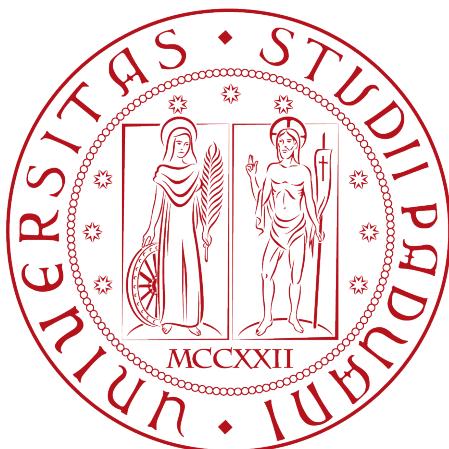


Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA “TULLIO LEVI-CIVITA”

CORSO DI LAUREA IN INFORMATICA



Gestione sicura di chiavi crittografiche su
dispositivi mobili

Tesi di Laurea

Relatore

Prof. Tullio Vardanega

Laureando

Gabriele Di Pietro

Matricola 2010000

ANNO ACCADEMICO 2024–2025

Gabriele Di Pietro: *Gestione sicura di chiavi crittografiche su dispositivi mobili*, Tesi di Laurea, © Dicembre 2025.

LOREM IPSUM

DOLOR SIT AMET, CONSECTETUER ADIPISCING ELIT.

— Oscar Wilde

Dedicato a ...

Sommario

“Life is really simple, but we insist on making it complicated”

— Confucius

Ringraziamenti

Padova, Dicembre 2025

Gabriele Di Pietro

Indice

1	Contesto aziendale	1
1.1	Presentazione azienda	1
1.2	Rami aziendali e progetti	2
1.3	<i>Way of working</i>	3
1.3.1	Tecnologie interne	3
1.3.2	<i>Smart working</i> e strumenti di comunicazione	5
1.4	Spirito di innovazione aziendale	6
2	Stage	8
2.1	Visione aziendale	8
2.1.1	Offerte aziendali	8
2.1.2	Stage in azienda	10
2.1.3	Ruolo del tutor aziendale	10
2.2	Motivazione dello <i>stage</i>	11
2.3	Progetto proposto	12
2.4	Obiettivi e vincoli	13
2.4.1	Obiettivi	13
2.4.2	Vincoli	14
2.5	Scelta dello <i>stage</i>	15
2.5.1	Motivazioni della scelta	15
2.5.2	Obiettivi personali prefissati	15
	Bibliografia	17

Elenco delle figure

1.1	Sedi operative dell'azienda - Fonte: synclab.it	1
1.2	Alcuni prodotti offerti dall'azienda - Fonte: synclab.it	2
1.3	Tecnologie impiegate nella realizzazione dell'applicativo.	3
1.4	Strumenti di supporto.	4
1.5	Strumenti di comunicazione	5
1.6	Progetto di <i>stage</i> come interesezione tra le aree di competenze consolidate di <i>SyncLab</i> e l'obiettivo di innovazione tecnologica dell'azienda.	6
2.1	Collaborazioni dell'azienda - Fonte: synclab.it	8
2.2	Contributo dei programmi di <i>stage</i> in SyncLab.	9
2.3	Investimento strategico degli <i>stage</i> per l'azienda	10
2.4	Confronto tra lo sviluppo nativo e l'approccio <i>cross-platform</i> con <i>Flutter</i>	11
2.5	Esempio di comunicazione criptata	13
2.6	Schema che rappresenta l'architettura di sistema, la chiave blu corrisponde alla chiave pubblica, quella rossa invece corrisponde alla chiave privata	14

Elenco delle tabelle

Capitolo 1

Contesto aziendale

Il presente capitolo introduce l'azienda **SyncLab S.r.l.**, presso cui ho svolto l'attività di *stage*, fornendo la base necessaria alla comprensione del progetto di tesi. Verranno descritti gli ambiti in cui l'azienda opera, gli strumenti e i processi di *Way of working* di cui ho avuto esperienza diretta e la sua propensione all'innovazione, elemento cruciale in relazione allo sviluppo di un'applicazione innovativa come quella descritta nei futuri capitoli.

1.1 Presentazione azienda

L'azienda ospitante, *SyncLab S.r.l.* è stata fondata nel 2002 a Napoli e si è affermata fin da subito come una realtà innovativa attenta ai paradigmi della trasformazione digitale. Nel corso degli anni, la società ha intrapreso un significativo processo di espansione a livello nazionale, che l'ha portata ad aprire sei sedi operative distribuite sul territorio italiano.



Figura 1.1: Sedi operative dell'azienda - Fonte: synclab.it

Inizialmente nata come *software house*, l'azienda si è dedicata allo sviluppo di soluzioni *software* innovative, progettate ex novo in base alle opportunità e alle esigenze del mercato. In tale contesto, la società si distingue per la sua vocazione all'innovazione tecnologica e alla trasformazione digitale, realizzando prodotti e fornendo servizi in diversi settori strategici, tra cui quello sanitario, energetico, industriale, finanziario e logistico.

