TRAGUARDO DI SICUREZZA DEL PRODOTTO GESTIONALE PER IL CONTROLLO ACCESSI PALAZZO ESERCITO

Versione 3.0
Marzo 11, 2009
9344-TDS-03.00

Indice

Indice delle Figure

Indice delle Tabelle

Revisioni del documento

Versione	Data emissione	Descrizione delle modifiche
1.0	10/08/07	Prima emissione
2.0	28/04/08	Modifiche relative all'intero documento in accordo alle osservazioni del laboratorio di valutazione indicate in VAL-R01/07/ROA/1
3.0	11/03/09	Modifiche relative all'intero documento in accordo alle osservazioni del laboratorio di valutazione indicate in VAL-R01/07/ROA-6/16

Lista degli Acronimi

ACL	Access Control List (Lista di controllo degli accessi)
API	Application Programming Interface (Interfaccia di programmazione di un'applicazione)
CA	Certification Authority (Autorità di Certificazione)
CC	Common Criteria
CMD	Carta Multiservizi Difesa
DBMS	Database Management System (Sistema di gestione dei database)
EAL	Evaluation assurance level (Livello di Garanzia della Valutazione)
ID	Identificatore
IE	Internet Explorer
IP	Internet Protocol (Protocollo Internet)
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
ODV	Oggetto della Valutazione
OS	Operating System (Sistema operativo)
PIN	Personal Identification Number (Numero identificativo personale)
PP	Protection Profile (Profilo di protezione)
PSO	Politica di sicurezza di un'organizzazione
SFP	Security Function Policy (Politica della funzione di sicurezza)
SFR	Security Functional Requirement (Requisito funzionale di sicurezza)
SHA	Secure Hash Algorithm (Algoritmo di sicurezza hash)
SOF	Strength of Function (Robustezza di una Funzione di Sicurezza)
SQL	Structured Query Language
SSL	Secure Sockets Layer
TDS	Traguardo di Sicurezza
TOE	Target of Evaluation (Oggetto della valutazione)

TSC TSF Scope of Control (Ambito di controllo della TSF)

TSF TOE security function (Funzione di sicurezza del TOE)

TSP TOE security policy (Politica di sicurezza del TOE)

Riferimenti

[CCP1] CCMB-2005-08-001 - Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, ver. 2.3, agosto 2005;

[CCP2] CCMB-2005-08-002 - Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, ver. 2.3, agosto 2005;

[CCP3] CCMB-2005-08-003 - Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, ver. 2.3, agosto 2005;

1. Introduzione del TDS

1.1. Identificazione del TDS

La seguente tabella contiene le informazioni per l'identificazione del presente traguardo di sicurezza.

Titolo:	Traguardo di Sicurezza del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito
Livello di garanzia:	EAL4
Autori:	Siemens
Versione CC:	2.3
Conformità ai PP:	N.A.
Versione del TDS:	3.0
Data:	11/03/09
ODV:	Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 2.33

Tabella 1 – Identificazione TDS

1.2. Descrizione del TDS

Il presente Traguardo di Sicurezza definisce i requisiti di sicurezza IT per il "Prodotto gestionale per il Controllo Accessi Palazzo Esercito v.2.33". Il Prodotto gestionale per il Controllo Accessi Palazzo Esercito v.2.33 (ODV) è un' applicazione web – based che rende disponibile ai propri utenti le funzioni che permettono la gestione di una infrastruttura adibita al controllo degli accessi ai punti di ingresso ad aree riservate. Gli utenti dell'applicazione si connettono ad essa da una postazione remota attraverso il web browser Internet Explorer, le funzionalità sulle quali possono agire dipendono dal ruolo che possiedono.

Il presente traguardo di sicurezza è costituito dai seguenti capitoli:

1. **Introduzione del TDS:** questo capitolo fornisce un'identificazione univoca ed una visione di insieme di questo traguardo di sicurezza.

2. **Descrizione dell'ODV:** questo capitolo fornisce una sintetica rappresentazione dell'ODV e ne descrive i confini logici e fisici.

3. **Ambiente di sicurezza dell'ODV:** questo capitolo descrive le ipotesi, le minacce e le politiche di sicurezza dell'organizzazione che riguardano l'ODV e l'ambiente nel quale è previsto il suo utilizzo.

4. **Obiettivi di sicurezza:** questo capitolo descrive gli obiettivi di sicurezza necessari per contrastare le minacce individuate e supportare le ipotesi e le politiche di sicurezza dell'organizzazione.

5. **Requisiti di sicurezza IT:** questo capitolo fornisce un insieme di requisiti funzionali di sicurezza che devono essere soddisfatti dall'ODV e dall'ambiente IT ed un insieme di requisiti di garanzia per l'ODV.

6. **Specifiche sommarie dell'ODV:** questo capitolo descrive le funzioni di sicurezza dell'ODV.

7. **Dichiarazione di conformità ad uno o più PP:** questo capitolo identifica i profili di protezione a cui è conforme questo traguardo di sicurezza.

8. **Motivazioni dell'ODV:** questo capitolo fornisce la corrispondenza, insieme alle motivazioni, tra l'ambiente di sicurezza, gli obiettivi di sicurezza, i requisiti di sicurezza e le funzioni di sicurezza, per stimare la loro completezza, consistenza e idoneità.

1.3. Conformità ai Common Criteria

Il presente Traguardo di Sicurezza è conforme con estensione ai [CCP2] per quanto riguarda i requisiti funzionali; è conforme ai [CCP3] per quanto riguarda i requisiti di garanzia rispettando quanto indicato per EAL4.
La struttura del presente Traguardo di Sicurezza è in accordo con quanto indicato in [CCP1].

2. Descrizione dell'ODV

2.1. Tipo di prodotto

L'ODV, denominato Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 2.33, è 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 alle aree riservate, e per controllare le funzionalità per la gestione dei dati delle funzioni di sicurezza dell'ODV stesso.

2.2. Infrastruttura gestita dall'ODV

L'infrastruttura 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.
Il terminale orologio è fornito di un display, un lettore di smart card e un rilevatore di impronte digitali.

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 (l'ID) della smart card è presente nella lista di controllo degli accessi (ACL), che il terminale orologio stesso possiede al proprio interno.

L'ODV permette di raggruppare, in modo logico, i terminali orologio in sottoinsiemi denominati varchi.
Un varco è costituito da uno o più terminali orologio che condividono una stessa lista di controllo degli accessi (ACL).
Varchi diversi sono caratterizzati dai differenti terminali che li compongono e dalle diverse ACL che possiedono.

In Figura 1 si descrive un'ipotesi di possibilità di accesso del possessore di una smart card in base a quanto appena esposto.

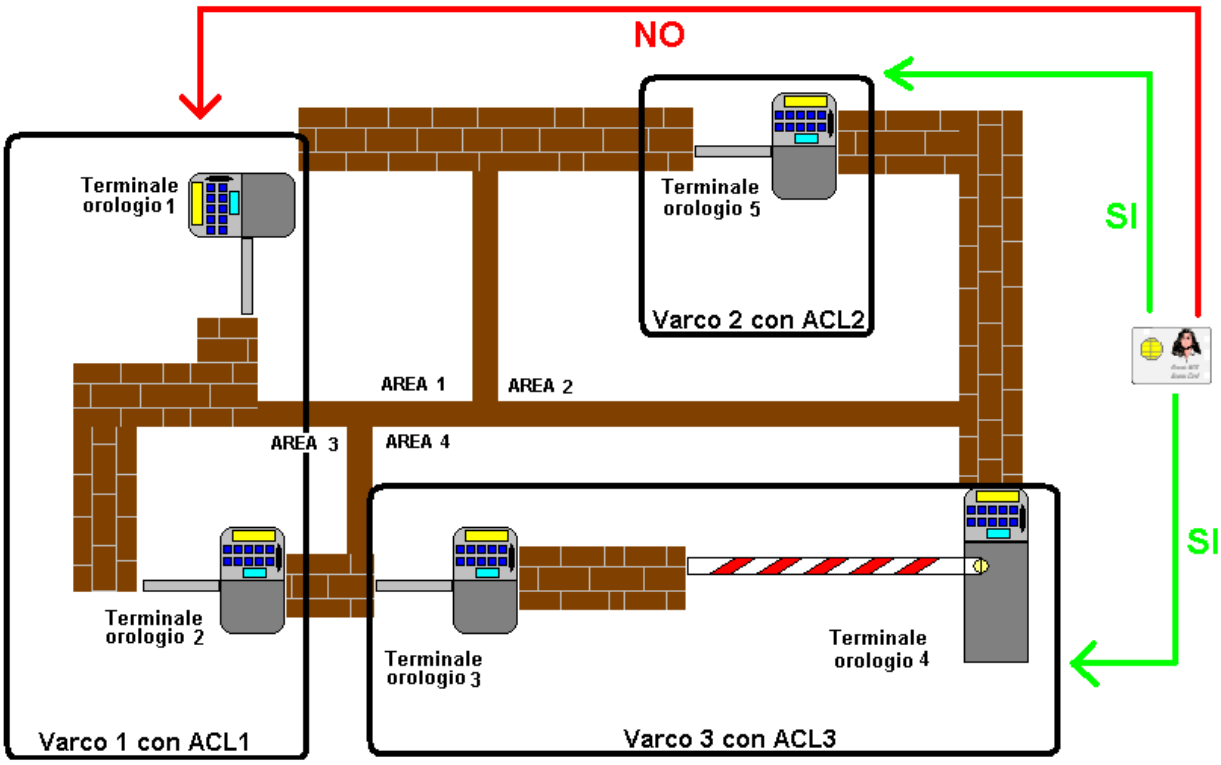

Figura 1 – Esempio di discriminazione degli accessi

L'ID della smart card è presente nella ACL del varco 2 e del varco 3. Il possessore della smart card può pertanto attraversare i tornelli associati ai terminali orologio 3, 4 e 5 che compongono i suddetti varchi. Invece l'accesso non è consentito attraverso i tornelli associati con i terminali orologio 1 e 2 poiché l'ID della smart card è assente nella ACL del varco 1.

