ALMA MATER STUDIORUM – UNIVERSITA' DI BOLOGNA
CAMPUS DI CESENA
SCUOLA DI INGEGNERIA E ARCHITETTURA

CORSO DI LAUREA IN INGEGNERIA ELETTRONICA E DELLE TELECOMUNICAZIONI

SISTEMI DI COMUNICAZIONE A CORTO RAGGIO: ANALISI SPERIMENTALE CON DISPOSITIVI NFC.

Elaborato in Telecomunicazioni

Relatore
Ch. mo Prof. Ing.
MARCO CHIANI

Correlatore
Ing.
ANDREA MARIANI

Presentata da
MARIO LAGHI

Sessione II
Anno accademico 2012-2013

PAROLE CHIAVE

RFID

READER

TAG

NFC

NDEF

SMART BRICK

Indice

Acronimi

3DES Triple Data Encryption Standard

Algoritmo di cifratura a blocchi ideata dall'IBM basata sulla ripetizione sequenziale del Data Encryption standard

AES Advanced Encryption Standard

Algoritmo di cifratura a blocchi utilizzata come standard dal Governo degli Stati Uniti d'America

ASK Amplitude Shift Keying

Schema di modulazione numerica in banda traslata. L'informazione è codificata nell'ampiezza della portante che assume valori discreti in funzione del bit o della sequenza di bit da trasmettere.

BPSK Bipolar Phase Shift Keying

Schema di modulazione numerica. L'informazione è codificata nella fase della portante che assume valori discreti in funzione del bit da trasmettere.

ECMA European Computer Manufactures Association

Associazione fondata nel 1961 che si dedica alla standardizzazione nel settore informatico e dei sistemi di comunicazione.

EEPROM Electrically Erasable Programmable Read Only Memory

E' un tipo di memoria non volatile, usata nei computer e in altri dispositivi elettronici. Le operazioni di scrittura, cancellazione e riscrittura hanno luogo elettricamente.

ETSI European Telecommunications Standards Institute

Organismo internazionale, indipendente e senza fini di lucro ufficialmente responsabile della definizione e dell'emissione di standard nel campo delle telecomunicazioni in Europa.

IEC International Electrotechnical Commission

Organizzazione internazionale per la definizione di standard in materia di elettricità, elettronica e tecnologie correlate. Questa commissione è formata da rappresentanti di enti di standardizzazione nazionali riconosciuti.

ISO International Organization for Standardization

Fondata nel 1947, è la più importante organizzazione a livello mondiale per la definizione di norme tecniche. Coopera strettamente con l'IEC per la standardizzazione di equipaggiamenti elettronici ed elettrici.

NDEF NFC Data Exchange Format

Protocollo di incapsulamento dati sviluppato dall'NFC Forum per standardizzare lo scambio di informazioni tra i dispositivi.

NFC Near Field Communication

Tecnologia di comunicazione wireless bidirezionale a corto raggio funzionante alla frequenza di 13.56 MHz.

NFCIP Near Field Communication Interface and Protocol

Protocollo di comunicazione NFC dove sono presenti le specifiche per i vari modi di utilizzo.

NRZ Non Return to Zero

Codifica che non prevede un stato di riposo, cioè codifica con un valore di tensione positiva un 1 e con un valore di tensione negativa uno 0.

OOK On Off Keying

Modulazione numerica che rappresenta il caso più semplice di modulazione ASK.

PCD Proximity Card Device

Reader per la lettura\scrittura di Smart Card aderenti al protocollo ISO14443. La comunicazione avviene per accoppiamento induttivo.

PICC Proximity Inductive Coupling Card

Trasponder che può essere letto da un PCD. Sono tag basati sullo standard ISO14443. Non hanno batteria e vengono alimentati dal campo magnetico generato dal reader (PCD).

PIN Personal Identification Number

E' una sequenza di caratteri numerici usata solitamente per verificare che la persona che utilizza un dispositivo, sia effettivamente autorizzata all'utilizzo del dispositivo quella operazione in quanto proprietaria dello stesso.

POS Point Of Sale

Dispositivo utilizzato presso gli esercizi commerciali, che consente di accettare pagamenti tramite carte di credito, di debito e prepagate. Il dispositivo è collegato, tramite linea telefonica, con il centro di elaborazione della banca che offre il servizio.

QR CODE Quick Response Code

È un codice a barre bidimensionale, ossia a matrice. Viene impiegato per Viene impiegato per memorizzare informazioni generalmente destinate a essere lette tramite un telefono cellulare o uno smartphone.

RFID Radio Frequency IDentification

Tecnologia di trasmissione radio per l'identificazione e/o memorizzazione dati, basata sulla capacità di memorizzazione di dati di appositi apparati chiamati TAG.

URI Uniform Resource Identifier

E' una stringa che identifica univocamente una risorsa generica che può essere un indirizzo Web, un documento, un'immagine, un file, un servizio, un indirizzo di posta elettronica, ecc.

UTF-8 Unicode Transormation Format 8bit

È una codifica dei caratteri Unicode in sequenze di lunghezza variabile

di byte.

VCD Vicinity Card Device

Reader per la lettura\scrittura di Smart Card aderenti al protocollo ISO15693. La comunicazione avviene attraverso accoppiamento induttivo.

WPAN Wireless Personal Area Network

Rete informatica senza fili che viene utilizzata per connettere più dispositivi fra loro a distanze dell'ordine di dieci metri.

CAPITOLO 1
INTRODUZIONE

Una delle tecnologie radio che negli ultimi anni ha subito il maggior sviluppo è quella dell'identificazione a radio frequenza (Radio Frequency Identification), utilizzata in un gran numero di ambiti quali la logistica, il tracciamento, l'autenticazione e i pagamenti elettronici. Tra le tecnologie specifiche legate all'RFID si ritrova la Near Field Communication (NFC). Questa è una tecnologia di trasmissione dati a corto raggio che rappresenta un'evoluzione dell'RFID. Una delle caratteristiche dell'NFC è quella di instaurare una comunicazione tra due dispositivi in maniera semplice e intuitiva. L'oggetto che instaura la comunicazione è il Reader, nell'ambito RFID è un dispositivo altamente specializzato, poiché può lavorare a diverse frequenze operative. L'elemento innovativo che ha consentito il successo dell'NFC è il fatto che questa tecnologia possa integrare il Reader in uno strumento di comunicazione di largo uso, ovvero lo smartphone. Questo permette di inizializzare lo scambio dati, sia esso di lettura di un circuito integrato passivo o una trasmissione peer-to-peer, a seguito del naturale gesto di avvicinare lo smartphone. Analisti ed esperti del settore sono convinti del successo dell'NFC, nonostante siano state smentite le attese che vedevano l'NFC integrato in oltre la metà dei cellulari entro il 2010. Questo convinzione è fornita dal grande numero di stakeholder che è coinvolto nel progetto NFC; ad essa sono fortemente interessati l'industria dei servizi di telefonia mobile, i produttori di smartphone, i consumatori, i commercianti, le istituzioni bancarie e le principali istituzioni finanziarie che processano i pagamenti come Visa, Mastercard e American Express. In Finlandia nella cittadina di Oulu si è svolto uno dei più grandi progetti legati all'NFC, in una di quelle sperimentazioni denominate NFC Cities. In questa cittadina si sono fatti dei test, cercando di capire l'impatto della tecnologia nella vita di tutti i giorni. Nel progetto lo smartphone è stato utilizzato come badge per l'identificazione degli studenti nelle scuole, come dispositivo sostitutivo ai parchimetri nei pagamenti, come menù elettronico nei ristoranti e infine come biglietto elettronico nei tram. Questo evidenzia come possa diventare pervasiva la tecnologia NFC.

Tra le molteplici applicazioni NFC in questo elaborato ci si soffermerà in particolare sul cosiddetto Smart Poster. Questo utilizzo può essere molto efficace avendo una gamma di impiego molto vasta. Si pensi al London Meseum che utilizza dei Tag di fianco alle opere d'arte per fornirne un descrizione artistica completa; un altro utilizzo decreterà la fine dei biglietti da visita: si pensi ad un Tag collocato all'esterno di un ufficio che contiene i recapiti di e-mail, telefono e fax. Questa funzione è utilizzata anche nelle

biblioteche per avere le descrizioni dei libri e nelle locandine del cinema per conoscere le trame dei film in uscita. Lo scopo dello Smart Poster è comunicare velocemente l'informazione a chi la richiede, ed è l'ideale per comunicare con uno Smart Poster. Questo tipo di utilizzo è molto simile al QR Code con la differenza che l'NFC ne migliora notevolmente velocità e durata di funzionamento. Per l'immagazzinamento dei dati nei Tag o nelle Smart Card si è utilizzato un protocollo d'incapsulamento dati chiamato NDEF (NFC Data Exchange Format) trattato nel capitolo 3 di questa trattazione. Questa codifica permette di inserire una serie d'informazioni prestabilite come ad esempio URL, SMS e vCard.

Nella seconda parte dell'elaborato si è realizzata una sperimentazione per misurare le distanze di funzionamento di cellulari e Reader per PC. In questo ambito si è realizzato quello che si è definito lo Smart Brick, cioè un mattone che comunica con dispositivi NFC grazie all'installazione di un Tag al suo interno. L'idea è nata in occasione della posa della prima pietra del futuro Campus di Ingegneria e Architettura dell'Alma Mater Studiorum Università di Bologna, Polo di Cesena. Si parlerà della realizzazione e degli strumenti software/hardware che hanno permesso di realizzare e programmare questo" mattone elettronico".

L'elaborato è strutturato in cinque capitoli di cui il primo è questa stessa introduzione.

Capitolo 2: viene definito il background tecnologico dell'NFC ovvero l'RFID. Vengono fornite le informazioni globali della tecnologia: i tipi di dispositivi, le frequenze di lavoro, la comunicazione dal punto di vista fisico e infine gli standard.

Capitolo 3: è analizzata la tecnologia NFC evidenziando in un primo momento differenze e analogie con l'RFID per poi sottolineare le novità portate dalla tecnologia. Successivamente verranno descritti i protocolli di comunicazione, e verrà approfondito il protocollo di incapsulamento NDEF. Infine verranno trattate le applicazioni e i problemi di sicurezza.

Capitolo 4: è una descrizione della strumentazione hardware e software utilizzata nella sperimentazione e verranno fatti alcuni esempi per visualizzare come vengono memorizzate le informazioni all'interno dei Tag.

Capitolo 5: viene descritta la fase sperimentale, ovvero le misurazioni tra i Reader e i Tag in gioco. Successivamente è trattata la costruzione e la programmazione dello Smart Brick.

CAPITOLO 2

SISTEMI RFID

In telecomunicazioni ed elettronica l'RFID (Radio Frequency IDentification) è una tecnologia a radiofrequenza per l'identificazione e/o memorizzazione dati automatica di oggetti, basata sulla capacità di memorizzazione di dati da parte di particolari dispositivi elettronici denominati Tag e sulla loro capacità di rispondere "all'interrogazione" a distanza da parte di appositi apparati fissi o portatili chiamati Reader, che attraverso onde radio, comunicano le informazioni in essi contenute.

Il primo prototipo di sistema RFID viene riconosciuto nel sistema "Identification Friend or Foe (IFF)" sviluppato in Inghilterra nella seconda guerra mondiale (1940). L'apparato a bordo degli aerei alleati, rispondeva, se interrogato, identificando così gli aerei alleati distinguendoli da quelli nemici. La tecnologia si è poi evoluta con un ampio numero di applicazioni quali sistemi per il tracciamento dei carri ferroviari, per l'automazione di processo e per la logistica in campo industriale, per la localizzazione del bestiame e degli animali selvatici [18]. L'infrastruttura di un sistema RFID è costituita tipicamente da tre elementi fondamentali :

- Tag o Trasponder
- Reader o Ricetrasmittente
- Sistema di Gestione o Management System

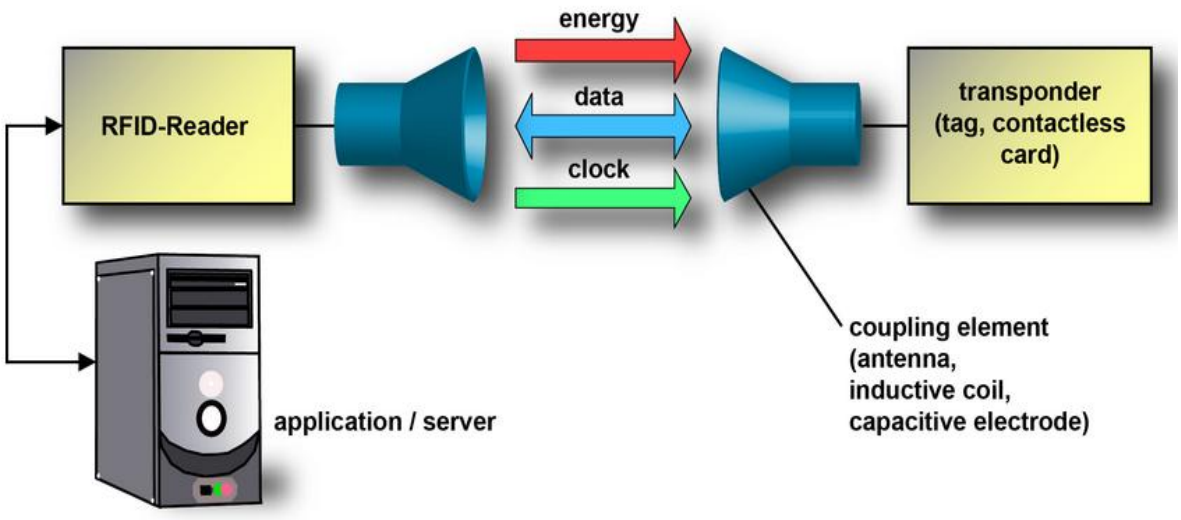

Figura 2.1: schema concettuale di un sistema RFID

Il Tag è un microchip usato per la memorizzazione di piccole quantità di informazioni che possono essere lette a radiofrequenza solo da alcuni dispositivi specializzati chiamati Reader. Il Tag è solitamente costituito da tre parti: un circuito integrato dove risiede la memoria su cui immagazzinare i dati, un antenna che serve per la ricezione e la trasmissione delle informazioni e infine un package che avvolge il congegno. I Reader sono dispositivi alimentati che identificano i Tag e con cui instaurano una comunicazione che consiste nella lettura o nella scrittura di dati. Per la comprensione e la elaborazione delle informazioni inviate dai Tag, i Reader sono supportati da un sistema di Gestione dei dati che può essere integrato nei dispositivi mobili nelle applicazioni più semplici, mentre può essere realizzato perfino da una rete di PC nelle applicazioni più complesse.

2.1 TAG

I Tag sono piccoli trasmettitori a radio frequenza dotati di un chip che ne assicura il corretto funzionamento logico. Il chip è interfacciato con una piccola area di memoria in cui è possibile immagazzinare piccole quantità di dati e da un antenna che assicura la connettività wireless del dispositivo. L'insieme di questi componenti forma il Tag che assume varie forme e composizioni a seconda del tipo e del costruttore. Nel vasto panorama dei Tag, essi possono essere classificati secondo vari criteri: caratteristiche energetiche, tipo di accoppiamento elettromagnetico e frequenza operativa.
Applicando il primo criterio, si possono distinguere tre tipi di Tag :

- Tag Passivi
- Tag Semi-Passivi
- Tag Attivi.

2.1.1 TAG PASSIVI

Privi di batterie o altre fonti di alimentazione, i Tag Passivi non utilizzano trasmettitori, riflettono il segnale RF (Radio Frequenza) ricevuto, modulandolo opportunamente secondo le informazioni contenute in memoria. Più precisamente l'energia del segnale è raccolta in un primo momento dall'antenna sotto forma di campo magnetico; successivamente, per la legge di Faraday, il campo magnetico crea una differenza di potenziale. Questa tensione genera una corrente che viene immagazzinata in un condensatore, che funge da batteria del Tag [1]. In tecnologia RFID poiché la potenza emessa dal Reader per il collegamento è fortemente limitata da vincoli normativi nazionali e internazionali, l'energia ricevuta dal Tag rende difficile la realizzazione di elaborazioni troppo complesse e rende il range di azione limitato. Nonostante ciò, questo tipo di Tag trova la sua forza in un processo produttivo dai costi ridotti e capace di generare grandi quantità di componenti utilizzabili nelle più comuni applicazioni, rendendo questo tipo di Tag il più diffuso. Allo scopo di contenere i costi, i chip di un

Tag sono realizzati usando tecnologie moderne per minimizzare la geometria del circuito; attualmente si realizzano chip di superficie 0,5 mm^2 per frequenze UHF [18]. Inoltre l'assenza di una alimentazione propria rende il ciclo di vita del dispositivo molto lungo rispetto alle altre tipologie. Questi Tag vengono generalmente integrati in oggetti come:

- Carte di credito
- Etichette adesive
- Elementi in plastica

La quantità di informazioni archiviate nelle memorie di questi Tag sono in genere limitate a qualche Kbyte. Inoltre una parte di memoria è non volatile EEPROM, su questa memoria si immagazzina l'identificatore universale (UID) che necessita almeno di 96 bit, esistono casi in cui l'UID richiede il doppio della memoria [18].
Si può quindi suddividere il Tag passivo in tre sezioni fondamentali [16]:

Figura 2.2: schema a blocchi di un tag passivo

Il primo blocco di alimentazione e trasmissione è formato da un'antenna generalmente realizzata in rame che, come detto in precedenza, sfrutterà il campo magnetico per alimentare il circuito. Il blocco di controllo, formato da un unico chip, gestisce le operazioni del Tag: la ricezione, la lettura e la trasmissione. In ambito RFID, i blocchi di memoria sono spesso di tipo Read Only, ovvero non rescrivibili, con dimensioni molto limitate dell'ordine di pochi Kbyte. Questa limitazione delle memorie è dovuta all'assenza di alimentazione che rende difficoltoso l'utilizzo di memorie programmabili [16].

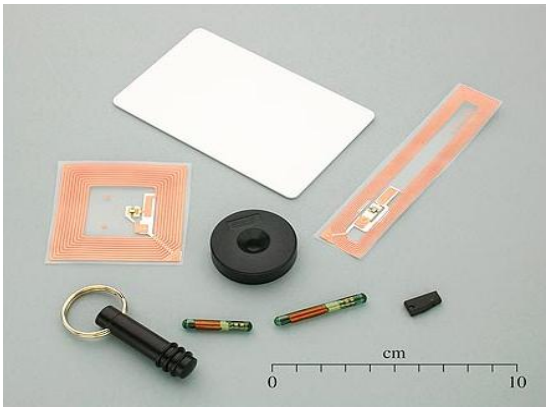

Figura 2.3: alcuni esempi di package per Tag passivi RFID

2.1.2 TAG SEMI ATTIVI

Questa tipologia di Tag è dotata di una batteria che viene utilizzata per alimentare il chip e altri eventuali dispositivi inseriti nel Tag come ad esempio: sensori di movimento, di temperatura o di pressione. Quindi la batteria ha lo scopo di alimentare il chip, mentre non è utilizzata per la trasmissione, la quale avviene ancora una volta modulando il segnale ricevuto dal Reader [18]. Grazie all'alimentazione, questo tipo di Tag può supportare memorie più complesse ed è possibile realizzare una logica più complessa che fa uso, ad esempio, di trasmissioni cifrate. L'alimentazione rappresenta anche una debolezza perché limita la vita dei Tag, per questo si è soliti usare sistemi di alimentazione che si attivano solo quando il dispositivo viene interrogato, o che ricevono l'energia necessaria grazie a sistemi come celle solari e meccanismi inerziali. Il costo dei Tag Semi-Passivi è di alcuni Euro, quindi nettamente superiore a quello dei Tag Passivi, che si aggira intorno ai 20 centesimi di Euro [16].

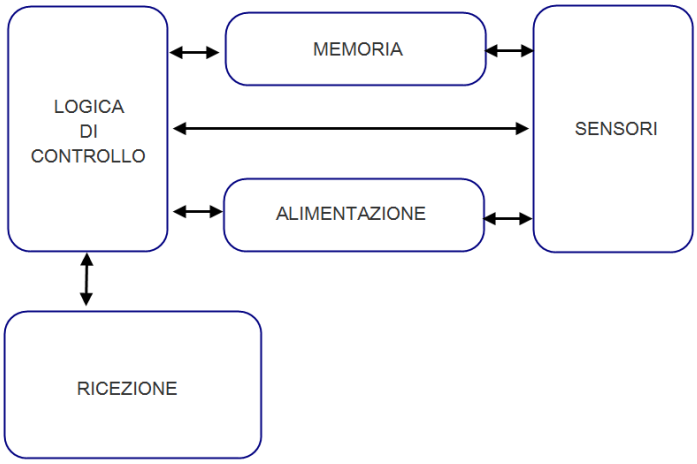

Figura 2.4: schema a blocchi di un Tag semi passivo.

2.1.3 TAG ATTIVI

I Tag Attivi si distinguono dai Tag semi-passivi perché sono dotati di un sistema di ricezione e trasmissione a radiofrequenza. Normalmente la memoria integrata ha dimensioni maggiori di quella dei Tag passivi e possono essere eseguite operazioni di lettura e scrittura su di essa [18]. Questi trasponder attivi lavorano a frequenze operative elevate (UHF e SHF), le quali gli permettono di raggiungere distanze di rilevamento di qualche Km. Il costo di produzione è elevato e supera la decina di Euro, poichè vengono utilizzati per applicazioni sofisticate destinate a mercati con richieste particolari [16].

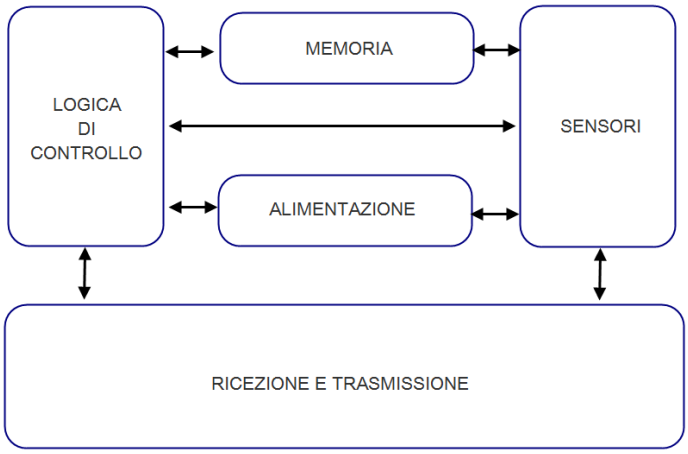

Figura 2.5: schema a blocchi di un Tag attivo

2.2 READER

I Reader, detti anche Controller, hanno la funzione di interrogare i Tag ricavandone le informazioni in essi archiviate. Nel caso di Tag Passivi, i Reader dovranno provvedere anche a fornire l'energia necessaria per attivare il Tag e permettere la comunicazione tra i due dispositivi. Spesso i Reader sono connessi ad un sistema informatico al fine di ricavare eventuali informazioni aggiuntive da database esterni. Attualmente non esiste un unico standard per la comunicazione tra Tag e Reader, pertanto è possibile utilizzare protocolli differenti a seconda della specifica applicazione.
Allo stesso modo dei Tag, è possibile classificare i Reader a seconda di vari elementi quali il tipo di accoppiamento, le frequenze operative e il loro grado di mobilità. Applicando quest'ultima classificazione, i Reader possono essere: fissi come quelli posti sui nastri trasportatori, sulle casse dei supermercati e cosi via; mobili che hanno dimensioni ridotte e sono simili ai lettori di codice a barre. Nel capitolo 4 si nota che nella tecnologia NFC i Readerpossono raggiungere dimensioni ancora inferiori.

2.3 FREQUENZE OPERATIVE

Le frequenze utilizzate per la trasmissione di informazioni tra Tag e Reader, variano a seconda dell'applicazione, della tipologia di Tag e del paese in cui essi vengono utilizzati. Le normative regolano anche la potenza massima e quindi la distanza massima di comunicazione. Le frequenze utilizzate possono essere identificate come:

- LF: Low Frequency, con banda che va da 120-145 kHz, rappresenta la prima banda di frequenze utilizzate per i sistemi RF ed è molto diffusa sul mercato;

- HF: High Frequency, con banda centrata sulla frequenza di 13,56 MHz. E' spesso definita frequenza universale in quanto tale frequenza viene utilizzata in tutto il mondo poiché non sono presenti limitazioni nazionali. Questa è inoltre la frequenza alla quale lavora la tecnologia NFC;
- UHF: Ultra High Frequency, con bande diverse per le varie zone del mondo 865-870Mhz per l'Europa, 902-928MHz per gli USA; l'utilizzo di tali frequenze impone dei forti limiti alla mobilità degli oggetti identificati, causati dall'inesistenza di un range comune di frequenze
- SHF: con banda centrata sulla frequenza di 2,4Ghz, e 5,8Ghz .

