

# FarmaByte

Lorenzo Guerra 00880376

Guglielmo Palaferri 00873714

Giacomo Romanini 00874849

Luglio 2021

# Indice

<b>1</b>	<b>Abstract</b>	<b>1</b>
<b>2</b>	<b>Documento dei Requisiti</b>	<b>2</b>
2.1	Raccolta dei requisiti . . . . .	2
2.2	Tabella dei Requisiti . . . . .	3
2.3	Analisi dei Requisiti . . . . .	4
2.3.1	Vocabolario . . . . .	4
2.3.2	Casi d'uso della farmacia . . . . .	5
2.3.3	Scenari . . . . .	6
2.4	Analisi del Rischio . . . . .	13
2.4.1	Tabella Valutazione dei Beni . . . . .	13
2.4.2	Tabella Minacce/Controlli . . . . .	14
2.4.3	Analisi Tecnologica della Sicurezza . . . . .	14
2.4.4	Security Use Case & Misuse Case . . . . .	15
2.4.5	Security Use Case & Misuse Case Scenari . . . . .	16
2.4.6	Requisiti di Protezione dei Dati . . . . .	17
<b>3</b>	<b>Analisi del Problema</b>	<b>18</b>
3.1	Analisi Documento dei Requisiti: Analisi delle Funzionalità . . . . .	18
<b>4</b>	<b>Progettazione</b>	<b>19</b>
4.1	Progettazione Architettuale . . . . .	19
4.1.1	Requisiti non funzionali . . . . .	19
4.1.2	Scelta dell'architettura . . . . .	19
4.1.3	Pattern architeturali e di design . . . . .	20
4.2	Progettazione di dettaglio . . . . .	22
4.2.1	Struttura . . . . .	22

# 1 Abstract

Il progetto riguarda la creazione di un applicativo software per la gestione interna dell'inventario delle farmacie e per l'interfacciamento con i clienti. Il cliente ha la possibilità di cercare quale sia la farmacia più vicina ad avere un certo medicinale e, dopo essersi autenticato, può inviare una prenotazione del farmaco. La farmacia quindi può ricevere la prenotazione del cliente registrato al servizio che verrà poi finalizzata in acquisto. Inoltre la gestione dell'inventario del negozio permette alle farmacie di controllare l'elenco dei farmaci disponibili e ne facilita la gestione degli ordini e delle rimanenze, segnalando all'operatore le medicine in scadenza e in esaurimento. L'applicativo fornisce anche una funzionalità di ricerca farmaci, per i clienti che desiderano verificare la disponibilità di un farmaco in una certa località.

## 2 Documento dei Requisiti

### 2.1 Raccolta dei requisiti

- I clienti delle farmacie hanno a disposizione due servizi: controllare se un farmaco è disponibile vicino alla loro posizione e/o prenotarlo.
- Il cliente fornisce la sua posizione che l'applicativo userà per indicargli le farmacie più vicine. Contemporaneamente specificherà il farmaco da cercare e l'applicativo fornirà le 10 farmacie più vicine ad averlo in magazzino indicandone se è disponibile o sta per terminare.
- Per la prenotazione è necessario possedere un account
- La prenotazione sarà composta da uno o più farmaci, dalla farmacia, e dal giorno.
- L'account viene creato in due fasi: 1. Registrazione con nome, cognome, password, data di nascita, email e codice fiscale 2. Autenticazione di persona in farmacia
- La email deve essere univoca, la password di almeno 8 caratteri, contenente almeno un numero e un carattere alfabetico.
- Per l'autenticazione è necessario mostrare il tesserino sanitario per l'identificazione in farmacia.
- Il cliente può vedere la lista delle sue prenotazioni in corso
- Il farmacista vede le prenotazioni, i farmaci disponibili in negozio e viene segnalato riguardo ai farmaci in esaurimento
- Il farmacista può confermare le prenotazioni andate a buon fine
- Se alla fine della giornata un utente non si presenta allora l'evento viene registrato, per poi avvisare il farmacista che può eventualmente bloccare l'utente per 1 mese.
- Il sistema sarà ovviamente distribuito e di natura client-server con la presenza di un database centrale dove memorizzare i dati
- La gestione delle vendite, degli ordini e modifiche di magazzino è gestita da un altro software
- Non va considerata la gestione dei dati del personale

## 2.2 Tabella dei Requisiti

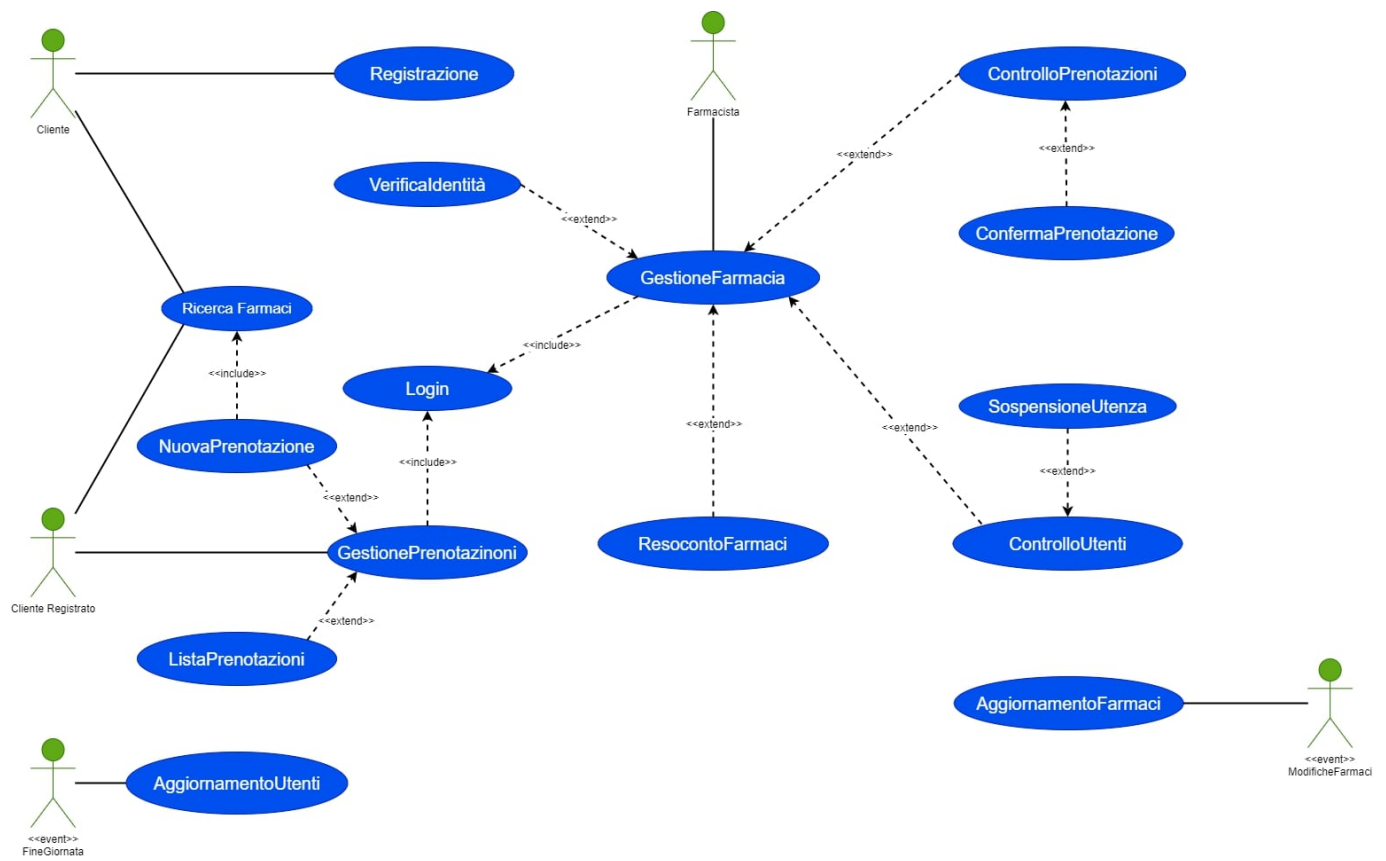
ID	Requisiti	Tipo
R1F	Localizzazione delle farmacie più vicine in base al farmaco da cercare	Funzionale
R2F	Specifica del farmaco da cercare da parte dell'utente	Funzionale
R3F	Presentazione delle farmacie che dispongono di un farmaco	Funzionale
R4F	Registrazione di un account tramite l'interfaccia web	Funzionale
R5F	Attivazione dell'account con identificazione fisica dell'utente con documento	Funzionale
R6F	La prenotazione sarà composta da uno o più farmaci, dalla farmacia e dal giorno	Funzionale
R7F	Identificazione attraverso email univoca e password di almeno 8 caratteri, contenente almeno un carattere alfabetico e un carattere numerico	Funzionale
R8F	Visualizzazione delle prenotazioni del cliente	Funzionale
R9F	Visualizzazione delle prenotazioni della farmacia	Funzionale
R10F	Visualizzazione del numero dei farmaci disponibili	Funzionale
R11F	Notifica dei farmaci in esaurimento o in scadenza	Funzionale
R12F	Conferma della prenotazione andata a buon fine	Funzionale
R13F	Notifica della mancata finalizzazione in acquisto di una prenotazione	Funzionale
R14F	Blocco dell'utente che effettua troppe prenotazioni senza presentarsi	Funzionale
R15F	Verrà memorizzato il numero di prenotazioni andate a buon fine	Funzionale
R1NF	Velocità di memorizzazione dei dati	Non Funzionale
R2NF	Velocità della ricerca dei dati	Non Funzionale
R3NF	Semplicità dell'interfaccia	Non Funzionale
R4NF	Un utente non può avere più di un account verificato	Non Funzionale
R5NF	la gestione delle vendite e ordini è gestita da un altro software	Non Funzionale
R6NF	Per prenotare l'utente deve essere registrato	Non Funzionale
R7NF	La gestione delle vendite, degli ordini e modifiche di magazzino è gestita da un altro software	Non Funzionale
R8NF	Non va considerata la gestione dei dati del personale	Non Funzionale