2.3. Funzionalità dell'ODV

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.
L'accesso è subordinato ad una politica di controllo 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.

I ruoli utente previsti dall'ODV sono:

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

Le funzionalità dell'ODV per la gestione dell'infrastruttura sono:

- Gestione varchi. Il software permette di eliminare varchi esistenti o di crearne di nuovi; di modificare l'insieme dei terminali orologio che formano il varco; di aggiungere automaticamente l'ID di una CMD o di un badge temporaneo all'ACL

del varco, nel momento della loro assegnazione ad un dipendente o visitatore; di visualizzare tutte le smart card contenute nell'ACL.

- Gestione ACL. Il software permette di ricercare una smart card, con diversi criteri, per verificare in quali ACL è presente il suo ID; aggiungere o eliminare l'ID di una smart card nell'ACL associata ad un varco.

- Gestione dei pass temporanei (giornalieri o per un periodo di tempo definito). Il software permette di assegnare ad un visitatore, dopo aver acquisito tutti i dati necessari, una smart card (badge temporaneo) con validità limitata nel tempo (un giorno o un tempo superiore, comunque determinato e in quest'ultimo caso l'operazione deve essere autorizzata dall'utente che può accedere alla funzionalità "Gestione autorizzazioni"), permettendone l'accesso ad uno o più varchi definiti in fase di assegnazione; registrare le smart card riconsegnate e quelle eventualmente smarrite; ricercare i badge non riconsegnati; ricercare le informazioni relative al badge temporaneo assegnato (identità assegnatario, motivo visita, ecc…).

- Acquisizione delle CMD. Il software permette di acquisire la smart card (CMD) di un militare o dipendente civile, dopo aver acquisito tutti i dati necessari, permettendone l'accesso ad uno o più varchi definiti in fase di assegnazione.

- 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, con diversi criteri, 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 di un pass temporaneo ad un visitatore.

Le funzionalità per la ricerca nel file di log sono:

- Ricerca nel file di Log. Il software permette di ricercare, con diversi criteri, nel file di Log gli eventi rilevanti per la sicurezza.

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

- Gestione dei ruoli degli utenti dell'ODV. Il software permette di assegnare al possessore di una CMD uno dei ruoli previsti come utente dell'ODV, abilitandolo a gestire le informazioni e le funzionalità dell'ODV assegnate a tale ruolo; revocare o modificare il ruolo associato ad un utente.

2.4. Confini dell'ODV

L'ODV è una 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 (in seguito genericamente indicati come dati dell'ODV se non diversamente specificato) sono contenute nel Database di controllo accessi.

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.

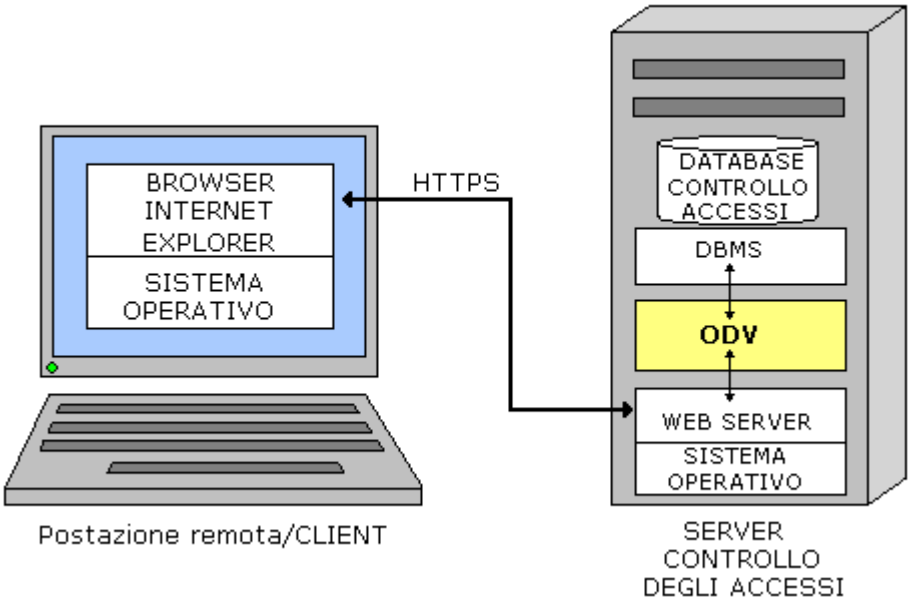

Figura 2 – Confini dell'ODV

L'ODV include solamente l'applicazione web che fornisce le interfacce utente attraverso il web browser della postazione remota.

L'ODV non include:

- alcun software o hardware della postazione remota;
- il sistema operativo e l'hardware sul quale è installato;
- il web server che permette lo scambio dei dati con la postazione remota;
- il database relazionale e il DBMS attraverso il quale comunica con l'ODV;
- i servizi applicativi e i servizi web installati sul server di controllo degli accessi e utilizzati dall'ODV (vedasi la sezione 2.5);
- alcun software o hardware, oltre quelli già menzionati, collegati alla rete, (vedasi la sezione 2.5).

Si noti come nella configurazione di valutazione l'ODV e il database di controllo degli accessi sono installati sulla stessa macchina.

2.5. Ambiente IT dell'ODV

La Figura 3 descrive la rete intranet senza alcun accesso all'esterno, utilizzata dall'infrastruttura, dall'ambiente IT e dall'ODV nella configurazione di valutazione.

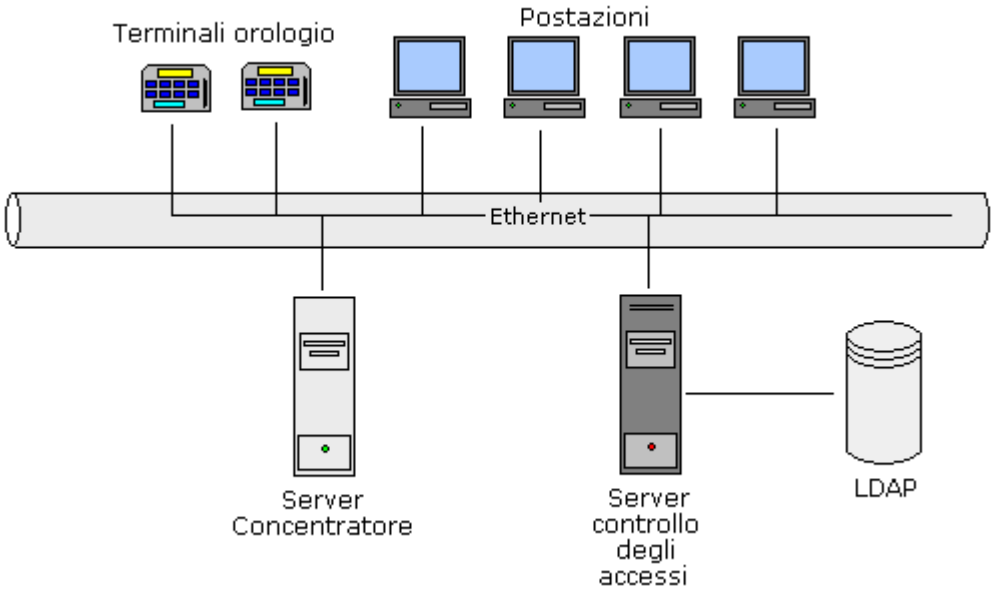

Figura 3 – Infrastruttura di rete e ODV

Alla rete intranet realizzata attraverso una rete Ethernet sono connessi:

- i terminali orologio;
- il server concentratore utilizzato per:
  - raccogliere le informazioni provenienti dai terminali orologio e registrarle nel Database di controllo degli accessi in una tabella separata da quelle gestite dall'ODV;
  - aggiornare le ACL che tali terminali contengono quando gli utenti dell'ODV effettuano qualche variazione.
- il server di controllo degli accessi, su cui è installato
  - il sistema operativo Microsoft Windows 2003 Server R2 SP2;
  - l'applicazione web che costituisce l'ODV;
  - il DBMS Microsoft SQL Server 2000 per la gestione del database di controllo degli accessi;
  - il web server Microsoft Windows IIS ver. 6.0;
  - Microsoft .NET Framework 1.1 SP1;
  - il servizio applicativo per le timbrature ed il controllo dello stato delle CMD e il servizio web per il Secure Messaging remoto.

  i requisiti minimi hardware della configurazione di valutazione del server di controllo accessi sono:
  - RAM di 1GB;
  - scheda di rete Ethernet;
- il server LDAP nel quale è presente la lista dei certificati digitali, registrati nelle CMD, che sono stati revocati;

- le postazioni remote costituite ognuna da:

  - un monitor;
  - una tastiera;
  - un mouse;
  - un lettore di smart card Siemens CardOS M4.01/A o compatibile per identificare e autenticare l'utente che accede all'ODV;
  - un computer.

  I requisiti minimi hardware della configurazione di valutazione delle postazioni remote sono:

  - RAM 512MB;
  - scheda di rete Ethernet.

sulle quale è installato:

- il Sistema Operativo Windows XP;
- il web browser (Microsoft Internet Explorer ver. 6.0);
- la libreria software CardOS API (Siemens CardOS API v. 2.4);
- l'ActiveX "SmartCardControl" per il controllo della smart card;
- Framework .net Siemens 1.1;
- .net Card Control;
- driver lettore di smart card;
- Adobe Reader 9.0.

