Gestione dei dati Sanitari, Infermerie e CMD

TRAGUARDO DI SICUREZZA

Codice: **SMD06_Traguardo_Di_Sicurezza_v4.1_16mag08.doc**

Versione: **v4.1**

Data: **16/05/2008**

Il presente documento è stato redatto da: EUTELIA S.p.A. per Blustaff S.p.A..

Approvazione

ORGANIZZAZIONE	NOME	FIRMA	DATA
BLUSTAFF S.p.A.	**Luigi Mastrangelo**		

Versione	Data	Pagine/Paragrafi modificati	Motivazioni
0.1 bozza	10/01/2007	Tutte	Redazione preliminare
1.0	16/01/2007	Pagg 1, 8, 9, 17, 18	Revisione
1.1	19/01/2007	Pagg 3, 19, 28, 29, 30, 35, 36	Revisione
2.0 bozza	07/02/2007	Pagg 1, 3, 8, 9, 11, 22, 25, 34, 38	Revisione
2.0	09/02/2007	Pagg 1, 3, 8, 11	Revisione
3.0 bozza	28/02/2007	Pagg 1, 3, 6, 9, 11, 12, 13, 16, 17, 19, 20-23, 30-35, 37, 38, 40, 41, 42	Revisione a seguito del ROA N.1
3.0	06/03/2007	Pagg 1, 2, 3,	Revisione
4.0	18/01/2008	Tutte	Revisione
4.1	16/05/2008	Par. 2.1, 6.1	Revisione a seguito del ROA N.7

INDICE DEI CONTENUTI

INDICE DELLE TABELLE

INDICE DELLE FIGURE

1. INTRODUZIONE

Questa sezione identifica il Traguardo di Sicurezza (TDS) e l'Oggetto Di Valutazione (ODV), la dimostrazione di conformità del TDS e l'organizzazione del TDS stesso.
L'ODV è un'applicazione software, sviluppata da Blustaff S.p.A., che fa parte di una infrastruttura adibita al trattamento delle informazioni sanitarie dello Stato Maggiore della Difesa.
L'ODV è inserito in un sistema che permette l'accesso, tramite postazioni remote, ad un database centrale che contiene i dati sanitari dei pazienti. Gli utenti abilitati ad accedere ai dati si identificano ed autenticano e successivamente interagiscono con il sistema mediante un'interfaccia web; completata con successo la procedura di identificazione/autenticazione, l'ODV abilita le funzionalità in base al profilo dell'utente.

Il Traguardo Di Sicurezza contiene, in aggiunta a tale introduzione, le seguenti sezioni:

- Descrizione dell'ODV (Sezione 2) – Questa sezione fornisce una breve introduzione sull'ODV, descrive l'ODV in termini dei suoi limiti fisici e logici, e definisce lo scopo dell'ODV.
- Ambiente di Sicurezza (Sezione 3) – Questa sezione descrive l'ambiente e le minacce che sono presenti nell'ODV e nel suo ambiente
- Obiettivi di sicurezza (Sezione 4) – Questa sezione dettaglia gli obiettivi di sicurezza dell'ODV e del suo ambiente
- Requisiti di sicurezza IT (Sezione 5) – La sezione presenta i requisiti funzionali di sicurezza (SFR) per l'ODV e per l'ambiente IT che supporta l'ODV, e dettaglia i requisiti di garanzia per EAL3
- Sommario delle specifiche dell'ODV (Sezione 6) – La sezione descrive le funzioni di sicurezza rappresentate nell'ODV che soddisfano i requisiti di sicurezza
- Conformità ai PP (Sezione 7) – Questa sezione presenta eventuali dimostrazioni di conformità ai PP
- Motivazioni (Sezione 8) – Questa sezione conclude il TDS con le giustificazioni relative agli obiettivi di sicurezza, ai requisiti e al sommario delle specifiche dell'ODV in termini di consistenza, completezza e fruibilità

1.1. TRAGUARDO DI SICUREZZA, ODV E CC

Titolo TDS – Traguardo di Sicurezza per il software interforze "Gestione dei dati Sanitari, Infermerie e CMD"
Versione TDS – 4.1
Data TDS – 16/05/2008
Autori TDS – LVS Eutelia S.p.A. per Blustaff S.p.A.
Identificazione TDS – SMD06_Traguardo_Di_Sicurezza_v4.1_16mag08
Identificativo ODV – SMD06 - Software interforze "Gestione dei dati Sanitari, Infermerie e CMD"
Versione ODV – v3.2.4
Evaluation Assurance Level (EAL) – EAL3.

1.2. CONFORMITA' AI CC

Questo ODV è conforme a:

- Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Requirements, Versione 2.3, August 2005, cod. CCMB-2005-08-002.
- Common Criteria for Information Technology Security - Evaluation Part 3: Security Assurance Requirements, Versione 2.3, August 2005, cod. CCMB-2005-08-003; conforme a livello di assurance EAL 3.

1.3. ACRONIMI

Gli acronimi utilizzati sono:

CC	Common Criteria
CMD	Carta Multiservizi della Difesa
DBS	Base Dati Sanitaria
DBP	Base Dati del Personale
EAL	Evaluation Assurance Level
ODV	Oggetto Di Valutazione
PIN	Personal Identification Number
PP	Protection Profile
ROA	Rapporto di Osservazione per Anomalia
SFR	Security Functional Requirements
SMD	Stato Maggiore della Difesa
SSL	Secure Socket Layer
ST	Security Target
TDS	Traguardo Di Sicurezza
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

2. DESCRIZIONE DELL'ODV (ASE_DES)

2.1. INTRODUZIONE

L'infrastruttura completa in cui si inserisce l'ODV è costituita da:

- Postazioni client remote,
- Web Server,
- Base Dati Sanitaria (DBS) e Base Dati del Personale (DBP) che costituiscono il Database centrale.

L'ODV è una Web Application costituita da pagine Jsp, Servlet, JavaBeans, file xml e controlli Javascript che viene invocata via web da postazioni client remote; l'ODV è installato su Oracle Application Server 10g che si occupa anche dell'instaurazione delle connessioni SSL con i client remoti.
All'atto della connessione viene scaricata sul client un'applet firmata dedicata alla gestione della CMD, che rimane attiva per tutta la sessione; tale applet non fa parte dell'ODV.
L'utente dell'ODV può effettuare la login con username e password oppure tramite CMD e PIN.
L'ODV effettua sempre l'identificazione dell'utente; qualora venga effettuata la login con username e password, l'ODV effettua anche l'autenticazione, mentre se la login viene effettuata tramite CMD e PIN l'autenticazione è implementata dall'ambiente IT.
Una volta identificato ed autenticato, l'utente accede soltanto alle funzioni o ai dati dell'ODV compatibili con il proprio profilo.
Alcune operazioni eseguite dall'ODV prevedono la connessione alla Base Dati Sanitaria per la visualizzazione, l'aggiornamento, la cancellazione o l'inserimento di dati secondo una logica transazionale: in questo caso l'ODV si connette al database tramite API JDBC.
Dalla Base Dati Sanitaria è possibile anche accedere alla Base Dati del Personale, che contiene tutte le informazioni anagrafiche degli utenti.
Tutte le operazioni eseguite dall'ODV, in risposta alle richieste dei client, sono tracciate all'interno di un archivio di audit, che può essere acceduto in sola consultazione e stampa dagli utenti autorizzati.

Nella seguente figura è rappresentata l'infrastruttura completa dell'ODV.