La variazione della frequenza di funzionamento incide sul progetto dei Tag, infatti avviene che al crescere delle frequenza operativa, diminuiscono le dimensioni delle antenne di questi dispositivi. Le due grandezze sono legate da un legge di proporzionalità inversa che lega la frequenza alla lunghezza d'onda del segnale: maggiore sarà la frequenza, minore sarà la lunghezza d'onda. L'antenna in sede di progetto spesso corrisponde ad un quarto delle lunghezza d'onda, quindi anche la dimensione dell'antenna dipenderà dalla frequenza. Tuttavia per trasmettere segnali a frequenza elevata, occorre più energia di quanta necessita un segnale a bassa frequenza. Per tali motivi la frequenza di 13.56MHz, forte anche della sua universalità, è diventata lo standard per la comunicazione tra Tag passivi e Reader, utilizzati in quelle applicazioni che consentono l'identificazione e l'accesso alle risorse di varia natura.

Le applicazioni che utilizzano tale frequenza possono lavorare teoricamente a distanze di 50 cm, nella pratica avviene che le distanze siano notevolmente inferiori. Per raggiungere distanze di rilevamento più elevate, sono invece utilizzati Tag attivi operanti in banda UHF. Per tali frequenze è possibile utilizzare antenne direzionali che permettono di coprire grandi distanze, anche dell'ordine delle centinaia di metri. In realtà la massima distanza di rilevamento è legata essenzialmente alla potenza del segnale inviato dal Reader. Questo non permette di definire in maniera definitiva la massima distanza di rilevamento per una determinata categoria di frequenze. E' quindi possibile che lo stesso Tag abbia un range di rilevamento diverso secondo le specifiche di potenza del Reader in oggetto.

Col crescere della frequenza, oltre a diminuire le dimensioni del Tag aumenta la velocità di Comunicazione tra Tag e Reader. Questo consente di inviare maggiori informazioni, in tempi più brevi e rappresenta un ulteriore vantaggio per l'uso della tecnologia RFID a frequenze più elevate.

2.4 ACCOPPIAMENTO TAG E READER

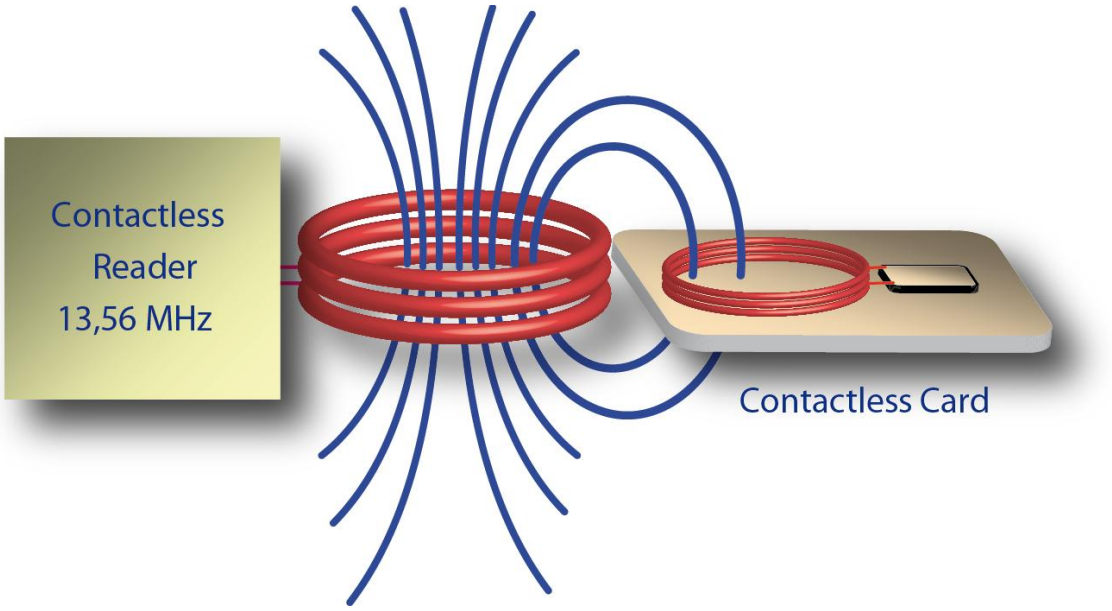

Figura 2.6: schema dell'accoppiamento per induzione magnetica tra un Reader e un Tag.

L'accoppiamento elettromagnetico è la tecnica utilizzata per stabilire un canale di comunicazione tra Tag e Reader. Per la comprensione del collegamento è necessario introdurre i concetti di Campo Lontano e Campo Vicino.
Se abbiamo una sorgente che genera e sostiene un campo elettromagnetico (EM) su una frequenza f, è possibile individuare nello spazio due regioni:

- "Campo Vicino", nel quale il campo EM ha le caratteristiche di un campo "statico" e quindi il campo vicino coincide con il campo statico istante per istante, cioè sulla base del valore istantaneo della sorgente [1];
- "Campo Lontano", nella quale il campo EM si propaga come un'onda sferica non uniforme che coincide con il campo di radiazione [16];

Poiché l'NFC instaura comunicazioni a distanze molto ridotte, tratteremo solo l'accoppiamento nella regione del cosiddetto campo vicino dell'onda elettromagnetica dove siamo in presenza sostanzialmente del solo campo magnetico [4].

2.4.1 CAMPO MAGNETICO

Ogni carica in movimento (gli elettroni in un filo o nel vuoto) genera un flusso di corrente. Ogni flusso di corrente è associato ad un campo magnetico, che può essere rilevato sperimentalmente con degli aghi magnetici.

Si introduce la legge di Ampere che relaziona il campo magnetico alla corrente: "l'integrale di linea del campo magnetico lungo una linea chiusa è uguale alla somma delle intensità di corrente concatenate alla linea".

$$\sum I = \oint H \cdot ds \tag{2.1}$$

Si può usare questa formula per calcolare l'intensità del campo magnetico per diversi tipi di conduttori. In un conduttore rettilineo il campo magnetico H, lungo una linea circolare a distanza r, è costante.

$$H = \frac{I}{2\pi r} \tag{2.2}$$

2.4.2 DIREZIONE DEL CAMPO MAGNETICO H IN UNA SPIRA

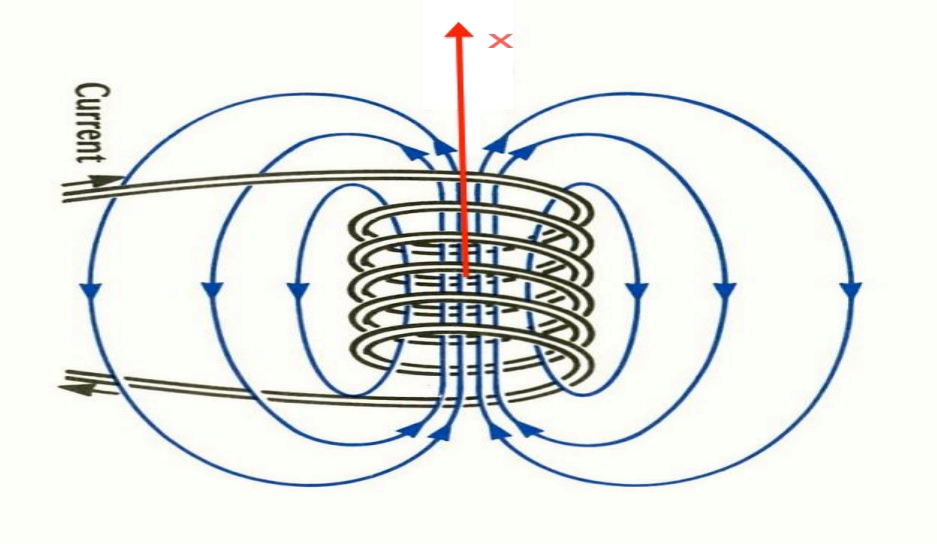

Figura 2.7: rappresentazione geometrica di un solenoide e del campo magnetico da esso generata. Dove x rappresenta la distanza dal centro lungo la direzione dell'asse del solenoide.

Spire e solenoidi sono utilizzate alla stregua di antenne per generare un campo magnetico alternato utilizzato nei sistemi RFID per la scrittura e la lettura dei dispositivi. Per instaurare una comunicazione è necessario pertanto sapere come costruire le antenne per indirizzare il campo magnetico. In questo senso si ottiene sperimentalmente che nel punto centrale della spira il modulo del campo magnetico è massimo, mentre, spostando il punto di misura lungo l'asse del solenoide (asse x), l'intensità del campo magnetico diminuirà. Attraverso l'equazione 2.3 si può stimare il campo magnetico lungo l'asse del solenoide.

$$H = \frac{INR^2}{2\sqrt{(R^2 + x^2)^3}} \tag{2.3}$$

dove N è il numero degli avvolgimenti, R è il raggio della spira e x è la distanza dal centro del solenoide lungo l'asse x. Come detto in precedenza a distanza nulla dal centro, il campo magnetico è massimo e si può semplificare la precedente formula ottenendo

$$H = \frac{IN}{2R} \ . \tag{2.4}$$

Molti Tag utilizzati all'interno delle Smart Card installano antenne costituite da avvolgimenti rettangolari. E' possibile calcolare l'intensità del campo magnetico di una spira rettangolare di dimensioni a , b usando l'equazione

$$H = \frac{N \cdot I \cdot ab}{4\pi\sqrt{\left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + x^2}} \left(\frac{1}{\left(\frac{a}{2}\right)^2 + x^2} + \frac{1}{\left(\frac{b}{2}\right)^2 + x^2} \right) \tag{2.5}$$

da questa formula si evince un aspetto importante: un'antenna molto piccola crea un grande campo magnetico al centro dell'antenna (cioè alla distanza = 0), ma a grandi distanze (x>R) un antenna di dimensioni più elevate genera un'intensità di campo magnetico più significativa. Quindi è necessario tener conto di questa proprietà nella progettazione delle antenne per sistemi RFID.

2.4.3 DIMENSIONAMENTO OTTIMO DELL'ANTENNA

Ora si riprende una bobina formata da spire circolari, facendo l'ipotesi che la corrente che è uguale in ogni spira. A questo punto, fissando una distanza x e variando il raggio dell'antenna del trasmettitore, si trova che l'intensità massima del campo magnetico dipende da un certo rapporto tra la distanza x e il raggio R. Questo significa che ad ogni distanza di lettura, corrisponde un ben determinato raggio R. Questo potrebbe portare a due casi limite se non si presta attenzione al dimensionamento: da una parte se l'antenna è troppo grande potremmo avere un intensità H così piccola da non permettere la trasmissione neanche per x=0; dall'altra, con un'antenna molto piccola, potremmo trovarci ad una quota x in cui il campo è già decaduto in maniera inversamente proporzionale a x^3.
Quindi per trovare il massimo relativo dobbiamo derivare l'eq. 2.3 rispetto al raggio R

$$H'(R) = \frac{d}{dR}H(R) = 2\frac{INR}{\sqrt{(R^2 + x^2)^3}} - \frac{3INR^3}{(R^2 + x^2)\sqrt{(R^2 + x^2)^3}} \tag{2.6}$$

Giunti a questo punto si trova il massimo della funzione H(R) in corrispondenza di uno zero della funzione H'(R)

$$2\frac{INR}{\sqrt{(R^2 + x^2)^3}} - \frac{3INR^3}{(R^2 + x^2)\sqrt{(R^2 + x^2)^3}} = 0 \tag{2.7}$$

Svolgendo i calcoli arriviamo alla forma

$$2INR(R^2 + x^2) - 3INR^3 = 0$$

$$2R^2 + 2x^2 - 3R^2 = 0$$

$$R^2 = 2x^2 \ . \tag{2.8}$$

Si ottengono due risultati

$$R_1 = x\sqrt{2} \tag{2.9}$$

$$R_2 = -x\sqrt{2} \tag{2.10}$$

In questo modo si è trovata la relazione tra la distanza di lettura (fissato da progetto) e il raggio dell'antenna. Come si nota dall'equazione 2.10 il secondo zero della derivata di H'(R) è negativo, questo perché il campo magnetico si propaga simmetricamente in entrambi i versi lungo l'asse x.

2.4.4 FLUSSO MAGNETICO, MUTUA INDUZIONE E COEFFICIENTE DI ACCOPPIAMENTO

Al campo magnetico viene associato il concetto di linee di forza del campo magnetico. Esse sono curve ideali chiuse che hanno come tangente in ogni punto la direzione del vettore del campo stesso. Il numero di linee è un indice quantitativo dell'intensità del campo stesso.

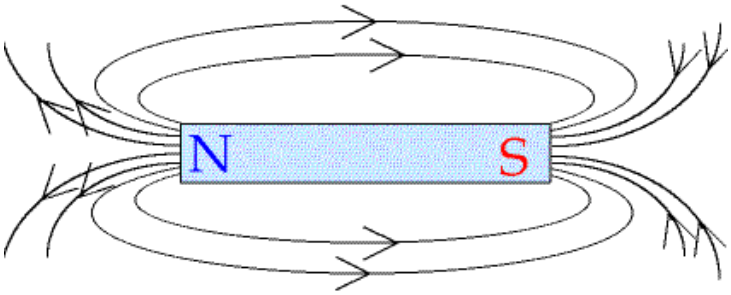

Figura 2.8: schematizzazione delle linee di campo generate da un magnete.

Il numero totale delle linee del campo magnetico che passano attraverso una bobina cilindrica, ad esempio, viene detto flusso del campo magnetico φ. Il flusso magnetico è espresso come

$$\phi = BA \tag{2.11}$$

dove A è l'area della singola spira e B è l'induttanza magnetica definita come:

$$B = \mu_0 \mu_r H = \mu H \tag{2.12}$$

dove μ_0 è la permeabilità magnetica nel vuoto e μ_r è la permeabilità magnetica relativa al materiale in cui si propaga il campo magnetico [1].
Nel caso in cui siano presenti due circuiti, ad esempio due spire, il flusso del campo H_1 (prodotto dalla corrente di intensità i_1 che percorre il circuito 1) concatenato con il circuito 2 si scrive come

$$\phi_2(B_1) = M_{12} I_1 \tag{2.13}$$

in cui M_{12} è detto coefficiente di mutua induzione. In modo analogo si può scrivere il flusso concatenato con il circuito 1, dovuto al campo B_2, ovvero

$$\phi_1(B_2) = M_{21} I_2 \tag{2.14}$$

si può inoltre dire che $M_{12} = M_{21}$ poiché M dipende solo dalla geometria dei due circuiti. [2]
Quindi la mutua induzione rappresenta l'accoppiamento magnetico di due circuiti elettrici. [1]

Se varia l'intensità di corrente, si ha anche una variazione del flusso concatenato con il circuito stesso. Si arriva cosi a definire un coefficiente di autoinduzione L, chiamato induttanza, legato al flusso del campo magnetico dalla relazione [2]

$$\phi(H) = LI \ . \tag{2.15}$$

Ora si considera un solenoide e si assume come ipotesi che l'intensità di corrente passante in ogni spira sia uguale, allora ogni spira darà uno stesso contributo ϕ al flusso totale

$$\Psi = \sum_{\mathrm{N}} \phi_N = \mathrm{N}\phi = N\mu HA \tag{2.16}$$

Quindi si può riscrivere l'equazione 2.15 come

$$L = \frac{\Psi}{I} = \frac{N\phi}{I} = \frac{N\mu HA}{I} \ . \tag{2.17}$$

Conseguentemente si riscrive l'equazione 2.14 adottando una semplificazione, ovvero ipotizzando che gli assi delle due spire coincidano [1]

$$M_{21} = \frac{\Psi_{21}(\mathrm{I}_1)}{\mathrm{I}_1} = \frac{\mu_0 H(I_1) N_2 A_2}{I_1} \tag{2.18}$$

sostituendo l'equazione del campo magnetico generato da N avvolgimenti, e considerando la spira di forma circolare, ovvero $A=2\pi R^2$, si ottiene

$$M_{21} = \frac{\mu_0 N_1 R_1^2 \, N_2 R_2^2 \pi}{2\sqrt{(R^2 + x^2)^3}} \tag{2.19}$$

Il coefficiente di mutua induzione M fra due circuiti, le cui induttanze sono L_1 e L_2 è legato a queste dalla relazione

$$M^2 = kL_1L_2 \tag{2.20}$$

da cui

$$k = \frac{M}{\sqrt{L_1 L_2}} \tag{2.21}$$

Il coefficiente k (0<k<1) misura il grado di accoppiamento: k è una misura della frazione del flusso magnetico generato da un circuito concatenato con un secondo circuito. Il caso di accoppiamento totale, che corrisponde a k=1, avviene in casi molto particolari, tipicamente nei toroidi. Per k=0 si ha disaccoppiamento totale, dovuto alla distanza o a una schermatura magnetica [2].

2.4.5 CIRCUITO EQUIVALENTE DEL TAG

Per descrivere il circuito equivalente, si parte dal fatto che la variazione del flusso magnetico ϕ genera una forza elettromotrice E_i, quindi la variazione temporale del flusso $\phi(H)$ del campo magnetico concatenato alla spira, genera una corrente all'interno del solenoide. La legge di Faraday o di induzione ne rappresenta la formulazione matematica:

$$E_i = -\frac{d\phi(B)}{dt} \tag{2.22}$$

Dove il segno negativo rappresenta in modo formale la legge di Lenz, cioè la forza elettromotrice indotta si oppone alla variazione del campo magnetico [2].
A questo punto si può costruire un circuito equivalente per l'accoppiamento induttivo di due spire.
Bisogna notare che nel caso dei sistemi RFID, l'induttanza L_1 rappresenta l'antenna del Reader, mentre L_2 rappresenta l'antenna del trasponder, dove R_2 è la resistenza della spira del trasponder, mentre R_L rappresenta il consumo di corrente del carico. Per tutto quello che si è detto in precedenza una variazione di flusso sulla seconda spira induce una forza elettromotrice che è misurabile ai capi, otteniamo così la formulazione di V_2:

$$V_2 = j\omega M i_2 - j\omega L_2 i_2 - i_2 R_2 \tag{2.23}$$

Ovvero una relazione in frequenza poiché le correnti sono sinusoidali. Se la corrente è variabile, si crea un campo magnetico variabile ed un conduttore posto nelle vicinanze del circuito viene investito da tale campo magnetico che a sua volta induce nel conduttore una corrente elettrica[4]. Perciò V_2 rappresenta la forza elettromotrice che alimenta il chip del trasponder. All'interno del circuito vi è in parallelo ad L_2 un condensatore C_2 così da creare un risonatore parallelo, con frequenza di risonanza che corrisponderà alla frequenza di funzionamento del sistema RFID in oggetto. Questa può essere trovata con l'equazione di Thomson:

$$f_R = \frac{1}{2\pi\sqrt{C_2 L_2}} \,. \qquad (2.24)$$

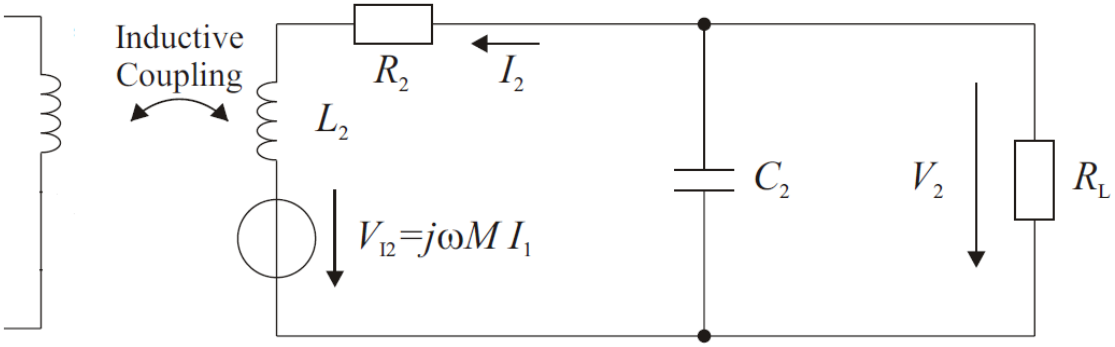

Figura 2.9: nel lato sinistro l'induttanza L1 che rappresenta l'antenna del Reader, a destra il circuito equivalente di un Tag passivo.

Chiamiamo Z_{LT} l'impedenza a valle di R_2

$$Z_{tag} = R_2 + Z_{LT} = \omega_0 L_2 \left(\frac{R_2}{\omega_0 L_2} + \frac{\omega_0 L_2}{R_L}\right) = \frac{\omega_0 L_2}{Q_2} \qquad (2.23)$$

Dove si esplicita Q_2

$$Q_2 = \left(\frac{R_2}{\omega_0 L_2} + \frac{\omega_0 L_2}{R_L}\right)^{-1} . \qquad (2.24)$$

Q_2 viene definito fattore di qualità perché rappresenta una misura dell'aumento della tensione e della corrente alla frequenza di risonanza. Come si vede nella formula (2.24), il fattore di qualità Q_2 aumenta quando il parametro R_2 diminuisce e quando R_L è molto grande, in modo da far diminuire il consumo di potenza.
Una volta fissati R_2 e R_L ci si focalizza sul valore di L_2 per avere fattore di qualità Q massimo. Tutto ciò va tenuto conto nella realizzazione di un trasponder, perché migliorando il fattore di qualità si può aumentare la forza elettromotrice indotta nel trasponder e di conseguenza anche la distanza di comunicazione tra Reader e Tag [1].
Oltre al fattore di qualità bisogna prestare attenzione alla tensione V_2, questa può raggiungere valori molto elevati dovuti alla risonanza del circuito, in molti casi valori troppo elevati per il corretto funzionamento dei Tag, fino a raggiungere in alcuni casi i 100Volt [4]. Nella pratica può avvenire che la comunicazione sia buona a massima

distanza (12-15 cm), mentre non avvenga ad una distanza inferiore (3-4cm). Questo è dovuto ad una tensione troppo alta nel trasponder [**3**]. Per risolvere questo problema, e perciò mantenere costante la tensione $V_{2,}$ si può vedere la resistenza R_L come il parallelo della resistenza del chip R_L con un resistore a resistenza variabile R_S [1]. Si ottiene un regolatore di resistenza (shunt regulator) che adatta l'alimentazione del Tag in funzione della distanza [3].

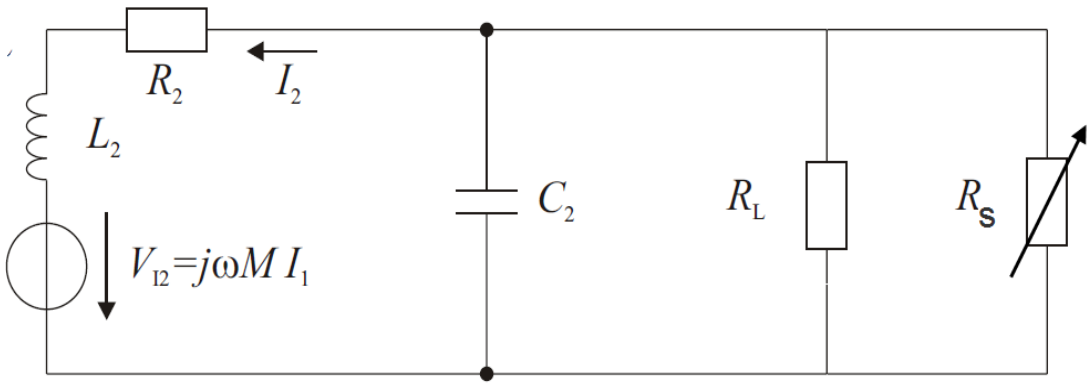

Figura 2.10: circuito equivalente con Shunt Regulator R_S.

Dove lo shunt regulator R_S può essere realizzato con un semplice circuito di questo tipo:

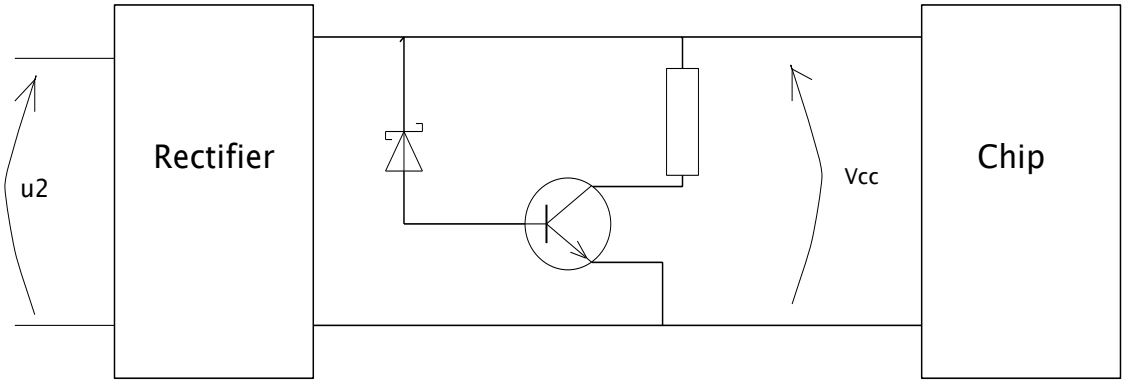

Figura 2.11: una realizzazione circuitale di uno shunt regulator.

2.4.6 ARCHITETTURA DI COMUNICAZIONE

La comunicazione tra Reader e Tag avviene modulando in ampiezza il campo magnetico generato dall'antenna del Reader con il segnale che deve essere trasmesso in banda base. Le tecniche di modulazione utilizzate in ambiente RFID, devono soddisfare criteri di efficienza sia per l'occupazione spettrale (rapporto bit/hertz) sia per potenza necessaria alla trasmissione (rapporto segnale/rumore). A questo si aggiunge la necessità di trasferire potenza elettrica al Tag in modo continuo [19].

