Università degli studi di Padova
Facoltà di Ingegneria
Corso di Laurea Triennale in Ingegneria Informatica

Relazione di tirocinio breve

Mobile Proximity: tecnologie e applicazioni

Laureando: Andrea Zambon
Relatore: Prof. Massimo Rumor

26 Aprile 2010
Anno accademico 2009/2010

Indice

Elenco delle figure

Capitolo 1

Introduzione

1.1 Mobile proximity

Tipicamente al giorno d'oggi, l'acquisto senza moneta cartacea avviene attraverso bancomat e carte di credito. Si sta sempre più diffondendo, però, il concetto di pagamento effettuato attraverso il telefonino, ovvero di Mobile Proximity Payment. Infatti sta crescendo l'interesse verso i sistemi di pagamento a corto raggio senza alcun contatto fisico (contactless), cioè la transazione avviene con un semplice tocco di una carta o di un dispositivo elettronico personale appropriato. Questi sistemi consentono di effettuare spese presso un punto vendita della grande distribuzione, il pagamento del biglietto su un mezzo di trasporto o il caffè da un distributore.
Ci sono diverse realtà o progetti pilota che permettono ai consumatori di effettuare transazioni inviando dati da un terminale mobile ad un POS (point of sale), le tecnologie di comunicazioni radio applicate sono tipicamente:

- Bluetooth
- 802.11x
- Infrarossi
- RFid
- GPRS e SMS.

Inoltre si sta diffondendo l'utilizzo di codici a barre bidimensionali nel telefonino e ben presto sentiremo parlare della nuova tecnologia NFC (Near Field Communications).

A livello internazionale, sono state lanciate alcune sperimentazioni di sistemi contactless che, in particolare, hanno riguardato i mezzi di trasporto. In alcuni Paesi dell'estremo oriente, per esempio Giappone e la Corea del sud, il pagamento

attraverso il telefonino risulta ormai una realtà quotidiana. Sempre in Giappone, per promuovere il turismo locale, è stato prodotto un mazzo di carte da gioco che aiuta i turisti a pianificare le loro visite. Le carte raffiguranti eventi, luoghi e prodotti locali, sono provviste di QR Code che fornisce informazioni e suggerimenti per il visitatore interessato.

Figura 1.1: Informazioni sugli aerei in partenza, aeroporto di Tokio

Le tipiche applicazioni in cui il telefonino può operare in Mobile Proximity sono:

Ticketing e identification. L'utente acquista un biglietto che viene memorizzato sul proprio telefono cellulare, ossia integrato nell'hardware: al momento dell'utilizzo del ticket, il dispositivo emittente è avvicinato ad un terminale ricevente (una obliteratrice, un parchimetro), il biglietto viene riconosciuto e l'accesso è consentito. Tutte le sperimentazioni internazionali sono guidate dai principali circuiti di carte di credito, Visa e MasterCard.

Marketing & Advertising Quando vi è un'interazione tra telefono cellulare e altri dispositivi elettronici (come schermi televisivi, torrette informative, "smart poster" pubblicitari, tabelloni degli orari di treni e autobus, etc.) con l'obiettivo di promuovere un prodotto o per la fruizione di altri servizi d'informazione e pubblicità.

L'introduzione di queste tecnologie, in particolare di NFC, rappresenta uno strumento complementare o addirittura sostitutivo della normale carta di pagamento, e diventa a tutti gli effetti un "borsellino elettronico" che integra diverse carte, ad esempio carte di credito, carte prepagate, carte fedeltà o abbonamento al trasporto pubblico.

Figura 1.2: Il telefonino diventa un “Borsellino elettronico”

1.2 Applicazioni in mobilità esistenti

Senza utilizzare il telefonino, possiamo già trovare alcune realtà italiane, ad esempio nelle stazioni della metropolitana delle principali città le obliteratrici sono dotate di tecnologia RFId per l’ingresso attraverso carta contactless.

Poste italiane è diventata un operatore telefonico mobile, la SIM del telefonino viene abbinata ad un conto postale o ad una carta per transazioni con importi ridotti tra i 5 e i 20 euro.

Trenitalia ha attivato il sistema “prontotreno”. Dall’home page del sito si scarica un software per il proprio telefonino per acquistare i biglietti per i viaggi nazionali. Oltre ad acquistare il tagliando di viaggio tramite la carta di credito è possibile anche richiedere informazioni sugli orari dei convogli e cambiare la propria prenotazione.

Telecom Italia ha lanciato una sperimentazione con l’ATM, l’azienda di trasporti pubblici di Milano. La sperimentazione, riguarderà 200 abbonati ATM ai quali saranno forniti, dalla stessa azienda di trasporti, cellulari basati su tecnologia NFC (Near field communication) ossia in grado di attivare la comunicazione wireless a corto raggio, già dai primi mesi del 2010. Secondo quanto sostengono le due aziende, il servizio di mobile ticketing sarà pienamente a regime e utilizzabile da chiunque viaggi sui mezzi di trasporto pubblico cittadino.

Il comune di Venezia ha avviato il progetto pilota “TagMyLagoon”, una guida della città che sfrutta un’apposita applicazione capace di decodificare QR Code disseminati lungo la città su delle piastrelle, collocate generalmente sui lampioni

o strutture simili, abilitando la ricezione di informazioni sul luogo e sul come raggiungere il punto di interesse successivo. L'obiettivo di questa soluzione è quello di condurre i visitatori alla scoperta della città, attraverso un percorso prestabilito e con la guida del proprio telefonino e dalla rete wi-fi.

Il consorzio Movincom, nell'autunno 2009, ha rilasciato la prima piattaforma in grado di abilitare l'acquisto e l'attivazione di servizi attraverso il telefonino con un occhio alla semplicità di utilizzo. Fino ad oggi la maggior parte dei servizi si basa su sms, ma con la piattaforma di Movincom e l'utilizzo di alcuni menu con dei widget che producono automaticamente gli sms corretti e dei codici a barre bidimensionali si potrà acquistare prodotti e servizi in modo molto semplice. L'obiettivo di Movincom è quello di permettere agli esercenti consorziati di ricevere dai propri clienti, abilitati al servizio, disposizioni di pagamento di beni e servizi semplicemente attraverso il telefonino. Il numero di telefono rappresenta infatti una chiave univoca ed il cliente può effettuare un acquisto in mobilità senza mai inserire i dati sensibili.
Le modalità in cui il cliente può effettuare acquisti o pagamenti via mobile sono:

- un ordine via SMS, attraverso l'invio di una specifica sintassi;
- una applicazione Java, scaricabile su telefono cellulare, che permette l'autocomposizione dell'SMS di richiesta attraverso un menu di selezione del bene desiderato;
- dei tag bidimensionali (es. QR Code) per l'invio automatico del messaggio SMS.

MobileTag è un'altra piattaforma in cui l'utente con il suo telefonino scatta una foto del codice a barre e riceve automaticamente informazioni supplementari. Inoltre è una tecnologia pensata per aiutare l'utente in fase di acquisto di biglietti, o per usufruire di buoni sconto. Non richiede che l'utilizzatore si connetta ad un sito wap né che l'azienda che fa ticketing invii mms. L'utente digita un codice segreto e il telefonino produce un tag che, una volta scannerizzato con i normali lettori di codici a barre presenti nei punti vendita o d'imbarco, diventa un pass per entrare o un metodo di pagamento.

Nel maggio 2008 il quotidiano "La Gazzetta dello Sport" ha lanciato Gazza&Play (fig. 1.3), un servizio mobile multimediale basato su tag a barre bidimensionali, che consente ai lettori d'approfondire le notizie pubblicate sul quotidiano mediante la fruizione di contenuti mobili multimediali (audio e video).

Figura 1.3: Gazza&Play

Il progetto francese “MeePass”, ha un funzionamento molto semplice, una volta che l’utente ha inserito il proprio codice segreto, il software MeePass crea un codice a barre in tempo reale. L’utente presenta quindi il telefonino al punto vendita per farlo leggere dal lettore di codici a barre. Scannerizzando semplicemente il tag di identificazione dell’utente, una richiesta di autorizzazione sarà inviata al server MeePass che istantaneamente approverà o rifiuterà l’identità (fig. 1.4). I dati di un qualsiasi database aziendale possono essere trasmessi al server MeePass per convalida (es. Pagamenti, programmi fedeltà, servizi di ticketing o couponing). Gli account degli utenti possono essere aperti nei punti vendita o online, secondo le modalità scelte dalla società per gestire il MeePass dei propri clienti. Il software MeePass funziona senza costi di connessione (SMS, MMS o WAP), e non utilizza un chipset NFC (Near Field comunication).

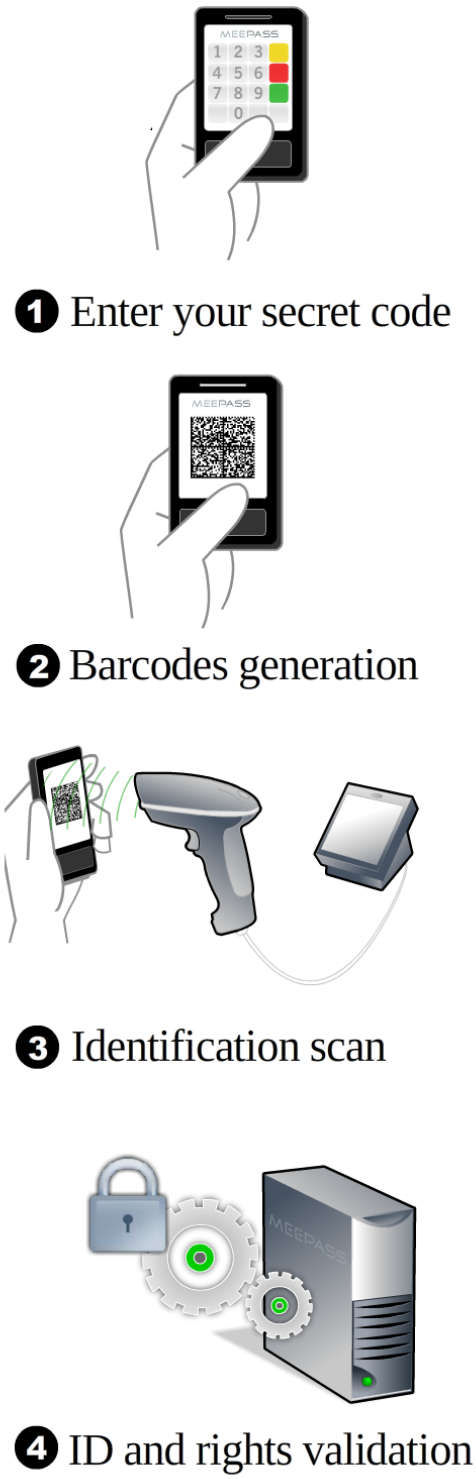

Figura 1.4: Funzionamento di MeePass

1.3 Obiettivi del tirocinio

Obiettivo del tirocinio svolto nel 2009 presso la JumpSolutions S.r.l. è stato la realizzazione di prototipi richiesti da alcuni clienti che hanno interesse ad investire nel campo del Mobile Proximity e Payament.
L'obiettivo d'insieme dei progetti è la realizzazione di applicativi destinati tanto alla vendita/distribuzione quanto alla formazione tecnica e commerciale, rappresentato da una migliore comprensione globale delle tecnologie.
Due sono i prototipi realizzati durante il tirocinio:

- **JTicketing** è l'applicazione sviluppata con particolare riferimento alle esigenze nell'ambito della Fiera del Riso di Isola della scala e che si occupa d'informatizzare il processo di convalida di ticket acquistati via web tramite un sito e-commerce. La tecnologia NFC allo stato attuale è limitata dalla scarsa diffusione di telefonini NFC, quindi JTicketing si propone di essere immediatamente fruibile sul mercato, sfruttando le tecnologie di ampia diffusione quali codice QR, MMS, e-mail.

- **JCheck** è l'applicazione destinata nell'ambito della autenticità dei prodotti, si occupa di fornire supporto tecnologico NFC al riconoscimento dell'autenticità dei prodotti dotati di tag RFID con, in aggiunta, la possibilità di visualizzare informazioni di marketing nei telefonini dei clienti. Il contesto preferenziale di applicazione del software è attualmente strettamente connesso all'ambito della tracciabilità dei prodotti vitivinicoli e dei capi di abbigliamento.

Capitolo 2

Codici a barre bidimensionali

2.1 Descrizione della tecnologia

Conosciamo già i codici a barre presenti nei prodotti per fini d'identificazione e di logistica. Tra i tipi più diffusi in Italia, senz'altro troviamo il codice EAN (European Article Number) che viene utilizzato nella grande distribuzione, seguito dal Farmacode o codice 32, adottato per l'identificazione dei farmaci. Nell'ambito industriale hanno trovato grande diffusione il codice 128, il codice 39 (alfanumerico) e il 2/5 interleaved.

Figura 2.1: Codice EAN, FarmaCode, Codice 128

I codici a barre bidimensionali permettono una maggiore capacità d'immagazzinamento. Questi tipi di codici sono in grado di memorizzare, oltre a numeri, anche lunghi testi, indirizzi internet, numeri di telefono e messaggi SMS già pronti per l'iscrizione a servizi. Li possiamo già trovare nei quotidiani, libri e cartelloni pubblicitari, permettendo di collegare le informazioni cartacee a informazioni digitali per il web.

Originariamente studiati dalla NASA nel 1987 per facilitare la tracciabilità dei componenti degli Shuttle Spaziali, i codici 2D sono rapidamente apparsi su ogni cosa: dalle scarpe da ginnastica fino ai componenti elettronici e ai prodotti farmaceutici.

Figura 2.2: Codice a barre bidimensionale - QR

Cosa poco risaputa è infatti che i produttori di cellulari stanno iniziando ad inserire di serie la capacità di leggere questi codici. Ad esempio, Nokia ha inserito questa funzionalità negli N93, N93i, N95 e E90, permettendo comunque ai possessori di altri modelli d'installare un semplice programma gratuito.

I codici Data Matrix, QR e altri codici a barre, diventano dei veri tag e possono essere letti con i telefonini, dotati di fotocamera, semplicemente scaricando un'applicazione compatibile con il proprio modello (sviluppata in Java oppure nativa Symbian, Windows Mobile, iPhone...) permettendo la scansione e la decodifica del codice. I codici possono essere usati in modo sicuro, indipendentemente dal supporto, con molteplici applicazioni:

- catturare un indirizzo internet da memorizzare e aprire direttamente con il browser del telefonino;
- catturare un numero di telefono da chiamare o memorizzare;
- ottenere un messaggio già pronto. Utile, per esempio, per iscriversi a servizi di notizie via sms/mms;
- visualizzare e salvare testi sul proprio telefonino, in modo molto più chiaro della semplice fotografia, per esempio gli orari dell'autobus;
- il tag può diventare un biglietto da visita, in modo da inserire il proprio contatto nella rubrica più velocemente sfruttando il protocollo vCard;
- visualizzare informazioni aggiuntive relative al prodotto pubblicizzato;
- l'advertising multimediale e il one-click content, ovvero il reperimento facile e l'invio veloce d'informazioni su terminali mobili.

Tutto ciò inquadrando semplicemente un'immagine, ovvero un tag anziché inserendo un indirizzo Internet (fig. 2.3). L'utilizzo dei tag diminuisce quindi fortemente

il numero di click per la ricerca d'informazioni in mobilità e al contempo consente di aumentare la visibilità dei contenuti.

Figura 2.3: Schema per l'apertura dell'URL relativo ad un'azienda.

2.2 Applicazioni della tecnologia

Comunemente il BarCode 2D vengono utilizzati per imprimere un codice per marcare piccoli oggetti, infatti esso può includere fino a 50 caratteri in una superficie di appena 2 o 3 mm quadrati ed è sufficiente un contrasto del 20% per distinguere le sue celle (ovvero per distinguere le celle chiare da quelle scure) e quindi per leggere i bit che compongono l'informazione.

I codici a barre bidimensionali richiedono scanner in grado di leggere in due dimensioni. In genere questo richiede una fotocamera e una elaborazione d'immagine. Questa è una tecnologia diversa da quella utilizzata da molti degli scanner laser per la lettura dei simboli del codice a barre lineari. Un simbolo lineare, può essere letto da un singolo raggio laser che passa attraverso la lunghezza del simbolo. Tuttavia, per leggere i simboli bidimensionali viene richiesta l'intera immagine, da leggere in entrambi gli assi X e Y. Sull'esatto funzionamento interno di una scansione e il sistema di decodifica utilizzato dagli scanner in particolare, sono normalmente informazioni commercialmente sensibili.

I codici DataMatrix stanno diventando comuni e vengono anche stampati su supporti cartacei come lettere o buste. Il codice può essere letto rapidamente da

uno scanner che permette al supporto di essere tracciato negli spostamenti, ad esempio nel caso di un pacco inoltrato al destinatario.

Ai fini dell'ingegneria industriale, i codici Data Matrix possono essere marcati direttamente sui componenti, assicurando così che ogni componente sia identificato dal proprio codice seriale. I codici possono essere marcati sui componenti con diversi metodi: all'interno dell'industrie sono comunemente usate stampe a getto d'inchiostro, incisioni ad aghi, incisioni laser e procedure d'incisione chimica (elettrolitica). Questi metodi permettono di realizzare una marchiatura permanente che dovrebbe durare per l'intera vita del componente. Quando il componente è nel mercato, il codice Data Matrix può essere letto da un'apposita fotocamera in grado di decodificare i dati contenuti nel Data Matrix che possono essere così usati per un gran numero di scopi, come il tracciamento degli spostamenti e la gestione dell'inventario delle merci.

In Italia, per esempio, i Data Matrix vengono usati dalle Poste per tracciare gli spostamenti delle buste da lettera (in particolar modo le raccomandate).

Semacode è invece il nome di una società che ha l'obbiettivo di promuovere i barcode 2D e il formato dei dati presenti nei barcode. Semapedia fa uso di questa tecnologia per "collegare il mondo virtuale con quello fisico, linkando uno specifico spazio fisico con le informazioni disponibili per Wikipedia"; l'obiettivo dei partecipanti al progetto è "distribuire ed applicare i Tag-Semapedia che sono veri e propri link fisici basati su codici a barre 2D, leggibili da telefoni cellulari muniti di fotocamera". E' così possibile promuovere un evento (l'url codificato può essere stampato su manifesti e volantini), dare maggiori informazioni su un luogo, un monumento o altro ancora.