In aggiunta nelle postazioni remote predisposte alle funzioni specifiche dei ruoli di Amministratore, Acquisitore CMD e Ufficio Pass deve esserci:

- un ulteriore lettore smart card Siemens CardOS M4.01/A (o compatibile) per le operazioni di gestione (ricerca, assegnazione ecc…) delle smart card sia degli utenti dell'ODV sia di coloro che devono accedere attraverso i varchi;
- un lettore di impronte digitali, per l'acquisizione di tale dato biometrico in fase di assegnazione pass temporaneo;

Sui computer di tali postazioni devono essere installati i driver di gestione del lettore di impronte digitali.

Hardware per l'autenticazione fornito agli utenti:

- Smart card Siemens 32k.

2.6. Identificazione, autenticazione e accesso degli utenti all'ODV

L'utente interagisce con l'ODV attraverso una delle postazioni remote descritte nelle sezioni 2.4 e 2.5.

Per accedere all'ODV, l'utente deve essere in possesso di una CMD, inserirla nel lettore di smart card per l'identificazione e l'autenticazione, collegato alla postazione remota, e digitare l'indirizzo che l'Amministratore dell'ambiente IT ha stabilito, nella barra degli indirizzi del browser Internet Explorer.

In ogni CMD è registrata la chiave privata di autenticazione con il corrispondente certificato digitale in formato X.509 v3 (contenente la chiave pubblica) che permette al server di controllo degli accessi, in possesso del certificato pubblico della Certification Authority (CA), che ha rilasciato il certificato contenuto nella smart card, di verificare l'identità del possessore della smart card che vuole stabilire la connessione.

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.

Si attiva infatti la libreria software CardOS API che gestisce la trasmissione dei certificati tra la smart card ed Internet Explorer. Quest' ultimo chiede, tramite un'interfaccia grafica, di selezionare il certificato registrato nel proprio repository, idoneo all'autenticazione; di seguito la libreria CardOS API chiede di inserire il PIN per sbloccare la chiave privata del certificato. Se il valore impostato è corretto Internet Explorer può instaurare una connessione con il web server utilizzando il protocollo SSL, che provvede all'identificazione e all'autenticazione.

Il web server, terminata la procedura di autenticazione, trasmette il certificato dell'utente all'ODV che ne calcola il valore hash SHA-1 e cerca nella tabella che contiene i certificati quello che genera la stessa "impronta" digitale. Trovata la corrispondenza verifica se nella stessa tabella precedente è associato al certificato uno degli identificativi del ruolo, in caso affermativo permette all'utente di accedere all'ODV con le funzionalità abilitate al suo ruolo.

Si noti come sia importante utilizzare, per l'emissione dei certificati, una CA che garantisca il rilascio dei certificati pubblici con uno scrupoloso controllo dell'identità del soggetto, altrimenti si abbassa sensibilmente il livello di sicurezza dell'intero processo di identificazione e autenticazione affidato all'ambiente IT.

Dalla descrizione precedente si evince, pertanto, che l'identificazione e l'autenticazione degli utenti è demandata all'ambiente IT che interagisce con l'ODV, mentre quest'ultimo si limita a identificare l'utente, verificando se possiede uno dei ruoli previsti.

2.7. Funzioni di sicurezza

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.

3. Ambiente di sicurezza dell'ODV

Lo scopo di questo paragrafo è quello di fornire una definizione del contesto in cui si trova ad operare l'ODV ed in particolare di definire la natura e l'ambito delle esigenze di sicurezza che l'ODV deve soddisfare, ossia la definizione dell'ambiente in cui l'ODV verrà utilizzato ed il modo in cui sarà impiegato.

3.1. Ipotesi

3.1.1. Ipotesi sull'ambiente IT

A.Autenticazione – Autenticazione degli utenti
Si assume che l'ambiente IT garantisca la corretta identificazione e autenticazione degli utenti dell'ODV.

A.Controllo_Accessi – Accessi non autorizzati
Si assume che l'ambiente IT garantisca che non si possa accedere alle funzionalità di gestione dell'ODV se non attraverso le funzionalità messe a disposizione dall'ODV stesso.

A.Monitor – Controllo integrità dati
Si assume che l'ambiente IT controlli l'integrità dei dati registrati nelle tabelle contenute nel Database di controllo degli accessi.

A.Data_affidabile – Data e ora affidabile
Si assume che l'ambiente IT fornisca all'ODV una data e un'ora affidabile.

3.1.2. Ipotesi sull'ambiente fisico

A.Accesso_Fisico – Protezione fisica dell'hardware
Si assume che gli ambienti che ospitano l'hardware su cui è installato l'ODV siano fisicamente sicuri rispetto ad accessi di personale non autorizzato.

3.1.3. Ipotesi sugli Amministratori dell'ODV

A.Amministratori – Amministratori addestrati e fidati
Si assume che gli Amministratori siano adeguatamente addestrati al corretto utilizzo dell'ODV e scelti tra il personale fidato dell'organizzazione.

3.1.4. Ipotesi sugli Amministratori dell'ambiente IT

A.Amministratori_ambiente IT – Amministratori dell'ambiente IT
Si assume che gli Amministratori dell'ambiente IT siano scelti tra il personale fidato e addestrati al corretto utilizzo di tutti i dispositivi che compongono l'ambiente IT.

3.1.5. Ipotesi sugli utenti

A.utenti_ID – Certificato utenti
Si assume che l'autorità di certificazione abbia correttamente associato il certificato contenuto nella smart card posseduta dall'utente all'identità dello stesso.

3.2. Minacce

I beni che l'ODV deve proteggere sono:

- **I dati dell'ODV;**
- **le funzionalità dell'ODV per la gestione dell'infrastruttura e dei dati delle funzioni di sicurezza.**

T.Abuso – Accesso illegale
Un utente autorizzato, scalando i privilegi previsti dal proprio ruolo (intenzionalmente o accidentalmente), accede a dati o funzionalità dell'ODV per i quali non è autorizzato.

T.Accesso – Accesso persona non autorizzata
Una persona non autorizzata accede ai dati o alle funzionalità dell'ODV cercando di impersonare un utente autorizzato.

T.Integrità – Integrità dati dell'ODV
La mancanza di integrità dei dati dell'ODV, generata da una qualsiasi causa, potrebbe non essere rilevata dagli utenti dell'ODV inducendoli ad operare con dati non coerenti.

3.3. Politiche di sicurezza dell'organizzazione (PSO)

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

4. Obiettivi di sicurezza

4.1. Obiettivi di sicurezza dell'ODV

Questa sezione definisce gli obiettivi di sicurezza dell'ODV. Gli obiettivi di sicurezza stabiliscono il comportamento atteso dell'ODV nel contrastare le minacce e nel supportare le ipotesi e le eventuali politiche di sicurezza dell'organizzazione.

O.Accesso_ODV – Accesso dati e funzionalità
L'ODV deve permettere agli utenti autorizzati di accedere solamente ai dati e alle funzioni dell'ODV consentite dai loro ruoli.

O.Audit – Audit e Accountability
L'ODV deve memorizzare gli eventi rilevanti per la sicurezza comprese le eccezioni inviategli dall'ambiente IT e riguardanti l'integrità dei dati dell'ODV.

O.Blocco – Interruzione sessione
L'ODV deve interrompere la sessione di collegamento con la postazione remota dell'utente se sono trascorsi più di dieci minuti di inattività dell'utente stesso o se ha ricevuto un'eccezione dall'ambiente IT riguardante l'integrità dei dati dell'ODV.

O.IDutente – Identificazione utente
L'ODV deve permettere l'accesso alle proprie funzioni e ai propri dati solamente agli utenti correttamente identificati.

O.Gestione – Gestione funzioni sicurezza
L'ODV deve fornire le funzioni necessarie per permettere agli utenti autorizzati la gestione delle sue funzioni di sicurezza.

4.2. Obiettivi di sicurezza dell'ambiente

Questi obiettivi di sicurezza sono a carico dell'ambiente dell'ODV. Essi sono necessari come supporto agli obiettivi di sicurezza dell'ODV nel contrastare i problemi di sicurezza e nel supportare le ipotesi definite nell'ambiente di sicurezza dell'ODV.

4.2.1. Obiettivi di sicurezza dell'ambiente IT

OE.Protezione – Protezione logica
L'ambiente IT deve garantire che nessuno possa accedere all'ODV aggirando le sue funzioni di sicurezza.

OE.Autenticazione – Autenticazione utenti
L'ambiente IT deve identificare ed autenticare gli utenti dell'ODV.

OE.Errori – Integrità dati e notifica ODV
L'ambiente IT deve controllare l'integrità dei dati dell'ODV e notificare a quest'ultimo eventuali violazioni.

OE.Data_affidabile – Data e ora affidabile
L’ambiente IT deve garantire all’ODV un’ora e una data affidabili.

4.2.2. Obiettivi di sicurezza dell’ambiente non IT

OE.Amministratori – Amministratori
Gli Amministratori devono essere scelti tra il personale fidato e addestrati al corretto utilizzo dell’ODV.

OE.Ambiente_fisico – Protezione ambiente fisico
I responsabili dell’ODV assicurano che i dispositivi hardware sui quali è installato l’ODV, e che fanno parte dell’ambiente IT, sono custoditi in locali nei quali l’accesso è consentito solamente al personale autorizzato.

