Ministero dello Sviluppo Economico

Comunicazioni - Istituto Superiore C.T.I.

Rapporto di Certificazione

ET 500 PLUS

Versione 1.0

Giugno 2008

1 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "ET 500 Plus", un dispositivo che fornisce l'accesso controllato alle periferiche in esso integrate, utilizzato per il rilascio e per la verifica dei nuovi documenti di identità elettronici.

Il prodotto ET 500 Plus 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 [ST] e nella configurazione riportata in Appendice B di questo rapporto.

Committente: ITALDATA Ingegneria dell'idea
Fornitore: ITALDATA Ingegneria dell'idea
Prodotto e Versione: ET 500Plus (1.0.0)
Descrizione: ET 500 Plus è un dispositivo che integra diverse tipologie di periferiche per il rilascio e per la verifica dei nuovi documenti di identità elettronici fornendone l'accesso controllato
CC Parte 2: Extended
CC Parte 3: Conformant
Livello di garanzia: EAL3
LVS: Consorzio RES
Data: Giugno 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 [ST], 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 valutazione è stato condotto in modo appropriato e che nessuna vulnerabilità
35 sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

2 Indice

3 Elenco degli acronimi

AT Applicativo di test
ATM Applicativo di test modificato
CC Common Criteria
CIE Carta di Identità Elettronica
DES Data Encryption Standard
EAL Evaluation Assurance Level
FW Firmware
HD Hard Disk
HW Hardware
IT Information Technology
LAN Local Area Network
LVS Laboratorio di Valutazione della Sicurezza
Kpr Key Profile
Ksc Key Smart Card
N/A Non applicabile
OCSI Organismo di Certificazione della Sicurezza Informatica
ODV Oggetto della Valutazione
PA Pubblica Amministrazione
PC Personal Computer
PIN Personal Identification Number
PL Postazione di Lavoro
PP Protection Profile
RFS Requisiti Funzionali di Sicurezza
RFV Rapporto Finale di Valutazione
SO Sistema Operativo
SOF Strength of Function
TDS Traguardo di Sicurezza
TSF TOE Security Function
USB Universal Serial Bus
VAC Volt di Corrente Alternata
VDC Volt di Corrente Continua

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

[ST] ET500 Plus – Security Target per l'ET500 Plus, versione 5.0, Dicembre 2007 (CO-06-034-TDS)

[RFV] Consorzio RES, Rapporto Finale di Valutazione 1.0RFV_V0506, versione 1.0, Gennaio 2008

135 [GUIDE] Documentazione relativa all'operatore, versione 2.0, Gennaio 2008 (CO-06-034-DRO); Procedure per installare, generare ed effettuare l'avvio dell'ODV in modo sicuro, versione 2.0, Gennaio 2008 (CO-06-034-PIA)

[SAP] Specifiche dell'Applicativo, versione 1.0, Novembre 2007 (CO-06-034-SAPP)

5 Riepilogo della valutazione

5.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza dell'ODV ET 500 Plus 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 Sicurezza [ST] che specifica i requisiti funzionali e di garanzia, e l'ambiente di utilizzo previsto.

5.2 Identificazione sintetica della certificazione

ID	A00000053
Nome dell'ODV	ET 500 Plus Versione 1.0.0
Traguardo di Sicurezza	CO-06-034-TDS Versione 5.0
Livello di garanzia	EAL 3
Robustezza delle funzioni di sicurezza	N/A
Fornitore	ITALDATA ingegneria dell'idea
Committente	ITALDATA ingegneria dell'idea
LVS	Consorzio RES
Versione dei CC	2.3
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	16-01-2007
Data di fine della valutazione	11-02-2008

Non è stato specificato il livello di robustezza dei meccanismi in quanto l'ODV non realizza meccanismi probabilistici o a permutazione.

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel Rapporto di Certificazione, e a condizione che siano rispettate le condizioni ambientali descritte nel Traguardo di Sicurezza [ST].

5.3 Prodotto valutato

L'ODV è un dispositivo che integra quattro periferiche e ne controlla l'accesso e l'abilitazione in funzione del profilo dell'operatore autenticato. La funzionalità operativa dell'ODV è quella di creare nuovi documenti di identità elettronici in adeguamento alle attuali esigenze di sicurezza, acquisendo direttamente i dati biometrici del richiedente e trasferendoli nel documento stesso; è possibile inoltre verificare l'identità del possessore confrontandone i dati memorizzati nel documento con quelli contenuti negli archivi Pubblici (Anagrafe Pubblica, Casellario Giudiziale, etc.).

