

Progetto di
Sicurezza Informatica e Internet
Progetto A2 - Encrypted 2D Barcodes

Giovanni Rossi - gio.rossi.1991@gmail.com
Pasquale Verlotta - pasquale.verlotta@gmail.com



Indice

Indice	I
Elenco delle figure	II
1 Introduzione	1
1.1 Scopo del progetto	1
1.2 Tecnologie Utilizzate	3
1.2.1 Strumenti di sviluppo	3
1.2.2 Linguaggio e librerie utilizzate	3
1.3 Le principali tecnologie	4
1.3.1 QR-Code	5
1.3.2 OCR	5
2 Progettazione	7
2.1 Requisiti	7
2.2 Architettura	9
2.3 Focus sulla sicurezza	12
2.3.1 Autenticazione	12
2.3.2 Composizione e lettura dei documenti	14
3 Funzionamento dell'applicazione	21
3.1 Server	21
3.2 Client	22
3.2.1 Cifratura	25
3.2.2 Decifrazione	26
4 Conclusioni	28

Elenco delle figure

1.1	Esempio di QR-Code	5
1.2	OCR	6
2.1	Use Case Diagram	8
2.2	Architettura del sistema	10
2.3	Sequence Diagram: Registrazione al Sistema	13
2.4	Template del documento	15
2.5	Flusso cifratura documento	17
2.6	Flusso decifrazione documento	19
3.1	GUI del server	22
3.2	Login	23
3.3	homelayout	24
3.4	GUI di encode	25
3.5	GUI di decode	26

Capitolo 1

Introduzione

1.1 Scopo del progetto

Il progetto sviluppato in questi mesi per il corso di “Sicurezza Informatica e Internet” si propone come scopo quello di realizzare un’applicazione che permetta di gestire un documento cartaceo in forma sicura. In particolare questo significa che chi utilizza tale sistema deve essere in grado di

- compilare un foglio con informazioni sensibili;
- cifrare tutto o alcune parti del foglio al fine di poterlo inviare a chiunque voglia;
- decifrare il contenuto di un documento ricevuto da un’altra persona.

Lo scopo ultimo è dunque quello di abilitare l’utente ad inviare ad un gruppo di persone il documento che ha appena creato. Tuttavia durante il trasferimento (funzione che non compete a questa applicazione) può succedere che il documento possa venire alterato in alcune sue parti se non si utilizzano canali sicuri; moltissime truffe avvenute in passato si sono basate su questa vulnerabilità. Dunque uno degli scopi è quello di garantire con opportune tecniche basate su crittografia asimmetrica che il documento cartaceo resti robusto ed inattaccabile qualunque sia il canale di comunicazione che l’utente finale sceglie per l’invio. Nel caso di questo progetto, l’elaborazione riguarda documenti cartacei, quindi non è possibile archiviare le informazioni sensibili in una qualche struttura dati. La sfida più importante è quella di trasportare insieme al documento stampato le informazioni segrete. Questo apre una serie di problematiche legate alla gestione delle informazioni che sono in formato digitale nella fase di composizione e diventano analogiche nella fase di acquisizione di un documento spedito (che può essere stampato

1.1. SCOPO DEL PROGETTO

e acquisito più volte durante il percorso - per esempio via fax). La tecnologia migliore per il trasporto dei dati su immagini è rappresentata dal *QR-Code*, un particolare tipo di codice a barre 2D che può contenere al suo interno una discreta quantità di informazioni. I dati possono essere rilette utilizzando algoritmi di riconoscimento robusti che hanno raggiunto nel tempo un'elevata maturità. Nell'ambito di questo progetto i QR-Code sono stati utilizzati sia per memorizzare le informazioni cifrate, sia per apporre una firma digitale al documento intero. Si risponde così alle esigenze di mantenere segreti alcuni contenuti e di rendere il documento robusto alle manipolazioni esterne.

Un'altra funzionalità importante che rientra negli scopi di questa applicazione, è quella di creare una gerarchia tra gli utenti che accedono al servizio. Può capitare, infatti, di voler pubblicare un certo documento e di voler permettere solo a pochi eletti di accedere alle informazioni cifrate. Questo implica che nel sistema si avranno utenti con livelli di privilegio diversi dove ognuno di questi può decifrare e leggere solo le informazioni adeguate al suo livello. In questo caso la soluzione più ovvia potrebbe essere quella di pubblicare versioni diverse dello stesso documento oscurando opportunamente sulle diverse copie le informazioni che si vogliono tenere segrete a ciascun gruppo. Questo processo può risultare lungo, macchinoso e poco sicuro: è possibile, infatti, che qualche copia possa finire al destinatario sbagliato se non si prendono opportune precauzioni. Ci si è quindi occupato di realizzare un sistema dove la cifratura viene effettuata con chiavi speciali (che da ora in poi verranno chiamate **chiavi di livello**), le quali vengono distribuite solo agli utenti che hanno un **livello di fiducia** (o **Trust Level**) adeguato. In questo caso un Trust Level basso corrisponde ad un basso livello di privilegio, mentre un Trust Level alto garantisce l'accesso a tutte le informazioni cifrate con le chiavi di livello più basso.

Riassumendo quindi, per quanto riguarda le funzionalità principali, il sistema dovrebbe permettere di:

- compilare un documento contenente qualsiasi tipo di informazione;
- cifrare in tutto o in parte il documento appena scritto;
- allegare le informazioni cifrate al documento stesso così che il o i destinatari possano leggerlo;
- firmare il documento in modo tale che il mittente non possa ripudiare la provenienza e i destinatari possano accorgersi di eventuali manomissioni durante il trasferimento;
- specificare diversi livelli di privilegio gerarchici per la lettura delle informazioni.

1.2 Tecnologie Utilizzate

Gli obiettivi appena illustrati, danno un'idea delle tante problematiche che l'applicazione deve affrontare. Per questo sono molte le tecnologie che sono state messe in gioco. Nel seguito di questo paragrafo verranno spiegate quelle utilizzate maggiormente.

1.2.1 Strumenti di sviluppo

Per quanto riguarda gli strumenti, si è fatto uso di

- **Eclipse Luna** come IDE per la gestione del progetto e dei file sorgente;
- **Apache Maven v2.2** per la gestione delle dipendenze e del ciclo di vita dell'applicazione;
- **Git** per il *versioning* e la condivisione dei sorgenti nel team (in particolare si è usato un repository pubblico¹ su *GitHub* come piattaforma online di condivisione²);

1.2.2 Linguaggio e librerie utilizzate

In questo progetto è stato utilizzato **Java** come linguaggio di programmazione principale. I motivi di questa scelta ricadono principalmente su:

- il paradigma Object-Oriented che ha permesso l'utilizzo di architectural e creational pattern per risolvere le problematiche più comuni, come Façade, Factory Method, Abstract Factory, DAO e Singleton che sono stati ampiamente utilizzati nello sviluppo;
- l'alta manutenibilità del codice;
- la portabilità su altre piattaforme diverse da quella di sviluppo;
- la grande quantità di librerie presenti a supporto degli obiettivi descritti prima.

Per quanto riguarda invece i singoli moduli del software sviluppato, si sono utilizzati diversi framework e librerie. Per la parte di sicurezza c'è:

¹Per certi versi si è seguito il principio di *Auguste Kerckhoffs* secondo cui “*in un sistema crittografico è importante tener segreta la chiave, non l'algoritmo di crittazione*”.