OE.Amministratori IT – Amministratori ambiente IT
Gli Amministratori dell’ambiente IT devono essere scelti tra il personale fidato e addestrati al corretto utilizzo di tutti i dispositivi che compongono l’ambiente IT.

OE.Certificati_utenti – Certificati utenti
I certificati registrati nelle smart card possedute dagli utenti devono essere associati correttamente alle identità degli utenti stessi.

5. Requisiti di sicurezza IT

5.1. Requisiti di sicurezza dell'ODV

Questa sezione contiene i requisiti di sicurezza che sono soddisfatti dall'ODV.
Il testo per le operazioni completate è messo in evidenza in grassetto.
Differenti iterazioni dello stesso requisito sono distinguibili da un numero fra parentesi tonde.

5.1.1. Requisiti funzionali dell'ODV

L'estensione di un requisito funzionale è riconoscibile dalla sostituzione dell'iniziale F con la lettera E.

Componente	Nome del Componente
EAU_GEN.1	Extended Audit Data Generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FCS_COP.1	Cryptographic Operation
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FIA_ATD.1	User attribute definition
FIA_UID.2 (1)	User identification before any action
FMT_MSA.1	Management of security attributes
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_RVM.1(1)	Non bypassability of the TSP
FTA_SSL.3	TSF-initiated termination
ETA_SSL.3	Extended TSF-initiated termination

Tabella 2 – Requisiti funzionali dell'ODV

EAU_GEN.1 Audit Data Generation
EAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) All auditable events for the **not specified** level of audit; and
b) The auditable events included in the following list:
   1. **Login**
   2. **Logout**
   3. **Failed login**
   4. **Automatic logout**
   5. **Temporary badge revocation**
   6. **Temporary badge restoration**
   7. **Exceptions sent by IT environment**

EAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definition of the functional components included in the ST:

Event	Information
Login	**Remote computer IP address**
Logout	**Remote computer IP address**
Failed login	**Remote computer IP address**
Automatic logout	**Automatic logout reason**
Temporary badge revocation	**Temporary badge ID number**
Temporary badge restoration	**Temporary badge ID number**
Exceptions sent by IT environment	**Remote computer IP address** **Error message**

Tabella 3 – Event / Information

Application note: This extended security functional requirement is directly modeled on [CCP2] SFR FAU_GEN.1 and reflects the fact that TOE functionality doesn't record Start-up and shutdown of the audit functions.

FAU_GEN.2 User identity association
FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review
FAU_SAR.1.1 The TSF shall provide **the Administrator** with the capability to read **all audit information within the Administrator's scope of control** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review
FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable audit review
FAU_SAR.3.1 The TSF shall provide the ability to perform **searches** of audit data based on **date or event criteria.**

FCS_COP.1 Cryptographic Operation
FCS_COP.1.1 The TSF shall perform **message digesting** in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes **[none]** that meet the following: **NIST FIPS PUB 180-1**

FDP_ACC.2 Complete access control
FDP_ACC.2.1 The TSF shall enforce the **role-based access policy** on the **subjects [all users] and objects [data concerning: passages, ACL passages, Cross passages, Presences, Logs, Roles, Temporary pass, Documents, CMD and Representatives]** 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.

FDP_ACF.1 Security attribute based access control
FDP_ACF.1.1 The TSF shall enforce the **role-based access policy** to objects based on the following:

Subjects with the following Capabilities	**Objects** **Data concerning:**	**Operations among subjects and objects**
Administrator	**Passages**	• Search • Create • Erase • Modify
	ACL passages	• Search • Add • Erase
	Cross passages	• Search
	Presences	• Search
	Logs	• Search • View information (except for exceptions sent by IT environment)
	Roles	• Search • Modify • Assign • Revoke
	Temporary pass	• Search • Assign • Record hand over • Check expired pass
	Documents	• Search • Add • Erase • Modify
	CMD	• Capture • Search • Modify data
	Representatives	• Search • Add • Erase

Pass Office	**Temporary pass**	• Search • Assign • Record hand over
Security Office	**Temporary pass**	• Clearances management
CMD enrolment user	**ACL passages**	• Search • Add • Erase
	CMD	• Capture

Tabella 4 – Role based access policy

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
subjects must have permissions assigned by their roles as listed in Tabella 4.

FDP_ACF.1.3 The TSF shall explicitly authorize 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 rules: **none**

FIA_ATD.1 User attribute definition
FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **Role**

FIA_UID.2 (1) User identification before any action
FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated action on behalf of that user.

FMT_MSA.1 Management of security attributes
FMT_MSA.1.1 The TSF shall enforce the **role-based access policy** to restrict the ability to **assign, modify, revoke and search** the security attributes
role assigned to users
to **Administrator.**

FMT_SMF.1 Specification of Management Functions
FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **subjects security attributes management.**

FMT_SMR.1 Security roles
FMT_SMR.1.1 The TSF shall maintain the roles:
- **Pass office**
- **Security office**
- **CMD enrolment user**
- **Administrator**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

FPT_RVM.1(1) Non-bypassability of the TSP
FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FTA_SSL.3 TSF-initiated termination
FTA_SSL.3.1 The TSF shall terminate an interactive session after **ten minutes of user inactivity.**

ETA_SSL.3 Extended TSF- initiated termination
ETA_SSL.3.1 The TSF shall terminate an interactive session after **receiving an exception from IT environment for TOE data integrity .**

Application note: This extended security functional requirement is directly modeled on [CCP2] SFR FTA_SSL.3 and reflects the fact that TOE functionality provides for terminating an interactive session immediately after receiving an exception from IT environment for TOE data integrity.

5.1.2. Requisiti di garanzia dell'ODV

I requisiti di garanzia per l'ODV comprendono i requisiti corrispondenti al livello di garanzia EAL4, come definito in [CCP3]. La Tabella che segue li riassume in termini di componenti di garanzia.

CLASSE DI GARANZIA	COMPONENTE DI GARANZIA	TITOLO DEL COMPONENTE
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start – up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high – level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low – level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life – cycle model
	ALC_TAT.1	Well – defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing high – level design

	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

Tabella 5 – Requisiti di Garanzia dell'ODV

Ulteriori informazioni in merito ai componenti di garanzia possono essere trovate in [CCP3].

5.2. Grado di robustezza minimo delle funzioni di sicurezza dell'ODV

Il grado di robustezza minimo dichiarato per le funzioni di sicurezza dell'ODV è "SOF-medium".

5.3. Requisiti di sicurezza per l'ambiente IT

Si elencano, nella tabella che segue, i requisiti per l'ambiente IT. Tutti i requisiti sono stati raffinati sostituendo la T in TSF con IT environment, dove necessario, per una migliore comprensione.

5.3.1. Requisiti funzionali dell'ambiente IT

Componente	Nome del Componente
FDP_SDI.2	Stored Data integrity monitoring and action
FIA_UAU.2	User authentication before any action
FIA_UID.2(2)	User identification before any action
FPT_RVM.1(2)	Non-bypassability of the TSP
FPT_SEP.3	Complete reference monitor
FPT_STM.1	Reliable time stamps
FTP_ITC.1	Inter-IT environment SF trusted channel

Tabella 6 – Requisiti funzionali dell'ambiente IT

FDP_SDI.2 Stored data integrity monitoring and action
FDP_SDI.2.1 The IT environment SF shall monitor user data integrity within TSC for **data integrity errors** on all objects based on the following attributes: **attributes defined in the DBMS[1].**

FDP_SDI.2.2 Upon detection of a data integrity error, the IT environment shall **send an exception to the TOE.**

[1]Per maggiori dettagli sull'integrità dei dati gestiti dal DBMS Microsoft SQL Server 2000 si veda il testo: "SQL Server 2000 Books online" e precisamente la sezione Data integrity del capitolo Creating and Maintaining Databases, raggiungibile all'indirizzo internet http://msdn2.microsoft.com/en-us/library/aa933058(SQL.80).aspx

FIA_UAU.2 User authentication before any action
FIA_UAU.2.1 The IT environment SF shall require each user to be successfully authenticated before allowing any other IT environment SF-mediated actions on behalf of that user.

FIA_UID.2 (2) User identification before any action
FIA_UID.2.1 The IT environment SF shall require each user to identify itself before allowing any other IT environment SF-mediated action on behalf of that user.

FPT_RVM.1 (2) Non-bypassability of the TSP
FPT_RVM.1.1 The IT environment SF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.3 Complete reference monitor
FPT_SEP.3.1 The unisolated portion of the IT environment SF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.3.2 The IT environment SF shall enforce separation between the security domains of subjects in the TSC.

FPT_SEP.3.3 The IT environment SF shall maintain the part of the IT environment SF that enforces the access control and/or information flow control SFPs in a security domain for its own execution that protects them from interference and tampering by the remainder of the IT environments SF and by subjects untrusted with respect to IT environment SP.

FPT_STM.1 Reliable time stamps
FPT_STM.1.1 The IT environment SF shall be able to provide reliable time stamps for its own use.

FTP_ITC.1 Inter-IT environment SF trusted channel
FTP_ITC.1.1 The IT environment SF shall provide a communication channel between itself and a remote trusted IT products that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The IT environment SF shall permit **the remote trusted IT product** to initiate communication via the trusted channel

FTP_ITC.1.3 The IT environment SF shall initiate communication via the trusted channel for **users identification and authentication.**

6. Specifiche sommarie dell'ODV

6.1. Funzioni di sicurezza dell'ODV

La sezione che segue descrive le funzioni di sicurezza dell'ODV.

6.1.1. Identificazione

L'identificazione da parte dell'ODV ha inizio dopo l'autenticazione eseguita dall'ambiente IT.
L'accesso all'ODV è permesso solamente dopo essere stati identificati come utenti autorizzati.
Per identificarsi l'utente deve mantenere inserita la propria smart card CMD nel lettore della postazione remota dalla quale intende connettersi all'ODV.