L'impiego dell'ODV è destinato agli Uffici Pubblici predisposti al servizio, dove è allestita una postazione di lavoro, ossia un Personal Computer, al quale viene collegato l'ODV tramite porta USB; su tale postazione è prevista l'installazione di un applicativo che fornisce le opportune interfacce per l'accesso alle periferiche integrate nell'ODV e soprattutto che supporta il processo di autenticazione dell'operatore. Tale processo si basa su operazioni crittografiche e sull'utilizzo di due chiavi condivise tra l'ODV e la smart card in dotazione personale agli operatori autorizzati, ed ha inizio con lo sblocco delle funzionalità contenute nella smart card tramite l'inserimento da parte dell'operatore di un PIN. Le due chiavi condivise sono utilizzate rispettivamente per autenticare la smart card e per autenticare il profilo associato all'operatore che abilita le periferiche, permettendo contestualmente anche la corretta identificazione dell'operatore stesso.

5.4 Ambito di valutazione dell'ODV

L'ODV si presenta come un contenitore plastico che integra quattro periferiche ed è collegato alla postazione di lavoro tramite una porta USB. Sulla postazione è quindi necessario installare i driver di comunicazione e un applicativo che supporti il processo di autenticazione e l'accesso alle periferiche. Tale applicativo è considerato

parte dell'Ambiente IT, quindi non è fornito con l'ODV, ma le specifiche sono dettagliate in un documento pubblico [SAP]. In particolare, l'applicativo deve essere compatibile con il sistema operativo Windows 2000/XP e deve supportare un protocollo di comunicazione seriale verso l'ODV.

Fanno parte dell'Ambiente IT anche le smart card di tipo "crittografico" in dotazione personale agli operatori. La caratteristica peculiare di queste smart card è di avere al loro interno un file system in grado di attivare le funzioni interne per la verifica del PIN di sblocco e per la cifratura con algoritmo 3DES, basato su chiavi simmetriche da 24 byte (Internal Authentication) memorizzate al loro interno.

L'attivazione delle singole periferiche è strettamente connessa all'esito positivo dell'autenticazione dell'operatore ed al relativo profilo associato e non è modificabile manualmente. Inoltre, l'operatore non può instaurare più sessioni concorrenti, ossia l'ODV non consente di impostare un profilo di abilitazione diverso da quello attivo in una determinata sessione di lavoro.

L'ODV inoltre implementa ulteriori meccanismi di protezione temporizzati, esclusi dall'ambito di questa certificazione. Un primo meccanismo impone il completamento del processo di autenticazione del profilo associato all'operatore entro un limite di tempo, codificato nel firmware, allo scadere del quale l'ODV si pone in attesa di un nuovo tentativo di autenticazione. Un secondo meccanismo attiva un tempo di inibizione al verificarsi di qualsiasi errore nel processo di autenticazione della smart card o del profilo associato all'operatore. Durante tale intervallo non è possibile inviare alcun comando ad eccezione della chiusura dell'applicativo; al suo scadere l'ODV si porterà di nuovo in attesa di richiesta di autenticazione o, se è stato richiesto, chiuderà l'applicativo.

5.5 Dichiarazioni sulla robustezza delle funzioni

Per questo ODV non sono state fatte dichiarazioni in merito alla robustezza delle funzioni in quanto non sono adottati meccanismi probabilistici o a permutazione.

5.6 Politica di sicurezza dell'ODV

Il Traguardo di Sicurezza [ST] identifica la seguente politica di sicurezza dell'organizzazione a cui l'ODV deve essere conforme:

– *P.Posses*: il Responsabile dell'ODV, all'interno dell'organizzazione, deve provvedere alla gestione sicura delle smart card.

5.7 Requisiti funzionali e di garanzia

215 Il Traguardo di Sicurezza [ST], 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], ad eccezione del seguente
220 requisito che è stato esteso:

– FIA_UID.1.(EXT) è un componente esteso derivato da FIA_UID.1 e comprende i due elementi:
  - *FIA_UID.1.1 (EXT)*: The TSF shall **carry out** [3DES authentication of user's Smart Card] on behalf of the user to be performed before the
225 user is identified.
  - FIA_UID.1.2

In particolare è stato necessario estendere l'elemento FIA_UID.1.1 per evidenziare come sia obbligatorio autenticare la smart card prima di poter identificare l'operatore, mentre l'elemento FIA_UID.1.2 è stato utilizzato nella versione standard.