## 2.3 Analisi dei Requisiti

### 2.3.1 Vocabolario

Voce	Definizione	Sinonimi
Cliente	Persona che usufruisce del servizio lato cliente	Utente
ClienteRegistrato	Cliente che possiede un account identificato con cui può effettuare prenotazioni	UtenteRegistrato
Farmacia	Farmacia che aderisce al servizio	Punto vendita
Farmaco	Medicinale che viene venduto in farmacia	
Farmacista	Utente che accede con le credenziali della farmacia	Operatore
Prenotazione	Richiesta di farmaci da comprare in negozio	
Data e ora prenotazione	Indicazione temporale del momento in cui avverrà la prenotazione	
Posizione	Luogo della ricerca o collocamento geografico della farmacia	
Credenziali	Insieme composto da email e password necessari per accedere al sistema	
Email	Indirizzo di posta elettronica del cliente utilizzata anche per l'autenticazione	
Password	Codice alfanumerico di almeno 8 caratteri	
Magazzino	Luogo fisico in cui vengono conservati i farmaci di un punto vendita	Deposito

## 2.3.2 Casi d'uso della farmacia



### 2.3.3 Scenari

<b>Titolo</b>	GestioneFarmacia
<b>Descrizione</b>	Gestione dell'utenza di un cliente registrato
<b>Attori</b>	Farmacista
<b>Relazioni</b>	Login, SospensioneUtenza, VerificaIdentità, ResocontoFarmaci, ResocontoPrenotazioni
<b>Precondizioni</b>	
<b>Postcondizioni</b>	
<b>Scenario Principale</b>	1. Login 2. Il farmacista può eseguire la verifica, sospendere un'account, controllare le prenotazioni e i farmaci in magazzino
<b>Scenari Alternativi</b>	
<b>Requisiti non funzionali</b>	Velocità di ricerca dei dati e semplicità di navigazione tra le diverse maschere
<b>Punti aperti</b>	

<b>Titolo</b>	ResocontoUtenti
<b>Descrizione</b>	Si controllano gli utenti con potenzialmente sospendibili
<b>Attori</b>	Farmacista
<b>Relazioni</b>	SospensioneUtenza, GestioneFarmacia
<b>Precondizioni</b>	
<b>Postcondizioni</b>	Viene mostrato l'elenco degli Utenti a rischio sospensione
<b>Scenario Principale</b>	1. Il Farmacista va nella schermata di visualizzazione utenti 2. Il sistema recupera l'elenco degli utenti a rischio 3. Il sistema mostra a video l'elenco degli utenti
<b>Scenari Alternativi</b>	
<b>Requisiti non funzionali</b>	Velocità di ricerca dei dati e semplicità di navigazione tra le diverse maschere
<b>Punti aperti</b>	

<b>Titolo</b>	ResocontoFarmaci
<b>Descrizione</b>	Viene mostrato l'elenco dei farmaci in scadenza o in esaurimento
<b>Attori</b>	Farmacista
<b>Relazioni</b>	GestioneFarmacia
<b>Precondizioni</b>	
<b>Postcondizioni</b>	Viene mostrato l'elenco degli Utenti a rischio sospensione
<b>Scenario Principale</b>	1. Il Farmacista va nella schermata di visualizzazione farmaci 2. Il sistema recupera l'elenco dei farmaci in esaurimento o in scadenza 3. Il sistema mostra a video l'elenco richiesto
<b>Scenari Alternativi</b>	
<b>Requisiti non funzionali</b>	Velocità di ricerca dei dati e semplicità di navigazione tra le diverse maschere
<b>Punti aperti</b>	



<b>Titolo</b>	ControlloPrenotazioni
<b>Descrizione</b>	Si controllano le prenotazioni non terminate
<b>Attori</b>	Farmacista
<b>Relazioni</b>	ConfermaPrenotazione,GestioneFarmacia
<b>Precondizioni</b>	
<b>Postcondizioni</b>	Viene mostrato l'elenco delle prenotazioni
<b>Scenario principale</b>	1. Il Farmacista va nella schermata di visualizzazione prenotazioni 2. Il sistema recupera l'elenco delle prenotazioni giornaliere 3. Il sistema mostra a video l'elenco delle prenotazioni
<b>Scenari Alternativi</b>	
<b>Requisiti non funzionali</b>	Velocità di ricerca dei dati
<b>Punti aperti</b>	

<b>Titolo</b>	ConfermaPrenotazione
<b>Descrizione</b>	Il Farmacista conferma la prenotazione avvenuta
<b>Attori</b>	Farmacista
<b>Relazioni</b>	ControlloPrenotazioni
<b>Precondizioni</b>	
<b>Postcondizioni</b>	La prenotazione viene confermata
<b>Scenario principale</b>	1. ControlloPrenotazioni 2. Il Farmacista conferma l'avvenuta prenotazione
<b>Scenari Alternativi</b>	
<b>Requisiti non funzionali</b>	Semplicità dell'interfaccia
<b>Punti aperti</b>	

<b>Titolo</b>	Registrazione
<b>Descrizione</b>	Il cliente si registra al servizio
<b>Attori</b>	Cliente
<b>Relazioni</b>	
<b>Precondizioni</b>	Il cliente dispone di un codice fiscale valido
<b>Postcondizioni</b>	Il cliente è registrato nel sistema ed è posto in attesa della verifica
<b>Scenario principale</b>	1. Il cliente accede alla sezione di registrazione 2. Il cliente inserisce i propri dati: nome, cognome, data di nascita, email e il codice fiscale 3. Il cliente termina la registrazione, se avvenuta con successo gli viene mostrata la conferma e viene reindirizzato alla pagina principale
<b>Scenari Alternativi</b>	Scenario a: il codice fiscale è già registrato 3. Il sistema verifica che è già presente un utente con quel codice fiscale, quindi notifica il cliente con un messaggio di errore.
<b>Requisiti non funzionali</b>	Semplicità dell'interfaccia
<b>Punti aperti</b>	

<b>Titolo</b>	VerificaIdentità
<b>Descrizione</b>	Verifica dell'identità dell'utente registrato
<b>Attori</b>	Cliente, Farmacista
<b>Relazioni</b>	GestioneFarmacia
<b>Precondizioni</b>	Il cliente è registrato
<b>Postcondizioni</b>	L'utente è stato verificato e il suo account viene abilitato per effettuare delle prenotazioni
<b>Scenario principale</b>	<ol style="list-style-type: none"> <li>1. Il cliente va in farmacia con il documento specificato in fase di registrazione</li> <li>2. Il cliente viene identificato dal farmacista</li> <li>3. Il farmacista chiede al sistema di recuperare l'utente</li> <li>4. Il farmacista attiva l'account dell'utente</li> </ol>
<b>Scenari alternativi</b>	4. Il sistema non trova nessun utente, segnala il farmacista
<b>Requisiti non funzionali</b>	Velocità di memorizzazione e semplicità di navigazione tra le diverse maschere
<b>Punti aperti</b>	

<b>Titolo</b>	SospensioneUtenza
<b>Descrizione</b>	Se un utente non ha concluso troppe prenotazioni allora viene proposta la sospensione dell'utente al farmacista
<b>Attori</b>	Farmacista
<b>Relazioni</b>	ResocontoPrenotazioni, GestioneFarmacia
<b>Precondizioni</b>	Il cliente è diffidato dal sistema (ha molte prenotazioni non concluse)
<b>Postcondizioni</b>	Il cliente non può più effettuare prenotazioni per 30 giorni
<b>Scenario principale</b>	<ol style="list-style-type: none"> <li>1. Si verifica l'evento FineGiornata</li> <li>2. Il Sistema recupera l'elenco delle prenotazioni e lo analizza</li> <li>3. Se il Sistema rileva un numero eccessivo di prenotazioni non concluse per un determinato utente, allora lo segnala al farmacista</li> <li>4. Il farmacista, se ritiene necessario, può confermare la sospensione dell'utente</li> </ol>
<b>Scenari alternativi</b>	
<b>Requisiti non funzionali</b>	Velocità nella ricerca dei dati e semplicità dell'interfaccia
<b>Punti aperti</b>	