Nel tempo, *SyncLab S.r.l.* ha ampliato il proprio raggio d'azione, assumendo un ruolo rilevante come *system integrator*. In questa veste l'azienda si occupa dell'ottimizzazione, integrazione e manutenzione di soluzioni *software* già esistenti per conto di clienti esterni, offrendo supporto tecnologico e consulenziale volto a favorire l'adozione delle

più recenti innovazioni digitali. Questa evoluzione ha permesso all'azienda di diventare uno dei principali *system integrator* del panorama italiano nel settore dell'*Information and Communication Technology (ICT)*.

La duplice identità coniuga la creatività e la proattività di una *software house* con l'approccio orientato all'efficienza e al cliente tipico di un *system integrator*, rappresenta uno dei principali punti di forza dell'azienda che è in grado di offrire soluzioni complete e personalizzate.

SyncLab S.r.l promuove attivamente la collaborazione interna, incoraggiando l'interazione non solo tra i membri della stessa sede, ma anche tra i colleghi di sedi diverse. La politica aziendale è volta a favorire un costante scambio di conoscenze e competenze, creando in tal modo un ambiente dinamico, in cui la crescita professionale di ogni individuo è il risultato del lavoro di squadra.

1.2 Rami aziendali e progetti

SyncLab S.r.l collabora con un ampio numero di clienti appartenenti a molteplici settori industriali e tecnologici. Nel corso degli anni l'azienda ha consolidato una presenza trasversale in diversi ambiti, tra cui *web*, *mobile*, *privacy*, *sanitario*, *blockchain* e *trasporti*, sviluppando soluzioni capaci di rispondere a esigenze eterogenee.



Figura 1.2: Alcuni prodotti offerti dall'azienda - Fonte: synlab.it

Alcuni dei *software* che l'azienda ha prodotto sono:

- **Sobereye** (ambito *web*): un'applicazione innovativa progettata per monitorare il rischio di deterioramento neuro-cognitivo dovuto a stanchezza, malori, alcol o stupefacenti all'interno dell'ambiente lavorativo.
- **SynClinic** (ambito sanitario): un sistema integrato che supporta la gestione completa dei processi clinici e amministrativi di ospedali, cliniche e case di cura, consentendo di organizzare e monitorare tutte le fasi del percorso di cura del paziente.
- **DPS 4.0** (ambito *web* e *privacy*): una piattaforma *web* che supporta i titolari, responsabili, *data protection officer* (DPO) nelle attività di conformità del Regolamento Generale Protezione Dati (GDPR) nel rispetto del principio di *accountability*.

- **Fast Ride** (ambito trasporti): una soluzione per la gestione di servizi di trasporto pubblico a chiamata, in contesti urbani ed extraurbani, pensata per integrare le linee tradizionali con un sistema flessibile, dinamico ed ecocompatibile.

1.3 Way of working

In questa sezione tratterò di alcune tecnologie di cui ho avuto esperienza diretta per lo sviluppo dell'applicazione.

1.3.1 Tecnologie interne

L'azienda utilizza una vasta gamma di tecnologie che includono linguaggi di programmazione e *framework* all'avanguardia. Per la mia esperienza e lo sviluppo di un applicazione mobile ho utilizzato:

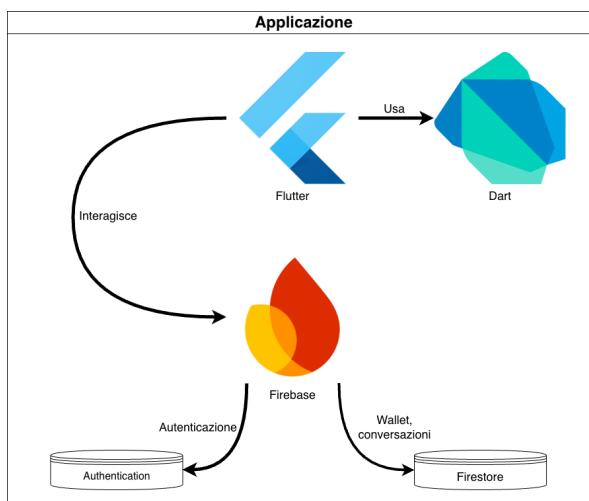


Figura 1.3: Tecnologie impiegate nella realizzazione dell'applicativo.

- **Dart**: linguaggio di programmazione orientato agli oggetti sviluppato da Google, noto per la sua versatilità. Offre numerosi vantaggi come:
 - lo sviluppo di un applicativo *cross-platform* che consente di creare applicazioni native per diversi sistemi da un'unica base di codice.
 - compilazione *Ahead-Of-Time (AOT)* che accelerano lo sviluppo.
 - supporto alla programmazione asincrona che riduce la gestione dei processi in *background*.
- **Flutter**: un *framework* basato su Dart per lo sviluppo di applicazioni multi-piattaforma, che offre vantaggi come:
 - **Hot-reload**: permette di visualizzare immediatamente le modifiche al codice durante lo sviluppo senza dover aspettare una nuova compilazione.
 - **Compatibilità con material**: mette a disposizione un ricco arsenale di *widget* per creare interfacce utente moderne e accattivanti, senza dover scrivere molte righe di codice.