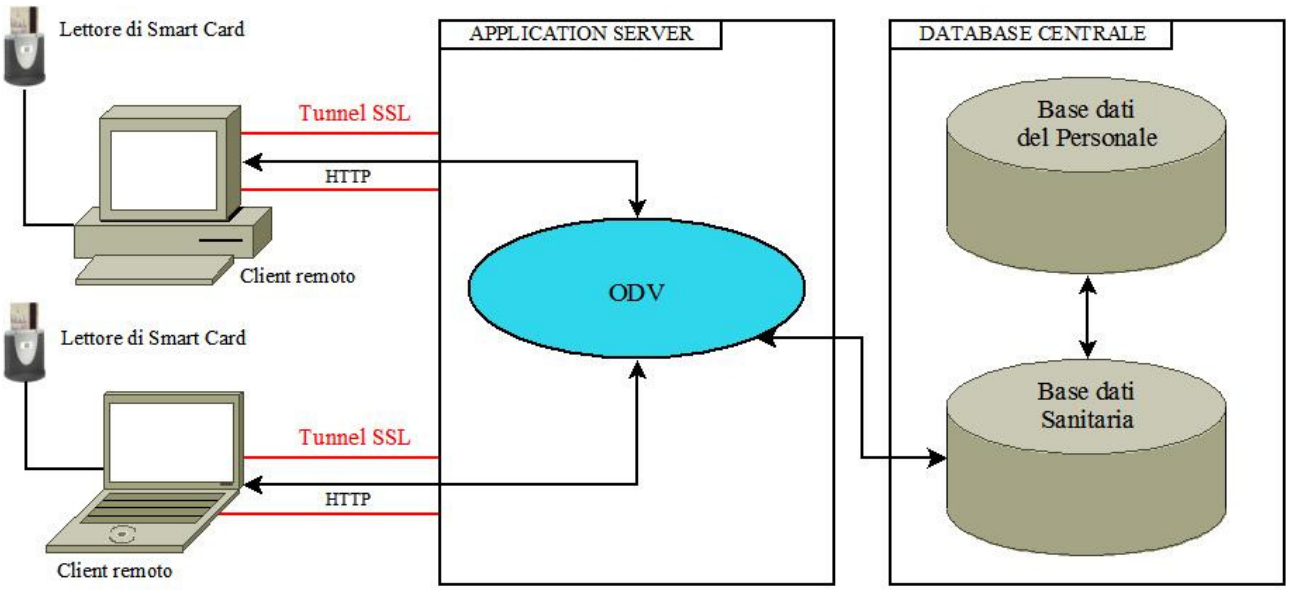

Figura 1: Infrastruttura ODV

Di seguito sono elencati i profili di utente (ruoli) dell'ODV previsti e le relative operazioni ad essi consentite:

- Amministratore:
  - Creazione degli utenti e associazione del relativo profilo;
  - Consultazione e stampa dei dati di Audit.
- Personale Medico:
  - Consultazione dati del paziente;
  - Inserimento dati (es: diagnosi, prescrizioni);
- Super-Amministratore:
  - Creazione degli utenti e associazione del relativo profilo;
  - Consultazione e stampa dei dati di Audit;
  - Consultazione dati del paziente;
  - Inserimento dati (es: diagnosi, prescrizioni).

2.2. ARCHITETTURA DELL'ODV

L'architettura dell'ODV è composta dai seguenti moduli:

- Identificazione ed autenticazione;
- Autorizzazione;
- Configurazione e gestione utenze a profili predefiniti;
- Registrazione dati di audit;
- Consultazione e stampa dati di audit.

2.2.1 Identificazione ed Autenticazione

Questo modulo è deputato ad identificare/autenticare gli utenti che vogliono operare sull'ODV e prevede due modalità:

- tramite digitazione di username e password;
- tramite Smart Card, inserendo la carta e digitandone il PIN.

Nel primo caso l'ODV effettua sia l'identificazione che l'autenticazione e cioè confronta le credenziali inserite dall'utente con quelle presenti nel Database centrale e, in caso di esito positivo, identifica ed autentica l'utente recuperando, dalla "tabella delle credenziali", il profilo ad esso associato.
Nel secondo caso invece l'ODV effettua soltanto l'identificazione in quanto l'autenticazione viene preventivamente effettuata dall'ambiente (Smart Card CMD): se l'autenticazione è andata a buon fine, l'applet scaricata sul client recupera i dati anagrafici presenti sulla CMD e li trasmette all'ODV, che li utilizza per identificare l'utente recuperando, dalla "tabella delle credenziali" del Database centrale, il profilo ad esso associato.

2.2.2 Autorizzazione

Tale modulo permette di recuperare le autorizzazioni associate al profilo di un utente; una tabella presente sulla DBS registra in modo predefinito e puntuale gli oggetti, le voci di menu, i pulsanti che un determinato profilo è autorizzato a vedere ed utilizzare.

2.2.3 Configurazione e Gestione Utenze e Profili

Tale modulo consente la creazione degli utenti dell'ODV attraverso la definizione di username e password per ogni utente, l'associazione ad un determinato profilo e l'impostazione di alcuni parametri. Le regole di creazione rispondono alle misure di sicurezza previste dal D.lgs. 196/2003.

2.2.4 Registrazione dati di Audit

Tale modulo consente di registrare in un archivio di audit le operazioni effettuate dagli utenti: pagine visitate, accessi al Database (modifiche o cancellazioni dei dati con salvataggio degli stessi prima delle modifiche), creazione di report.
Per ogni evento l'ODV tiene traccia delle seguenti informazioni:

- data ed ora dell'operazione;
- IP della macchina che ha effettuato l'operazione;
- identificativo dell'utente;
- operazione eseguita;
- query effettuata e relativa entità del Database interessata;
- identificativo del soggetto i cui dati sanitari sono stati modificati.

2.2.5 Consultazione e stampa dati di Audit

Tale modulo dell'ODV permette la consultazione e la stampa dei dati di audit, limitatamente agli utenti autorizzati (profili super-amministratore ed amministratore). La consultazione è facilitata dall'impostazione di opportuni criteri di restrizione, ad esempio intervallo di date, tipo di informazioni da visualizzare, etc.

2.3. CONFIGURAZIONE VALUTATA

Nella configurazione valutata, l'ODV utilizza un Web Server per l'esecuzione del software di cui è composto l'ODV e per lo scambio delle informazioni con i client su connessione SSL ed un Database centrale per la memorizzazione dei dati. Entrambi sono esterni all'ODV.

2.4. DEFINIZIONE DELL'AMBIENTE DELL'ODV

L'ambiente IT a supporto dell'ODV comprende il Web Server che permette l'esecuzione del software di cui è composto l'ODV e si occupa dell'instaurazione delle connessioni SSL con i client e il Database centrale per la memorizzazione dei dati sanitari e dei dati personali. In particolare l'ambiente IT comprende i seguenti pacchetti software:

- Web Server
  - Sistema operativo Windows 2003 Server
  - Oracle Application Server 10g
- Postazioni remote client
  - Sistema operativo Windows XP

- Smart Card Siemens CardOS M 4.01 (SLE66CX320P)
- Database centrale
  - Sistema operativo Windows 2003 Server
  - Oracle Database 10g Enterprise Edition Release 1

2.5. LIMITI DELL'ODV

2.5.1 Limiti fisici

L'ODV è un'applicazione software, per cui i suoi limiti fisici sono rappresentati dalle comunicazioni tra i componenti software dell'ODV, il web server ed il DB centrale.

2.5.2 Limiti logici

I limiti logici dell'ODV includono le funzioni di sicurezza implementate dall'ODV. Tali funzioni includono:

- Identificazione/autenticazione degli utenti;
- controllo degli accessi, differenziato in base al profilo dell'utente;
- audit.

3. AMBIENTE DI SICUREZZA (ASE_ENV)

L'ambiente di sicurezza dell'ODV descrive gli aspetti di sicurezza dell'ambiente nel quale l'ODV è utilizzato e la maniera in cui l'ODV dovrebbe essere utilizzato. In questo capitolo si definiscono:

- Le assunzioni fatte sull'ambiente operativo e l'uso previsto per l'ODV;
- Le minacce che l'ODV potrebbe incontrare;
- Le politiche di sicurezza dell'organizzazione.

3.1. ASSUNZIONI

A.LOCATE L'ODV ed i componenti del suo ambiente sono fisicamente allocati e protetti in un unico ambiente ad accesso controllato.

A.NOEVIL Il personale responsabile dell'utilizzo, della gestione e della configurazione dell'ODV non è malintenzionato, né negligente e segue attentamente tutte le istruzioni fornite dalla documentazione di guida.

A.TRAINING Il personale responsabile dell'utilizzo, della gestione e della configurazione è ben formato e competente nell'esecuzione sicura e corretta delle sue mansioni.

3.2. BENI CHE RICHIEDONO PROTEZIONE

I beni dell'ODV da proteggere sono:

- Dati di identificazione/autenticazione degli utenti dell'ODV;
- Dati sanitari;
- Dati di audit.