Negli ultimi anni sono stati sviluppati client da installare su terminale mobile che sfruttano le API di gestione delle fotocamere dei telefoni cellulari per effettuare la scansione del tag e acquisirne, mediante collegamento WAP, le relative informazioni. I barcone reader sono ormai maturi e molti sono in grado di leggere sia barcode lineari sia bidimensionali. La maggior parte è in grado di leggere più simbologie. Tra i più gettonati sembrerebbe il reader di I-Nigma (http://www.i-nigma.com) e Kaywa Reader (http://reader.kaywa.com)

2.3 Tipi e formati

MaxiCode:

MaxiCode è di dominio pubblico, adatto per il tracciamento e la gestione della spedizione dei colli, assomiglia ad un codice a barre, ma utilizza punti disposti in una griglia esagonale, appare come un quadrato da 1 pollice, con un occhio di bue nel

mezzo, circondato da un pattern di punti esagonale. Si possono memorizzare circa 93 caratteri d'informazioni, e fino a 8 simboli possono essere concatenati insieme per trasmettere più dati. Questo codice è a dimensione e capacità fissa ed è stato studiato per letture ad alta velocità soprattutto per linee di smistamento merci.

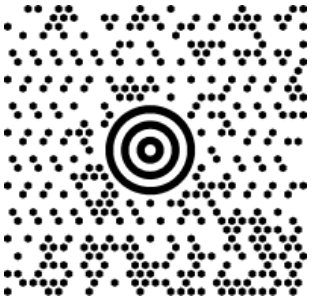

Figura 2.4: Codice a barre MaxiCode

Aztec codec:

Aztec Code è un tipo di codice a barre 2D, è stato pubblicato da AIM International nel 1997 e anche se il codice è brevettato, è stato rilasciato al pubblico dominio. Il simbolo completo supporta formati fino a 151x151, possono codificare 3.832 cifre, 3067 lettere, o 1.914 byte di dati. Si possono concatenare fino a 26 codici quando è necessario una grande capacità di dati

Figura 2.5: Codice a barre Aztec

PDF417:

PDF417 è una pila lineare utilizzato in una varietà di applicazioni, soprattutto di trasporto, carte di identità, e la gestione delle scorte. PDF sta per Portable Data File. È un formato di pubblico dominio, chiunque può implementare i sistemi che utilizzano questo formato, senza alcuna licenza. Il codice a barre PDF417 è costi-

tuito da 3 a 90 righe, ciascuna delle quali è come un piccolo codice a barre lineari. Il codice PDF417 ha una capacità di 2500 caratteri.

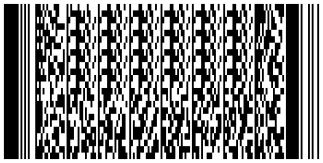

Figura 2.6: Codice a barre Pdf417

ShotCode:

ShotCode è un barcode circolare creato da High Energy Magic of Cambridge University. Si utilizza un cerchio simile a un bersaglio, tipo occhio di bue, mentre cerchi di bit che lo circondano rappresentano i dati. I ShotCodes differiscono dai codici a barre a matrice perché non memorizza i dati in una regione rettangolare ma sfrutta l'apertura angolare per determinare i bit d'informazione. Nota dolente è il fatto che non sia una tecnologia libera.

Figura 2.7: Codice a barre SchotCode

BarCode a colori:

High Capacity Color Barcode (HCCB) è il nome coniato da Microsoft per la sua tecnologia proprietaria di codifica dei dati utilizzando dei triangoli colorati al posto dei "pixel" tradizionalmente associati ai codici a barre 2D. In questo modo la densità dei dati aumenta perché si utilizza una tavolozza di 4 o 8 colori invece che solo bianco o nero. Per esempio, una stringa di 100 caratteri necessita in generale di 100 byte quindi di 800 punti (bit), mentre con 4 colori sono sufficienti 200 punti. Permette quindi di contenere più informazioni nello stesso spazio di un codice QR. Nota dolente è il fatto che non sia una tecnologia libera.

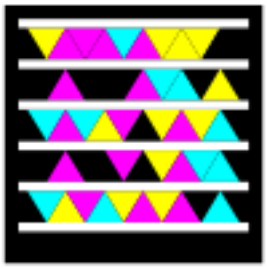

Figura 2.8: Microsoft Tag

Attualmente i codici a barre bidimensioni più popolari e diffusi sono i DataMatrix e il QR-Code.

2.4 Caratteristiche dei codici DataMatrix

I DataMatrix sono di forma quadrara (a volte rettangolari) e sono suddivisi in celle, ognuna delle quali rappresenta un bit. In base alla situazione una cella di colore chiaro può rappresentare il bit 0 e una di colore scuro il bit 1 (o viceversa). L'usuale dimensione dei dati va da pochi byte fino a 2 kilobytes in genere la lunghezza dei dati codificati dipende dalla dimensione del simbolo usato.

Figura 2.9: DataMatrix: Forma quadrata singola e rettangolare a 2 regioni.

Inoltre è previsto un sistema di correzione degli errori che aggiunge byte al messaggio codificato in modo da rendere leggibile anche un Data Matrix parzialmente danneggiato. Un simbolo Data Matrix può immagazzinare fino a 2.335 caratteri alfanumerici.

Data Matrix si compone di due parti distinte: il "pattern Finder" e l'area dei dati effettivi. Il pattern finder è utilizzato dallo scanner per individuare il simbolo, definisce la forma (quadrata o rettangolare), la dimensione e il numero di righe e colonne nel simbolo. Due bordi adiacenti sono colorati in modo uniforme e formano una "L", principalmente utilizzato per determinare la dimensione, l'orientamento e la distorsione del simbolo. Gli altri due bordi adiacenti appaiono tratteggiati a causa dell'alternan-

za di celle di colore bianco e nero, noto come “Clock Track”. Questo definisce la struttura di base del simbolo, la dimensione e può anche aiutare a determinare la distorsione. I dati veri e propri vengono poi codificati in una matrice all’interno del ”pattern Finder”.

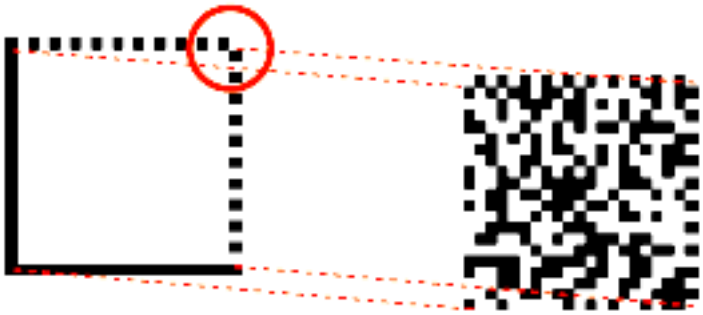

Figura 2.10: DataMatrix: Pattern Finder e la regione dei dati

All’interno di questi bordi troviamo tutte le celle che compongono l’informazione codificata. Man mano che il numero dei dati aumenta, il numero di righe e di colonne cresce. In genere le sue dimensioni variano da 10x10 a 144x144.

Un Data Matrix è infinitamente scalabile, nelle applicazioni commerciarli può essere piccolo fino a 300 micrometri (per esempio è possibile incidere a laser un Data Matrix su un dispositivo di silicio di 600 micrometri) e grande a piacere, dipende dallo strumento di acquisizione.

ECC200 è la nuova versione presente nei Data Matrix e supporta avanzati algoritmi di controllo e di correzione degli errori (come Reed-Solomon). ECC200 permette la ricostruzione fino al 30% dell’intera serie dei dati codificati. Ciò significa che anche quando il simbolo è per il 30% danneggiato esso è ancora leggibile, cosa che sarebbe impossibile utilizzando codici a barre lineari. La versione Data Matrix ECC 200 supporta diverse strutture di codifica che possono essere utilizzate nel simbolo stesso contemporaneamente. Esempi includono: ASCII, ISO / IEC 646, C40, Testo, X12, EDIFACT e Base 256. Queste strutture offrono la possibilità di massimizzare l’efficienza di codifica dei dati richiesti in un simbolo Data Matrix (solo testo, solo numerico, maiusolo/minusculo, esadecimale...). I blocchi d’informazione, composti da 8 bit, non sono disposti in modo ordinato e lineare, tipo da sinistra verso destra o dall’alto verso il basso. Il blocco è a forma di “UTAH” cioè come la forma del noto stato negli Stati Uniti e disposti a scaglie in diagonale (fig. 4.8).

Data Matrix è coperto da diversi standard ISO/IEC ed è di pubblico dominio per molte applicazioni, ciò significa che esso può essere usato liberamente senza pagare licenza o royalities.
Esistono in rete una grande quantità di software commerciali per la gestione di tali

Dimensione simbolo	n. Regioni	Capacità Byte	Livello correz. %
10x10	1	3	62.5
12x12	1	5	58.3
14x14	1	8	55.6
16x16	1	12	50
18x18	1	18	43.8
20x20	1	22	45
22x22	1	30	40
24x24	1	36	40
26x26	1	44	38.9
32x32	4	62	36.7
36x36	4	86	32.8
40x40	4	114	29.6
44x44	4	144	28
48x48	4	174	28.1
52x52	4	204	29.2
64x64	16	280	28.6
72x72	16	368	28.1
80x80	16	456	29.6
88x88	16	576	28
96x96	16	696	28.1
104x104	16	816	29.2
120x120	36	1050	28
132x132	36	1304	27.6
144x144	36	1558	28.5

Figura 2.11: Datamatrix: dimensioni e capacità

barcode, mentre la risorsa opensouce di riferimento è libdmtx scaricabile dal portale di Sourceforge.

2.5 Caratteristiche dei codici QR

Un Codice QR è un codice a barre bidimensionale creato dalla giapponese Denso-Wave nel 1994. Il "QR" deriva da "Quick Response" (Risposta Rapida), poiché il creatore pensava ad un codice che consentisse una rapida decodifica del suo contenuto. I codici QR sono molto comuni in Giappone e sono attualmente il più popolare tipo di codice bidimensionale del paese. Sebbene inizialmente utilizzato per tracciare molti pezzi nella costruzione di veicoli, i codici QR sono ora utilizzati per la gestione delle scorte in un'ampia varietà d'industrie. Più recentemente, sono state sviluppate applicazioni orientate verso la comodità, finalizzate a sollevare l'utente dal noioso compito d'inserire dati nel proprio telefono cellulare. Anche l'aggiunta di codici QR sui biglietti da visita sta diventando comune, semplificando notevolmente il compito d'inserire i dettagli personali di una nuova conoscenza nella rubrica del proprio telefonino.

BEGIN:VCARD
VERSION:2.1
FN:Mario Gianni Rossi
TEL;CELL;VOICE:123456789
ADR;HOME:;;ViaG.Garibaldi,23;Roma
EMAIL;PREF;INTERNET:mario@rossi.it
URL;HOME:http://www.rossi.it
...
END:VCARD

Figura 2.12: QR contenente un contatto in formato vCard

Le quantità dei dati che possono essere inseriti in un codice QR sono:

Solo Numerico	Max 7.089 caratteri
Alfanumerico	Max 4.296 caratteri
Binario (8 bit)	Max 2.953 byte
Kanji/Kana	Max 1.817 caratteri

I codici QR usano la correzione degli errori Reed-Solomon ed è possibile scegliere diversi livelli per aumentare la ridondanza d'informazione:

Livello L 7% delle parole in codice può essere ripristinato.
Livello M15% delle parole in codice può essere ripristinato.
Livello Q25% delle parole in codice può essere ripristinato.
Livello H30% delle parole in codice può essere ripristinato.

Lo standard giapponese per i codici QR, corrispondente allo Standard Internazionale ISO, ISO/IEC 18004, è stato approvato nel giugno del 2000. Dal sito di Denso-Wave si cita: “Il codice QR è aperto, nel senso che è rivelata la sua specifica e che il diritto di brevetto posseduto da Denso Wave non è esercitato”, motivo del suo successo e diffusione.

L’elemento più piccolo (ogni singolo quadratino) del codice QR si chiama modulo. Un codice QR è composto dalla combinazione di moduli in bianco e nero, e descrivono le informazioni sul formato, il livello di correzione degli errori, l’area dati e codici di correzione degli errori.

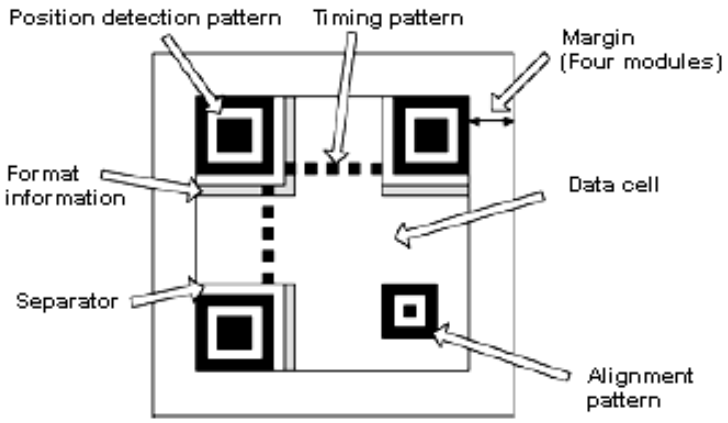

Figura 2.13: Struttura del QR-Code

Per codificare i dati in un simbolo QR si devono eseguire i seguenti passi principali. La stringa di input (che può essere qualsiasi valore ASCII tra 0-255) è codificata, lo scopo primario della codifica è quello di comprimere i dati in una forma molto più breve. Se necessario, i dati sono riempiti fino alla capacità della dimensione del simbolo. Una volta che la stringa è stata codificata, vengono aggiunti i valori di codici di correzione degli errori in modo che i dati possano essere recuperati, anche se una parte del simbolo è stata distrutta, per esempio da uno strappo o coperto da una macchia. Infine, i dati codificati e i codici di correzione dell’errore si collocano nel simbolo secondo un algoritmo specificato nella norma ISO, questo è fatto mettendo ogni bit di ogni byte di dati in una posizione specifica nel simbolo.

Dimensione simbolo	Capacità Byte (H - 30%)	Capacità Byte (L - 7%)
21x21	7	17
25x25	14	32
29x29	24	53
33x33	34	78
37x37	44	106
41x41	58	134
45x45	64	154
49x49	84	192
53x53	98	230
57x57	119	271
77x77	120	520
97x97	557	858
101x101	587	929
117x117	779	1273
137x137	1080	1732
141x141	1150	1840
149x149	1307	2068
153x153	1394	2188
161x161	1530	2431
169x169	1658	2699
177x177	1852	2953

Figura 2.14: QR-code: dimensioni e capacità

2.6 Confronto Monodimensionale, DataMatrix e QR

I codici a barre monodimensionali contengono una ridotta quantità d'informazioni sufficienti per contenere un codice identificatore. L'hardware richiesto per la lettura è più economico rispetto i barcode 2D. Per questi motivi sono principalmente utilizzati nel campo logistico e nei magazzini. Quando si ha necessità di una maggiore capacità d'informazioni occorre utilizzare i codici a barre bidimensionali. L'uso di standard come DataMatrix, va riservato ai casi in cui le sue caratteristiche siano davvero indispensabili per risolvere il problema: ad esempio nel caso di oggetti troppo piccoli per ospitare codici a barre, ambienti che comportino un'alta probabilità di danneggiamento dell'etichetta, o su substrati che non si adattino alla stampa di codici a barre né all'applicazione delle normali etichette.

La disponibilità di strumenti integrati con le codifiche di barcoding 2D è uno degli elementi chiave per la loro diffusione e successo commerciale. Il supporto delle specifiche Datamatrix dalle industrie è notevolmente più ampio rispetto a quello dei QR. Il DataMatrix non contiene informazioni di formato ed ha un minimo numero di elementi per la cattura (finder), quindi consente una densità maggiore rispetto il QR. Il DataMatrix, come i QR, utilizzano i codici di correzione ReedSolomon. Il numero d'errori rilevabili e correggibili è determinato dal numero di codici di correzione extra, inclusi nel messaggio originario. DataMatrix utilizza un livello fisso di correzione degli errori che non è configurabile dall'utente. La percentuale di correzione varia dal 62.5% per i simboli più piccoli, fino al 28% per quelli più grandi. I barcode QR invece, ha 4 livelli di correzione, che consentono una capacità di recupero di cerca il 7%, 15%, 25% o 30%. Quando la dimensione del simbolo è un problema si dovrebbe ottimizzare la massima dimensione con il massimo livello di correzione ammissibile.

Nelle applicazioni in tempo reale, dove il tempo per decodificare l'immagine è importante si deve valutare quanto tempo occorre a individuare il simbolo. Meno elementi ci sono da individuare e soprattutto la caratteristica di unicità dell'elemento, è un fattore determinante. Il QR ha il vantaggio rispetto il DataMatrix di avere un unico elemento di ricerca (uno dei 3 quadrati negli angoli). DataMatrix ha invece una "L" tratteggiata ed è facilmente confondibile con il resto del simbolo. DataMatrix non contiene informazioni sul formato utilizzato, mentre QR permette velocemente di far sapere le dimensioni del simbolo e quindi di confermare la sua correttezza. Al riguardo alcuni studi hanno realizzato dei test: la lettura dei QR è stata più veloce di 4 volte. In USA, un comitato indipendente dell'Associazione per l'Elettronica di Consumo (CEA) ha analizzato queste due tipologie di codifica delle informazioni con l'intento di sviluppare le specifiche IEC62090. La conclusione a cui è arrivata è che il

DataMatrix ha una migliore gestione dello spazio tra tutti i barcodes bidimensionali. In figura 2.15, i simboli incorporano entrambi l'url "http://www.google.it". Notiamo che a parità di dimensione dei punti, QR è formato da 25 punti per lato mentre DataMatrix da 18, con un risparmio del 61% di spazio.

Figura 2.15: QR e DataMatrix a confronto

In conclusione, possiamo dire che in applicazioni in cui la dimensione del simbolo deve essere ridotta al minimo a discapito della performance di lettura è consigliabile utilizzare DataMatrix. Quando la velocità d'elaborazione è di primaria importanza è meglio scegliere QR.

2.7 Codici di correzione degli errori - ECC

I codici a barre, una volta creati, possono tuttavia subire dei disturbi (distorsione, strappi, macchie), soprattutto durante il trasporto su un lungo tragitto o posizionati in ambienti esterni. Per questo motivo è necessario controllare la validità dei dati, esistono dei meccanismi che permettono di garantire un certo livello di integrità dei dati. DataMatrix e QR-code fanno uso dello schema di codifica di Reed Solomon per la correzione degli errori. I codici di correzione Reed-Solomon furono inventati nel 1960 da Irving S. Reed e Gustave Solomon. Il codice Reed-Solomon è un codice utilizzato per correggere errori di flusso in svariate applicazioni di comunicazione digitale e memorizzazione di dati. Si basa sul sovracampionamento di un polinomio costruito partendo dai dati da trasmettere. Il polinomio è quindi calcolato in più punti di quanti sarebbero sufficienti a identificarlo univocamente; il valore di questi punti viene trasmesso o registrato. Alla ricezione o alla lettura è possibile ricostruire il polinomio originario, e conseguentemente i dati, anche in presenza di errori. Un codificatore Reed-Solomon prende un blocco di dati e aggiunge bit di ridondanza. Il numero di errori che il codice riesce a correggere dipende dalle caratteristiche del codice.