²Link del repository:<https://github.com/WAFcoding/ProgettoSicurezza.git>

1.3. LE PRINCIPALI TECNOLOGIE

- **JCA/JCE** (Java Cryptographic Architecture/Java Cryptographic Extension) come framework e provider dei principali algoritmi di cifratura, firma e hashing;
- **BouncyCastle** che si integra con JCA/JCE e fornisce un maggior numero di algoritmi di cifratura e firma nonché funzioni di generazione di certificati;

Per il modulo di elaborazione dei documenti:

- **ImageMagik** per la manipolazione delle immagini dei documenti acquisiti per la decodifica;
- **ZXing** per la generazione e lettura di QR-Code (in generale supporta molti tipi di codici a barre sia 1D che 2D);
- **iTextPDF** per la generazione di documenti ad alta risoluzione ed il posizionamento preciso di testo e QR-Code nel documento;
- **Tesseract** ed in particolare il wrapper Java **Tess4J** per il recupero del testo dopo la scansione dei documenti.

Per la parte di persistenza invece si è fatto uso di:

- **MySQL** come database relazionale per il sistema di *provisioning* delle chiavi e la gestione degli utenti;
- **SQLite** per la gestione dei dati locali di ogni singolo utente (sotto forma di database cifrato);
- **Hibernate** come framework per la gestione dei database (MySQL e SQLite), ed in particolare il modulo **ORM** (Object-Relational Mapping).

1.3 Le principali tecnologie

Di seguito una breve panoramica dello stato dell'arte delle tecnologie utilizzate maggiormente nello sviluppo di questo progetto. Si analizzeranno in particolar modo il **QR-Code** e l'**OCR**.

1.3.1 QR-Code

Il *QR-Code* (Quick Response Code in virtù del fatto che il codice fu sviluppato per permettere una rapida decodifica del suo contenuto) è un codice a barre bidimensionale, ossia a matrice, composto da moduli neri disposti all'interno di uno schema di forma quadrata. Viene impiegato per memorizzare informazioni generalmente destinate a essere lette tramite un dispositivo mobile. In un solo codice QR possono essere contenuti oltre 7089 caratteri numerici o 4296 alfanumerici. Il QR-Code fu sviluppato nel 1994 dalla compagnia giapponese *Denso Wave* allo scopo di tracciare le componenti di automobili nelle fabbriche della Toyota. Vista la capacità del codice di contenere più dati di un codice a barre venne in seguito utilizzato per la gestione delle scorte da diverse industrie. Tuttavia essendo un codice che deve essere riportato su un documento cartaceo, può subire dei danni che possono provocare degli errori nella seguente lettura. Per questo viene utilizzato il codice Reed-Solomon per la rilevazione e correzione d'errore che permette di ricostruire i dati persi, ripristinando, durante la decodifica, fino al 30% delle informazioni codificate.

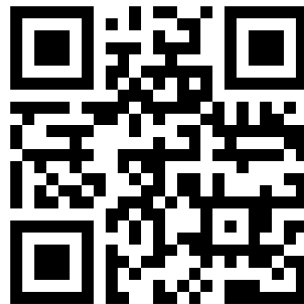


Figura 1.1: Un esempio di QR-Code.

1.3.2 OCR

La parola *OCR* (Optical Character Recognition) descrive una classe di sistemi di riconoscimento ottico dei caratteri. Gli OCR sono programmi dedicati alla conversione di un'immagine contenente testo, solitamente acquisite tramite scanner (come nel caso di questo progetto), in testo digitale modificabile con un normale editor. Il testo può essere convertito in formato ASCII semplice, Unicode o, nel caso dei sistemi più avanzati, in un

1.3. LE PRINCIPALI TECNOLOGIE

formato contenente anche l'impaginazione del documento. L'OCR è un importante campo di ricerca dell'intelligenza artificiale, della visione artificiale e del pattern recognition, legati al riconoscimento delle immagini. I sistemi OCR per funzionare correttamente richiedono una fase di "addestramento". Durante questa fase al sistema vengono forniti degli esempi di immagini col corrispondente testo in formato ASCII o simile in modo che gli algoritmi si possano calibrare sul testo che usualmente andranno ad analizzare. Gli ultimi software di OCR utilizzano algoritmi in grado di riconoscere i contorni e in grado di ricostruire oltre al testo anche la formattazione della pagina. Gli OCR possono essere usati per riconoscere:

- caratteri stampati, per i quali gli algoritmi noti hanno un tasso di errore del 1%;
- scrittura a mano libera, problema tutt'altro che risolto, per la quale gli algoritmi hanno tassi di accuratezza dell'80% - 90%;
- caratteri in corsivo, che è un campo in fase di studio, per il quale si hanno tutt'oggi risultati poco soddisfacenti a livello di accuratezza.

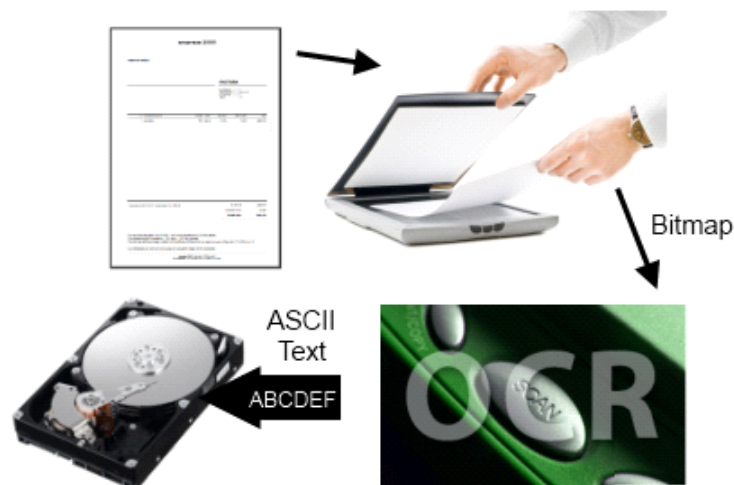


Figura 1.2: Processo da seguire per utilizzare un sistema OCR.

Capitolo 2

Progettazione

In questo capitolo verranno analizzate in dettaglio le scelte progettuali che hanno permesso la realizzazione del sistema software. Dopodiché si analizzerà, attraverso la rappresentazione dei diagrammi **UML**, la definizione delle fasi di sviluppo, ossia la progettazione delle funzionalità correnti dell'applicazione.

2.1 Requisiti

Come primo aspetto della progettazione si analizzeranno adesso i requisiti del sistema. Innanzitutto si deve specificare che l'intero sistema è pensato per essere utilizzato in un ambito amministrativo dove gli utenti possono essere per esempio i dipendenti di un'azienda. Questo vuol dire che ci si trova in un sistema chiuso in cui le persone che usano il sistema sono note. Tuttavia è possibile che nel tempo i dipendenti si licenzino oppure che ne sopraggiungano di nuovi, quindi deve essere presente una procedura che consenta di inserire nuovi utenti ed eventualmente di rimuovere quelli esistenti. In questo sistema dove gli utenti sono noti, immaginiamo la presenza di un utente **amministratore** che agisce come supervisore ed è l'unico ad avere la facoltà di abilitare gli utenti all'utilizzo del servizio nonché di assegnare il *Trust Level*.

Di seguito viene mostrato il diagramma dei casi d'uso che rappresenta una vista generale delle funzionalità che il sistema deve avere.

