PRODOTTO: **ET 500 Plus**

TITOLO DEL DOCUMENTO: **TRAGUARDO DI SICUREZZA**

Funzione	Nome	Data	Firma
Autore del documento	M.Caparrelli	05/12/2007	
Riesaminato da	F.Barboni	05/12/2007	
Validato da	R.Tartaro	05/12/2007	
Approvato da	R.Boccacci	05/12/2007	

Modifiche			
VERSIONE	**PAGINA**	**CAPITOLO/PARAGRAFO**	**MODIFICHE**
1.0			
2.0	Intero documento		In seguito alle osservazioni riportate in 1.0RO01_V0506, fare riferimento al documento 1.0DR01_V0506.
3.0	Intero documento		In seguito alle osservazioni riportate in 1.0RO02_V0506, fare riferimento al documento 1.0DR02_V0506.
4.0	Intero documento		In seguito alle osservazioni riportate in 1.0RO05_V0506, fare riferimento al documento 1.0DR05_V0506.
5.0	Intero documento		In seguito alle osservazioni riportate in Nota Dell'Organismo di Certificazione (NOC) – Versione 0.1, 24/10/2007 (CERT/001/07-01), fare riferimento al documento 1.0RN01.

Lista di distribuzione			
SOCIETÀ	**NOME**	**FUNZIONE**	**N° DI COPIE**
Consorzio RES	E.Campaiola	LVS	1
OCSI	L.Gratta	Organismo di Certificazione per la Sicurezza Informatica	1

INDICE

INDICE DELLE FIGURE

INDICE DELLE TABELLE

1 INTRODUZIONE

Questo Traguardo di Sicurezza (TDS) descrive gli obiettivi, i requisiti e le motivazioni di sicurezza per l'ET 500 Plus (OdV). L'ET 500 Plus è un dispositivo per il rilascio e per la verifica dei nuovi documenti di identità elettronici. L'OdV è destinato ad essere collegato ad un Personal Computer, nel contesto di un generico ufficio della Pubblica Amministrazione.

Identificazione del Traguardo di Sicurezza
Titolo: Traguardo di Sicurezza
Versione: 5.0
Data : 05 dicembre 2007

Identificazione dell'OdV
Nome del prodotto: ET 500 Plus
Codice del prodotto: A00000053
Versione: 1.0.0

Conformità alle direttive
L'OdV è aderente alle seguenti direttive dei Common Criteria (CC):

- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 2.3 August 2005;
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 2.3 August 2005.

Livello Robustezza
Non ci sono meccanismi probabilistici o permutazionali per i quali può essere definito un livello di robustezza.

Livello di Garanzia
EAL3 Common Criteria

1.1 Scopo del documento

Il presente TDS, in linea con quanto previsto dai Common Criteria, vuole fornire le informazioni per l'identificazione univoca dell'ET500 Plus e delle componenti ad esso correlate.

Il suo contenuto si prefigge lo scopo di:

- fornire la descrizione per grandi linee dell'OdV;
- identificare le possibili minacce a cui l'OdV è sottoposto, nell'ambiente operativo previsto;
- focalizzare gli obiettivi di sicurezza dell'OdV;
- focalizzare i requisiti di sicurezza dell'OdV;
- identificare le funzioni di sicurezza che permettono di contrastare le minacce previste ed attuare le politiche di sicurezza dell'organizzazione;
- dimostrare che l'OdV è coerente con gli obiettivi di sicurezza predefiniti.

1.2 Struttura del documento

Il documento è strutturato nelle seguenti sezioni:

- **introduzione**: contiene una breve spiegazione dello scopo e della struttura del documento stesso;
- **descrizione dell'OdV:** chiarisce lo scopo, l'ambiente operativo e le caratteristiche tecniche dell'OdV;
- **definizione dell'ambiente di sicurezza**: focalizza i rischi che caratterizzano l'ambiente nel quale viene utilizzato l'OdV;
- **obiettivi di sicurezza:** focalizza le finalità di sicurezza che si intendono perseguire per l'OdV e per il contesto ambientale;
- **requisiti di sicurezza:** evidenzia i requisiti funzionali di sicurezza dell'OdV ed i requisiti di garanzia della sicurezza;
- **sommario delle specifiche:** evidenzia le funzioni di sicurezza dell'OdV e le misure di garanzia adottate;
- **costruzione delle motivazioni del TDS**: si prefigge di dimostrare che la realizzazione dell'OdV è coerente con gli obiettivi predefiniti e che le misure di garanzia applicate rispettano il livello di certificazione EAL3.

1.3 Acronimi

CC Common Criteria

CIE Carta di Identità Elettronica

EAL Evaluation Assurance Level

FW Firmware

HW Hardware

IT Information Technology

LAN Local Area Network

MB Megabyte

OdV Oggetto della Valutazione

PA Pubblica Amministrazione

PC Personal Computer

PIN Personal Identification Number

PL Postazione di Lavoro

PP Protection Profile

SOF Strenght of Function

TOE Target of Evaluation

TDS Traguardo di Sicurezza

TSC TSF Scope of Control

TSF TOE Security Function

USB Universal Serial Bus

1.4 Documenti di riferimento

[RD1] CO-06-034-SAPP (Specifiche dell'Applicativo, versione 1.0)
[RD2] Smart card standard ISO 7816

2 DESCRIZIONE DELL'ODV

2.1 Contesto

L'OdV è un dispositivo per il rilascio e per la verifica dei nuovi documenti di identità elettronici, in risposta all'esigenza, nell'ambito Nazionale ed Internazionale, di adeguamento alle attuali esigenze di sicurezza.
Nella *Figura 1*, viene mostrata sinteticamente l'architettura del contesto operativo dell'OdV.
Il processo d'emissione del documento elettronico prevede l'acquisizione dei dati biometrici ed anagrafici presso gli uffici della Pubblica Amministrazione (PA) dislocati sul territorio nazionale di riferimento (Uffici comunali, Uffici Postali, etc.).