Attualmente viene utilizzato in diversi sistemi come supporti di memorizzazione (compact disc, DVD) e Sistemi di telecomunicazione (Dispositivi mobili e wireless, comunicazioni satellitari e xDSL).

Implementazioni per la generezione di codici Reed-Solomon, si trovano nel portale di SourceForge e in particolare nelle librerie libdmtx.

Capitolo 3

Near Field Communications

3.1 Sistemi RFid

NFC è una tecnologia derivata da RFid. L'infrastruttura di un sistema RFid è formata da 3 componenti: il tag, un reader e il software di gestione. Il tag o transponder, è un trasmettitore a radio frequenza di piccole dimensioni e può assumere le più svariate forme; da un etichetta di pochi centimetri, un bottone o un portachiavi. All'interno del tag troviamo un chip che ne assicura il funzionamento, un area di memoria e un antenna per la comunicazione con il il reader. Il reader, oltre a comunicare le operazioni richieste dal software di gestione, in genere fornisce l'energia necessaria per l'attivazione del tag.

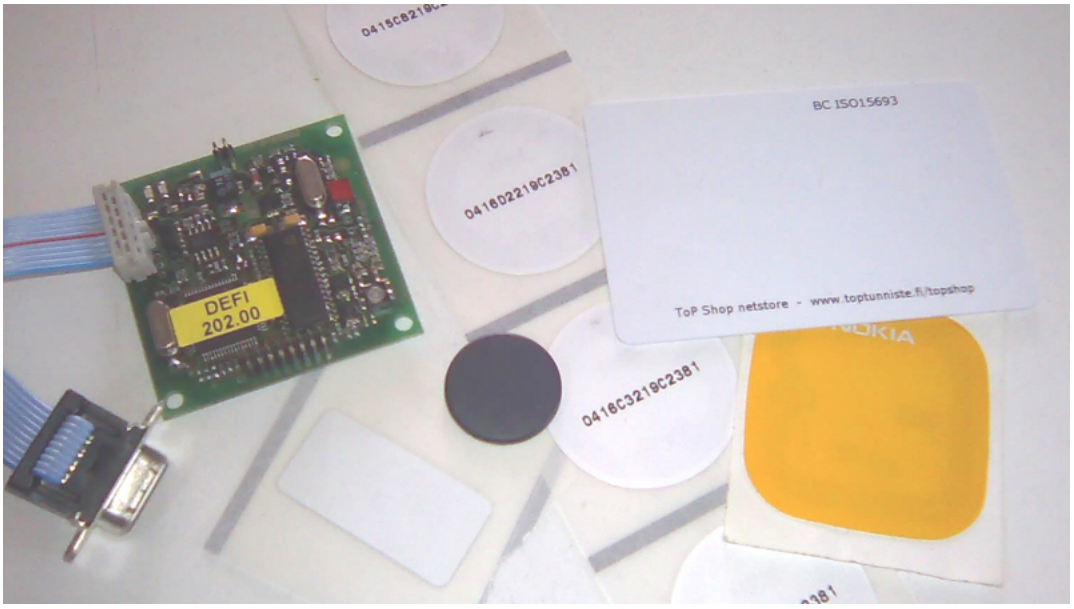

Figura 3.1: Reader e vari tipi di tag

3.1.1 Applicazioni

L'utilizzo di tag RFid per gestire oggetti nella logistica di produzione e di identificazione nel settore del commercio è gà una realtà. Il progresso della tecnologia RFid promette che tutti gli articoli di consumo nei supermercati siano muniti di tag RFid, ma al momento non si è ancora giunti ad un'ampia diffusione.

Sistemi RFid sono integrati nel controllo degli accessi, nei documenti per l'identificazione, nel controllo degli animali, i tag sono presenti negli autoveicoli, abiti calzature o in un tappo di una bottiglia di vino. Un settore nella quale l'uso degli RFid è ampiamente utilizzato è quello relativo alla catena di distribuzione delle merci, infatti il parlamento Europeo, nel 2005, ha varato una legislazione che rende obbligatoria la tracciabilità dei beni, fattore che ne aumenterà l'adozione di RFid. Rispetto ai codici a barre, gli RFid si prestano meglio per veicolare informazioni a sistemi d'interrogazione come i database. Grazie ai codici identificatori universali (EPC) e ad un basso costo dei Tag si potrà fruire un enorme quantità d'informazioni riguardo i prodotti verso i produttori, distributori e consumatori.

3.1.2 Classificazione

Le frequenze di comunicazione tra Reader e TAG dipendono sia dalla natura del TAG, sia dalle applicazioni previste e sono regolate (per controllare le emissioni di potenza e prevenire interferenze) dai consueti organismi internazionali e nazionali.

La dimensione dell'antenna è legata alla frequenza operativa. Infatti al crescere della frequenza diminuisce la lunghezza d'onda e quindi la dimensione dell'antenna del TAG può essere minore. L'aumento della frequenza comporta anche un aumento di energia necessaria per trasmettere un segnale rispetto un segnale a bassa frequenza. La frequenza operativa più utilizzata è a 13.56 Mhz e permette una distanza massima di comunicazione di circa 50 cm. Per raggiungere distanze più elevate è necessario utilizzare TAG attivi a frequenza più elevata. L'aumento della frequenza comporta anche una maggiore velocità di comunicazione e consente un trasferimento con una maggiore quantità d'informazioni.

Le frequenze sono classificate nei seguenti gruppi:

- LF - 120-145 kHz.
- HF - 2 a 15 Mhz.
- UHF - 865-870 Mhz in Europa e 902-928 Mhz USA.
- SHF - 2.4 Ghz a 5.8Ghz.

Gli RFid si possono classificare secondo le seguenti caratteristiche energetiche:

- TAG passivi. Sono alimentati dalla potenza irradiata dall'antenna del reader quando questo li interroga. La comunicazione avviene a piccole distanze meno di 10m. La loro architettura permette bassi costi di produzione.
- TAG semipassivi: hanno una fonte di alimentazione indipendente dal reader ma trasmettono solo se interrogati, la batteria è in grado di alimentare il circuito integrato ma utile anche per tenere attiva una memoria RAM statica nella quale memorizzare tutti i dati relativi al TAG. In trasmissione si comportano come TAG passivi, la comunicazione può coprire distanze di decine di metri, la batteria ha comunque una elevata autonomia. I tag semipassivi hanno costi più elevati rispetto ai tag passivi.
- TAG attivi. Hanno una fonte di alimentazione indipendente dal reader e la capacità di trasmettere senza essere interrogati. Possono coprire grandi distanze (100m - 1km), hanno un'autonomia limita e presentano costi elevati. Possono essere equipaggiati con sensori in grado di rilevare i parametri climatici (temperatura, pressione, umidità, ecc.) dell'ambiente in cui sono.

Un'altra classificazione dipende dai casi d'uso:

- LF 120-145 kHz. Controllo accessi, controllo animali.
- HF 13.56 Mhz. Etichette impiegate principalmente per il controllo degli accessi, identificazione e micropagamenti, controllo bagagli e biblioteche.
- UHF 865-870 Mhz in Europa e 902-928 Mhz USA. Identificazione di oggetti in movimento.
- SHF 2.4 Ghz a 5.8Ghz. Tag attivi per il controllo veicolare (Telepass)

Gli Rfid Si possono ulteriormente classificare in base al tipo di memoria:

- Tag a bit unico: sono impiegati nei sistemi EAS (anti-taccheggio)
- Tag Read-only: i transponder contengono una memoria interna piccolissima e non volatile. Per questo motivo sono di facile costruzione ed economici.
- Tag Read-Write: i transponder hanno la possibilità di scrivere e memorizzare dati per più volte o solo una volta. I tag passivi in genere possono contenere qualche decina di Kb di dati mentre tag attivi possono avere capacità anche dell'ordine del Mb.
- Transponder con funzionalità crittografiche: sono TAG che prevedono l'impiego di tecniche di cifratura. Normalmente i tag non prevedono alcuna protezione e quindi qualsiasi reader può accedere alle informazioni presenti nel tag. Per

evitare gli accessi non autorizzati in questo tipo di dispositivi viene richiesta una password ad ogni tentativo di lettura o scrittura.

- Killable tag: in risposta alle obiezioni mosse dai Garanti della Privacy è stata realizzata una nuova tipologia di tag che possono essere messi fuori uso in modo temporaneo o definitivo.

L'utilizzo dei tag per applicazioni di logistica e identificazione di oggetti, è regolamentata da molti standard. In particolare lo standard EPC (Electronic Product Code) i tag possono appartenere a:

- Classe 0: tag obsoleti a 900 Mhz passivi, sono read-only, si può soltanto leggere l'id identificatore. Fanno parte i tag AES.

- Classe 1 - Generazione 1: i tag lavorano da 13.45 Mhz a 900 Mhz, sono read/write una sola volta, il che significa che è possibile programmare qualsiasi numero all'interno del chip (questa fase viene chiamata commisioning del tag) presso la propria location e successivamente leggere l'informazione un numero illimitato di volte.

- Classe Epc Gen2 significa EPC Generation 2. È il protocollo EPC di seconda generazione, progettato per operare a livello internazionale. L'EPC Gen è al centro dell'attenzione perché sembra probabile una convergenza fra gli standard UHF Gen 2 e una revisione dell'ISO 18000-6. Tutte le parti in causa (industria, ISO, EPC Global) hanno l'interesse che ciò avvenga. Il processo di unificazione potrebbe contribuire ad accelerare l'adozione su scala globale dell'Rfid.

3.1.3 Protocolli di comunicazione

I sistemi RFID passivi si basano su un accoppiamento magnetico fra reader e tag. Quando il tag transita attraverso il campo magnetico vicino al reader, ai terminali viene indotta una tensione in grado di attivare il chip. La comunicazione che si instaura tra TAG e Reader è digitale e avviene grazie a diversi tipi di codifiche che convertono il segnale in binario. Le codifiche dei frame sono molteplici e variano da tag a tag. Quelle più usate sono Manchester, PIE e Miller. Una volta codificato il segnale, lo si invia sfruttando una modulazione che in genere può essere ASK o FSK, dipende dal tag. In generale il frame è composto dai seguenti campi:

- FLAG: campo di 8 bit presente sia in testa che in coda al frame ed ha la funzione di delimitare il messaggio;

- ADDRESS: campo estendibile a multipli di 8 bit, contiene l'indirizzo della stazione trasmettenti o ricevente a seconda del tipo di comunicazione;
- CONTROL: campo di 8 o 16 bit, specifica il tipo di frame trasmesso;
- INFORMATION: campo di lunghezza variabile, costituisce il messaggio vero e proprio della comunicazione;
- FCS: campo di 16 o 32 bit, svolge funzioni di rilevazione di errori nel frame.

In certi sistemi più complessi, si ha la possibilità di fare letture di più TAG contemporaneamente con lo stesso Reader. Occorre stabilire in questo caso un protocollo che gestisca la comunicazione multi-punto, operazione svolta da algoritmi "anti-collisione" che regolano gli intervalli di tempo nei quali i TAG devono essere letti evitando così la sovvrapposizione di segnali diversi. Sistemi di questo tipo sfruttano algoritmi del tipo "Binary Tree" o "Aloha".

I protocolli riguardanti gli RFid sono:

- ISO 18000: è lo standard di riferimento. Il protocollo ISO 18000 prevede caratteristiche particolari per i vari range di frequenza sui quali i transponder possono operare. Il protocollo è suddiviso in 7 parti ognuna delle quali descrive i transponder a seconda delle frequenze (135 Khz, 13.56 Mhz, 433 Mhz, 860-930 Mhz, 2.45 Ghz). Per esempio, l'ISO 18000-3 regolamenta la comunicazione dei sistemi con frequenza portante a 13.56MHz definendo due modalità operative: Mode1 e Mode2, le quali descrivono l'interoperabilità tra Reader e Tag.
- ISO 7810: specifica le caratteristiche delle smart card a contatto. È suddiviso in 4 parti: caratteristiche fisiche, radiofrequenza e modulazione (modalità A o modalità B), inizializzazione ed anti-collisione, protocollo di trasmissione.
- ISO 18092: definisce lo standard per le contactless smartcard. La ISO 18092 deriva dalle seguenti specifiche: la ISO 15693 e la ISO 9798, regolamentano il protocollo di comunicazione a mutuo riconoscimento. Da tali specifiche deriva quindi l'utilizzo di un sistema dedicato ai micropagamenti e dunque adatto per sistemi di bigliettazione elettronica. In particolare l'ISO 9798-2 prevede che entrambi i soggetti (Reader e Tag) verifichino reciprocamente la conoscenza di una chiave segreta. Dopo la fase di mutua autenticazione le communicazioni tra le due entità avviene in modalità criptata.
- ISO 15693. Il protocollo è stato creato per regolamentare le contactless vicinity card e si basa su sistemi operanti a 13.56MHz con range di operabilità fino ad un metro e mezzo. Le carte vicinity operano con una logica di controllo

più semplive rispetto ISO 14443. In genere sono carte utilizzate per il controllo degli accessi.

- ISO 14443. Il protocollo ISO 14443 è nato per la regolamentazione delle contactless smart cards operanti a 13.56 MHz. Lo standard ISO 14443 si compone di due differenti tipologie di protocollo che sono Type A e Type B. Ci sono anche altri protocolli simili che sono successivamente stati denominati C,D,E. Molte caratteristiche dello standard ISO 14443 sono del tutto simili a quelli dello standard ISO 7816 che regolamenta le contact smart card in modo da permettere la transizione dalle card a contatto con quelle contactless. Il documento si compone di quattro differenti parti:
  • Parte 1: definisce le caratteristiche hardware;
  • Parte 2: definisce l'interfaccia RF sia per quanto riguarda i segnali che la potenza da trasmettere dal reader verso il tag;
  • Parte 3: descrive la tecnica e le procedure necessarie ad evitare fenomeni di anti-collisione;
  • Parte 4: definisce invece il protocollo di comunicazione impiegato.
  I dispositivi di Tipo A usano una modulazione ASK al 100% con codifica dei dati basata su tecnica Miller per la comunicazione Reader-Tag, mentre per la comunicazione Tag-Reader si fa uso di una Modulazione OOK con codifica Manchester. I dispositivi di Tipo B usano invece una modulazione ASK al 10% con codifica NARZ dei dati trasmessi per la comunicazione Reader-Tag, mentre per la comunicazione tag-Reader si fa uso di una modulazione BPSK.

Esistono comunque, soluzioni basate su protocollo proprietario che fanno uso di un trasponder e di un lettore generalmente prodotti dalla stessa azienda e tali da interagire fra di loro. Esempi di transponder sono quelli prodotti da Texas Instrument, Sony o della NXP-Philips che si basano su uno standard privato per la comunicazione a radio frequenza.

In particolare Philips e NXP semiconduttor hanno realizzato la tecnologia contactless MIFARE, che è la più diffusa al mondo, sembra essere identico al protocollo ISO14443, ma in realtà essendo proprietario si differenzia sui protocolli di criptaggio e di accesso ai dati che si basa su scelte proprietarie. È basata sullo standard ISO 14443, tipo A (RFID a 13.56 MHz). La distanza tipica di lettura/scrittura tra tag e reader è di circa 10 cm, ma la reale distanza dipende dal campo di potenza generato dal lettore e dalla dimensione dell'antenna. Le carte MIFARE Classic e MIFARE UltraLight sono fondamentalmente solo dispositivi di memoria, dove la stessa memoria è divisa in segmenti e blocchi con semplici meccanismi di controllo degli accessi, hanno quindi limitato potere computazionale. Grazie al basso cos-

to ed all'affidabilità, queste carte sono largamente usate per borsellini elettronici, controllo degli accessi, trasporti o biglietti per manifestazioni sportive.

Le MIFARE UltraLight hanno solo 512 bit di memoria (cioè 64 byte), senza sicurezza.

Un nuovo prodotto a basso costo sono i MIFARE UltraLight C dove l'area dei dati è protetta dall'algoritmo 3DES.

Le MIFARE Standard 1k offrono 1024 byte per l'immagazzinamento dei dati, divisi in 16 "settori"; ogni settore è protetto da due diverse chiavi, chiamate A e B. Esse possono essere programmate per operazioni come lettura, scrittura, incremento del valore dei blocchi, ecc. Le MIFARE Standard 4k offrono 4096 byte divisi in 40 settori. Nel dicembre 2007 un gruppo di ricerca ha dichiarato di essere riuscito a superare l'algoritmo di cifratura delle carte Classic. Un analogo risultato è stato ottenuto nel marzo 2008 da un altro gruppo di ricerca. NXP ha confermato e riconosciuto il problema, che esiste solo per le carte Classic.

Le MIFARE ProX e SmartMX sono carte basate su microprocessori programmati attraverso un sistema operativo dedicato. Spesso il microprocessore è associato ad un cooprocessore dedicato al rapido calcolo crittografico (Triple DES, Advanced Encryption Standard, RSA, ecc.). Queste carte sono in grado di eseguire operazioni complesse, sicure e veloci, allo stesso livello delle smart card a contatto. Queste carte possono supportare sistemi operativi sia aperti che proprietari, compreso il sistema operativo Java Card (JCOP).

La MIFARE DESFire è una speciale versione della piattaforma Philips ProX e SmartMX, con caratteristiche di sicurezza superiori rispetto alla versione Classic. È venduta già programmata con un sistema operativo dedicato (DESfire).

3.2 NFC

Near Field Communications è l'unione di un reader e di un tag in un unico dispositivo permettendo una comunicazione di tipo "PeerToPeer". NFC è una tecnologia di comunicazione wireless a corto raggio che permette a due dispositivi in stretto contatto di scambiarsi dati. i dispositivi interessati all'introduzione della tecnologia NFC sono palmari e telefonini. NFC consente una comunicazione a distanza di circa 10 centimetri e una velocità dai 106 a 848 kbit/s. L'obbiettivo principale sono creare servizi contactless sul mobile come micropagamenti, i consumatori possono fare acquisti e pagare utilizzando i propri telefoni NFC. Altri servizi saranno la lettura d'informazioni, dal prodotto di un negozio fino al monumento di una città. La mancanza di standardizzazione e di un modello di business condiviso dai vari partner e sponsor, ha rallentato la diffusione della tecnologia. Attualmente si stima che nel 2012, il 20% dei telefonini immessi nel mercato saranno telefoni NFC. L'integrazione del NFC nei lettori musicali portatili, TV, e altri elettrodomestici consente di trasferire facilmente materiale multimediale. NFC è compatibile con gli attuali sistemi contactless usate per il ticketing, trasporto e pagamenti.