2.1. REQUISITI

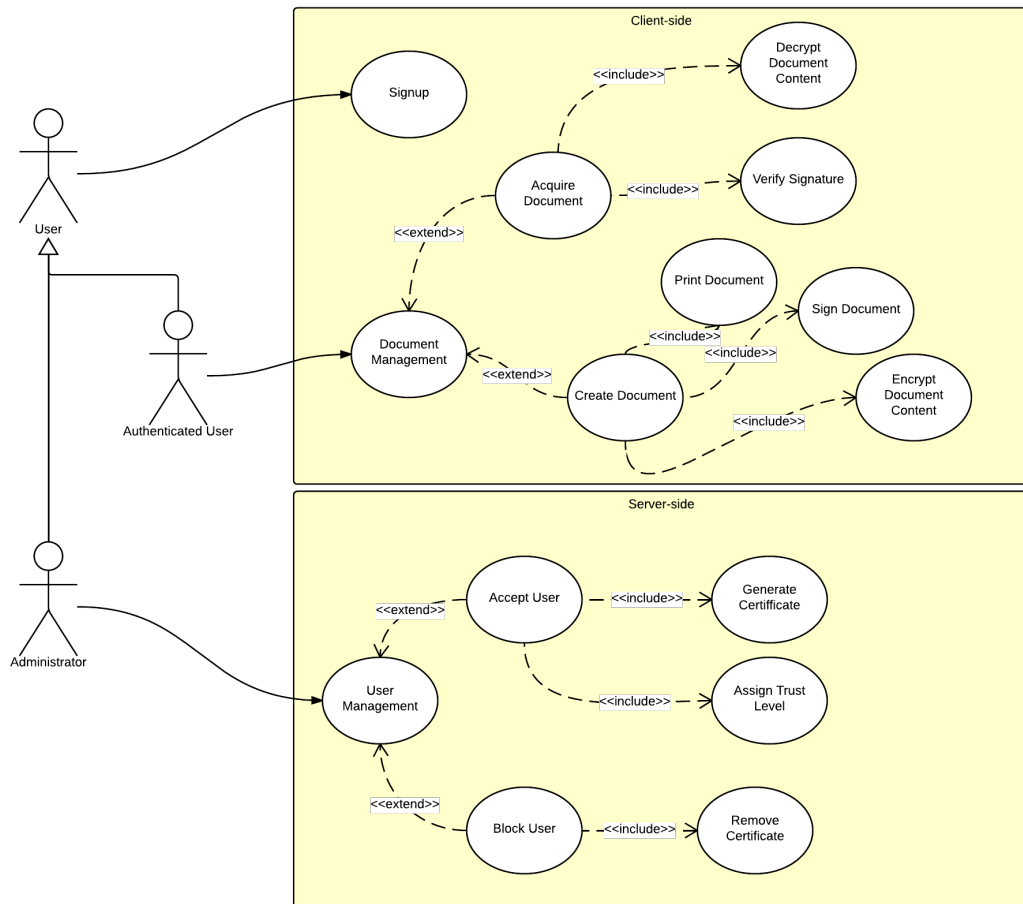


Figura 2.1: Diagramma dei casi d'uso del sistema software realizzato

La prima cosa che va evidenziata è che il tutto è strutturato secondo un architettura di tipo client/server. Questi due componenti dialogano tra di loro utilizzando una connessione sicura basata su SSL¹. Da quello che si può evincere, il server è un componente fondamentale che espone la funzionalità di *provisioning* delle chiavi. Esso mantiene sia le chiavi di livello necessarie per la cifratura del documento, sia le chiavi pubbliche degli utenti registrati al sistema.

Da quello che si può vedere dalla figura 2.1 nel sistema si hanno 3 attori importanti: l'amministratore, l'utente registrato (autenticato) e l'utente

¹Dettagli maggiori saranno dati nel paragrafo 2.3.

semplice che non ha mai utilizzato il sistema. Come è stato già detto, l'amministratore si occupa di gestire l'accesso degli utenti. Questo vuol dire che ha piena facoltà di abilitare gli utenti all'utilizzo del sistema verificandone l'identità con procedure interne all'azienda che possono variare di caso in caso e che esulano completamente dagli scopi di questo progetto. Oltre a questo può decidere di limitare l'accesso al sistema bloccando l'utente con una semplice procedura, grazie alla quale il server è in grado di comprendere se l'utente che si connette è autorizzato oppure no ad ottenere le chiavi di un certo livello. Altro compito fondamentale è quello dell'assegnazione del Trust Level che viene deciso in fase di abilitazione dell'utente al sistema. Tuttavia questo può essere anche cambiato successivamente. Grazie al Trust Level, l'utente sarà abilitato a conoscere solo i segreti per cui è stato autorizzato, quindi l'assegnazione di questo parametro è fondamentale e richiede la massima attenzione.

L'utente registrato (o come riportato in figura 2.1 "autenticato") rappresenta una qualsiasi persona che è stata abilitata dall'amministratore ad usare l'applicazione in tutte le sue funzionalità attuali. Un utente di questo tipo dispone di una coppia di chiavi asimmetriche RSA a 1024 bit e di un certificato X.509 che viene utilizzato per le connessioni al server che richiedono mutua autenticazione. L'utente autenticato ha la possibilità di comporre un documento, oscurarlo in alcune sue parti utilizzando le chiavi di livello a cui può accedere, e firmarlo con la propria chiave privata RSA. Naturalmente oltre alla composizione del documento, l'utente registrato ha anche la facoltà di leggere quello che è stato inviato a lui o agli utenti con il suo stesso Trust Level².

Per quanto riguarda l'utente semplice, si è sicuramente notato che questo ha l'unica facoltà di registrarsi al sistema. Questo perché non dispone ancora di un certificato da usare per l'autenticazione e quindi non ha alcuna possibilità di leggere le informazioni se non provando ad eseguire un attacco sulla sicurezza del sistema o del documento cartaceo.

2.2 Architettura

Data una panoramica dei requisiti e delle funzionalità principali del sistema, si passerà adesso ad analizzare più in dettaglio l'architettura del sistema realizzato.

²Si rimanda al paragrafo 2.3 per una trattazione più approfondita di questo aspetto.

2.2. ARCHITETTURA

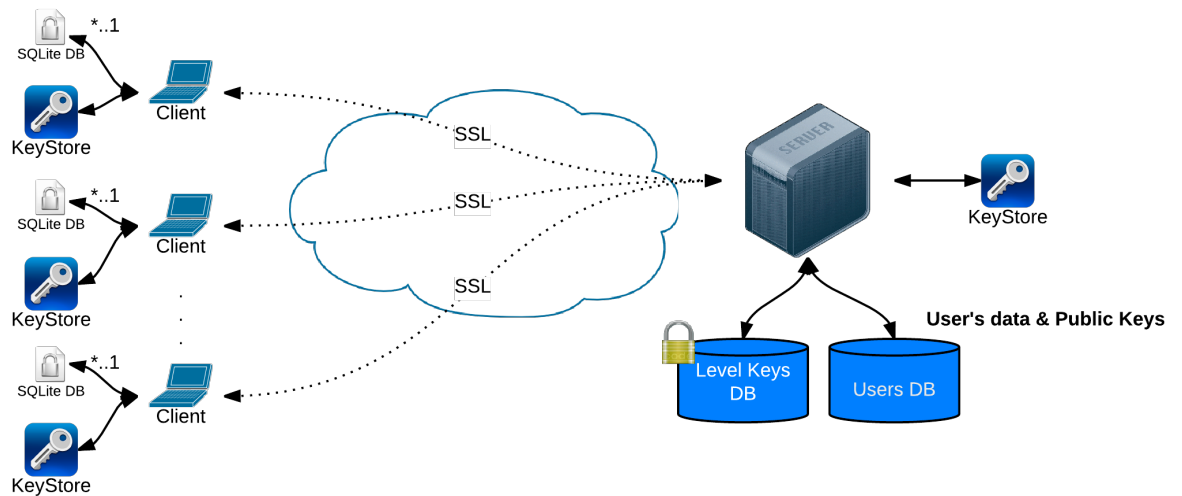


Figura 2.2: In questa figura sono rappresentate le componenti del sistema software realizzato.