<b>Titolo</b>	ResocontoPrenotazioni
<b>Descrizione</b>	Si controllano le prenotazioni non terminate per utente
<b>Attori</b>	Farmacista, FineGiornata
<b>Relazioni</b>	Resoconto, SospensioneUtenza, GestioneFarmacia
<b>Precondizioni</b>	
<b>Postcondizioni</b>	Viene mostrato l'elenco delle prenotazioni
<b>Scenario principale</b>	1. Il Farmacista va nella schermata di visualizzazione farmaci 2. Il sistema recupera l'elenco delle prenotazioni giornaliere 3. Il sistema mostra a video l'elenco delle prenotazioni
<b>Scenari Alternativi</b>	
<b>Requisiti non funzionali</b>	Velocità di ricerca dei dati e semplicità di navigazione tra le diverse maschere
<b>Punti aperti</b>	

<b>Titolo</b>	RicercaFarmaci
<b>Descrizione</b>	L'utente verifica la disponibilità di un particolare farmaco nelle farmacie più vicine a lui
<b>Attori</b>	Cliente
<b>Relazioni</b>	
<b>Precondizioni</b>	
<b>Postcondizioni</b>	Si visualizza la lista delle farmacie con disponibilità
<b>Scenario principale</b>	<ol style="list-style-type: none"> <li>1. Il cliente si reca nella pagina di ricerca</li> <li>2. Il cliente inserisce il nome del farmaco per cui eseguire la ricerca</li> <li>3. Il sistema ottiene la lista delle farmacie aventi il farmaco specificato entro un range dalla località specificata.</li> <li>4. Il sistema ordina la lista in base alla distanza geografica dalla zona dell'utente, in ordine crescente</li> <li>5. La lista viene mostrata all'utente</li> </ol>
<b>Scenari Alternativi</b>	<p>Scenario alternativo A:</p> <ol style="list-style-type: none"> <li>1. Il cliente registrato effettua il login</li> <li>2. Il cliente si reca nella pagina di ricerca</li> <li>3. Il cliente inserisce il nome del farmaco per cui eseguire la ricerca</li> <li>4. Il sistema ottiene la lista delle farmacie aventi il farmaco specificato entro un range dalla località specificata.</li> <li>5. Il sistema ordina la lista in base alla distanza geografica dalla zona dell'utente, in ordine crescente</li> <li>6. La lista viene mostrata all'utente</li> <li>7. L'utente può selezionare il farmaco per cominciare una prenotazione di quel farmaco nella farmacia scelta</li> </ol> <p>Scenario alternativo B:</p> <ol style="list-style-type: none"> <li>1. Il cliente registrato effettua il login</li> <li>2. Il cliente avvia una nuova prenotazione dalla home</li> <li>3. Il cliente seleziona la farmacia in cui effettuare la prenotazione</li> <li>4. Il cliente inserisce il nome del farmaco per cui eseguire la ricerca</li> <li>5. Il sistema ottiene la lista dei farmaci disponibili nella farmacia scelta il cui nome inizia per il testo inserito dall'utente</li> <li>6. La lista viene mostrata all'utente</li> <li>7. L'utente può selezionare il farmaco corrispondente, se è presente nella lista, ed aggiungerlo alla prenotazione in corso</li> </ol>
<b>Requisiti non funzionali</b>	Velocità di ricerca dei dati e semplicità di navigazione tra le diverse maschere
<b>Punti aperti</b>	

<b>Titolo</b>	NuovaPrenotazione
<b>Descrizione</b>	L'utente prenota a suo nome una lista di farmaci
<b>Attori</b>	ClienteRegistrato
<b>Relazioni</b>	GestionePrenotazioni
<b>Precondizioni</b>	
<b>Postcondizioni</b>	Il sistema ha memorizzato i dati della prenotazione, in attesa di conferma da parte della farmacia
<b>Scenario principale</b>	<ol style="list-style-type: none"> <li>1. Il cliente esegue il <b>Login</b></li> <li>2. Il cliente seleziona i farmaci che vuole prenotare, la quantità, e inserisce la data di ritiro desiderata</li> <li>3. Il cliente invia la richiesta di prenotazione</li> <li>4. Il sistema pone la richiesta in attesa di conferma</li> </ol>
<b>Scenari Alternativi</b>	<p>Scenario a: La farmacia non dispone dei farmaci richiesti.</p> <ol style="list-style-type: none"> <li>4. Il sistema nota che la farmacia non ha disponibilità di almeno uno dei farmaci specificati</li> <li>5. Viene inviato al cliente un messaggio di errore</li> </ol>
<b>Requisiti non funzionali</b>	Velocità di verifica dei dati e semplicità di navigazione tra le diverse maschere
<b>Punti aperti</b>	

<b>Titolo</b>	ListaPrenotazioni
<b>Descrizione</b>	L'utente ottiene la lista delle proprie prenotazioni passate ed in corso
<b>Attori</b>	ClienteRegistrato
<b>Relazioni</b>	GestionePrenotazioni
<b>Precondizioni</b>	
<b>Postcondizioni</b>	Al cliente viene mostrata la lista delle prenotazioni passate ed in corso
<b>Scenario Principale</b>	<ol style="list-style-type: none"> <li>1. Il cliente esegue il Login</li> <li>2. Il cliente seleziona l'opzione di visualizzazione della lista delle prenotazioni</li> <li>3. Al cliente viene mostrato l'elenco delle prenotazioni effettuate</li> </ol>
<b>Scenari Alternativi</b>	
<b>Requisiti non funzionali</b>	Velocità di verifica dei dati e semplicità di navigazione tra le diverse maschere
<b>Punti aperti</b>	

<b>Titolo</b>	GestionePrenotazioni
<b>Descrizione</b>	Gestione delle prenotazioni di un cliente registrato
<b>Attori</b>	ClienteRegistrato
<b>Relazioni</b>	Login, ListaPrenotazioni, NuovaPrenotazione
<b>Precondizioni</b>	
<b>Postcondizioni</b>	
<b>Scenario Principale</b>	1. Il cliente registrato esegue il login 2. Il cliente può visualizzare le proprie prenotazioni passate o in corso e può effettuare nuove prenotazioni.
<b>Scenari Alternativi</b>	
<b>Requisiti non funzionali</b>	Velocità di verifica dei dati e semplicità di navigazione tra le diverse maschere
<b>Punti aperti</b>	

<b>Titolo</b>	Login
<b>Descrizione</b>	Permette di accedere al sistema
<b>Attori</b>	ClienteRegistrato, Farmacista
<b>Relazioni</b>	NuovaPrenotazione, GestioneFarmacia
<b>Precondizioni</b>	
<b>Postcondizioni</b>	L'utente ha accesso al sistema, limitato in base ai suoi privilegi
<b>Scenario principale</b>	1. L'utente inserisce le credenziali di accesso 2. Il sistema verifica le credenziali 3. Se le credenziali sono corrette, viene presentata la schermata iniziale
<b>Scenari Alternativi</b>	Scenario a: Credenziali non riconosciute. 3. Il sistema non riconosce le credenziali e rispedisce l'utente alla schermata di login con un messaggio di errore
<b>Requisiti non funzionali</b>	Velocità di verifica delle credenziali
<b>Punti aperti</b>	

<b>Titolo</b>	AggiornamentoUtenti
<b>Descrizione</b>	Aggiorna l'elenco degli utenti a rischio sospensione
<b>Attori</b>	FineGiornata
<b>Relazioni</b>	
<b>Precondizioni</b>	
<b>Postcondizioni</b>	Il DataBase degli utenti è aggiornato
<b>Scenario principale</b>	1. Si verifica l'evento FineGiornata 2. Il sistema controlla le prenotazioni non andate a buon fine 3. Il sistema aggiorna i dati relativi alle infrazioni degli utenti
<b>Scenari Alternativi</b>	
<b>Requisiti non funzionali</b>	Velocità della ricerca dei dati
<b>Punti aperti</b>	

<b>Titolo</b>	Aggiornamento Farmaci
<b>Descrizione</b>	Aggiorna l'elenco dei farmaci in magazzino
<b>Attori</b>	ModificheFarmaci
<b>Relazioni</b>	
<b>Precondizioni</b>	
<b>Postcondizioni</b>	Il DataBase dei farmaci è aggiornato
<b>Scenario principale</b>	1. Si verifica l'evento ModificheFarmaci 2. Il sistema recupera le modifiche dal DataBase Remoto 3. Il sistema aggiorna i dati relativi ai farmaci in magazzino
<b>Scenari Alternativi</b>	
<b>Requisiti non funzionali</b>	Velocità della ricerca dei dati
<b>Punti aperti</b>	