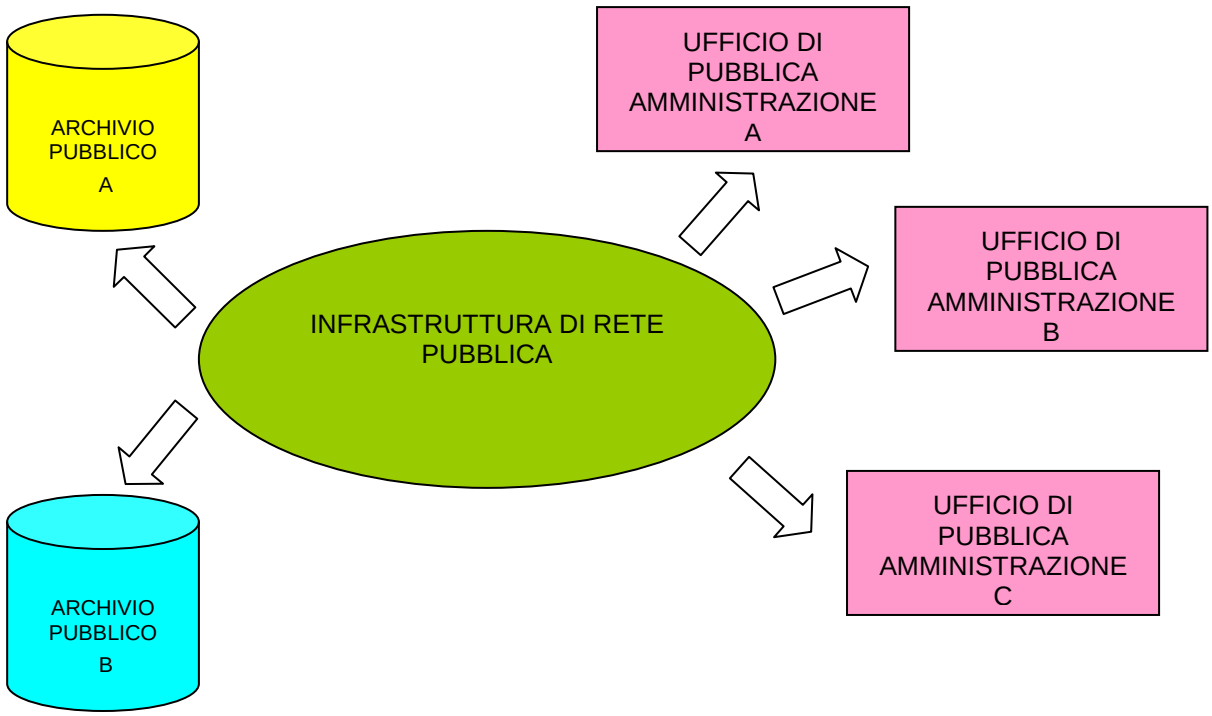

Figura 1: Contesto operativo dell'OdV

Nell'Ufficio Pubblico, dove è allestita la postazione di lavoro (che viene descritta nel *Paragrafo 2.1.1*), vengono acquisiti i dati biometrici della persona attraverso l'OdV e successivamente trasferiti nel documento elettronico. Contestuale all'acquisizione dei dati vengono eseguite delle interrogazioni verso gli archivi Pubblici (Anagrafe Pubblica, Casellario Giudiziario, etc.), finalizzate alla verifica dell'identità ed all'accertamento di eventuali responsabilità penali (controllo della fedina penale).

2.1.1 Descrizione della postazione di lavoro

La Postazione di Lavoro (PL), rappresentata nella *Figura 2*, è composta dal Personal Computer (PC) al quale viene collegato, tramite porta USB, l'OdV. Inoltre, come è visibile nella *Figura 2*, la PL è collegata alle Rete Informatica della Pubblica Amministrazione (LAN).

Il Personal Computer è basato su una architettura HW INTEL con installato un Sistema Operativo[1] del tipo Windows XP / Windows 2000 con i seguenti requisiti minimi del processore e della memoria dati:

- Pentium P3, 1 GHz (2,4 GHz consigliati), 128 MB RAM (256 MB consigliati);

Indipendentemente dalla versione del sistema operativo, il PC dovrà essere corredato, al minimo, delle seguenti risorse:

- 200 MB di spazio disponibile sull'HD (il disco rigido),
- Unità CDROM,
- Scheda video a colori a 16 bit,
- Porta USB 1.1 o 2.0 (USB 2.0 consigliata).

Dal punto di vista della connettività è necessaria la presenza di almeno 1 porta USB (per l'OdV) e di una porta LAN (per la connessione alla rete).

[1] Gli utenti del sistema operativo non vanno confusi con gli operatori dell'OdV: la policy che definisce gli attributi degli uni (accesso alle risorse locali e di rete) e degli altri (profilo di abilitazione delle periferiche) è completamente distinta.

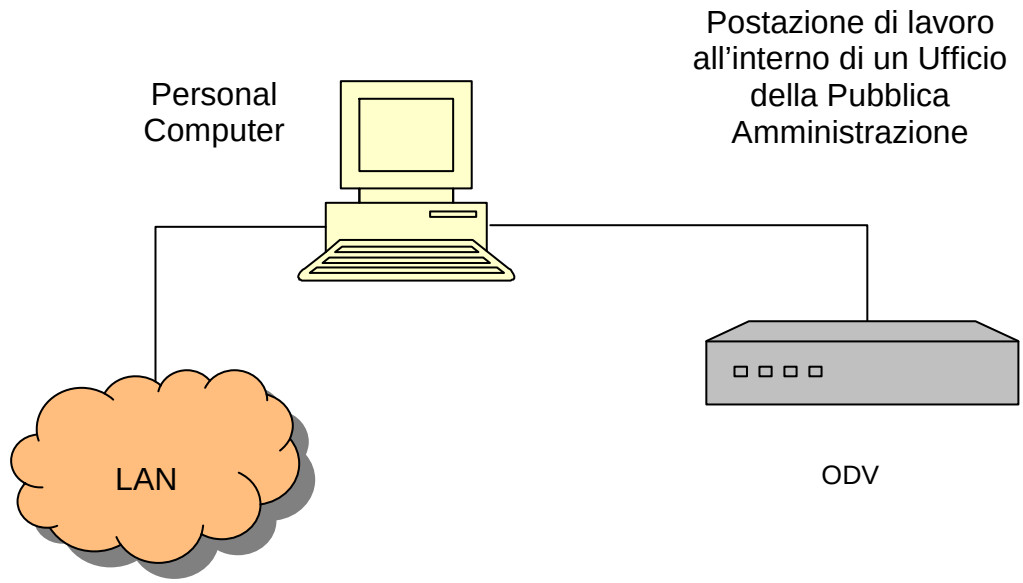

Figura 2: Postazione di Lavoro

2.2 Ambiente IT

L'ambiente IT dell'OdV è costituito da:

- un applicativo, il cui compito è quello di supportare il processo di autenticazione dell'operatore e di fornire le opportune interfacce per l'accesso alle periferiche integrate nell'OdV,
- da smart card, opportunamente inizializzate, alle quali è associato il profilo di abilitazione delle periferiche dell'OdV.

L'applicativo deve essere compatibile con il sistema operativo Windows 2000/XP e deve supportare un protocollo di comunicazione seriale verso l'OdV. Le specifiche dell'applicativo e la descrizione dettagliata del protocollo di comunicazione tra applicativo e OdV sono riportate nel documento [RD1].

La smart card consente all'operatore di autenticarsi presso l'OdV. Le smart card previste sono cinque: ognuna è associata ad un determinato profilo a cui corrisponde una precisa configurazione delle periferiche integrate nell'OdV. Solo l'operatore in possesso di una determinata smart card e a conoscenza del corrispondente PIN di sblocco può essere autenticato dall'OdV. La digitazione del corretto codice PIN permette l'autenticazione

dell'operatore sulla smart card. L'abilitazione della smart card consente lo sblocco delle operazioni crittografiche e l'utilizzo delle chiavi di cifratura condivise con l'OdV.
La smart card condivide con l'OdV due chiavi di cifratura[2]: la prima viene utilizzata per autenticare la smart card inserita nel relativo lettore, la seconda per autenticare il profilo di abilitazione delle periferiche e quindi per identificare, in modo corretto, l'operatore.

La smart card in dotazione all'operatore è di tipo "crittografico", ovvero ha al suo interno un *file system* in grado di attivare funzioni interne per la verifica del PIN e di cifratura con algoritmo 3DES, basato su chiavi simmetriche da 24 byte (Internal Authentication). Il PIN consente di abilitare le funzioni di cifratura 3DES della smart card, la quale diventa inutilizzabile[3] qualora il PIN venga digitato erroneamente per 3 volte consecutive. Lo standard di riferimento delle smart card è descritto in [RD2].