Quella mostrata in figura 2.2 è l'architettura del sistema che è stato realizzato per questo progetto. Come si può vedere (anche da quanto già accennato nei paragrafi precedenti) il sistema si compone di due applicazioni separate: un server e un client. Entrambe queste applicazioni comunicano con il protocollo TCP/IP con l'aggiunta del layer di sicurezza realizzato da SSL.

Per quanto riguarda il server esso offre 2 servizi differenti. Il primo (sulla porta 8888) che richiede che gli utenti in connessione confermino la loro identità inviando il loro certificato così come previsto dallo standard SSL quando il server richiede, come requisito nella fase di handshake, il certificato del client al fine di verificare la mutua autenticazione. Le funzionalità offerte da questo primo servizio sono:

- fornire le chiavi di livello agli utenti autenticati che le richiedono (purché ne abbiano diritto in base al loro livello di fiducia);
- fornire le chiavi pubbliche degli utenti registrati al sistema, così che gli utenti possano verificare le firme digitali apposte sui documenti cartacei.

Il secondo servizio (sulla porta 8889) non richiede invece autenticazione mutua, in quanto è quello che permette agli utenti nuovi di comunicare i loro dati al server al fine di richiedere un'abilitazione all'utilizzo del sistema.

2.2. ARCHITETTURA

Da come si può vedere in figura 2.2 il server dispone di una connessione a due database MySQL separati e ad un *Java KeyStore*³. Il KeyStore serve a memorizzare i certificati degli utenti, in modo che possano essere identificati univocamente nella fase di handshake della connessione. Il primo dei due database si occupa di gestire le chiavi di livello necessarie per la cifratura del documento. Le chiavi sono memorizzate cifrate con **AES** tramite una chiave robusta e ad ognuna di queste è associato il livello di fiducia relativo. L'altro database si occupa di mantenere le informazioni degli utenti registrati, comprese le loro rispettive chiavi pubbliche. Si è deciso di separare i due database in quanto essi devono soddisfare requisiti di sicurezza differenti in quanto dalla segretezza delle chiavi di livello (che dovrebbero essere cambiate periodicamente) dipende la robustezza dell'intero sistema di cifratura dei documenti. La separazione permetterebbe allora di ospitare su server differenti i due database, che sarebbero quindi protetti con password robuste e differenti e con l'aggiunta di altri sistemi di sicurezza, quali *VPN* e *Firewall*, per la protezione da attacchi esterni.

All'applicazione stand-alone lato client compete invece tutta la gestione dei documenti, ossia la cifratura, la firma e la decifrazione delle immagini. Dal diagramma dell'architettura si vede come anche questo componente presenti una connessione ad un KeyStore e a diversi database di tipo SQLite. Per quanto riguarda il KeyStore, questo assolve alla stessa funzione di quello del server, ossia mantiene il certificato pubblico del server e la chiave privata di ciascun utente insieme al suo rispettivo certificato. Ogni entry del KeyStore (che nella pratica non è altro che una mappa indicizzata per una stringa chiamata *alias*) è cifrata con la password personale di ciascun utente. In più anche il file del KeyStore stesso è cifrato con una master key. I database SQLite, invece, servono a memorizzare i dati locali di ciascun utente compresa anche la coppia di chiavi asimmetriche RSA. Ogni utente ha il proprio database personale cifrato con la sua password. Il motivo di questa scelta riguarda soprattutto il fatto che i database SQLite non sono altro che file binari che sono gestiti da un software molto leggero (dimensioni nell'ordine delle centinaia di KiloByte). Quindi possono essere manipolati molto meglio rispetto per esempio ad un file di configurazione personalizzato per cui si sarebbe dovuta implementare una logica di gestione. Quindi la facilità di gestione e la leggerezza sono stati i principali responsabili di questa scelta.

³Un Java KeyStore (JKS) è un repository di certificati pubblici e chiavi utilizzato per la cifratura dei pacchetti su connessioni SSL.

2.3 Focus sulla sicurezza

Dopo aver trattato in dettaglio l'architettura del sistema, si può passare a descrivere tutte le procedure che sono state implementate per gestire la sicurezza del sistema e dei documenti cartacei. Di seguito i dettagli riguardanti la sicurezza.

2.3.1 Autenticazione

Come già detto nei paragrafi precedenti, per funzionare in modo sicuro, il sistema ha bisogno che gli utenti che lo utilizzano siano ben noti. Questo significa che ogni utente deve disporre di un certificato che comunichi la sua identità. Infatti, il requisito più importante per stabilire una comunicazione con il server per ottenere chiavi è l'autenticazione del client nella fase di handshake della connessione SSL. Affinché sussista la mutua autenticazione il server deve però conoscere già a priori il certificato del client. E allo stesso modo anche il client deve conoscere il certificato del server. Nel caso di questo progetto, si è deciso di mettere da subito a disposizione del client il certificato del server come configurazione di base. In questo modo si è sicuri che da subito l'applicazione client inizierà a parlare con il server certificato. Tuttavia lo stesso non può essere fatto dalla parte del server, in quanto questo non può conoscere a priori tutti i possibili utenti che entreranno nel sistema. Quindi si è deciso di prevedere una procedura di registrazione nella quale il risultato finale è il rilascio all'utente di un certificato autenticato dal server che a sua volta lo aggiungerà nel proprio KeyStore. Da osservare il fatto che nella fase di registrazione l'utente dialogherà col server senza comunicare la sua identità. È per questo che si è resa necessaria la figura dell'**amministratore** che si occuperà di verificare la reale identità dell'utente durante questa fase critica, ed eventualmente lo abiliterà ad usare il sistema.