- **Firebase:** un *database* sviluppato da Google e ben integrato con Flutter che offre una serie di funzionalità di *backend* pronte all'uso per la propria applicazione.
 - **Authentication:** servizio che offre i servizi di *backend* e librerie pronte all'uso per autenticare gli utenti nell'applicazione in molteplici modi.
 - **Firestore:** *database NoSQL* orientato ai documenti, che permette di archiviare i documenti in raccolte, dove queste ultime fungono da contenitori per organizzare i dati e facilitare le interrogazioni.

Per garantire continuità operativa e un'efficace gestione dei processi collaborativi, è necessario disporre di strumenti in grado di coordinare e sincronizzare le attività del *team*. Di seguito sono elencati alcuni *software* progettati a questo scopo:



Figura 1.4: Strumenti di supporto.

- **Git:** un sistema di controllo versione distribuito che permette di tracciare in modo efficiente le modifiche ai *file* e di coordinare il lavoro tra più sviluppatori. Questo strumento consente ai membri del gruppo di collaborare in maniera strutturata, gestire eventuali conflitti, apportare modifiche senza rischiare di sovrascrivere il lavoro altrui, creare *branch* dedicati allo sviluppo di nuove funzionalità e recuperare agevolmente versioni precedenti dei *file*.
- **Android Studio:** è un ambiente di sviluppo integrato (*IDE*) gratuito, progettato per lo sviluppo di applicazioni **Android**. Questo *software* mette a disposizione degli sviluppatori diverse funzionalità. Ad esempio un sistema di dispositivi *Android* sia fisici, accoppiabili tramite cavo o *Wi-Fi*, che virtuali. Questi ultimi lavorano tramite emulatore integrato che permette di emulare telefoni *smartphone* o *smartwatch*.
- **Xcode:** è un ambiente di sviluppo integrato (*IDE*), sviluppato e mantenuto da Apple che contiene una *suite* di strumenti utili per lo sviluppo di applicazioni per sistemi proprietari Apple.
- **UMLet:** è uno strumento gratuito e *open source* che permette di creare diagrammi UML¹. In particolare diagrammi dei casi d'uso, di sequenza e attività e di esportarli in diversi formati.

¹UML: (Unified Modeling Language) è un linguaggio di modellazione e di specifica

1.3.2 Smart working e strumenti di comunicazione

L'azienda adotta un modello di lavoro prevalentemente da remoto: la presenza in sede è richiesta solitamente due volte a settimana, il lunedì e il venerdì, salvo specifiche esigenze. Questi momenti sono dedicati al confronto diretto sul lavoro svolto, ai progressi raggiunti e alle eventuali difficoltà emerse.

Nel mio caso, trattandosi di un progetto di *scouting* tecnologico, gli incontri con il responsabile designato sono stati più frequenti rispetto alla media. Inoltre, ho mantenuto un contatto costante attraverso un server Discord aziendale dedicato, dove aggiornavo regolarmente lo stato di avanzamento, segnalando nuove scoperte, sviluppi dell'applicazione o problemi riscontrati.

Per garantire una gestione efficace delle attività e tracciare correttamente l'evoluzione del progetto, ho utilizzato diversi strumenti digitali:

- **Google Calendar:** un calendario condiviso che permette la creazione e la modifica di eventi, specificandone durata e luogo. È stato utilizzato principalmente per organizzare le presenze in sede, pianificare riunioni e segnalare eventi interni, come ad esempio incontri sindacali.
- **GitHub Projects:** una sezione di GitHub dedicata alla gestione dei *ticket*, preferita in alternativa a **Trello** normalmente utilizzato dall'azienda. Questo strumento consente di creare *roadmap* e schede integrate con le *issue* dei *repository*, facilitando la pianificazione e il monitoraggio delle attività sia a livello individuale che di *team*.

Per la comunicazione interna durante il lavoro da remoto:

- **Discord:** utilizzato dai dipendenti per lo scambio di informazioni tramite *chat* testuali e vocali. La piattaforma funge anche da spazio per condividere aggiornamenti interni, materiali informativi e risorse formative.



Figura 1.5: Strumenti di comunicazione

1.4 Spirito di innovazione aziendale

L'azienda *SyncLab* si caratterizza per una forte propensione all'innovazione, elemento che guida in modo significativo le sue scelte strategiche e operative. Questa attitudine si manifesta attraverso un duplice orientamento:

1. **Miglioramento delle dinamiche interne:** l'azienda investe costantemente nell'ottimizzazione dei processi di gestione dei progetti e nel consolidamento delle relazioni con i clienti. Parallelamente, promuove la crescita professionale del *team* tramite aggiornamenti continui su metodologie e tecnologie emergenti, in linea con la propria identità di *system integrator*.
2. **Proposizione di soluzioni d'avanguardia:** L'impegno innovativo non si limita all'organizzazione interna, ma si estende alla progettazione di prodotti e servizi allineati alle prospettive future del mercato. In qualità di *software house*, *SyncLab* sviluppa soluzioni pensate non solo per rispondere alle esigenze attuali dei clienti, ma anche per anticipare *trend* tecnologici, generando valore nel medio-lungo periodo.