## 2.4 Analisi del Rischio

### 2.4.1 Tabella Valutazione dei Beni

<b>Bene</b>	<b>Valore</b>	<b>Esposizione</b>
Sistema Informativo	Alto. Fondamentale per il funzionamento del servizio	Alta. Perdita finanziaria e di immagine
Informazioni dei clienti	Alto. Dati generali dei clienti della farmacia, comprese le credenziali	Alta. Perdita di immagine dovuta alla divulgazione di dati sensibili
Informazioni relative al personale	Alto. Dati relativi ai farmacisti, incluse le credenziali di accesso all'area riservata	Molto Alta. Perdita finanziaria dovuta a usi impropri delle credenziali con privilegi elevati. Perdita di immagine possibile con la divulgazione dei dati relativi ai clienti
Dati delle prenotazioni	Alto. Necessario per tenere traccia delle prenotazioni	Molto Alta. Perdita finanziaria dovuta allo smarrimento di prenotazioni. Perdita di immagine con la divulgazione dei farmaci prenotati dai clienti

### 2.4.2 Tabella Minacce/Controlli

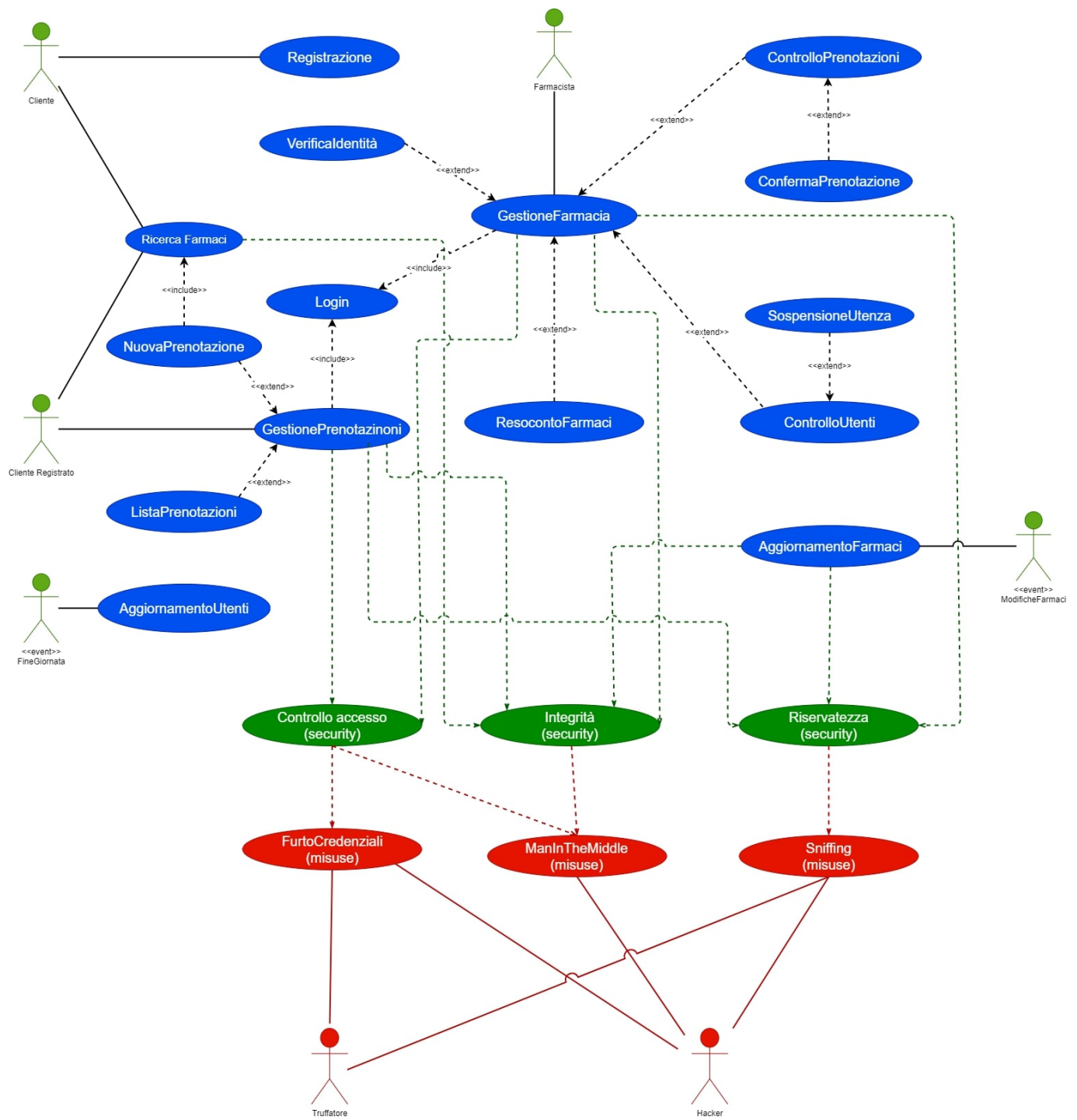
Minaccia	Probabilità	Controllo	Fattibilità
Furto credenziali Farmacista	Alta	Controllo sulla sicurezza della password - Log delle operazioni	Costo implementativo molto basso
Furto credenziali Cliente	Alta	Controllo sulla sicurezza della password - Log delle operazioni	Costo implementativo molto basso
Alterazione o intercettazione delle comunicazioni	Alta	Utilizzo di un canale sicuro - Log delle operazioni	Basso costo di realizzazione con determinati protocolli
Accesso non autorizzato al database	Bassa	Accesso da macchine sicure - Log di tutte le operazioni	Basso costo di realizzazione, il server deve essere ben custodito
DoS	Bassa	Controllo e limitazione delle richieste	Media complessità di implementazione
Saturazione del database	Bassa	1. Limitazione delle richieste in un dato intervallo di tempo. 2. Limite di tempo per la verifica di un cliente	Media complessità di implementazione

### 2.4.3 Analisi Tecnologica della Sicurezza

Tecnologia	Vulnerabilità
Autenticazione email/password	<ul style="list-style-type: none"> <li>• Utente rivela volontariamente la password Utente rivela la password con un attacco di ingegneria sociale</li> <li>• Utente non esce dal sistema dopo aver eseguito le operazioni</li> <li>• Password banali</li> </ul>
Cifratura comunicazioni	<ul style="list-style-type: none"> <li>• In caso di cifratura simmetrica particolare attenzione va alla lunghezza delle chiavi ed alla loro memorizzazione</li> <li>• La memorizzazione è un fattore fondamentale anche nella cifratura asimmetrica</li> </ul>
Architettura Client/Server	<ul style="list-style-type: none"> <li>• DoS</li> <li>• Man in the Middle</li> <li>• Sniffing delle comunicazioni</li> </ul>



## 2.4.4 Security Use Case & Misuse Case



## 2.4.5 Security Use Case & Misuse Case Scenari

<b>Titolo</b>	Riservatezza
<b>Descrizione</b>	I dati non sono accessibili da chi non ne ha i permessi
<b>Misuse case</b>	Sniffing
<b>Relazioni</b>	
<b>Precondizioni</b>	L'attaccante ha i mezzi per intercettare i messaggi del sistema
<b>Postcondizioni</b>	Il sistema impedisce all'attaccante di decifrare (in tempi utili) i messaggi intercettati
<b>Scenario principale</b>	<ol style="list-style-type: none"> <li>1. Il Sistema protegge i messaggi</li> <li>2. L'attaccante riesce ad intercettare un messaggio</li> <li>3. L'attaccante prova a decifrare i messaggi, ma non riesce a trovare un modo per farlo abbastanza velocemente</li> </ol>
<b>Scenari di un attacco avvenuto con successo</b>	<ol style="list-style-type: none"> <li>1. Il Sistema protegge i messaggi</li> <li>2. L'attaccante riesce ad intercettare un messaggio</li> <li>3. L'attaccante riesce a decifrare i messaggi e a leggerne il contenuto, ma solamente per una sessione di un utente</li> </ol>

<b>Titolo</b>	Integrità
<b>Descrizione</b>	Integrità dei dati del sistema
<b>Misuse case</b>	ManInTheMiddle
<b>Relazioni</b>	
<b>Precondizioni</b>	<ol style="list-style-type: none"> <li>1. L'attaccante ha i mezzi per intercettare i messaggi del sistema</li> <li>2. L'attaccante ha i mezzi per modificare i messaggi</li> <li>3. L'attaccante ha i mezzi per spedire il messaggio modificato al destinatario</li> </ol>
<b>Postcondizioni</b>	Il sistema rileva il messaggio contraffatto
<b>Scenario principale</b>	<ol style="list-style-type: none"> <li>1. Il Sistema protegge i messaggi</li> <li>2. L'attaccante riesce ad intercettare un messaggio e lo modifica</li> <li>3. Il sistema si accorge del messaggio contraffatto e lo segna nei log</li> </ol>
<b>Scenari di un attacco avvenuto con successo</b>	<ol style="list-style-type: none"> <li>1. Il Sistema protegge i messaggi</li> <li>2. L'attaccante riesce ad intercettare un messaggio e lo modifica</li> <li>3. Il sistema accetta il messaggio e agisce di conseguenza, segnando il messaggio nei log</li> </ol>