2.3. FOCUS SULLA SICUREZZA

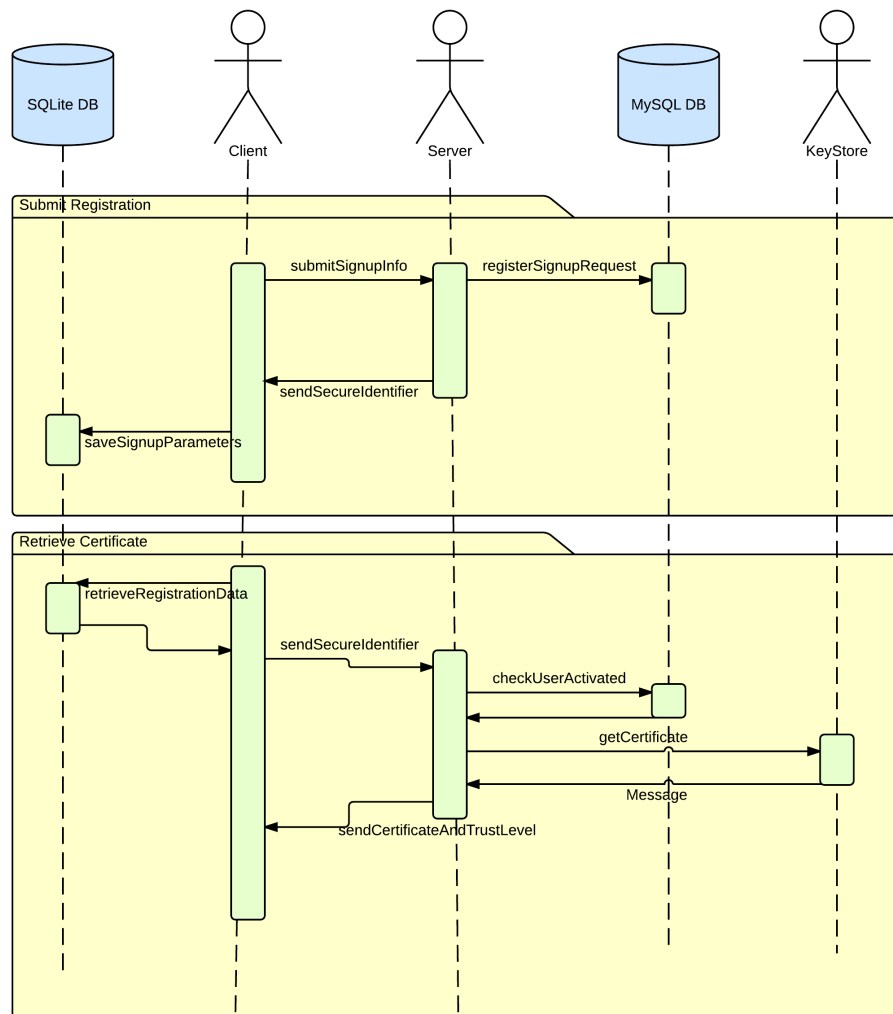


Figura 2.3: Diagramma di sequenza rappresentante le due fasi principali della registrazione al sistema

La fase di registrazione, i cui passi principali sono illustrati nel diagramma di sequenza in figura 2.3, è composta di due fasi. Nella prima fase il nuovo utente comunica al server autenticato le proprie credenziali (nome, cognome, chiave pubblica, organizzazione di appartenenza, città e paese di residenza) che vengono salvate nel database in attesa di elaborazione. Come risposta della presa in consegna della richiesta, il server genera un token unico (**SecureID**) che successivamente il client può utilizzare per recuperare

2.3. FOCUS SULLA SICUREZZA

il proprio certificato e che deve essere tenuto segreto dall'utente. La fase di elaborazione viene eseguita dall'amministratore che si accerta che i dati sottomessi dall'utente siano corretti e veri. A questo punto, l'amministratore ha due possibilità: abilitare l'utente all'uso del sistema oppure respingere la sua domanda. Nel secondo caso non avverrà nulla e l'utente verrà informato al successivo accesso che la sua richiesta è stata respinta. Nel caso in cui invece la richiesta venga accolta, viene generato un certificato utilizzando le credenziali e la chiave pubblica dell'utente e firmato utilizzando la chiave privata del server. Questo farà sì che il server possa stabilire in un secondo momento l'autenticità del certificato e capire quindi se è stato emesso da lui oppure no (decisione importante per capire se l'utente può accedere alle varie funzionalità). Successivamente il certificato generato viene salvato nel KeyStore del server. Nella seconda fase (corrispondente al blocco in basso in figura 2.3) l'utente utilizza il **SecureID** per recuperare il proprio certificato. Da quel momento in poi potrà utilizzare a pieno tutte le funzionalità del sistema compatibilmente con il **livello di fiducia** assegnato.

Quello appena descritto è ciò che avviene dal punto di vista del server. Per quanto riguarda l'applicazione client, la procedura di registrazione prepara all'utente l'ambiente per l'utilizzo del sistema. In particolare vengono generate directory dedicate dove verranno posti i dati temporanei delle elaborazioni e soprattutto il database SQLite cifrato dove sono memorizzati i dati sensibili dell'utente. Durante la registrazione inoltre viene generato un codice (diverso dal precedente **SecureID**) che l'utente utilizzerà successivamente per eseguire il login al sistema. È stato dunque messo in piedi un login con doppia autenticazione per ridurre al minimo le probabilità di furto di identità.

2.3.2 Composizione e lettura dei documenti

Si tratterà adesso l'aspetto principale di questo progetto: l'elaborazione dei documenti. Si descriveranno in modo dettagliato le procedure che sono state implementate per costruire, cifrare e decifrare i contenuti.

Costruzione del documento

In questo paragrafo verrà analizzata l'impaginazione del documento cartaceo che ha il formato di un foglio A4 molto comodo per il processo di stampa di scansione con periferiche esterne.

2.3. FOCUS SULLA SICUREZZA

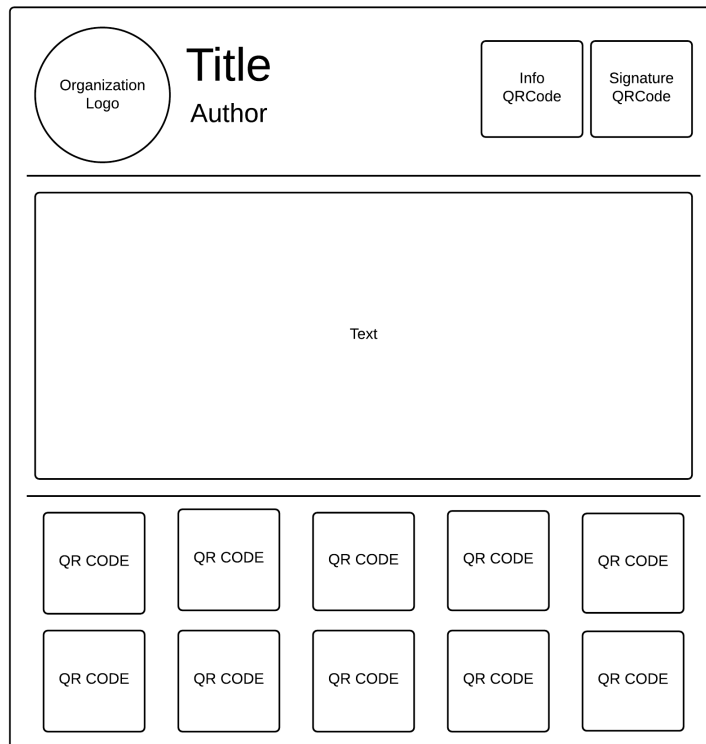


Figura 2.4: Schema delle principali sezioni del documento.

La figura 2.4 illustra le sezioni principali del documento. In alto si ha un'intestazione dove sono presenti un campo per il titolo, uno per l'autore e due QR-Code: in uno sarà impressa la firma dell'utente e nell'altro verranno trasportate informazioni utili a recuperare il contenuto cifrato tra cui:

- titolo;
- mittente;
- UID del mittente (per consentire al destinatario di recuperare la chiave pubblica del mittente e verificare la firma);
- destinatario.

Nella parte centrale c'è il corpo del documento dove l'utente può inserire il testo da inviare. Nella parte in basso vengono posizionati, infine, i QR-Code contenenti il testo cifrato e le informazioni per il posizionamento nel testo che sono anch'esse cifrate.

Cifratura del Documento

Quello mostrato nella figura 2.5 è un diagramma di flusso che ha lo scopo di illustrare la procedura che viene eseguita da quando si compone il documento a quando si produce l'immagine in output (delle proporzioni di un foglio A4 ma a 400 DPI) pronta per essere stampata (la qualità media di stampa di una stampante commerciale è intorno ai 300 DPI).