In questo contesto, orientato alla ricerca dell'avanguardia si è collocata la mia esperienza di *stage*. La vocazione aperta al cambiamento e la flessibilità dell'azienda sono state condizioni centrali che hanno reso possibile lo sviluppo di un progetto basato su Dart e Flutter, tecnologie ancora poco diffuse all'interno dell'organizzazione.

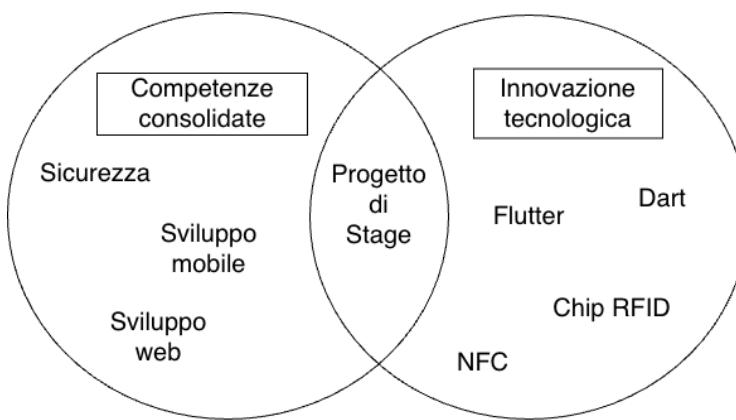


Figura 1.6: Progetto di *stage* come intersezione tra le aree di competenze consolidate di *SyncLab* e l'obiettivo di innovazione tecnologica dell'azienda.

Il progetto si è inserito coerentemente nella strategia aziendale, contribuendo su due fronti principali:

- **Scouting tecnologico:** L'utilizzo di Flutter per la realizzazione di un'applicazione, caratterizzata da requisiti in ambito di sicurezza (crittografia e NFC²), si colloca all'interno di una più ampia iniziativa di valutazione dell'adozione di framework *cross-platform* di nuova generazione per i futuri prodotti aziendali.
- **Adattamento di competenze consolidate:** sebbene *SyncLab* possiede già un panorama della sicurezza e dello sviluppo mobile (come descritto nel Paragrafo 1.2), il progetto ha richiesto la reinterpretazione di alcune conoscenze come la gestione dei *chip* RFID³/NFC e l'impiego di algoritmi crittografici all'interno di un contesto tecnologico completamente nuovo.

L'approccio fondato su posizioni all'avanguardia di *SyncLab* ha rappresentato quindi un motore concreto che ha reso possibile la realizzazione di una soluzione tecnologicamente avanzata. Il progetto di *stage* è stato un vero e proprio banco di prova per l'introduzione di nuove tecnologie, contribuendo alla strategia aziendale di ampliamento e aggiornamento continuo delle competenze interne.

²NFC: Near Field Communication è una tecnologia di ricetrasmissione che fornisce connettività senza fili bidirezionale a distanza a corto raggio

³RFID: Identificazione a radiofrequenza è una tecnologia di riconoscimento e validazione e/o memorizzazione automatica di informazioni a distanza

Capitolo 2

Stage

2.1 Visione aziendale

2.1.1 Offerte aziendali

Per *SyncLab*, i programmi di *stage* rappresentano uno strumento strategico per favorire l'innovazione interna e sostenere l'evoluzione continua delle competenze aziendali. L'azienda considera infatti l'inserimento di stagisti come un'opportunità per acquisire nuove conoscenze e approfondire aree emergenti dell'*information technology*, integrando tali contributi nei progetti esistenti o cogliendo l'opportunità di esplorare tecnologie non ancora adottate. Lo *stage* diventa così un mezzo per cercare soluzioni e idee che, nell'impegno continuo sulle attività operative quotidiane, difficilmente verrebbero affrontate. Al tempo stesso, offre allo stagista un contesto professionale nel quale sviluppare nuove competenze e specializzarsi in ambiti di interesse. Questo modello è reso possibile da una rete consolidata di collaborazioni con università italiane ed estere, che garantisce un continuo scambio di conoscenze e talenti.



Figura 2.1: Collaborazioni dell'azienda - Fonte: synclab.it

I programmi di *stage* si articolano principalmente in tre aree:

- **Integrazione:** gli stagisti contribuiscono al perfezionamento di *software* già in uso, intervenendo su funzionalità specifiche. Tale attività consente di ampliare la comprensione delle potenzialità delle soluzioni aziendali e di migliorarne progressivamente le *performance*.
- **Analisi e ottimizzazione:** questa area prevede una valutazione approfondita delle soluzioni *software* esistenti, con l'obiettivo di individuare inefficienze, proporre miglioramenti e ottimizzare i processi. L'approccio critico e analitico adottato permette di valorizzare al massimo il patrimonio tecnologico dell'azienda.
- **Innovazione:** in questo ambito gli stagisti svolgono analisi teoriche e sperimentazioni su tecnologie emergenti, con *focus* specifici allineati agli obiettivi strategici aziendali. Questa attività valuta il potenziale innovativo delle nuove tendenze e di identificare possibili applicazioni operative.