Si fornisce una schema a blocchi che riassume il funzionamento della comunicazione all'interno del Tag:

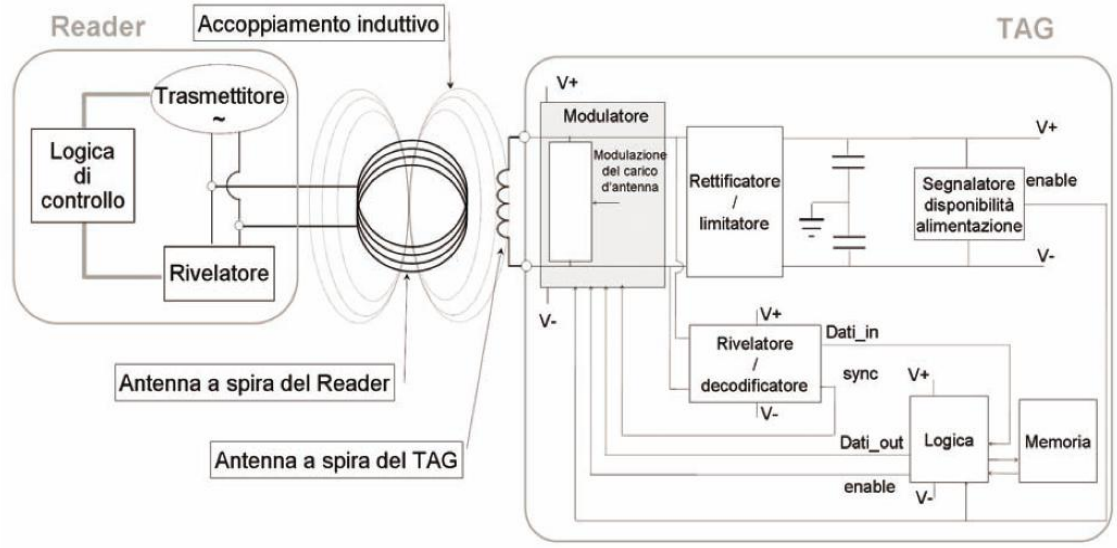

Figura 2.12: a sinistra architettura del Reader, a destra architettura del Tag.

Il blocco "modulatore" presente nell'architettura del Tag entra in gioco quando il Tag risponde al Reader ed utilizza una Load Modulation. Questa tecnica permette di variare i parametri del circuito risonante per mezzo dei dati da trasmettere al Reader. Sostanzialmente si modula l'impedenza del circuito, cioè si varia la fase o l'ampiezza, in dipendenza dei dati. Due sono i modi in cui possono essere alterati i dati da trasmettere: o variando la resistenza di carico (ohmic load modulation) quindi l'ampiezza del segnale, oppure variando la capacità in parallelo (capacitive load modulation). Il Reader al suo interno avrà un circuito che permette di riconoscere i due tipi di variazione del segnale associata al dato trasmesso [4].

In sintesi la comunicazione tra Reader e Tag si svolge con la seguente sequenza:

1. La logica di controllo del Reader invia i dati (dell'interrogazione) al trasmettitore che genera il segnale per l'antenna a spire.
2. La corrente nell'antenna del Reader induce un campo magnetico pulsante che si concatena con l'antenna a spire del Tag.
3. La potenza di alimentazione viene estratta da un circuito rettificatore / limitatore.
4. Un circuito di segnalazione abilita il funzionamento dei rimanenti circuiti segnalando la disponibilità di alimentazione.
5. Il rivelatore/decodificatore fornisce i dati decodificati alla logica di controllo (che eventualmente provvederà a scriverli nella memoria).
6. Il rivelatore/decodificatore segnala al modulatore gli istanti in cui è possibile attivare la trasmissione dei dati verso il Reader.

7. La logica di controllo del Tag legge i dati nella sua memoria e segnala la disponibilità al modulatore che genererà il segnale di pilotaggio negli istanti opportuni (modula l'impedenza d'antenna del Tag medesimo).
8. Il Reader percepisce (tramite il rivelatore) le variazioni d'impedenza dell'antenna del Tag (essendo le spire del Tag e del Reader accoppiate come gli avvolgimenti di un trasformatore) e trasmette i dati ricevuti alla sua logica di controllo.

2.5 CENNI AGLI STANDARD RFID

L'utilizzo sempre più diffuso di dispositivi RFID ha suggerito, nel corso degli anni, la necessità di stabilire delle regole generali che debbono essere seguite per realizzare sistemi basati su questa tecnologia. Lo sviluppo delle regole di standardizzazione è compito del comitato internazionale denominato ISO (International Standards Organization). Il comitato ISO raggruppa le istituzioni che nel mondo si occupano di standardizzazione a livello nazionale, per esempio il comitato DIN in Germania, il CEI in Italia ed il comitato Ansi negli Stati Uniti.

2.5.1 ALCUNI ESEMPI DI STANDARD ISO

Una prima serie di standard sono quelli dedicati alle problematiche relative all'identificazione degli animali all'interno degli allevamenti, e sono: ISO 11784, ISO 11785, ISO 14223.
Nel caso dell'identificazione di animali, lo scopo dei dispositivi RFID è quello di permettere il tracciamento dei singoli capi, per verificare, ad esempio, l'avvenuta somministrazione di farmaci od altre sostanze. In questo senso è necessario dotare ogni animale di un codice identificativo. Da un lato lo standard **ISO 11784** descrive appunto la struttura e le informazioni che questo codice gestisce, mentre dall'altra parte lo standard **ISO 11785** regola le modalità di interazione tra Reader e trasponder. Lo standard ISO 11785 stabilisce la frequenza operativa del Reader che dovrà essere di 134.2 KHz, inoltre stabilisce che il Reader debba generare un campo elettromagnetico con un periodo di attivazione di 50 ms ed un periodo di disattivazione di 3ms. Lo standard si occupa anche delle pratiche operative da mettere in atto per rendere possibile la presenza nella stessa area di diversi Reader evitando collisioni nelle richieste dati. Gli standard citati in precedenza prevedono che il trasponder comunichi con il Reader inviando soltanto un semplice codice identificativo. Lo standard **ISO 13233** rappresenta un'evoluzione perché permette di gestire più informazioni. Per di più questo standard contiene sia i protocolli sulla struttura dei dati sia i protocolli che gestiscono le comunicazioni tra Reader e trasponder [5].

2.5.2 STANDARD ISO RIFERITI A SISTEMI CHE UTILIZZANO TRASPONDER NELLA FORMA DI *SMART CARD*

Gli standard che regolamentano le realizzazione di sistemi di identificazione di questo tipo sono: ISO 10536, ISO 14443, ISO 15693.

Lo standard **ISO 10536** identifica uno standard per Smart Card operante alla frequenza 4.92 Mhz. In realtà è uno standard poco utilizzato a causa della scarsa distanza operativa, circa 1 cm, da cui il nome "close coupling" [5]. Questo standard è composto da 4 parti:

1. Caratteristiche fisiche;
2. Dimensione delle zone di accoppiamento induttivo;
3. Segnali elettrici e procedure di reset;
4. Reset e protocolli di trasmissione [1].

Lo standard **ISO15693** è uno standard destinato alle Smart cards della famiglia delle Vicinity Cards ovvero carte che possono essere lette e scritte da distanze superiori al metro, teoricamente fino 1,5 metri. Questo tipo di carte sono poco potenti dal punto di vista computazionale usate soprattutto per data storage. In particolare sono dotate di una memoria a blocchi a cui si può accedere e scrivere, oltre all'identificatore univoco [6]. La comunicazione, anche in questo standard, avviene per accoppiamento induttivo. Generalmente i trasponder sono di tipo passivo, sfruttano così il campo elettromagnetico generato dal Reader per comunicare [5]. Anche in questo caso lo standard si suddivide in 4 parti:

1. Caratteristiche fisiche;
2. Radiofrequenza e Modulazione;
3. Protocolli;
4. Registrazione di applicativi.

2.6 STANDARD ISO 14443

Le Smart Cards che aderiscono allo standard **ISO 14443** appartengono alla famiglia delle Proximity Cards, queste funzionano a distanze maggiori dell'ISO 10536, infatti si raggiungono anche i 10 cm. Sono dispositivi più potenti delle Vicinity card e ne esistono vari tipi con veri e propri processori general purpose che si avvalgono di sistemi operativi integrati. Sono dotati anche di sistemi di sicurezza e di crittografia dei dati, questo è uno dei principali motivi per il quale sono tra le Smart Card più utilizzate anche nell'ambito NFC [6]. Questi apparati trovano utilizzo ad esempio nel campo dei pagamenti e in quello dei mezzi pubblici. In pratica, grazie a questi dispositivi il passeggero non deve più annullare il biglietto mediante la classica timbratura, ma il suo passaggio è registrato grazie all'utilizzo di un biglietto RFID. I dispositivi appartenenti a questo standard utilizzano trasponder passivi, che funzionano sfruttando il principio

fisico dell'accoppiamento induttivo, descritto in precedenza [5]. Ora per rispettare la terminologia dello standard si introduce il PCD (Proximity Card Device) che rappresenta il Reader e il PICC (Proximity Integrated Circuit Card) che sostituisce il termine Tag (che potrà essere chiamato anche "carta").
Il protocollo si divide ed è descritto in 4 parti:

1. **Caratteristiche fisiche.** Si definiscono le proprietà meccaniche delle Smart Cards, le dimensioni in accordo con ISO 7810 (carte di credito)[8] ovvero 85.72 mm x 54.03 mm x o.76 mm. Inoltre vengono elencate alcune specifiche sulla torsione delle carte e su alcuni test riguardanti l'esposizione ai raggi UV, ai raggi x e infine alle radiazioni elettromagnetiche [1].
2. **Radiofrequenza e Modulazione.** Si stabiliscono alcuni parametri: alimentazione tramite campo magnetico alternato a 13.56 MHz, avvolgimento di accoppiamento con 3-6 spire perimetrali, campo minimo per il funzionamento del trasponder dev'essere H_{min}=1.5 A/m, mentre per quanto riguarda il campo generato dal lettore 1.5 A/m < H < 7.5 A/m [8]. In quanto in fase di definizione dello standard non si è trovato un accordo per quanto riguarda su un'unica interfaccia di comunicazione: sono presenti un Tipo A e un Tipo B, significativamente diversi. Una carta conforme allo standard deve supportare un solo tipo di interfaccia [8]. Il PCD deve funzionare in maniera alternata, ovvero passare dal metodo A e B, fino a che non viene riscontrata la presenza di un PICC di tipo A o di tipo B. Solo un interfaccia deve rimanere attiva durante una sessione di comunicazione. Alla fine della comunicazione si potrà utilizzare anche l'altra interfaccia [6].

- Modalità A. In DownLink (PCD to PICC) abbiamo codifica 100% ASK con codifica di Miller modificata, lo standard impone tutti i tempi di salita e di discesa. In Uplink (PICC to PCD) abbiamo modulazione del carico con sottoportante: f_{sc}=847 Khz (13.56 Mhz/16), la modulazione della sottoportante è OOK con codifica i Manchester. La velocità di trasferimento in uplink che in downlink: 106 kbit/s [8].
- Modalità B. in Downlink abbiamo modulazione 10% ASK con codifica NRZ, anche in questo caso lo standard definisce tutti i transitori. In Uplink si ha modulazione del carico con sottoportante: f_{sc}=847 Khz. La modulazione della sottoportante è BPSK a 180° con codifica NRZ [8].

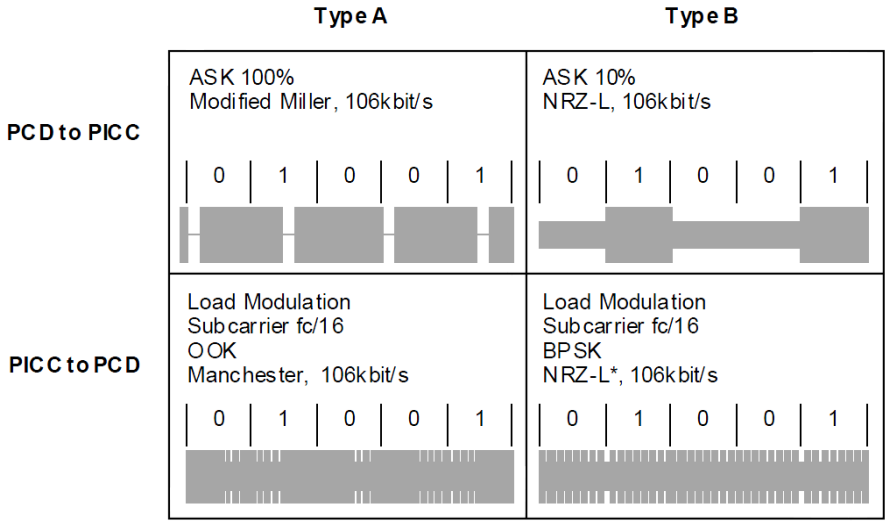

Tabella 2.1: in alto le modulazioni presenti in un collegamento tra Reader e Tag, in basso modulazioni di un Tag che risponde al Reader.

3. **Inizializzazione e Anticollisione.** Ora ci focalizzeremo solo sul protocollo parte B, perché le carte appartenenti all'ISO14443-B sono le più comuni e anche per il fatto che le carte Mifare che vengono trattate nel capitolo 4 appartengono a questo standard.
   Appena la carta entra nella regione di interrogazione di un lettore ed è alimentata, il microprocessore si inizializza:
   - Se la carta è "dual interface" verifica se il modo di funzionamento è a contatto o RF.
   - La carta passa nello stato IDLE e vi rimane finchè non riceve un comando REQB (Request B)
   - Il comando REQB ha un parametro AFI (Application Family Identifier) che specifica il tipo di applicazione e ha un parametro N (dentro PARAM) che specifica il numero di slot disponibili per la risposta (1,2,4,8,16) (Protocollo Aloha Slotted)
   - La carta controlla che l'AFI ricevuto nel REQB corrisponda al proprio. Se sì e se N>1 estrae a caso un numero M tra 1 e N.
   - La carta allo slot M trasmette il comando ATQB, che contiene: il numero seriale o un numero random di 4 byte che fa da numero seriale per la sessione (PUPI), il Protocol Info e l'Application Data.
   - Appena il lettore riceve un ATQB senza collisioni può selezionare la carta, inviando il comando ATTRIB, che contiene l'identificativo della carta, altri parametri della comunicazione (Param) e il primo comando dell'applicazione.
   - Struttura della trama degli altri comandi dell'applicazione.

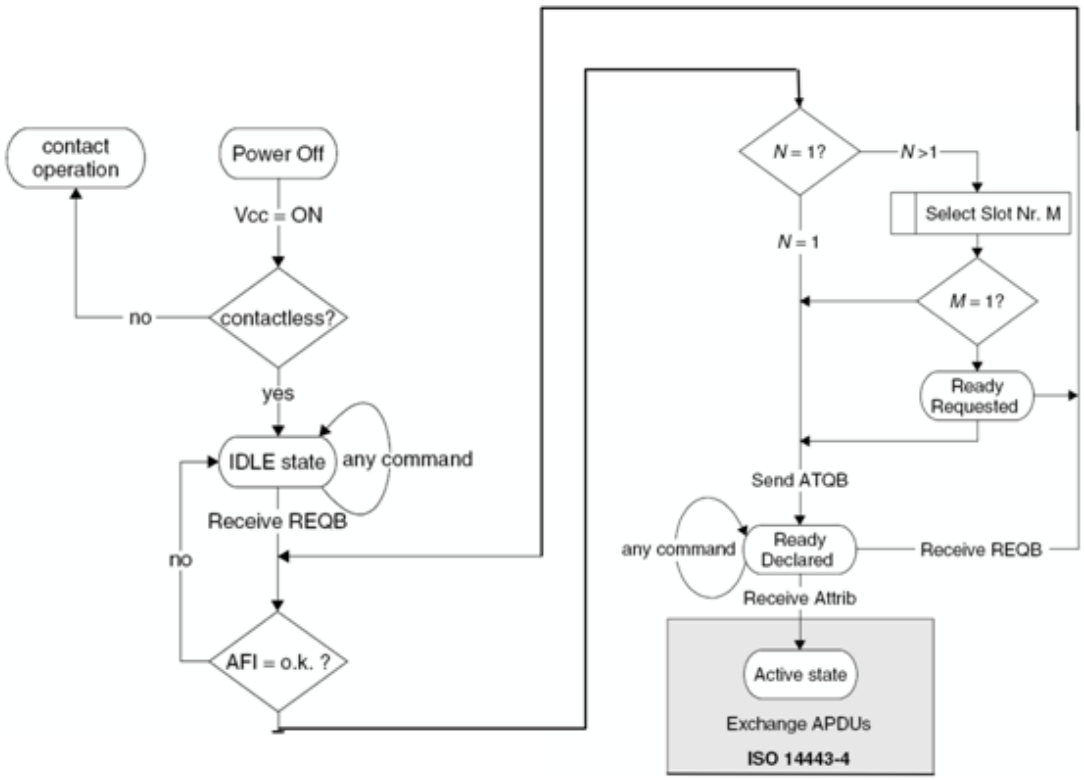

Figura 2.13: diagramma a stati della parte 3 del protocollo ISO14443 di tipo B.

4. **Protocollo di Trasmissione.** La comunicazione lettore-carta segue la struttura master-slave, ovvero la carta si pone in attesa di un comando dal lettore, conseguentemente la carta esegue l'istruzione e risponde al lettore. Per le carte di tipo A è necessario che dopo il protocollo anticollisione siano trasferite alcune informazioni dalla carta al lettore, mentre nelle carte di tipo B queste informazioni sono passate con il comando ATQB. Inizializzazione del protocollo (tipo B):
   - La carta risponde con il comando ATS (Answer To Select) che possiede informazioni per la definizione del protocollo.
   - Il lettore invia il PPS (Protocol Parameter Selection), in cui specifica il baud rate per uplink e downlink.

2.6.1 MIFARE

Mifare è una tecnologia proprietaria brevettata da NXP Semiconductors basata sullo standard ISO 14443-A (non tutte le tessere Mifare lo implementano per intero). Esse sono dispositivi di memoria forniti di un identificatore univoco con un certo livello di sicurezza che varia da modello a modello. La tecnologia proprietaria Mifare è

implementata nelle Smart Card quanto nei lettori, quindi, se si vuole lavorare con tutta la tecnologia, bisognerà realizzare un ricevitore coerente con questa.

2.6.2 MIFARE CLASSIC

Le più comuni carte Mifare, sono le Mifare Classic che sono implementate con circuiti integrati ed hanno scarsa potenza di calcolo, infatti sono per lo più utilizzate come dispositivi di memoria, ove lo spazio è diviso in segmenti e blocchi protetti da semplici meccanismi di controllo degli accessi. Esistono diverse Mifare Classic, che si distinguono tra loro, per la memoria. Ad esempio, le Mifare Classic 1k dispongono di 1024 byte di memoria suddivisi in 16 blocchi. Ogni settore è protetto da due chiavi che vengono chiamate A e B, 16 byte sono riservati alle chiavi e alle condizioni di accesso e non possono essere utilizzati per i dati utente; mentre 16 byte della tessera contengono il numero di serie univoco e altri dati riguardanti il produttore. Ovviamente questi dati sono di sola lettura. Alla stessa famiglia appartengono anche la MIFARE Classic 2k e 4k, che forniscono un maggior memoria ai dati utenti.

La particolarità è che queste tessere utilizzano le prime 3 parti dello standard ISO 14443, mentre un protocollo proprietario sostituisce la quarta parte: trasmissione dati. L'esistenza di un protocollo proprietario non permette in alcun modo l'accesso tramite lettori e funzioni standard del protocollo ISO-14443 [6].

CAPITOLO 3

NEAR FIELD COMMUNICATION-NFC

Figura 3.1: raffigurazione dell'N-Mark il simbolo registrato dall'NFC Forum che permette agli utenti di identificare con facilità i dispositivi abilitati all'NFC. [19]

La Near Field Communication, che in italiano significa letteralmente comunicazione di prossimità, è una tecnologia di comunicazione wireless bidirezionale a corto raggio. L'NFC rappresenta una ridefinizione e un'evoluzione della tecnologia RFID. E' pensata per il trasferimento di piccole quantità di dati, l'obbiettivo è dotare i dispositivi di un tipo di comunicazione wireless semplice e veloce da realizzare, che serva da ponte a servizi già esistenti o che permetta la realizzazione di un nuovo tipo di servizi. La ridefinizione consiste nel fatto che i dispositivi che utilizzano l'NFC non sono dei dispositivi a se stanti, bensì l'NFC viene abilitato nel dispositivo più comune al mondo: il telefono cellulare.

L'NFC è stata sviluppata grazie alla cooperazione di una serie di aziende che, unendosi con l'obbiettivo di promuovere e migliorare la tecnologia, hanno dato vita nel 2004 all'NFC Forum che ad oggi conta più di cento membri tra grandi e piccole aziende quali Philips, Sony, Samsung, Nokia, Visa, Mastercard. L'NFC forum si prefigge l'obbiettivo di standardizzare i protocolli dati e di tracciare le linee guida che gli sviluppatori devono seguire per le loro applicazioni al fine di garantire la massima interoperabilità tra sistemi e dispositivi realizzati dai vari produttori. In particolare secondo le direttive rilasciate dal forum, un sistema NFC dovrà [16]:

- Permettere la comunicazione tra due dispositivi posti a breve distanza, considerando un range di comunicazione massimo di 10 cm.
- Integrare la tecnologia in dispositivi attivi che possano operare sia in modalità Tag, sia in modalità Reader, come avviene negli smartphone.
- Avere queste specifiche fisiche: lavorare alle frequenze operative di 13,56 Mhz con una larghezza di banda di 2 MHz, effettuare connessioni ad un bit rate moderato, in generale 424 Kbit/s e supportare il trasferimento dati a 106, 212, 424 o 848 Kbit/s, infine effettuare il trasferimento dati utilizzando la codifica Miller con modulazione al 100% e la codifica Manchester con modulazione al 10%.
- Garantire la compatibilità con le carte ISO/IEC 14443 e opzionalmente con il protocollo ISO/IEC 15693.

3.1 DIFFERENZE E AFFINITA' TRA NFC E RFID

Nel capitolo 2 si è svolta una panoramica sul background tecnologico dell'NFC. Ora si vogliono elencare le differenze e le analogie tra RFID e NFC [15]:

- RFID e NFC sono tecnologie wireless che operano entrambe con una modalità di comunicazione attiva o passiva dal punto di vista dell'alimentazione energetica per permettere lo scambio di dati tra dispositivi elettronici.
- La tecnologia RFID si avvale della trasmissione dei dati attraverso accoppiamento elettromagnetico. Mentre nel caso NFC, gli applicativi funzionano sempre nel cosiddetto campo vicino dove avviene solo accoppiamento induttivo.
- Come si è discusso nella sezione 2.3, i sistemi RFID utilizzano un ampio spettro di frequenza radio, queste variano in base alle applicazioni, ai Tag utilizzati e in base alle varie regolamentazioni nazionali. L'NFC invece permette la comunicazione solamente alla frequenza radio di 13,56 MHz.
- L'RFID può operare su distanze di alcune decine di metri, risultando inadatto per applicazioni che richiedono un elevata sicurezza. L'NFC è studiata per comunicazioni che arrivino a distanze di 10cm, mentre succede nella pratica che le distanze di impiego siano inferiori.
- I Tag RFID possono essere sia attivi che passivi, in ambito NFC non esiste questa distinzione. Nella tecnologia NFC esistono solo Tag passivi e Reader, che possono essere contenuti in un unico dispositivo come ad esempio uno smartphone. Per quanto riguarda i Tag passivi, questi sono molto simili nelle due tecnologie, basti pensare all'interoperabilità dei Tag che adottano il protocollo di comunicazione ISO 14443 [15].

3.1.1 LE TRE MODALITA' DELL'NFC

Una delle differenze più significative rispetto all'RFID sono le tre modalità in cui può funzionare l'NFC. L'RFID lavora in modalità Reader\Writer, mentre l'NFC aggiunge due modi d'uso: la modalità *peer-to-peer* e la modalità *card emulation*.

- La modalità di comunicazione Reader/Writer è quella che permette ad un dispositivo abilitato NFC di leggere e scrivere un Tag passivo.
- La card emulation mode è quella modalità che permette ad un dispositivo di emulare un Tag NFC. Gli standard che possono essere emulati dallo smartphone sono l'ISO 14443-A, l'ISO 14443-B e infine lo standard Felica, realizzato dalla Sony. La particolarità di questo tipo di funzionamento è che lo smartphone si comporta come un componente passivo. [21]
- Terza modalità di utilizzo è il peer-to-peer: questo è un tipo di comunicazione bidirezionale che avviene tra due dispositivi o smartphone abilitati all'NFC. Quindi in maniera alternata ogni dispositivo si comporterà da Reader e poi da Tag.

3.2 ASPETTI INNOVATIVI

L'NFC, oltre ad avere diverse analogie con l'RFID, racchiude una serie di innovazioni. Per descriverle, si sfrutta il contributo di due ingegneri del Team di Android, Jeff Hamilton e Nick Pelly. I due ingegneri hanno introdotto la tecnologia nella conferenza "How to NFC" tenutasi a San Francisco il 10 maggio 2011. Questi sviluppatori evidenziano le 3 caratteristiche principali dell'NFC.