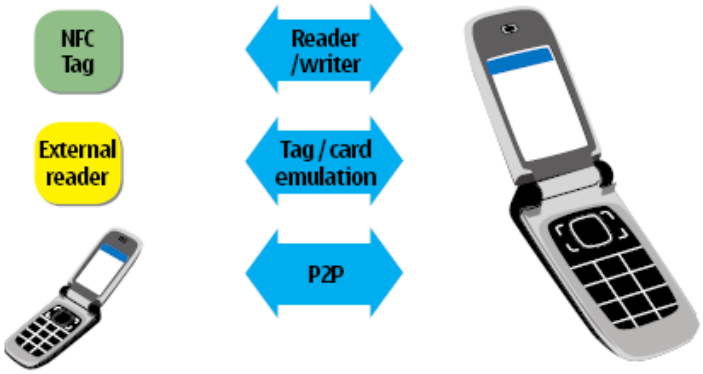

Figura 3.2: Modalità operative di un telefonino NFC

Un telefonino NFC opera in tre modalità differenti: scrittore-lettore, emulazione carta e PeerToPeer.

In modalità lettore-scrittore, un telefonino NFC può essere utilizzato come un lettore-scrittore di tag e smart card. In questa modalità fornisce un modo semplice e veloce per creare un biglietto da visita, messaggi SMS, richiesta di chiamata o per accedere a un indirizzo web. L'NFC Forum specifica il formato dei dati da memorizzare su un tag.

In modalità di emulazione carta un telefonino NFC emula una smartcard ISO-14443 o un Mifare classic 4K tag integrate nel telefono.

La modalià Peer-to-Peer (P2P) è una modalità che consente a due telefoni cellulari NFC o altri dispositivi, di condividere i dati toccandosi a vicenda.

Le modalità sopracitate permettono di eseguire le seguenti principali attività:

Biglietteria. Un telefono è come un biglietto: i dati di viaggio vengono memorizzati nell'area protetta del telefonino. Consente di accedere oltre i tornelli dei trasporti o fungere come carta di autorizzazione, ed è possibile visualizzare le transazioni recenti sul display del telefonino.

SmartCard: il telefonino diventa una smartcard contactless per il pagamento e permette di effettuare acquisti nei negozi. Le credenziali sono salvate nell'area protetta del telefonino. Applicazioni apposite permetteranno di visualizzare la cronologia delle transazioni effettuate.

Scambio dati: in caso di utilizzo con un PC potranno effettuare funzioni di scambio d'informazioni o di sincronizzazione. È possibile velocizzare il processo di pairing con dispositivi Bluetooth o Wifi. È possibile inviare immagini via Bluetooth toccando una etichetta su una stampante oppure semplicemente toccando due telefonini NFC.

Lettori di tag: avvicinando il telefonino a Tag RFiD si può leggerne i contenuti ed effettuare azioni. Nel caso di un cartellone pubblicitario sarà possibile scaricare contenuti legati all'informazione ed accedere ad Internet per effettuare registrazioni. È possibile salvare l'ora della sveglia in un tag sul nostro comodino o lasciare un messaggio sulla porta di casa.

Per consentire l'interazione tra il telefono cellulare dell'utente e i sistemi di pagamento è necessario integrare nel terminale POS, presenti nei negozi con un chip contactless. Adeguare tutti i POS presenti in Italia richiede, perciò, un investimento elevato in termini sia di tempo sia di denaro. Un dispositivo NFC può comunicare sia i lettori e card ISO 14443, quindi è già compatibile con le infrastrutture RFID esistenti per il pagamento e trasporto pubblico.

Figura 3.3: Telefonino NFC e relativo POS

3.3 Confronto tra le comunicazioni wireless.

Perché utilizzare una nuova tecnologia di comunicazione rispetto ad altre tecnologie esistenti come il bluetooth? L'NFC ha il vantaggio di avere tempi di configurazione e inizializzazione della connessione più brevi. Spesso occorre una configurazione manuale complessa per attivare la connessione con i sistemi wireless tradizionali mentre l'inizializzazione delle connessioni con dispositivi NFC è praticamente immediata. Per evitare il complicato processo di configurazione, NFC può essere utilizzato per la configurazione di tecnologie wireless, come Bluetooth. Anche se la velocità di trasmissione dei dati è più lenta rispetto il Bluetooth, l'NFC si rende adatto ad essere utilizzato in aree affollate garantendo un maggior grado di sicurezza, avendo una distanza di comunicazione molto inferiore.

	NFC	**IrDa**	**Bluetooth**	**802.11x**
Inizializzazione	0.1 ms	0.5 s	6 s	6 s
Distanza operativa	10 cm	5 m	10 m	100 m
Usabilità	Facile	Facile	Media	Media
Casi d'uso	Pagamenti, Accessi, Piccole transazioni	Controllo, Scambio dati	Scambio dati	Scambio dati
Configurazione	Nessuna	Nessuna	Manuale	Manuale

Figura 3.4: Confronto tra comunicazioni WireLess

3.4 Protocolli di comunicazioni

Il protocollo NFC è stato sviluppato congiuntamente da Sony e Philips nel 2004. Nel 2004 viene fondato l'NFC Forum, che ad oggi conta più di 100 membri come Nokia, Samsung, Visa, Mastercard e altre aziende dei settori delle telecomunicazioni e finanziarie, con l'obbiettivo di standardizzare i protocolli e garantire la massima interoperabilità tra sistemi e applicazioni. Gli standard sono definiti in ISO,ECMA e ETSI, si suddividono:

- NFCIP-1: interfaccia radio, inizializzazione, anti-collisione, protocolli di scambio dati e gestione degli errori.
- NFCIP-2: meccanismo di scambio tra i protocolli di comunicazione ISO 14443 e ISO 15693 sempre a frequenza 15.63 Mhz.
- NFCIP-WI: guida il meccanismo di comunicazione tra chip NFC e dispositivo ospitante.

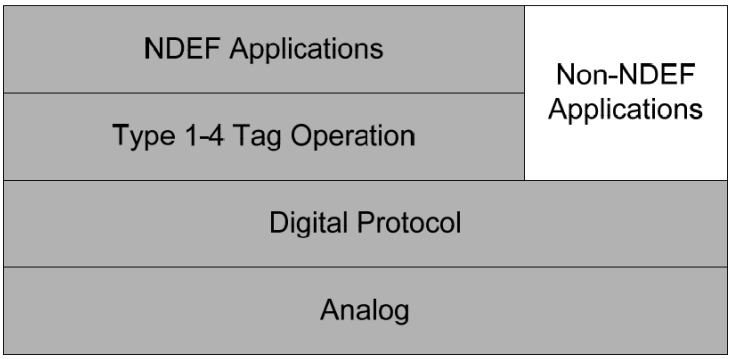

Figura 3.5: NFC Forum Protocol Stack in Read/Write Mode

L'NFC Forum Device Architecture in Reader/Writer mode ((fig. 3.6) consiste in uno stack formato dai seguenti elementi:

- Digital Protocol, Analog: Protocolli a basso livello [NFCIP-1].
- Type Tag 1-4 Operation: comandi e istruzioni usati dall' NFC Forum Device per gestire i tipi di tag supportati.
- NDEF Applications: (Messaggi NDEF, SmartPoster, v-Card, etc.)
- Non NDEF applications: Applicazioni non basate sul protocollo NDEF

3.4.1 NDEF

NFC Data Exchange Format (NDEF) descrive un formato e lo scambio di dati tra dispositivi e TAG, utilizzando messaggi NDEF.
Come avviene nella maggior parte dei protocolli di incapsulamento, NDEF descrive il formato delle informazioni scambiate tra dispositivi NFC. I messaggi NDEF sono composti da recordNDEF. É possibile concatenare tra loro più record per ottenere un carico di dati di dimensione maggiore. L'utilizzo di questo formato consente allo sviluppatore e alle applicazioni la possibilità di scambiarsi dati NDEF con oggetti senza conoscere la specifica struttura fisica.

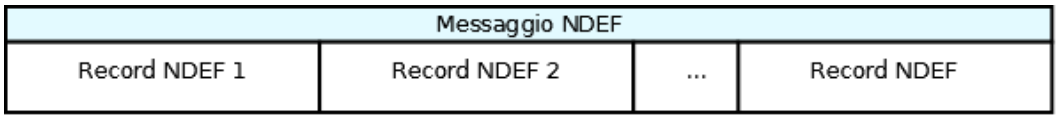

Figura 3.6: Messaggio e record NDEF

Ogni messaggio NDEF è composto da concatenazione di di record NDEF. Il record è composto da un HEADER e da un PAYLOAD che rappresenta l'informazione da trasmettere. L'HEADER contiene un insieme d'informazioni utili ad identificare sia il record all'interno del messaggio sia il contenuto del record stesso, la dimensione del PAYLOAD e il tipo di dati contenuto. Nulla vieta di utilizzare nello stesso messaggio NDEF tipi differenti di record.

3.4.2 RTD

NFC Record Type Definition (RTD) definisce i formati dei Record presenti nei messaggi NDEF. Si dividono in due categorie, creati dall'NFC Forum "Well Know Types" (WKT) e non.

I tipi WKT sono suddivisi in sotto categorie:

- NFC URI:
  - URL: "http://www.nxp.com"
  - Numeri di telefono "tel: +494056135013"
  - SMS: "sms: +494056235023?Body=Ciao!!"
  - E-mail: "mailto:nfc@nfc.com"
- TEXT:
  - "Hello World!"

- SmartPoster.
- Handover Parameters:
  - Bluetooth (PIN, address..)
  - Wifi (SSID, WEP key...)
- Business Card: vCard, orari e appuntamenti.

I Record di Tipo URI (Uniform Resurce Identifier) sono record che contengono una stringa di testo che permette di identificare in maniera certa e univoca una particolare risorsa, come ad esempio un indirizzo web, un numero di telefono di fax e così via. Tali tipi di record possono essere incapsulati in un messaggio NDEF e trasferiti da un dispositivo all'altro.

Il Record di tipo Testo contiene al suo interno un testo in chiaro. È possibile avere uno o più record di testo, associati alla stessa risorsa, ma di lingua diversa. Sono presenti anche una serie di parametri come la codifica usata per una corretta visualizzazione.

Il tipo di Record Smart Poster permette di realizzare applicazioni che scambiano tra loro percorsi URI come Indirizzi Web, Numeri di telefono e cosi via, allegando ad esse informazioni testuali di varia natura. Essi rappresentano un'estensione del concetto di record URI, permettendo d'interpretare l'URI ricevuto e di richiamare l'applicazione delegata alla gestione di quest'ultima. Inoltre essi sono in grado di far eseguire in maniera semplice applicazioni sul dispositivo NFC. Grazie alla potenza espressiva dell'URI che permette di identificare qualsiasi tipo d'informazione è possibile associare ad un qualsiasi oggetto tantissime informazioni ausiliare, spaziando dalla semplice descrizione di un oggetto o di un servizio, ad un riferimento web.

3.4.3 NFC Tipi di Tag

Non tutti i tag che lavorano a frequenza 13.45 Mhz sono compatibili con un telefonino NFC. Nella documentazione dell'NFC-Forum sono specificati 4 tipi di tag.

- Tipo 1: Sono tag basati sull'ISO 14443A, sono tag a basso costo, possibilità di lettura e scrittura e di diventare a sola lettura. Hanno una ridotta capacità di immagazzinamento fino a 96 bytes. Tipicamente sono i tag Innovision Topaz;
- Tipo 2: Sono tag basati sull'ISO 14443A, sono tag a basso costo, possibilità di lettura e scrittura e di diventare a sola lettura. Hanno una ridotta capacità di immagazzinamento da 44 bytes a 144 bytes. NXP MIFARE Ultralight;

- Tipo 3: Sono i tag conosciuti come FeliCa. La disponibilità di memoria è variabile, il limite teorico è di 1 Mbyte;

- Tipo 4: Sono i tag pienamente compatibili con gli standard ISO14443A e B parte 4. NXP DESFire, SmartMX con JCOP. Sono tag costosi.

Sono specificati anche tag extra come NXP MIFARE Classic da 1k o 4k.

3.5 API Contactless J2ME

3.5.1 Classi JSR 257 e JSR 177

J2ME (Java 2 Micro Edition) è una macchina virtuale java alleggerita di molte funzionalità rispetto al JVM di Java Standard Edition. In realtà J2ME incorpora pacchetti con funzionalità proprie e utili per piccoli dispositivi. Queste API addizionali permettono di accedere per esempio alle funzionalità multimediali come la videocamera o riprodurre file multimediali nel dispositivo (JSR 135), gestione dell'invio di SMS che MMS (JSR 120), gestione delle connessioni Web (JSR 172) oppure le più interessanti nel campo del mobile, le funzionalità contactless (JSR 257) e api per crittografia e smart card (JSR 177).

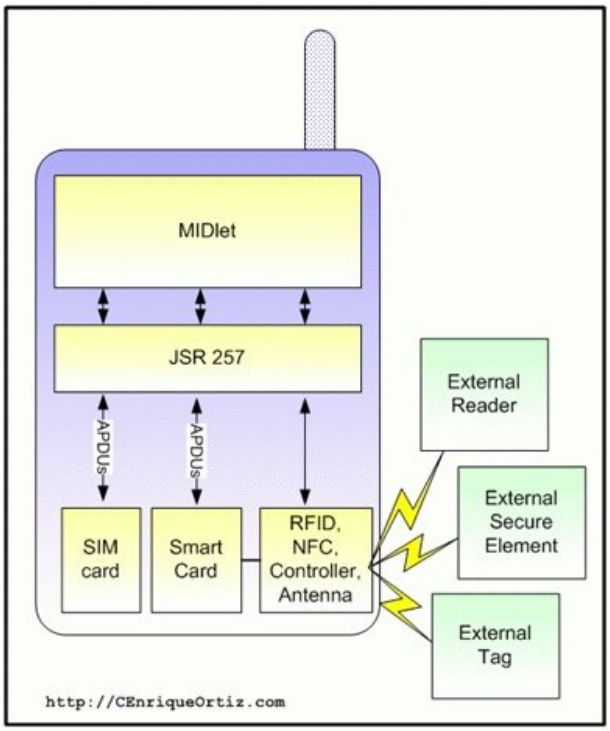

Figura 3.7: API JSR 257 e telefonino NFC

Le applicazioni J2ME, create per piccoli dispositivi con ridotte capacità di elaborazione, sono chiamate MIDLet e sono utili per fornire applicazioni di lettura e la scrittura dei tag, creare applicazioni per interagire con un altro telefonino NFC o altri collegamenti esterni, ad esempio come il Web, SMS o Bluetooth. Le MIDLet possono essere utilizzate per fornire all'utente una interfaccia di gestione per le applicazioni che utilizzano il Secure Element. L' API ContactLess JSR-257 è un pacchetto J2ME opzionale contenente le funzioni necessarie per accedere alle informazioni a smartcard, tag NFC e codici a barre. Ha svariate funzionalità per costruire messaggi basati sul protocollo NDEF. Inoltre consente la comunicazione con le SmartCard compatibili con il protocollo ISO 14443 e utilizza i comandi ADPU per la comunicazione con le stesse e con il Secure Element presenti nei telefonini NFC.
Le interfacce più importanti sono:

- javax.microedition.contactless: package principale. In particolare consente di rilevare la presenza di TAG e alla instaurazione delle connessione.

- javax.microedition.contactless.ndef: consente la comunicazione dei TAG e dei dati contenuti nello standard NDEF.

- javax.microedition.contactless.sc: consente la comunicazione con le SmartCard.

- javax.microedition.contactless.visual: consente di interagire con i TAG Visivi.

In generale un telefonino NFC rileva e gestisce un oggetto contactless alla volta, se ci sono più oggetti, viene scelto solo uno con cui comunicare. Lo scambio d'informazioni tra un dispositivo NFC e un altro dispostivo NFC o TAG avviene attraverso il protocollo NDEF. L'interfaccia contactless.ndef di JSR-257 si avvale della formattazione descritta dal protocollo NDEF e quindi fornisce una connessione a qualsiasi dispositivo che supporta i dati NDEF. L'utilizzo di questo formato consente alle applicazioni la possibilità di scambiarsi dati NDEF con oggetti senza conoscere la specifica struttura fisica.

Le API JSR 177 offrono funzioni addizionali sui sistemi di crittografia. Queste API supportano il salvataggio e lo scambio sicuro di dati e l'identificazione e autenticazione dell'utente. JSR 177 mette a disposizione API per la comunicazione con smartcard, USIM e token di sicurezza. JSR 177 implementa i protocolli ADPU e JavaCard per la comunicazione con le smartcard.