3.3. MINACCE ALLA SICUREZZA

T.ACCESSO_AUDIT Utenti non autorizzati potrebbero accedere ai dati di audit attraverso l'ODV.

T.CONTROLLO_ACCESSO Un utente autorizzato dell'ODV, attraverso l'ODV, potrebbe accedere ai beni dell'ODV senza i permessi necessari.

T.AUTENTICAZIONE Un utente, attraverso l'ODV, potrebbe accedere ai beni dell'ODV senza essere identificato ed autenticato.

T.CONFIDENTIALITY Un utente non autorizzato potrebbe acquisire le informazioni che transitano tra l'ODV e il suo ambiente.

3.4. POLITICHE DI SICUREZZA DELL'ORGANIZZAZIONE

P.ACCOUNTABILITY Le azioni che gli utenti dell'ODV svolgono all'interno dell'ODV saranno registrate e ad essi ricondotte.

P.GESTIONE I ruoli degli utenti all'interno dell'ODV potranno essere modificati solo da utenti con privilegi amministrativi.

4. OBIETTIVI DI SICUREZZA (ASE_OBJ)

Questa sezione definisce gli obiettivi di sicurezza dell'ODV e l'ambiente di supporto. Gli obiettivi di sicurezza, suddivisi in obiettivi IT per l'ODV, obiettivi IT per l'ambiente e obiettivi non-IT per l'ambiente, riflettono l'intenzione di contrastare le minacce e/o conformarsi alle politiche di sicurezza e seguire le assunzioni identificate.

4.1. OBIETTIVI DI SICUREZZA PER L'ODV

O.AUTH L'ODV deve garantire che solo utenti correttamente identificati e autenticati, tramite password, possano accedere ai dati dell'ODV.

O.IDE L'ODV deve garantire che solo utenti correttamente identificati ed autenticati, tramite CMD e PIN, possano accedere ai dati dell'ODV.

O.AUDIT L'ODV deve memorizzare le azioni rilevanti per la sicurezza effettuate dagli utenti dell'ODV.

O.ACCESSO_AUDIT L'ODV deve presentare le informazioni di audit solo agli utenti autorizzati.

O.CONTROLLO_ACCESSO L'ODV deve controllare l'accesso alle risorse in base alle identità degli utenti. L'ODV deve permettere solo agli utenti autorizzati di definire i permessi di accesso degli utenti alle risorse.

O.GESTIONE L'ODV deve fornire tutte le funzionalità necessarie per supportare gli utenti con privilegi amministrativi responsabili della gestione dell'ODV e deve garantire che solo questi siano in grado di accedere a tali funzionalità.

4.2. OBIETTIVI DI SICUREZZA PER L'AMBIENTE IT

OE.TIME L'ambiente IT deve garantire la corretta generazione del riferimento temporale in supporto alle TSF dell'ODV.

OE.TRSF_WKS L'ambiente IT deve garantire che l'utente possa instaurare un canale fidato con l'ODV prima di inviare le proprie credenziali di accesso.

OE.TRSF_DB L'ambiente IT deve garantire integrità, autenticità e confidenzialità delle informazioni riservate tra l'ODV e il database centrale.

OE.DATI L'ambiente IT deve garantire che i dati siano protetti per quel che riguarda l'integrità e la confidenzialità.

OE.AUTH L'ambiente IT deve garantire che i soli utenti correttamente autenticati tramite inserimento di CMD e PIN possano essere successivamente identificati dall'ODV.

4.3. OBIETTIVI DI SICUREZZA PER L'AMBIENTE NON-IT

OE.LOCATE L'ODV ed i componenti del suo ambiente devono essere fisicamente allocati e protetti in un unico ambiente bunker, schermato, il cui accesso viene strettamente controllato e permesso al solo personale autorizzato.

OE.MNGM I responsabili dell'ODV devono garantire che la gestione e la configurazione dell'ODV sia effettuata da personale fidato e competente, in accordo con le procedure interne di sicurezza.

OE.INSTALL I responsabili dell'ODV devono garantire che tutte le informazioni di sicurezza (password) siano caricate sull'ODV in modo sicuro.

OE.USE Gli utenti dell'ODV non devono essere malintenzionati, né negligenti e seguono attentamente tutte le istruzioni fornite dalla documentazione di guida per l'utente e quanto stabilito dai responsabili dell'ODV.

5. REQUISITI DI SICUREZZA IT (ASE_REQ)

Questo capitolo definisce i requisiti funzionali di sicurezza per l'ODV e i requisiti di garanzia presi in considerazione nella valutazione dell'ODV. I requisiti di sicurezza dell'ODV sono ricavati dalla Parte 2 dei Common Criteria, versione 2.3.

5.1. REQUISITI FUNZIONALI DI SICUREZZA DELL'ODV

La seguente tabella descrive i requisiti funzionali di sicurezza che devono essere soddisfatti dall'ODV:

Classi funzionali	Componenti funzionali
Identification and Authentication (FIA)	FIA_AFL.1 Authentication failure handling FIA_ATD.1 User attribute definition FIA_UID.2 User identification before any action FIA_UAU.2 User authentication before any action FIA_UAU.7 Protected authentication feedback FIA_SOS.1 Specification of secrets
Access control policy (FDP)	FDP_ACC.1 Subset access control FDP_ACF.1 Security attribute based access control
Security management (FMT)	FMT_MSA.1 Management of security attributes FMT_MSA.3 Static attribute initialisation FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Security audit (FAU)	FAU_GEN.1 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 FAU_SAA.1 Potential violation analysis

Tabella 1: Requisiti funzionali di sicurezza

5.1.1 Identification and Authentication (FIA)

5.1.1.1. FIA_AFL Authentication failures

FIA_AFL.1 Authentication failure handling

FIA_AFL_1.1 The TSF shall detect when [***tre***] unsuccessful authentication attempts occur related to [***tentativi di login***].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [***blocco dell'utenza***].

5.1.1.2. FIA_ATD User attribute definition

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [***ruolo, password***].

5.1.1.3. FIA_UID User identification

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.4. FIA_UAU User authentication

FIA_UAU.2 (a) User authentication before any action

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.

FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only [***il numero di caratteri inseriti***] to the user while the authentication is in progress.

5.1.1.5. FIA_SOS Specification of secrets

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [***la seguente Politica delle Password:***

1. ***deve essere definita come una stringa alfanumerica di almeno otto caratteri di lunghezza***
2. ***deve soddisfare almeno tre dei quattro requisiti che seguono:***
   - ***contenere almeno una lettera Maiuscola***
   - ***contenere almeno una lettera Minuscola***
   - ***contenere almeno una cifra numerica***
   - ***contenere almeno un carattere "speciale"; i caratteri speciali possono essere tutti quelli non alfanumerici, tranne i seguenti: / (slash), \ (backslash), ‘ (apice), “ (doppio apice), Tabulazione***
3. ***non deve contenere riferimenti facilmente associabili all'utente, conformemente alle misure minime di sicurezza previste dal D.lgs 196/2003***].

5.1.2 User data protection(FDP)

5.1.2.1. FDP_ACC Access control policy

FDP_ACC.1 (a) Subset access control

FDP_ACC.1.1(a) The TSF shall enforce the [***politica di controllo di accesso ai dati sanitari***] on [soggetti: ***utenti con profilo medico, amministratore e super-amministratore***, oggetti: ***dati sanitari***, operazioni: ***lettura, scrittura***].

FDP_ACC.1(b) Subset access control

FDP_ACC.1.1(b) The TSF shall enforce the [***politica di controllo di accesso ai dati di audit***] on [soggetti: ***utenti con profilo medico, amministratore e super-amministratore***, oggetti: ***record di audit***, operazioni: ***consultazione e stampa***].

5.1.2.2. FDP_ACF Access control functions

FDP_ACF.1(a) Security attribute based access control

FDP_ACF.1.1(a) The TSF shall enforce the [***politica di controllo di accesso ai dati sanitari***] to objects based on the following: [attributo del soggetto: ***ruolo***].

FDP_ACF.1.2(a) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***il personale medico ed il super-amministratore possono accedere ai dati sanitari in lettura e in scrittura***].