3.2.1 SHORT RANGE E LOW SPEED WIRELESS TECHNOLOGY

Per Hamilton e Pelly l'NFC è una tecnologia di comunicazione wireless a corto raggio simile al Bluetooth e al WIFI ma che si differenzia da queste sostanzialmente per la distanza alla quale avviene la comunicazione, Bluetooth e WIFI hanno distanze operative molto maggiori. L'NFC inoltre utilizza un basso baud-rate che varia tra i 106 e i 424 Kbps. Per quanto riguarda il network, Bluetooth e WIFI generano una wireless personal area network (WPAN) all'interno della quale possono comunicare più dispositivi contemporaneamente e può arrivare a fino ad una decina di metri; mentre l'NFC non crea una rete bensì instaura comunicazioni punto-punto tra due dispositivi alla volta.

3.2.2 LOW FRICTION SET-UP

Verrebbe dunque spontaneo chiedersi perché si dovrebbe utilizzare l'NFC, Pelly e Hamilton rispondono alla domanda introducendo il concetto di low friction set-up: in

modalità peer-to-peer, lo scambio di dati tra due dispositivi abilitati alla tecnologia è pressoché istantaneo, non è necessario ricercare il dispositivo con cui connettersi come avviene sia nelle comunicazioni Bluetooth e WIFI. Inoltre non è necessario aspettare il pairing che avviene nell'ambito Bluetooth e non sono necessarie password per attivare la comunicazione. Quello che attiva la comunicazione è un movimento fisico, qualcosa di veramente innovativo Pelly definisce un "bridging" tra il mondo fisico e il mondo virtuale; cioè dalla naturalezza di avvicinare due dispositivi scaturisce l'inizializzazione dello scambio dati. Sempre per quanto riguarda il peer-to-peer, l'NFC può supportare la comunicazione WIFI e Bluetooth nell'abbassare la loro high friction set-up: in questo senso si instaura un collegamento NFC tra due dispositivi attivi abilitati permettendo il pairing nel caso del Bluetooth o la connessione WIFI istantanea senza ricerca. Questa metodologia è già stata sviluppata nel mondo dei giochi multiplayer del settore degli smartphone, pioniere in questo campo è stato il famoso gioco "Fruit Ninja". In questo caso gli sviluppatori hanno fatto in modo che fosse sufficiente avviare il gioco in modo che raggiunga la schermata iniziale, poi avvicinando i due dispositivi, questi si scambino le informazioni riguardanti il Bluetooth tramite NFC, così in pochi secondi è possibile instaurare una partita multiplayer [15].

3.2.3 MODALITA' DI FUNZIONAMENTO

La modalità Reader\Writer rappresenta un ulteriore motivo della forza di questa tecnologia, permette di leggere Tag o circuiti integrati nella forma di stickers che sono applicabili su una gran varietà di oggetti anche di piccole dimensioni [20]. Se ad esempio si utilizza uno smartphone che utilizza un sistema operativo Android, come Gingerbread, la lettura sarà pressoché istantanea: si avvicina lo smartphone abilitato NFC al Tag che si vuole interrogare, e senza alcun lancio di programmi di lettura, sullo schermo del cellulare comparirà l'effettivo contenuto del Tag. Per fare un paragone, la lettura di un Tag NFC è molto simile alla lettura di un QR CODE, ma con alcune differenze: la lettura di un QR CODE necessita il lancio di un applicazione dedicata come ad esempio "BARCODE Reader" che a loro volta inizializzano la fotocamera, successivamente l'utente deve fotografare il bersaglio, e poi il programma elaborerà lo schema e risponderà finalmente con le informazioni contenute nello sticker. Il QR Code presenta altri difetti: può risultare inutilizzabile nel caso in cui vi sia scarsa luminosità e nel caso avvenga un deterioramento o un imbrattatura della superficie.

Figura 3.2: QR Code codificati con l'url: http://www.ingegneriarchitettura.unibo.it in figura a) il QR Code originale, in figura b) esempio di QR Code non leggibile a causa della superficie rovinata, in figura c) QR Code compromesso a causa di una macchia.

Da questo si capisce come sia notevolmente più efficiente la tecnologia NFC, inoltre la tecnologia QR Code può contenere al massimo 1kbyte di informazioni mentre con l'NFC si possono raggiungere fino ad 8kb, senza contare il fatto che la tecnologia è ancora in fase di sviluppo [20].
E' di grande importanza anche il funzionamento card emulation: questa modalità permette agli smartphone di essere utilizzati come Smart Card, quindi permette di emulare un Tag nel quale salvare informazioni che, opportunamente codificate, possono trasformare il telefono cellulare ad esempio in una carta di credito, in un badge o in un biglietto elettronico per la metro [21]. Tutto ciò fa intuire che l'NFC non è un'innovazione fine a se stessa, ma una evoluzione che permetterà di migliorare e ampliare lo scambio di informazioni tra una varietà sempre maggiore di dispositivi.

3.3 PROTOCOLLI DI COMUNICAZIONE

L'NFC utilizza una serie di standard di comunicazione realizzati in modo identico da ECMA e ISO. In questi protocolli di comunicazione sono presenti anche specifiche di compatibilità per i dispositivi RFID. Sono presenti anche alcuni protocolli di incapsulamento dati che definiscono il tipo e la struttura dei dati.

3.3.1 NFCIP-1

ECMA 340 e ISO\IEC 18092 definiscono le specifiche di comunicazione per l'NFC Interface and Protocol 1 (NFCIP-1). Gli standard indicano da una parte le caratteristiche della modalità attiva, ovvero quelle del Reader che inizia la trasmissione; dall'altra indicano le caratteristiche in modalità passiva, cioè quelle di un Tag che deve rispondere

al Reader. ECMA 340 ed ISO\IEC 18092 definiscono per ogni modalità: schemi di modulazione, le codifiche, le velocità di trasmissione, i formati delle trame dell'interfaccia a radio frequenza, gli schemi di inizializzazione e anticollisione e i protocolli di trasporto [26].

3.3.2 NFCIP-2

ECMA 352 e ISO\IEC 21481 definiscono l'NFC Interface and Protocol 2 (NFCIP-2). Questo standard specifica il meccanismo di selezione dei protocolli funzionanti alla frequenza di 13,56 MHz.

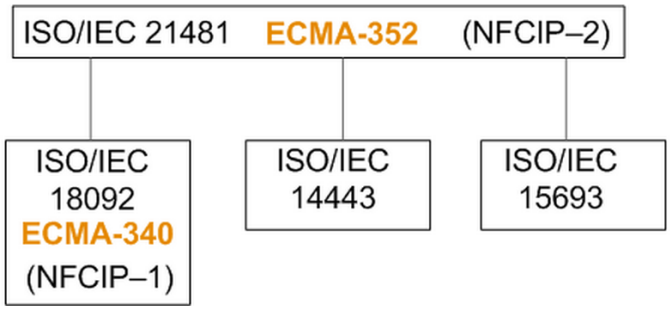

Figura 3.3: schema gerarchico dei protocolli NFC.

Questo protocollo prevede che i dispositivi possano comunicare utilizzando l'NFCIP-1, oppure gli standard ISO\IEC 14443 e ISO\IEC 15693. Questo protocollo permette all'NFC di essere molto elastico permettendo di supportare anche la carte di vicinità e di prossimità della tecnologia RFID.

Lo standard NFCIP-2, oltre al protocollo, distinguerà anche se il dispositivo lavora in modalità attiva (Initiator) o in modalità passiva (Target). Per scegliere il tipo di funzionamento del dispositivo, il protocollo esegue la seguente sequenza [27].

1. Il dispositivo deve annullare il proprio campo magnetico.
2. Se è selezionata la modalità PICC, allora il dispositivo comincia a lavorare in modalità PICC.
3. Se il dispositivo individua un campo magnetico esterno con specifiche contenute nel protocollo ECMA 340, il dispositivo entra in modalità NFC come Target.
4. Se il dispositivo non individua il campo magnetico esterno ed è selezionata la mdalità NFC, allora il dispositivo entra in modalità NFC come Initiator.
5. Se il dispositivo non individua il campo magnetico esterno ed è selezionata la modalità PCD o la modalità VCD, si aspetterà un tempo definito sempre nell'ECMA 340 per ciascuna modalità, se il periodo non viene rispettato il dispositivo ricomincia la sequenza, altrimenti viene confermata la modalità di funzionamento.

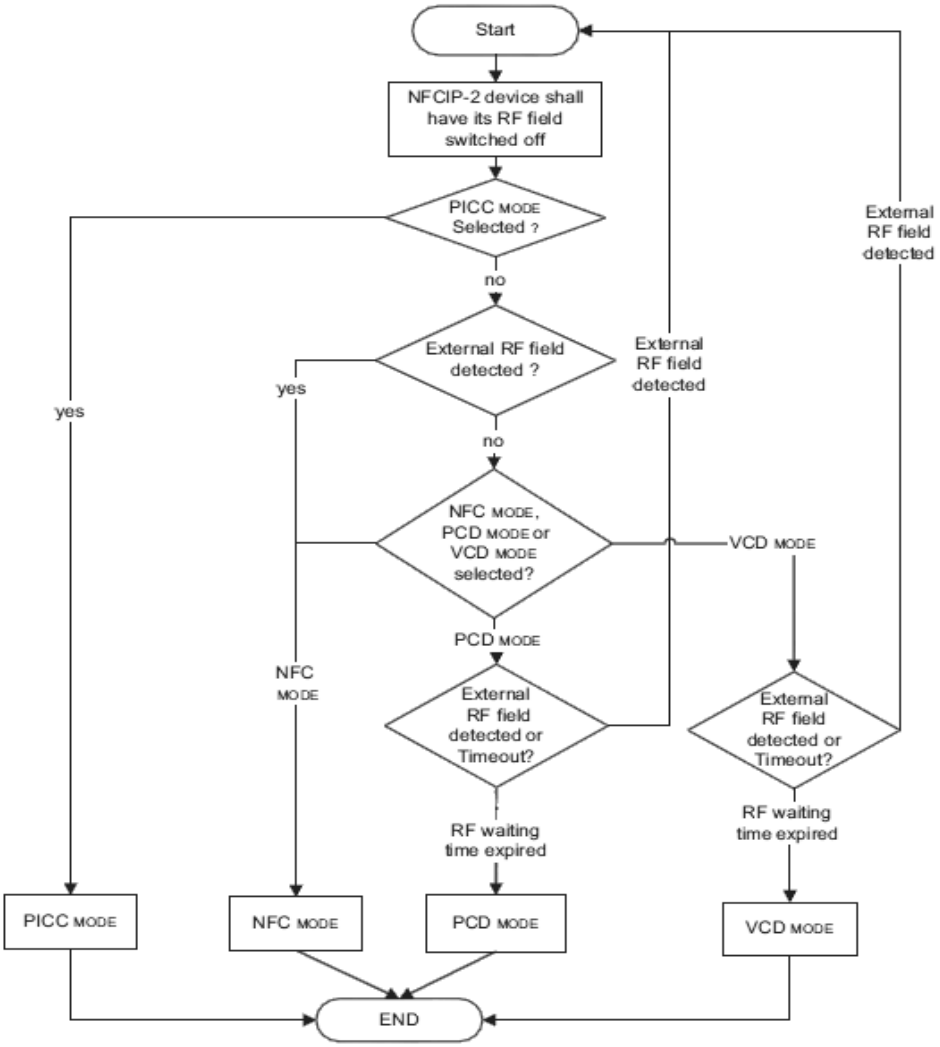

Figura 3.4: diagrammi a stati del protocollo NFCIP-2

3.3.3 PROTOCOLLO DI INCAPSULAMENTO DATI

L'NFC Forum ha inoltre rilasciato una serie di specifiche riguardanti il formato dei dati, che non compaiono nei protocolli di comunicazione ISO ed ECMA. La più importante è l'NFC Data Exchange Format (NDEF). Consiste in un formato di incapsulamento dei dati, per lo scambio di informazioni tra dispositivi e Tag aderenti all'NFC Forum. Questo protocollo definisce la struttura dell'incapsulamento delle informazioni e il meccanismo per specificare le applicazioni relative ai dati contenute nel messaggio NDEF, mentre non definisce il tipo delle informazioni. L'NDEF quindi incapsula una serie di informazioni di qualsiasi tipo che siano riferite ad applicazioni definite. Nella sezione 3.4 si spiegherà dettagliatamente questo protocollo, perché sarà di importanza primaria nella sperimentazione [23].

3.4 NFC DATA EXCHANGE FORMAT - NDEF

Il protocollo NFC Data Exchange Format (NDEF) descrive il formato per l'incapsulamento delle informazioni all'interno dei messaggi scambiati dai dispositivi NFC. Esso è basato sul concetto di messaggio "leggero", permettendo di incapsulare qualsiasi tipo di informazione nella forma di record, come spesso avviene nella maggior parte dei protocolli di incapsulamento [16]. Ogni messaggio NDEF è il costrutto fondamentale definito dalla specifica NDEF, che deve essere scambiato in modalità *read* o *peer-to-peer* [23]. E' composto di uno o più record NDEF come si vede in figura 3.2.

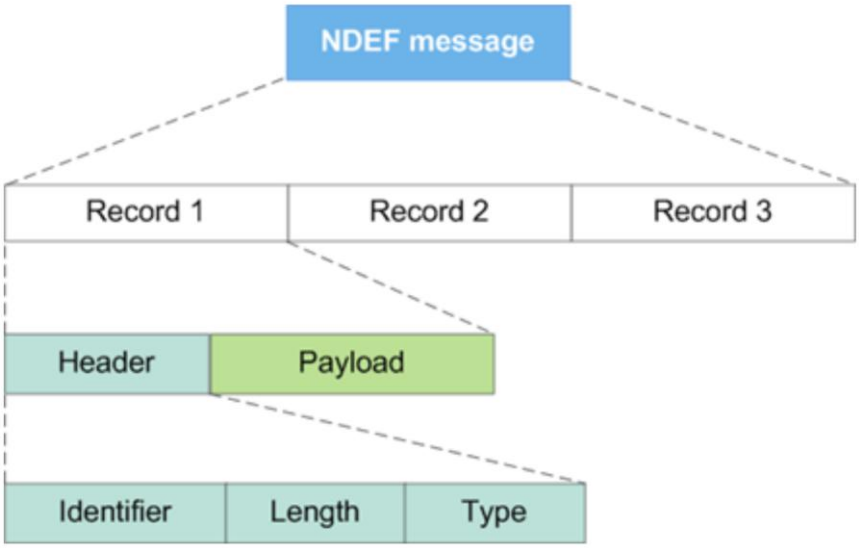

Figura 3.5: composizione di un messaggio NDEF.

3.4.1 RECORD NDEF: STRUTTURA E CONCATENAMENTO.

I Record NDEF rappresentano l'informazione elementare di un messaggio NDEF. Infatti come spesso avviene nei protocolli di incapsulamento, i dati vengono distribuiti su più record collegati tra loro. Si utilizza questo concatenamento di record per trasportare una maggiore quantità di informazioni all'interno di un messaggio NDEF. I Record sono formati da due parti: un Header che contiene specifiche di stato sulla composizione del record e un Payload che rappresenta l'informazione effettiva che si vuole inviare.

7	6	5	4	3	2	1	0	Bit
MB	ME	CF	SR	IL	TNF			HEADER
TYPE LENGTH								
PAYLOAD LENGTH 3								
PAYLOAD LENGTH 2								
PAYLOAD LENGTH 1								
PAYLOAD LENGTH 0								
ID LENGTH								
TYPE								
ID								
PAYLOAD … … … … … …								PAYLOAD

Figura 3.6: struttura di un Record NDEF

L'HEADER è formato da un numero di byte variabile che può essere 4,6 e 9; si compone di:

1. Un byte che contiene i flag di stato del record NDEF:
   - MB: flag Message Begin, che indica il record del primo messaggio
   - ME: flag Message End, che ne indica la fine.

NDEF Message						
R_1 MB=1	…	R_r	…	R_s	…	R_t ME=1

Figura 3.7: schematizzazione di messaggio NDEF dove si mostrano i flag Message Begin e Message End.

   - CF: Chunk Flag, indica il record facente parte di una catena di record, se il suo valore fosse 1 allora vorrebbe dire che ci sarebbe almeno un altro record nella catena. Nel caso in cui il flag non è settato, allora si tratterà di un Record singolo oppure dell'ultimo elemento di una catena. Si noti che CF e ME non possono essere entrambi settati.

Messaggio NDEF				
R1 MB = 1 ME = 0 CF = 0	R(k-1) MB = 0 ME = 0 CF = 1	Rk MB = 0 ME = 0 CF = 1	R(k+i) MB = 0 ME = 0 CF = 0	Rn MB = 0 ME = 1 CF = 0
Record singolo	Record concatenati			Record singolo

Figura 3.8: esempio di messaggio NDEF composto di un concatenamento di Record. Ogni blocchetto rappresenta un Record NDEF, dove viene rappresentato il numero del record, e rispettivamente i flag Message Begin, Message End e Chunk Flag [16].

   - SR: flag Short Record, se settato indica che il record corrente è di tipo short e quindi la PAYLOAD LENGTH sarà espressa da un singolo byte. In caso contrario la PAYLOAD LENGTH sarà di 4 byte.

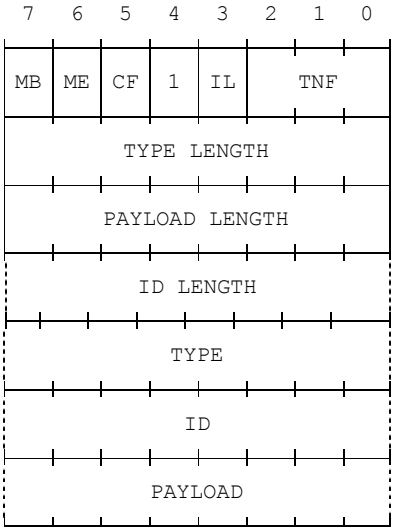

Figura 3.9: struttura di uno short record NDEF (SR=1) [23].

- IL: flag ID_Length indica se nel record è presente un Identificatore. Questo flag, se non è abilitato, significa che non sono presenti né il campo Lunghezza identificativo record (ID Length) né il campo identificativo Record (ID).
- TNF: Type Name Format, indica la struttura del campo Type. Esso è composto di tre bit e può assumere valori che vanno da 0 a 6, il 7 è riservato.

Valore	Descrizione	Tipi Accettati
0	Empty; il record vuoto. Non contiene dati, è utile per i record di chiusura	
1	Internal Type; i tipi definiti dall'NFC Forum. Indica che il tipo utilizzato è stato definito dall'NFC Forum (RTD)	Tutti quelli definti dall'NFC Forum
2	Media-Type; indica un tipo di dati multimediale definito nell'RFC 2046	Image/jpeg message/http
3	Absolute URI; indica un tipo di dati e una risorsa URI definita nell'RFC 3986	"Identificazione Uniforme di Risorsa", un percorso web, un IPV6 o IPV4
4	External Type; tipi definiti dall'NFC Forum per i tipi di dati esterni allo standard NFC RTD	
5	Sconosciuto, ovvero non definito dall'NFC Forum	
6	Uguale al precedente utilizzato per i record concatenati successivi al primo	
7	Riservato ad usi futuri, se utilizzato il PARSER lo tratterà come tipo sconosciuto.	

Tabella 3.1: possibili valori dl campo TNF [16].

2. Un byte che individua il campo TYPE_LENGTH: esso indica la lunghezza in byte del campo TYPE.
3. Un byte individua il campo ID_LENGTH: esso indica la lunghezza in byte del campo ID. Tale campo è presente se il flag ID_LENGTH (IL) è settato, altrimenti non vi sarà il campo ID.

4. Generalmente 4 byte. Nel caso SR sia settato, il campo è formato da un byte. Questi byte individuano il campo PAYLOAD_LENGTH, che indica la lunghezza in byte del campo PAYLOAD. Se si hanno 4 byte, si leggeranno i byte con la convenzione Most Significant Bit first.
5. Un byte serve ad individuare il campo TYPE o PAYLOAD_TYPE che specifica il tipo di dato trasportato. Il suo valore segue le specifiche imposte dal campo TNF. Un PARSER NDEF, ovvero il modulo che decodifica i messaggi NDEF, quando riceve un record con un valore corretto di TNF ma un TYPE errato dovrebbe segnalare errore.
6. Un byte che individua il campo ID, cioè il PAYLOAD_IDENTIFIER che rappresenta un identificativo unico del record espresso sotto forma di URI. L'URI è l'acronimo di Uniform Resource Identifier ed è una stringa utilizzata anche in altri ambiti per identificare univocamente una risorsa generica. Nel caso di record concatenati l'ID sarà presente solo nel primo record e sarà settato a zero nei successivi.

Una particolarità interessante per quanto riguarda la pratica con dispositivi NFC è che i campi all'interno del messaggio vengono ordinati con lo stesso ordine con cui sono stati inseriti. Quindi le informazioni saranno passate dal PARSER alle rispettive applicazioni secondo l'ordine di inserimento [16].

3.4.2 Tipologie di record – RTD (Record Type Definition)

L'NFC Forum distingue le tipologie dei record in due macro famiglie: NFC Forum Well-known Type e NFC Forum External Type. I primi rappresentano le tipologie pensate per essere salvate sui Tag; mentre la seconda categoria è composta da tipi di risorse utilizzati per altri scopi. Da questo punto in poi, per rispettare la terminologia utilizzata nell'NFC Forum, le tipologie verranno chiamate Type. Focalizzando l'attenzione sui Type che vengono memorizzati nei Tag, si fornirà una descrizione dei Well-known Type. Questa categoria è composta da 4 Type: Text RTD, Signature RTD, URI RTD, Smart Poster RTD [21].

1. **Text RTD.** E' il più comune dei record Type, contiene testo in chiaro e può essere utilizzato per una descrizione degli oggetti o per dei servizi connessi ai Tag NFC, ad esempio per descrivere una risorsa quale può essere un URL, o per altre esigenze. All'interno di un Text Record dovranno essere presenti una serie di informazioni affinché, chi riceve il messaggio di testo, lo possa visualizzare correttamente. In questo senso sarà specificata la lingua utilizzata nel record, e verrà dichiarata la codifica di testo utilizzata per convertire il testo stesso in sequenza di bit per poi sapere come decodificare il messaggio.

Trattando la struttura di un record di testo, si può dire innanzitutto che il valore del TNF è uguale ad 1 poiché i RecordText sono del tipo WKT. Il nome di tale tipo di record è semplicemente "T" (0x54) che, convertita in binario, sarà rappresentato dal valore 01010100. I dati, nel PAYLOAD del record. Il PAYLOAD avrà questo formato:

Offset	Length	Contenuto
0	1	Byte di stato. Un solo bit indicanti il formato di codifica adottato e altri bit per la lunghezza del codice IANA utilizzato per indicare la lingua del testo
1	n	ISO/IANA codice lingua : es. "ita", "en-US"
n+1	m	Il testo codificato a UTF-8 o UTF-16 cosi come indicato nel byte di stato

Tabella 3.2: formato del PAYLOAD di un Record di testo.

Considerando questa struttura avremo pertanto:

- Il byte di stato. Esso contiene informazioni riguardanti il messaggio di testo, come la codifica utilizzata e la lunghezza del codice che identifica la lingua.

Bit Number (0 is LSB)	Indica
7	0 : UTF-8 1 : UTF-16
6	RFU : Riserverd Future Use, posto sempre a 0
5...0	Lunghezza del codice della lingua

Tabella 3.3: spiegazione dei bit di stato

- I byte che rappresentano il codice della lingua possono variare da 2 a 5, a seconda che venga specificato il dialetto ("en-UK", "en-USA", ecc.) o semplicemente la lingua.
- Il resto del PAYLOAD è utilizzato per contenere il testo che si vuole trasferire. Si noti che la lunghezza del testo (m) si ottiene sottraendo alla lunghezza del PAYLOAD la lunghezza del codice della lingua (n). Ora si veda un esempio di testo, in cui si è utilizzato come input: "Hello, World".

Offset	Contenuto	Len		
0		1	IL=0; Nessun ID; MB=1; ME=1; SF=1; Record Short; TNF=0x01	HEADER
1	0x01	1	Lunghezza del Tipo utilizzato (1 Byte)	
2	0x10	1	Lunghezza del Payload (16 Bytes)	
3	"T":0x54	1	Tipo Record Testo	
4	0x02	1	Codifica UTF-8 2 Byte per la lingua	PAYLOAD
5	"en"	2	Lingua del messaggio	
7	"Hello, World"	12	Codifica UTF-8 del testo	

Tabella 3.4: esempio di Record di testo con contenuto "Hello World". [17]

2. **URI RTD.** I record URI (Uniform Resurce Identifier) contengono al loro interno una stringa che definisce in maniera univoca il tipo di risorsa, come ad esempio un indirizzo web, un numero di telefono o fax e così via. E' possibile incapsulare più file URI all'interno di un messaggio NDEF, in modo da mandare una varietà di informazioni completa. A questo punto sarà compito dell'applicazione riuscire a interpretare correttamente i singoli URI. Ora si osservi la struttura del record URI, questo tipo appartiene alla macro categoria Well Known Types, quindi avrà il TNF settato ad 1. Il nome di tale tipo è indicato con "U" (0x55) ed avrà lunghezza di un byte. La struttura del PAYLOAD sarà:

Offset	Lenght	Contenuto
0	1	URI CODE
1	n	URI FIELD

Tabella 3.5: struttura del PAYLOAD di un record URI

L'URI CODE specifica il protocollo per accedere a tale risorsa, e rappresenta il primo byte del PAYLOAD. Per ogni valore compreso tra 0x00 e 0x23 viene utilizzato un particolare protocollo con il suo prefisso che concatenato al valore presente nell'URI FIELD costituisce il percorso completo della risorsa da raggiungere. Il Campo URI fields contiene il nome della risorsa da identificare. Essa sarà convertita utilizzando la codifica UTF-8 in una sequenza di byte che potrà essere poi correttamente visualizzata dal destinatario [16].