230 Il Traguardo di Sicurezza [ST] definisce inoltre gli RFS per l'Ambiente IT. In particolare, il seguente requisito è stato raffinato per evidenziare il meccanismo di autenticazione dell'operatore verso la smart card in suo possesso:

– User authentication before any action (FIA_UAU.2 (B))
  - *FIA_UAU.2.1* The TOE IT Environment shall require each user to be
235 successfully authenticated, **by smart card PIN code insertion**, before allowing any other TSF-mediated actions on behalf of that user.

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
240 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 suo Traguardo di Sicurezza [ST], 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 Consorzio RES.

La valutazione è terminata in data 11 febbraio 2008 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV]. Tale rapporto è stato ricevuto il 18 febbraio 2008 dall'Organismo di Certificazione che, dopo averlo analizzato, lo ha approvato il 15 aprile 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 [ST] e con riferimento all'ambiente operativo ivi specificato. La configurazione valutata è quella specificata in Appendice B. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti, e a prestare attenzione alle raccomandazioni contenute in questo Rapporto.

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 stare messe a punto patch di sicurezza e se tali patch siano state valutate e certificate.

6 Esito della valutazione

6.1 Risultato della valutazione

275 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 ET500 Plus soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL3, in relazione alle funzionalità di
280 sicurezza riportate nel Traguardo di Sicurezza [ST], se configurato secondo la configurazione valutata (Appendice B).

L'OCSI ha inoltre verificato che nell'ODV non sono implementati meccanismi probabilistici o a permutazione per cui fosse necessario dichiarare la robustezza.

6.2 Raccomandazioni

285 Le conclusioni dell'Organismo di Certificazione sono riassunte nella dichiarazione di Certificazione a pagina 2.

Si raccomanda ai potenziali acquirenti di ET 500 Plus versione 1.0 di comprendere correttamente lo scopo specifico della certificazione leggendo questo rapporto in riferimento al Traguardo di Sicurezza [ST].

290 L'ODV deve essere utilizzato in accordo all'ambiente di sicurezza specificato nella sezione 3 del Traguardo di Sicurezza [ST]. 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
295 **valutato**, la cui configurazione è specificata in Appendice B.

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.

300 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 dell'applicativo con cui si interfaccia installato sulle postazioni
305 di lavoro, nonché delle smart card in dotazione agli operatori. Le specifiche dell'applicativo sono descritte nel documento [SAP].

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 costruttivo 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 contenuto dell'imballaggio per la consegna dell'ODV al cliente finale è il seguente:

- ODV;
- documentazione relativa all'operatore;
- documentazione contenente le procedure per installare, generare ed effettuare l'avvio dell'ODV in modo sicuro;
- N° 1 CD-ROM, contenente i driver di installazione delle periferiche integrate dell'ODV;
- N° da 1 a 5 Smart Card (in base alla richiesta del cliente), ognuna con associato un diverso profilo di abilitazione delle periferiche;
- N° 1 Alimentatore da 220 Vac/12 Vdc;
- N° 1 Cavo USB.

L'imballaggio contenente l'ODV è corredato da opportuni documenti di trasporto e dalle buste contenenti i PIN associati alle smart card.

Il cliente finale, al momento della ricezione dell'imballaggio, dovrebbe verificare, oltre all'integrità dell'imballaggio stesso, che l'ODV consegnato corrisponda a quello sottoposto a certificazione CC e che la sicurezza dell'ODV non è stata compromessa durante la consegna. Tra i dati presenti sull'etichetta, visibile sul retro dell'ODV, si consiglia in particolare di verificare che il Part Number del prodotto sia uguale a

"A00000053". Inoltre il cliente finale dovrebbe accertarsi che l'ODV non sia stato visibilmente manomesso e/o danneggiato.

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.

L'unico ruolo previsto per l'ODV nella sua configurazione valutata è quello di "operatore", ossia utente autorizzato all'uso delle periferiche ed in possesso di una determinata smart card e del relativo codice PIN di sblocco.

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 di ET 500 Plus [ST];
- documentazione contenente le procedure per installare, generare ed effettuare l'avvio dell'ODV in modo sicuro [GUIDE];
- documentazione relativa all'Operatore [GUIDE];
- specifiche dell'Applicativo di Gestione dell'ET 500 Plus [SAP].

8 Appendice B - Configurazione valutata

Nella tabella 1 di seguito riportata, sono elencati tutti i componenti hardware e firmware che identificano univocamente l'ODV. Per ogni componente sono stati riportati il codice e la versione. È stato inserito anche il CD-ROM di installazione dei driver ed il codice assegnato all'ODV stesso.