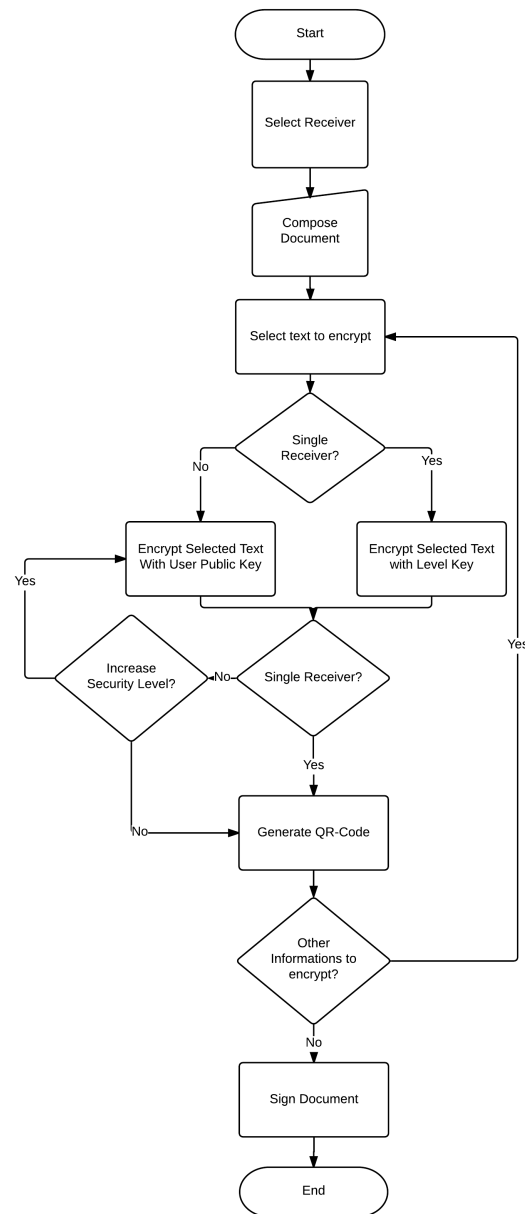


Figura 2.5: Diagramma di flusso per l'operazione di cifratura del documento

Da quello che si può vedere in figura 2.5 il primo passo è rappresentato dalla scelta del destinatario. Dopodiché l'utente compone il documento e può iniziare da subito a cifrare le porzioni di testo che vuole mantenere segrete. A questo punto la procedura può seguire due strade a seconda del tipo di

destinatario: se è uno solo, il testo viene cifrato usando la chiave pubblica dell'utente. In questo modo ci si accerta che solo il possessore della chiave privata possa decifrare. Se invece il messaggio è destinato ad un gruppo di utenti si sceglie preventivamente il livello di fiducia (che individua univocamente il gruppo di utenti). In tal caso si chiederanno al server le chiavi fino al livello scelto (purché si disponga dell'autorizzazione necessaria), e poi si cifrerà il testo selezionato con l'algoritmo AES partendo dalla chiave di livello più basso fino a quella di livello più alto per aumentare il livello di sicurezza proporzionalmente al livello di fiducia richiesto (si ricorda che la quantità di informazioni cui si ha accesso è direttamente proporzionale al Trust Level). Passo finale è la generazione del QR-Code ed il posizionamento di quest'ultimo in fondo al documento. Quando l'utente ha terminato di oscurare le parti sensibili, si passa alla firma del documento. Quello che viene firmato è l'hash dell'immagine comprensiva del corpo del documento e dei QR-Code sottostanti relativi al testo cifrato. L'hash viene calcolato utilizzando una funzione di **perceptual hashing**. Il perceptual hash, è un particolare tipo di hash che presenta uno scarsissimo **avalanche effect**. Questo significa che a scarse variazioni dell'immagine corrispondono scarse variazioni dell'hash. Questa tecnica è particolarmente utile in questo caso; utilizzare funzioni di hash crittografico come ad esempio la SHA1 non è, infatti, opportuno perché presentando un forte **avalanche effect** basterebbe che un solo byte dell'immagine cambiasse per produrre un hash quasi totalmente diverso. Dopo un processo di Print & Scan è normale che l'immagine originale subisca delle alterazioni per quanto riguarda risoluzione, colore o contrasto e addirittura disturbi, per esempio una banale piegatura del foglio. Il perceptual hashing aiuta quindi a non preoccuparsi di tutte le possibili variazioni che possono avvenire nei vari processi. Tuttavia dal punto di vista della sicurezza questo non è il massimo a cui si può ambire. Purtroppo è possibile che alcune particolari manipolazioni dell'immagine non vengano rilevate, problema che tutt'ora rimane aperto.

Decifrazione del Documento

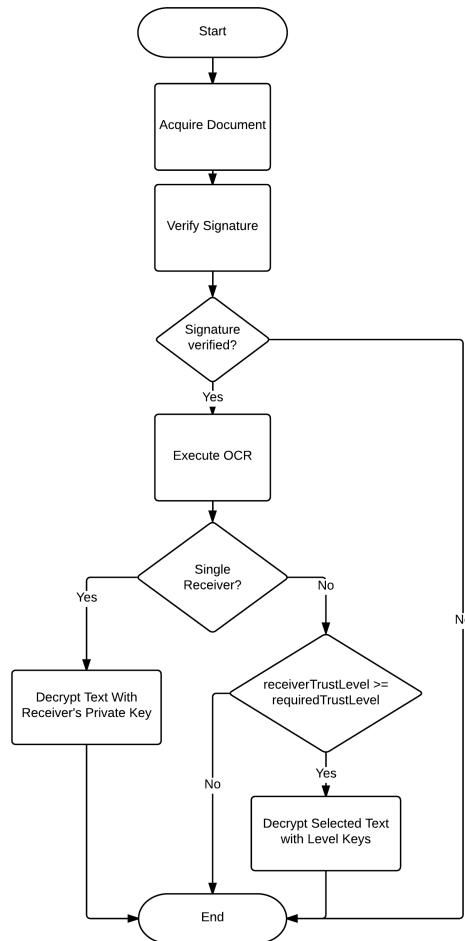


Figura 2.6: Diagramma di flusso per l'operazione di decifrazione del documento

Come si può immaginare il processo di decifrazione è esattamente l'inverso del processo di cifratura. Il primo passo è, infatti, l'acquisizione del documento, e poi successivamente la verifica della firma. La verifica avviene nel seguente modo:

1. si legge il QR-Code relativo alla firma;
2. si decodifica la firma con la chiave pubblica del mittente;

2.3. FOCUS SULLA SICUREZZA

3. si esegue il **perceptual hashing** del documento (corpo più QR-Code in basso);
4. si confronta l'hash ottenuto con quello derivato dalla decodifica della firma. Il confronto consiste nel calcolare la distanza di Hamming tra le due stringhe e nello stabilire quanti sono i caratteri diversi. Tale confronto può essere effettuato agevolmente perché l'output della funzione di perceptual hashing è una stringa composta di 0 e 1. Si è deciso di stabilire in maniera empirica un compromesso sulla percentuale di match al 90%.

Dopo la verifica della firma, la procedura di decifrazione è esattamente l'inverso di quella di cifratura tenendo conto anche della distinzione dei casi in cui il destinatario sia singolo o un gruppo di utenti. L'output finale non è altro che il documento ricomposto utilizzando il sistema OCR per recuperare il testo in chiaro e i QR-Code decodificati e decriptati per la parte cifrata. Il testo così ottenuti è di nuovo modificabile e riutilizzabile per una successiva spedizione.

Capitolo 3

Funzionamento dell'applicazione

In questo capitolo si illustreranno le modalità di funzionamento dell'applicazione implementata. Come già detto nel capitolo 2, l'applicazione si compone di due parti: server e client.

3.1 Server

Il server ha lo scopo di gestire gli utenti, i certificati relativi e di distribuire le chiavi di livello e le chiavi pubbliche degli utenti certificati.