FDP_ACF.1.3(a) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***nulla***].

FDP_ACF.1.4(a) The TSF shall explicitly deny access of subjects to objects based on the following rule [***l'amministratore non può accedere ai dati sanitari***].

FDP_ACF.1(b) Security attribute based access control

FDP_ACF.1.1(b) The TSF shall enforce the [***politica di controllo di accesso ai dati di audit***] to objects based on the following: [attributo del soggetto: ***ruolo***].

FDP_ACF.1.2(b) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***l'amministratore e il super-amministratore possono accedere ai dati di audit in consultazione e stampa***]

FDP_ACF.1.3(b) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***nulla***].

FDP_ACF.1.4(b) The TSF shall explicitly deny access of subjects to objects based on the following rule [***il personale medico non può accedere ai dati di audit***].

5.1.3 Security management (FMT)

5.1.3.1. FMT_MSA Management of security attributes

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [***politica di controllo di accesso ai dati sanitari ed ai dati di audit***] to restrict the ability to [***cambiare***] the security attributes [***Date di validità dell'account, Max. periodo di inattività dell'account, Periodo di validità della password***] to [***amministratore, super-amministratore***].

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [***politica di controllo di accesso ai dati sanitari ed ai dati di audit***] to provide [***restrittivi***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [***amministratore, super-amministratore***] to specify alternative initial values to override the default values when an object or information is created.

5.1.3.2. FMT_SMR Security management roles

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [***personale medico, amministratore, super-amministratore***].

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

5.1.3.3. FMT_SMF Specification of Management Functions

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [***l'amministratore può modificare la data di validità di un profilo medico in caso di gravi situazioni di errore nell'ODV***].

5.1.4 Security audit (FAU)

5.1.4.1. FAU_GEN Security audit data generation

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [***dettagliato***] level of audit; and
c) [***nulla***].

FAU_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 definitions of the functional components included in the ST, [***operazione effettuata e relativa entità del Database interessata, identificativo del soggetto i cui dati sono stati modificati***].

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.

5.1.4.2. FAU_SAR Security audit review

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [***amministratori, super-amministratori***] with the capability to read [***informazioni di audit***] 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 [***ricerca e selezione***] of audit data based on [***intervallo di date, utente che ha effettuato le operazioni, tipo di operazione, IP utente, entità coinvolta***].

5.1.4.3. FAU_SAA Security audit analysis

FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of [***tre tentativi di login falliti consecutivamente per lo stesso username***] known to indicate a potential security violation;
b) [***non specificato***].

5.2. REQUISITI FUNZIONALI DI SICUREZZA PER L'AMBIENTE IT

La seguente tabella descrive i requisiti funzionali di sicurezza soddisfatti dall'ambiente IT dell'ODV. Per una migliore comprensione, nel seguito di questo paragrafo i requisiti sono stati raffinati sostituendo la sigla *TSF* con *IT environment*, dove necessario.

Classi funzionali	Componenti funzionali
Identification and Authentication (FIA)	FIA_UAU.2 User authentication before any action
Protection of the TSF (FPT)	FPT_STM.1 Reliable time stamps
User data protection (FDP)	FDP_ROL.1 Basic rollback
Cryptographic support (FCS)	FCS_COP.1 Cryptographic operation
Trusted path/channels (FTP)	FTP_TRP.1 Trusted path

Tabella 2: Requisiti funzionali di sicurezza per l'ambiente IT

5.2.1 Protection of the TSF (FPT)

5.2.1.1. FPT_STM Time stamps

FPT_STM.1 Reliable time stamps

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

5.2.2 User data protection(FDP)

5.2.2.1. FDP_ROL Rollback

FDP_ROL.1 Basic rollback

FDP_ROL.1.1 The IT environment shall enforce [***politica di controllo di accesso ai dati sanitari ed ai dati di audit***] to permit the rollback of the [***scrittura dati***] on the [***tabelle del Database centrale***].

FDP_ROL.1.2 The IT environment shall permit operations to be rolled back within the [***ogni eccezione che si verifica all'interno di una transazione***].

5.2.2.2. FCS_COP Cryptographic operation

FCS_COP.1 (WKS) Cryptographic operation

FCS_COP.1.1 The IT environment shall perform [***cifratura***] in accordance with a specified cryptographic algorithm [***DES***] and cryptographic key sizes [***56 bit***] that meet the following: [***standard internazionale***].

FCS_COP.1 (DB) Cryptographic operation

FCS_COP.1.1 The IT environment shall perform [***cifratura***] in accordance with a specified cryptographic algorithm [***DES***] and cryptographic key sizes [***56 bit***] that meet the following: [***standard internazionale***].

5.2.3 Trusted path/channel (FTP)

5.2.3.1. FTP_TRP Trusted path

FTP_TRP.1 Trusted path

FTP_TRP.1.1 The IT environment shall provide a communication path between itself and [***remoti***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The IT environment shall permit [***utenti remoti***] to initiate communication via the trusted path.

FTP_TRP.1.3 The IT environment shall require the use of the trusted path for [***identificazione/autenticazione iniziale dell'utente***].

5.3. REQUISITI DI GARANZIA DELL'ODV

L'ODV sarà conforme al livello EAL3 dei CC.

6. SOMMARIO DELLE SPECIFICHE DELL'ODV (ASE_TSS)

6.1. FUNZIONI DI SICUREZZA DELL'ODV

ODV.Autenticazione *Tutti gli utenti che accedono all'ODV sono identificati/autenticati*

L'ODV impone l'identificazione/autenticazione di tutti gli utenti tramite username e password oppure tramite Smart Card CMD e PIN. L'ODV protegge la password, durante l'immissione a video, sostituendo i caratteri digitati con un carattere "segnaposto". La funzione autentica l'utente se l'associazione username e password inserita dall'utente corrisponde a quanto memorizzato sulle tabelle presenti sul DBS oppure se i dati anagrafici estratti dalla CMD (che ha effettuato l'autenticazione) corrispondono ad un utente del presente sul DBS.
Nel caso di username e password ogni volta che l'utente effettua il login l'ODV verifica formalmente che username e password siano di almeno otto caratteri e verifica la presenza della combinazione username-password sulla tabella utenti presente sul DBS; in caso negativo invia al client uno specifico messaggio di errore; altrimenti controlla la validità della password stessa secondo la "regola dei 3 mesi", per la quale la password non può essere valida per un periodo superiore ai tre mesi, oltre il quale è necessario cambiarla.
Per ogni tentativo di login l'ODV controlla, per un certo username riconosciuto, la validità temporale dell'account associato e, successivamente, che il numero di tentativi falliti di inserimento della password non superi un numero massimo prefissato (pari a tre tentativi), oltre il quale l'utente viene disabilitato.
Se è la prima volta che accede, l'ODV obbliga anche l'utente a cambiare la password assegnatagli dall'amministratore.
Nel caso di utilizzo della CMD e relativo PIN, l'utente inserisce la CMD e l'applet scaricata sul client (che non fa parte dell'ODV) ne controlla la validità, verifica se la carta appartiene ad un profilo "medico" e ne chiede il PIN, per confrontarlo con quello a bordo della CMD stessa; se l'autenticazione è andata a buon fine, l'applet recupera i dati anagrafici presenti sulla CMD e li trasmette all'ODV, che li utilizza per identificare l'utente confrontando tali dati con quelli presenti nelle tabelle del DBS.
Per ogni utente, inoltre, l'ODV applica la "regola dei 6 mesi", secondo cui gli utenti che non utilizzano il sistema per sei mesi continui devono essere disattivati.

ODV.ControlloAccessi *L'accesso all'ODV è controllato e differenziato in base al profilo dell'utente*

L'ODV permette ad ogni utente autenticato di accedere soltanto a determinate operazioni o alle sole funzionalità/schermate/pulsanti/dati previsti dal profilo al quale risulta associato. Una volta che l'utente si è identificato/autenticato, infatti, l'ODV rileva il profilo a lui associato, ne verifica la validità in termini temporali e determina quali operazioni sono abilitate, confrontando la mappa completa delle funzioni applicative con le informazioni contenute nel profilo, memorizzate sul DBS.
A questo punto le informazioni relative all'utente (codice fiscale e profilo) sono inserite in sessione in modo da essere testate durante la navigazione su una qualunque funzione per attestare l'avvenuta autenticazione dell'utente. In caso negativo l'utente verrà reindirizzato alla pagina di Login.