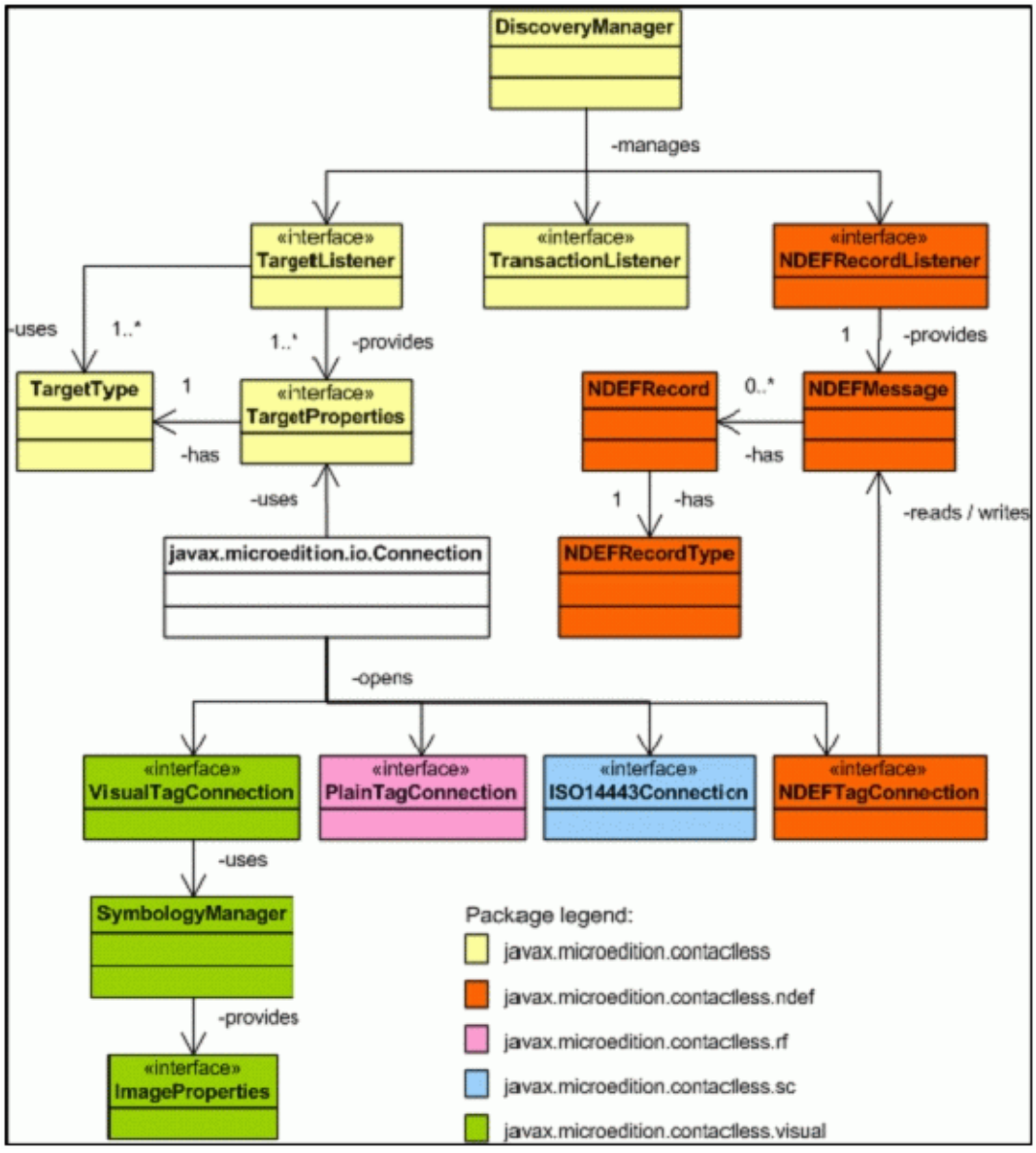

Figura 3.8: Il package JSR 257

3.6 Secure Element

3.6.1 SmartCard e applicazioni Java Card

Esempio tipico di smartcard sono le carte di credito, la SIM telefonica o schede di sicurezza per l'accesso. La smart card è costituita da un supporto di plastica nel quale è incastonato un microchip connesso ad un'interfaccia di collegamento che può essere una contattiera o un'antenna. Il microchip fornisce funzionalità di calcolo e memorizzazione dati ed è in grado di elaborare e conservare informazioni sensibili utilizzando elevati algoritmi di sicurezza come AES, DES e RSA. Tale disponibilità ha avviato una fase di notevole e sorprendente sviluppo che è partita dall'implementazione delle SIM card in ambito GSM fino ad arrivare alla realizzazione della Carta d'Identità Elettronica, delle carte di credito "intelligenti" e dei titoli di viaggio elettronici. Le SmartCard sono dispositivi resistenti alle manomissioni, qualsiasi manomissione comporta la distruzione dei dati in esso. Le SmartCard sono fortemente usate nelle procedure di autenticazione perché permette di memorizzare le credenziali dell'utente in modo sicuro, l'accesso alle credenziali è subordinato alla verifica di un PIN (Personal Idetification Number).

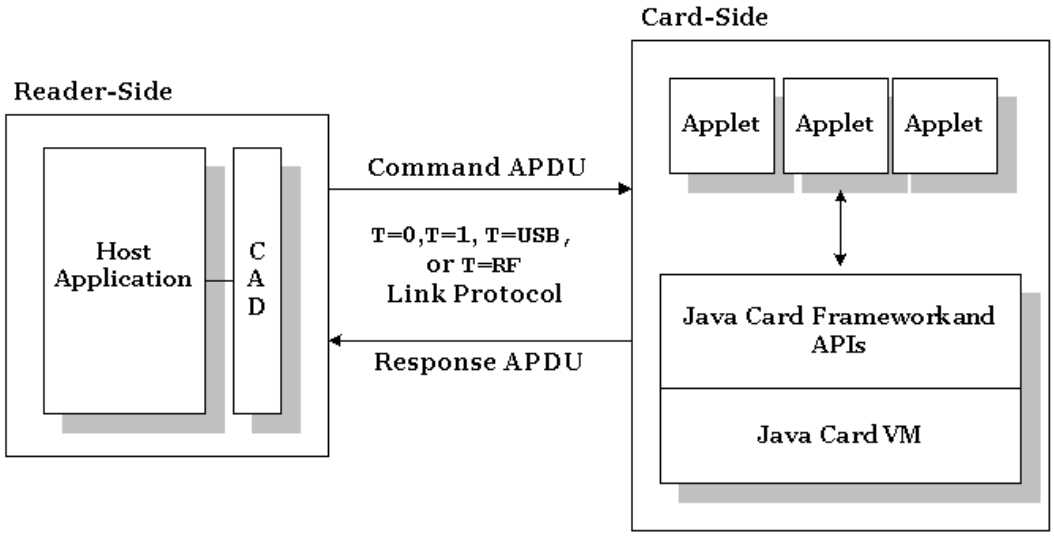

Figura 3.9: Schema Reader-SmartCard

Il microchip è l'unità che conferisce alla smart card potenzialità di calcolo e di memorizzazione. È formata dal una CPU, tipicamente da 8 o 32 bit e con una frequenza di Clock pari da 5 Mhz fino a 40 Mhz, una RAM per elaborare le applicazioni e i dati, una ROM per conservare le applicazioni e i dati statici. In sostanza si tratta di un mini personal computer. La ROM ospita anche il sistema operativo che implementa la logica operativa della smart-card. L'unità di comunicazione sono i comandi

ADPU e permettono la comunicazione tra la SmartCard e un lettore di SmartCard. Le specifiche dei comandi ADPU sono le ISO/IEX 7816. I comandi ADPU permetto di selezionare l'applicazione di interesse presente nella SmartCard e di effettuare in seguito le transizioni. Un comando ADPU è formato generalmente da 7 campi, i primi 4 determinano il particolare comando, i restanti gli eventuali parametri del comando. La tecnlogia Java Card trasferisce un sottoinsieme del linguaggio Java sulle piattaforme ottimizzate, tipiche dei piccoli dispositivi portatili, dotate di scarse risorse e di memoria come le SmartCard. Java Card intende definire uno standard di ambiente applicativo per smart card che consenta alla stessa applicazione Java Card di funzionare su diverse smart card, così come una applet Java gira su diversi computer. Come in Java, questo è consentito dalla Java Card Virtual Machine.

Per realizzare applicazioni da eseguire nelle SmartCard occorre seguire i seguenti passi:

- Scrivere il codice Java
- Compilare il codice Java
- Convertire le classi in una rappresentazione binaria composta sia dalle classi e dei packages utilizzati. Ovvero generare il file .cap
- Installazione del file cap.

Gli strumenti di sviluppo sono forniti dalla Sun con il Java Card Development Kit che include tutti gli strumenti necessari per lo sviluppo, il testing e anche la simulazione dell'esecuzione dei file cap.

3.6.2 Secure Element

Un telefonino NFC, oltre ad interagire con i Tag RFid contiene un microchip di sicurezza per gestire le informazioni sensibili. La parte dedicata alla memorizzazione ed elaborazione dei dati è chiamata "Secure Element" che lo qualifica a tutti gli effetti come carta di credito, ma che può anche essere usato come elemento identificativo sicuro di una persona, di un titolo di viaggio, etc..

L'interfaccia javax.microedition.contactless.sc consente la comunicazione con dispositivi compatibili con le smart card (API ISO 14443-4), come con l'elemento di sicuro presente nel telefonino NFC mediante comandi ADPU.

Il Secure Element può essere:

- Integrato nel telefonino separato dalla SIM card.
- Integrata nella SIM card.

- Integrato in una Secure Digital card esterna al telefonino.

Il Secure Element presente in un telefonino NFC protegge i dati sentibili, per questo è usato per il pagamento e applicazioni di ticketing. È possibile accedere al Secure Element internamene o esternameente da MIDLet e da lettori esterni, infatti è compatibile con le attuali infrastrutture contactless. La diffusione dei telefonini NFC, è molto critica poiché oltre ai componenti NFC, richiede l'adeguamento del "Secure element" del device. L'elemento sicuro è diviso in 2 parti: Java Card Area che consiste in una SmartCard e Mifare 4K Area. L'area in Java Card è usato tipicamento per i casi d'uso riguardanti i pagamenti, l'identificazione mentre il Tag Mifare è usato tipicamente per applicazioni di Ticketing. Gli sviluppatori possono creare applicazioni MIDLet per interagire con entrambe le parti, mentre le applicazioni inserite nella SmartCard si chiamano AppletCard. La capacità complessiva del SecureElement è di 72 Kb. Il sistema operativo presente nel Secure Element dei Nokia è Java Card, il produttore Giesecke& Devrient's (G & D) Sm@rtCafé Expert 3.1. L'area di Java Card è conforme alle specifiche Global Platform 2.1.1 e Java Card 2.2.1.

Java Card Open Platform (JCOP) è un sistema operativo sviluppato per piattaforma Java Card da IBM. Nel 2007 il supporto e lo sviluppo è passato a Philips-NXP.

Global Platform è un'organizzazione non-profit per la standardizzazione e lo sviluppo delle SmartCard multi applicazione. Definisce le specifiche per l'installazione e la gestione delle applicazioni nella scheda, i set di comandi, la sequenza di transazione e le interfacce. La maggior parte delle funzioni di sicurezza in ambito NFC sono basate sulle specifiche GlobalPlatform. Le specifiche sono disponibili gratuitamente presso il sito web di Global Platform.

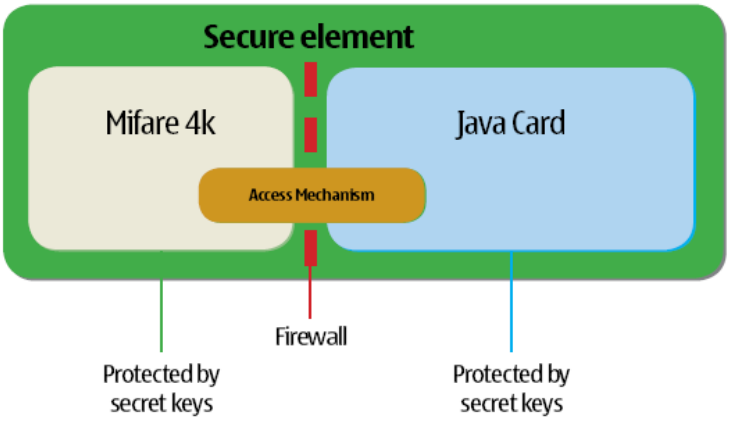

Figura 3.10: Struttura del Secure Element

I maggior produttori sono all'opera per la commercializzazione dei telefonini NFC. In particolare la Nokia ha già sviluppato cinque modelli di telefonini NFC. I più recenti sono il Nokia 6131, Nokia 6212 e il Nokia 6216. Il 6131 e il 6212 sono molto simili e utilizzano come Secure Element un chip dedicato mentre il 6216 utilizza come area di protezione la SIM card telefonica. L'idea di utilizzare la SIM card come Secure Element genera delle problematiche a livello di collegamento con il telefonino perché i contatti elettrici che connettono la SIM card tradizionale con le parti elettriche del telefono sono occupati per altri servizi come stabilito dallo standard GSMA. L'assenza di standard tecnologici condivisi per la connessione tra SIM card, Secure Element e chip NFC integrati o removibili è uno degli elementi che maggiormente frena la diffusione di questi sistemi. Il Secure Element potrà essere inserito nelle SIM Card della prossima generazione.

Il Secure Element è disciplinato da norme rigorose di sicurezza e dalle procedure del ciclo di vita, come avviene per le SmartCart. Ci sono due diverse chiavi di autenticazione per accedere al Secure Element, uno per l'area Java Card e uno per il Mifare 4K. Se si desidera accedere alla parte interna del Secure Elemet (Java Card o Mifare 4K area), la MIDLet deve essere firmata nel dominio di sicurezza della carta con una firma di fiducia certificata da terze parti, che viene acquistato da autorità di certificazione. Se la MIDLet non è firmato con almeno un certificato di terze parti, si riceve un'eccezione di protezione quando si tenta di accedere alla parte interna sicura dal MIDLet. Quando il Secure Element è operativo, le transazioni possono essere notificate alla MIDLet.

Infine è recente la notizia che il formato di memoria flash SecureDigital (SD), che già domina il mercato delle memory card tradizionali, potrebbe presto imporsi anche in quello delle schede cosiddette "contactless", capaci, cioè, di essere lette a breve distanza (pochi millimetri) da appositi lettori. Quindi è possibile introdurre la tecnologia NFC e le sua applicazioni utilizzando un telefonino attuale non NFC.

Il tipo di applicazione che si vorrà sviluppare dovrà tener conto dell'infrastuttura utilizzata e dell'ambiente in cui opera il Secure Element. In particolare si deve scegliere quale parte utilizzare del Secure Element, considerando:

- Il Mifare 4K area può essere considerata come una memoria con controllo di accesso e di solito, è più semplice da implementare rispetto la smart card. Il Mifare contiene i dati, mentre le smartcard contengno anche un programma per gestire i dati sensibili.

- L'area Java Card offre l'ambiente di alta sicurezza, significa che può essere utilizzato per applicazioni più complesse. Java Card supporta ben noti algoritmi di sicurezza.

- La gestione delle diverse applicazioni sul Mifare 4K area può essere impegnativa avendo uno spazio sicuro ma comune. Sul lato Java Card, la quantità di applicazioni è tecnicamente limitata solo dalla quantità di memoria disponibile.

3.7 Sicurezza e privacy

La tecnlogia NFC essendo figlia dei sistemi RFid, ne eredita quasi tutte le problematiche di sicurezza, infatti risulta che l'NFC in alcuni casi sia meno predisposto a certi tipi di attacchi. Particolare attenzione va anche alle problematiche di sicurezza e privacy nell'uso degli RFid, soprattutto al tracciamento illecito dei TAG per mezzo della quale è possibile violare la privacy personale/industriale nelle temeatiche della localizzazione. Le problematiche di sicurezza degli RFId dipendono in modo particolare dalla "silenziosità" e "invisibilità" delle azioni svolte da chi vuole ottenere informazioni dagli RFid. Infatti quando le aziende introducono in modo massiccio gli RFid nei prodotti di vendita al dettaglio generano il clamore di società, gruppi e difensori della privacy; il loro timore è quello che gli RFid generino un effetto "Grande Fratello". Alcuni usi sproporzionati della tecnologia RFid potrebbero violare il diritto alla protezione dei dati personali e determinare forme di controllo sulle persone. Con l'uso di sistemi RFid sempre più evoluti si potrebbe infatti raccogliere dati sulle abitudini dei consumatori e seguire perfino gli spostamenti delle persone senza che esse se ne accorgono. Quindi occorre permettere la possibilità di disinserire o addirittura distruggere (strappando) gli RFid di prodotti acquistati.

I TAG contengono informazioni. Le possibili minacce di sicurezza sottoposte agli RFid sono l'acquisizione o l'alterazione indiscriminata delle informazioni contenute utilizzando Reader a lungo raggio, oppure, occultando un Reader portatile in prossimità dei TAG, ad esempio alcuni ricercatori recentemente hanno mostrato delle vulnerabilità nelle smart card wireless Mifare, utilizzate per gli accessi a zone riservate, sfruttando proprio la raccolta d'informazioni con Reader nascosti. Quando due dispositivi comunicano tramite tecnologia NFC, un utente malintenzionato può naturalmente utilizzare un antenna per ricevere i segnali trasmessi, si presuppone che l'attaccante possa avere le necessarie conoscenze e le attrezzature necessarie, su come estrarre i dati trasmessi dal segnale RF. La comunicazione NFC di solito è fatto tra due dispositivi nelle immediate vicinanze. Purtroppo, non esiste un limite di distanza che assicura l'impossibilità di ricevere un segnare RF fuori dalla regione interessata perché il numero di parametri è enorme. Quando un dispositivo ha inviato dati in modalità attiva, l'intercettazione può essere fatta fino ad una distanza di circa 10 m, mentre quando il dispositivo di invio è in modalità passiva, questa distanza è notevolmente ridotta a circa 1 m.

Un utente malintenzionato può tentare di modificare i dati che vengono trasmessi. Nel caso più semplice l'attaccante vuole solo disturbare la comunicazione in modo tale che il ricevitore non è in grado di comprendere i dati inviati dal dispositivo. La corruzione dei dati può essere realizzata mediante invio di dati su frequenze dello spettro validi in un momento giusto (attacco Denial of Service). L'inserimento d'informazioni durante una comunicazione RF avrà successo solo se i dati inseriti possono essere trasmessi, prima che il dispositivo originale inizi con la risposta. Se entrambi i flussi di dati si sovrappongono, i dati verranno danneggiati e nessun tipo di comunicazione potrà avvenire, questo è anche il caso che si presenta nelle problematiche dell'attacco "Man-in-the-middle". Gli attacchi Man in the Middle, sono un'ampia e variegata collezione di attacchi che, come si può intuire dal nome, hanno in comune la presenza di un intruso che si insinua in maniera del tutto trasparente tra i due capi di una comunicazione creando dei canali indipendenti con ciascuno dei due attori e potendo così intercettare i dati che essi si scambiano. I due attori, credono di parlare tra loro ma in realtà sono ingannati da un terzo attore malevolo. Tale tipo di attacco è considerato praticamente impossibile in ambito NFC. Il motivo principale del fallimento di questi tipi di attacchi sta nel fatto che un lato della comunicazione è attiva mentra l'altra è passiva, ovvero l'oggetto passivo (tag) risponde immediatamente dopo l'induzione da parte del reader, un eventuale interferenza o inserimento genera un messaggio non compatibile. NFC di per sè non protegge le intercettazioni. L'unica vera soluzione per le intercettazioni è quello di stabilire un canale sicuro, data la mole di lavoro richiesta dalla cifratura, nei tag passivi non è implementata. Per instaurare un canale sicuro, in genere occorre che le parti si accordino su una chiave comune. Questo può essere fatto molto facilmente, perché l'NFC non è suscettibile teoricamente al "Man-in-the-middle". Il segreto condiviso può quindi essere utilizzato per ottenere una chiave simmetrica come 3DES o AES [18]. In modalità di comunicazione attiva o tra lettore e smartcard, conviene instaurare un canale sicuro, come è specificato nell'ISO 9798.