In tabella 3.6 si fornisce un esempio di record URI, indicante la risorsa http://www.nfc.com [17].

Offset	Contenuto	Len		
0		1	IL=0; Nessun ID; MB=1; ME=1; SF=1; Record Short; TNF=0x01	HEADER
1	0x01	1	Lunghezza del Tipo utilizzato (1 Byte)	
2	0x08	1	Lunghezza del Payload (10 Bytes)	
3	"U":0x55	1	Tipo Record URI	
4	0x01	1	URI Identifier: "http://www."	PAYLOAD
5	0x6E 0x66 0x63 0x2E 0x63 0x6F 0x6D	9	URI Fields "nfc.com" in UTF-8	

Tabella 3.6: descrizione di record URI, con Uri Field: "nfc.com".

3. **Signature RTD.** Questo Type contiene una signatur (firma digitale) relativa ad uno o più record contenuti all'interno di un messaggio NDEF. La firma digitale può essere utilizzata per verificare l'integrità e l'autenticità dell'intero messaggio NDEF. Il PAYLOAD del Signature Record contiene i seguenti campi [21]:

- Version: dove viene indicata la versione della specifica.
- Signature: dove viene inserita la firma digitale, o un riferimento alla locazione della firma digitale.
- Certificate Chain: un campo opzionale che include informazioni aggiuntive sulla firma.

Signature Record		
Version	Signature	Certificate Chain

Figura 3.10: struttura di un signature Record [28].

4. **Smart Poster RTD.** Rappresenta uno degli utilizzi chiave in tecnologia NFC. L'NFC Forum ha sviluppato questa specifica per lo scambio rapido di informazioni da un Tag verso uno smartphone abilitato. Infatti attraverso l'utilizzo di questo record, lo smartphone abilitato all'NFC, dovrebbe essere subito in grado di scegliere l'applicazione con cui aprire i dati. Per realizzare questa funzionalità i record Smart Poster contengono un record ACTION che permette di aprire, per ogni dato compatibile, un'applicazione contenuta nello smartphone NFC. Quindi ad esempio lo Smart Poster potrebbe lanciare il browser web se il Tag, che si sta leggendo, contiene un indirizzo web [17]. Il concetto di "Smart" indica capacità di rendere interattivo un messaggio NDEF [16]. Quindi lo Smart Poster è un record che viene associato a uno o

più Record URI che a loro volta servono ad identificare un gran numero di informazioni.

Quando all'interno di un messaggio NDEF è presente il Record Smart Poster, questo è specificato nell'Header. Mentre tutti i Record ai quali si vogliono applicare le funzionalità dello Smart Poster sono innestati nel PAYLOAD del Record Smart Poster. Questo Payload è detto anche Master Record.

Quindi in generale all'interno del messaggio si avranno zero, uno o più record tra i seguenti [17]:

- Title Record: indica il titolo del servizio a cui è associato. Può essere in varie lingue, è un record facoltativo.
- Uri Record: indica la risorsa a cui fa riferimento il record. Come detto in precedenza è l'unico record obbligatorio.
- Action Record: indica in che modo dovrà agire il dispositivo remoto sul record. L'Action potrebbe "suggerire" allo smartphone di aprire un browser, di salvare il record, di aprire l'editor sms, tutto ciò in base al valore dell'Action Record. Per i record annidati nel Master Record il Type di tale Record ha il nome "act" (0x61 0x63 0x74) e ha valore locale, ossia per la particolare risorsa riferita in quello Smart Record.

Value	Action
0	Do the action (send the SMS, launch the browser, make the telephone call)
1	Save for later (store the SMS in INBOX, put the URI in a bookmark, save the telephone number in contacts)
2	Open for editing (open an SMS in the SMS editor, open the URI in an URI editor, open the telephone number for editing).
3..FF	RFU

Tabella 3.7: elenco delle possibili "action" di un Smart Poster.

- Icon Record: Uno Smart Poster può associare una o più immagini al record, solo una verrà visualizzata dall'utente. Anche in questo caso il record è opzionale.
- Size Record: indica le dimensioni della risorsa specificata nel record. È un campo utile al dispositivo, che interpretando le dimensioni della risorsa, può decidere se scaricarla o meno [16].
- Type Record: specifica il tipo di oggetto della risorsa, anche in questo caso può essere utile al dispositivo che può sapere come trattarlo [17].

3.4.3 CONFRONTO TRA RECORD URI E SMART POSTER

Si è voluto immagazzinare in un Tag l'url del sito web della Scuola di Ingegneria e Architettura, cioè "http//www.ingegneriarchitettura.unibo.it". Prima nella forma di Record URI in Tabella 3.9 poi in quelle di Smart Poster in Tabella 3.10. Per fare la conversione dell'indirizzo url della facoltà si è utilizzata la conversione esadecimale della codifica UTF-8 (Unicode Transformation Format, 8 bit).

Le differenze tra Record URI e Smart Poster risultano subito evidenti. Nel primo caso, come si vede nella tabella 3.9, ci sono un solo HEADER ed un solo PAYLOAD. L'HEADER descrive la struttura e il tipo di record contenuto, mentre nel PAYLOAD c'è la vera risorsa che si vuole immagazzinare. Nella tabella 3.10 si nota, come si è descritto in precedenza, la presenza di più record e conseguentemente più HEADER e PAYLOAD. Si nota che l'HEADER dello Smart Poster contiene informazioni sulla lunghezza del PAYLOAD e sul tipo contenuto. Il PAYLOAD dello Smart Poster è diviso in due parti: una riferita al Record URI che si è voluto incapsulare all'interno dello Smart Poster, mentre la seconda parte rappresenta l'azione che dovrà compiere il dispositivo che vorrà leggere l'informazione.

OFFSET	CONTENUTO	LEN.	DESCRIZIONE	
0	0xD1	1	IL=0; Nessun ID; MB=1; ME=1; SF=1; Record Short; TNF=0x01	HEADER
1	0x01	1	Lunghezza del Tipo utilizzato (1 Byte)	
2	0x1F	1	Lunghezza del Payload (31 Bytes)	
3	"U":0x55	1	Tipo Record URI	
4	0x01	1	URI Identifier: "http://www."	PAYLOAD
5	0x69 0x6e 0x67 0x65 0x67 0x6e 0x65 0x72 0x69 0x61 0x72 0x63 0x68 0x69 0x74 0x65 0x74 0x74 0x75 0x72 0x61 0x2e 0x75 0x6e 0x69 0x62 0x6f 0x2e 0x69 0x74	30	**URI Fields "ingegneriarchitettura.unibo.it" in uTF-8**	

Tabella 3.9: esempio di un messaggio NDEF composto da un URI Record contenente l'indirizzo web: http://www.ingegneriarchitettura.unibo.it

OFFSET	CONTENUTO	LEN.	DESCRIZIONE		
0	0xD1	1	IL=0; Nessun ID, MB=1,ME=1 SF=1;Record Short TNF=0x01	HEADER	
1	0x02	1	Lunghezza del Tipo utilizzato (2 Byte)		
2	0x2A	1	Lunghezza del Payload (42 Bytes)		
3	"Sp"	2	Tipo Record Smart Poster		
5	0xD1	1	IL=0; Nessun ID, MB=1,ME=1 SF=1;Record Short TNF=0x01	HEADER	PAYLOAD
6	0x01	1	Lunghezza del Tipo utilizzato (1 Byte)		
7	0x1F	1	Lunghezza del Payload (31 Bytes)		
8	"U"	1	Tipo Record URI		
9	0x01	1	URI Identifier: "http://www."	PAYLOAD	
10	0x69 0x6e 0x67 0x65 0x67 0x6e 0x65 0x72 0x69 0x61 0x72 0x63 0x68 0x69 0x74 0x65 0x74 0x74 0x75 0x72 0x61 0x2e 0x75 0x6e 0x69 0x62 0x6f 0x2e 0x69 0x74	30	**URI Fields "ingegneriarchitettura.unibo.it" in uTF-8**		
40	0xD1	1	IL=0; Nessun ID, MB=1,ME=1 SF=1;Record Short TNF=0x01	HEADER	
41	0x03	1	Lunghezza del Tipo utilizzato (1 Byte)		
42	0x01	1	Lunghezza del Payload (1 Byte)		
43	"act"	3	Tipo di Record		
46	0x00	1	Avvia il gestore predefinito. In questo caso il browser web.	PAYLOAD	

Tabella 3.10: esempio di messaggio NDEF Smart Poster. All'interno del messaggio abbiamo 2 Record NDEF, il Record URI di Tabella 3.8 più il record "act".

Binary	Dec	Hex	Graph.	Binary	Dec	Hex	Graph.	Binary	Dec	Hex	Graph.
0010 0000	32	20	(blank)	0100 0000	64	40	@	0110 0000	96	60	`
0010 0001	33	21	!	0100 0001	65	41	A	0110 0001	97	61	a
0010 0010	34	22	"	0100 0010	66	42	B	0110 0010	98	62	b
0010 0011	35	23	#	0100 0011	67	43	C	0110 0011	99	63	c
0010 0100	36	24	$	0100 0100	68	44	D	0110 0100	100	64	d
0010 0101	37	25	%	0100 0101	69	45	E	0110 0101	101	65	e
0010 0110	38	26	&	0100 0110	70	46	F	0110 0110	102	66	f
0010 0111	39	27	'	0100 0111	71	47	G	0110 0111	103	67	g
0010 1000	40	28	(	0100 1000	72	48	H	0110 1000	104	68	h
0010 1001	41	29	)	0100 1001	73	49	I	0110 1001	105	69	i
0010 1010	42	2A	*	0100 1010	74	4A	J	0110 1010	106	6A	j
0010 1011	43	2B	+	0100 1011	75	4B	K	0110 1011	107	6B	k
0010 1100	44	2C	,	0100 1100	76	4C	L	0110 1100	108	6C	l
0010 1101	45	2D	-	0100 1101	77	4D	M	0110 1101	109	6D	m
0010 1110	46	2E	.	0100 1110	78	4E	N	0110 1110	110	6E	n
0010 1111	47	2F	/	0100 1111	79	4F	O	0110 1111	111	6F	o
0011 0000	48	30	0	0101 0000	80	50	P	0111 0000	112	70	p
0011 0001	49	31	1	0101 0001	81	51	Q	0111 0001	113	71	q
0011 0010	50	32	2	0101 0010	82	52	R	0111 0010	114	72	r
0011 0011	51	33	3	0101 0011	83	53	S	0111 0011	115	73	s
0011 0100	52	34	4	0101 0100	84	54	T	0111 0100	116	74	t
0011 0101	53	35	5	0101 0101	85	55	U	0111 0101	117	75	u
0011 0110	54	36	6	0101 0110	86	56	V	0111 0110	118	76	v
0011 0111	55	37	7	0101 0111	87	57	W	0111 0111	119	77	w
0011 1000	56	38	8	0101 1000	88	58	X	0111 1000	120	78	x
0011 1001	57	39	9	0101 1001	89	59	Y	0111 1001	121	79	y
0011 1010	58	3A	:	0101 1010	90	5A	Z	0111 1010	122	7A	z
0011 1011	59	3B	;	0101 1011	91	5B	[	0111 1011	123	7B	{
0011 1100	60	3C	<	0101 1100	92	5C	\	0111 1100	124	7C	|
0011 1101	61	3D	=	0101 1101	93	5D	]	0111 1101	125	7D	}
0011 1110	62	3E	>	0101 1110	94	5E	^	0111 1110	126	7E	~
0011 1111	63	3F	?	0101 1111	95	5F	_				

Tabella 3.8: tabella di conversione per codifica UTF-8

3.5 PROGETTI ED UTILIZZI

La tecnologia NFC offre il vantaggio di essere molto versatile, in quanto può essere sfruttatata per vari scopi. Molte aziende provenienti da differenti campi industriali e commerciali hanno unito i loro sforzi per dare vita a programmi pilota per lo sviluppo di applicazioni sempre differenti. Ora si citeranno alcuni progetti negli ambiti più comuni di sviluppo.

3.5.1 TICKETING

Uno degli scenari di impiego dell'NFC è sicuramente la bigliettazione elettronica. Questa funzionalità prevede l'utilizzo dello smartphone in modalità Card Emulation, così da emulare il biglietto del trasporto pubblico. In questo modo si può risparmiare carta, rendere obsoleto il sistema di obliterazione, evitare che il consumatore possa perdere il biglietto e infine il Reader elettronico sarà meno sottoposto agli agenti atmosferici poiché sarà all'interno di un package.

Un progetto pilota sulla bigliettazione è stato realizzato dalla RMV (Rhein-Main-Verkehrsverbund), che è una delle maggiori compagnie di trasporto locale in Europa e serve 5 milioni di abitanti. La RMV insieme a Nokia, Vodafone e l'autorità dei trasporti di Francoforte, hanno dato il via ad un esperimento che è iniziato nel 2005 con 200 utenti. In questo esperimento gli utenti della RMV hanno usato il Nokia 3220, una dei primi cellulari a dotare l'NFC, mentre le informazioni sui biglietti dei clienti erano contenuti in una Smart Card integrata all'interno del cellulare.

Figura 3.11: Uso del Nokia 3220 come biglietto elettronico all'interno di un autobus.

A fine progetto la società tedesca ha svolto un sondaggio rivolto ai partecipanti dell'iniziativa ed in generale l'uso del cellulare al posto delle Smart Card è risultato di grande interesse. Nel progetto pilota della RMV sono state introdotte anche altre applicazioni, ad esempio programmi di fedeltà e metodi per effettuare il pagamento sempre tramite NFC [21].

A Manchester, la società di telecomunicazioni Orange UK, ha lanciato un esperimento sul servizio di bigliettazione in collaborazione con la società sportiva Manchester City Football Club. Il progetto è stato lanciato nell'agosto del 2006 ed ha coinvolto 20 abbonati della società a cui è stato fornito un Nokia 3220. Questi 20 tifosi avvicinando il loro dispositivo al Reader presente ai tornelli venivano riconosciuti dal sistema, ed entravano allo stadio, guadagnando tempo e senza dover mostrare documenti di riconoscimento al personale della sicurezza [21]. Un esperimento simile è stato realizzato anche in Olanda dalla società Roda JC Football Club, in questo caso le persone coinvolte erano 50. La differenza è che i tifosi del Roda potevano utilizzare il loro cellulare come carta di credito nei bar e nei negozi all'interno dello stadio [24].

Uno dei progetti più importanti e forse quello che avrà gli sviluppi più importanti è quello condotto dalla società telefonica O2. Questa ha lanciato il progetto "O2 wallet" nel 2007 in collaborazione della società dei trasporti Londinese Oyster, Nokia, Innovision NXP, Barclaycard e Visa. Questo progetto prevede l'utilizzo di un Nokia 6131 da parte di 500 utenti, i quali hanno utilizzato il loro dispositivo NFC come carta di viaggio nella metropolitana e nei bus di Londra, semplicemente avvicinando il cellulare ai Reader presenti alle stazioni e nei bus.

3.5.2 MOBILE PAYMENT

L'obbiettivo del Mobile Payment è l'utilizzo del cellulare nei pagamenti elettronici al posto delle carte di credito magnetiche. In questo caso il cellulare lavora in modalità Card Emulation in modo che possa essere letto da un POS (Point Of Sale) o da un distributore automatico abilitato all'NFC [15].

Nella sezione 3.5.1 si è parlato del progetto "O2 wallet". All'interno di questa iniziativa, la collaborazione di Visa e Barclaycard ha permesso di usare gli stessi dispositivi all'interno di oltre 500 esercizi, sostituendo le rispettive carte di credito con il dispositivo fornito dalla Nokia. Dai sondaggi e dalle interviste ai partecipanti si capisce l'impatto favorevole dell'NFC sui consumatori, questo ha convinto la O2 a sviluppare ulteriori servizi preparando così il lancio commerciale dell'O2 wallet [21].

Un esperimento di Mobile Payment è stato condotto dal gruppo bancario HBSC in collaborazione con Mastercard nel 2007 negli Stati Uniti. Il pagamento veniva garantito dove veniva accettato il servizio Mastercard PayPass. Ben 36000 commercianti disponevano di tale servizio, ed oltre 200 agenzie del gruppo HBSC tra New York e Chicago hanno permesso agli utenti di trasferire le informazioni delle proprie carte di credito sul dispositivo NFC.

Figura 3.12: pagamento attraverso un POS abilitato NFC.

Payez Mobile è un'iniziativa lanciata nel 2007 che ha coinvolto 500 partecipanti tra Caen e Strasburgo. In questo progetto hanno partecipato 5 compagnie di telecomunicazioni, 8 gruppi bancari e infine Mastercard e Visa. L'importanza di questo progetto è che i vari partner hanno cercato di standardizzare il processo del Mobile Payment, creando una sola applicazione che fosse compatibile con i vari gruppi bancari, creare un solo protocollo presso gli esercizi abilitati, ed usare più dispositivi NFC. Payez Mobile ha anche definito i metodi di pagamento, ad esempio se l'importo è inferiore ai 20 euro, sarà sufficiente avvicinare il cellulare al POS per completare la transazione, mentre per importi superiori sarà necessario digitare un PIN [21].

3.5.3 SMART POSTER

Il cellulare in questo caso funziona in modalità Reader e avvicinandolo ad uno Smart Poster localizzato presso un punto vendita è possibile ottenere informazioni sui prodotti che si desidera acquistare e scaricare sul proprio smartphone i coupon di sconto o eventuali carte di fidelizzazione. Gli Smart Poster possono essere anche utilizzati per fornire informazioni differenti da quelle necessarie per un acquisto: si potrebbe scaricare da questi sul proprio dispositivo la tabella degli orari presso la fermata dell'autobus oppure ottenere informazioni sulle opere esposte presso un museo [15].

Figura 3.13: sulla sinistra esempio di Smart Poster, utilizzato al London Museum.

Una speciale applicazione inerente allo Smart Poster è stata sviluppata nel "Smart Touch Project" che si è svolto ad Oulu, in Finlandia. Questo progetto è stato coordinato da 9 aziende tra il 2006 e il 2008 esaminando il ruolo che può avere l'NFC nella vita di tutti i giorni. Questo progetto ha introdotto applicativi NFC nelle case, negli ospedali, nei parcheggi e nei luoghi commerciali. Un'applicazione che è stata introdotta dal progetto Smart Touch è "Amazing NFC". Questa prevedeva un percorso culturale della cittadina di Oulu. I partecipanti, muovendosi nel centro di Oulu, incontravano dei luoghi di interesse contrassegnati con dei Tag NFC che, avvicinati da uno Smartphone NFC, rispondevano con le informazioni di quel luogo.
Sempre nella cittadina di Oulu gli Smart Poster sono stati anche utilizzati nei cinema e nei ristoranti. Nei cinema ad esempio in corrispondenza di ogni locandina dei film c'era un tag, questo se veniva interrogato da un dispositivo NFC inviava il link web per il trailer del rispettivo film. Allo stesso modo al teatro si poteva vedere la programmazione futura degli spettacoli [21].

Per quanto riguarda i parcheggi, ai cittadini di Oulu era stato fornito un Tag identificativo da attaccare nel parabrezza. L'utente che si recava in un parcheggio a pagamento, doveva avvicinare il cellulare al Tag posto sull'autovettura, poi avvicinarlo ad un Tag posto su un palo dell'illuminazione che identificava l'ubicazione del parcheggio, lo smartphone completava successivamente il pagamento. Questa applicazione potrebbe permettere il superamento dei parchimetri e l'eliminazione di tutti i costi relativi.

Figura 3.14: locandina del film "Zero Dark Thirty" con Smart Poster. Gli utenti che si connettevano con questo Smart Poster potevano partecipare ad un concorso premi e vedere il trailer del film.

3.5.4 IDENTIFICAZIONE

Un'altra applicazione sviluppata nella cittadina di Oulu è stata lo "student attendance". Questa pratica ha sostituito nelle scuole l'appello da parte dei professori. Questa sperimentazione ha dotato ogni ragazzo di una Smart card nominale, la quale era avvicinata tutte le mattine allo smartphone NFC in dotazione dell'insegnante. Il cellulare era collegato alla banca dati della scuola, questo permetteva di caricare in tempo reale la situazione delle presenze e delle assenze su internet. Questo sistema rendeva agile il compito degli insegnanti e permetteva ai genitori di sapere se i propri figli erano arrivati a scuola in orario.

3.6 SICUREZZA

La tecnologia NFC essendo un evoluzione dell'RFID, ne eredita anche le problematiche di sicurezza, sebbene risulti in alcuni casi meno predisposta a certi tipi di attacchi. Oltre alla comunicazione, anche i Tag presentano una serie di problematiche di sicurezza. Le possibili minacce di sicurezza a cui essi potranno essere sottoposti sono tutte quelle che possono provocare un'acquisizione, o un'alterazione illecita delle informazioni. L'acquisizione o l'alterazione illecita dei dati contenuti nei Tag può avvenire sia attraverso interrogazioni fraudolente dei Tag con Reader non autorizzati, sia mediante intercettazione delle informazioni, tramite ricevitori radio, durante una lettura delle stesse da parte di un Reader autorizzato. Ciò potrà essere ottenuto 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 di informazioni con Reader nascosti [16].

3.6.1 INTERCETTAZIONI

L'intercettazione dei dati detta in inglese Eavesdropping è uno degli attacchi più comuni nell'ambito delle comunicazioni wireless. Per portare a termine questa tipologia di attacco è necessario utilizzare una strumentazione specifica con antenne e Reader costruiti ad hoc. Questo attacco è un attacco molto comune nel campo RFID dove le distanze e le potenze maggiori degli apparati forniscono all'hacker un maggiore margine di manovra, mentre nell'ambito NFC questo attacco è molto più difficile da realizzare. Questo non significa che i sistemi NFC ne siano immuni, infatti si deve tener conto di una serie di fattori:

- Potenza emessa dall'apparato sotto intercettazione
- Caratteristiche del campo RF emesso dall'apparato sotto intercettazione
- Modalità attiva o passiva dell'apparato sotto intercettazione
- Fattori ambientali
- Caratteristiche dell'attrezzatura dell'hacker
- Presenza o meno di crittografia

Da questo elenco si evince che le comunicazioni con Tag passivi siano meno esposti alle intercettazioni riguardanti quelli attivi.
Un'eventuale contromisura può essere quella di minimizzare il campo magnetico ed aumentare la direzionalità delle antenne. Un'altra efficace contromisura è allestire un canale sicuro di comunicazione. Si genera un canale sicuro cifrando i dati con una chiave segreta K, il ricevitore decripta i dati cifrati usando la stessa chiave (simmetrica) o la chiave K' (asimmetrica). Alcuni tipi di crittografia utilizzati ad esempio nelle carte MIFARE sono la 3DES (Triple Data Encryption Standard) e la AES (Advanced Encryption Standard) [16].

3.6.2 ALTERAZIONE DEI DATI

Questo tipo di minaccia è molto pericolosa perché risulta trasparente all'utente e nello stesso tempo può causare molti danni, fortunatamente la realizzazione di questo attacco è molto complicata. Lo scopo di questa minaccia è modificare i dati trasmessi e farli risultare validi. In generale questo tipo di attacco dipende dalla modulazione utilizzata per la trasmissione. La riuscita dell'attacco dipende molto anche dall'ampiezza dei segnali che il ricevitore ammette in ingresso. Per il codice Miller modificato con indice di modulazione al 100%, l'attacco è possibile soltanto su certi bit perché sarebbe necessario impostare una portante esattamente in contro fase per modificare i restanti bit; mentre per il codice Manchester con indice di modulazione al 10% l'attacco è possibile su tutti i bit [16].

3.6.3 INSERIMENTO DI FALSI MESSAGGI

Questo attacco prevede l'inserimento di dati nella comunicazione facendoli apparire come dei messaggi validi scambiati tra gli apparati. Tipicamente l'attacco necessita di alcune condizioni temporali, infatti il messaggio dell'hacker deve essere inserito prima della reale risposta e senza sovrapporsi ad essa. Nell'ambito NFC anche questo tipo di attacco è di difficile realizzazione, poiché i tempi di risposta del dispositivo interrogato sono molto brevi. Si possono attuare due tipi di contromisure: la prima è ridurre ulteriormente il tempo di risposta rendendo impossibile l'attacco, mentre la seconda consiste nell'ascolto del canale per un tempo lungo, permettendo di svelare l'eventuale attacco.