2.3 Composizione dell'OdV

2.3.1 Hardware dell'OdV

L'OdV comprende 4 periferiche integrate in un contenitore plastico a forma di parallelepipedo. La *Figura 3* seguente fornisce l'illustrazione dell'architettura HW dell'OdV:

[2] Le chiavi sono definite nel codice firmware dell'OdV e non sono leggibili né modificabili.

[3] Il blocco della smart card è irreversibile, non è previsto l'utilizzo del PUK.

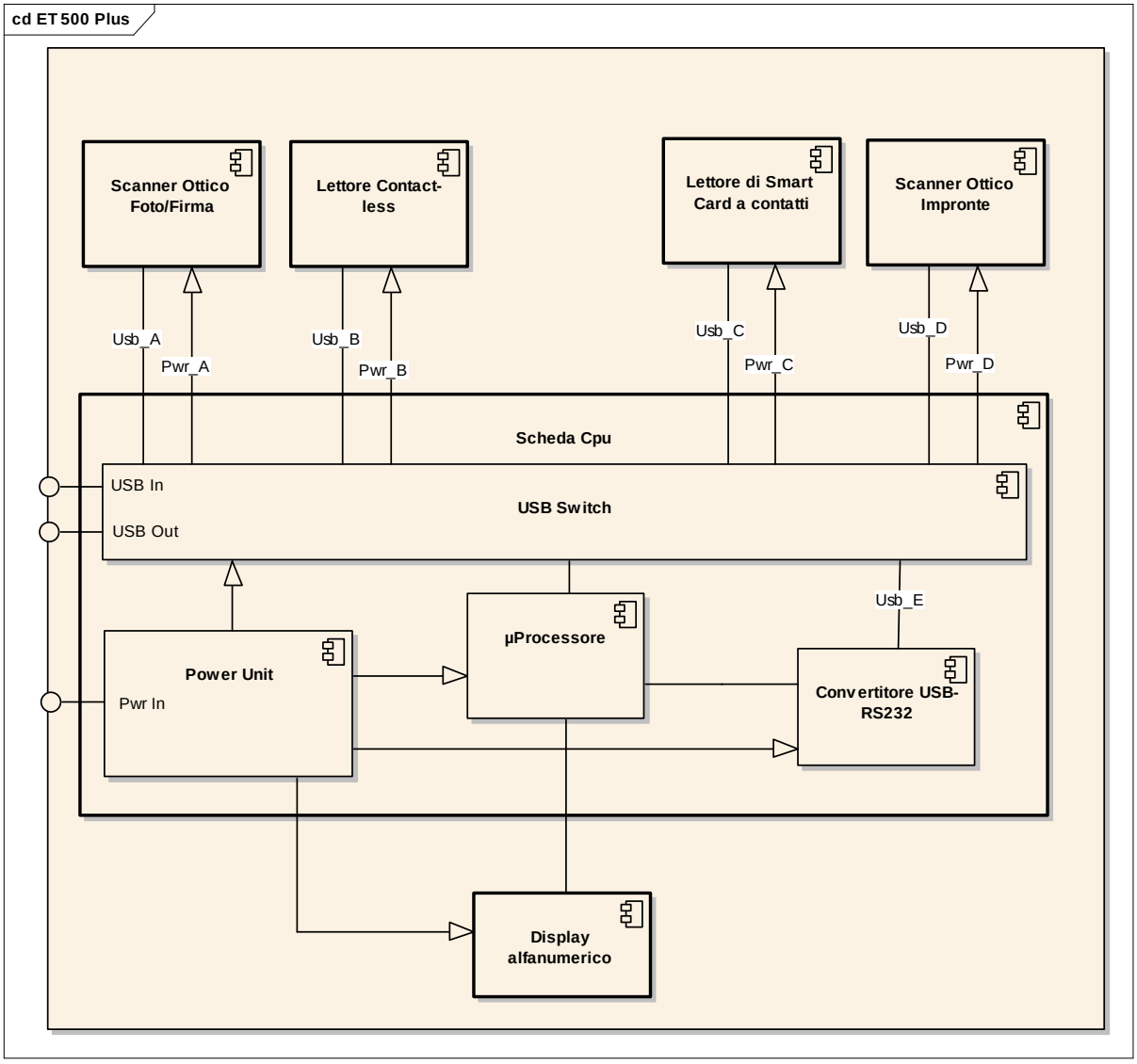

Figura 3: Schema interno dell'OdV

Con riferimento alla *Figura 3*, di seguito una sintetica descrizione dei 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 compatto scanner ottico statico (senza parti in movimento) per l'acquisizione della firma autografa e per l'acquisizione della foto in formato tessera;
- un lettore di smart card "contact" dove inserire sia la smart card per l'autenticazione dell'operatore, sia il documento elettronico (ad es. la CIE) allo scopo di trasferirvi 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'HW di controllo delle periferiche ed il µProcessore nel quale è caricato il FW operativo dell'OdV. Nella scheda CPU è anche presente il

componente convertitore USB-RS232 che consente al µProcessore di comunicare con l'applicativo.

e la legenda delle sigle utilizzate:

- 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).

2.3.2 Firmware dell'OdV

L'applicativo Firmware dell'OdV è stato realizzato in linguaggio "C". Dopo la compilazione (dalla quale si ottiene il codice binario), il FW viene caricato all'interno della memoria del µProcessore sulla scheda CPU. In generale il firmware dell'OdV può essere considerato come un insieme di "macro funzioni" o moduli che comprendono, a loro volta, altre funzioni più elementari e che scambiano dati tra loro attraverso memoria condivisa e/o chiamate a funzioni. Questi moduli vengono identificati nell'elenco seguente:

- **Main**, è il modulo che si occupa dello start up del programma e di consentire agli altri moduli di svolgere le funzioni specifiche di loro pertinenza;
- **Event Manager**, è il modulo che si occupa della rilevazione degli eventi che avvengono nel contesto del funzionamento dell'OdV e ne coordina le attività conseguenti;
- **Display Manager**, è il modulo che si occupa della gestione dell'interfaccia display, visualizzando i messaggi relativi alla condizione operativa dell'OdV;
- **Authentication_Manager**, è il modulo che si occupa della gestione del processo di autenticazione dell'operatore;
- **Communication Manager**, è il modulo che governa lo scambio dati tra l'applicativo di gestione, installato sul PC, e l'OdV attraverso la connessione USB. Interpreta il set di comandi previsto dal protocollo di comunicazione e all'OdV di inviare e ricevere sulla connessione USB i dati formattati secondo tale protocollo;
- **Timer1 Manager**, è un modulo che implementa un gruppo di 8 timer virtuali programmabili sulla base di un intervallo temporale pari ad un centesimo di secondo;
- **Timer2 Manager**, è un modulo che implementa un gruppo di 8 timer virtuali programmabili sulla base di un intervallo temporale pari ad un decimo di secondo;

- **Input Manager**, è un modulo che gestisce un gruppo di 8 input virtuali[4], per i quali è definito un valore di inerzia[5]; ad ogni input virtuale viene assegnato il controllo di un input fisico (una linea di input del µProcessore) che fa capo al circuito HW;
- **Output Manager**, è un modulo che gestisce un gruppo di 8 output virtuali[6], ad ogni output virtuale viene assegnato il controllo di un output fisico (una linea di output del µProcessore) che fa capo al circuito HW.