Capitolo 4

Sviluppo applicazione JTicketing

4.1 Descrizione del progetto

L'applicazione si occupa d'informatizzare il processo di convalida di titoli di acquisto precedentemente acquisiti tramite e-commerce.
L'applicazione può agevolmente essere destinata all'ambito del ticketing semplice: musei, spettacoli, accessi in generale. Può però anche gestire ambiti di acquisto più complessi, come nel caso pilota della "Fiera del riso", ovvero la convalida e quindi il ritiro di merce connessi ad acquisto online con fruizione/ritiro merce presso un luogo fisico. In questo senso, possiamo anche prendere in considerazione l'acquisto di elettrodomestici e prodotti di elettronica con la modalità "compra e ritira in negozio" cioè il "cash and carry", proposta da alcune catene di grande distribuzione del settore. Con la diffusione della tecnologia NFC non è da escludersi l'applicazione del modello al contesto della grande distribuzione in generale o per esempio all'ambito delle spedizioni tramite corriere. Si pensi in questo senso alla possibilità di munire addetti a prelievi e/o consegne di lettore NFC in grado di convalidare acquisti effettuati tramite e-commerce, dalla spesa di casa al ritiro di merce da inviare o da consegnare.
Poste le notevoli possibilità applicative, il progetto di sviluppo di JTicketing si basa sull'obiettivo di eliminare la coda alle casse destinate all'acquisto di pietanze presso gli stand di "Fiera del Riso".

4.1.1 Requisiti

La Fiera del riso ha lo scopo di promuovere i ristoratori di riso di Isola della Scala, permettendogli di far conoscere e degustare i prodotti tipici ai partecipanti della fiera. In genere i ristoratori trattano soltanto la consumazione di piatti di riso, mentre per acqua, vino, caffè e bibite sono prodotti venduti in altri stand dedicati. Il riso può

essere di tipo e di condimento diverso ma hanno tutti lo stesso prezzo. Il flusso di persone attirate dalla fiera è molto alto, non solo nei primi giorni d'apertura ma per tutta la durata della fiera, tanto da generare il problema della congestione alle casse per l'acquisto dei biglietti.
L'esigenza principale per l'amministrazione della fiera è ridurre tale fenomeno veicolando alcuni clienti verso gli stands grazie a una prenotazione eseguita online prima dell'arrivo in fiera.

Le azioni necessarie compiute da un cliente, per acquistare i prodotti online sono (fig. 4.1):

- Il cliente utilizza un Personal Computer per eseguire l'ordine di acquisto dei prodotti online, per esempio da casa.
- Acquista i prodotti utilizzando i metodi di pagamento online come PayPal o carta di credito.
- Riceve la conferma e il ticket di convalida via e-mail.
- Si reca alla fiera
- Convalida il BarCode
- Viene servito

4.2 Situazione di partenza

Per degustare i prodotti alla Fiera del Riso, i clienti seguono le tipiche azioni che si compiono ad ogni festa paesana, ovvero:

- All'arrivo alla fiera, il visitatore si reca ad una delle casse per acquistare i ticket.
- Consegna i ticket allo stands del marchio di riso preferito e riceve la porzione di risotto.

Il sistema attuale è molto semplice ed efficace perché ogni attore sa cosa deve fare ed è competente nella sua mansione. Il sistema, però a volte non è efficiente, un flusso elevato di clienti può generare lunghe code alle casse. Aggiungere molte casse risolve il problema ma fa aumentare i costi, sia l'operatore addetto alle casse che l'hardware e le strutture necessarie per la realizzazione delle casse stesse. Attualmente la "Fiera del Riso" utilizza un secondo metodo per l'acquisto dei titoli di consumazione. La fiera si svolge per tutto il mese di settembre e già da Agosto è

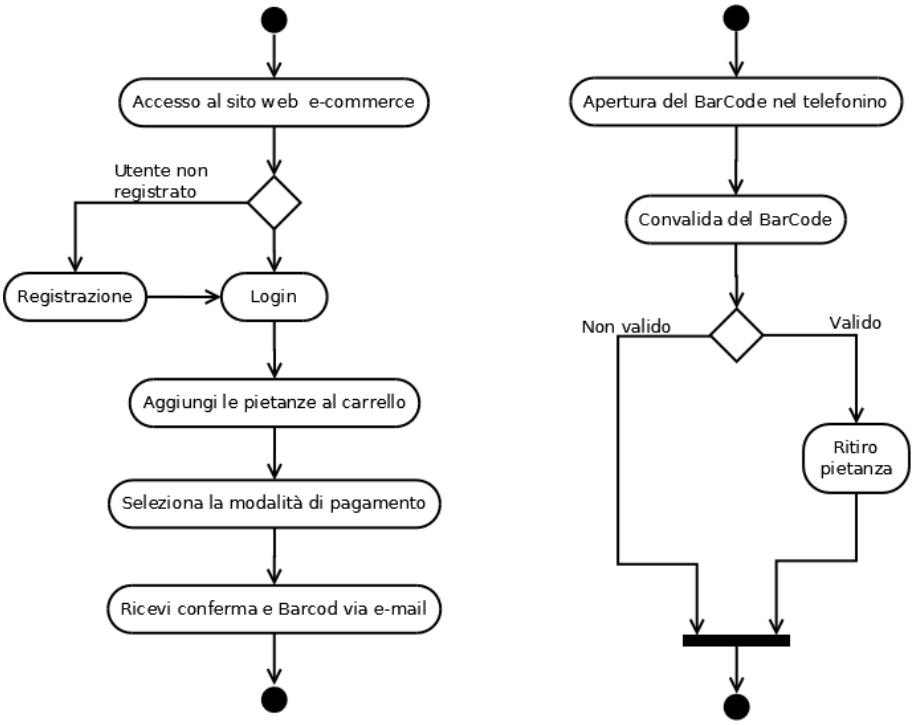

Figura 4.1: JTicketing: diagramma delle attività

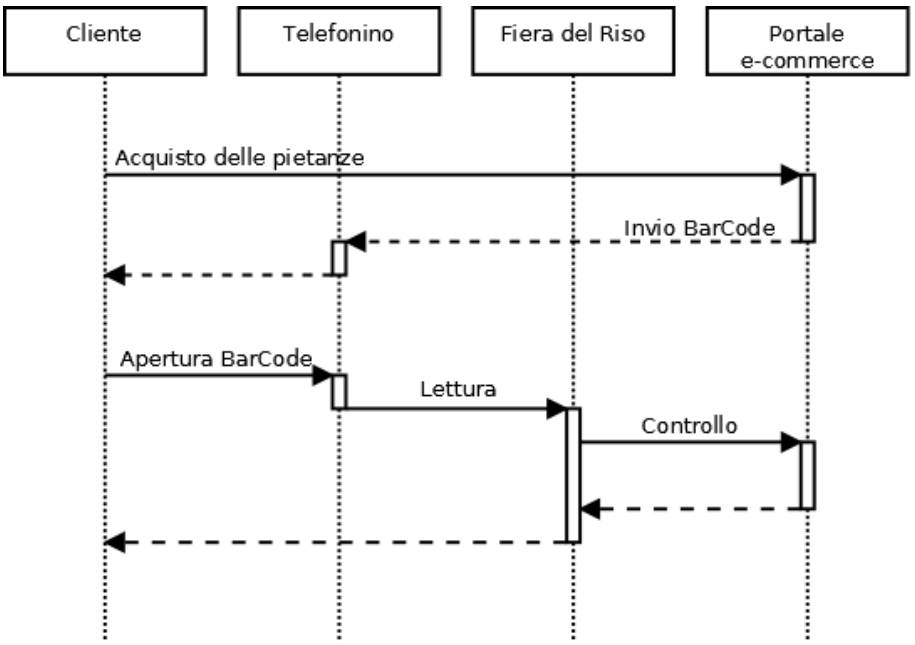

Figura 4.2: JTicketing: diagramma delle sequenze

possibile acquistare i biglietti presso negozi, supermercati sparsi in tutto il veneto e in particolare nei negozi delle vie principali di Isola della Scala.

Riguardo gli aspetti d'integrazione e collegamento, l'inserimento di un acquisto online non sconvolge l'attuale organizzazione della "Fiera del Riso". Infatti gli operatori e le casse continuano ad eseguire la loro attività. Mentre per i cuochi occorrerà prestare attenzione alle scelte di organizzazione e implementazione perché con l'introduzione del pagamento online dovranno imparare una diversa forma di convalida. All'interno della fiera è disponibile un accesso a internet Wireless e se necessario anche cablato, la copertura di rete è disponibile nei due padiglioni principali. Sono presenti inoltre due sale convegni in cui avvengono presentazioni multimediali.

Esistono diversi prodotti e servizi disponibili sul mercato per risolvere il problema delle code nelle casse: la "Fiera del Riso" ha già in progetto l'introduzione delle casse automatiche. Tramite la cassa automatica è possibile effettuare i pagamenti utilizzando monete o banconote o, tramite un terminale POS, carte di credito o bancomat. La cassa automatica rilascia i biglietti a seconda della somma versata.

Esistono dei vincoli legislativi in merito all'acquisto online di prodotti e servizi. In particolare occorre richiedere il nullaosta dal comune in cui risiede l'attività e attendere 30 giorni. Per questo motivo, il progetto è stato solo presentato.

4.3 Tecnologie a disposizione

L'azienda sede del tirocinio è già fornita di uno spazio web e database MySql remoto nel quale sarà realizzato il portate web e-Commerce. La scelta per la realizzazione del portate è ricaduta sulla soluzione opensource Joomla e le sue estensioni.

Il CMS Opensource Joombla è un software di content management per siti web, realizzato completamente nel linguaggio PHP. È pubblicato con licenza open source. Un content management system, in acronimo CMS, letteralmente "sistema di gestione dei contenuti", è uno strumento software installato su un server web studiato per facilitare la gestione dei contenuti di siti web, svincolando l'amministratore da conoscenze tecniche di programmazione. Una delle applicazioni più utili dei sistemi di CMS„ è nella gestione dei portali (intranet, extranet, community, siti di e-commerce...), dove vengono impiegati come strumento di pubblicazione flessibile e multiutente. Un CMS permette di costruire e aggiornare un sito dinamico, anche molto grande, senza necessità di scrivere una riga di HTML e senza conoscere linguaggi di programmazione lato server (come PHP) o progettare un apposito database. L'aspetto esteriore delle pagine può essere personalizzato scegliendo un foglio di stile CSS appositamente progettato per un determinato CMS. I componenti di Joomla sono estensioni specifiche che permettono di aggiungere funzionalità

complesse. VirtueMart è una soluzione per la creazione di siti e-commerce gratuita, è un software open source stabile e collaudato, per essere utilizzato ha bisogno del CMS Joomla. Come Joomla anche VirtueMart è scritto in linguaggio PHP e poggia sul database MySQL. Il componente base di Virtuemart copre le funzionalità base di un negozio on line (presentazione di cataloghi online, download di file, carrello) ma sono disponibili componenti aggiuntivi che implementano ulteriori funzionalità come per esempio la ricerca dei prodotti, visualizzazione in anteprima, statistiche e molto altro.

La decodifica di un codice a barre può essere svolta da un telefonino o da un palmare attraverso la sua fotocamera. Esistono molte applicazioni MIDLet basate sul JAVA Micro Edition, gratuite o commerciali, per la decodifica di codici a barre come il DataMatrix e QR già descritti nel capitolo 2. Questi dispositivi inoltre possono avere l'hardware necessario per un collegamento Wi-fi, da utilizzare per convalidare il codice a barre in un DBMS remoto.

In commercio sono disponibili lettori adatti alla scansione di codici a barre dal display di un telefonino. Un esempio è lo scanner Exio di NeoMedia per applicazioni su cellulari da utilizzare nei punti di vendita o nei punti di accesso. Riconosce velocemente codici 2D dal display dei telefonini inviati come SMS, EMS e MMS. Questi lettori possono essere facilmente integrati in un sistema esistente al fine di fornire una maggiore flessibilità presso il punto di vendita (centri commerciali, negozi di alimentari, e uffici) o punto di accesso (locali, parchi a tema, cinema, eventi sportivi), lotterie, mobile advertising (biglietti e tagliandi) e carte d'imbarco. In particolare collegato ad un sistema POS, PC o altri sistemi embedded, XELIA è ideale nella vendita al dettaglio presso il punto vendita. L'integrazione della stampante, display e tastiera, EXIO forma una soluzione completa per lavorare con i codici, la stampa buoni e le transazioni di esecuzione. Inoltre, il modulo integrato GSM permette di comunicare con una base di dati via GPRS oltre al collegamento LAN.

Figura 4.3: Lettori di codici dal telefonino

4.4 Ipotesi di progetto

Possiamo dividere il sistema da sviluppare in due componenti distinti:
1) Il cliente effettua il pagamento online da casa (il portale web e-commerce).
2) Si reca in Fiera, convalida i codici a barre, ritira la sua consumazione (il sistema di convalida dei codici).

4.4.1 Applicazione e-Commerce Joomla

La scelta per implementare il portale web e-Commerce ricade senza dubbio sulla piattaforma Joombla e VirtueMart. Grazie alla piattaforma Joomla, l'applicazione web appare più professionale, elegante ed affidabile. Inoltre si riduce il tempo di sviluppo e i costi d'implementazione.

I requisiti richiesti per l'applicazione web:

- Registrazione del cliente.
- Scelta della consumazione
- Pagamento online.
- Stampa dei codici a barre.
- Invio del codice a barre via MMS / Mail.
- Visione delle consumazioni prepagate e ristampa dei codici.
- Blocco di tutti o parte degli ordini richiesti.
- Visione delle consumazioni non erogate in fiera per un eventuale rimborso o bonus.

Alcuni dei precedenti requisiti non sono soddisfatti dalla piattaforma Joomla e l'estensione VirtueMart. Occorre infatti aggiungere la funzionalità di generazione codici a barre e dell'invio al cliente via MMS o e-mail. Le modifiche alla piattaforma Joomla e al DBMS non sono estremamente intrusive. L'invio della conferma via MMS è una soluzione molto efficace perché arriva direttamente nel telefonino del cliente ed è di facile visualizzazione. Gli EMS sono un'estensione dello standard SMS. I telefoni che supportano EMS possono inviare e ricevere messaggi contenenti testo formattato, disegni e suoni. La tecnologia alla base dei messaggi EMS è cioè la stessa degli SMS, cosa cambia è il modo in cui viene interpretato il contenuto del messaggio. Questo significa che per la rete telefonica non vi è distinzione

fra messaggi EMS e messaggi SMS e che tutti i telefoni in grado di ricevere SMS possono ricevere EMS, solo non sono in grado di visualizzarli correttamente. Infatti alcuni test hanno dimostrato alcune incompatibilità con alcuni telefonini. Si deve comunque tenere presente anche la realizzazione delle opportune procedure di comunicazione con tali servizi. Sotto il profilo economico, tali servizi presentano costi approssimativi di 0,08 euro + IVA per l'invio di un sms (il prezzo varia molto in funzione delle quantità) e 0,39+IVA per l'invio di un MMS. Tali costi paragonati al costo di una singola porzione venduta sono elevati. Si preferisce quindi utilizzare un' e-mail, soluzione veloce ed economica. Il cliente può recarsi in fiera con la stampa dell'e-mail contente il codice a barre oppure utilizzare il proprio telefonino se abilitato alla ricezione di e-mail.

4.4.2 Convalida codici

La convalida dei biglietti può essere fatta direttamente dal cuoco attraverso dei terminali a disposizione in ogni punto vendita. Il cliente visualizza il codice ricevuto precedentemente nel suo telefonino da un'e-mail e lo espone al lettore presente nello stand del cuoco. Il cuoco attende la conferma della convalida del codice e serve l'ordine richiesto dal cliente.

Vanno fatte alcune considerazioni: è molto probabile che il cuoco non abbia nessuna esperienza con lettori, computer e quant'altro. Il cuoco potrebbe essere contrario a compiere tale azione, perché va a peggiorare la sua attività consueta nella fiera, considerando che, senza nessun sistema di automazione, il suo compito era solo quello di strappare un biglietto e servire il cliente. Inoltre non permette ai clienti di scegliere liberamente la marca del prodotto preferito, perché sono vincolati dal fatto che non tutti gli stands supportano o hanno accettato l'utilizzo del pagamento online. Si deve valutare anche il costo di fornire ogni stand dei lettori di convalida necessari. Teniamo presente che alla fiera del riso ci possono essere dai 20 ai 40 espositori.

Una seconda ipotesi per la convalida del biglietto consiste in una stazione di convalida che converte il codice a barre in un biglietto tradizionale. Quindi il cliente si reca in qualunque stand per essere servito. Con questo sistema si ha il timore che le stazioni convalidatrici generino altre code facendo perdere l'obbiettivo finale del sistema. Salvo inconvenienti e se il sistema è efficiente, il tempo di sosta è molto breve. Il cliente può acquistare il prodotto preferito da tutti gli stands. Considerando che i benefici nell'uso del nuovo sistema è rivolto proprio ai clienti, potranno saltare il passaggio delle lunghe code alle casse semplicemente avvicinando il telefonino

al totem dei biglietti. I costi sono notevolmente ridotti dato che, sono necessari uno o due lettori.

La lettura di un codice a barre stampato in un foglio non dà problemi di lettura acquisendo l'immagine con una videocamera o con una webcam a bassa risoluzione. Il problema sorge quando si posiziona il codice a barre visualizzato sul display del telefonino. Infatti la luce irradiata dal display "acceca" la videocamera e l'immagine catturata è molto luminosa, sfocata e irriconoscibile.

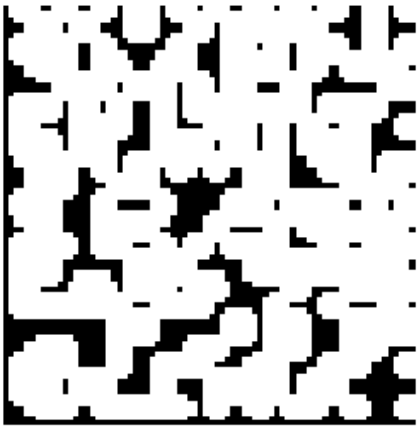

Figura 4.4: Effetto del' illuminazione di un display in una webcam

Anche tentando di migliorare manualmente l'immagine con dei filtri di correzione o utilizzando dei pacchetti commerciali appositi non ha raggiunto risultati soddisfacenti. Migliore è l'utilizzo di una videocamera di un telefonino o palmare odierno, la quale è predisposta alla acquisizione di immagini di qualità anche in presenza di fonti di luce forti. La soluzione finale è che per raggiungere un buon livello di velocità di lettura bisogna utilizare uno scanner apposito.