ODV.Audit *Gli eventi di audit sono registrati dall'ODV e possono essere consultati*

L'ODV consente la registrazione di tutte le operazioni eseguite dall'ODV all'interno di un archivio di audit; in particolare le informazioni soggette ad audit sono:

- Tentativi di accesso riusciti e falliti;
- Elenco operazioni effettuate da un utente durante l'accesso;
- Informazioni accedute da un utente;
- Informazioni modificate da un utente (tracciando l'immagine precedente e successiva);
- Informazioni cancellate da un utente;
- Identificativo utente e IP della macchina che ha effettuato una particolare operazione;
- Data e ora in cui è stata effettuata una particolare operazione.

Solo gli utenti autorizzati (amministratore e super-amministratore) possono consultare i dati di audit, in sola lettura e stampa; l'ODV consente a tali utenti autorizzati di consultare i dati di audit definendo anche i criteri di ricerca delle informazioni da visualizzare o stampare.

6.2. *MISURE DI GARANZIA DI SICUREZZA DELL'ODV*

6.2.1 Gestione della configurazione

La gestione della configurazione evidenzia le procedure necessarie per garantire l'integrità dell'ODV durante l'intero processo di sviluppo e fornisce un riferimento unico per garantire che non ci siano ambiguità sulla configurazione dell'ODV da valutare. La garanzia di sicurezza fornita dalla gestione della configurazione soddisfa i seguenti requisiti per il livello EAL3:

- ACM_CAP.3
- ACM_SCP.1

6.2.2 Consegna e messa in opera dell'ODV

Il documento di consegna e messa in opera dell'ODV contiene le procedure necessarie per garantire la sicurezza durante l'installazione, la generazione e lo start up dell'ODV.
La garanzia di sicurezza fornita dalla consegna e messa in opera sicura dell'ODV soddisfa i seguenti requisiti di per il livello EAL3:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Processo di sviluppo dell'ODV

Il processo di sviluppo dell'ODV include le specifiche funzionali, la descrizione del progetto ad alto livello ed una dimostrazione informale della corrispondenza della rappresentazione.
Il documento di specifiche funzionali descrive le funzioni di sicurezza dell'ODV e le sue interfacce esterne utilizzando uno stile informale, sottolineandone lo scopo e il metodo d'utilizzo, gli eventi, le eccezioni e i messaggi di errore.

Il progetto ad alto livello raffina le specifiche funzionali, fornendo una descrizione più dettagliata dell'ODV in termini di sottosistemi e relative funzioni, mostrando, inoltre, tutte le relazioni tra i sottosistemi.
La rappresentazione delle corrispondenze è una verifica molto più dettagliata dell'accuratezza della rappresentazione delle funzioni di sicurezza, in modo da dimostrare che tali funzioni sono un'accurata, consistente e completa istanziazione dei requisiti di sicurezza forniti nel TDS.
La garanzia di sicurezza fornita dal processo di sviluppo dell'ODV soddisfa i seguenti requisiti per il livello EAL3:

- ADV_FSP.1
- ADV_HLD.2
- ADV_RCR.1

6.2.4 Documentazione di guida

La documentazione di guida comprende i manuali destinati agli utenti ed agli amministratori, e descrive le tecniche di interfacciamento con l'ODV, le istruzioni e le linee guida per una gestione ed un utilizzo sicuro dell'ODV.
La garanzia di sicurezza fornita dalla documentazione di guida destinata agli utenti ed agli amministratori dell'ODV soddisfa i seguenti requisiti per il livello EAL3:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Ciclo di vita dell'ODV

La documentazione relativa al ciclo di vita dell'ODV descrive le misure di sicurezza messe in atto durante lo sviluppo e la manutenzione dell'ODV.
La garanzia di sicurezza fornita dalla documentazione sul ciclo di vita dell'ODV soddisfa i seguenti requisiti per il livello EAL3:

- ALC_DVS.1

6.2.6 Test

La documentazione di test fornisce una descrizione completa di tutti i test eseguiti sull'ODV correttamente installato e, tramite i risultati effettivi, dimostra che tutti gli aspetti di sicurezza evidenziati nei precedenti documenti di specifiche funzionali e di progettazione ad alto livello sono stati appropriatamente testati.
La garanzia di sicurezza fornita dalla documentazione di test soddisfa i seguenti requisiti per il livello EAL3:

- ATE_COV.2
- ATE_DPT.1
- ATE_FUN.1
- ATE_IND.2.

6.2.7 Analisi di vulnerabilità

La documentazione sull'analisi delle vulnerabilità descrive le operazioni dell'ODV e come è possibile mantenere uno stato sicuro all'interno dell'ODV, tenendo conto anche delle assunzioni, dei requisiti e della robustezza delle funzioni di sicurezza.
La garanzia di sicurezza fornita dalla documentazione di analisi delle vulnerabilità soddisfa i seguenti requisiti per il livello EAL3:

- AVA_MSU.1
- AVA_SOF.1
- AVA_VLA.1

7. CONFORMITA' AD UN PROTECTION PROFILE

Questo Traguardo Di Sicurezza non ha alcun Profilo Di Protezione di riferimento.

8. MOTIVAZIONI

Questo capitolo fornisce una dimostrazione della completezza e della consistenza del TDS e copre le seguenti aree:

- Obiettivi di sicurezza
- Requisiti funzionali di sicurezza
- Requisiti di garanzia di sicurezza
- Robustezza delle funzioni
- Dipendenze tra i requisiti
- Sommario delle specifiche dell'ODV
- Conformità ad un PP.

8.1. MOTIVAZIONE DEGLI OBIETTIVI DI SICUREZZA

Lo scopo di questo paragrafo è dimostrare che gli obiettivi di sicurezza individuati sono:

- Sufficienti per soddisfare i bisogni di sicurezza
- Necessari dato che non ci sono obiettivi di sicurezza ridondanti.

8.1.1 Assunzioni, politiche e minacce

Obiettivi di sicurezza dell'ODV / Assunzioni Politiche Minacce	O.AUTH	O.IDE	O.AUDIT	O.ACCESSO_AUDIT	O.CONTROLLO_ACCESSO	O.GESTIONE	OE.TIME	OE.TRSF_WKS	OE.TRSF_DB	OE.DATI	OE.MNGM	OE.INSTALL	OE.LOCATE	OE.USE	OE.AUTH
A.LOCATE													X		
A.NOEVIL											X	X		X	
A.TRAINING											X	X		X	
P.ACCOUNTABILITY			X	X			X								
P.GESTIONE						X									
T.ACCESSO_AUDIT	X	X		X											X
T.CONTROLLO_ACCESSO	X	X			X										X
T.AUTENTICAZIONE	X	X								X					X
T.CONFIDENTIALITY								X	X						

Tabella 3: Mapping tra obiettivi di sicurezza e assunzioni/politiche/minacce

8.1.2 Dimostrazione di sufficienza degli obiettivi di sicurezza

Assunzioni	Obiettivi di sicurezza	Motivazione
A.LOCATE	OE.LOCATE	OE.LOCATE garantirà la protezione dell'ODV e dei componenti del suo ambiente tramite allocazione fisica degli stessi in un ambiente bunker, schermato, il cui accesso viene strettamente controllato e permesso al solo personale autorizzato.
A.NOEVIL	OE.MNGM OE.INSTALL OE.USE	OE.MNGM garantirà che la gestione e la configurazione dell'ODV sia effettuata da personale fidato e non malintenzionato. OE.INSTALL garantirà che tutte le informazioni di sicurezza (password) siano caricate sull'ODV in modo sicuro da personale fidato e non malintenzionato. OE.USE garantirà che l'ODV verrà utilizzato da personale non malintenzionato, né negligente e che seguirà attentamente tutte le istruzioni fornite dalla documentazione di guida per l'utente e quanto stabilito dai responsabili dell'ODV.
A.TRAINING	OE.MNGM OE.INSTALL OE.USE	OE.MNGM garantirà che la gestione e la configurazione dell'ODV sia effettuata da personale competente e ben formato. OE.INSTALL garantirà che tutte le informazioni di sicurezza (password) siano caricate sull'ODV in modo sicuro da personale competente e ben formato. OE.USE garantirà che l'ODV verrà utilizzato da personale non malintenzionato, né negligente e che seguirà attentamente tutte le istruzioni fornite dalla documentazione di guida per l'utente e quanto stabilito dai responsabili dell'ODV.