<b>Titolo</b>	ControlloAccessi
<b>Descrizione</b>	L'accesso alle funzionalità del sistema deve essere controllato
<b>Misuse case</b>	FurtoCredenziali, ManInTheMiddle
<b>Relazioni</b>	
<b>Precondizioni</b>	L'attaccante ha i mezzi per carpire in tutto o in parte le credenziali di accesso di un cliente o di un farmacista
<b>Postcondizioni</b>	Il sistema blocca l'accesso non autorizzato e notifica il tentativo di accesso
<b>Scenario principale</b>	<ol style="list-style-type: none"> <li>1. L'attaccante tenta di accedere al servizio spacciandosi per un utente legittimo, di cui conosce le credenziali solo in parte (ad esempio mediante attacco con dizionario)</li> <li>2. Il sistema non riconosce le credenziali, restituendo un errore</li> <li>3. In seguito ad un numero fissato di tentativi falliti, il sistema blocca temporaneamente l'accesso a quell'utente e notifica l'anomalia a chi di dovere</li> </ol>
<b>Scenari di un attacco avvenuto con successo</b>	<ol style="list-style-type: none"> <li>1. L'attaccante riesce a carpire le credenziali di accesso complete di un utente in un qualsiasi modo</li> <li>2. Il sistema riconosce la correttezza delle credenziali, e fornisce l'accesso al soggetto malevolo</li> <li>3. L'attaccante ha libero accesso al sistema, con privilegi diversi in base al tipo di utente</li> </ol>

#### 2.4.6 Requisiti di Protezione dei Dati

Sussistono inoltre i seguenti requisiti inerenti alla protezione dei dati:

1. I dati salvati devono essere protetti da un attaccante che abbia accesso al sistema, prendendo misure di sicurezza fisica, eventualmente cifrando i dati.
2. I dati inviati tra le parti remote devono essere protetti, utilizzando la cifratura dei dati.
3. Tutte le azioni avvenute sul sistema devono essere tracciate tramite un sistema di log.

La visione e l'analisi dei log verrà gestita con un editor di testo esterno, accessibile solo al personale autorizzato.

<b>ID</b>	<b>Requisiti</b>	<b>Tipo</b>
R16F	Implementazione di un sistema di log per tracciare tutti i messaggi tra i client e i server, inclusi gli accessi, le richieste di prenotazione, di conferma, di sospensione e di invio e ricezione di dati	Funzionale
R9NF	I dati salvati devono essere protetti da un attaccante che abbia accesso al sistema, prendendo misure di sicurezza fisica, eventualmente cifrando i dati	Non Funzionale
R10NF	I dati inviati tra le parti remote devono essere protetti, utilizzando la cifratura dei dati	Non Funzionale

### 3 Analisi del Problema

#### 3.1 Analisi Documento dei Requisiti: Analisi delle Funzionalità

Tabella delle Funzionalità

Funzionalità	Tipo	Grado di complessità	Requisiti Collegati
Gestione Farmacia	Memorizzazione dati e gestione dati	complessa	R5F, R9F, R10F, R11F, R12F, R13F, R14F, R15F
Registrazione	Interazione esterno e memorizzazione dati	semplice	R4F
RicercaFarmaci	Interazione esterno e lettura dati	semplice	R1F, R2F, R3F
Login	Interazione esterno e lettura dati	semplice	R7F
GestionePrenotazioni	Interazione esterno e memorizzazione dati	comp	R2F, R6F, R8F
ScritturaLog	Memorizzazione dati	semplice	R16F

GestioneFarmacia: Tabella Informazioni/Flusso

Informazione	Tipo	Livello protezione/privacy	Input / Output	Vincoli
Nome Cliente	semplice	Protezione alta	Output	Non più di 40 caratteri
Cognome Cliente	semplice	Protezione alta	Output	Non più di 40 caratteri
Codice Fiscale Cliente	semplice	Protezione media	Output	Deve essere di 16 caratteri
Stato Cliente	semplice	Protezione media	Output	
Lista Farmaci	composto	Protezione alta	Output	
Lista Prenotazioni	composto	Protezione molto alta	Output	

## 4 Progettazione

### 4.1 Progettazione Architettuale

#### 4.1.1 Requisiti non funzionali

Dall'analisi dei requisiti sono emersi i seguenti requisiti non funzionali:

- Tempo di risposta
- Usabilità
- Integrità dei dati
- Protezione dei dati
- Sicurezza delle comunicazioni

La protezione dei dati e delle comunicazioni assume fondamentale importanza vista la natura del software, che deve trattare dati personali e sanitari dei clienti. La compromissione di questi risulterebbe in una grave perdita finanziaria e di immagine, senza considerare i danni apportati alla privacy degli utenti. Inoltre, sarà necessario assicurare la sicurezza fisica dei dati immagazzinati nel sistema. L'introduzione di misure di sicurezza delle comunicazioni e protezione dei dati non compromette l'usabilità del sistema, ma potrebbe peggiorarne leggermente le prestazioni: è possibile comunque bilanciare le due esigenze senza eccessive complicazioni mediante le tecnologie esposte in seguito. Va notato inoltre che il sistema non presenta vincoli di tempo particolarmente stringenti (nessun vincolo real-time).

#### 4.1.2 Scelta dell'architettura

Dopo una rapida analisi, si è constatato che l'architettura più adeguata per il sistema è l'**architettura client-server a 3 livelli**.

##### **L1 – Client**

La componente lato Client sarà implementata da due interfacce differenti:

- Un'interfaccia per le funzionalità relative ai clienti (registrati e non)
- Un'interfaccia per la gestione della farmacia da parte di un operatore (farmacista)

##### **L2 – Server**

Rispettando il principio del "minimo privilegio" per limitare i danni in caso di attacco e per distribuire meglio il carico, si è deciso di scomporre i server in base alle funzionalità offerte. Si hanno quindi tre server:

- Un server che fornisce i servizi ai clienti registrati e non
- Un server che funge da pannello di controllo per i farmacisti
- Un server per le funzionalità di autenticazione

## L3 – Persistenza

La gestione della persistenza verrà implementata in un server dedicato sul quale sarà installato un DBMS che gestisca i dati di tutte le farmacie aderenti al servizio. Su tale server sarà installato il DBMS IBM DB2. L'interfacciamento con il DBMS avverrà mediante la metodologia "forza bruta" utilizzando i metodi CRUD. Per quanto riguarda il log delle operazioni, invece, questo verrà salvato su file system (un semplice file sul server adibito)

### 4.1.3 Pattern architetturali e di design

Infine, dopo un'attenta analisi, si è optato per l'adozione del pattern **Broker**: un componente verrà interposto alla comunicazione Client-Server e avrà il compito di indirizzare le richieste dei client al relativo server, effettuando un controllo sulle sessioni attive per determinare lo stato del client. La scomposizione in diversi client e server consente di avere una separazione netta tra gli applicativi del cliente e del farmacista, in modo da localizzare le operazioni critiche e ottenere maggiore protezione dei dati. Il pattern Model View Controller (**MVC**) è stato invece scelto come pattern architetturale. Chiaramente l'affidabilità del sistema dipende dalla robustezza del broker e soprattutto del sistema di autenticazione.

Si riportano di seguito i diagrammi di package e componenti che descrivono l'architettura del sistema.