L'applicativo può essere eseguito in due modi:

- da riga di comando tramite l'istruzione:
`java -jar -DprogettoSII.configuration=<path-to-conf.properties>
<path-to-jar>/server.jar;`
- tramite l'IDE *Eclipse* impostando opportunamente il percorso del file `conf.properties` nella configurazione di esecuzione (**Run Configuration**).

Se l'applicazione viene lanciata da riga di comando è necessario inserire una password che serve a sbloccare il keystore. Dopo aver eseguito questo passaggio è possibile impartire comandi al server direttamente dal terminale. I comandi che sono disponibili ora sono: **quit** e **adminconf**. Il primo chiude il server in maniera *graceful* mentre il secondo avvia l'interfaccia grafica che consente all'amministratore di interagire con i dati degli utenti.

3.2. CLIENT

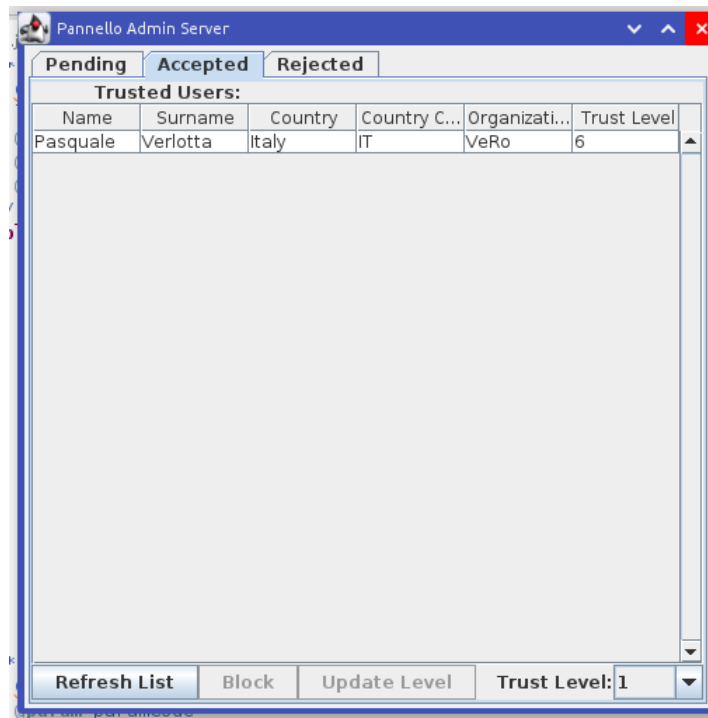


Figura 3.1: Interfaccia grafica del server.

Come si vede nella figura 3.1 ci sono tre schede riferite ad altrettante liste:

- **Pending** in cui compare la lista degli utenti che intendono registrarsi al sistema e attendono l'intervento dell'amministratore ;
- **Accepted** in cui c'è la lista degli utenti certificati che sono autorizzati all'accesso al sistema;
- **Rejected** in cui compare la lista degli utenti bloccati a cui è negato l'accesso.

I pulsanti in basso consentono di accettare o rifiutare o aggiornare le richieste degli utenti.

3.2 Client

Il client ha lo scopo di gestire le funzionalità di registrazione, login, cifratura e decrittazione. La registrazione consiste nel riempire un form con dati

3.2. CLIENT

anagrafici e i percorsi dei file delle cartelle necessarie per salvare i documenti cifrati/decifrati. Se la registrazione va a buon fine, cioè il server autentica l'utente, viene rilasciato un **SecureID**, che insieme con i dati inseriti viene scritto su un pdf generato automaticamente e salvato nella cartella di output scelta. Il login consente di accedere all'applicazione e consiste nel riempire un form con Nome, Cognome, Password e il Codice rilasciato all'atto della registrazione.



The image shows a graphical user interface (GUI) for a login system, titled "Progetto SII". The interface has a yellow background. It contains several input fields and buttons:

- Two input fields for "First Name" and "Second Name" at the top.
- A password input field with masked characters (dots).
- A "Code" input field.
- Two blue buttons labeled "LOGIN" and "CANCEL" below the input fields.
- A text prompt "Se e' il primo avvio registrati" (If it's the first start, register).
- A blue button labeled "REGISTRATION" below the prompt.

Figura 3.2: GUI di login

Dopo aver effettuato il login si accede alla schermata principale

3.2. CLIENT

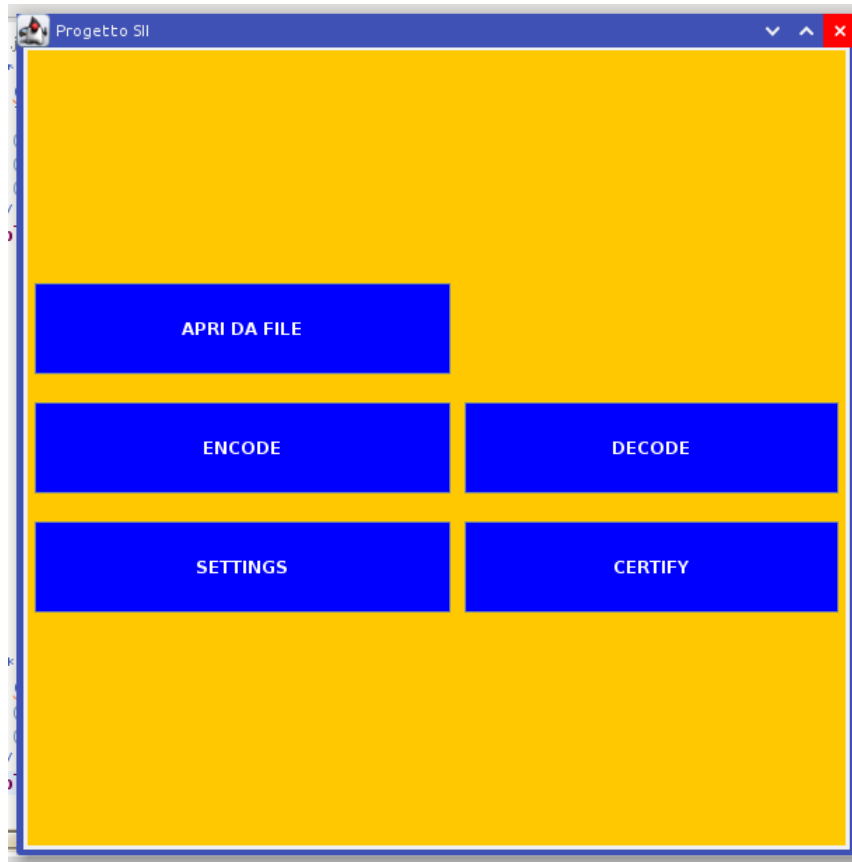


Figura 3.3: GUI della schermata principale

Da questa schermata si accede alle funzionalità dell'applicazione cliccando i diversi pulsanti

- **APRI** - consente di scegliere un file dal file system locale. Se il file scelto è un'immagine viene caricata la GUI per la decodifica, mentre se il file è un testo (.txt) viene caricata la GUI per la codifica;
- **ENCODE** - carica la GUI per la codifica;
- **DECODE** - carica la GUI per la decodifica;
- **CERTIFY** - la funzionalità necessaria per essere abilitati alla codifica e decodifica. Al primo login occorre, infatti, scaricare il certificato dal server, se l'amministratore ha autorizzato l'utente, ed aggiornarne i dati.

3.2. CLIENT

3.2.1 Cifratura

La seguente figura 3.4 illustra la GUI per la composizione di un file da criptare. Vi si accede cliccando **ENCODE** nella schermata principale, e selezionando un file.