3.6.4 MAN IN THE MIDDLE ATTACK

Questo è uno degli attacchi più pericolosi per i sistemi wireless e può arrecare danni elevati ai sistemi che lo subiscono. Mentre due apparati A e B stanno comunicando, tra loro entra in gioco l'hacker attraverso un terzo apparato estraneo (Man in the Middle) che inganna le loro comunicazioni. Durante le comunicazioni avviene che i due apparati A e B non si accorgano di non parlare tra di loro, bensì l'hacker simula, alterandoli i dati di entrambi. Quest'attacco è vanificato se viene allestito un "canale sicuro", ovvero i due apparati A e B concordano una chiave che useranno per criptare i dati. Potrebbe però succedere che l'apparato dell'hacker negozi una chiave con A e una con B e continui a porsi nel mezzo della comunicazione. Fortunatamente anche in questo caso la realizzazione di questo attacco è complesso poiché comporterebbe la visibilità fisica dell'hacker [16].

3.6.5 PISHING

Questa problematica appartiene soltanto al mondo NFC e non deriva dai sistemi RFID. Sappiamo che il tipo URI identifica una risorsa remota, nei record che contengono URI (URI record e Smart Poster record). Il pishing si basa sul concetto di ingannare l'utente e cercare di portarlo a compiere azioni diverse da quelle. Questo può essere implementato, nel caso di Smart Poster, semplicemente cambiando il Title record contenente il titolo della risorsa in modo che non rispecchi la vera risorsa a cui è riferita. Recentemente alcuni ricercatori hanno scoperto altri metodi per mettere in atto un attacco del genere; questi fanno uso di caratteri speciali, come quelli di tabulazione, che permettono di mostrare ad un utente un URI e in realtà lo collegano ad un altro. Questo tipo di attacco può essere la base per altri tipi di attacchi. Ad esempio si potrebbe generare un Worm e farlo scaricare all'utente tramite questo meccanismo. La situazione è aggravata dal fatto che i Tag passivi, ovvero quelli più comuni e commerciali, sembrano essere i componenti più esposti a questo tipo di attacco.

CAPITOLO 4

STRUMENTAZIONE E SOFTWARE NFC

In questo capitolo si darà una descrizione di alcune prove pratiche dell'NFC. La sperimentazione verte sull'utilizzo del protocollo NDEF, per permettere di effettuare alcuni test con uno Smartphone.

4.1 HARDWARE UTILIZZATO

In questa sezione verranno tratti gli strumenti hardware: il Reader SCL3711, una gamma di Smart Card e Tag aderenti al protocollo 14443-A appartenenti alla famiglia MIFARE e infine per testare la compatibilità con i cellulari abilitati all'NFC, si è impiegato un Samsung Galaxy S3.

4.1.1 READER SCL3711

Figura 4.1: fotografia del Reader SCL3711

Il Reader Identive SCL3711, è un dispositivo di comunicazione wireless ultracompatto. La frequenza di lavoro è 13.56 Mhz +/- 50 ppm, nel rispetto degli standard contactless. L'antenna è stata ottimizzata a livello di fattore di forma per aumentare la distanza di lettura, che rimane in ogni caso molto limitata.

Le sue dimensioni sono 65.4(L) x 23(W) x 10(H)mm, per un peso di 10.2 grammi. Per avere un'interfaccia user-friendly è stato inserito un led rispetto alla versione precedente, per segnalare se il dispositivo è acceso o se è in fase di lettura [9].
Il Reader interfacciato al computer attraverso lo standard USB, da cui è alimentata. La modulazione non è univoca, varia secondo il protocollo di comunicazione utilizzato, quindi dipende dal Tag con cui si instaura la comunicazione. La forza del campo

magnetico generato dal Reader è 1.5 A/m che rappresenta il minimo dello standard ISO 14443. Il modesto valore del campo magnetico emesso unito alle dimensioni ridotte dell'antenna sono la ragione di un range di funzionamento molto limitato. Il massimo baud rate è di 848 Kbps [10].

Il Reader è compatibile con gli standard:

- ISO/IEC 14443 A
- ISO/IEC 14443 B
- MIFARE: Classic 1k e 4k, MIFARE plus, DESfire, Ultralight
- My-d NFC
- Felica
- NFC forum tag type 1,2,3,4
- ISO/IEC 18902 [9]

L'hardware è supportato dalla maggior parte dei sistemi operativi: Windows XP, Windows 7, Windows 8, Mac Os X, Linux.

4.1.2 MIFARE CLASSIC 1K ,2K, 4K

La famiglia MIFARE Classic è la precorritrice nell'ambito delle contactless Smart Card funzionanti a 13.56 MHz. Realizzate in accordo allo standard ISO14443 sono utilizzate soprattutto nel campo dei trasporti e nel controllo degli accessi [13]. Sono di grande utilità perché sono compatibili con SmartCard Commander e questo ci permetterà di leggere la codifica dei dati che vi introduciamo.

4.1.3 MIFARE DESFIRE EV1 8K

Le Desfire Sono attualmente le carte più evolute dal punto di vista della memoria, infatti hanno 8192 byte di EEPROM. Sono contactless Smart Card sviluppate da NXP e Philips, funzionano con accoppiamento induttivo come in accordo allo standard ISO14443 tipo A.

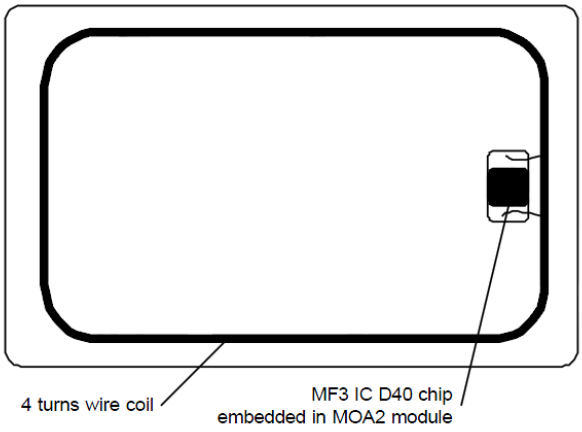

Figura 4.2: sezione di una carta Mifare. Lungo il bordo della carta è implementata l'antenna interconnessa al chip che si trova in posizione decentrata.

Queste carte, appartengono alla famiglia dei trasponder passivi, quindi l'alimentazione per instaurare la comunicazione viene fornita dal Reader. L'interfaccia del collegamento permette alla carta di trasmettere fino a 424 kbit/s [11]. Queste carte come specifica supportano tutti i servizi e le applicazioni definite nell'NFC Forum, ovvero L'NFC Data Exchange Format (NDEF). Rispetto alle Mifare Classic, le DESFire hanno una maggiore flessibilità, infatti il microprocessore presente nel chip permette di gestire fino a 32 file. Un'altra notevole differenza è la crittografia, le DESFire sono all'avanguardia utilizzando crittografia AES, DES e 3DES. Questa caratteristica è realizzata in ambiti che richiedono una sicurezza maggiore come ad esempio nei pagamenti elettronici [11].

4.1.4 SAMSUNG GALAXY S3

Per le prove realizzate con il cellulare si è utilizzato un Samsung Galaxy S3 con sistema operativo Android. Questo modello installa un microcontrollore per dispositivi mobili NXP PN544 che gestisce tutte le funzionalità NFC, questo chip è compatibile alla comunicazione con Tag aderenti all'ISO 14443-A, ISO 14443-B, Sony Felica e Mifare Classic [29]. Il chip inoltre supporta le comunicazioni aderenti all'NFCIP-1, pertanto supporta le modalità di Card Emulation e di Peer-to-peer [14]. Per rientrare nei requisiti di potenza dei vari produttori di smartphone, il PN544 supporta varie modalità di potenza che possono essere configurate via hardware e via software. Il microcontrollore, infine utilizza diverse modulazioni e regimi di potenza secondo il protocollo di comunicazione utilizzato [29].

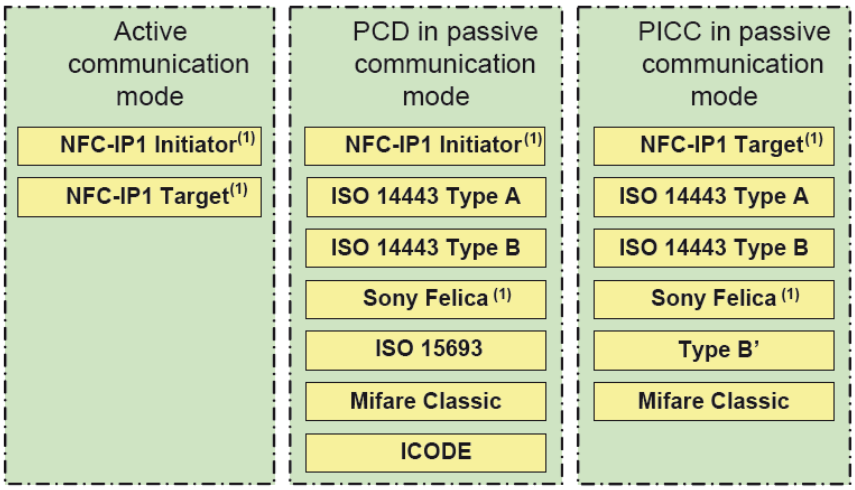

Figura 4.3: protocolli compatibili con il microcontrollore PN544.

Dopo aver disassemblato il cellulare, il Chip PN544 è visibile nella parte bassa del telefono come si può notare in figura 4.5. Mentre l'antenna non può essere visualizzata perché installata nella batteria dello smartphone. Per questo motivo il miglior accoppiamento si otterrà avvicinando un Tag al dorso dello smartphone in maniera parallela al cellulare.

Figura 4.4: a sinistra foto del Galaxy S3, a destra una foto del suo interno.

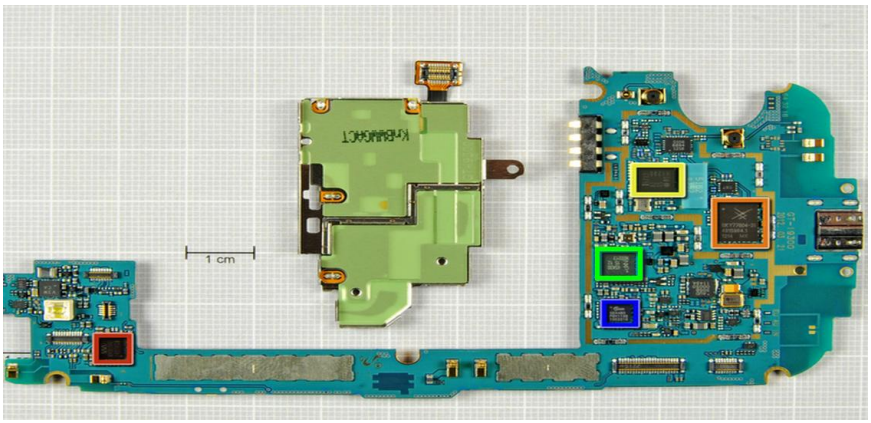

Figura 4.5: una sezione della circuiteria del Galaxy S3. Nel riquadro verde è presente il chip PN544.

4.2 SOFTWARE UTILIZZATO

4.2.1 GOTOTAGS

GoToTags permette di memorizzare nei Tag una serie di dati prestabiliti come ad esempio: Sms, Vcard, GeoLocation, indirizzi web. L'applicazione memorizza i dati secondo le specifiche del protocollo NDEF, in modo che i Tag siano leggibili dagli attuali smartphone abilitati all'NFC.
Per codificare un Tag con protocollo NDEF si creano nella finestra principale i dati che si vogliono memorizzare poi, in un secondo momento, si clicca su "Encode NFC Tags" nella barra degli strumenti. In seguito si avvicina l'NFC Tag in cui si vogliono salvare le informazioni al Reader/Writer, e si attende che l'operazione di codifica sia terminata.

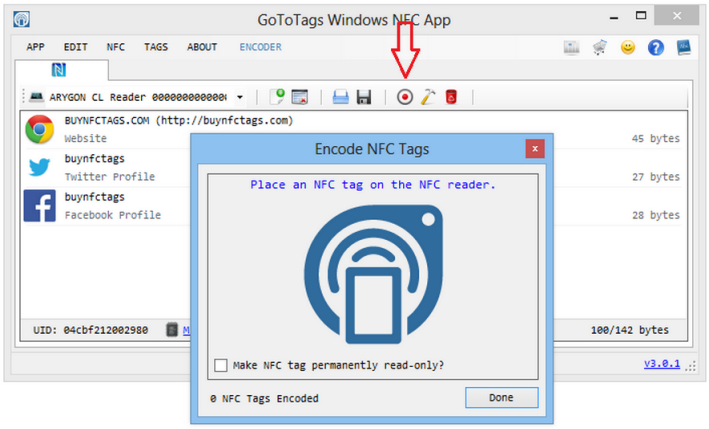

Figura 4.6: schermata che appare al momento della codifica del Tag.

Se si vuole impedire che i dati vengano sovrascritti da una nuova codifica, si può scegliere l'opzione di bloccaggio dati, denominata "Read-Only". Nel caso si scelga quest'opzione, il Tag diverrà disponibile solo per la lettura e il contenuto non sarà più modificabile. Per applicarlo è necessario aprire il menù a tendina "NFC" e cliccare su "Make Nfc Tag Read-Only".

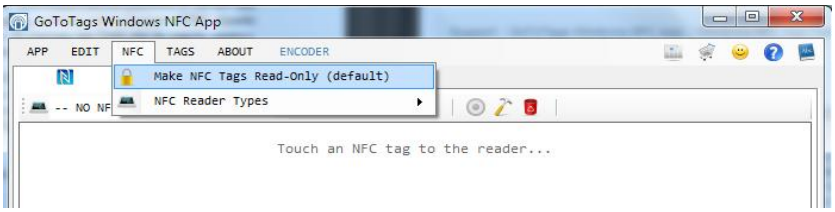

Figura 4.7: opzione Read-Only.

Una particolarità del protocollo di incapsulamento è la formattazione NDEF dei Tag. La maggior parte dei Tag non è inizialmente compatibile al protocollo di incapsulamento, per renderli abilitati è necessario effettuare questo tipo di formattazione. In altri casi la formattazione è necessaria perché alcuni smartphone NFC, come ad esempio i Windows Mobile, leggono solo Tag con questa specifica. GoToTags permette di eseguire la formattazione NDEF, il comando si trova nella barra degli strumenti e come nel caso della codifica basta avvicinare il Tag al Reader e aspettare il termine dell'operazione.
Il programma può anche eliminare i dati di un Tag. La cancellazione dei dati avviene solo nel caso in cui i Tag siano riscrivibili, ovvero non Read-Only. Il comando si trova nella barra degli strumenti [30].

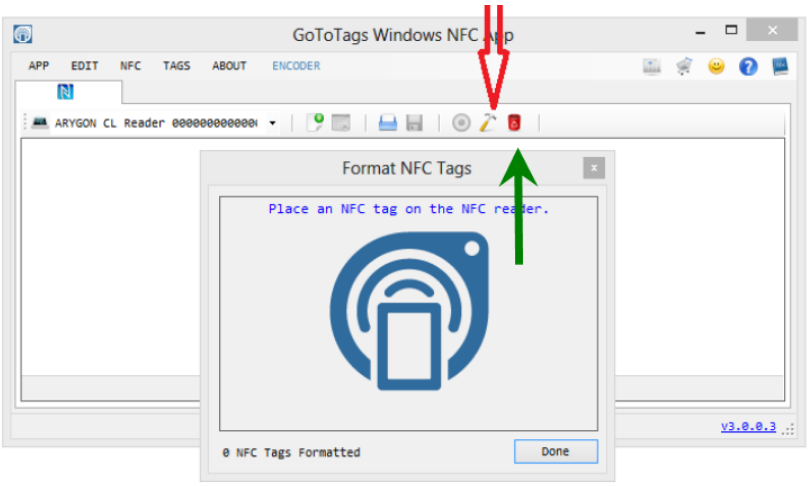

Figura 4.8: la freccia rossa indica il pulsante per la formattazione NDEF del Tag. La freccia verde indica l'opzione di eliminazione dei dati.

Quando il Reader legge un Tag, l'applicazione raccoglie una serie di informazioni che mostra all'utente nella barra di stato inferiore. Queste sono:

- UID (Unique IDentifier)
- Tipo di Tag
- Se è stata fatta la formattazione NDEF
- Se il chip è settato come Read-Only
- La quantità di memoria occupata
- La quantità di memoria libera

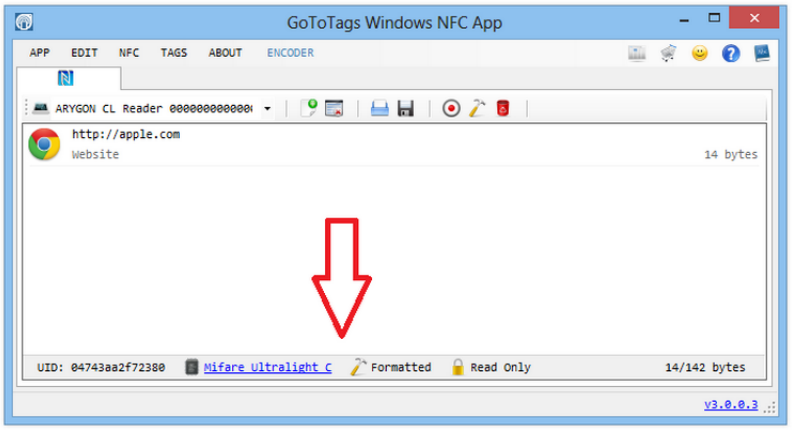

Figura 4.9: la freccia indica la barra di stato dove sono presenti le informazioni sul Tag.

GoToTags permette all'utente di variare l'ordine dei file che si vogliono memorizzare a proprio piacimento. Esiste quest'opzione perché lo smartphone NFC legge i dati con lo stesso ordine con cui sono memorizzati all'interno del Tag [30].

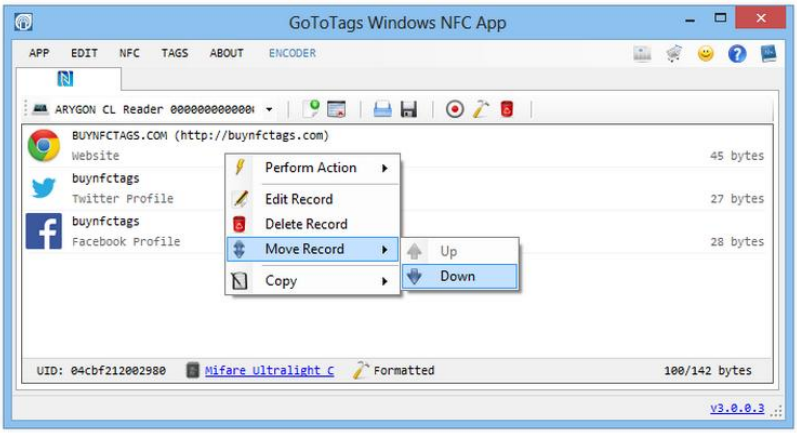

Figura 4.10: menù di ricollocazione dei Record.

Il programma fornisce all'utente la possibilità di salvare i file contenuti nel Tag. Permettendo in seguito di poter memorizzarlo in un altro dispositivo.
L'applicazione quando esegue la codifica dei dati, può associare alla prima risorsa memorizzata il Record Action: un Record che viene concatenato alla prima informazione salvata e permette alla risorsa di essere aperta in automatico da un programma standard dello smartphone. Questa è una specifica di default del programma, che però può essere disabilitata.

4.2.1 CHIPDRIVE SMARTCARD COMMANDER

Per affiancare GoToTags si è scelto SmartCard Commander. Questa applicazione della SCM Microsystems permette di visualizzare la memoria a blocchi del Tag. Questi blocchi vengono visualizzati per caratteri esadecimali, questo permette di vedere la codifica dei file secondo le specifiche NDEF.

Nella parte alta della finestra principale il programma mostra l'hardware, quindi il Reader/Writer utilizzato e l'eventuale Tag con cui si è instaurata la comunicazione.

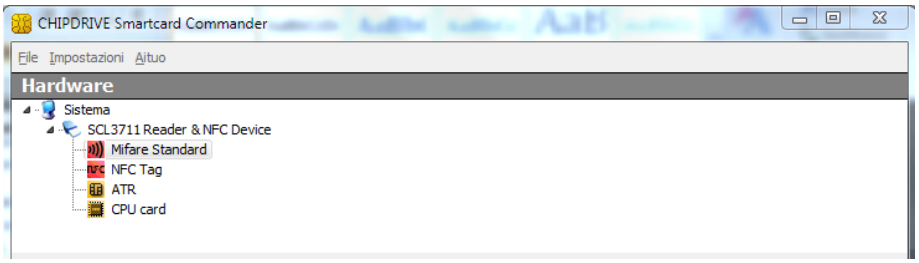

Figura 4.11: menù a discesa, nella schermata principale di SmartCard Commander.

Se si clicca sulla dicitura del Reader, che nel nostro caso è SCL3711, il programma apre una schermata che contiene le informazioni generali del dispositivo, come ad esempio: nome della periferica, produttore, frequenza di clock, data rate e se disponibile il power management.

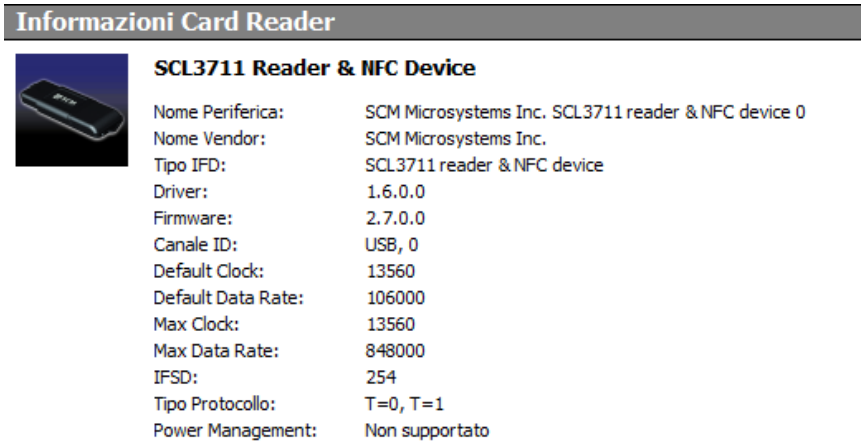

Figura 4.12: schermata riguardante le informazioni del Card Reader.

Nel momento in cui entra nel range di comunicazione un Tag, nella finestra di esplorazione dell'hardware appare un menù a discesa, dove sono disponibili le informazioni riguardanti il Tag.
In particolare, utilizzando una MIFARE Classic 4k, nel menù a discesa compare un elemento denominato "MIFARE Standard". Cliccandovi, il programma esegue la lettura di ogni blocco di memoria e lo riporta a schermo.

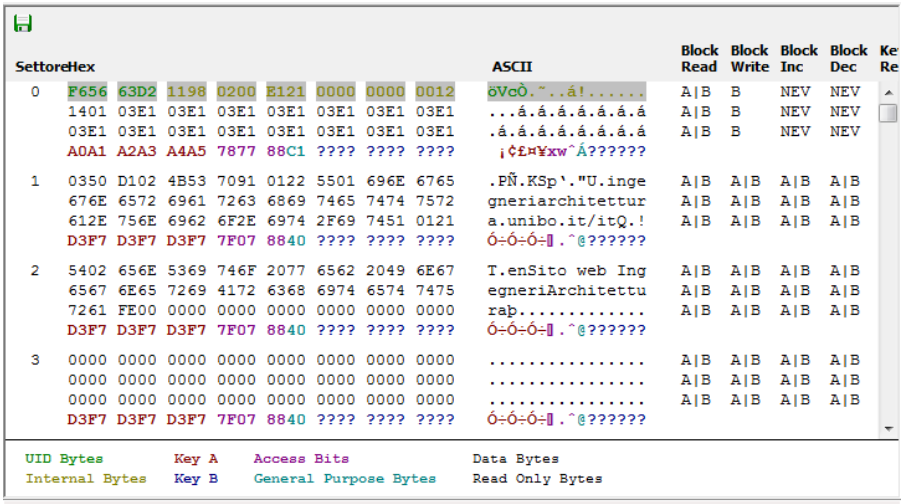

Figura 5: visualizzazione della memoria di un Tag.

L'output della memoria utilizza caratteri con colori diversi per distinguere i vari campi. Ad esempio si utilizza il verde per i caratteri esadecimali che caratterizzano l'UID, il giallo per byte riservati al Tag, in rosso e in blu i caratteri relativi alle chiavi di crittografia, in viola i byte di indirizzamento, mentre i caratteri neri rappresentano i dati memorizzati dall'utente.

4.3 ESEMPI DI CODIFICA NDEF

4.3.1 ESEMPIO CON INDIRIZZO HTML

Ora si riprende l'esempio della sezione 3.4.3 riguardante lo Smart Poster. Si vuole salvare l'indirizzo web della facoltà di ingegneria su una MIFARE Classic 4k. Quindi per prima cosa si effettua la formattazione NDEF della Smart Card o del Tag, utilizzando GoToTags. In seguito nella barra degli strumenti clicchiamo su "Add new Record" e scegliamo "website". Si apre una finestra con due campi, nel primo denominato "URL" inseriamo "http://www.ingegneriarchitettura.unibo.it", mentre nel secondo denominato "Title" non inseriamo alcun carattere poiché è un campo facoltativo.