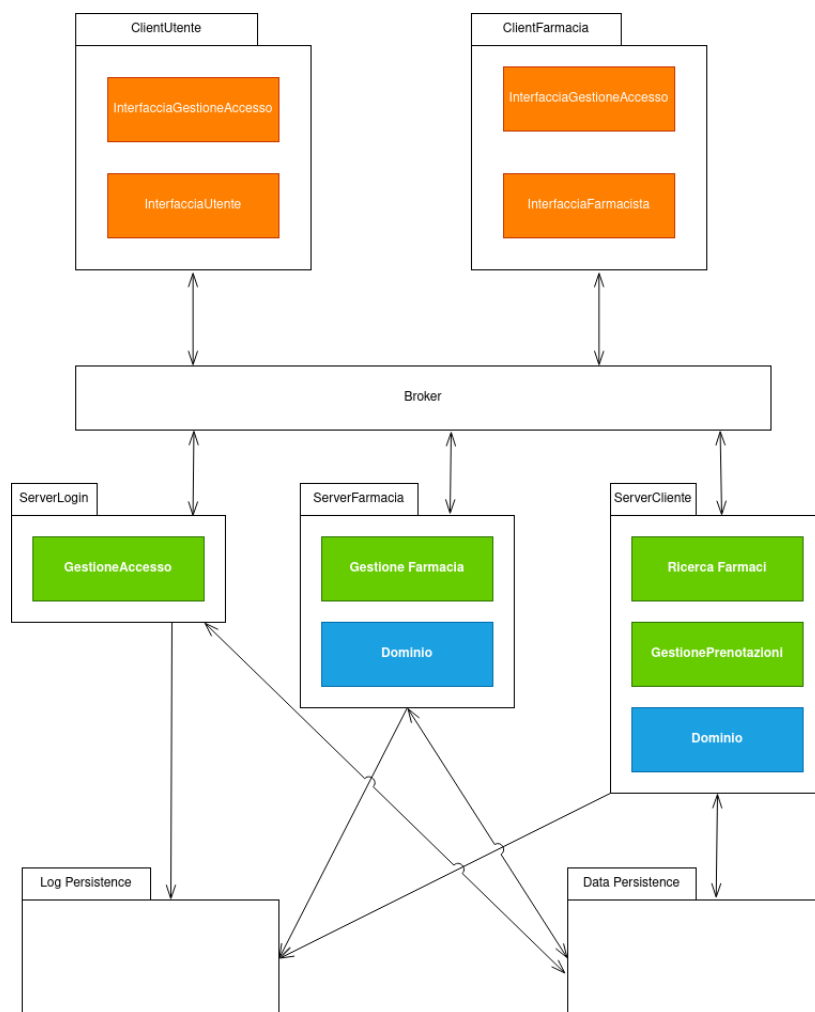


Figura 1: Diagramma dei package

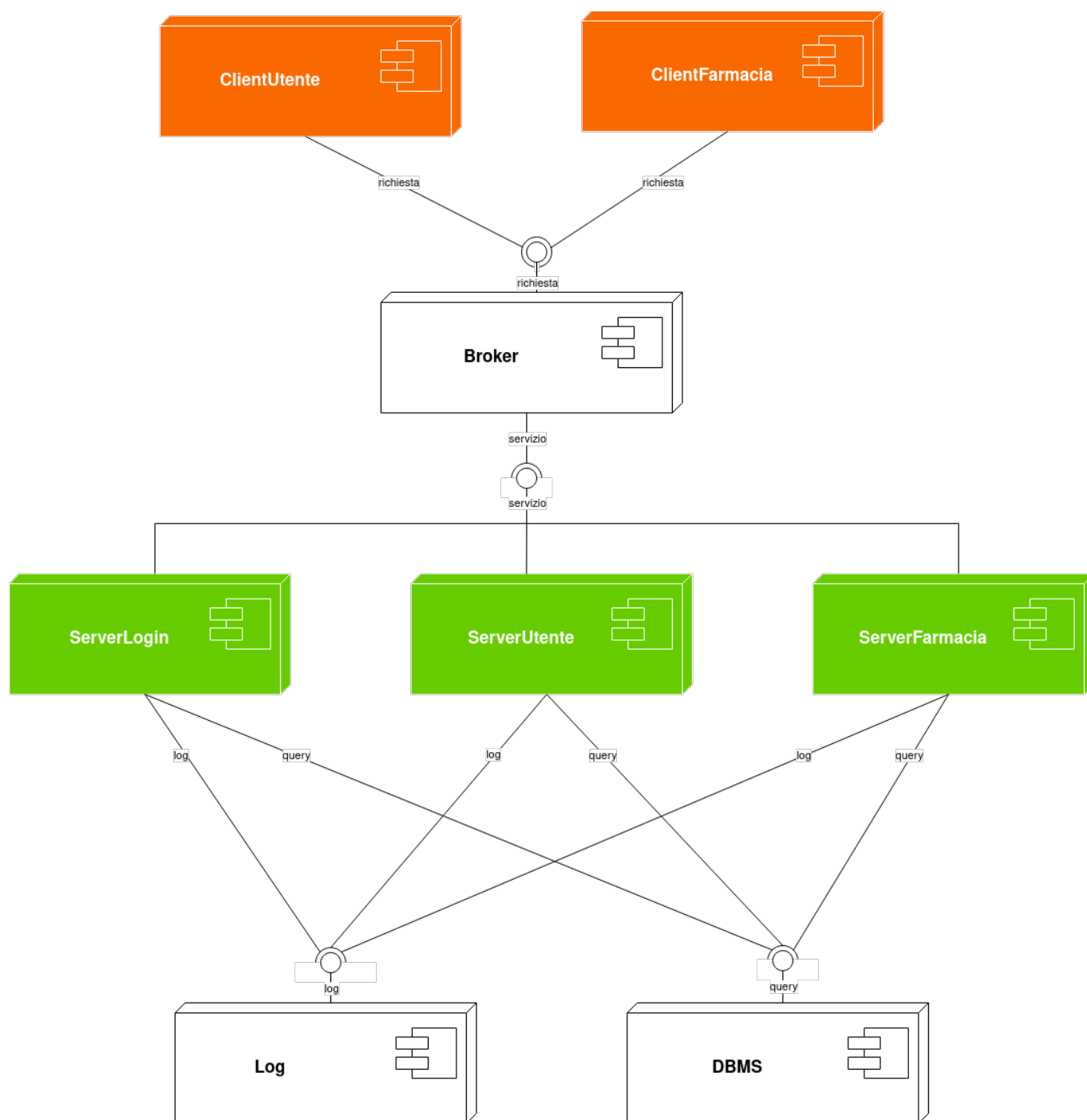


Figura 2: Diagramma dei componenti

## 4.2 Progettazione di dettaglio

### 4.2.1 Struttura

#### Struttura: Dominio

Per quanto riguarda il dominio, i diagrammi rimangono sostanzialmente uguali a quelli visti in analisi. Nonostante il dominio del cliente sia pressoché identico a quello del farmacista, si è comunque deciso di distinguere i due domini al fine di evitare l'introduzione di classi non necessarie. In particolare, la parte di applicativo relativa al cliente non dovrà gestire né conoscere i farmacisti legati ad ogni farmacia (informazione nota solo al server delle farmacie).