In ogni CMD è memorizzato un certificato digitale X.509 v3 idoneo per l'identificazione e autenticazione ad opera dell'ambiente IT.
Tutti i suddetti certificati di tutte le CMD assegnate sono registrati in una tabella contenuta nel Database di controllo degli accessi, dove sono associati all'identificativo dell'eventuale ruolo del possessore della CMD.

[ID1] L'ODV verifica se colui che tenta di stabilire una connessione con esso, possiede un ruolo. La verifica è condotta controllando nell' apposita tabella del database di controllo degli accessi se al certificato, avente lo stesso valore hash SHA – 1 del certificato della CMD, è associato un numero identificativo del ruolo. In caso affermativo l'ODV identifica il possessore della CMD come proprio utente.

[ID2] La non corretta identificazione impedisce qualunque accesso all'ODV, il quale risponderà al fallito tentativo con un messaggio di errore.

Questa funzione di sicurezza è implementata da un meccanismo permutazionale il cui grado di robustezza appropriato è indicato in "SOF – medium".

6.1.2. Controllo accessi

[AC1] L'ODV permette l'accesso alle tabelle del Database di controllo degli accessi ed alle proprie funzioni applicando a tutti gli utenti una politica di controllo accessi basata sul ruolo.
Per ogni ruolo sono definite le funzioni e i dati dell'ODV a cui può accedere.
I ruoli previsti sono:

1. Ufficio Pass
2. Ufficio Sicurezza
3. Acquisitore CMD

4. Amministratore.

[AC2] L'ODV permette, solamente agli utenti con ruolo di Amministratore, di:

- assegnare un ruolo ad un nuovo utente;
- modificare il ruolo assegnato ad un utente;
- revocare qualsiasi ruolo ad un utente, negandogli ogni possibilità di accesso all'ODV;
- cercare gli utenti che possiedono un ruolo.

[AC3] L'ODV termina la sessione di collegamento con la postazione remota dell'utente nel caso in cui quest'ultimo rimanga inattivo per più di dieci minuti oppure se ha ricevuto dall'ambiente IT, una notifica di eccezione riguardante l'integrità dei dati contenuti nel Database di controllo accessi.

6.1.3. Audit e Accountability

L'ODV implementa una funzione di audit e accounting che registra gli eventi attinenti alla sicurezza in un file. Tale funzione è sempre abilitata, non è ammesso ad alcun ruolo la possibilità di escluderla.

[AUD1] L'ODV registra in una tabella del Database di Controllo degli accessi le azioni rilevanti per la sicurezza. Queste azioni sono:

- Login
- Logout
- Login fallito
- Logout automatico
- Revoca badge temporaneo
- Riabilitazione badge temporaneo

L'ODV registra in un file sul server di controllo degli accessi, le eccezioni inviate dall'ambiente IT.

[AUD2] Ogni azione registrata è legata all'identità dell'utente che l'ha generata attraverso l'ID della sua smart card, in aggiunta per le azioni

- Login
- Logout
- Login fallito

è registrato l'indirizzo IP del terminale dal quale l'utente ha compiuto l'azione, per l' azione

- Logout automatico

è registrato il motivo che ha generato l'evento, ed infine per le azioni

- Revoca badge temporaneo
- Riabilitazione badge temporaneo

è registrato il numero seriale del badge temporaneo revocato o riabilitato

- per le eccezioni inviate dall'ambiente IT

è registrato l'indirizzo IP del terminale dell'utente che ha compiuto l'azione che ha generato un'eccezione dell'ambiente IT e il messaggio di errore.

[AUD3] Ad ogni azione è legata una data ed un'ora affidabile.

[AUD4] L'ODV presenta i file di audit in maniera chiara e leggibile.

[AUD5] L'ODV permette la lettura del file di audit che registra

- Login
- Logout
- Login fallito
- Logout automatico
- Revoca badge temporaneo
- Riabilitazione badge temporaneo

solamente agli utenti con il ruolo di Amministratore, proibendone l'accesso a qualunque altro utente.
L'accesso al file che registra le eccezioni dell'ambiente IT non è consentito ad alcun utente dell'ODV[2].

[AUD6] L'ODV permette la ricerca degli eventi all'interno del file di audit utilizzando come criterio la data o la tipologia dell'evento stesso.

6.2. Misure di garanzia

Non sono richieste misure di garanzia oltre quelle fornite dalla documentazione prevista dai requisiti di garanzia contenuti in EAL4.

[2]L'accesso al file che registra le eccezioni dell'ambiente IT è consentito solamente all'Amministratore dell'ambiente IT.

7. Dichiarazione di conformità ad uno o più PP

Il presente Traguardo di Sicurezza non è conforme ad alcun Profilo di Protezione.

8. Motivazioni dell'ODV

8.1. Motivazioni degli obiettivi di sicurezza

Questa sezione dimostra che ogni obiettivo di sicurezza contrasta almeno una minaccia o sostiene un'ipotesi, e che ogni minaccia o ipotesi è associata ad almeno un obiettivo di sicurezza.

Minacce e Ipotesi	Obiettivi
T.Abuso	O.Accesso_ODV, O.Audit, O.Gestione, OE.Certificati_utenti
T.Accesso	O.IDutente, OE.Autenticazione OE.Certificati_utenti, O.Blocco
T.Integrità	O.Blocco, O.Audit
A.Autenticazione	OE.Autenticazione OE.Certificati_utenti
A.Controllo_Accessi	OE.Protezione
A.Monitor	OE.Errori
A.Data_affidabile	OE.Data_affidabile, OE.Amministratori IT
A.Accesso_Fisico	OE.Ambiente_fisico
A.Amministratori	OE.Amministratori
A.Amministratori_ambiente IT	OE.Amministratori IT
A.utenti_ID	OE.Certificati_utenti

Tabella 7 – Corrispondenza Obiettivi – Minacce / Ipotesi

T.Abuso – Accesso illegale
O.Accesso_ODV contrasta la minaccia di accesso illegale in quanto tale obiettivo prevede esplicitamente che ad ogni utente sia permesso di accedere solamente ai dati e alle funzioni consentite dal proprio ruolo. Tale obiettivo è coadiuvato da O.Audit, poiché registrare le azioni degli utenti è un deterrente per ogni comportamento non autorizzato, e da O.Gestione che permette agli Amministratori di assegnare i ruoli corretti e verificare il comportamento di ogni utente attraverso l'esame dei dati di audit. Anche l'obiettivo per l'ambiente IT OE.Certificati_utenti contribuisce a contrastare la minaccia in quanto

prevede la corretta associazione tra il certificato registrato nella smart card dell'utente e l'identità dello stesso.

T.Accesso – Accesso persona non autorizzata
O.IDutente contrasta la minaccia di accesso da parte di persone non autorizzate, in quanto l'obiettivo prevede che qualunque accesso all'ODV sia subordinato all'identificazione dell'utente. Tale obiettivo è coadiuvato in modo importante da OE.Autenticazione in quanto, come già descritto, una prima identificazione e soprattutto l'autenticazione di chi tenta di accedere è demandata all'ambiente IT e da OE.Certificati_utenti che prevede la corretta associazione tra il certificato registrato nella smart card dell'utente e l'identità dello stesso, garantendo la corretta implementazione del meccanismo di identificazione dell'utente eseguita dall'ODV. Anche l'obiettivo O.Blocco contribuisce a contrastare la minaccia, poiché prevede l'interruzione della sessione di collegamento tra la postazione remota dell'utente e l'ODV dopo dieci minuti di inattività, evitando che la sessione di collegamento, in un periodo di temporanea assenza dell'utente dalla postazione, possa essere sfruttata da persone non autorizzate, consentendo loro di ottenere l'accesso all'ODV.

T.Integrità – Integrità dati dell'ODV
O.Blocco contrasta la minaccia del non rilevamento da parte degli utenti della mancanza di integrità dei dati, poiché prevede che la sessione di collegamento tra l'ODV e la postazione remota dell'utente, si interrompa qualora il primo riceva un'eccezione dall'ambiente IT che segnala un errore di integrità dei dati, consentendo all'utente di avere evidenza dell'evento ed evitando che continui ad operare con dati corrotti. L'obiettivo è coadiuvato da O.Audit che registra le eccezioni, riguardanti l'integrità dei dati, inviate dall'ambiente IT.

A.Autenticazione – Autenticazione degli utenti
L'ODV non prevede l'autenticazione degli utenti, ma questa fondamentale funzione di sicurezza è demandata all'ambiente IT, come specificato in OE.Autenticazione che pertanto sostiene questa ipotesi. OE.Certificati_utenti contribuisce a sostenere l'ipotesi poiché prevede la corretta associazione tra il certificato registrato nella smart card dell'utente e l'identità dello stesso garantendo la correttezza del meccanismo di autenticazione dell'ambiente IT.

A.Controllo_Accessi – Accessi non autorizzati
E' necessario che l'hardware e il software dell'ambiente IT non permettano in alcun modo che si possa accedere ai dati gestiti dall'ODV se non attraverso le procedure previste dall'ODV stesso. OE.Protezione prevede tale funzionalità sostenendo l'ipotesi.

A.Monitor – Controllo integrità dati
L'ODV non ha alcuna funzionalità per il controllo dell'integrità dei propri dati, pertanto questa ipotesi è supportata dall'obiettivo dell'ambiente IT OE.Errori che prevede tale controllo e la notifica delle violazioni d'integrità all'ODV.