2.4 Modalità operativa dell'OdV

L'unico ruolo previsto per gli utilizzatori dell'OdV, relativamente allo scenario operativo descritto, è quello di "operatore". L'Operatore è un utente autorizzato all'uso delle periferiche integrate dell'OdV perché dotato di una opportuna smart card di tipo crittografico, alla quale è associato il "profilo[7]" di abilitazione delle periferiche integrate dell'OdV. Non esistono parametri configurabili o modificabili : per tale ragione non esiste un ruolo di tipo Amministratore che si occupi della gestione dell'OdV. È previsto solo l'intervento di un ente terzo per le procedure di installazione.
Per utilizzare l'OdV l'operatore in possesso della smart card e del corrispondente codice PIN viene sottoposto ad un processo di autenticazione da parte dell'OdV. L'autenticazione dell'operatore è finalizzata alla determinazione del suo profilo. Tale profilo è memorizzato all'interno della smart card in possesso dell'operatore stesso. Ad autenticazione avvenuta, l'operatore può utilizzare l'OdV in base al profilo di abilitazione rilevato dalla propria smart card; ad ogni profilo è associato lo stato di abilitazione di ciascuna delle periferiche integrate dell'OdV. Il numero massimo di smart card è pari a 5 e, come detto, ciascuna corrisponde ad un determinato profilo di abilitazione delle periferiche.
Durante una "sessione di lavoro" risulteranno abilitate solo le periferiche corrispondenti al profilo di abilitazione della smart card in possesso dell'operatore che ha aperto la sessione. In particolare, ogni sessione di lavoro ha inizio con l'abilitazione delle periferiche dell'OdV e termina in seguito ai seguenti casi:

- interruzione del collegamento fra la postazione di lavoro e l'OdV (disconnessione fisica del collegamento USB),
- chiusura dell'applicativo.

[4] Con "input virtuale" si intende un registro di memoria che contiene il riferimento all'input fisico, allo stato (ON/OFF), ed al valore di inerzia.

[5] Quando l'input fisico cambia stato (da ON a OFF e viceversa) il valore assegnato all'inerzia stabilisce la durata minima di persistenza dell'input nel nuovo stato prima di considerare la variazione come effettiva.

[6] Con "output virtuale" si intende un registro di memoria che contiene il riferimento all'output fisico, allo stato di attivazione, al tempo di attivazione ed alla modalità di attivazione (impulsivo o statico).

[7] Nel proseguo del documento, le espressioni "profilo associato all'operatore" e "profilo di abilitazione delle periferiche integrate dell'OdV" si riferiscono indistintamente allo stato di abilitazione di ciascuna delle periferiche integrate dell'OdV.

Per consentire l'attivazione del processo di autenticazione dell'operatore in possesso di smart card, l'OdV parte con il lettore di smart card sempre abilitato. Non c'è connessione tra ruolo "operatore" dell'OdV e ruoli "amministratore" e "utente" del Sistema Operativo.

L'uso dei profili trova la sua ragione nell'ambito operativo dell'OdV che spazia dalla semplice verifica del documento di identità elettronico (l'accertamento che il medesimo sia autentico), alla sua generazione (processo di acquisizione dei dati biometrici, verifiche presso gli Archivi della PA, inizializzazione dei dati, rilascio e consegna); pertanto l'OdV prevede diversi profili per abilitare gli operatori ai diversi ambiti operativi.

2.5 Beni da proteggere

L'OdV, attraverso le sue funzioni di sicurezza, deve proteggere l'accesso alle sue periferiche integrate.

3 DEFINIZIONE DELL'AMBIENTE DI SICUREZZA

3.1 Ipotesi

3.1.1 Ipotesi sul personale

A.NOEVIL si assume che gli operatori dell'OdV siano persone fidate, opportunamente istruite al corretto utilizzo dell'OdV.

3.1.2 Ipotesi sull'ambiente non-IT

A.PROTECT si assume che l'OdV sia utilizzato sempre in un ambiente presidiato da un operatore o da personale autorizzato.

3.1.3 Ipotesi sull'ambiente IT

A.APPLICATION si assume che l'applicativo descritto in [RD1] supporti il processo di autenticazione implementato dall'OdV e l'accesso controllato alle sue periferiche integrate.

A.CARD si assume che le smart card utilizzate per accedere alle periferiche integrate dell'OdV siano di tipo crittografico, antitampering, in grado di mantenere la confidenzialità e l'integrità delle chiavi di cifratura condivise con l'OdV.

3.2 Minacce

T.ACCOUNT utenti non autorizzati potrebbe far uso dell'OdV.

T.ACCOUNT_PROFILE un operatore potrebbe utilizzare l'OdV diversamente da quanto definito dal suo profilo.

3.3 Politiche di sicurezza dell'organizzazione

P.POSSES il Responsabile dell'OdV, all'interno dell'organizzazione, deve provvedere alla gestione sicura delle smart card.

4 OBIETTIVI DI SICUREZZA

4.1 Obiettivi di sicurezza dell'OdV

O.AUTHENTICATION l'OdV deve sottoporre l'operatore ad un processo di autenticazione prima di consentirgli l'utilizzo dell'OdV stesso.

O.PROFILE_SELECTION l'OdV deve consentire l'utilizzo delle periferiche integrate in base al profilo associato alla smart card in possesso dell'operatore.

O.SINGLE_SESSION_PROFILE l'OdV non deve consentire l'attivazione di sessioni di lavoro multiple.

4.2 Obiettivi di sicurezza per l'ambiente IT

OE.CRYPTO le smart card utilizzate per accedere all'OdV devono essere di tipo crittografico.

OE.ENV l'ambiente IT deve supportare il processo di autenticazione dell'OdV e l'accesso alle sue periferiche integrate.

4.3 Obiettivi di sicurezza per l'ambiente non-IT

OE.NOEVIL gli operatori devono essere fidati ed opportunamente istruiti sul corretto utilizzo dell'OdV e dell'ambiente IT.

OE.AUTHETINCATION l'uso delle smart card deve essere consentito solo ai legittimi proprietari.

OE.MANAGE l'OdV e le smart card crittografiche ad esso associate devono essere gestiti in modo sicuro all'interno dell'organizzazione.

5 REQUISITI FUNZIONALI DI SICUREZZA

Nella *Tabella 1* è riportato l'elenco dei Requisiti Funzionali dell'OdV e dell'Ambiente IT:

Requisiti Funzionali
FIA_UID.1(EXT): Timing of identification
FIA_UAU.2 (A), (B): User authentication before any action
FDP_ACC.2: Complete access control
FDP_ACF.1: Security attribute based access control
FTA_TSE.1: TOE session establishment
FCS_COP.1 (A), (B), (C): Cryptographic operation

Tabella 1:Requisiti Funzionali di Sicurezza

5.1 Requisiti Funzionali di Sicurezza dell'OdV

5.1.1 Identification & Authentication (FIA)

5.1.1.1 Timing of identification (FIA_UID.1(EXT))

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 user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Note Applicative: il requisito **FIA_UID.1(EXT)** deriva direttamente dal requisito **FIA_UID.1**. L'estensione è stata necessaria per evidenziare l'obbligatorietà dell'autenticazione della smart card prima dell'identificazione dell'operatore.