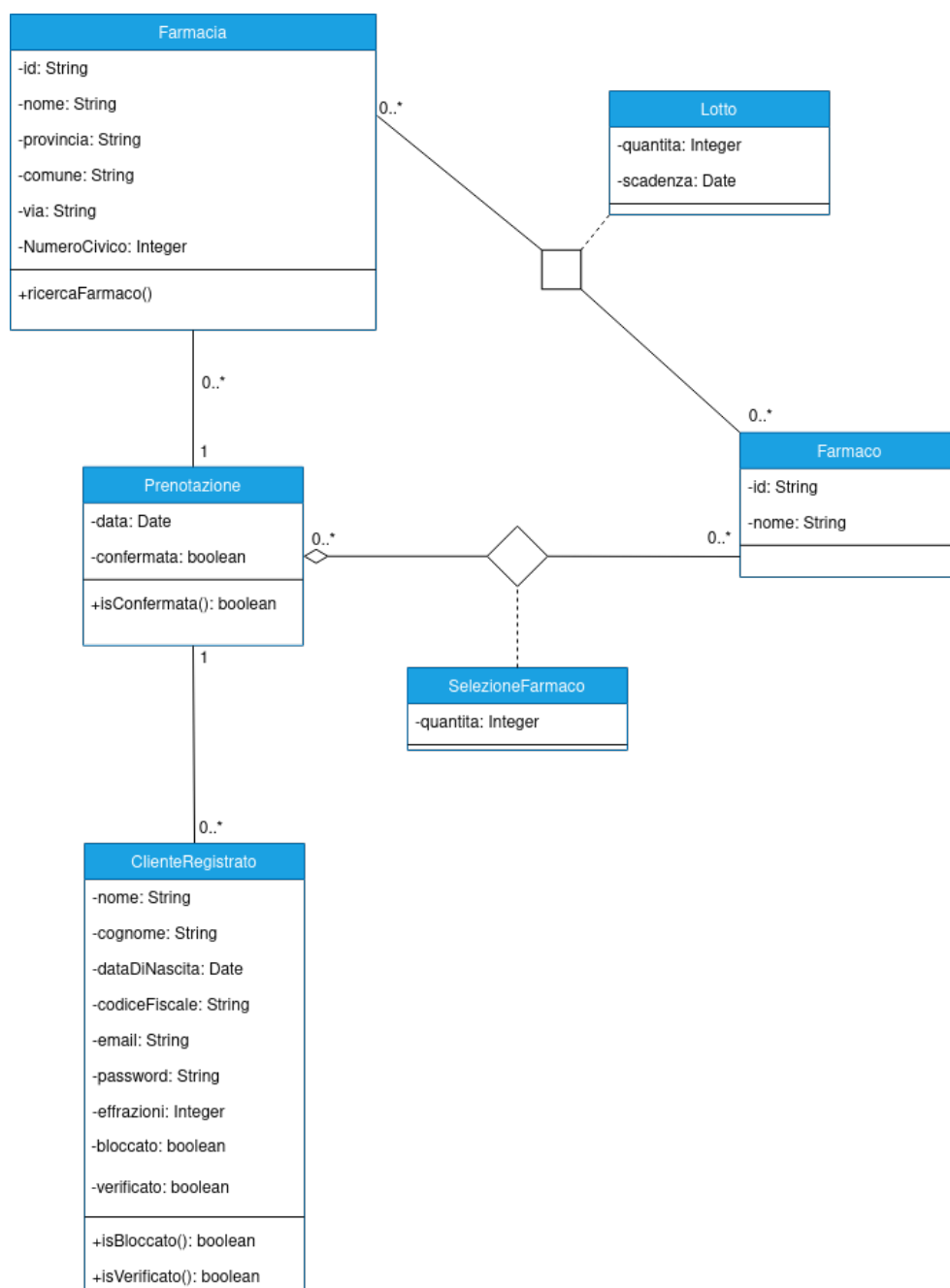


Figura 3: Diagramma di dettaglio: Dominio Clienti



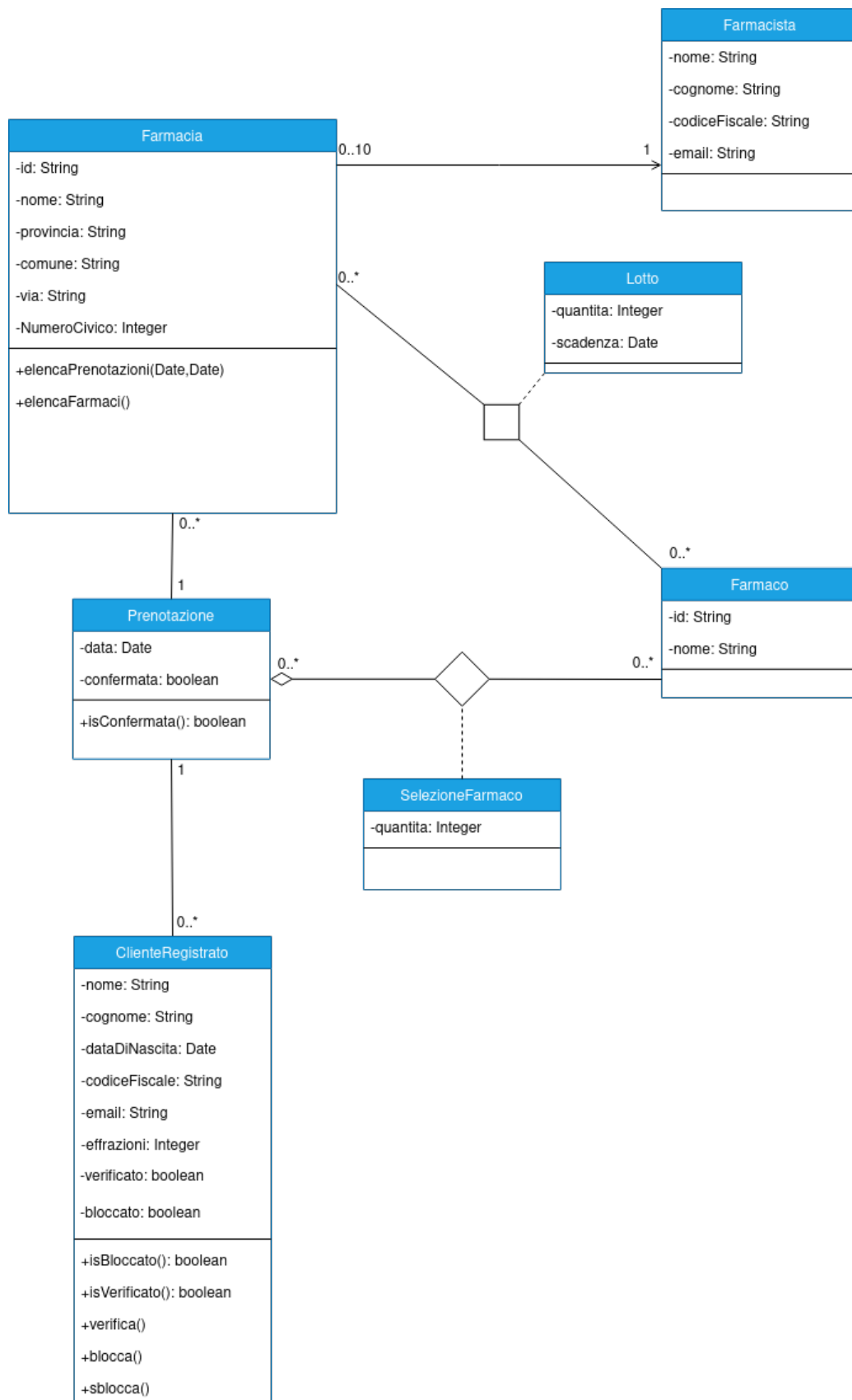


Figura 4: Diagramma di dettaglio: Dominio Farmacia

Come si può notare, il dominio della farmacia presenta diversi metodi aggiuntivi (in particolare per effettuare operazioni sul cliente e per elencare farmaci) non necessari al cliente e anzi da nascondere ad esso per evitare che i permessi o privilegi vengano aggirati. Inoltre, le associazioni **Lotto** e **SelezioneFarmaco** sono state mantenute nei diagrammi per chiarezza. L'associazione **Lotto** dovrà necessariamente essere una classe a sé stante, mentre l'associazione **SelezioneFarmaco** potrà essere concretizzata in classe o sostituita da un semplice Integer. Quest'ultima scelta è lasciata agli implementatori. Le associazioni vere e proprie dovranno poi essere implementate mediante una **mappa**, ad esempio con un oggetto del tipo `HashMap<Farmaco, Lotto>`

## Struttura: Interfacce



Figura 5: Diagramma di dettaglio: Interfacce

L'aggiunta di tali interfacce consente di applicare il *Dependency Inversion Principle* in modo da disaccoppiare gli utilizzatori dalle implementazioni, che potrebbero cambiare.

## Struttura: Controller

Si è deciso di utilizzare una classe **Controller** in cui inserire le funzionalità relative alla persistenza (Database e Log). Si è pensato di posizionare questa classe in cima alla gerarchia dei controller: in questo modo, le funzionalità comuni di lettura/scrittura su database e log sono riutilizzabili dai controller figli senza bisogno di reimplementarle. Nonostante il controller "monolitico" non rispetti il *Single Responsibility Principle*, abbiamo comunque optato per questa soluzione, in quanto le funzionalità relative al database e al logging risultano facilmente accoppiabili essendo entrambe legate a un qualche tipo di persistenza. Inoltre, non si prevede alcun tipo di estensione/modifica per quanto riguarda la persistenza.