4.5 Implementazione

Base di dati: La principale base di dati è realizzata dal portale Web, in cui saranno registrati i clienti, gli ordini, e le avvenute consumazioni. In particolare si ha la necessità di gestire e memorizzare i seguenti dati:

- i dati di riconoscimento dell'utente: id, nome, cognome, indirizzo, e-mail, telefono, conferma consenso informativa privacy, nome utente, password.
- il catalogo prodotti in vendita: id, denominazione, prezzo.
- i dati di ogni ordine: id, singole voci acquistate, quantità per prodotto, contatore per quantità prodotto (si decrementa a seguito della consegna), id cliente,

data, I dati “quantità” e “contatore” sono differenziati per conservare lo storico dell’ordine.

Joomla: Come ogni comune catalogo per l’acquisto in e-commerce, l’interfaccia presenta la possibilità di selezionare i singoli prodotti a catalogo, ne mostra il prezzo e consente di scegliere la quantità desiderata. L’interfaccia deve essere realizzata secondo i più comuni modelli interattivi del processo di acquisto online tramite carrello. Deve quindi essere possibile accedere alla selezione di tutti i prodotti, deve essere visualizzabile il carrello nel suo stato di compilazione in ogni momento, deve essere possibile eliminare voci dal carrello e deve essere presente un campo “totale” che visualizza l’ammontare del conto. Nella conferma dell’ordine che sarà inviata via e-mail dovrà essere allegato il codice a barre. Il codice a barre potrebbe rappresentare l’id del cliente o il singolo ordine, considerando il caso specifico, si utilizzerà l’id del cliente perché gli ordini hanno sempre un unico prodotto. Il software di convalida diminuirà il contatore voce per voce di ogni ordine appartenenti allo stesso cliente. Più precisamente, l’interfaccia si compone di tre pagine:

- pagina catalogo: presenta i prodotti, ne consente la selezione e l’input delle quantità (fig. 4.5);
- pagina riepilogo e acquisto: mostra il riepilogo dell’ordine per poi procedere alla scelta del pagamento (fig. 4.6);
- pagina di conferma avvenuta transazione: invia al cliente una mail che contiene il dettaglio dell’ordine e il codice QR (fig. 4.7).

Generazione del codice DataMatrix: La piattaforma Joomla non ha componenti aggiuntivi per la generazione di codici a barre. Inoltre è necessario che lo script sia realizzato con un linguaggio compatibile al web server. Esistono molti siti che permettono la generazione online d’informazioni in DataMatrix e molte applicazioni commerciali specializzate a tale scopo. Nella ricerca di software opensource è stato trovato soltanto un unica soluzione, libdmtx. Libdmtx è una libreria opensource molto efficiente per la generazione e decodifica di codici datamatrix scritta in C, comprende anche porting per altri linguaggi come python e java, non adatte ad una applicazione web eseguita nel web server Apache disponibile dall’azienda. La ricerca di applicazioni php o cgi ha portato a testare alcune applicazioni demo prima dell’acquisto ma si sono dimostrate non funzionanti.

È stato deciso d’implementare uno script php che generi l’immagine del codice a barre attraverso le librerie grafiche “GD Graphics Library “. GD può creare immagini in formato jpeg e png utilizzando forme geometriche come linee, reattangoli, archi, testi e bitmap. Le informazioni necessarie per realizzare il simbolo sono state

Figura 4.5: ScreenShot del catalogo

Figura 4.6: ScreenShot del carrello

Figura 4.7: ScreenShot della conferma e relativo DataMatrix

prese dalla documentazione di libdmtx, dai suoi sorgenti, dalla documentazione dello standard GS1 e altre risorse web.

Un esempio per la codifica della stringa numerica “123456” in un datamatrix è descritto dai seguenti passi:
Il primo passo consiste nella codifica dei dati. In questo caso, come indicato dalle specifiche del DataMatrix ECC200 i numeri possono essere compressi utilizzando la codifica a 2 cifre, quindi otteniamo:

“12” = 12 + 130 = 142
“34” = 34 + 130 = 164
“56” = 56 + 130 = 186

I blocchi dati sono: 142 164 186
Consultando la tabella dei formati Data Matrix, possiamo vedere che i dati richiedono un simbolo di dimensione 10 righe x 10 colonne. Allo stesso modo occorrono anche 5 blocchi aggiuntivi di codici di correzione degli errori. Nel caso ci siano dei blocchi non utilizzati, perché il datamatrix è più grande del necessario, lo spazio rimanente viene riempito con blocchi di codici di correzione aggiuntivi. Utilizzando l’algoritmo di Reed-Solomon (ISO/IEC 16022), le 5 parole del codice di correzione degli errori ci danno la catena dei blocchi finali:

142 164 186 114 25 5 88 102

La traduzione degli otto blocchi binari diventa:

10001110 10100100 10111010 01110010
00011001 00000101 01011000 01100110

Ultimo passo dello script è la mappatura dell'informazione binaria nella matrice grafica. I blocchi finali vengono inseriti nella matrice come specificato dall'algoritmo descritto nell'allegato F dall' ISO/ IEC16022 (fig. 4.8): dove (1,1) corrispondente al blocco 1 e primo bit; (1.2) corrisponde al blocco 1 e secondo bit; e così via. La libreria GD ci fornisce le funzioni necessarie per generare l'immagine finale, utilizzando quadrati bianchi e neri (fig. 4.9).

2.1	2.2	3.6	3.7	3.8	4.3	4.4	4.5
2.3	2.4	2.5	5.1	5.2	4.6	4.7	4.8
2.6	2.7	2.8	5.3	5.4	5.5	1.1	1.2
1.5	6.1	6.2	5.6	5.7	5.8	1.3	1.4
1.8	6.3	6.4	6.5	8.1	8.2	1.6	1.7
7.2	6.6	6.7	6.8	8.3	8.4	8.5	7.1
7.4	7.5	3.1	3.2	8.6	8.7	8.8	7.3
7.7	7.8	3.3	3.4	3.5	4.1	4.2	7.6

Figura 4.8: Matrice della disposizione dei bit.

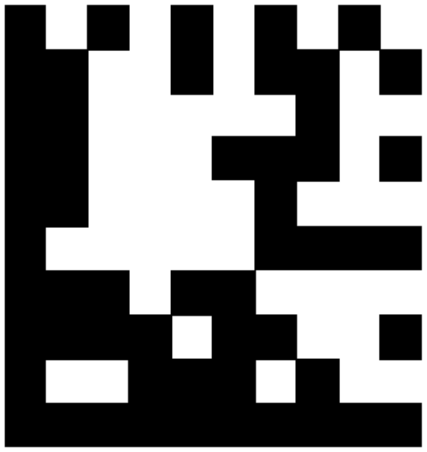

Figura 4.9: Datamatrix contentente “123456”

Applicazione di convalida: In via sperimentale e di presentazione, la convalida dei codici sarà simulato da una applicazione in java che leggerà il codice a barre da un lettore ottico.

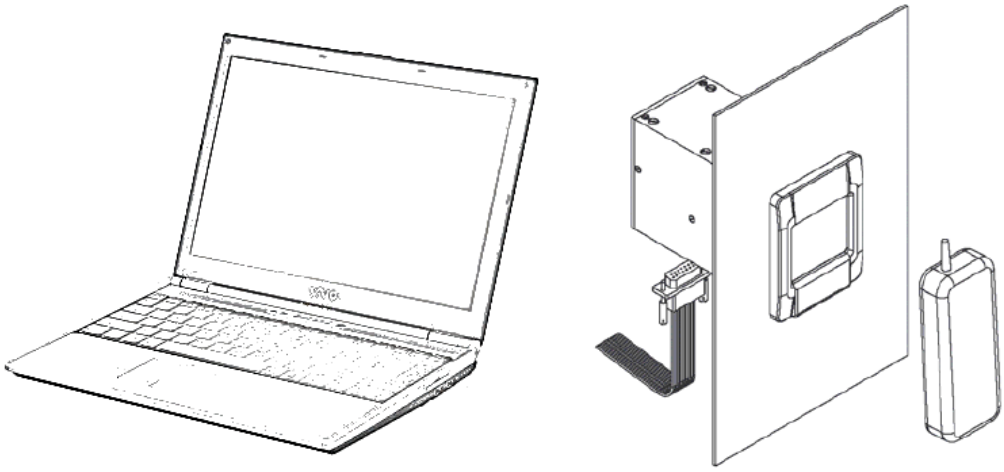

Figura 4.10: Host di controllo e lettore ottico

La scelta è ricaduta sul Gavitec MD20. Un lettore ottico studiato per la cattura dei codici a barre visualizzati sul display di un telefonino concesso in uso da una azienda di Brescia esperta nel settore delle vending machine. Il lettore in questione è configurato per la lettura dei codici a barre bidimensionale datamatrix (motivo per cui si è scelto di usare il Datamatrix).

MD20 è un modulo versatile che fornisce prestazioni elevate e flessibilità nella la lettura dei codici bidimensionali dal display dei telefoni cellulari. Equipaggiato con un processore ad alta velocità per la elaborazione del segnale digitale e una video-

Figura 4.11: Lettore codici a barre ottico MD20

camera ad alta risoluzione, MD20 legge con estrema precisione e rapidità i codici a barre 2D inviati tramite MMS (Multimedia Message Service), EMS (Enhanced Message Service) e Picture SMS (Short Message Service) dal telefono cellulare. Si utilizza nelle postazioni fisse per una vasta gamma di applicazioni: couponing mobile, mobile ticketing e mobile marketing permettendo così al telefono di essere usato come un biglietto. Può essere interfacciato con il sistema host di gestione attraverso la porta seriale RS232 o LAN.

La comunicazione tra l'applicazione e il reader avviene con un cavo seriale. Java non supporta nativamente l'interfaccia hardware della porta seriale, quindi si è scelto di utilizzare le API esterne opensource RXTXcomm.

La classe *Reader* estende la classe RXTXcomm. La prima funzione è la ricerca del lettore MD20, inizializza la porta seriale e avvia la routine di intercettazione dei dati inviati dal lettore.

La classe *Convalida* utilizza le classi fornite da Java per eseguire richieste Http verso il portale web e-commerce. Ad ogni richiesta il portale ritorna un valore "True" o "False" e le rimanenti pietanze non consumate. Ad ogni convalida viene decrementato il contatore delle pietanze negli ordini del cliente.

La classe *Form* che estende la classe dell'interfaccia utente, visualizza la risposta dal server web. Nel caso di una risposta positiva, l'applicazione di controllo visualizzerà un semaforo verde e le consumazioni rimanenti emettendo un segnale acustico, nel caso di risposta negativa visualizzerà un semaforo rosso.

4.6 Conclusioni e sviluppi futuri

Considero il sistema nella sua generalità applicabile a molte realtà quotidiane. Può essere usato per acquistare biglietti per musei e spettacoli, può sostituire l'abbonamento a servizi come il trasporto o per l'acquisto di prodotti da macchinette distributrici. Un sistema simile è già impiegato da alcune compagnie aeroportuali, i viaggiatori acquistano il biglietto online e si presentano all'imbarco con il codice a barre. Non è molto adatto in altre situazioni: per esempio quando sono richiesti molti punti di convalida, si pensi ad ogni cassa di un supermercato o ai tornelli dei trasporti pubblici, si richiederebbe l'installazione di molti scanner ottici dei quali il costo è elevato. Altre situazioni non pertinenti al sistema sono quando è necessaria una autenticazione del cliente e non solo della "quantità di servizio" acquistato, il codice a barre una volta generato è di facile copiatura. Un sistema più complesso adatto a tali scopi è il progetto MeePass, presentato brevemente nel primo capitolo, in cui il codice a barre è generato da una applicazione del telefonino con opportuni algoritmi di sicurezza. In ogni caso i codici a barre sono molto utili come tecnologia

Supported codes

Code types	2d: Data Matrix ECC200 1d: UCC/EAN (UPC/EAN/JAN), 2/5 Interleaved, Code 29, Code 128, Code 93 Optional: QR code

Optical Data

Optical system	CMOS sensor 1280 x 1024
Reading direction	Omni-directional
Reading window	Typ. 40 x 30 mm (max. 47 x 42 mm)

Electrical Data

Operating voltage	12 VDC
Power supply	< 5 Watts

Interfaces

Interface type	RS-232 for code output Keyboard wedge Ethernet RJ45 10/100Mbit/s
Connections	2 opto-galvanic decoupled digital input lines 2 opto-galvanic decoupled digital output lines
Display	Beeper for successful reading

Mechanical Data

Housing	Metal
Weight	480 g
Dimensions	60 mm (L) x 80 mm (B) x122 mm (H)

Environmental Data

Ambient temperature	5°C to 40°C (40°F to 104°F)
Humidity	5 to 90% (non-condensing)

Figura 4.12: Specifiche tecniche MD20

“ponte” verso il “Near Field Communications”, infatti le caratteristiche di un telefonino NFC sono appropriate per la conservazione in sicurezza di titoli e le infrastrutture necessarie sono più economiche di uno scanner ottico di codice a barre.

Capitolo 5

Sviluppo applicazione JCheck

La falsificazione dei prodotti di qualità genera perdite elevate ai produttori e confusione nel mercato con danni importanti al consumatore finale. Il problema della contraffazione affligge moltissime aziende italiane, che dopo avere fatto ingenti investimenti sul proprio marchio si trovano di fronte a una concorrenza fraudolenta che crea non poche difficoltà. In genere, il consumatore, dopo aver acquistato il prodotto in cui è presente il codice, che identifica singolarmente il prodotto, rimuove il sigillo anti-effrazione, dopodiché ha a disposizione una serie di opzioni per la verifica dell'autenticità. Il codice può essere:

- inviato tramite un SMS ad un numero prefissato;
- inviato tramite e-mail ad un indirizzo prefissato;
- digitato sul sito dopo essersi collegato con il telefonino;
- digitato sul sito da PC dopo essersi registrato indicando il numero di telefonino a cui ricevere la risposta.

Il sistema comunica l'esito della verifica mediante un SMS: se positiva indica anche il prodotto ed eventuali offerte e servizi personalizzati. Tutte le segnalazioni di anomalie vengono trasmesse al produttore che può così intraprendere opportune azioni d'indagine. Tutte le richieste di verifica vanno a costituire un database di utenti che il produttore può utilizzare per promuovere le proprie iniziative via SMS.
Altre soluzioni più innovative si avvalgono dell'uso di barcode bidimensionali ma solo per generare un messaggio SMS già pronto o l'apertura automatica di un URL al portale web dell'azienda produttrice. In ogni caso, sono codici prestampati nell'etichetta del prodotto e per questo soggetti a una facile "clonazione". Infatti la migliore soluzione anticontraffazione non è tanto nell'uso della tecnologia utilizzata, ma la quantità d'informazioni che si possono far avere al consumatore specifiche del

prodotto acquistato. Infatti l'anti-contraffazione è legata alla tracciabilità del prodotto. Con l'avvento dei telefonini NFC, è possibile allegare al prodotto un tag RFid. Un telefonino NFC funziona anche in modalità "reader" e quindi creare un facile ponte a un URL. Inoltre un tag RFid non è facilmente clonabile, compreso il suo UID, o per lo meno non è alla portata di tutti. L'UId dei transponder è un codice unico a livello mondiale. L'unicità è garantita direttamente dai produttori dei chip affermando che duplicare un transponder è praticamente impossibile.
Questo confronto dimostra che è molto probabile che il sistema RFID sia destinato a sostituire il tradizionale sistema a codici a barre nell'ambito degli strumenti di identificazione dei prodotti. Le funzionalità dei transponder sono infatti molto superiori a quelle del bar code e determineranno una vera e propria rivoluzione nel campo dell'identificazione che diventerà:

- automatica (nel vero senso della parola), poiché la lettura del transponder non richiede alcuna attività manuale;
- univoca, poiché il codice interno di ogni tag permette di identificare individualmente il transponder;
- incrementale, poiché le informazioni contenute nel tag possono essere modificate e aggiornate a seconda delle necessità.

La sicurezza dei sistemi, ad esempio, nel trasporto pubblico contro le frodi, dipende da molte componenti; in questo caso le smartcard ne escono vincitrici. In genere, per ridurre i costi, gli integratori di sistemi scelgono carte relativamente economiche (come le Mifare Classic) e concentrano i propri sforzi nelle operazioni di back office. Vari sistemi sono quindi utilizzati per rendere inutilizzabile la tessera eventualmente clonata, ed inserirla in apposite black list che, comunicate ai validatori, rendono impossibile l'uso della tessera clonata.

5.1 Analisi dei requisiti del progetto

JCheck è l'applicazione NFC destinata alla convalida dell'autenticità dei prodotti. L'azienda sede del tirocinio vorrebbe sviluppare un prototipo che realizza sia un sistema di verifica dell'autenticità dei prodotti sia dia la possibilità di creare nuove forme di marketing, couponig e advertising. Infatti nelle interviste effettuate, le aziende interessate si sono dimostrate più attratte alla possibilità di visualizzare sul browser del telefonino messaggi pubblicitari che l'effettiva validità del prodotto acquistato. I requisiti richiesti dal progetto da parte dell'utente è che deve aver la possibilità di ricevere il maggior numero d'informazioni possibili riguardo il prodotto

acquistato. L'azienda fornitrice del prodotto deve invece aver la possibilità di far visualizzare varie informazioni pubblicitarie variabili nel tempo. In particolare si vuole realizzare un'applicazione mobile, che interagendo con Tag RFid presenti nella confezione o nel prodotto stesso, porti l'utente a visualizzare informazioni sul display del telefonino del cliente.

Per la realizzazione del progetto occorre utilizzare le tecnologie RFid e NFC descritte nel capitolo 3. Occorre inoltre ricordare che telefonini NFC non sono ancora disponibili sul mercato, le previsioni stimano una introduzione della tecnologia NFC nel 2012. I tag Mifare Ultralight ricordiamo, sono tag senza sicurezza, hanno un identificativo numerico di 7 byte, presentano uno spazio di memorizzazione di 64 byte ed hanno un costo molto ridotto.

5.2 Ipotesi di progetto

Le ipotesi di progetto possibili sono molteplici.

1. La soluzione più semplice si basa sulla garanzia dei produttori dei tag, ovvero sull'unicità dell'UID. Quindi si inserisce un URL nella memoria del tag verso una pagina del portale dell'azienda produttrice, in questo modo si permette un ritorno da parte del server di tutte le informazioni del prodotto, messaggi pubblicitari e marketing. All'acquirente del prodotto, avvicinando il proprio telefonino al tag RFid, gli verrà suggerito di aprire una pagina web nel browser. Questo può essere fatto senza scrivere programmi particolari perché un cellulare NFC è programmato ad elaborare i contenuti dei Tag rilevati se contengono informazioni in formato NDEF.