A.Data_affidabile – Data e ora affidabile
L'ODV non ha funzionalità per garantirsi una data e un'ora affidabile, pertanto questa funzione gli è fornita dall'ambiente IT, come previsto da OE.Data_affidabile, che sostiene l'ipotesi. L'obiettivo OE.Amministratori IT contribuisce a sostenere l'ipotesi in quanto è compito degli Amministratori dell'Ambiente IT assicurarsi che il meccanismo che

garantisce l'ora affidabile sia perfettamente funzionante attraverso gli strumenti messi a disposizione dell'ambiente IT stesso.

A.Accesso_Fisico – Protezione fisica dell'hardware
L'ODV non ha alcuna funzionalità di sicurezza che assicuri la protezione fisica dell'hardware su cui è installato. OE.Ambiente_fisico prevede che l'hardware sia custodito in locali protetti nei quali non è consentito ad alcuno di accedere se non esplicitamente autorizzato dall'organizzazione, pertanto tale obiettivo sostiene l'ipotesi A.Accesso_Fisico.

A.Amministratori – Amministratori addestrati e fidati
Gli Amministratori potrebbero compiere delle azioni che pongono l'ODV in uno stato non sicuro, assegnando ad esempio un ruolo sbagliato ad un utente. Inoltre gli Amministratori hanno accesso alle informazioni contenute nel file di audit. Per questi motivi è necessario che siano adeguatamente addestrati e siano selezionati tra il personale fidato come previsto da OE.Amministratori che pertanto sostiene l'ipotesi.

A.Amministratori_ambiente.IT – Amministratori dell'ambiente IT
Gli Amministratori dell'ambiente IT hanno la responsabilità del corretto funzionamento dei dispositivi che compongono l'ambiente IT, a cui sono demandate importanti funzioni di sicurezza come descritto nella sezione 5.3. Per questo motivo è necessario che siano adeguatamente addestrati al corretto utilizzo di tutti i dispositivi che compongono l'ambiente IT e selezionati tra il personale fidato, come previsto da OE.Amministratori IT che pertanto sostiene l'ipotesi.

A.utenti_ID – Certificato utenti
Per il corretto funzionamento della funzione di identificazione e autenticazione demandata all'ambiente IT e dell'identificazione ad opera dell'ODV dell'utente, è importante che l'identità di quest'ultimo sia correttamente associata al certificato della smart card che possiede. L'obiettivo OE.Certificati_utente prevede proprio che i certificati registrati nelle smart card possedute dagli utenti, siano associati correttamente alle identità degli stessi e pertanto sostiene l'ipotesi.

8.2. Motivazione dei requisiti di sicurezza

In questa sezione si dimostra come i requisiti di sicurezza per l'ODV e per l'ambiente IT sono necessari e sufficienti a contrastare ognuno degli obiettivi di sicurezza dell'ODV e dell'ambiente IT individuati nel capitolo 4.

8.2.1. Motivazioni dei requisiti funzionali dell'ODV

Questa sezione descrive i motivi per cui sono necessari e sufficienti i requisiti funzionali di sicurezza dell'ODV individuati in 5.1.1, dimostrando che ognuno di essi è indirizzato al soddisfacimento di almeno un obiettivo di sicurezza dell'ODV, e che ognuno degli obiettivi di sicurezza dell'ODV è soddisfatto da almeno un requisito funzionale di sicurezza dell'ODV.

La Tabella 8 che segue illustra quanto appena esposto.

Obiettivi	Requisiti
O.Audit	EAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU.SAR.2, FAU_SAR.3
O.Blocco	FTA_SSL.3, ETA_SSL.3
O.IDutente	FIA.UID.2(1), FCS_COP.1, FTA_SSL.3, FIA_ATD.1, FPT_RVM.1(1)
O.Accesso_ODV	FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FIA_ATD.1, FPT_RVM.1(1), FMT_SMR.1, FTA_SSL.3.
O.Gestione	FMT_MSA.1, FDP_ACF.1, FMT_SMF.1, FMT_SMR.1,FAU_SAR.1, FAU.SAR.2, FAU_SAR.3.

Tabella 8 – Corrispondenza Requisiti funzionali ODV – Obiettivi

O.Audit – Audit e Accountability
L'obiettivo richiede che l'ODV memorizzi gli eventi rilevanti per la sicurezza e le eccezioni inviategli dall'ambiente IT riguardanti l'integrità dei dati dell'ODV.

Questo obiettivo è soddisfatto da:

- EAU_GEN.1, FAU_GEN.2 che definiscono quali eventi sono registrati nel file di audit e stabiliscono che ad ogni evento sia associata l'identità dell'utente che lo ha generato.
  Il requisito funzionale EAU_GEN.1 è un requisito esteso modellato sul requisito funzionale FAU_GEN.1 dal quale è stato eliminato il punto a) dal suo elemento FAU_GEN.1.1 per riflettere il fatto che l'ODV non registra l'avvio e la chiusura della funzione di sicurezza di audit e accountability. Poiché questa è l'unica modifica che giustifica l'introduzione del requisito esteso i requisiti di garanzia previsti per il livello EAL4 risultano applicabili e appropriati per supportarlo.
- FAU_SAR.1, FAU_SAR.2 e FAU_SAR.3 che garantiscono agli Amministratori, e solamente a loro, la possibilità di leggere e cercare le informazioni contenute nel file di audit;

O.Blocco – Blocco accesso ODV
L'obiettivo dichiara che l'ODV deve interrompere la sessione di collegamento con la postazione remota dell'utente se sono trascorsi più di dieci minuti di inattività dell'utente stesso o se ha ricevuto un'eccezione dall'ambiente IT riguardante l'integrità dei suoi dati.
Questo obiettivo è soddisfatto da:

- FTA_SSL.3 che prevede che la sessione di collegamento tra la postazione remota dell'utente e l'ODV sia interrotta nel caso in cui siano trascorsi più di dieci minuti di inattività dell'utente nella sua postazione remota.
- ETA_SSL.3 che prevede che la sessione di collegamento tra la postazione remota dell'utente e l'ODV sia interrotta nel caso in cui l'ODV abbia ricevuto un'eccezione dall'ambiente IT riguardante l'integrità dei suoi dati.
  Questo requisito funzionale esteso è stato modellato sul requisito FTA_SSL.3 per tenere conto del fatto che l'ODV termina la sessione interattiva con la postazione remota dell'utente, se riceve un'eccezione dall'ambiente IT riguardante l'integrità

dei dati dell'ODV stesso. Rispetto al requisito FTA_SSL.3 è stata modificata l'operazione di assegnazione sostituendo il tempo di inattività dell'utente con l'invio da parte dell'ambiente IT di un'eccezione riguardante l'integrità dei dati dell'ODV. Poiché questa è l'unica modifica che giustifica l'introduzione del requisito esteso i requisiti di garanzia previsti per il livello EAL4 risultano applicabili e appropriati per supportarlo.

O.IDutente – Identificazione utente
L'obiettivo dichiara che l'ODV deve permettere l'accesso alle proprie funzionalità e ai propri dati solamente agli utenti correttamente identificati.

Questo obiettivo è soddisfatto da:

- FIA_UID.2(1) che richiede che ogni utente sia identificato prima di poter compiere qualunque azione sull'ODV;
- FCS_COP.1 che prevede l'utilizzo dell'algoritmo SHA – 1 per l'identificazione;
- FTA_SSL.3 che garantisce la terminazione di una sessione dopo 10 minuti di inattività prevenendo l'utilizzo dell'ODV da parte di utenti che non sono stati identificati;
- FIA_ATD.1 che prevede l'esistenza di una lista che associa ad ogni utente il certificato digitale contenuto nella sua CMD e l'identificativo del ruolo; tale lista è utilizzata dalla funzione di identificazione;
- FPT_RVM(1) che assicura che non si possa aggirare in alcun modo la fase di identificazione dell'utente.

O.Accesso_ODV – Accesso dati e funzionalità
L'obiettivo richiede che l'ODV permetta agli utenti autorizzati di accedere solamente ai dati e alle funzioni dell'ODV definiti dai loro ruoli.

Questo obiettivo è soddisfatto da:

- FDP_ACC.2, che garantisce l'esistenza di una politica di controllo degli accessi basata sul ruolo per ogni operazione che l'ODV può compiere, definendo i soggetti e gli oggetti sotto il controllo di tale politica;
- FDP_ACF.1, che stabilisce quali sono gli attributi di sicurezza e le regole che governano le operazioni e permettono l'accesso dei soggetti agli oggetti;
- FMT_SMR.1, che definisce tutti i ruoli che possono possedere gli utenti;
- FMT_MSA.1, la quale assicura che, definiti i ruoli, questi non possono essere cambiati se non dall'Amministratore;
- FIA_ATD.1, che prevede l'esistenza di una lista che associa ad ogni utente il certificato digitale contenuto nella sua CMD e l'identificativo del ruolo;
- FPT_RVM.1(1), che assicura che non si possa aggirare in alcun modo la politica di controllo degli accessi;
- FTA_SSL.3, che garantisce la terminazione di una sessione dopo 10 minuti di inattività, prevenendo l'eventualità che altri utenti possano utilizzare l'ODV sfruttando la sessione aperta da un utente autorizzato.

O.Gestione - Gestione funzioni sicurezza
L'obiettivo stabilisce che l'ODV fornisca agli utenti autorizzati le funzioni necessarie alla gestione delle sue funzioni di sicurezza.

