingerPrint Reader.zip	0C355FA3CD2DBA6F8586485CBD4D2B87CD48A63B
Omnikey CardMan3x21PCSCdriverV1.1.1.3.exe	1B3C2A1382EDFE0335F1622FA92C143538FAAC80
Omnikey CardMan4000_V3_5_0_12.exe	D0317504352A1F93C1430BBB3AC032C459D847EF
Precise Biometrics Drivers.zip	344034B37190646EF4C2D26AF9B1D4F8531F0E40
BDA.cab	31713F533548833AF5E5B91AE9E87FDE3E24A59C
BDANT.cab	69D8DA84AB833958AA4C5A7DB3F717DC6599DA0F
BDAXP.cab	B5E24E7364E4A56F90C1C85427175F44144928BA
DSETUP.dll	F561888FB9AC1ECA6AB82A987348C0391A21F2DE
DirectX.cab	382163A4469A6BA63251D78C2D09D7DA81EBCE4B
ManagedDX.CAB	949383081F64E342AAE50C4924081D1521CC780D
dsetup32.dll	3809B761004E553910AD8E6D780009C5066685CD
dxnt.cab	8FBEA73A9E94D0BD2BB01FA37294F859787F6BB2
dxsetup.exe	7234CB81E06E72EA9C4160CF70CACA19EC163ACA

Nome File	Impronta SHA-1
Siemens COGENT Finger Print Control.msi	1005CAE1A67E5C7CEC7F20E49593A67E7E819FC0
Siemens Precise Finger Print Control.msi	2B9D54455EEE98FC2DDB62CB59B63FF90E6E6429
cmdtemp_data.sql	500CE04310C2203CD017F5C771CEBFB666C8AACA
Comuni_Belfiore_SQLSERVER.sql	50C24D012D13621147E573EF87E27519ABCB8EF4
SCRIPT_DB_SQL_2505.sql	29E4F200B5E1D911AB41541DA7850FA61927D6BE
sqlserver_appoggio_cms.sql	4105E443704A16700EEA0796D54CACCB24EFCE45
sqlserver_appoggio_schema.sql	8B5324B6D8EA45FBC1F1D99EE847644BD4F90CCA
Microsoft .net Framework 1_1.exe	16A354A2207C4C8846B617CBC78F7B7C1856340E
Microsoft WSE 2.0 SP3.msi	FDD1E50C7E191C96EFBDCFCD2C34612981EBD5A3
Siemens .net Framework.msi	C18FAD18E2C3DC4A747B2BBC5D244DCD4CC197AE
Crystal Report.msi	80912846CF758944C823B3AC22BB7127D3F6780F
Siemens Web Accessi.msi	EDE496D23AAFE0A8CBCCF7B650E7DFDCA08FDB53
Siemens RemoteSM Web Service.msi	14E7F2413849C52058E982E9529C142DA9E253F9
Siemens Servizi Controllo Accessi.msi	5690D3F86F4BAB3F3F6CE5D3252212FC96C3554C
Esporta Certificato Hex.exe	0EEF68ABBB156AAC185C32283CA7433D581B96EF

Tabella 2 - Lista di configurazione dell'ODV

[56] La configurazione software dell'ambiente IT valutato, necessaria per il funzionamento dell'ODV, è quella che si ottiene applicando le procedure descritte nel documento di installazione generazione e start-up [MINST].

[57] In particolare, su tutti i server deve essere installato il sistema operativo Microsoft Windows Server 2003.

[58] Inoltre, per il server web (server di controllo degli accessi) deve essere installato il seguente software:

- Microsoft IIS 6.0;
- Microsoft .NET Framework 1.1;
- Microsoft SQL Server 2000.

[59] Per il server dedicato alla funzione di concentratore dei terminali orologio deve essere installato il software di gestione dei terminali stessi (Italdata SA015000 o Solari TermTalk).

[60] Sulle postazioni degli utenti deve essere installato il seguente software:

- Sistema operativo Microsoft Windows XP;
- Driver lettore impronte COGENT o Precise;
- Acrobat Reader o equivalente software per la lettura dei *report* PDF.

9.2 Hardware

[61] L'ODV è costituito solo da componenti software e non richiede specifiche componenti firmware o hardware; i requisiti hardware minimi richiesti per il server di controllo degli accessi e per le postazioni client sono quelli necessari all'esecuzione del software dell'ambiente IT, riportati in [TDS], cap. 2.5.

[62] In particolare per il server:

- RAM di 1GB;
- scheda di rete Ethernet.