5.1.1.2 User authentication before any action (FIA_UAU.2(A))

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.2 User and Data protection (FDP)

5.1.2.1 Complete access control (FDP_ACC.2)

FDP_ACC.2.1 The TSF shall enforce the [*integrated devices access policy*] on [subjects: *operator*
object*: integrated devices*]
and all operations among subjects and objects covered by the **SFP.**

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.2.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [*integrated devices access policy*] to objects based on the following:

[subjects attributes: *operator profiles*
objects attributes: *integrated devices permission bits*]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*the permission bit, associated with the (operator profile- integrated device) correspondence, is set up to enable*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [*none*].

5.1.3 TOE Access (FTA)

5.1.3.1 TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [*TOE state*].

5.1.4 Cryptographic support (FCS)

5.1.4.1 Cryptographic operation (FCS_COP.1 (A))

FCS_COP.1.1 The TSF shall perform [*data decryption*] in accordance with a specified cryptographic algorithm [*3DES*] and cryptographic key sizes [*24 byte long*] that meet the following:[*3DES extension ANSI X9.52-1998, FIPS 46-3*].

5.1.4.2 Cryptographic operation (FCS_COP.1 (B))

FCS_COP.1.1 The TSF shall perform [*random number generation*] in accordance with a specified cryptographic algorithm [*SHA-1*] and cryptographic key sizes [*64 byte long*] that meet the following:[*FIPS 140-2*].

5.2 Requisiti Funzionali di Sicurezza dell'Ambiente IT

5.2.1.1 User authentication before any action (FIA_UAU.2 (B))

FIA_UAU.2.1 The TOE IT Environment shall require each user to be successfully authenticated, **by smart card PIN code insertion**, before allowing any other TSF-mediated actions on behalf of that user.

Note Applicative: il requisito **FIA_UAU.2,** per l'Ambiente IT**,** è stato raffinato per evidenziare il meccanismo di autenticazione dell'utente.

5.2.1.2 Cryptographic operation (FCS_COP.1 (C))

FCS_COP.1.1 The TOE IT Environment shall perform [*data encryption*] in accordance with a specified cryptographic algorithm [*3DES*] and cryptographic key sizes [*24 byte long*] that meet the following:[*3DES extension ANSI X9.52-1998, FIPS 46-3*].

5.3 Dichiarazione di robustezza per i requisiti

Non ci sono requisiti di sicurezza per i quali occorre indicare una dichiarazione di robustezza, in quanto l'OdV non utilizza meccanismi probabilistici o permutazionali.

5.4 Requisiti di garanzia della sicurezza

Per la determinazione dei requisiti di garanzia della sicurezza (Tabella 2) si fa riferimento al livello 3 (EAL3) come specificato nella parte 3 dei Common Criteria.

ACM_CAP.3	**Authorisation controls**
ACM_SCP.1	**TOE CM coverage**
ADO_DEL.1	**Delivery process**
ADO_IGS.1	**Installation, generation and start up procedures**
ADV_FSP.1	**Informal functional specification**
ADV_HLD.2	**Security enforcing high-level designe**
ADV_RCR.1	**Informal correspondence demonstration**
AGD_ADM.1	**Administrator guidance**
AGD_USR.1	**User guidance**
ALC_DVS.1	**Identification of security measures**
ATE_COV.2	**Analysis of coverage**
ATE_DPT.1	**Testing: high level design**
ATE_FUN.1	**Functional testing**
ATE_IND.2	**Indipendent testing- sample**
AVA_MSU.1	**Examination of guidance**

AVA_VLA.1	**Developer vulnerability analysis**

Tabella 2: Requisiti di garanzia della Sicurezza

6 SOMMARIO DELLE SPECIFICHE

6.1 Funzioni di sicurezza dell'OdV

6.1.1 F1: Autenticazione dell'operatore da parte dell'OdV

L'OdV autentica l'operatore in possesso della smart card attraverso due fasi successive: autenticazione della smart card in suo possesso e autenticazione del profilo associato all'operatore (l'identificazione del profilo associato all'operatore è contestuale alla sua autenticazione).

Nell'OdV è stata implementata una logica in grado di effettuare un'autenticazione basata su chiave simmetrica (algoritmo 3DES). È vincolante che questa autenticazione abbia esito positivo, affinché il personale autorizzato possa utilizzare le periferiche integrate dell'OdV.
Il processo di autenticazione dell'operatore da parte dell'OdV è supportato da un processo di riconoscimento dell'identità dell'operatore da parte della smart card.

6.1.2 F2: Accesso controllato alle periferiche

L'operatore, attraverso l'applicativo di gestione dell'OdV, può accedere solo alle periferiche associate al suo profilo.

Dal profilo dell'operatore, acquisito durante il processo di autenticazione, viene ricavato lo stato di abilitazione per ciascuna delle periferiche integrate. L'operatore potrà quindi fare uso solo delle periferiche che risulteranno essere abilitate.

6.1.3 F3: Blocco delle sessioni multiple

L'OdV non consente l'instaurazione di sessioni multiple.

L'OdV non consente di impostare un profilo di abilitazione diverso da quello attivo in una determinata sessione di lavoro, ovvero l'operatore non può stabilire più sessioni concorrenti. Ogni tentativo di apertura di una nuova sessione, oltre quella già attiva, comporta la disabilitazione di tutte le periferiche attive.

Il cambio del profilo attivo è possibile chiudendo la sessione corrente e riaprendone un'altra, con una nuova smart card. La chiusura della sessione può essere una conseguenza

dell'interruzione del collegamento fra la postazione di lavoro e l'OdV (disconnessione fisica del collegamento USB) e dell'uscita dall'applicativo.

6.2 Dichiarazione SOF per le funzioni di sicurezza

Non ci sono funzioni di sicurezza per le quali sia necessario indicare una dichiarazione di robustezza, in quanto l'OdV non utilizza meccanismi probabilistici o permutazionali.

6.3 Misure di Garanzia

Con riferimento alla *Tabella 3* che segue, vengono messi in relazione i componenti di garanzia previsti dai Common Criteria con i documenti di riferimento redatti nel contesto della valutazione dell'OdV.

Componenti di garanzia	Documentazione di riferimento	Motivazione
ACM_CAP.3 **ACM_SCP.1**	• Documentazione relativa alla gestione della configurazione; • Elenco degli elementi della configurazione.	Nei documenti è descritto il processo di gestione delle configurazioni, la modalità con la quale è gestita la tracciatura delle configurazioni dell'OdV nel sistema di revisione aziendale, nonché la lista relativa alla configurazione dell'OdV e alla documentazione relativa al processo di valutazione dello stesso.
ADO_DEL.1	• Documentazione relativa alla consegna.	Nel documento sono descritte le modalità di consegna dell'OdV al cliente.
ADO_IGS.1	• Procedure per installare, generare ed effettuare l'avvio dell'OdV in modo sicuro.	Nel documento è descritta la procedura di installazione ed attivazione dell'OdV.
ADV_FSP.1	• Specifiche funzionali.	Nel documento vengono identificate le specifiche funzionali a copertura dei requisiti dell'OdV.