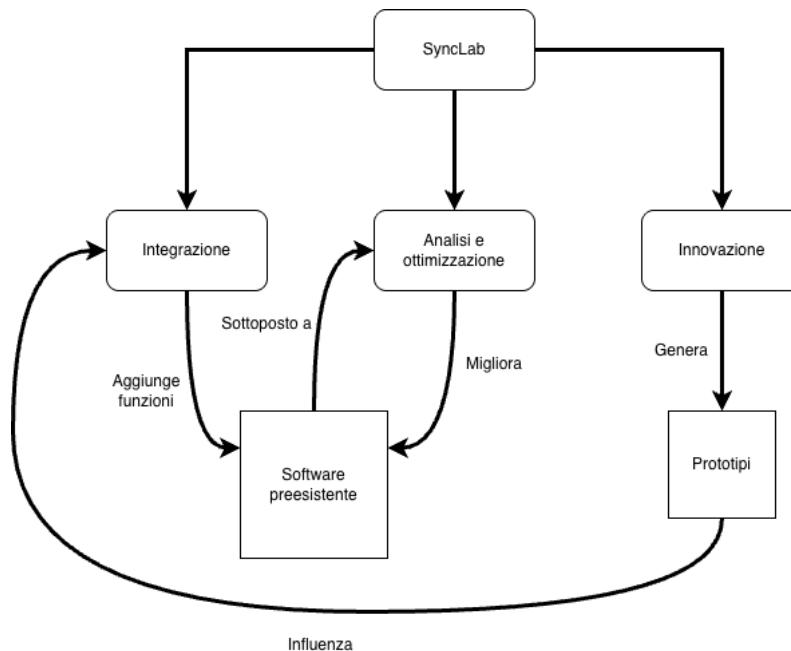


Figura 2.2: Contributo dei programmi di *stage* in SyncLab.

2.1.2 Stage in azienda

Gli *stage* presso *SyncLab* rappresentano un investimento strategico bidirezionale, che riflette la duplice identità aziendale, orientata alla crescita interna e all'avanguardia tecnologica. I programmi sono concepiti come un ciclo continuo di apprendimento, dove l'azienda trae valore dalle competenze degli stagisti quanto questi ultimi traggono esperienza dall'organizzazione. Questo approccio si manifesta attraverso due obiettivi fondamentali:

- 1. Formazione e inserimento di risorse qualificate:** Il programma di *stage* funge da canale primario per identificare e valutare talenti. L'azienda offre un'immersione pratica, consentendo loro di applicare le conoscenze accademiche a problemi reali. La società valuta in modo approfondito il potenziale dei candidati, e gli stagisti che mostrano valore e impegno ricevono offerte di assunzione come membri effettivi del *team*. Questo garantisce all'azienda una *pipeline* costante di nuove risorse già integrate nel proprio ecosistema.
- 2. Acquisizione di nuove competenze:** Il programma di *stage* funge da banco di prova per l'innovazione continua, riducendo così i rischi associati all'adozione di nuove tecnologie. Attraverso questo meccanismo l'azienda rimane all'avanguardia e adatta le competenze consolidate a contesti tecnologici inediti.

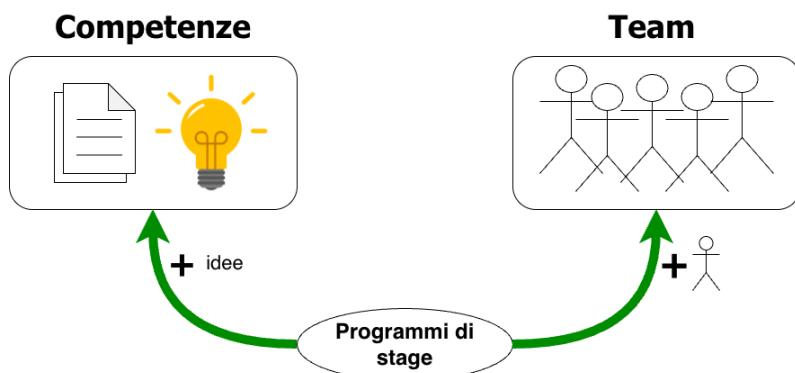


Figura 2.3: Investimento strategico degli *stage* per l'azienda

2.1.3 Ruolo del tutor aziendale

Durante il percorso ad ogni stagista è assegnato a un *tutor*. Il *tutor* è una figura professionale che opera nello stesso ambito in cui lo stagista svolge le proprie attività costituendo di fatto un punto di riferimento. Il suo ruolo ha tre funzioni principali:

- Guida:** il *tutor* propone linee guida su come organizzare il lavoro e fornisce allo stagista materiali utili che possono aiutarlo alla comprensione delle tecnologie da utilizzare nel progetto.
- Supporto:** il *tutor* offre una serie di suggerimenti o soluzioni possibili ai problemi incontrati, questo per scongiurare l'eventualità che il lavoro venga bloccato per lungo tempo e per garantire allo stagista un confronto con una figura preparata stimolando una soluzione concreta.