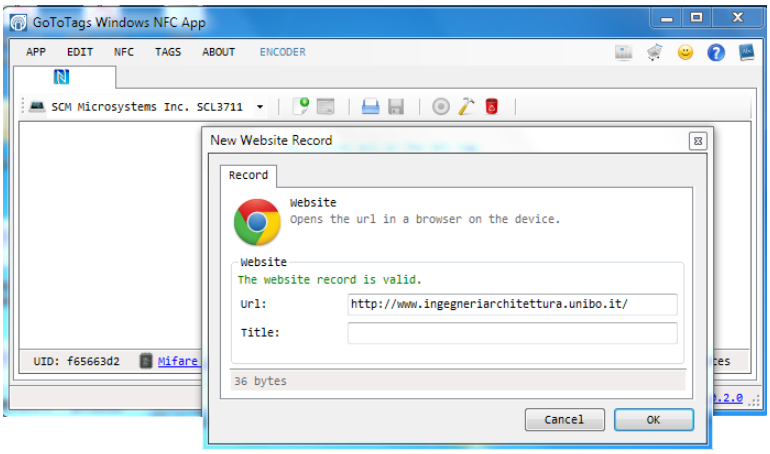

Figura 4.14: schermata di inserimento di un nuovo record WebSite in GoToTags.

A questo punto si aspetta che avvenga il trasferimento dei dati. Successivamente verifichiamo sempre con GoToTags la memorizzazione dei dati. In realtà se la memorizzazione ha avuto successo, GoToTags aprirà direttamente l'indirizzo web della scuola d'ingegneria e architettura. Questa funzionalità in ambiente Windows è stata introdotta nella versione 3.0.2.0 rilasciata a luglio 2013.

In seguito si utilizza l'applicazione Smart Commander per visualizzare la codifica del sito web, che in ambito NDEF è un URI Type.

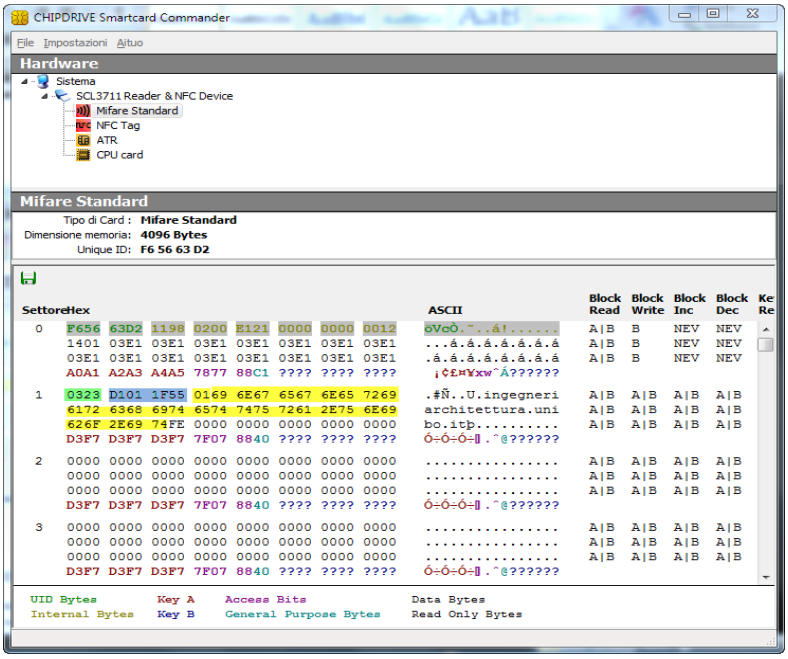

Figura 4.15: lettura della memoria della Mifare Classic 4k. Nel blocco 1 è memorizzato l'URL: "http://www.ingegneriarchitettura.unibo.it".

Evidenziato in blu, D1 rappresenta l'Header del Record Uri, 01 indica la lunghezza del Type Name, 1F la lunghezza del Payload, 55 codifica la lettera "U" che corrisponde al tipo URI. Infine evidenziato in giallo si ha il Payload del Record URI, dove 01 corrisponde all'URI Identifier "http//:www.", mentre il resto dei caratteri esadecimali è la semplice codifica delle lettere del sito web.

4.3.2 ESEMPIO CON RECORD DI TESTO E RECORD URI

Si vuole realizzare un esperimento in cui si memorizzano due Record NDEF. Con GoToTags inseriamo un Record di Testo, seguito da un Record Uri. Il Record di Testo conterrà la frase "benvenuto alla scuola di ingegneria e architettura", mentre il Record URI contiene l'indirizzo utilizzato nella sezione 4.6.

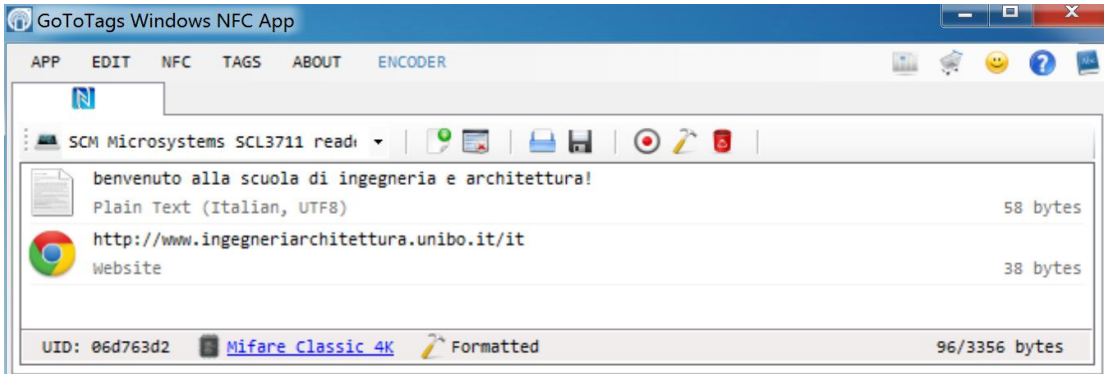

Figura 4.16: codifica di un Record di testo e di un Record URI.

Al termine della trascrizione dei dati, per verificare la corretta memorizzazione, si prova ad avvicinare il Tag al Reader. Si nota che il trasferimento delle informazioni è andato a buon fine poiché viene aperto in automatico il "Blocco Note" di Windows con cui leggiamo il primo Record memorizzato. Nel menù dello Smartphone di Android otteniamo un menù in cui compaiono i due Record.
Per visualizzare la codifica del messaggio NDEF utilizziamo il programma SmartCard Commander come nella sezione 4.6. Sottolineato in arancione abbiamo l'Header del Record di Testo. I due caratteri esadecimali 0x91 e 0x01 in bit valgono 1001 e 0001. Quindi con 1001 abbiamo che: MB=1, ME=0, CF=0, SR=1. Quindi è specificato che il Record rappresenta l'inizio del messaggio, ma non è l'ultimo Record, che non è concatenato con un altro Record, e infine che è uno Short Record. Con 0001 si decodifica che IL=0, TNF=001. Questo ci permette di capire che il Record non ha identificatori e che il Tipo appartiene alle definizioni dell'NFC Forum.
Sempre in arancione abbiamo 0x36, 0x54 che rappresentano rispettivamente la lunghezza del Payload e il Type del record. 0x54 infatti decodificato indica "T" ovvero "Text". Infine abbiamo la sequenza 0x02 0x69 0x74, dove 0x02 indica il numero dei caratteri della lingua, mentre 0x69 e 0x74 decodificandoli indicano "it" ovvero lingua italiana. Sempre in figura 4.16 i caratteri evidenziati in giallo indicano il Payload del Record di Testo codificato in UTF-8.

Ora si ha il secondo Record. In figura 4.16 si è sottolineato in azzuro l'Header e in verde il Payload. Analizzando l'Header si ha come primo byte 0x51, quindi "0101 0001". Questo si traduce in: MB=0, ME=1, CF=0 e SR=1. Mentre come nel caso del primo Record si avrà IL=0 e TNF=1.
In seguito si avrà 0x01, 0x22, 0x55, 0x01, che rispettivamente indicano la lunghezza del Type Name, la lunghezza del Payload, il tipo "U" mentre 0x01 indica l'identificatore URI che indica "http://www". Sottolineato in verde invece si nota il Payload che contiene i caratteri dell'indirizzo web.

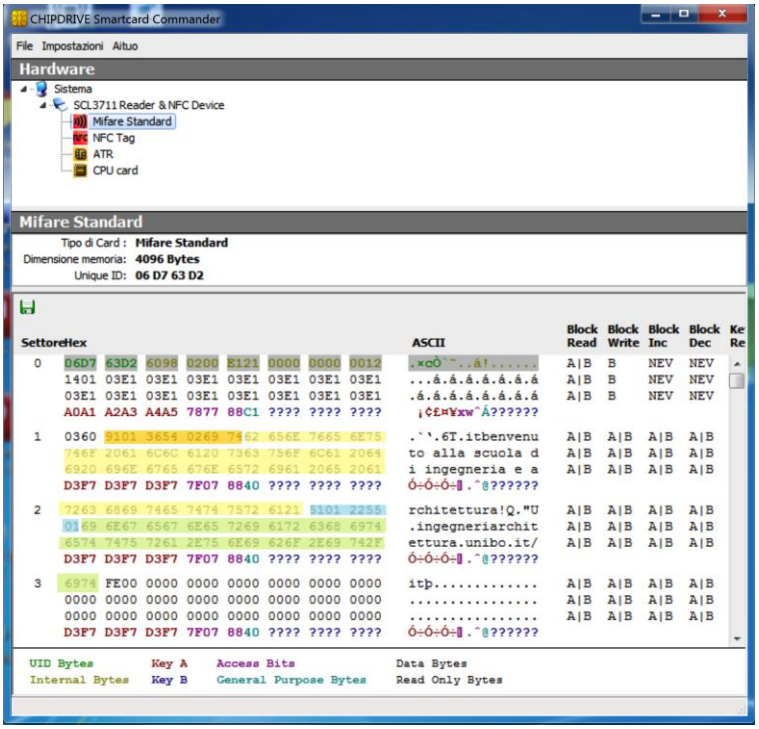

Figura 4.16: lettura del Tag attraverso SmartCard Commander.

CAPITOLO 5

SMART BRICK

In questa sezione si tratterà la realizzazione di un "mattone elettronico", cioè un mattone nel quale possano essere immagazzinate delle informazioni, recuperabili tramite la comunicazione con smartphone NFC. Questo oggetto è stato chiamato Smart Brick, ovvero un mattone intelligente che abbia le funzionalità di uno Smart Poster.

5.1 NASCITA DELLO SMART BRICK

L'idea dello Smart Brick nasce in concomitanza della posa della prima pietra del futuro Campus di Ingegneria e Architettura dell'Alma Mater Studiorum Università di Bologna, Polo di Cesena. Si intende realizzare un mattone "intelligente" che conservi al suo interno alcune informazioni riguardanti la forma della struttura, le coordinate geografiche e altri elementi che potessero rimanere negli anni. Volendo realizzare una memoria all'interno di un mattone è nata l'esigenza di utilizzare componenti passivi, ovvero non alimentati. In questo senso si è scelto di impiegare una tecnologia a radio frequenza, ovvero l'NFC. Questa decisione nasce dall'esigenza di permettere al maggior numero di persone ci contattare la pietra, cioè non utilizzando un particolare Reader RFID bensì il proprio Smartphone abilitato all'NFC.

5.2 REALIZZAZIONE

Per la costruzione dello Smart Brick si è utilizzato un mattone traforato, come mostrato in figura 5.1, comunemente utilizzato nella costruzione di pareti divisorie, oppure per pareti portanti nei piani più elevati.

Figura 5.1: tipologia di mattone utilizzato.

Installando un Tag all'interno dei fori si evidenzia che non si riesce a sostenere la comunicazione con lo smartphone, così è stato installato il Tag nella superficie più esterna del mattone. Per questo scopo è stato realizzato un solco nel lato lungo del mattone utilizzando una smerigliatrice angolare, profondo circa un centimetro. Successivamente si è ricoperto lo scasso con stucco per pareti fino ad un millimetro dal bordo del mattone e su questo strato è stato collocato il Tag, ottenendo un perfetto allineamento con il bordo. Infine si è ricoperto il tutto con un ulteriore strato di stucco dello spessore di circa 3mm. Una volta asciutto si è levigata la superficie esterna per renderla il più regolare possibile. Come Tag utilizzato si è scelto il Mifare DESFIRE 8k, una Smart Card aderente al protocollo 14443, che il produttore garantisce per 10 anni. Questa Smart Card è adatta per due motivi: il primo è la memoria più elevata presente sul mercato attuale dei Tag, secondo perché come tipologia di Tag adotta l'antenna più performante.

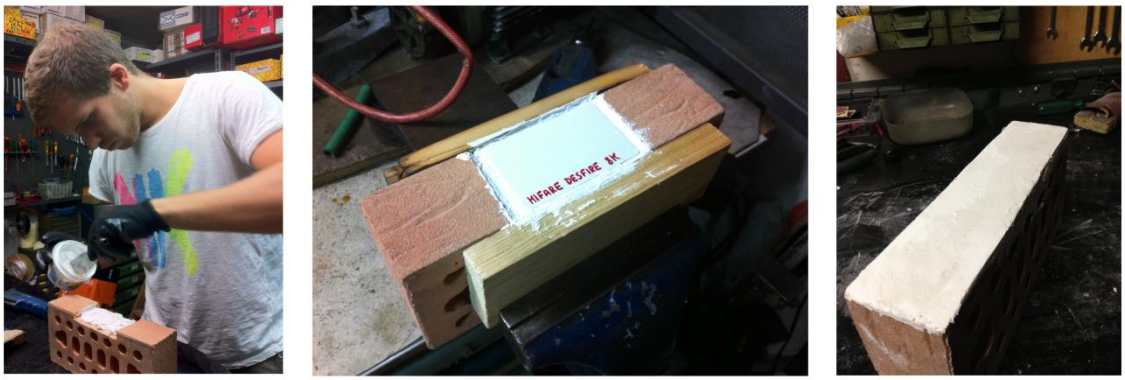

Figura 5.2: da sinistra verso destra le fasi della realizzazione dello Smart Brick: a sinistra il riempimento dello scasso, al centro il posizionamento del Tag, infine a destra la ricopertura finale.

5.3 PROVE SULLA DISTANZA DI FUNZIONAMENTO

In seguito alla realizzazione dello Smart Brick sono state effettuate una serie di prove sperimentali con l'obbiettivo di quantificare la distanza operativa. In questi test si è deciso di avvicinare Smartphone in posizione verticale, come mostrato in figura 5.2, poiché in primo luogo è ipotizzabile che l'utente che vuole interpellare il mattone avvicini lo smartphone in questo modo, e in secondo luogo questa posizione consente di ottenere il massimo coefficiente di accoppiamento.

Figura 5.2: modo con cui viene avvicinato lo Smartphone nei test al bordo del mattone.

Le misurazioni sono state svolte installando il Reader e lo Smartphone su un supporto verticale mobile, e l'effettivo Range è stato calcolato con l'utilizzo di un calibro. Si sono eseguite 4 tipologie di misura che hanno coinvolto il Reader SCL3711, lo smartphone Samsung S3, la Smart Card Mifare DESFIRE e lo Smart Brick.

5.3.1 READER – SMARTBRICK

Prova numero	Range dalla superficie	Spessore stucco
1	2.0cm	0.3cm
2	1.8cm	0.3cm
3	1.7cm	0.3cm
4	1.7cm	0.3cm
5	1.7cm	0.3cm
6	1.8cm	0.3cm
7	1.6cm	0.3cm
8	1.7cm	0.3cm
9	1.6cm	0.3cm
10	1.7cm	0.3cm
Media=1.73cm		
Moda=1.7cm		
Mediana=1.7cm		

Tabella 5.1: dati sperimentali del test Reader - Smart Brick.

Con questa prova si calcola la distanza operativa tra il Reader e lo Smart Brick. Al range ottenuto in tabella 5.1 deve essere aggiunto lo spessore dello stucco.

5.3.2 READER – SMART CARD

Misura della distanza di funzionamento tra Reader e Smart Card, misura necessaria per evidenziare l'effetto della copertura nel caso dello Smart Brick.

Prova numero	Range
1	2.3cm
2	2.5cm
3	2.5cm
4	2.4cm
5	2.5cm
6	2.4cm
7	2.5cm
8	2.5cm
9	2.4cm
10	2.4cm
Media=2.44cm	
Moda=2.5cm	
Mediana=2.45cm	

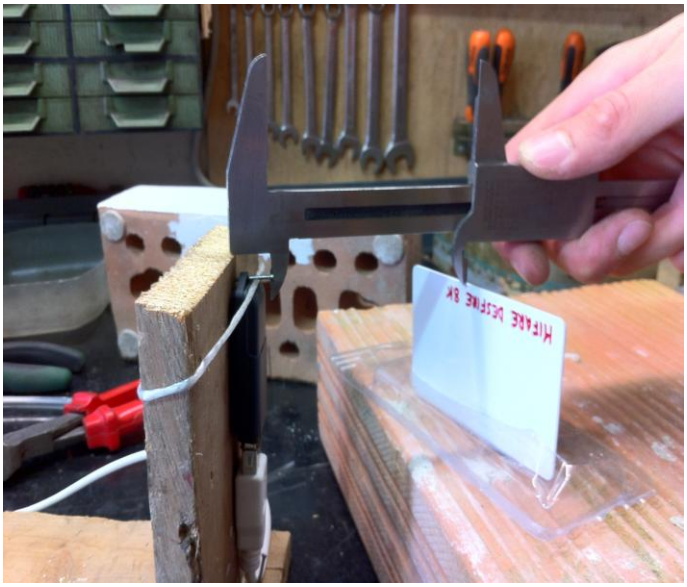

Tabella 5.2: dati sperimentali del test Reader – Smart Card.

Notando i dati di Tabella 5.2 si nota che il range effettivo si è ridotto di circa 4mm. Questo scostamento è da attribuire alla attenuazione introdotta dallo spessore dello stucco.

5.3.3 SMARTPHONE – SMART BRICK

In questo test si nota come il range sia differente dai test effettuati con il Reader. In particolare si nota che la distanza di funzionamento è sensibilmente inferiore. La motivazione potrebbe essere la posizione dell'antenna, forse collocata troppo internamente e disturbata dalla circuiteria del cellulare.

Il test è comunque positivo perché all'inizio ci si aspettava che il cellulare funzionasse a contatto con il mattone, mentre si è constatato che il Galaxy S3 riesce ad instaurare la comunicazione ad una distanza di circa 1cm.

Prova numero	Range dalla superficie	Spessore stucco
1	1.3cm	0.3cm
2	1,2cm	0.3cm
3	1.3cm	0.3cm
4	1.1cm	0.3cm
5	1.1cm	0.3cm
6	1.2cm	0.3cm
7	1.3cm	0.3cm
8	1.3cm	0.3cm
9	1.2cm	0.3cm
10	1.0cm	0.3cm
Media=1.2cm		
Moda=1.3cm		
Mediana=1.2cm		

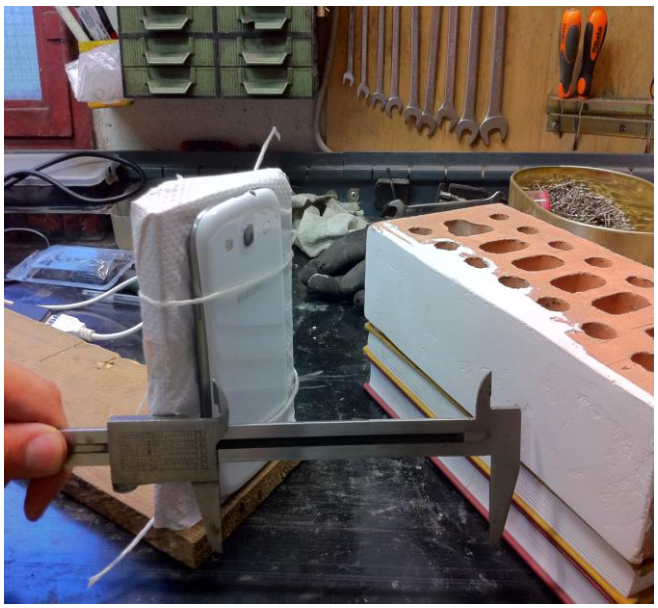

Tabella 5.3: dati sperimentali del test tra Galaxy S3 - Smart Brick.

5.3.4 SMARTPHONE – SMART CARD

Quest'ultimo test permette di quantificare il range tra lo Smartphone e la Smart Card. Osservando i dati di tabella 5.4 si osserva che il range medio con la carta è circa 2.12 cm mentre nel caso dello Smart Brick era 1.2 cm. Questo fa intuire che lo smartphone percepisce un attenuazione maggiore rispetto al Reader, infatti lo stucco genera nel caso dello Smart Brick un'attenuazione di circa 6 mm.

Prova numero	Range
1	2.0cm
2	2.0cm
3	2.1cm
4	2.3cm
5	2.3cm
6	2.1cm
7	2.0cm
8	2.2cm
9	2.2cm
10	2.0cm
Media=2.12cm	
Moda=2.0cm	
Mediana=2.1cm	

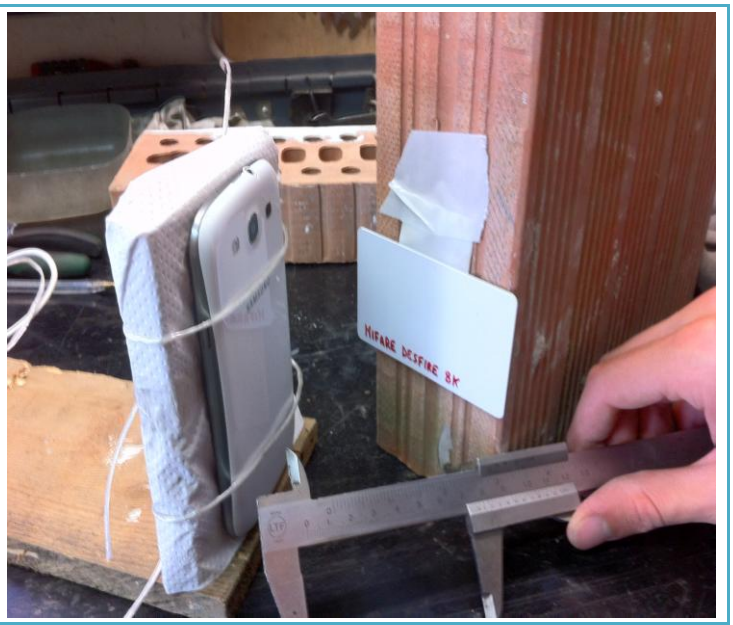

Tabella 5.4: dati sperimentali del test tra Galaxy S3 – Smart Card.

5.4 PROGRAMMAZIONE SMART BRICK

La fase che segue la realizzazione dello Smart Brick è la sua programmazione. L'obbiettivo è inserire una serie di informazioni che descrivessero alcune caratteristiche del nuovo campus di ingegneria e architettura. La difficoltà di questa fase è stata senza dubbio la scarsa elasticità della codifica NDEF. Infatti come si è visto nella sezione 4.2.1 GoToTags può codificare un numero molto limitato di informazioni. Questi vincoli ci hanno indirizzato ad inserire questa serie di informazioni: due file di testo, alcuni link web, coordinate geografiche del Campus e una bozza e-mail.

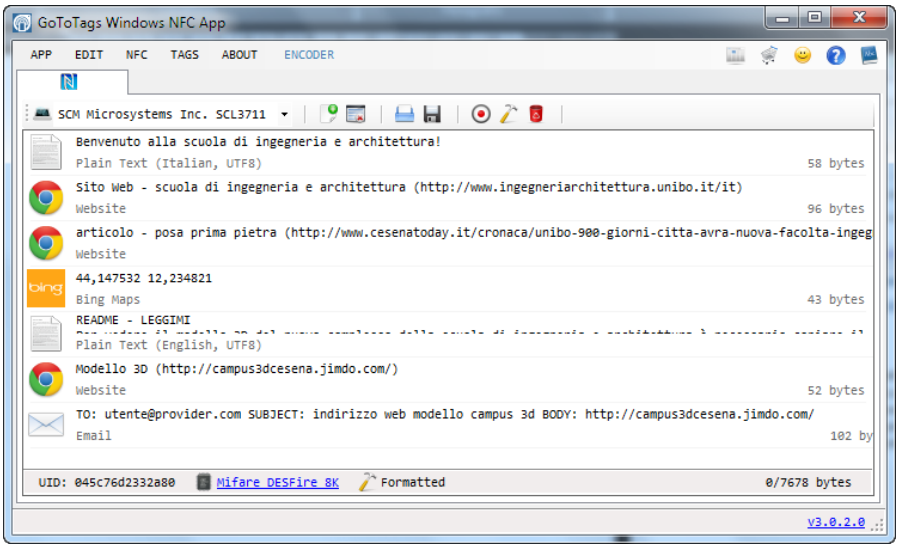

Figura 5.3: codifica dello Smart Brick in GoToTags.