ADV_HLD.2	• Progetto ad alto livello.	Nel documento vengono identificati i principali sottosistemi dell'OdV implementanti le funzioni di sicurezza.
ADV_RCR.1	• Specifiche funzionali; • Progetto ad alto livello.	I requisiti di garanzia relativi a questo componente sono soddisfatti nei documenti Specifiche funzionali e Progetto di Alto Livello.
AGD_ADM.1 **AGD_USR.1**	• Documentazione relativa all'operatore	Nel documento sono descritte le operazioni per l'uso corretto e sicuro dell'OdV.
ALC_DVS.1	• Documentazione relativa alla sicurezza del processo di sviluppo dell'OdV.	Nel documento sono descritte tutte le misure di sicurezza necessarie per proteggere la confidenzialità e l'integrità del progetto e la sua implementazione.
ATE_COV.2 **ATE_DPT.1** **ATE_FUN.1** **ATE_IND.2**	• Documentazione relativa ai test.	Nella documentazione è descritto il piano di test. Sono inoltre riportati i test per la verifica delle funzionalità dell'OdV e sono descritte le modalità per l'esecuzione dei test e la registrazione dei risultati.
AVA_MSU.1	• Documentazione relativa all'operatore.	Nel documento sono descritte le operazioni per l'uso corretto e sicuro dell'OdV.
AVA_VLA.1	• Analisi di vulnerabilità; • Informazioni aggiornate sulle vulnerabilità evidenti.	Nei documenti è riportata un'analisi dettagliata delle vulnerabilità note e aggiornate dell'OdV.

Tabella 3: Misure di garanzia

7 CONFORMITÀ AD UN PP

Il presente TDS non fa riferimento ad alcun PP.

8 COSTRUZIONE DELLE MOTIVAZIONI DEL TDS

8.1 Motivazioni degli obiettivi di sicurezza

La *Tabella 4* mette in relazione assunzioni, minacce e politiche di sicurezza dell'organizzazione con gli obiettivi di sicurezza dell'OdV e dell'ambiente.
Dalla medesima si evince come ogni obiettivo di sicurezza contrasta e/o considera almeno un'esigenza di sicurezza definita nell'ambiente di sicurezza dell'OdV (condizione sufficiente per dimostrare la necessarietà di ciascun obiettivo).
Per dimostrare la sufficienza degli obiettivi ad affrontare le esigenze di sicurezza, nei paragrafi a seguire, si riporteranno opportune motivazioni.

	O.AUTHENTICATION	O.SINGLE_SESSION_PROFILE	O.PROFILE_SELECTION	OE.CRYPTO	OE.ENV	OE.AUTHENTICATION	OE.NOEVIL	OE.MANAGE
A.NOEVIL							**X**	
A.PROTECT							**X**	
A.APPLICATION					**X**			
A.CARD				**X**		**X**		**X**
T.ACCOUNT	**X**			**X**		**X**		**X**
T.ACCOUNT_PROFILE		**X**	**X**			**X**		**X**
P.POSSES							**X**	**X**

Tabella 4: Mappatura degli Obiettivi di Sicurezza dell'OdV

8.1.1 A.NOEVIL

Si assume che gli operatori dell'OdV siano persone fidate, opportunamente istruite al corretto utilizzo dell'OdV.

Questa ipotesi è sostenuta da OE.NOEVIL che garantisce che gli operatori abilitati all'uso dell'OdV siano persone fidate ed opportunamente istruite. L'affidabilità del personale è sotto la responsabilità dell'organizzazione delegata all'uso dell'OdV; mentre l'istruzione del personale viene opportunamente supportata da manualistica fornita a corredo.

8.1.2 A.PROTECT

Si assume che l'OdV sia utilizzato sempre in un ambiente presidiato da un operatore o da personale autorizzato.

Questa assunzione è sostenuta da OE.NOEVIL per gli aspetti legati all'affidabilità ed al livello di istruzione degli operatori abilitati all'uso dell'OdV.

8.1.3 A.APPLICATION

Si assume che l'applicativo descritto in [RD1] supporti il processo di autenticazione implementato dall'OdV e l'accesso alle sue periferiche integrate.

OE.ENV è un obiettivo direttamente riconducibile a A.APPLICATION, poiché l'assunzione identifica i requisiti dell'ambiente che devono essere rispettati per garantire la sicurezza dell'OdV.

8.1.4 A.CARD

Si assume che le smart card utilizzate per accedere alle periferiche integrate dell'OdV siano di tipo crittografico, antitampering, in grado di mantenere la confidenzialità e l'integrità delle chiavi di cifratura condivise con l'OdV.

OE.CRYPTO garantisce che le smart card utilizzate per accedere alle periferiche dell'OdV sono di tipo crittografico ed è supportato da OE.MANAGE per ciò che concerne la corretta gestione delle smart card all'interno delle organizzazioni in cui l'OdV verrà utilizzato. Inoltre OE.AUTHENTICATION garantisce che l'uso delle smart card sia consentito solo ai legittimi proprietari, cioè operatori fidati e debitamente istruiti all'uso sicuro di esse.

8.1.5 T.ACCOUNT

Utenti non autorizzati potrebbero far uso dell'OdV.

Questa minaccia è contrastata da O.AUTHENTICATION. Infatti l'obiettivo assicura che prima di accedere alle risorse dell'OdV l'operatore deve essere autenticato dall'OdV stesso. L'autenticazione darà l'autorizzazione all'uso dell'OdV solo se correttamente eseguita. O.AUTHENTICATION è inoltre supportato da OE.CRYPTO, OE.MANAGE e OE.AUTHENTICATION: il primo dà garanzia sul fatto che le smart card utilizzate dagli operatori sono di tipo crittografico; OE.MANAGE garantisce che l'OdV e le smart card sono gestite in modo sicuro all'interno delle organizzazioni in cui l'OdV verrà utilizzato; OE.AUTHENTICATION stabilisce che l'uso delle smart card deve essere consentito solo ai legittimi proprietari (i.e. operatori che ne conoscono il relativo PIN).

8.1.6 T.ACCOUNT_PROFILE

Un operatore potrebbe utilizzare l'OdV diversamente da quanto definito dal suo profilo di account.

Questa minaccia è contrastata da O.SINGLE_SESSION_PROFILE e O.PROFILE_SELECTION. Ad ogni smart card è associato soltanto un profilo di abilitazione che consente all'operatore di utilizzare le risorse dell'OdV esclusivamente secondo quanto previsto da quel profilo: è quanto viene garantito da O.PROFILE_SELECTION. Attivato un profilo, l'OdV non consente di attivarne uno diverso, se non chiudendo la sessione corrente per riaprirne una nuova, a partire dall'autenticazione dell'operatore, e ciò è assicurato da O.SINGLE_SESSION_PROFILE.
Inoltre i due obiettivi sono supportati da OE.MANAGE per contrastare l'eventuale gestione non sicura dell'OdV, e/o delle smart card assegnate agli operatori, che potrebbe causare un uso dell'OdV non permesso e da OE.AUTHENTICATION che dà garanzia sull'uso delle smart card, riservandolo solo agli operatori che ne conoscono il relativo PIN.

8.1.7 P.POSSES

Il Responsabile dell'OdV, all'interno dell'organizzazione, deve provvedere alla gestione sicura delle smart card.

Questa politica di sicurezza è supportata da OE.MANAGE, perché l'obiettivo assicura che la gestione dell'OdV e delle smart card avviene in modo sicuro all'interno dell'organizzazione in cui l'OdV verrà utilizzato. Inoltre tale obiettivo è supportato da OE.NOEVIL che garantisce che, nel caso in cui il Responsabile coincida con un operatore, quest'ultimo è opportunamente istruito sul corretto uso dell'OdV.

8.2 Motivazioni dei requisiti di sicurezza

8.2.1 Motivazione dei requisiti funzionali di sicurezza

La *Tabella 5* indica la relazione diretta fra i requisiti funzionali di sicurezza e gli obiettivi che ciascun requisito soddisfa.