- **Supervisore:** il *tutor* offre *feedback* allo stagista nella valutazione del lavoro svolto per verificarne la qualità e supportarlo al miglioramento. Questa attività è molto utile in quanto migliorativa nei confronti dello stagista per formarlo verso un percorso professionale.

Nel mio caso i dialoghi con il *tutor* assegnato sono stati molto importanti in quanto senza il suo confronto, e i suoi *feedback*, avrei incontrato maggiori ostacoli, ed i conseguenti ritardi, nello sviluppo del progetto. Anche i suggerimenti sull'architettura di sistema, l'organizzazione delle cartelle, e un congruo supporto all'analisi del problema sono state fondamentali per la progettazione dell'applicazione e per la comprensione dei vari componenti da utilizzare.

2.2 Motivazione dello *stage*

Lo *stage* si è posto l'obiettivo di valutare la fattibilità e il potenziale impiego di nuove tecnologie nello sviluppo di prodotti futuri. Lo sviluppo nativo per **Android** e **iOS** richiede competenze eterogenee e la gestione di *codebase* separate, con conseguenti costi di manutenzione e sviluppo elevati che potrebbero rappresentare un costo elevato. Un'altra dimensione riguarda l'utilizzo di una cifratura *end-to-end* che consente di rendere dei messaggi inseriti nell'applicazione illeggibili ad un intercettatore, implementando quindi un'applicazione mobile capace di generare e gestire dei *wallet* crittografici, comprensivi di coppie private e pubbliche. Per questo motivo, lo stage ha previsto lo studio e la valutazione del *framework Flutter* e linguaggio Dart, che consentono di sviluppare un'applicazione mobile per diversi dispositivi tramite un'unica *codebase*.

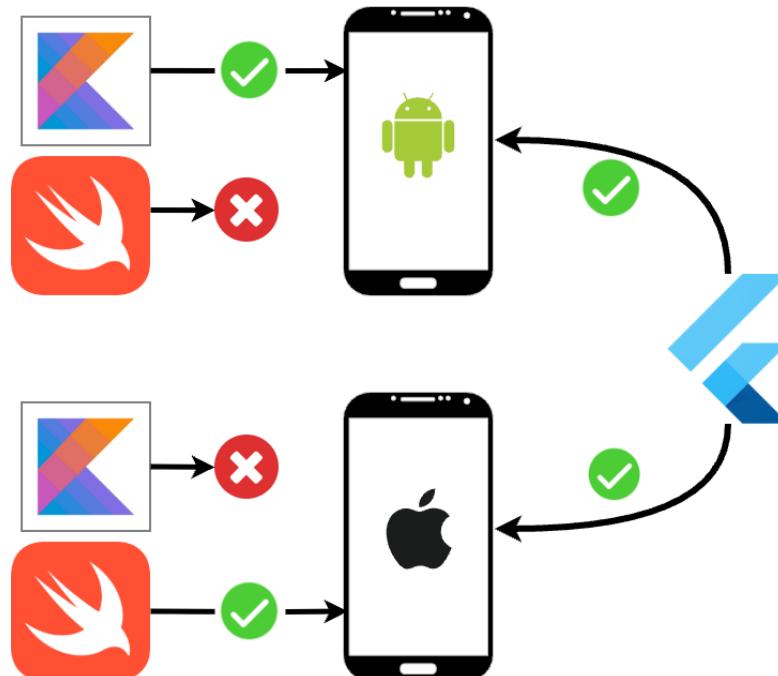


Figura 2.4: Confronto tra lo sviluppo nativo e l'approccio *cross-platform* con *Flutter*

2.3 Progetto proposto

Nel contesto attuale, i dispositivi mobili rappresentano uno strumento di comunicazione ampiamente diffuso e accessibile. Tuttavia, l'utilizzo di canali comuni espone gli utenti a potenziali rischi di intercettazione e compromissione della *privacy*. In questo scenario, la protezione delle comunicazioni assume un ruolo centrale e richiede soluzioni tecniche in grado di garantire riservatezza e integrità dei messaggi scambiati.

Si richiede la progettazione e l'implementazione di un'applicazione in grado di generare e gestire *wallet* crittografici, comprensivi di coppie di chiavi private e pubbliche.

La realizzazione del progetto ha comportato l'identificazione e la risoluzione delle seguenti sfide progettuali e tecnologiche.

Sviluppo multipiattaforma

L'applicazione deve essere sviluppata interamente tramite il *framework* Flutter, e deve poter girare su dispositivi diversi con architetture diverse, sia *Android* che *iOS* a partire da un'unica base di codice in modo tale che sia mantenibile senza l'impiego di numerose risorse. Questo richiede uno studio approfondito del *framework* e del linguaggio di programmazione Dart, che potrebbe rappresentare un onere importante.

Algoritmi di crittografia

Sviluppare un'applicazione che permetta di verificare che gli algoritmi di crittografia vengano impiegati correttamente in modo tale che i messaggi inseriti nell'applicazione vengano letti solo da interessati e non da esterni. Questo richiede uno stratagemma oppure lo sviluppo di qualcosa che consenta allo *stakeholders* di vedere come i messaggi vengano criptati e decriptati.