Codice	Versione	Componente
A00000053	1.0	ODV
PM0001070	1.0	Telaio contenitore (semiparte superiore)
PM0001071	1.0	Telaio contenitore (semiparte inferiore)
310000098	1.0	Lettore Contact-less
EC0000089	1.0	Console Display
EC0000133	1.0	Scheda Cpu
EM0000121	1.0	Scanner Ottico Foto/Firma
EM0000133	1.0	Scanner Ottico Impronte
EM0000125	1.0	Lettore di Smart Card a contatti
FA001400	1.0.0	Firmware operativo dell'ODV inserito nel µProcessore e contenente le istruzioni.
CD11000001	1.0	CD-ROM con i driver delle periferiche integrate

Tabella 1 - Elementi di configurazione HW e FW dell'ODV

L'ambito della valutazione è descritto nel cap. 5.4.

8.1 Configurazione dell'ODV

L'ODV deve essere configurato secondo quanto descritto nella documentazione
365 riportata nel par. 7.1. I valutatori hanno ripetuto l'installazione dell'ODV 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

370 L'ODV è stato sottoposto ad attività di valutazione in presenza dell'ambiente IT specificato in par 5.4 e configurato in base a quanto riportato nella documentazione di supporto [GUIDE]. Durante la ripetizione della installazione dell'ODV, i valutatori hanno verificato la presenza nella documentazione di indicazioni precise su come configurare correttamente l'ambiente operativo.

9 Appendice C – Architettura di sicurezza

Questa appendice riporta un'introduzione delle principali caratteristiche architetturali dell'ODV. Maggiori dettagli legati all'ambito della valutazione sono forniti in Appendice B.

L'ODV comprende quattro periferiche integrate in un contenitore plastico a forma di parallelepipedo ed è interamente costituito da parti hardware e firmware.

La figura che segue schematizza l'architettura hardware dell'ODV da cui si evincono i seguenti componenti:

- uno scanner ottico per l'acquisizione delle impronte digitali;
- un lettore di chip "contact-less" (standard ISO 14443 A/B) per la lettura del Passaporto Elettronico;
- un scanner ottico statico compatto (senza parti in movimento) per l'acquisizione della firma autografa e della foto in formato tessera;
- un lettore di smart card "contact" utilizzato per la smart card in dotazione agli operatori in fase di autenticazione o per i documenti elettronici (ad es. la CIE) allo scopo di verificare o trasferire i dati dell'utente generico (biometrici ed anagrafici);
- una console composta da un display alfanumerico, un segnalatore acustico e due tasti;
- la scheda CPU dove risiede l'hardware di controllo delle periferiche ed il µProcessore nel quale è caricato il firmware operativo dell'ODV. In particolare, la presenza del componente convertitore USB-RS232 consente al µProcessore di comunicare con l'applicativo installato sulla postazione di lavoro.