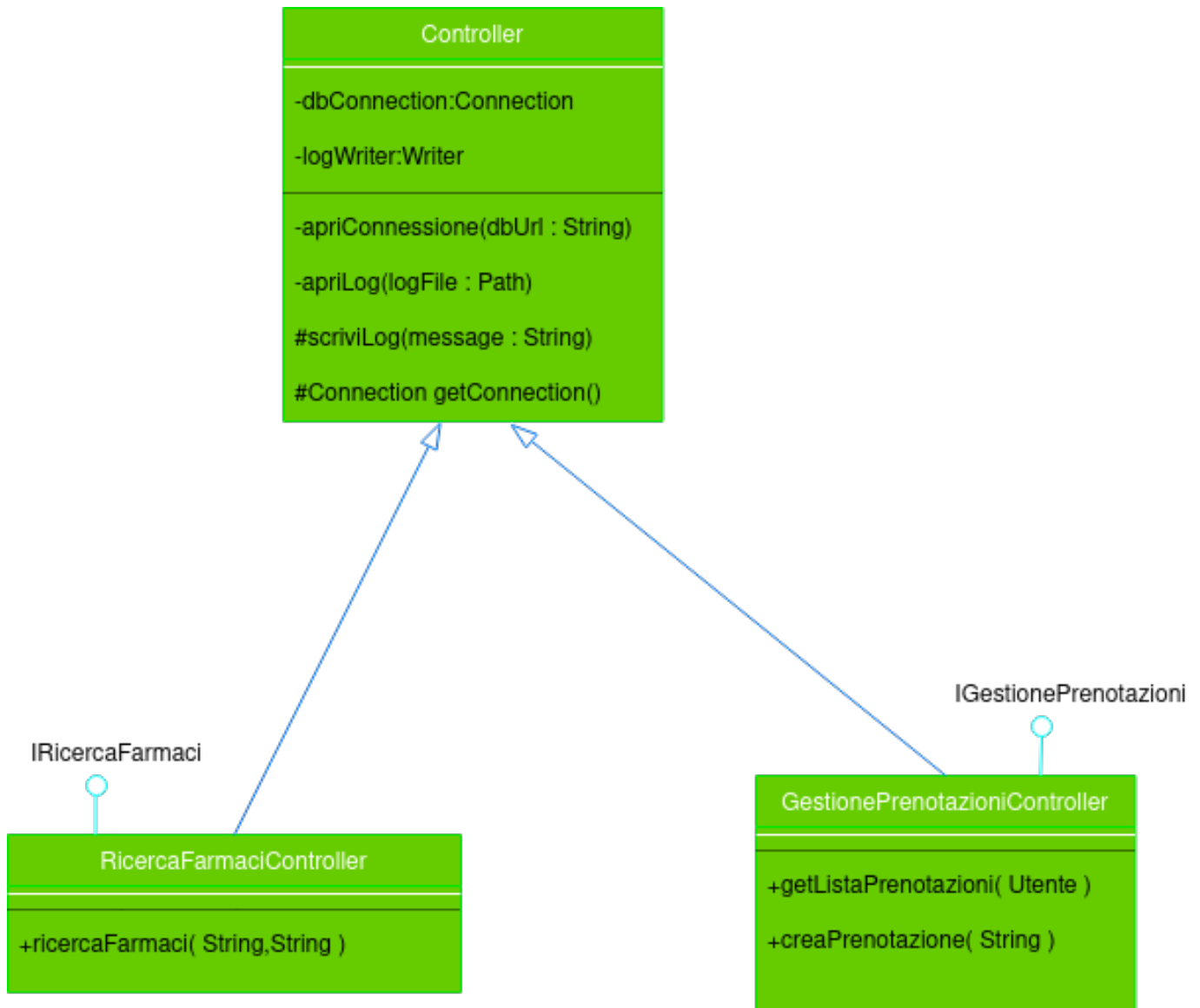


Figura 6: Diagramma di dettaglio: RicercaFarmaci, GestionePrenotazioni

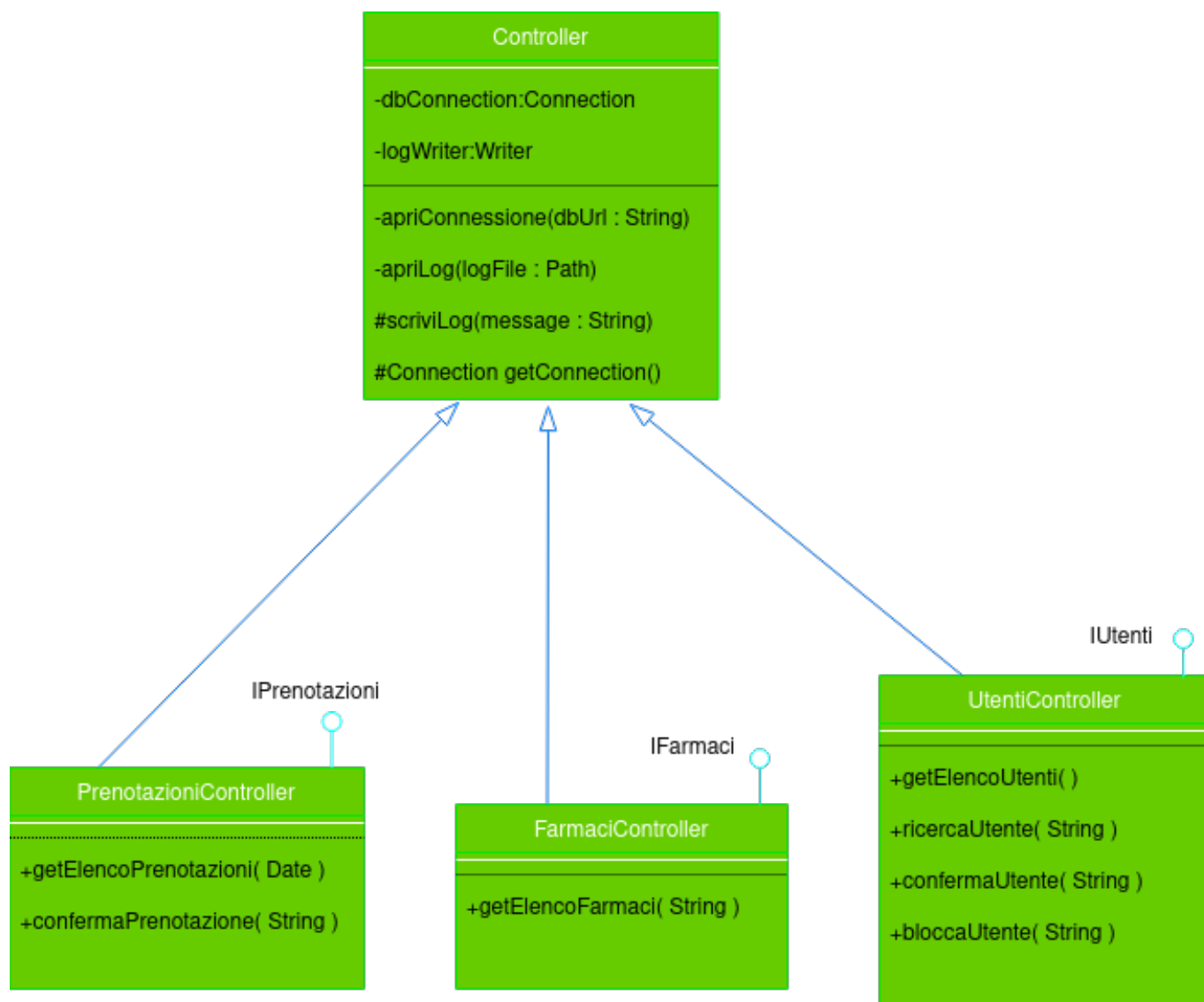


Figura 7: Diagramma di dettaglio: GestioneFarmacia

Anche i controller presenti sul server relativo alle farmacie seguono lo stesso principio esposto sopra.

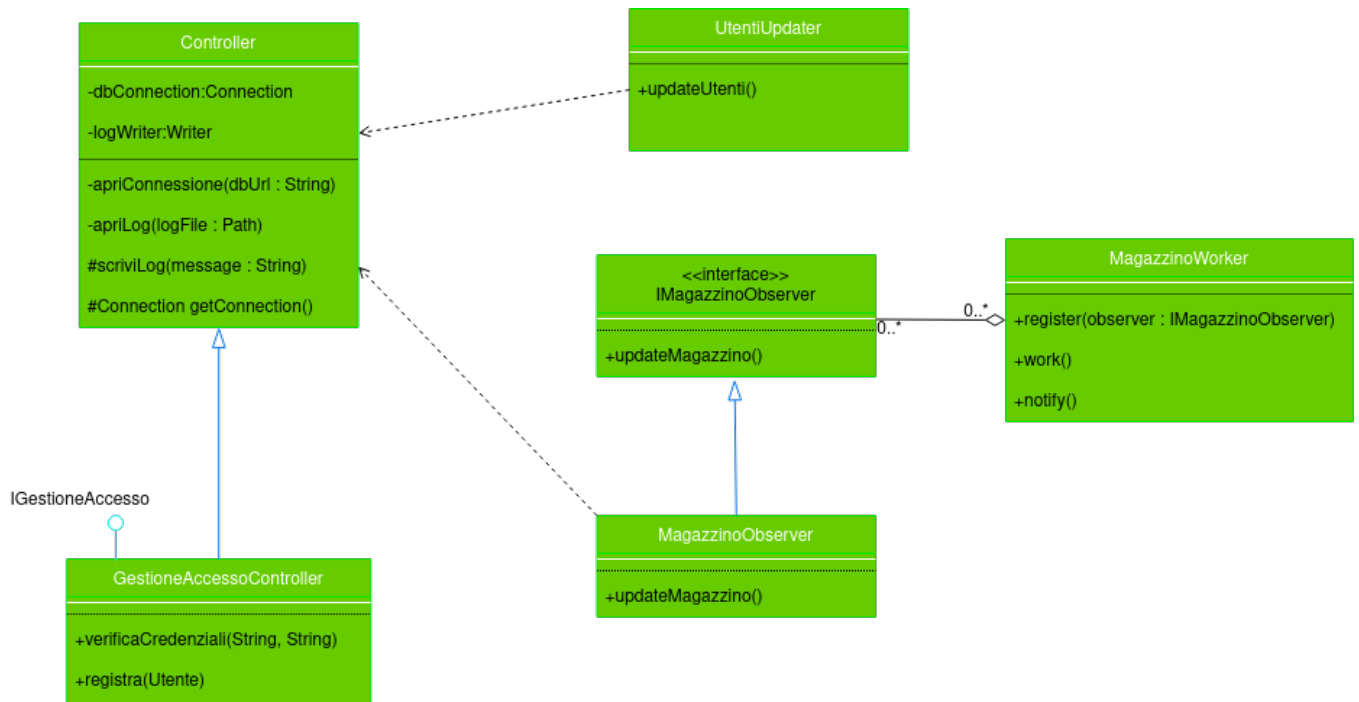


Figura 8: Diagramma di dettaglio: GestioneAccesso

Il diagramma di dettaglio del server login risulta più complesso degli altri due poiché contiene le ulteriori classi necessarie per implementare l'aggiornamento dello stato dei clienti e caching del database in seguito al ricevimento di eventi. In particolare, per implementare il caching locale del database remoto contenente i dati dei magazzini, si è deciso di utilizzare un pattern *Observer*: Un'istanza della classe **MagazzinoObserver** viene registrata nel **MagazzinoWorker**. Quest'ultimo poi comunicherà con il server remoto mediante un protocollo prestabilito e, alla ricezione di un aggiornamento da parte del server, notificherà l'Observer. Lo scambio dei dati riguardanti l'aggiornamento può avvenire tra Worker e Observer in diversi modi, pertanto la scelta viene lasciata agli implementatori.

Si noti che la scelta del pattern Observer è dettata dal fatto che l'evento di aggiornamento del database remoto può risultare importante anche per future estensioni del software: per questo motivo l'Observer si basa sull'interfaccia **IMagazzinoObserver**.

Per quanto riguarda invece l'aggiornamento dello stato dei clienti a fine giornata, il metodo `updateUtenti()` della classe **UtentiUpdater** verrà invocato automaticamente allo scattare di un nuovo giorno, in base all'orario del server.