Gestione delle chiavi crittografiche

Il recupero della chiave privata usata per decifrare un messaggio rappresenta una grossa sfida in quanto l'applicazione deve poter generare più chiavi crittografiche e soprattutto l'applicazione deve supportare il passaggio dati da un dispositivo ad un altro nuovo in caso di smarrimento. Quindi ci deve essere una base di dati che consente il recupero di informazioni sul dispositivo, ma alcune di queste informazioni devono essere trasmesse in modo differente.

Integrazione con il lettore NFC

L'applicazione deve supportare l'utilizzo del lettore NFC presente sui dispositivi mobili in modo da associare i documenti con chip RFID validi alle chiavi salvate sul dispositivo. Quindi bisogna capire che dati si possono prendere dai documenti tramite l'utilizzo di librerie Flutter/Dart e come poterle integrare nell'applicazione.

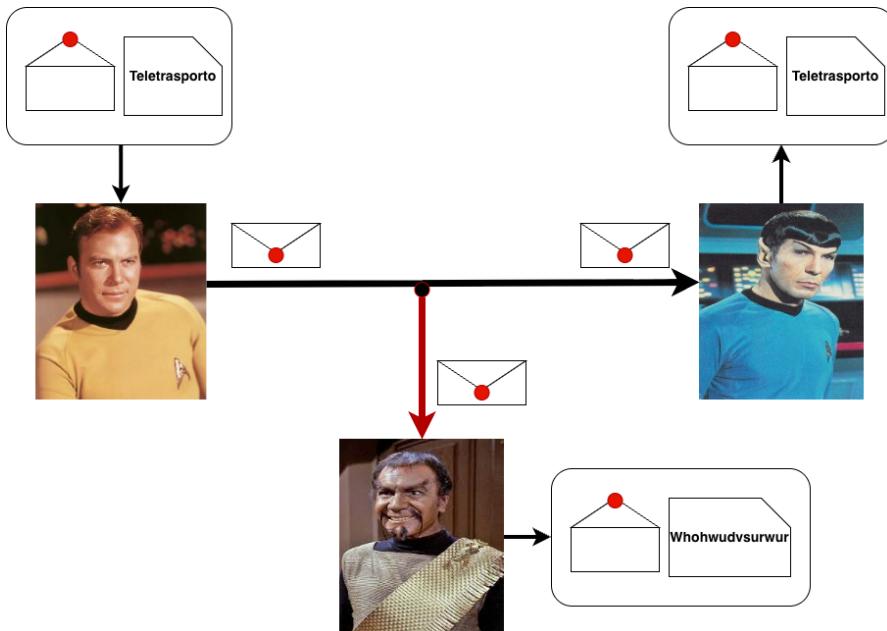


Figura 2.5: Esempio di comunicazione crittata

2.4 Obiettivi e vincoli

2.4.1 Obiettivi

Il progetto proposto è stato guidato da una serie di obiettivi volti al fine di garantirne il successo e la produzione di risultati concreti. In particolare gli obiettivi specifici del progetto sono: lo **studio di fattibilità** e un successivo **sviluppo di una applicazione** da eseguire almeno sui dispositivi *Android*.

Studio di fattibilità: effettuare uno studio dettagliato e un’analisi approfondita sulla fattibilità tecnica sull’utilizzo di Flutter e delle sue librerie per la realizzazione di un applicazione funzionante. In particolare uno studio concentrato su:

- l’integrazione con il *server Firebase*;
- il funzionamento del lettore NFC;
- la generazione di una coppia di chiavi (pubblica e privata) crittografiche;

Questo per permettere di valutare le potenzialità e i limiti degli strumenti, in modo da individuare i migliori da utilizzare per lo sviluppo dell’applicazione.

Sviluppo di una applicazione: per verificare che i componenti applicativi funzionino bene tra di loro, e che permetta di associare i documenti scansionati con le coppie di chiavi generate direttamente dall’applicazione.

2.4.2 Vincoli

Nella realizzazione di un progetto è fondamentale considerare i vincoli ovvero delle restrizioni e limitazioni che devono essere considerate per garantire il successo del progetto. Questi ultimi infatti incidono in modo incisivo sulle scelte architetturali da prendere in considerazione durante la progettazione.

- **Vincoli tecnologici:**

- **Utilizzo obbligatorio del framework Flutter:**

L'intera applicazione deve essere sviluppata interamente tramite *Flutter*, che comporta l'utilizzo del linguaggio *Dart* per tutta l'implementazione della logica applicativa. Questo rappresenta un vincolo rilevante poiché rispetto ad altri linguaggi come Java la comunità di sviluppatori è più contenuta. Di conseguenza, la disponibilità di pacchetti e librerie potrebbe risultare limitata o acerba, specialmente per funzionalità specifiche.

- **Utilizzo del piano gratuito di Firebase:**

L'uso di *Firebase* presenta alcune limitazioni derivanti dal piano gratuito, che esclude funzionalità specifiche presenti solo nelle versioni a pagamento. Queste restrizioni incidono sulla progettazione di alcune componenti e sulle scelte implementate.