Questo obiettivo è soddisfatto da:

- FDP_ACF.1, che specifica la politica di controllo accessi basata sul ruolo;
- FMT_MSA.1, che assicura che tale politica è applicata anche agli Amministratori per restringere ad essi la possibilità di assegnare, modificare o revocare qualunque ruolo ad un utente;
- FMT_SMF.1, che specifica la possibilità delle funzioni di sicurezza di gestire gli attributi di sicurezza degli utenti;
- FMT_SMR.1, che definisce tutti i ruoli che possono possedere gli utenti;
- FAU_SAR.1, FAU_SAR.2 e FAU_SAR.3 che garantiscono agli Amministratori, e solamente a loro, la possibilità di leggere e cercare le informazioni contenute nel file di audit.

8.2.2. Motivazioni dei requisiti funzionali dell'ambiente IT

Questa sezione descrive i motivi per cui sono necessari e sufficienti i requisiti funzionali di sicurezza dell'ambiente IT individuati in 5.3.1, dimostrando che ognuno di essi è indirizzato al soddisfacimento di almeno un obiettivo di sicurezza dell'ambiente IT, e che ognuno degli obiettivi di sicurezza dell'ambiente IT è soddisfatto da almeno un requisito funzionale di sicurezza dell'ambiente IT.

La Tabella 9 che segue illustra quanto appena esposto.

Obiettivo ambiente IT	Requisiti
OE.Protezione	FPT_RVM.1(2), FPT_SEP.3
OE.Autenticazione	FIA_UAU.2, FIA_UID.2(2), FTP_ITC.1
OE.Errori	FDP_SDI.2
OE.Data_affidabile	FPT_STM.1

Tabella 9 – Corrispondenza Requisiti funzionali ambiente IT – Obiettivi

OE.Protezione – Protezione logica
L'obiettivo dichiara che l'hardware e il software che costituiscono l'ambiente IT devono garantire che nessuno possa accedere all'ODV aggirando le sue funzioni di sicurezza.

Questo obiettivo è soddisfatto da:

- FPT_RVM.1(2) e FPT_SEP.3 i quali insieme costituiscono il sottosistema, definito reference monitor, che deve possedere l'ambiente IT. Tale sottosistema assicura che le politiche funzionali di sicurezza siano "invocate" ad ogni tentativo di accesso all'ODV e non possano essere in alcun modo aggirate.

OE.Autenticazione – Autenticazione utenti
L'obiettivo dichiara che l'ambiente IT deve identificare ed autenticare gli utenti dell'ODV.

Questo obiettivo è soddisfatto da:

- FIA_UID.2(2), che garantisce che l'ambiente IT esegua l'identificazione degli utenti prima di ogni altra azione;
- FIA_UAU.2, che garantisce che l'ambiente IT esegua l'autenticazione prima di ogni altra azione;

- FTP_ITC.1, che garantisce che l'ambiente IT instauri un canale fidato per stabilire una comunicazione sicura tra il browser IE ed il web server per l'identificazione e l'autenticazione degli utenti.

OE.Errori – Integrità dati e notifica ODV
L'obiettivo dichiara che l'ambiente IT deve controllare l'integrità dei dati registrati nelle tabelle contenute nel Database di controllo accessi e notificarne all'ODV eventuali violazioni.

Questo obiettivo è soddisfatto da:
- FDP_SDI.2, che prevede che l'ambiente IT controlli l'integrità dei dati utilizzati dall'utente e invii all'ODV un'eccezione in caso verificasse l'esistenza di errori.

OE.Data_affidabile – Data e ora affidabile
L'obiettivo dichiara che l'ambiente IT deve garantire all'ODV un'ora e una data affidabile.

Questo obiettivo è soddisfatto da:
- FPT_STM.1, che prevede che l'ambiente IT fornisca una data e un'ora affidabile all'ODV.

8.2.3. Motivazione dei requisiti di garanzia dell'ODV

L'ODV è stato progettato per gestire il controllo accessi agli ingressi di aree appartenenti ad organizzazioni che richiedono un livello di sicurezza stimabile in moderato/alto. Il livello di garanzia EAL4 appare pertanto adeguato.

8.2.4. Dipendenza dei requisiti funzionali di sicurezza

La tabella che segue fornisce un quadro dell'analisi delle dipendenze dei requisiti funzionali di sicurezza.
La dipendenza si considera soddisfatta anche se è stato inserito un componente gerarchicamente superiore. Può accadere pertanto che sia stato selezionato un componente che non corrisponde perfettamente a quello richiesto dai CC per soddisfare la dipendenza, ma uno gerarchicamente superiore.

Componente	Dipendenze	Dipendenze mancanti	Motivazioni
EAU_GEN.1	FPT_STM.1	FPT_STM.1	nota 1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	Nessuna	nota 2
FAU_SAR.1	FAU_GEN.1	Nessuna	nota 2
FAU_SAR.2	FAU_SAR.1	Nessuna	
FAU_SAR.3	FAU_SAR.1	Nessuna	
FCS_COP.1	FCS_CKM.1, FCS.CKM.4, FMT_MSA.2	FCS_CKM.1, FCS.CKM.4, FMT_MSA.2	nota 3

FDP_ACC.2	FDP_ACF.1	Nessuna	
FDP_ACF.1	FDP_ACC.2, FMT_MSA.3	FMT_MSA.3	nota 4
FIA_ATD.1	Nessuna	Nessuna	
FIA_UID.2(1)	Nessuna	Nessuna	
FMT_MSA.1	FDP_ACC.2, FMT_SMR.1, FMT_SMF.1	Nessuna	
FMT_SMF.1	Nessuna	Nessuna	
FMT_SMR.1	FIA_UID.1	Nessuna	
FPT_RVM.1(1)	Nessuna	Nessuna	
FTA_SSL.3	Nessuna	Nessuna	
ETA_SSL.3	Nessuna	Nessuna	nota 5

Tabella 10 – Dipendenza requisiti funzionali

Componente	Dipendenze	Dipendenze mancanti	Motivazioni
FDP_SDI.2	Nessuna	Nessuna	
FIA_UAU.2	FIA_UID.1	Nessuna	
FIA_UID.2(2)	Nessuna	Nessuna	
FPT_RVM.1(2)	Nessuna	Nessuna	
FPT_STM.1	Nessuna	Nessuna	
FPT_SEP.3	Nessuna	Nessuna	
FTP_ITC.1	Nessuna	Nessuna	

Tabella 11 – Dipendenza requisiti funzionali dell'ambiente IT

nota 1: EAU_GEN.1 è un componente funzionale esteso che deriva direttamente da FAU_GEN.1 avendo eliminato da questo componente solamente il punto elenco a). Risulta idoneo che la dipendenza di questo componente sia la stessa che per FAU_GEN.1 cioè FPT_STM.1. La dipendenza da questo requisito è soddisfatta tenendo conto che FPT_STM.1 è presente tra i requisiti dell'ambiente IT. La data e ora affidabile è fornita all'ODV dal sistema operativo Windows 2003 server sul quale è installato.

nota 2: La dipendenza può ritenersi implicitamente soddisfatta da EAU_GEN.1, in quanto il componente funzionale esteso deriva direttamente da FAU_GEN.1 avendo eliminato da questo componente solamente il punto elenco a).

nota 3: l'ODV prevede solamente l'utilizzo dello standard SHA-1 nel calcolo dell'hash dei certificati memorizzati nelle smart card degli utenti, non prevede né la generazione né la distruzione di chiavi segrete, non è pertanto necessario soddisfare la dipendenza da FCS_CKM.1, FCS_CKM.4 e da FMT_MSA.2.

nota 4: Non è possibile per i nuovi oggetti della SFP, definita in FDP_ACF.1, avere differenti attributi di sicurezza di default, poiché l'ODV non prevede meccanismi per specificare i permessi di accesso al momento della loro creazione.

nota 5: ETA_SSL.3 è un componente funzionale esteso che deriva direttamente da FTA_SSL.3 avendo sostituito, nell'operazione di assegnazione, il tempo di inattività dell'utente con l'invio da parte dell'ambiente IT di un'eccezione riguardante l'integrità dei dati per interrompere la sessione di collegamento. Risulta idoneo che la dipendenza di questo componente sia la stessa che per FTA_SSL.3 cioè nessuna.

8.2.5. Dipendenza dei requisiti di garanzia di sicurezza

Il livello di garanzia selezionato per questo ODV è EAL4 con nessuna modifica. Le dipendenze sono definite dai criteri e poiché non sono modificate in questo ODV, tutte le dipendenze dei componenti di garanzia in questo Traguardo di Sicurezza sono soddisfatte.

8.2.6. Mutuo supporto dei requisiti di sicurezza

In questo capitolo si è mostrato che:

1. I requisiti funzionali di sicurezza soddisfano ognuno degli obiettivi di sicurezza, che a loro volta contrastano ognuna delle minacce.

2. I requisiti di garanzia di sicurezza sono appropriati per l'ODV.

3. Le dipendenze tra i requisiti funzionali di sicurezza, definiti in questo Traguardo di Sicurezza, che non sono soddisfatte sono state adeguatamente motivate.

Per questi motivi si può affermare che l'insieme dei requisiti di sicurezza definiti in questo Traguardo di Sicurezza si supportano mutuamente e sono internamente consistenti.