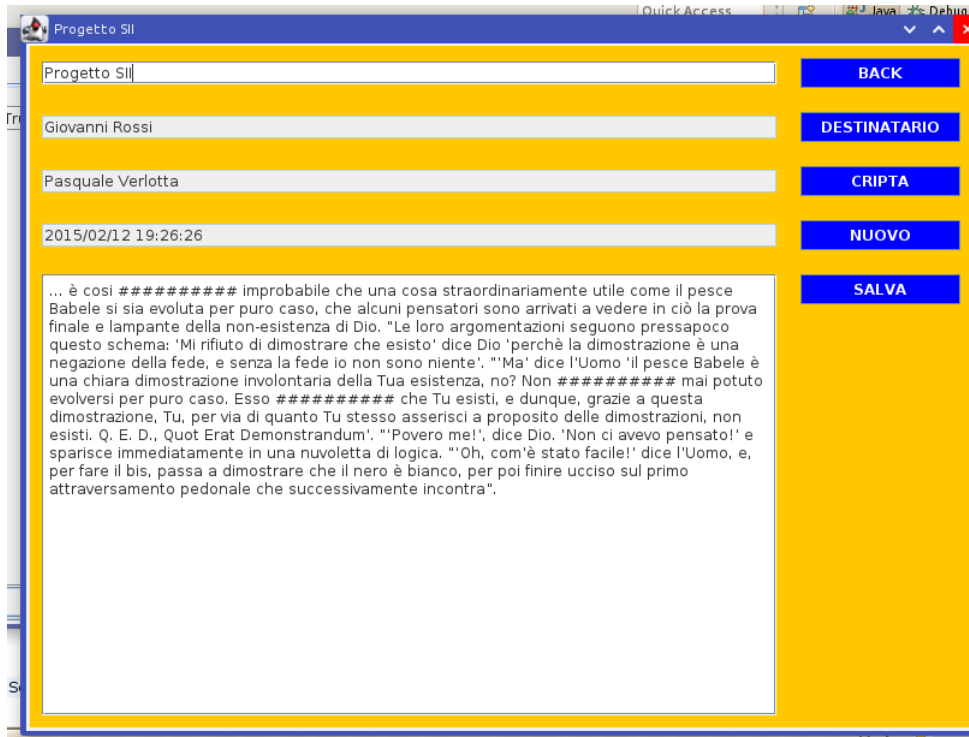


Figura 3.4: Intefaccia grafica per la codifica

La schermata si compone di cinque campi:

- Il **titolo** che comparirà nell'intestazione del documento;
- L'**autore** del documento, che viene riempito in automatico con il nome e cognome dell'utente loggato;
- Il **destinatario** che viene impostato tramite il pulsante **DESTINATARIO**, che consente di scegliere se cifrare per un singolo utente, o per un livello;
- Le **informazioni** che per il momento consistono in data e ora della creazione del documento;

3.2. CLIENT

- L'area nella quale verrà inserito automaticamente il testo preso dal file selezionato.

e di cinque pulsanti, con funzioni autoesplicative.

Una volta selezionato il destinatario del documento si seleziona il testo da cifrare e si preme il pulsante **CRIPTA** che esegue la cifratura tramite RSA con la chiave pubblica del destinatario o tramite AES con le chiavi di livello, partendo dal livello 1 fino al livello scelto, ed infine sostituisce il testo selezionato con una serie di hashtag. Il pulsante **SALVA** genera il QR-Code contenente la firma del documento cifrata, il QR-Code con le informazioni in chiaro per decrittare, e i QR-Code relativi alle parti di testo criptate. Una volta terminata la cifratura viene generata l'immagine come descritto nel capitolo 2.

3.2.2 Decifrazione

La seguente figura 3.5 illustra la GUI per la composizione di un file da decrittare. Vi si accede cliccando **DECODE** nella schermata principale, e selezionando un file.

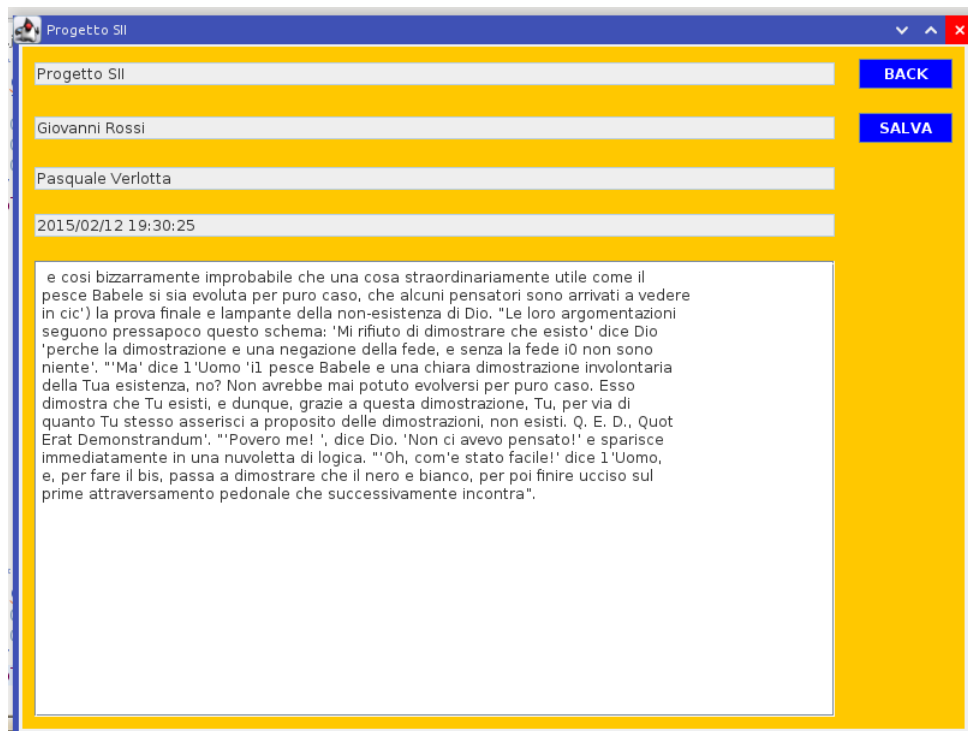


Figura 3.5: Interfaccia grafica per la decodifica

3.2. *CLIENT*

La GUI ha gli stessi campi della GUI per l'encode, con la differenza che questi sono riempiti in automatico dal sistema in fase di decriptazione del documento e il testo è in chiaro, decriptato quindi. Nel caso il testo contenga ancora gli hashtag significa che non si ha il privilegio di decriptare il file, perché o non si ha il livello autoritativo necessario o non si è il destinatario del documento.

Capitolo 4

Conclusioni

Nel corso di questo progetto, si è sviluppato un prototipo funzionante dell'applicazione richiesta completa di tutte le principali funzionalità. Tuttavia ancora molto si potrebbe fare per migliorarla e per superare le limitazioni che tuttora sussistono. Tra queste ci sono limitazioni riguardanti per esempio il numero di pagine del documento prodotto che non possono essere superiori a 1. Un altro problema da superare è la limitata quantità di QR-Code che si possono inserire nella parte sottostante del documento.

Quindi tra gli sviluppi futuri di questo progetto ci sono:

- la possibilità di produrre un documento di più pagine;
- la possibilità di inserire un maggior numero di QR-Code o di utilizzare questi ultimi al massimo delle loro possibilità per memorizzare quante più informazioni cifrate possibili;
- la possibilità di inserire immagini nel corpo del documento;
- migliorare l'affidabilità della funzione di perceptual hashing implementata conducendo studi di natura più avanzata;
- implementare un'applicazione mobile o un' interfaccia web che renda più agevole l'uso del servizio (sfruttando magari la realtà aumentata nel caso mobile...).