- **Vincoli architettura di sicurezza:**

- **Protezione della chiave privata:**

L'architettura deve impedire la trasmissione *online* della chiave privata, garantendo però un meccanismo sicuro che consenta all'utente di recuperare il proprio *wallet* che in caso di smarrimento o migrazione su un nuovo *smartphone*.

- **Associazione delle chiavi ai documenti:**

Ogni coppia di chiavi deve essere associata a un documento, e non a tag *NFC* generici.

- **Unicità del *wallet* per documento e *account*:**

Non deve essere consentita la creazione di più *wallet* associati allo stesso documento per un medesimo *account*. Preservando l'unicità della coppia di chiavi per ogni documento, evitando di generare più *wallet* per lo stesso documento, compromettendo la coerenza del sistema.

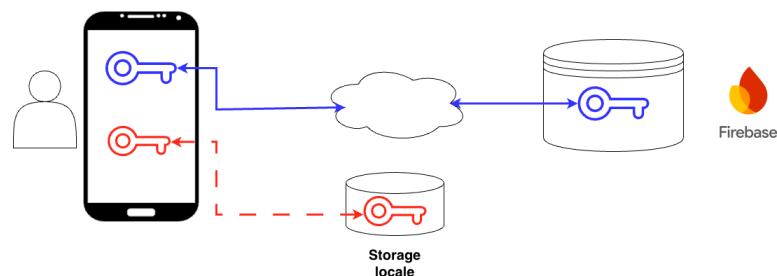


Figura 2.6: Schema che rappresenta l'architettura di sistema, la chiave blu corrisponde alla chiave pubblica, quella rossa invece corrisponde alla chiave privata

2.5 Scelta dello *stage*

2.5.1 Motivazioni della scelta

Ho conosciuto *Synclab* nel mese di aprile attraverso una comunicazione telefonica, inizialmente ho rifiutato l'opportunità proposta poiché intendeva valutare altre possibilità. In seguito, durante il mese di giugno, ho deciso di ricontattare l'azienda, che mi ha presentato due proposte di progetto particolarmente interessanti: la prima riguardava lo sviluppo di un'applicazione con backend basato su Odoo ERP, mentre la seconda consisteva nella realizzazione di un'applicazione mobile sviluppata tramite il framework Flutter, dedicata alla generazione di wallet contenenti chiavi pubbliche e private.

Parallelamente, durante il periodo estivo avevo ricevuto ulteriori offerte di stage da altre aziende e stavo valutando alcune alternative per avviare un percorso lavorativo tempestivamente, nella consapevolezza che l'inizio effettivo dello stage sarebbe comunque avvenuto a settembre per la pausa estiva.

Alla fine ho scelto di intraprendere il mio percorso in *Synclab* per i seguenti motivi:

- **Possibilità di lavorare da remoto**, condizione per me fondamentale poiché, dovendomi spostare frequentemente e non disponendo di un mezzo di trasporto personale, avrei avuto difficoltà a raggiungere quotidianamente la sede aziendale.
- **Elevato livello di autonomia offerto dal progetto**, trattandosi di uno *scouting* tecnologico finalizzato alla valutazione dei punti di forza e delle criticità del framework Flutter. Ciò mi avrebbe permesso di affrontare un lavoro altamente esplorativo, con ampi margini decisionali.

2.5.2 Obiettivi personali prefissati

Nell'attuale contesto tecnologico, l'uso dei dispositivi mobili è divenuto parte integrante della vita quotidiana: la maggior parte delle persone possiede almeno uno smartphone, attraverso il quale comunica e accede a numerosi servizi. Tuttavia, molte applicazioni di messaggistica sono oggi controllate dalle *big tech* e sia l'*hardware* sia il *software* risultano sempre più gestiti da grandi compagnie e sempre meno direttamente dagli utenti.

L'introduzione della proposta di legge europea relativa al controllo delle chat e alla possibilità di analizzare i dati delle conversazioni ha ulteriormente alimentato in me domande sulla reale tutela dei dati personali e sensibili. Le chiavi private degli utenti, che idealmente dovrebbero rimanere sotto il loro esclusivo controllo, sono spesso memorizzate su server esterni per ragioni di praticità.

Da qui è nata la domanda che ha guidato parte della mia motivazione: esiste un modo per conservare le chiavi private in spazi realmente sicuri all'interno del dispositivo, garantendo una protezione efficace e impedendo l'accesso da parte di terzi?

Nello sviluppo dell'applicazione mi ero quindi posto i seguenti obiettivi:

- Progettare un'applicazione capace di gestire i dati privati degli utenti in modo distinto rispetto a quelli pubblici, incrementandone la sicurezza complessiva;
- Apprendere lo sviluppo di applicazioni per dispositivi mobili attraverso l'utilizzo del framework Flutter;
- Acquisire i principi di crittografia necessari a consentire una comunicazione sicura tra due dispositivi mobili.

In conclusione, lo stage presso *Synclab* costituiva per me un'importante occasione per approfondire i concetti di sicurezza informatica affrontati durante il percorso universitario e applicarli in un contesto reale, concreto e di grande rilevanza come il settore delle applicazioni mobili.

Bibliografia

Siti web consultati

Sito SyncLab. URL: <https://www.synclab.it>.