2. Una seconda soluzione è l'utilizzo di un RFid Tag, riconosciuto e letto attraverso una MIDLet da installare nel telefonino. La MIDLet preleva l'UID del TAG e il contenuto del payload. Nella memoria del tag è possibile inserire una stringa esadecimale di sicurezza che svolge una funzione di firma, anche se, l'uid del tag è già sufficiente per garantire la provenienza del prodotto. La MIDLet può richiedere la connessione al portale dell'azienda per la verifica della chiave e la registrazione del tag in modo tale che il server invii informazioni pubblicitarie o di marketing. Questa soluzione permette inoltre di inviare al server web anche degli id univoci del telefonino come per esempio l'IMEI o il numero di telefono. In questo modo l'azienda può rilevare eventuali anomalie, come per esempio un numero esagerato di convalide di uno stesso tag.

   La stringa di sicurezza potrebbe essere generata dalla funzione:

stringasicurezza =
MD5(uidtag + eventuali informazioni + chiave azienda);

La funzione MD5 genera una somma di controllo crittografica per un messaggio, quindi non è possibile che un impostore crei una stringa di sicurezza valida con un tag fasullo avente un uid diverso e in assenza della chiave aziendale. In questo modo, legando la chiave e l'uid del tag, si permette di evitare la semplice clonazione del contenuto del tag in un tag fasullo o meglio, non registrato dall'azienda in fase di produzione. Il lato server dovrà: controllare se l'uid è registrato nel database ed eseguire il confronto "stringadisicurezza" = MD5("uidtag" + "eventuali informazioni" + "chiave azienda") e controllare la registrazione del tag nei propri database. Se la memoria del tag è sufficiente per contenere informazioni sul prodotto leggibili offline allora la stringa di sicurezza è particolarmente utile per verificare che le informazioni presenti nella memoria del tag non siano state alterate. La stringa di sicurezza può essere utile, assieme all'uid, per idetificare univocamente il prodotto perchè spesso l'acquisto in stock di tag rfid presentano uid consecutivi. Un falsificatore potrebbe utilizzare diversi uid consecutivi nei propri prodotti falsi, in modo da nascondere l'effetto di molteplici richieste al server database di un solo prodotto. Nel caso l'azienda può accorgersi di tale anomalia.

3. Per garantire la massima sicurezza di non riproducibilità del tag, la scelta ricade sull'utilizzo di TagRFid in sola lettura e con capacità di crittografia (SmartTag). In particolare occorre garantire l'impossibilità di realizzare un secondo tag con le stesse caratteristiche. Purtroppo eventuali soluzioni di questo tipo sono subito scartate dato il costo degli SmartTag.

Occorre considerare anche altri aspetti:

- L'utilizzo del server web come convalidatore comporta un costo per l'utente nelle transazioni remote dato l'uso di traffico dati internet.
- L'utilizzo di una MIDLet comporta anche la sua installazione nel telefonino del cliente, quindi occorre un passaggio ulteriore. L'installazione può essere svolta attraverso una richiesta via SMS, il download dal portale web o in negozio via BlueTooth.

La caratteristica fondamentale nella scelta dell'ipotesi migliore è senz'altro un motivo economico. L'utilizzo di smart tag con funzioni crittografiche adatte all'anticlonazione comporta un costo per singolo oggetto considerato troppo oneroso per l'azienda richiedente. In attesa di soluzioni più economiche adeguate si è deciso di utilizzare i tag semplici come i Mifare UltraLight senza sicurezza.

In definitiva, considerando la fondamentale necessità di inviare al server web degli id identificativi del telefonino (per esempio il numero di telefono a conferma dell'utente) per ricevere poi in risposta informazioni pubblicitarie e di marketing, si considera d'implementare la seconda soluzione sviluppando un'applicazione MIDLet.

5.3 Implementazione

5.3.1 Nokia 6212 e Nokia NFC SDK

Il kit di sviluppo fornitomi dall'azienda sede del tirocinio comprende:

- Due telefonini NFC Nokia 6212
- Un catalogo di tag RFid, in particolare MIFARE Classic, Ultralight e Standard.
- Un lettore RFid compatibile per la lettura di SmartCard (PCSC).
- Driver e cablaggi necessari.

Per approfondire l'esperienza con l'NFC, è stato utile utilizzare il Nokia Unlock Service MIDLet, per sbloccare il Secure Element e utilizzare le chiavi di sicurezza standard. Sbloccando il telefonino si ha una maggiore flessibilità nello sviluppo delle applicazioni inerenti al Secure Element ma non è più possibile sviluppare applicazioni di sicurezza.

Per lo sviluppo dell'applicazione JCheck è stato usato l'ambiente di sviluppo Eclipse integrando la suite NOKIA SDK NFC 6212.

Il tool NOKIA SDK NFC 6212 consente di creare ed emulare le applicazioni Java con funzionalità NFC per il telefono cellulare Nokia 6212 classic:

- Emulazione di tag in lettura e scrittura per i tipi definiti dal Forum NFC
- Contactless Communication API (JSR-257) con estensioni per lo sviluppo di applicazioni Java sul telefono cellulare
- Secure Element integrato con supporto per l'emulazione della carta Mifare 4K e ISO / Global Platform smart card, ISO 14443-4 compatibile
- Nokia 6131 NFC è compatibile con i lettori contactless (pagamento e ticketing)
- Uso di lettori Pegoda o OMNIKEY.

L'SDK replica l'interfaccia utente del telefono cellulare Nokia 6212 classic, compreso il suo look, layout dei tasti, messaggi di errore e la selezione dei menu (fig. 5.1).

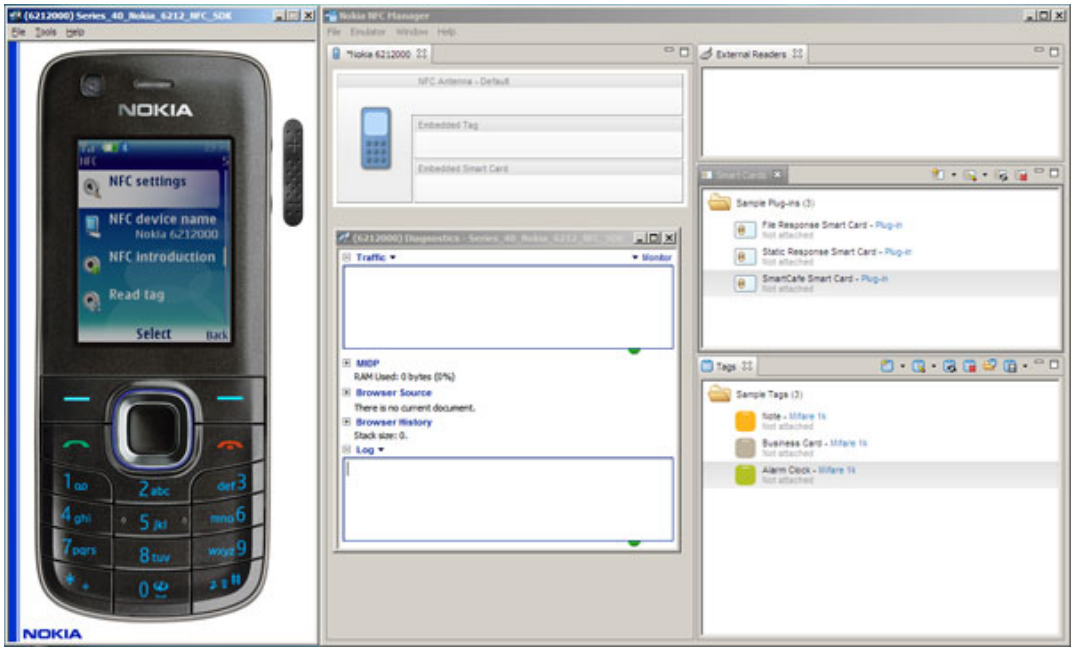

Figura 5.1: Nokia NFC SDK 6212

5.3.2 MIDLet JCheck

La MIDLet realizzata permette di individuare il tag e di aprire una connessione http al server web, ho utilizzato il DBMS MySql e Apache Web Server dell'azienda sede del tirocinio. L'applicazione web realizzata in php ha due funzionalità, dal lato dell'azienda permette d'inserire i dati del prodotto come il modello, la data di produzione, il negozio in cui è esposto ed eventuali messaggi promozionali. L'applicazione web permette dal lato del cliente di visualizzare le informazioni relativo al prodotto acquistato dal proprio Personal Computer oppure dal display del telefonino attraverso l'applicazione MIDLet JCheck.

La MIDLet è scaricabile dal suddetto sito web oppure dai negozi dell'azienda attraverso bluetooth. Inoltre è possibile installare applicazioni OTA attraverso la richiesta con un SMS.

La MIDLet realizzata permette di individuare il tag e di aprire una connessione http al server web [12] .

La classe principale è *JCheck* che estende la classe MIDLet, implementa le interfacce *TargetListener*, *CommandListener* (fig. 5.3). Questa classe, oltre ad offrire il rendering dell'interfaccia utente, eredita il metodo *targetDetect*. Il metodo *targetDetect* è richiamato quando avviene un rilevamento di un tag nelle strette vicinanze del telefonino. Quando ciò avviene, il metodo prosegue con il prelievo dell'UID del tag per poi passare al metodo *recordDetect*, per elaborare eventuali contenuti del tag. A questo punto si chiede all'utente di aprire la connessione http al server web

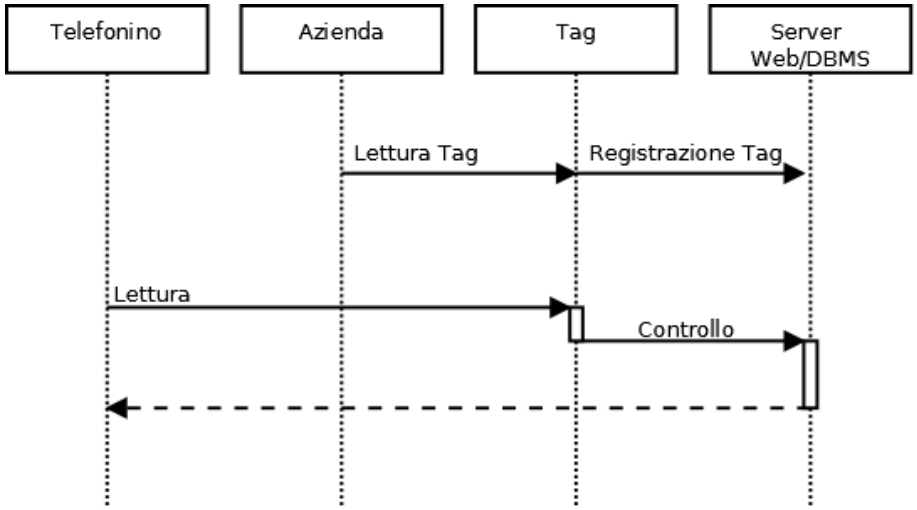

Figura 5.2: JCheck: Diagramma delle sequenze

e si attende la risposta. La risposta conterrà, in caso positivo, informazioni sul prodotto, in caso negativo, un messaggio di non validità del tag esaminato (fig. 5.4).

5.4 Conclusioni e sviluppi futuri

Il prototipo realizzato può essere una buona base di partenza per realizzare una piattaforma completa. Oltre alla visualizzazione delle informazioni riguardanti un prodotto è possibile includere forme di marketing come la raccolta punti, partecipare a concorsi a premi, diventare una carta fedeltà ed essere utilizzato per acquisire bonus e sconti. Allo stesso tempo, può sostituire l'applicazione JTicketing diventando un borsellino elettronico. Infatti l'uso dei barcode sarà presto sostituito dalle tecnologie RFid e NFC. Le applicazioni su barcode sono sviluppate principalmente per essere una tecnologia "ponte" in modo che l'NFC sia di più facile inserimento.

Ovviamente l'utilizzo del barcode ha il vantaggio di essere molto economico, non servono RFid e software particolari. A mio modesto parere il barcode sono e saranno sempre più utilizzati nelle visualizzazioni d'informazioni pubblicitarie, orari degli autobus e tutte quelle situazioni in cui occorra salvare rapidamente informazioni nel proprio telefonino.

La situazione più favorevole nell'uso dell'NFC è quando si ha a che fare con acquisti come biglietti per l'autobus o qualunque altra situazione di micropagamenti. Il "Secure Element" permette di conservare informazioni sensibili e quindi rende l'NFC adatto a tali scopi.

```
import javax.microedition.contactless.TargetListener;
import javax.microedition.contactless.DiscoveryManager;
import javax.microedition.io.HttpConnection;
import javax.microedition.lcdui.Display;
:
public class JChecky extends MIDLet implements TargetListener,CommandListener {
/**
 * A new target has been detected. This method is invoked by the platform.
 * @param prop the properties for the detected target
 */
public void targetDetected(TargetProperties[] prop) {
        // Get UID
        String uid = prop[0].getUid();
        // Get Connection Classes
        Class[] classes = prop[0].getConnectionNames();
        // Get Target Types
        TargetType[] types = prop[0].getTargetTypes();
        // Connect to each Target
        String url = prop[0].getUrl();
        try {
            // Open NDEFTagConnection to the target
            NDEFTagConnection conn =
                    (NDEFTagConnection) Connector.open(url);
            :
        } catch (IOException e) {
            // ...
        }
}

/**
 * Called by the platform, when the requested NDEF record type is
 * discovered by the device from the contactless target.
 * @param ndefMessage the NDEF message to process
 */
public void recordDetected(NDEFMessage ndefMessage) {
    // Get records and record types from NDEF Message
    NDEFRecordType[] rTypes = ndefMessage.getRecordTypes();
    NDEFRecord[] records = ndefMessage.getRecords();
    for (int i=0; i<records.length; i++) {
        // Handle data, based on type of NDEFMessage
        NDEFRecordType t = recordTypes[i];
        NDEFRecord r = records[i];
        byte[] id = r.getId();
        long len = r.getPayloadLength();
        byte[] p = r.getPayload();
        // Process the record
        // ...
    }
}
...
```

Figura 5.3: Classe JCheck, metodo targetDetect e recordDetect

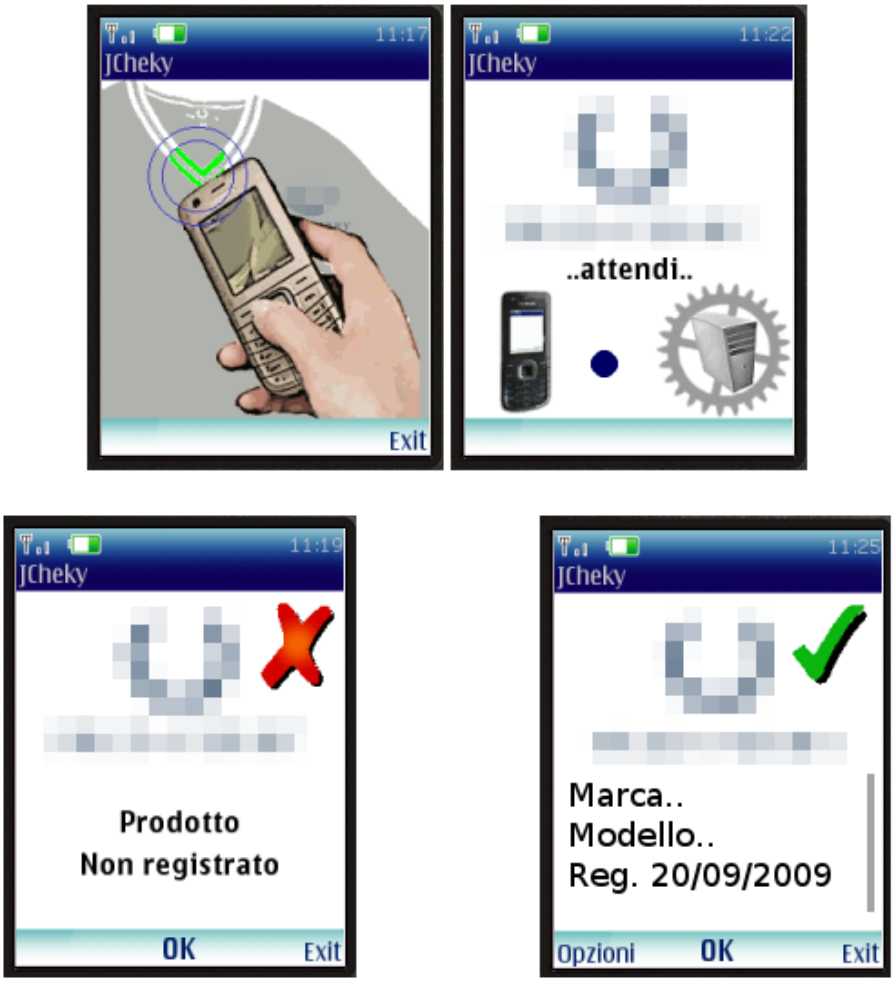

Figura 5.4: Applicazione mobile JCheck

Bibliografia

[1] Wikipedia, Barcode, http://en.wikipedia.org/wiki/Barcode, 2010

[2] Wikipedia, QR Code, http://en.wikipedia.org/wiki/QRCode, 2010

[3] Wikipedia, Data matrix, http://en.wikipedia.org/wiki/Datamatrix, 2010

[4] ISO/IEC 16022, “Data Matrix bar code symbology specification”, 2006

[5] GS1 BarCodes, “Introduction to GS1 DataMatrix”, 2009

[6] Denso Wave, “QR Code”, 2006

[7] Paolo Talone, Giuseppe Russo, Fondazione Ugo Bordoni, “RFID Tecnologia e applicazioni”, 2008

[8] Nokia Wiki, “White Papar - Near Field Communications”, 2007

[9] NFC Forum, “NFC Forum Type 2 Tag Operation Specification” , 2007

[10] NFC Forum, “NFC Data Exchange Format (NDEF)” , 2007

[11] NFC Forum, “NFC Record Type Definition (RTD) “ , 2007

[12] C. Enrique Ortiz, “An Introduction to Near-Field Communication and the Contactless Communication API”, 2008

[13] Sun, JSR-257: “Contactless Communication API”

[14] C. Enrique Ortiz, “An Introduction to Java Card Tecnology”, 2008

[15] Ugo Chirico, “Programmazione delle SmartCard”, 2006

[16] NXP Philips, “NFC Forum Type Tags - white papae v1.0”, 2009

[17] NXP Philips, “MIFARE Ultralight Features and Hints”, 2008

[18] NXP Philips, Ernst Haselsteiner, Klemens Breitfub, “Security in Near Field Communications”, 2007

[19] Vario materiale dal web, forum Nokia e Sun.