Dalla tabella si evince come i requisiti di sicurezza coprono tutti gli obiettivi di sicurezza: ogni requisito di sicurezza affronta almeno un obiettivo (condizione di sufficienza per dimostrare la necessarietà di ciascun requisito di sicurezza) e ciascun obiettivo dell'OdV è affrontato da almeno un requisito di sicurezza (condizione di sufficienza dei requisiti). Inoltre, per la dimostrazione della sufficienza dei requisiti di sicurezza individuati si riporteranno, nei paragrafi a seguire, opportune motivazioni.

	O.AUTHENTICATION	O.PROFILE_SELECTION	O.SINGLE_SESSION_PROFILE	OE.CRYPTO	OE.AUTHENTICATION	OE.ENV
FIA_UID.1(EXT)	X					X
FIA_UAU.2(A)	X					X
FIA_UAU.2(B)					X	X
FDP_ACC.2		X				
FDP_ACF.1		X				
FTA_TSE.1			X			
FCS_COP.1(A)	X					X
FCS_COP.1(B)	X					X
FCS_COP.1(C)	X			X		X

Tabella 5: Mappatura dei Requisiti Funzionali di Sicurezza con gli Obiettivi di Sicurezza dell'OdV e dell'Ambiente IT

8.2.1.1 O.AUTHENTICATION

L'OdV deve sottoporre l'operatore ad un processo di autenticazione prima di consentirgli l'utilizzo dell'OdV stesso.

L'OdV garantisce che l'operatore venga autenticato prima che sia possibile l'uso delle sue periferiche integrate (FIA_UAU.2 (A)). L'autenticazione si basa sull'uso di 2 chiavi crittografiche condivise tra smart card e OdV: una servirà ad autenticare la smart card e l'altra ad autenticare il profilo associato all'operatore. In entrambi i casi, l'OdV implementerà operazioni di decifratura utilizzando le suddette chiavi (FCS_COP.1 (A)), mentre le operazioni di cifratura delle chiavi sono realizzate da meccanismi crittografici delle smart card

(FCS_COP.1(C)). Inoltre l'OdV utilizzerà un generatore di numeri random per la generazione dei numeri che verranno scambiati tra OdV, applicativo e smart card durante le fasi di autenticazione dell'operatore per permettere la realizzazione del meccanismo di challenge-response (FCS_COP.1 (B)).
Le uniche azioni permesse dalle funzioni di sicurezza prima dell'autenticazione dell'operatore sono quelle relative all'autenticazione della smart card (FIA_UID.1(EXT)). L'autenticazione dell'operatore termina con l'autenticazione del profilo associato all'operatore. Tale profilo permetterà l'abilitazione delle periferiche integrate nell'OdV ad esso relative.

8.2.1.2 O.PROFILE_SELECTION

L'OdV deve consentire l'utilizzo delle periferiche integrate in base ai diritti dell'operatore che si è autenticato.

Questo obiettivo di sicurezza è soddisfatto perché nell'OdV è stata definita ed implementata una politica di controllo accessi alle risorse che stabilisce che ogni operatore può utilizzare le periferiche dell'OdV in base al profilo associato alla smart card in suo possesso, secondo la politica definita in FDP_ACC.2 e la regola definita in FDP_ACF.1.

8.2.1.3 O.SINGLE_SESSION_PROFILE

L'OdV non deve consentire l'attivazione di sessioni di lavoro multiple.

Questo obiettivo di sicurezza è soddisfatto perché l'OdV non consente la selezione di un profilo avendone già attivo uno (FTA_TSE.1), indipendentemente dal fatto che il profilo sia uguale o diverso da quello corrente. In ogni caso questa eventualità viene considerata dall'OdV come un tentativo di violazione che determina l'interruzione della sessione di lavoro ed il ripristino della condizione operativa che precede l'autenticazione dell'operatore.

8.2.1.4 OE.CRYPTO

Le smart card utilizzate per accedere alle periferiche integrate dell'OdV devono essere di tipo crittografico.

Questo obiettivo di sicurezza è soddisfatto in quanto le smart card utilizzate dagli operatori realizzano operazioni crittografiche per supportare il processo di autenticazione degli operatori stessi (FCS_COP.1 (C)).

8.2.1.5 OE.AUTHENTICATION

L'uso delle smart card deve essere consentito solo ai legittimi proprietari.

I meccanismi utilizzati per realizzare l'autenticazione dell'operatore da parte dell'OdV sono supportati da un meccanismo di autenticazione dell'operatore da parte della smart card, attraverso il riconoscimento dell'identità del legittimo proprietario della stessa, con l'uso del PIN (FIA_UAU.2(B)).

8.2.1.6 OE.ENV

L'ambiente IT deve supportare il processo di autenticazione dell'OdV e l'accesso alle sue periferiche intergrate.

Le smart card sono utilizzate durante le sfide di challenge-response (relativamente all'autenticazione della smart card e all'autenticazione del profilo) per le operazioni di cifratura (FCS_COP.1(C)) e forniscono un meccanismo di autenticazione dell'operatore (sulla smart card), attraverso il riconoscimento dell'identità del legittimo proprietario della stessa, con l'uso del PIN (FIA_UAU.2(B)).
L'applicativo permette la trasmissione di dati e comandi tra smart card e OdV dopo opportuno adattamento di protocollo ([RD1]), sia nella fase di autenticazione dell'operatore sulla smart card (FIA_UAU.2(B)) che durante il processo di autenticazione dell'OdV (FIA_UID.1(EXT) e FIA_UAU.2(A)). In quest'ultimo caso, l'applicativo riceve dall'OdV i dati che devono essere cifrati dalla smart card e restituisce all'OdV i dati cifrati dalla smart card, permettendo la realizzazione dei meccanismi di challenge-response del processo di autenticazione (FCS_COP.1(A) e FCS_COP.1(B)). Inoltre l'applicativo fornisce all'operatore le opportune interfacce per poter utilizzare le periferiche intergrate dell'OdV, secondo quanto riportato in [RD1].

8.2.2 Motivazioni delle Dipendenze dei Requisiti

Nella *Tabella 6* vengono indicate le dipendenze dei requisiti di sicurezza. Per le dipendenze previste dai Common Criteria (livello di garanzia EAL3), ma non soddisfatte dall'OdV, verranno fornite opportune motivazioni.

Requisiti del TDS	Dipendenze richieste dal CC	Dipendenze soddisfatte
FIA_UID.1(EXT)	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.1(EXT)(*)
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.2
FTA_TSE.1	None	None
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 and FMT_MSA.2	None
ACM_CAP.3	ALC_DVS.1	ALC_DVS.1

ACM_SCP.1	ACM_CAP.3	ACM_CAP.3
ADO_DEL.1	None	None
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1
ADV_RCR.1	None	None
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ALC_DVS.1	None	None
ATE_COV.2	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_DPT.1	ADV_HLD.1 and ATE_FUN.1	ADV_HLD.1 and ATE_FUN.1
ATE_FUN.1	None	None
ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 AGD_USR.1 and ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 AGD_USR.1 and ATE_FUN.1
AVA_MSU.1	ADO_IGS.1 and ADV_FSP.1 AGD_ADM.1 and AGD_USR.1	ADO_IGS.1 and ADV_FSP.1 AGD_ADM.1 and AGD_USR.1
AVA_VLA.1	AGD_FSP.1 and ADV_HLD.1 AGD_ADM.1 and AGD_USR.1	AGD_FSP.1 and ADV_HLD.1 AGD_ADM.1 and AGD_USR.1

Tabella 6: Motivazioni delle Dipendenze dei Requisiti

(*) La dipendenza richiesta dai CC è comunque soddisfatta. Il requisito FIA_UID.1(EXT) deriva direttamente dal requisito FIA_UID.1, aggiungendo solo un aspetto di obbligatorietà alle possibili operazioni definibili in FIA_UID.1.