8.2.7. Motivazione del grado di robustezza delle funzioni di sicurezza dell'ODV

L'ODV descritto in questo Traguardo di Sicurezza è ideato per essere utilizzato in un ambiente IT custodito in locali con una buona protezione fisica rispetto ad accessi di personale non autorizzato e per essere gestito da Amministratori competenti.
Utilizzando l'ODV in questo contesto si assume che eventuali attaccanti abbiano un moderato potenziale di pericolosità, per questo motivo è adeguato un grado di robustezza "medium".
Si noti che l'unico meccanismo per cui appare adeguata una dichiarazione di robustezza è quello che interviene nel requisito funzionale FCS_COP.1

8.3. Motivazioni delle specifiche sommarie dell'ODV

8.3.1. Funzioni di sicurezza IT

Lo scopo di questa sezione è quello di identificare le funzioni di sicurezza dell'ODV demandate all'implementazione di ognuno dei requisiti funzionali di sicurezza.
La corrispondenza tra le funzioni di sicurezza e tutti i requisiti funzionali di sicurezza dell'ODV dimostra che le funzioni di sicurezza si supportano mutuamente avendolo già dimostrato in 8.2.6 per i requisiti di sicurezza.

EAU_GEN.1
La funzione di sicurezza Audit e Accountability soddisfa il requisito come descritto in [AUD1], [AUD2] e [AUD3] poiché prevede:

- la registrazione in un file degli eventi e delle informazioni specificate nel requisito;
- che ad ogni azione sia legata una data ed un'ora affidabile.

FAU_GEN.2
La funzione di sicurezza Audit e Accountability soddisfa il requisito come descritto in [AUD2] poiché prevede:

- che ad ogni azione registrata sia legata l'identità dell'utente che l'ha generata.

FAU_SAR.1
La funzione di sicurezza Audit e Accountability soddisfa il requisito come descritto in, [AUD4] e [AUD5] poiché prevede che:

- il file di audit sia presentato in modo chiaro e leggibile;
- il file di audit sia leggibile solo dagli Amministratori.

FAU_SAR.2
La funzione di sicurezza Audit e Accountability soddisfa il requisito come descritto in [AUD5] poiché prevede:

- che solamente l'Amministratore possa leggere il file di audit.

FAU_SAR.3
La funzione di sicurezza Audit e Accountability soddisfa il requisito come descritto in [AUD6] poiché prevede:

- la ricerca degli eventi all'interno del file di audit utilizzando come criterio la data o la tipologia dell'evento stesso.

FCS_COP.1
La funzione di sicurezza Identificazione soddisfa il requisito come descritto in [ID1] poiché prevede:

- l'utilizzo dell'algoritmo SHA-1 per calcolare l'impronta digitale del certificato associato a ciascun utente al fine di identificare quest'ultimo.

FDP_ACC.2
La funzione di sicurezza Controllo accessi soddisfa il requisito come descritto in [AC1] poiché prevede:

- l'applicazione della politica di controllo degli accessi basata sul ruolo dell'utente.

FDP_ACF.1
La funzione di sicurezza Controllo accessi soddisfa il requisito come descritto in [AC1] poiché prevede:

- l'applicazione della politica di controllo degli accessi sulla base di quanto descritto nel requisito funzionale.

FIA_ATD.1
La funzione di sicurezza Identificazione soddisfa il requisito come descritto in [ID1] poiché prevede:

- l'esistenza della tabella dei certificati, dove per ogni certificato registrato su una CMD assegnata ad un utente è presente la corrispondenza con il ruolo che l'utente possiede.

FIA_UID.2 (1)
La funzione di sicurezza Identificazione soddisfa il requisito come descritto in [ID1] e [ID2] poiché prevede:

- l'identificazione dell'utente che accede all'ODV tramite il ruolo associato al certificato digitale registrato sulla sua CMD;
- l'impossibilità di qualunque azione se non si è stati correttamente identificati.

FMT_MSA.1
La funzione di sicurezza Controllo accessi soddisfa il requisito come descritto in [AC1] e [AC2] poiché prevede che:

- l'ODV implementi una politica di controllo accessi che definisca le azioni rese possibili agli utenti in base al ruolo dagli stessi ricoperto;
- solamente l'Amministratore possa assegnare, modificare, revocare o ricercare un ruolo associato ad un utente.

FMT_SMF.1
La funzione di sicurezza Controllo accessi soddisfa il requisito come descritto in [AC2] poiché prevede:

- che l'ODV permetta la gestione degli attributi di sicurezza degli utenti.

FMT_SMR.1
La funzione di sicurezza Controllo accessi soddisfa il requisito come descritto in [AC1] poiché prevede:

- la definizione dei ruoli Ufficio pass, Ufficio sicurezza, Acquisitore CMD e Amministratore come definito nel requisito funzionale.

FPT_RVM.1(1)
Le funzioni di sicurezza Identificazione e Controllo accessi soddisfano il requisito come descritto in [ID2] e [AC1] poiché prevedono:

- che la politica di sicurezza dell'ODV non possa essere aggirata, in quanto la non corretta identificazione impedisce qualunque accesso all'ODV;
- che la politica di sicurezza dell'ODV non possa essere aggirata, in quanto il controllo accessi basato sul ruolo è applicato ad ogni utente, permettendogli l'accesso solamente alle funzionalità e ai dati gestiti dall'ODV previsti dal ruolo che possiede.

FTA_SSL.3
La funzione di sicurezza Controllo accessi soddisfa il requisito come descritto in [AC3] poiché prevede:

- che la sessione di collegamento tra l'ODV e la postazione remota dell'utente sia terminata nel caso in cui quest'ultimo rimanga inattivo per più di dieci minuti;

ETA_SSL.3
La funzione di sicurezza Controllo accessi soddisfa il requisito come descritto in [AC3] poiché prevede

- che la sessione di collegamento tra l'ODV e la postazione remota dell'utente sia terminata se l'ODV riceve un'eccezione di integrità dei dati del database di controllo degli accessi dall'ambiente IT.

8.3.2. Motivazione del grado di robustezza delle funzioni di sicurezza dell'ODV

Come già descritto in 8.2.7 l'ODV è ideato per essere utilizzato in un ambiente IT custodito in locali con una buona protezione fisica rispetto ad accessi di personale non autorizzato e per essere gestito da Amministratori competenti.
Utilizzando l'ODV in questo contesto si assume che eventuali attaccanti abbiano un moderato potenziale di pericolosità, per questo motivo è adeguato un grado di robustezza "medium".
Si noti che l'unico meccanismo per cui appare adeguata una dichiarazione di robustezza è quello che interviene nella funzione di sicurezza di identificazione.

8.3.3. Misure di garanzia

Con riferimento alla Tabella 12 che segue, vengono messi in relazione i componenti di garanzia previsti per il livello EAL4 con i documenti redatti nel contesto della valutazione dell'ODV e le relative motivazioni.

Componenti di garanzia	Documentazione di riferimento	Motivazione
ACM_AUT.1 **ACM_CAP.4**	• Gestione della Configurazione per il prodotto Controllo Accessi	Nei documenti è descritto il processo di gestione delle configurazioni, la modalità

ACM_SCP.2	Palazzo Esercito v. 3.0	con la quale è gestita la tracciatura delle configurazioni dell'ODV nel sistema di revisione aziendale, la lista di configurazione dell'ODV e i tool automatici utilizzati come ausilio al controllo configurazione.
ADO_DEL.2 **ADO_IGS.1**	• Procedure di Consegna per il Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 2.0 • Procedure di installazione, generazione e start-up del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 3.0	Nei documenti sono descritte le modalità di consegna dell'ODV al cliente e la procedura di installazione ed attivazione dell'ODV.
ADV_FSP.2 **ADV_HLD.2** **ADV_IMP.1** **ADV_LLD.1** **ADV_RCR.1** **ADV_SPM.1**	• Specifiche funzionali per il Controllo Accessi Palazzo Esercito v. 3.0 • Disegno di alto livello del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 3.0 • Rappresentazione dell'implementazione del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 3.0 • Disegno di basso livello del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 3.0 • Modello della politica di sicurezza del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 3.0	Nei documenti vengono identificate le specifiche funzionali a copertura dei requisiti dell'ODV, i principali sistemi, sottosistemi, moduli e implementazioni delle funzioni di sicurezza; l'analisi di corrispondenza tra le rappresentazioni adiacenti in termini di astrazione.
AGD_ADM.1 **AGD_USR.1**	• Manuale Amministratore del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 3.0 • Manuale Utente del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 3.0	Nei documenti è descritta la procedura d'uso per l'Amministratore e per gli utenti
ALC_DVS.1 **ALC_LCD.1** **ALC_TAT.1**	• Sicurezza del processo di sviluppo per il Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 2.0 • Definizione del Ciclo di Vita per il Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 2.0	Nei documenti sono descritte le misure di sicurezza necessarie per proteggere la confidenzialità e integrità del progetto e la sua implementazione; il modello utilizzato per sviluppare e mantenere l'ODV; tutti i tool utilizzati per l'implementazione

	• Strumenti di sviluppo ben definiti per il Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 2.0	
ATE_COV.2 **ATE_DPT.1** **ATE_FUN.1** **ATE_IND.2**	• Documentazione relativa ai test del Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 2.0	Nella documentazione sono descritti puntualmente i piani di test per la verifica delle funzionalità dell'ODV e sono descritte le modalità per l'esecuzione e la registrazione dei test.
AVA_MSU.2 **AVA_SOF.1** **AVA_VLA.2**	• Analisi dell'uso improprio indotto dalla documentazione per il Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 2.0 • Analisi di Robustezza delle funzioni di sicurezza per il Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 2.0 • Analisi delle Vulnerabilità per il Prodotto Gestionale per il Controllo Accessi Palazzo Esercito v. 2.0	Nella documentazione è descritta la procedura d'uso, l'analisi della robustezza delle funzioni di sicurezza, l'analisi delle vulnerabilità note e la loro non sfruttabilità.

Tabella 12 – Misure di garanzia

8.4. Motivazione della dichiarazione di conformità ad uno o più PP

Non applicabile. Non ci sono dichiarazioni di conformità ad uno o più PP.