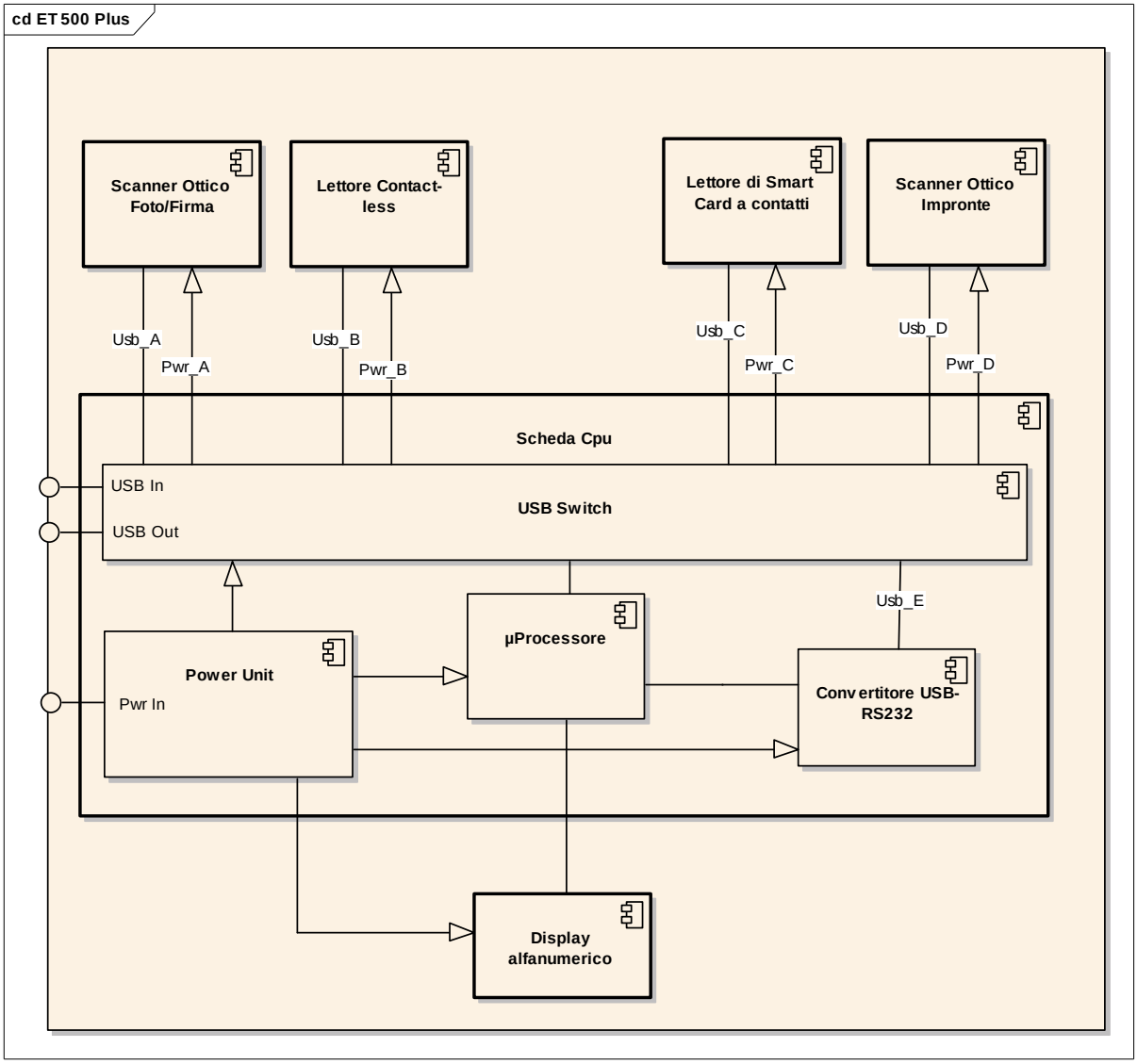

Figura 1 - Architettura

Le sigle riportate in figura hanno il seguente significato:

- Usb_A / Usb_D, bus USB di collegamento dalla scheda CPU alle Periferiche;
- Usb_E, bus USB interno alla scheda CPU di collegamento all'interfaccia RS232;
- Pwr_A / Pwr_D, collegamenti di alimentazione dalla scheda CPU alle Periferiche;
- Pwr_In, ingresso dell'alimentazione primaria dell'ODV;
- USB_In, ingresso collegamento USB al PC;

– USB_Out, uscita USB che replica la porta impegnata dal PC per il collegamento con l'ODV (in pratica l'ODV non sottrae risorse di connessione al PC).

10 Appendice D- 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.

10.1 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. Conseguentemente, l'ODV è stato testato servendosi di una postazione allestita presso i laboratori del Fornitore ed avente le caratteristiche hardware e software riportate nella seguente tabella:

Equipaggiamento hardware	
Piattaforma	Intel
Caratteristiche	Processore Pentium III 1,0 GHz Ram: 256 MB
Modello	Reckon
Equipaggiamento software	
Sistema Operativo	Windows XP Professional Versione 2002 Service Pack 2
Applicativo di Gestione	"ET500Plus.exe"
Applicativo di test (AT)	"Test_ET500Plus_2.exe"
Applicativo di test modificato (ATM)	"Test_ET500Plus_Serial.exe"

Dispositivi esterni collegati	
OdV	ET500 Plus
Lettore smart card	

Tabella 2 - Caratteristiche hardware e software della postazione utilizzata per i test

Gli applicativi di test AT e ATM sono stati appositamente sviluppati dal Fornitore per fornire supporto alla fase di test funzionali e di intrusione. In particolare, il primo è stato utilizzato per verificare in modo puntuale tutti i comandi previsti dal protocollo di comunicazione dell'ODV [SAP] e, nel contesto della procedura di autenticazione dell'operatore, il comportamento dell'ODV nei casi più significativi; l'applicativo ATM è invece l'applicativo di test modificato rispetto ad AT per poter interagire con smart card inserite nel secondo lettore esterno.

A completamento dell'ambiente di test il Fornitore ha messo a disposizione cinque smart card con associati i cinque profili previsti per l'ODV e due smart card di test, contenenti rispettivamente una chiave Ksc non condivisa con l'ODV e una chiave Kpr associata ad un profilo inesistente.

Gli stessi strumenti sono stati utilizzati dai valutatori per svolgere le prove di intrusione.

10.2 Test funzionali svolti dal Fornitore

Il Fornitore ha testato 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 [ST] sono state implementate come richiesto.

10.3 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.

10.4 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 o 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 è presente e quindi sfruttabile.