Per quanto riguarda le dipendenze non soddisfatte, di seguito ne vengono fornite le giustificazioni.

FDP_ITC.1 e FDP_ITC.2: l'OdV non prevede l'importazione di dati utente.

FCS_CKM.1 e FCS_CKM.4: l'OdV non prevede né la generazione di chiavi crittografiche né la loro distruzione.

FMT_MSA.2 e FMT_MSA.3: l'OdV non prevede la possibilità di gestire gli attributi di sicurezza. L'OdV non prevede, in alcun caso, di modificare i parametri di configurazione, e di conseguenza la possibilità di definire differenti valori di default che possano essere utilizzati per creare un nuovo oggetto.

8.2.3 Giustificazione sulla scelta dei requisiti di garanzia

I requisiti di garanzia previsti per il livello EAL3 forniscono una moderata garanzia per la protezione dell'OdV nei confronti delle minacce individuate nel suo contesto operativo. Infatti il soddisfacimento, da parte dell'OdV, dei requisiti contenuti nel pacchetto EAL3 permette di avere evidenze circa le misure di sicurezza applicate all'ambiente di sviluppo dell'OdV e sul sistema di gestione della configurazione utilizzato. Inoltre con i requisiti di garanzia relativi ad EAL3 si approfondisce l'analisi del comportamento delle funzioni di sicurezza con conseguente perfezionamento nella scoperta di eventuali vulnerabilità dell'OdV .

8.3 Motivazioni del Sommario delle specifiche dell'OdV

8.3.1 Motivazioni delle funzioni di sicurezza

In questo paragrafo sono descritte, come si evince dalla *Tabella 7*, le relazioni tra le funzioni di sicurezza dell'OdV ed i requisiti funzionali di sicurezza.
Dalla tabella si evince come le funzioni di sicurezza soddisfano tutti i requisiti funzionali di sicurezza: ogni funzione di sicurezza implementa almeno un requisito (condizione di sufficienza per dimostrare la necessarietà di ciascuna funzione di sicurezza) e ciascun requisito dell'OdV è soddisfatto da almeno una funzione di sicurezza (condizione di sufficienza delle funzioni). Inoltre, per la dimostrazione della sufficienza delle funzioni di sicurezza individuate si riporteranno, a seguire, opportune motivazioni.

	Autenticazione dell'operatore da parte dell'OdV	Accesso controllato alle periferiche	Blocco delle sessioni multiple
FIA_UID.1(EXT)	X		
FIA_UAU.2(A)	X		
FDP_ACC.2		X	
FDP_ACF.1		X	
FTA_TSE.1			X
FCS_COP.1(A)	X		
FCS_COP.1(B)	X		

Tabella 7: Mappatura tra Funzioni di Sicurezza e Requisiti di Sicurezza

FIA_UID.1(EXT) definisce la capacità, da parte dell'OdV, di permettere operazioni prima che l'operatore (utente) venga identificato.

Questo requisito viene implementato dalla funzione "Autenticazione dell'operatore da parte dell'OdV (F1)". Infatti l'autenticazione dell'operatore da parte dell'OdV si sviluppa in due fasi successive: la prima ha lo scopo di autenticare la smart card in suo possesso (FIA_UID.1(EXT)) e la seconda consente di autenticare il profilo di abilitazione associato alla

sua smart card. L'identificazione del profilo associato all'operatore (*i.e.* identificazione dell'utente) è contestuale alla sua autenticazione.

FIA_UAU.2(A) definisce la capacità da parte dell'OdV di autenticare l'operatore (utente), prima di permettergli ogni altra interazione con l'OdV stesso.

Questo requisito viene implementato dalla funzione "Autenticazione dell'operatore da parte dell'OdV (F1)". L'autenticazione dell'operatore, come descritto per FIA_UID.1(EXT), è finalizzata alla determinazione del profilo associato all'operatore, attraverso la smart card in suo possesso. Soltanto in questo modo è possibile abilitare l'uso delle periferiche integrate dell'OdV.

FDP_ACC.2 definisce la politica di controllo accesso alle risorse dell'OdV.

Questo requisito viene implementato dalla funzione "Accesso controllato alle periferiche (F2)". Infatti, a seguito dell'autenticazione dell'operatore, l'OdV attiva le sole periferiche previste dalla sua configurazione interna, relativamente al profilo associato alla smart card dell'operatore. Ad ogni smart card è associato un solo profilo; il numero massimo di smart card disponibili è 5; pertanto, il numero massimo di profili configurabili per l'OdV è 5.

FDP_ACF.1 descrive la politica di controllo accessi alle risorse dell'OdV, definita attraverso il requisito FDP_ACC.2.

Questo requisito viene implementato dalla funzione "Accesso controllato alle periferiche (F2)". L'OdV è in grado di permettere l'utilizzo delle risorse integrate solo dopo aver riconosciuto la presenza di un profilo di abilitazione valido, associato alla smart card dell'operatore.

FTA_TSE.1 definisce la capacità dell'OdV di identificare gli attributi di sicurezza attraverso i quali può negare l'apertura delle sessioni di lavoro.

Questo requisito viene implementato dalla funzione "Blocco delle sessioni multiple (F3)". L'OdV non consente di impostare un profilo di abilitazione diverso da quello attivo in una determinata sessione di lavoro. Il cambio del profilo attivo è possibile chiudendo la sessione corrente e riaprendone un'altra, con una nuova smart card. La chiusura della sessione può essere una conseguenza dell'interruzione del collegamento fra la postazione di lavoro e l'OdV (disconnessione fisica del collegamento USB) e dell'uscita dall'applicativo. Una sessione di lavoro ha inizio con l'abilitazione delle periferiche associate alla smart card dell'operatore che si è autenticato e termina con l'uscita dall'applicazione, eventualmente con la disconnessione dell'OdV o con la violazione del protocollo di accesso alle sue risorse.

FCS_COP.1(A), (B) descrive le operazioni crittografiche implementate dall'OdV.

Questi requisiti vengono implementati dalla funzione "Autenticazione dell'operatore da parte dell'OdV (F1)". L'OdV utilizzerà un generatore di numeri random per la generazione dei numeri che verranno scambiati tra OdV, applicativo e smart card durante le fasi di autenticazione dell'operatore, per permettere la realizzazione del meccanismo di challenge-response (FCS_COP.1(B)). Durante il processo di autenticazione dell'operatore, l'OdV

esegue operazioni di decifratura relativamente ai numeri scambiati con la smart card (FCS_COP.1(A)).

8.4 Adeguatezza delle misure di garanzia

Nella *sezione 6.2* si è dimostrato come ogni Requisito di Garanzia è affrontato da una appropriata misura di garanzia. Tali misure sono sufficienti per il livello di garanzia EAL3, fissati le esigenze di sicurezza dell'ambiente IT ed gli obiettivi.