Tabella 4: Dimostrazione di sufficienza degli obiettivi di sicurezza

Politiche di sicurezza	Obiettivi di sicurezza	Motivazione
P.ACCOUNTABILITY	O.AUDIT O.ACCESSO_AUDIT OE.TIME	O.AUDIT garantirà la memorizzazione delle azioni rilevanti per la sicurezza effettuate dagli utenti dell'ODV. O.ACCESSO_AUDIT garantirà che le informazioni di audit siano mostrate solo agli utenti autorizzati. OE.TIME garantirà la corretta generazione del riferimento temporale.
P.GESTIONE	O.GESTIONE	O.GESTIONE fornirà tutte le funzionalità di supporto agli amministratori dell'ODV e garantirà che solo questi siano in grado di accedere a tali funzionalità.

Tabella 5: Dimostrazione di sufficienza degli obiettivi di sicurezza

Minacce	Obiettivi di sicurezza	Motivazione
T.ACCESSO_AUDIT	O.ACCESSO_AUDIT O.AUTH O.IDE OE.AUTH	O.ACCESSO_AUDIT garantirà che le informazioni di audit siano mostrate solo agli utenti autorizzati. O.AUTH garantirà che solo gli utenti, che accedono con username e pwd, correttamente identificati ed autenticati possano accedere alle risorse dell'ODV. OE.AUTH e O.IDE garantiranno, rispettivamente, che solo gli utenti, che accedono con CMD e PIN, correttamente autenticati ed identificati possano accedere alle risorse dell'ODV.
T.CONTROLLO_ACCESSO	O.CONTROLLO_ACCESSO O.AUTH O.IDE OE.AUTH	O.CONTROLLO_ACCESSO controllerà l'accesso alle risorse in base alle identità degli utenti e permetterà solo agli utenti autorizzati di definire i permessi di accesso degli utenti alle risorse. O.AUTH garantirà che solo gli utenti, che accedono con username e pwd, correttamente identificati ed autenticati possano accedere alle risorse dell'ODV. OE.AUTH e O.IDE garantiranno, rispettivamente, che solo gli utenti, che accedono con CMD e PIN, correttamente autenticati ed identificati possano accedere alle risorse dell'ODV.
T.AUTENTICAZIONE	O.AUTH O.IDE OE.DATI OE.AUTH	O.AUTH garantirà che solo utenti correttamente autenticati possano accedere alle risorse dell'ODV. OE.DATI garantirà la confidenzialità e l'integrità delle credenziali di ogni utente. OE.AUTH e O.IDE garantiranno, rispettivamente, che solo gli utenti, che accedono con CMD e PIN, correttamente autenticati ed identificati possano accedere alle risorse dell'ODV.
T.CONFIDENTIALITY	OE.TRSF_WKS OE.TRSF_DB	OE.TRSF_WKS garantirà la presenza di un canale fidato tra l'utente e l'applicazione prima di inviare le proprie credenziali di accesso. OE.TRSF_DB garantirà integrità, autenticità e confidenzialità delle informazioni riservate tra l'applicazione e il database centrale.

Tabella 6: Dimostrazione di sufficienza degli obiettivi di sicurezza

8.2. *MOTIVAZIONE DEI REQUISITI DI SICUREZZA*

Questa sezione dimostra che i requisiti di sicurezza dichiarati si supportano mutuamente e sono internamente consistenti. La consistenza interna è dimostrata nell'analisi delle dipendenze tra i requisiti (cfr. par. 8.2.2 e 8.2.3).
Il mutuo supporto è mostrato attraverso considerazioni riguardanti le interazioni tra i requisiti di sicurezza e gli obiettivi (cfr. par. 8.2.1).

8.2.1 Motivazione dei requisiti funzionali di sicurezza

Lo scopo di questa sezione è dimostrare che i requisiti di sicurezza identificati (Sezione 5) sono in grado di soddisfare gli obiettivi di sicurezza (Sezione 4). La seguente tabella mostra che ogni requisito di sicurezza è necessario, nel senso che è mappato su ogni obiettivo di sicurezza IT e viceversa.

Obiettivi di sicurezza IT / Requisiti funzionali di sicurezza (SFR)	O.AUTH	O.IDE	O.AUDIT	O.ACCESSO_AUDIT	O.CONTROLLO_ACCESSO	O.GESTIONE	OE.TIME	OE.TRSF_WKS	OE.TRSF_DB	OE.DATI	OE.AUTH
FIA_AFL.1	X										
FIA_ATD.1					X						
FIA_UID.2		X									
FIA_UAU.2 (a)	X										
FIA_UAU.7	X										
FIA_SOS.1	X										
FDP_ACC.1 (a)					X						
FDP_ACC.1 (b)				X							
FDP_ACF.1 (a)					X						
FDP_ACF.1 (b)				X							
FMT_MSA.1					X	X					
FMT_MSA.3						X					
FMT_SMR.1					X						
FMT_SMF.1					X	X					
FAU_GEN.1			X								
FAU_GEN.2			X								
FAU_SAR.1				X							
FAU_SAR.2				X							
FAU_SAR.3				X							
FAU_SAA.1				X							
FPT_STM.1							X				
FIA_UAU.2 (b)											X
FCS_COP.1 (WKS)								X		X	
FCS_COP.1 (DB)									X	X	
FDP_ROL.1									X	X	
FTP_TRP.1								X		X	

Tabella 7: Mapping tra requisiti funzionali di sicurezza e obiettivi di sicurezza

Obiettivi di sicurezza IT	Requisiti funzionali di sicurezza(SFR)	Motivazione
O.AUTH	FIA_AFL.1 FIA_UAU.2(a) FIA_UAU.7 FIA_SOS.1	FIA_AFL.1 richiede che l'ODV individui il numero di autenticazioni fallite, dopo il quale l'utenza viene bloccata. FIA_UAU.2(a) richiede che ogni utente sia autenticato con successo prima di eseguire ogni altra operazione sull'ODV. FIA_UAU.7 richiede che l'ODV fornisca un feedback all'utente che richiede l'autenticazione. FIA_SOS.1 richiede che l'ODV verifichi le password degli utenti secondo una specifica Politica delle Password.
O.IDE	FIA_UID.2	FIA_UID.2 richiede che ogni utente si identifichi prima di eseguire ogni altra operazione sull'ODV.
O.AUDIT	FAU_GEN.1 FAU_GEN.2	FAU_GEN.1 richiede la creazione di record di audit per gli eventi di start-up e shutdown delle funzioni di audit e per l'accesso in lettura e scrittura ai dati. Per ogni evento di audit richiede la registrazione di data, tipo, soggetto, componente coinvolto ed output dell'evento. FAU_GEN.2 richiede l'associazione di ogni evento di audit all'identità del soggetto che ha causato l'evento.
O.ACCESSO_AUDIT	FIA_ATD.1 FDP_ACC.1(b) FDP_ACF.1(b) FAU_SAR.1 FAU_SAR.2 FAU_SAR.3 FAU_SAA.1	FIA_ATD.1 richiede la presenza di una lista che identifichi il ruolo associato ad ogni utente. FDP_ACC.1 (b) richiede un controllo di accesso ai record di audit relativamente agli utenti che vi accedono in lettura e stampa. FDP_ACF.1 (b) richiede un controllo di accesso ai dati di audit in base al ruolo dell'utente: l'amministratore e il super-amministratore accedono in lettura ma il personale medico non può accedere. FAU_SAR.1 richiede che solo gli utenti autorizzati possano leggere i record di audit e che l'ODV fornisca i record di audit in un formato comprensibile. FAU_SAR.2 richiede che l'ODV blocchi l'accesso ai record di audit a tutti gli utenti ad eccezione di quelli esplicitamente autorizzati. FAU_SAR.3 richiede che l'ODV fornisca la possibilità di eseguire ricerche e ordinamenti sui record di audit sulla base di specifici criteri FAU_SAA.1 richiede l'applicazione di un set di regole, quali il controllo dei login falliti, allo scopo di monitorare gli eventi di audit allo scopo di identificare potenziali violazioni delle policy.