5.4.1. FILE DI TESTO

Il primo file che è stato inserito è un file di testo con "benvenuto alla scuola di ingegneria e architettura" di cui si è descritta la codifica nella sezione 4.3.2. Si è deciso di essere concisi nel file di benvenuto poiché si è notato che nello smartphone i file di testo venivano letti se erano più corti di un centinaio di byte. Nel caso si usino testi più lunghi, i caratteri oltre i 100 byte non vengono visualizzati e pertanto sono persi. Questo succede perché non esiste un programma standard all'interno di Android per aprire i file testuali come avviene in ambiente Windows.

5.4.2 LINK WEB

In seguito al file di testo si sono inseriti due link a due indirizzi web. Il primo è quello già citato in sezione 4.3.2 ed è quello istituzionale del Campus, URL: http://www.ingegneriarchitettura.unibo.it/it . Il secondo link web è un link ad un articolo della giornale online "Cesena Today" che illustra la posa della prima pietra. URL: http://www.cesenatoday.it/cronaca/unibo-900-giorni-citta-avra-nuova-facolta-ingegneria-e-architettura.html .

5.4.3 COORDINATE GEOGRAFICHE

All'interno del mattone si sono anche inserite le coordinate geografiche dell'indirizzo di via Nicolo Machiavelli dove sorgerà il nuovo Campus, ovvero 44.147532° Nord e 12.234821° Est. Nella figura 5.3 si può notare il nome Bing, questo è il motore di ricerca di mappe stradali sul quale viene effettuata la ricerca delle coordinate inserite.

5.4.4 MODELLO 3D CON CODICE MATLAB – FORMATO TESTUALE

Non potendo caricare le immagini, si è pensato di realizzare un file che contenesse tutte le coordinate dei punti chiave dell'edificio in formato testuale. L'applicazione di questa idea non forniva all'utente una visione chiara dell'edificio, così si è realizzato un modello 3D in Matlab che riproducesse la struttura esterna dell'edificio. Successivamente alla realizzazione del modello, abbiamo salvato tutto il codice in questo file di testo in modo che rimanesse all'interno dello Smart Brick.

Per la creazione del modello si sono utilizzate le planimetrie del progetto architettonico del Campus su cui sono state effettuate misurazioni per fare una previa mappa dei punti. In Matlab si sono sfruttate le funzioni: "plot3" necessaria a graficare plot in tre dimensioni, "surf" per creare delle maschere per le superfici. Il resto del codice è composto da una lunga serie di terne di vettori che rappresentano le coordinate x,y,z di ogni piano realizzato. Si è programmato il modello affinchè venisse visualizzata una prima figura, in cui appare un subplot composto dalla singola veduta di ogni piano (figura 5.4); mentre nella seconda figura c'è un plot complessivo dell'edifico (figura 5.5). I grafici sono stati impostati in modo che i piani fossero di diversi colori per essere individuabili spostandosi dalla prima alla seconda figura.

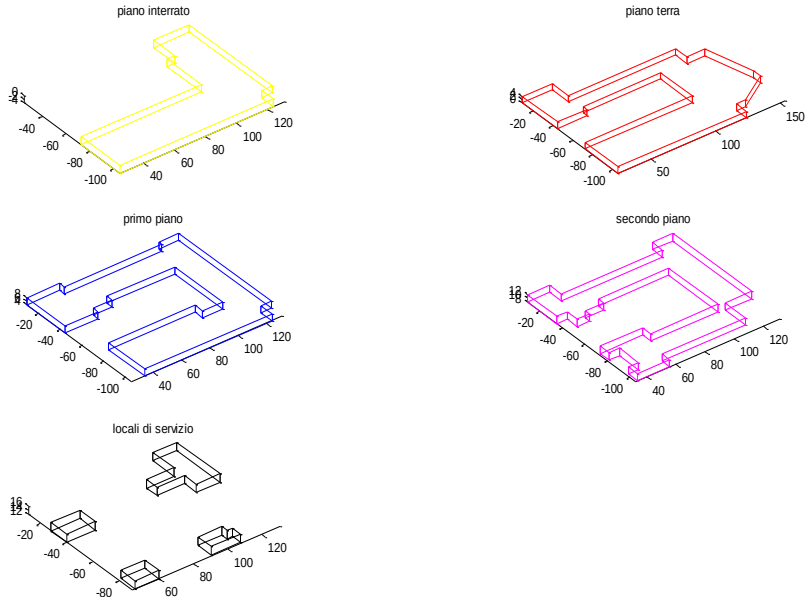

Figura 5.4: il subplot realizzato in Matlab con la visualizzazione di tutti i piani.

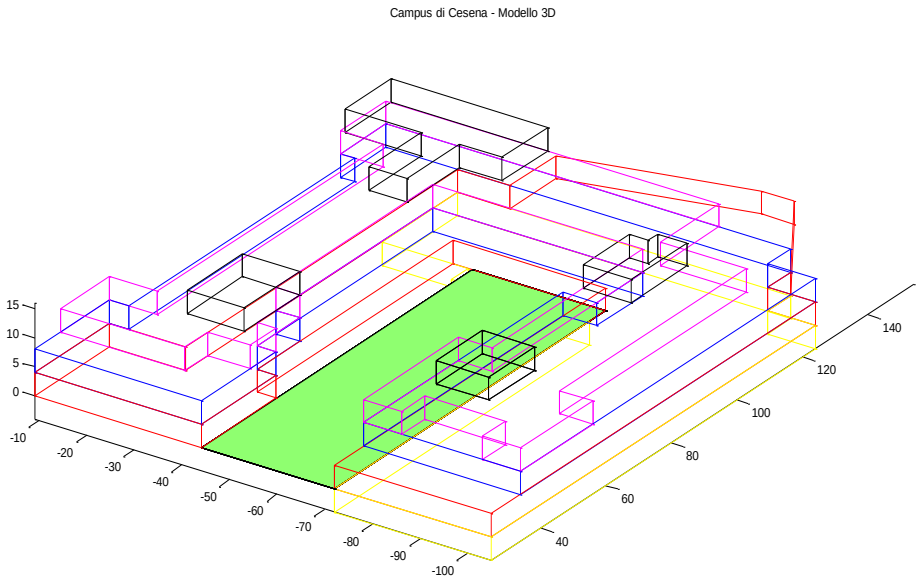

Figura 5.5: modello 3D dell'edificio.

```
%
%REALIZZATO DA LAGHI MARIO
%
ptx=[25 124 124 131 154 154 145 131 131 48 48 25 25 48 48 108 108 25 25];
pty=-[105 105 95 95 80 73 36 36 25 25 9 9 44 44 40 40 72 72 105];
ptz=zeros(1,19);
p1x=[34 124 124 131 131 117 117 48 48 25 25 48 48 61 61 109 109 95 95 34 34];
p1y=-[105 105 95 95 10 10 13 13 9 9 44 44 40 40 35 35 79 79 72 72 105];
p1z=zeros(1,21)+4;
ptsx=[25 25 124 124 124 124 124 124 131 131 131 154 154 154 154 154 154 145 145 145 131 131 131 131 131 131 48 48 48
48 48 48 25 25 25 25 25 25 48 48 48 48 48 48 108 108 108 108 108 108 25 25 25 25];
ptsy=-[105 105 105 105 105 95 95 95 95 95 95 80 80 80 73 73 73 36 36 36 36 36 36 25 25 25 25 25 25 9 9 9 9 9 9 44 44 44 44
44 44 40 40 40 40 40 40 72 72 72 72 72 72 105];
ptsz=[0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4];
p1sx=[34 34 124 124 124 124 124 124 131 131 131 131 131 131 117 117 117 117 117 48 48 48 48 48 48 25 25 25 25 25 25
48 48 48 48 48 48 61 61 61 61 61 61 109 109 109 109 109 109 95 95 95 95 95 34 34 34 34];
p1sy=-[105 105 105 105 105 95 95 95 95 95 95 10 10 10 10 10 10 13 13 13 13 13 13 9 9 9 9 9 9 9 44 44 44 44 44 44 40 40 40 40
40 40 35 35 35 35 35 35 79 79 79 79 79 79 72 72 72 72 72 72 105];
p1sz=[0 4 4 0 4 4 ptsz]+4;
p2x=[34 56 56 113 113 131 131 117 117 48 48 33 33 40 40 48 48 61 61 109 109 63 63 34 34 41 41 34 34];
p2y=-[105 105 98 98 80 80 10 10 19 19 9 9 35 35 44 44 40 40 35 35 79 79 72 72 80 80 97 97 105];
p2z=zeros(1,29)+8;
p2sx=[34 34 56 56 56 56 56 56 113 113 113 113 113 113 131 131 131 131 131 131 117 117 117 117 117 117 48 48 48 48 48 48
33 33 33 33 33 33 40 40 40 40 40 40 48 48 48 48 48 48 61 61 61 61 61 61 109 109 109 109 109 109 63 63 63 63 63 63 34 34 34
34 34 34 41 41 41 41 41 41 34 34 34 34];
p2sy=-[105 105 105 105 105 98 98 98 98 98 98 80 80 80 80 80 80 10 10 10 10 10 10 19 19 19 19 19 19 9 9 9 9 9 9 35 35 35 35
35 35 44 44 44 44 44 44 40 40 40 40 40 40 35 35 35 35 35 35 79 79 79 79 79 79 72 72 72 72 72 72 80 80 80 80 80 80 97 97 97
97 97 97 105];
p2sz=[0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 0 4 4 ptsz]+8;
cas1x=[46 60 60 46 46 46 60 60 60 60 60 60 46 46 46 46];
cas1y=-[90 90 79 79 90 90 90 90 90 79 79 79 79 79 79 90];
cas1z=[12 12 12 12 12 16 16 12 16 16 12 16 16 12 16 16];
cas2x=[91 108 108 105 105 91 91 91 108 108 108 108 108 108 105 105 105 105 105 105 91 91 91 91];
cas2y=-[89 89 83 83 79 79 89 89 89 89 89 83 83 83 83 83 83 79 79 79 79 79 79 89];
cas2z=[12 12 12 12 12 12 12 16 16 12 16 16 12 16 16 12 16 16 12 16 16 12 16 16];
cas3x=[117 131 131 117 117 101 101 117 117 117 131 131 131 131 131 131 117 117 117 117 117 117 101 101 101 101 101
101 117 117 117 117];
cas3y=-[44 44 11 11 27 27 35 35 44 44 44 44 44 11 11 11 11 11 11 27 27 27 27 27 27 35 35 35 35 35 35 44];
cas3z=[12 12 12 12 12 12 12 12 12 16 16 12 16 16 12 16 16 12 16 16 12 16 16 12 16 16 12 16 16 12 16 16];
cas4x=[44 61 61 44 44 44 61 61 61 61 61 61 44 44 44 44];
cas4y=-[40 40 28 28 40 40 40 40 40 28 28 28 28 28 28 40];
cas4z=cas1z;
pintx=[25 124 124 131 131 108 108 103 103 25 25];
pinty=-[105 105 95 95 25 25 43 43 72 72 105];
pintz=zeros(1,11)-4;
pintsx=[25 25 124 124 124 124 124 124 131 131 131 131 131 131 108 108 108 108 108 108 103 103 103 103 103 103 25 25 25
25];
pintsy=-[105 105 105 105 105 95 95 95 95 95 95 25 25 25 25 25 25 43 43 43 43 43 43 72 72 72 72 72 72 105];
pintsz=-[4 0 0 4 0 0 4 0 0 4 0 0 4 0 0 4 0 0 4 0 0 4 0 0 4 0 0 4 0 0 4 0 0 4 0 0 4 0 0];
g1x=[25,108,108,25,25];
g1y=-[72,72,44,44,72];
[G1X,G1Y]=meshgrid(g1x,g1y);
G1Z=zeros(5);
figure (1); subplot(3,2,1); plot3(pintx,pinty,pintz,'-y',pintsx,pintsy,pintsz,'-y'), title('piano interrato'), axis ('equal');
figure (1); subplot(3,2,2); plot3(ptx,pty,ptz,'-r',ptsx,ptsy,ptsz,'-r'), title('piano terra'), axis ('equal');
figure (1); subplot(3,2,3); plot3(p1x,p1y,p1z,'-b',p1sx,p1sy,p1sz,'-b'), title('primo piano'), axis ('equal');
figure (1); subplot(3,2,4); plot3(p2x,p2y,p2z,'-m',p2sx,p2sy,p2sz,'-m'), title('secondo piano'), axis ('equal');
figure (1); subplot(3,2,5); plot3(cas1x,cas1y,cas1z,'-k',cas2x,cas2y,cas2z,'-k',cas3x,cas3y,cas3z,'-k',cas4x,cas4y,cas4z,'-k'),
title('locali di servizio'), axis ('equal');
figure (2); plot3(ptx,pty,ptz,'-r',p1x,p1y,p1z,'-b',ptsx,ptsy,ptsz,'-r',p1sx,p1sy,p1sz,'b',p2x,p2y,p2z,'-m',p2sx,p2sy,p2sz,'-
m',pintx,pinty,pintz,'-y',pintsx,pintsy,pintsz,'-y',cas1x,cas1y,cas1z,'-k'), axis ('equal'), title('Campus di Cesena - Modello 3D');
hold on;
figure (2); plot3(cas1x,cas1y,cas1z,'-k',cas2x,cas2y,cas2z,'-k',cas3x,cas3y,cas3z,'-k',cas4x,cas4y,cas4z,'-k');
figure (2); surf(G1X,G1Y,G1Z);
```

Figura 5.4: codice Matlab

5.4.5 LINK PER IL MODELLO 3D

Come visto in sezione 5.4.1, si sono constatati dei problemi per l'apertura effettiva dei file di testo su cellulare; infatti si è notato che sul Samsung S3 si riuscivano a visualizzare solo 2 righe dell'intero codice. Per creare qualcosa che potesse essere visualizzabile da tutti i dispositivi si è creato un sito web in cui si è inserita un piccola descrizione del modello 3D e il codice Matlab. All'interno dello Smart Brick si è così inserito anche il link a questo sito web. URL: http://campus3dcesena.jimdo.com/

5.4.6 BOZZA MAIL

L'ultima informazione contenuta dallo Smart Brick è una bozza mail contenente l'indirizzo web descritto in sezione 5.4.5. Questo è stato pensato per il fatto che l'utente può visualizzare il modello 3D solo sul computer. Quindi l'utente può può salvare la bozza nel proprio archivio o direttamente inviarla all'indirizzo del proprio computer e visualizzare il modello in un secondo momento.

CAPITOLO 6

CONCLUSIONI

In questo elaborato è stata trattata una delle più recenti tecnologie nell'ambito della radio frequenza, ovvero l'NFC. L'NFC non necessita l'utilizzo di Reader appositi come avviene nei sistemi RFID, bensì prevede di essere integrata nei dispositivi di comunicazione più comuni, ovvero gli smartphone. Pertanto questa tecnologia, sfruttando la modalità di funzionamento "card emulation", potrebbe permettere allo smartphone di rendere obsolete le attuali carte magnetiche.

Un punto di forza dell'NFC è il protocollo di comunicazione che offre una "backward compatibility", cioè permette ai cellulari abilitati di comunicare anche con i protocolli RFID ISO14443 e ISO15693. Questo è risultato utile nella sperimentazione infatti è stata utilizzata una Smart Card aderente ISO14443 che permetteva di utilizzare fino a 8k di memoria, unico Tag passivo con un simile spazio di archiviazione.

Una caratteristica innovativa è lo standard NDEF che ci permette di codificare le informazioni in un modo comprensibile per tutti i cellulari abilitati NFC. Si è riusciti a immagazzinare una serie di informazioni all'interno dello Smart Brick e successivamente a leggerle con più dispositivi abilitati. Lavorando con questo standard si è capito che la tecnologia NFC è una tecnologia non adatta allo scambio dati, sia per la velocità che per le memorie dei dispositivi in gioco, mentre potrebbe essere definita un link-tecnology, ossia in grado di interagire con più tecnologie. Nel nostro caso infatti è indispensabile che l'NFC sia affiancato da WIFI o dall'UMTS per poter sfruttare le risorse che si intendono inserire in un Tag. Gli stessi esempi della teoria lo confermano, come il pairing del bluetooth trattato nella sezione 3.2.2.

Per quanto riguarda la distanza di funzionamento, si è capito che la distanza non può essere migliorata agendo sul dispositivo passivo, bensì è necessario agire sul Reader. Per aumentare i range di comunicazione sarebbe necessario innalzare la forza del campo magnetico generata da questi dispositivi. Quindi un eventuale aumento della distanza dipende dalle aziende che producono gli smartphone. Inoltre si è notato che lo stesso package può incidere sulla distanza di funzionamento; infatti Reader e Smartphone lavorano a distanze operative diverse.

Per quanto concerne lo Smart Brick si possono evidenziare alcuni aspetti positivi soprattutto in ambito di sicurezza. Infatti utilizzando il Tag all'interno di un mattone e non nella forma di etichetta si possono evitare molti attacchi esterni. Per questo un eventuale hacker che voglia manipolare i dati contenuti nello Smart Brick o sostituire il Tag dovrebbe manomettere il mattone.

BIBLIOGRAFIA

1. K. Finkenzeller, RFID Hanbook: fundamentals and Application in contactless Smart Cards and Identification, Munich, Wiley, 2003.
2. S. Focardi, I. Massa, A.Uguzzoni: Fisica Generale. Elettromagnetismo, Milano, Casa Editrice Ambrosiana, 2009.
3. C. Marechal and D. Paret, "The Loading Effect of Proximity Contactless Smart Card. Incidences of Impedance of the Shunt Regulator.," Int Conf. On *Wireless Communications, Networking and Mobile Computing, WiCOM '08,* Oct. 2008.
4. P. Cambriani, Realizzazione di un beamforming analogico per sistemi RFID, Tesi di dottorato di Ricerca in "Ingegneria delle Telecomunicazioni e Microelettronica", Università degli Studi di Roma Tor Vergata.
5. L. Barbieri, Progetto e sviluppo di un ambiente in grado di controllare, programmare e gestire etichette intelligenti basate sulla tecnologia RFID, Tesi di Laurea in Ingegneria Elettronica, Università degli studi di Genova.
6. N. Bertolini, Realizzazione infrastrutture per Accesso ai servizi tramite carte multifunzione, Tesi di laurea in ingegneria informatica, Università degli studi di Padova.
7. ISO\IEC, Final comittee draft ISO 14443: Identification cards – Contactless integrated circuit(s) cards – Proximity cards, 1999.
8. G. Iannaccone, Lezioni de "Infrastrutture elettroniche per l'habitat", Università degli studi di Pisa. On Line: http://www.iet.unipi.it/g.iannaccone/infrastrutture/lucidi_2005/lezioni_18_22_aprile_2005.pdf
9. SCM Microsystems, SCL3711 Contactless Reader & NFC enabling accessory**.** On line: http://www.identive-group.com/images/pdfs/datasheets/en/Dat_SCL3711_e.pdf
10. SCM Microsystem, SCL3711 Reference Manual v1.5 Multiprotocol contactless mobile Reader. Online: http://www.identiveinfrastructure.com/fileadmin/products/datasheets/SCL3711.MANUAL.VER15.pdf
11. Philips, COntactless Multi-Application IC with DES and 3-DES security Mifare Desfire, Product Short Form Specification Revision 3.0, 2004.
12. NXP, Mifare Desfire as Type 4 Tag, application Note, Rev. 2.4, 2013.
13. NXP, MF1S503x MIFARE Classic 1K - Mainstream contactless smart card IC for fast and easy solution development, Product Data Sheet, Rev. 3.1, 2011.
14. NXP, NFC controller PN544 for mobile phones and portable equipment. On Line: http://www.nxp.com/documents/leaflet/75016890.pdf
15. F. Meo, Near Field Communication (NFC): interazione fisica-interazione virtuale, Tesi di laurea magistrale in Economia e Gestione delle Aziende, Università Ca'

Foscari Venezia.
16. C. Perrotta, Studio della tecnologia NFC e sperimentazioni in applicazioni per il tracciamento , Tesi di Laurea in Ingegneria Informatica, Università degli Studi di Napoli Federico II.
17. NFC FORUM, Smart Poster Record Type Definition, technical specification, 2006.
18. P. Talone e G. Russo, Rfid: tecnologie e applicazioni, Fondazione Ugo Bordoni. On line: http://www.rfid.fub.it/edizione_2/rfid_fondamenti_tecnologia_2.htm
19. NFC FORUM: http://www.nfc-forum.org/resources/N-Mark/
20. N. Pelly, J. Hamilton, Google Developer Conference, San Francisco, 2011. On line: http://www.google.com/events/io/2011/sessions/how-to-nfc.html
21. V. Coskun, K. Ok, B. Ozdenizci, Near Field Communication: from Theory To Practice, Istanbul, Wiley, 2012.
22. NFC FORUM, NFC Record Type Definition (RTD), technical specification, 2006.
23. NFC FORUM, NFC Data Exchange Format (NDEF), technical specification, 2006.
24. A.Ashon and M.Ilyas, NFC Handbook, Boca Raton, CRC Press, 2012.
25. ECMA international: http://www.ecma-international.org/publications/standards/Ecma-340.htm
26. ECMA international, NFCIP-1,Near Field Communication – Interface and Protocol, Standard ECMA-340: http://www.ecma-international.org/publications/files/drafts/tc47-2008-002.pdf
27. ECMA international, NFCIP-2,Near Field Communication – Interface and Protocol, Standard ECMA-352: http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-352.pdf
28. NFC FORUM, Signature Record Type Definition, technical specification, 2006.
29. NXP, NFC controller, objective short datasheer, 2007.
30. Sito web Gototags: http://support.gototags.com/entries/25059248-Encode-NFC-Tags

Ringraziamenti

Arrivati al conseguimento di un grande obbiettivo come questo della laurea in ingegneria, è necessario guardarsi indietro e ringraziare tutti quelli che hanno contribuito a questo successo.

La prima persona a cui vanno i più sentiti ringraziamenti è senza dubbio il professor Chiani che mi ha permesso di svolgere una tesi di grande interesse personale. Inoltre se devo essere sincero sentirsi dire "ottimo lavoro" da un professore del suo calibro ha un gusto particolare. Subito a ruota ringrazio l'ingegner Mariani per la disponibilità, la gentilezza e il tempo che mi ha concesso, senza le sue indicazioni e i suoi suggerimenti questo elaborato non avrebbe mai raggiunto gli obbiettivi iniziali. Inoltre ringrazio l'ingegner Vitucci per il suo supporto.

A questo punto è inevitabile che ringrazi la ragazza che mi è stata a fianco in questo sprint finale: la mia Fede, in tutti i sensi. Ha sopportato il mio stress e i miei nervosi cronici, senza batter ciglio.. No questo non è vero, però mi è sempre stata a fianco, mi ha sorretto nei momenti più bui e spero di poter essere alla sua altezza quando sarà il mio turno.

A questo punto comincia la parte difficile, ovvero ricordarsi tutte le persone che hanno accompagnato il mio cammino e voi sapete quanto sia breve la mia memoria.

Grazie a mia sorella Isa, a Sandro e a Fede per avermi mostrato sostegno e per avermi sempre ascoltato.

Grazie a Enrico, amico e compagno fidato, con cui ho iniziato quest'avventura. Lo ringrazio perché ha sempre trovato tempo per aiutarmi anche nei giorni peggiori e nelle settimane più concitate, i suoi appunti sono diventati spesso i miei libri di testo, senza di te non sarei qua.

Grazie a Malto e a Cava che hanno condiviso con me le difficoltà e le gioie di quest' università e con cui ho passato le mie serate più belle.

Grazie a Fabio che conosco da quando sapevo a mal la pena contare. E' stato sempre uno dei miei punti di riferimenti e un amico prezioso.

Grazie a Pietro che conosco ormai da 13 anni e con cui non ho mai litigato. Lo ringrazio per la sua pazienza, per il suo supporto e per le serate passate assieme, e per aver sempre guidato lui. Ringrazio assieme a Pietro anche Marco per avermi rimesso in forma dopo una lunga sosta obbligata.

Grazie a Pole e a Jack che in questi anni mi hanno sempre fatto ridere come poche persone, e mi hanno alleggerito spesso da ansie varie.

Grazie a Prato e Mambo, compagni di tante battaglie a pallone, senza di voi forse avrei smesso molto prima di giocare a pallone.

Grazie a Checco e Giamma che nonostante le diverse strade intraprese, qualche volta riusciamo ancora a vederci e farci qualche risata assieme.

Grazie a tutti i miei compagni della vecchia Enterprise che hanno reso questi anni molto più leggeri. E ringrazio anche mister Taba con cui ho condiviso la mia riabilitazione dopo la rottura del crociato.

Grazie a tutti i miei compagni dell'università e in particolare Andrea, Davide, Simone, Dave e Manuel che mi hanno aiutato in innumerevoli esami.

Grazie a tutti coloro che mi sono stati a fianco, che mi hanno sostenuto e soprattutto quelli che mi hanno fatto ridere in questi 5 anni. Scusatemi se non vi ho menzionati tutti.

Per ultimi ma non in ordine d'importanza ringrazio la mia unica certezza: i miei genitori che mi sono stati vicini nei momenti felici e in quelli meno felici, mi hanno dato un sostegno incondizionato veramente unico.