[63] Per le postazioni remote i requisiti hardware minimi sono:

- RAM di 512MB;
- un lettore di *smart card* Siemens CardOS M4.01/A o compatibile per identificare e autenticare l'utente che accede all'ODV;
- scheda di rete Ethernet.

10 Appendice C - Attività di Test

[64] Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL4 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.

10.1 Configurazione per i Test

[65] I test indipendenti e di intrusione sono stati svolti dai Valutatori dell'LVS nel proprio laboratorio durante l'intero svolgimento della Valutazione, senza essere accorpati in sessioni specifiche.

[66] L'ambiente di test è stato approntato dai Valutatori nel proprio laboratorio, con lo scopo di definire la configurazione dei sistemi con i quali interagisce l'ODV per consentire la corretta riproducibilità delle condizioni di test.

[67] L'ambiente di test è stato realizzato utilizzando due PC, un server ed un client, connessi in rete locale, le cui configurazioni basilari hardware/software sono riportate di seguito:

Server:

- Desktop, processore AMD Athlon 2600+, 512MB RAM, scheda di rete Ethernet.
- Sistema operativo Microsoft Windows Server 2003 R2 Standard Edition, Service Pack 2 + tutti gli hotfix di sicurezza rilasciati dalla Microsoft, tramite Windows Update, fino alla data del 07/07/2008.
- DBMS Microsoft SQL Server 2000 Service Pack 4 + hotfix KB916287.
- Microsoft .NET Framework 1.1 Service Pack 1.

Client:

- Notebook, processore AMD Turion64 X2 Mobile, 1GB RAM, scheda di rete Ethernet.

- Lettore di Smartcard Athena ASE IIIe USB con relativi driver.
- Lettore di Smartcard Bit4id miniLECTOR con relativi driver.
- Lettore di impronte digitali ITALDATA ET10 con relativi driver.
- Sistema operativo Microsoft Windows XP Professional, Service Pack 3 + tutti gli hotfix di sicurezza rilasciati dalla Microsoft, tramite Windows Update, fino alla data del 07/07/2008.
- Web *browser* Microsoft Internet Explorer 6.0.

[71] Su tali postazioni sono state effettuate sempre le installazioni software e le configurazioni indicate nel documento che descrive le procedure di installazione, generazione e start-up [MINST]; in particolare, per il server è stata effettuata, prima dell'inizio dei test, una formattazione del disco fisso con successiva installazione del sistema operativo, a cui sono poi seguite tutte le azioni indicate nel suddetto documento.

[72] Per individuare eventuali vulnerabilità dell'ambiente IT in cui opera l'ODV, i Valutatori hanno effettuato apposite scansioni di sicurezza sia sul client, sia sul server, utilizzando il prodotto Tenable Nessus v.3.2.1 installato su piattaforma Microsoft Windows XP Professional Service Pack 3. Le scansioni sono state del tipo *whitebox*, effettuate cioè inserendo nello strumento Nessus le credenziali di utente amministratore per i sistemi oggetto delle scansioni; per effettuare tali scansioni è stato inoltre necessario abilitare, sulla specifica interfaccia di rete utilizzata sul server, i componenti "Client for Microsoft Networks", "File and Printer Sharing for Microsoft Network" ed il driver "NetBIOS over TCP/IP" che sono stati invece disabilitati nelle fasi di test sull'ODV, secondo quanto richiesto nel documento [MINST].

[73] Per l'attività di test non sono stati utilizzati strumenti/software particolari, ad eccezione di un editor di testo per la visualizzazione dei codice HTML delle pagine ricevute dal *browser* client.

10.2 Test funzionali svolti dal Fornitore

[74] I test progettati dal Fornitore hanno preso in considerazione tutte le funzioni di sicurezza e le relative interfacce, identificate nelle specifiche funzionali. 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 EAL4 dichiarato per l'ODV.

[75] 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.

10.3 Test funzionali ed indipendenti svolti dai Valutatori

[76] 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.

[77] 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.

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

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

10.4 Analisi delle vulnerabilità e test di intrusione

[80] I Valutatori hanno progettato un insieme di test di intrusione basandosi sull'analisi di vulnerabilità indipendente. Nell'individuazione dei test di intrusione sono stati considerati solamente attacchi attuabili con un potenziale di attacco non superiore a quello richiesto per il livello di valutazione dell'ODV (EAL4).

[81] I Valutatori, per quanto riscontrato durante l'attività di test, non hanno individuato vulnerabilità sfruttabili né vulnerabilità residue dell'ODV.