Obiettivi di sicurezza IT	Requisiti funzionali di sicurezza(SFR)	Motivazione
O.CONTROLLO_ACCESSO	FIA_ATD.1 FDP_ACC.1(a) FDP_ACF.1(a) FMT_MSA.1 FMT_SMR.1 FMT_SMF.1	FIA_ATD.1 richiede la presenza di una lista che identifichi il ruolo associato ad ogni utente. FDP_ACC.1 (a) richiede un controllo di accesso ai dati sanitari relativamente agli utenti che vi accedono in lettura e scrittura. FDP_ACF.1 (a) richiede un controllo di accesso ai dati sanitari in base al ruolo dell'utente: il personale medico ed il super-amministratore possono accedere ai dati sanitari in lettura e in scrittura, mentre l'accesso è precluso all'amministratore. FMT_MSA.1 richiede che il personale medico non sia autorizzato a cambiare gli attributi di sicurezza degli account utente. FMT_SMR.1 richiede la memorizzazione dei profili corrispondenti ad ogni utente. FMT_SMF.1 richiede che l'ODV offra all'amministratore la possibilità di modificare le date di validità di un profilo in caso di gravi situazioni di errore.
O.GESTIONE	FMT_MSA.1 FMT_MSA.3 FMT_SMF.1	FMT_MSA.1 richiede che solo l'amministratore ed il super-amministratore siano autorizzati a cambiare gli attributi di sicurezza degli account utente. FMT_MSA.3 richiede una politica di controllo di accesso per la definizione degli attributi di sicurezza di default. FMT_SMF.1 richiede che l'ODV offra all'amministratore la possibilità di modificare le date di validità di un profilo in caso di gravi situazioni di errore.
OE.AUTH	FIA_UAU.2(b)	FIA_UAU.2(b) richiede che l'ambiente IT autentichi (tramite CMD e PIN) ogni utente prima di eseguire ogni altra operazione sull'ODV
OE.TIME	FPT_STM.1	FPT_STM.1 richiede che l'ambiente IT sia in grado di fornire marche temporali affidabili.
OE.TRSF_WKS	FCS_COP.1 (WKS) FTP_TRP.1	FCS_COP.1 (WKS) richiede la cifratura dei dati inviati al client secondo l'algoritmo DES e con chiave a 56 bit tramite il protocollo SSL. FTP_TRP.1 richiede che l'ambiente IT instauri con l'utente che si vuole autenticare, un canale di comunicazione logicamente separato dagli altri, usato per la protezione dei dati.
OE.TRSF_DB	FCS_COP.1 (DB) FDP_ROL.1	FCS_COP.1 (DB) richiede la cifratura dei dati memorizzati sul Database centrale secondo l'algoritmo DES e con chiave 56 bit. FDP_ROL.1 richiede che l'accesso al Database centrale sia consentito solo agli utenti autorizzati e che l'ambiente IT permetta il rollback delle operazioni di scrittura qualora si verifichino eccezioni durante operazioni incluse in transazioni.

Obiettivi di sicurezza IT	Requisiti funzionali di sicurezza(SFR)	Motivazione
OE.DATI	FCS_COP.1 (WKS) FCS_COP.1 (DB) FDP_ROL.1 FTP_TRP.1	FCS_COP.1 (WKS) richiede la cifratura dei dati inviati al client secondo l'algoritmo DES e con chiave a 56 bit tramite il protocollo SSL. FCS_COP.1 (DB) richiede la cifratura dei dati memorizzati sul Database centrale secondo l'algoritmo DES e con chiave a 56 bit FDP_ROL.1 richiede che l'accesso al Database centrale sia consentito solo agli utenti autorizzati e che l'ambiente IT permetta il rollback delle operazioni di scrittura qualora si verifichino eccezioni durante operazioni incluse in transazioni. FTP_TRP.1 richiede che l'ambiente IT instauri con l'utente che si vuole autenticare, un canale di comunicazione logicamente separato dagli altri, usato per la protezione dei dati.

Tabella 8: Dimostrazione di sufficienza dei requisiti funzionali di sicurezza

8.2.2 Motivazione delle dipendenze tra i requisiti

La seguente tabella mostra l'analisi delle dipendenze dei requisiti funzionali di sicurezza individuati nell'ODV. Essi sono mostrati nella seconda colonna, mentre le dipendenze richieste dai CC sono mostrate nella terza colonna. L'ultima colonna mostra il numero del componente che supporta le dipendenze, in accordo con la numerazione della prima colonna. Se la dipendenza non è supportata nell'ultima colonna ci sarà un "N/A".

N. Componente	Requisiti funzionali del TDS	Dipendenze	Soddisfatto dal Componente N.
1.	FIA_AFL.1	FIA_UAU.1	4
2.	FIA_ATD.1	Nessuna	--
3.	FIA_UID.2	Nessuna	--
4.	FIA_UAU.2 (a)	FIA_UID.1	3
5.	FIA_UAU.7	FIA_UAU.1	4
6.	FIA_SOS.1	Nessuna	--
7.	FDP_ACC.1 (a)	FDP_ACF.1 (a)	9
8.	FDP_ACC.1 (b)	FDP_ACF.1 (b)	10
9.	FDP_ACF.1 (a)	FDP_ACC.1 FMT_MSA.3	7 12

N. Componente	Requisiti funzionali del TDS	Dipendenze	Soddisfatto dal Componente N.
10.	FDP_ACF.1 (b)	FDP_ACC.1 FMT_MSA.3	8 12
11.	FMT_MSA.1	[FDP_ACC.1 o FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	7 14 13
12.	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	11 13
13.	FMT_SMR.1	FIA_UID.1	3
14.	FMT_SMF.1	Nessuna	--
15.	FAU_GEN.1	FPT_STM.1	21
16.	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	15 3
17.	FAU_SAR.1	FAU_GEN.1	15
18.	FAU_SAR.2	FAU_SAR.1	17
19.	FAU_SAR.3	FAU_SAR.1	17
20.	FAU_SAA.1	FAU_GEN.1	15
21.	FPT_STM.1	Nessuna	--
22.	FIA_UAU.2 (b)	FIA_UID.1	3
23.	FCS_COP.1 (WKS)	[FDP_ITC.1 o FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	N/A N/A N/A
24.	FCS_COP.1 (DB)	[FDP_ITC.1 o FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	N/A N/A N/A
25.	FDP_ROL.1	[FDP_ACC.1 o FDP_IFC.1]	7 e 8
26.	FTP_TRP.1	Nessuna	--

Tabella 9: Dipendenze tra i requisiti

8.2.3 Motivazione delle dipendenze non supportate

FDP_ITC.1 è una dipendenza di FCS_COP.1 e non risulta supportata dall'ODV dal momento che non si possono importare dati privi di attributi di sicurezza.

FCS_CKM.4 è una dipendenza di FCS_COP.1 e non risulta supportata dal momento che non è prevista la distruzione delle chiavi all'interno dell'ODV.

FMT_MSA.2 è una dipendenza di FCS_COP.1 e non risulta supportata dal momento che l'ODV non effettua controlli di validità sugli attributi di sicurezza inseriti dall'amministratore o dal super-amministratore.

8.2.4 Dimostrazione di robustezza dei requisiti

La robustezza dei requisiti di sicurezza è di tipo SOF-high ed è consistente con gli obiettivi di sicurezza dell'ODV (cfr. O_CONTROLLO_ACCESSO). Il requisito funzionale per cui è appropriata una dichiarazione di robustezza è FIA_SOS.1 supportato da FIA_AFL.1.

8.2.5 Motivazione dei requisiti di garanzia di sicurezza

Questo TDS contiene i requisiti di garanzia di sicurezza per il livello EAL3 dei Common Criteria. Questo ODV è stato sviluppato per un ambiente specifico, per il quale si assume un livello medio di rischio sui beni. Si assume che l'ambiente dell'ODV sia fisicamente sicuro. L'ODV può essere configurato soltanto durante la fase di inizializzazione. Per tali motivazioni si ritiene che il livello EAL3 sia appropriato per garantire la sicurezza delle funzioni offerte dall'ODV.

8.3. MOTIVAZIONE DEI REQUISITI ESPLICITI

In questo TDS non ci sono requisiti di sicurezza espressi in modo esplicito.

8.4. MOTIVAZIONE DEL SOMMARIO DELLE SPECIFICHE

8.4.1 Motivazione delle funzioni di sicurezza IT

Funzioni di Sicurezza Requisiti Funzionali di Sicurezza	ODV.Autenticazione	ODV.ControlloAccessi	ODV.Audit
FIA_AFL.1	X		
FIA_ATD.1		X	
FIA_UID.2	X		
FIA_UAU.2 (a)	X		
FIA_UAU.7	X		
FIA_SOS.1	X		
FDP_ACC.1 (a)		X	
FDP_ACC.1 (b)		X	X
FDP_ACF.1 (a)		X	
FDP_ACF.1 (b)		X	X
FMT_MSA.1		X	
FMT_MSA.3		X	
FMT_SMR.1		X	
FMT_SMF.1		X	
FAU_GEN.1			X
FAU_GEN.2			X
FAU_SAR.1		X	X
FAU_SAR.2		X	X
FAU_SAR.3			X
FAU_SAA.1			X

Tabella 10: Mapping tra requisiti funzionali di sicurezza e funzioni di sicurezza

I requisiti funzionali di sicurezza appaiono sulla sinistra di ogni riga. Le funzioni corrispondenti sono indicate con una 'X' nella colonna appropriata.
La seguente tabella descrive il modo in cui le funzioni di sicurezza IT coprono i corrispondenti requisiti funzionali di sicurezza.

Requisiti funzionali di sicurezza	Funzioni di sicurezza IT	Mapping
FIA_AFL.1	**ODV.Autenticazione**	L'ODV impone l'autenticazione di tutti gli utenti tramite username e password; il numero massimo di tentativi di autenticazione falliti non deve superare un numero massimo predefinito.
FIA_ATD.1	**ODV.ControlloAccessi**	L'ODV permette ad ogni utente autenticato di accedere soltanto a determinate operazioni o alle sole funzionalità/schermate/pulsanti/dati previsti dal profilo al quale l'utente risulta associato.
FIA_UID.2	**ODV.Autenticazione**	L'ODV impone l'identificazione di tutti gli utenti tramite username e password oppure tramite i dati anagrafici estratti dalla Smart Card (dopo l'autenticazione effettuata dall'ambiente tramite Smart Card e PIN).
FIA_UAU.2(a)	**ODV.Autenticazione**	L'ODV impone l'autenticazione di tutti gli utenti tramite username e password.
FIA_UAU.7	**ODV.Autenticazione**	Durante l'autenticazione degli utenti tramite username e password l'ODV mostra a video soltanto il numero di caratteri inseriti (sostituisce i caratteri con un carattere "segnaposto").
FIA_SOS.1	**ODV.Autenticazione**	L'ODV impone l'autenticazione di tutti gli utenti tramite username e password; l'ODV verifica le password degli utenti secondo una specifica Politica delle Password .
FDP_ACC.1 (a)	**ODV.ControlloAccessi**	L'ODV permette ad ogni utente autenticato di accedere soltanto a determinate operazioni o alle sole funzionalità previste dal profilo al quale l'utente risulta associato.
FDP_ACC.1 (b)	**ODV.ControlloAccessi**	L'ODV permette ad ogni utente autenticato di accedere soltanto a determinate operazioni o alle sole funzionalità previste dal profilo al quale l'utente risulta associato.

Requisiti funzionali di sicurezza	Funzioni di sicurezza IT	Mapping
	ODV.Audit	L'ODV consente la registrazione di tutte le operazioni eseguite dall'ODV all'interno di un archivio di audit. Solo gli utenti autorizzati possono consultare i dati di audit, in sola lettura e stampa.
FDP_ACF.1 (a)	**ODV.ControlloAccessi**	L'ODV permette ad ogni utente autenticato di accedere soltanto a determinate operazioni o alle sole funzionalità previste dal profilo al quale l'utente risulta associato.
FDP_ACF.1 (b)	**ODV.ControlloAccessi**	L'ODV permette ad ogni utente autenticato di accedere soltanto a determinate operazioni o alle sole funzionalità previste dal profilo al quale l'utente risulta associato.
	ODV.Audit	L'ODV consente la registrazione di tutte le operazioni eseguite dall'ODV all'interno di un archivio di audit. Solo gli utenti autorizzati possono consultare i dati di audit, in sola lettura e stampa.
FMT_MSA.1	**ODV.ControlloAccessi**	L'ODV permette ad ogni utente autenticato di accedere soltanto a determinate operazioni o alle sole funzionalità previste dal profilo al quale l'utente risulta associato.
FMT_MSA.3	**ODV.ControlloAccessi**	L'ODV permette ad ogni utente autenticato di accedere soltanto alle sole funzionalità previste dal profilo al quale l'utente risulta associato.
FMT_SMR.1	**ODV.ControlloAccessi**	L'ODV permette ad ogni utente autenticato di accedere soltanto a determinate operazioni, in base agli attributi di sicurezza definiti in modo restrittivo dall'amministratore/super-amministratore.
FMT_SMF.1	**ODV.ControlloAccessi**	L'ODV permette all'amministratore di modificare le date di validità di un profilo, disabilitandolo, in caso di gravi situazioni di errore.
FAU_GEN.1	**ODV.Audit**	L'ODV consente la registrazione di tutte le operazioni eseguite dall'ODV

Requisiti funzionali di sicurezza	Funzioni di sicurezza IT	Mapping
		all'interno di un archivio di audit.
FAU_GEN.2	**ODV.Audit**	L'ODV consente la registrazione di tutte le operazioni eseguite dall'ODV all'interno di un archivio di audit.
FAU_SAR.1	**ODV.ControlloAccessi**	L'ODV permette ad ogni utente autenticato di accedere soltanto a determinate operazioni o alle sole funzionalità previste dal profilo al quale l'utente risulta associato.
	ODV.Audit	L'ODV consente la registrazione di tutte le operazioni eseguite dall'ODV all'interno di un archivio di audit. Solo gli utenti autorizzati possono consultare i dati di audit, in sola lettura e stampa.
FAU_SAR.2	**ODV.ControlloAccessi**	L'ODV permette ad ogni utente autenticato di accedere soltanto a determinate operazioni o alle sole funzionalità previste dal profilo al quale l'utente risulta associato.
	ODV.Audit	L'ODV consente la registrazione di tutte le operazioni eseguite dall'ODV all'interno di un archivio di audit. Solo gli utenti autorizzati possono consultare i dati di audit, in sola lettura e stampa.
FAU_SAR.3	**ODV.Audit**	L'ODV consente la registrazione di tutte le operazioni eseguite dall'ODV all'interno di un archivio di audit. Solo gli utenti autorizzati possono consultare i dati di audit. L'ODV consente di definire i criteri di ricerca delle informazioni da visualizzare o stampare.
FAU_SAA.1	**ODV.Audit**	L'ODV consente la registrazione di tutte le operazioni eseguite dall'ODV all'interno di un archivio di audit. Solo gli utenti autorizzati possono consultare i dati di audit, in sola lettura e stampa per identificare eventuali violazioni della sicurezza.

Tabella 11: Corrispondenza tra requisiti e funzioni di sicurezza

8.4.2 Motivazione della robustezza delle funzioni

La robustezza della funzione di sicurezza di identificazione/autenticazione **ODV.Autenticazione**, realizzata tramite il meccanismo di username e password, è alta. Questo significa che tale meccanismo è resistente ad un attacco con un elevato potenziale. Tutti i dettagli di chiarimento saranno forniti nella documentazione relativa.

8.4.3 Motivazione delle misure di garanzia

Il mapping tra le misure di garanzia e i requisiti di garanzia di sicurezza possono essere trovati nella sezione 6.2.

8.5. MOTIVAZIONE DELLA CONFORMITA' AL PP

Vedere sezione 7.