POLITECNICO DI BARI

DIPARTIMENTO DI INGEGNERIA ELETTRICA E DELL'INFORMAZIONE

CORSO DI LAUREA MAGISTRALE IN INGEGNERIA INFORMATICA

Tema d'anno di Sicurezza Informatica

Da RFID a NFC: la ricetta medica digitale

Docente del corso:

Prof. Giuseppe Mastronardi

Studente:

Basile Giorgio

Sommario

Capitolo 1

Radio-Frequency IDentification

1.1 Panoramica

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 storage 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, in caso contrario si trattava di aerei 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. 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

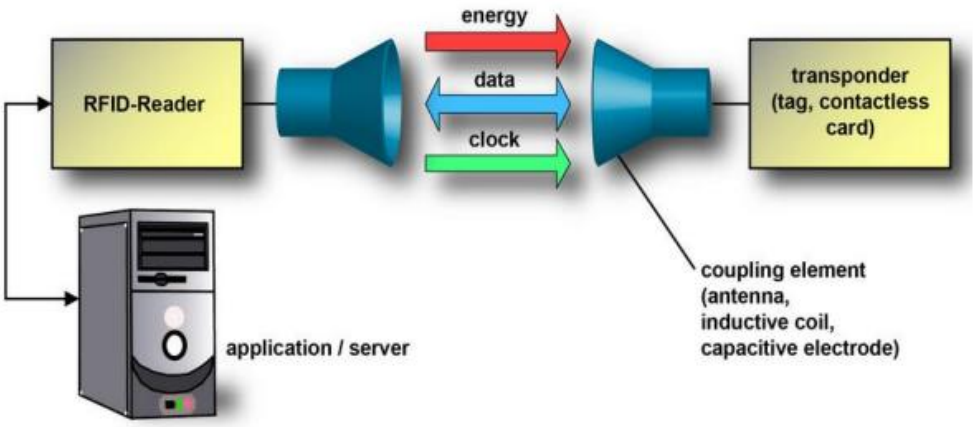


Figura 1. Schema concettuale di un sistema RFID

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.

1.2 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.

1.2.1 Tag passivi

Privi di batterie o altre fonti di alimentazione, i Tag Passivi (Figura 3) 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. 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. 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. Si può quindi suddividere il Tag passivo in tre sezioni fondamentali, mostrate in Figura 2.

Figura 2. Schema a blocchi di un Tag RFID 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.

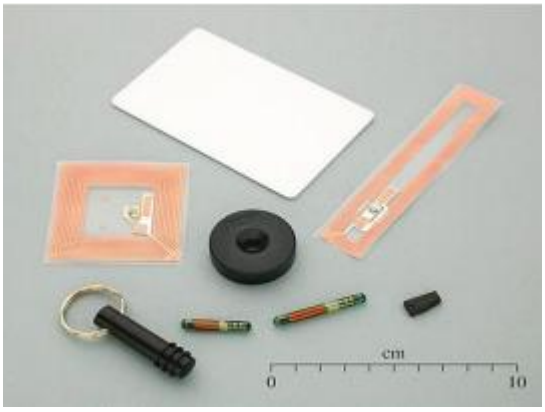


Figura 3: alcuni esempi di package per Tag passivi RFID

1.2.2 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. 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.

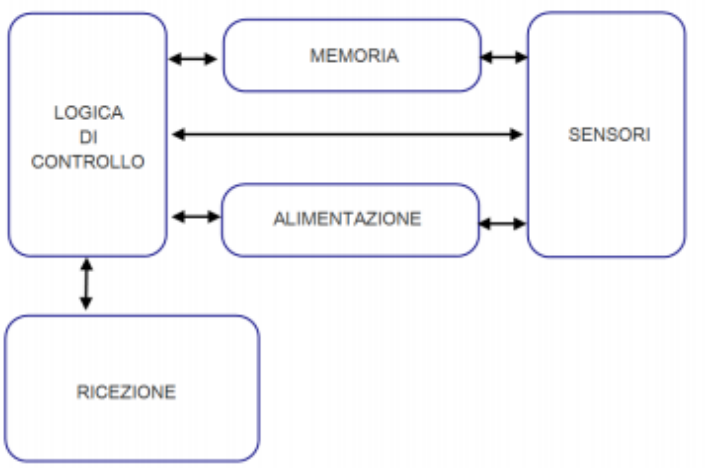


Figura 4. Schema a blocchi di un Tag semi-attivo

1.1.3 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. 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.

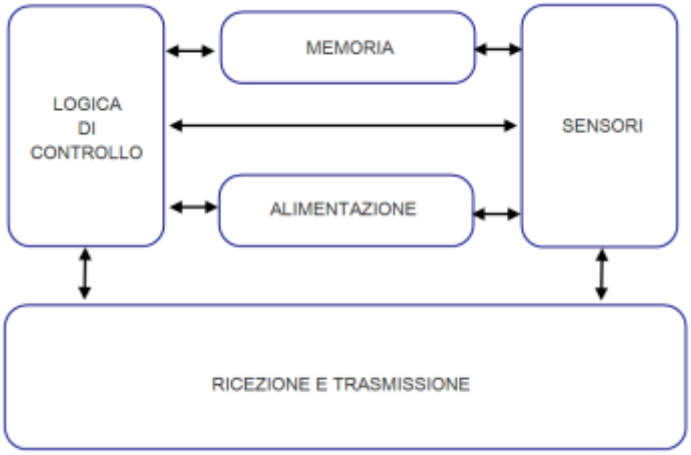


Figura 5. Schema a blocchi di un Tag attivo

1.3 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, oppure mobili, con dimensioni ridotte e simili ai lettori di codice a barre. Nei successivi capitoli verrà sottolineato che nella tecnologia NFC i Reader possono raggiungere dimensioni ancora inferiori.

1.4 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 865-870 Mhz per l'Europa, 902-928 MHz 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*: *Super High Frequency*, con banda centrata sulla frequenza di 2.4 Ghz 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 13.56 MHz, 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.

1.5 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.

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.

Capitolo 2

Near-Field Communication

2.1 Da RFID ad NFC

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'obiettivo 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'obiettivo 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'obiettivo 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:

a) Permettere la comunicazione tra due dispositivi posti a breve distanza, considerando un range di comunicazione massimo di 10 cm.
b) Integrare la tecnologia in dispositivi attivi che possano operare sia in modalità Tag, sia in modalità Reader, come avviene negli smartphone.
c) 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%.
d) Garantire la compatibilità con le carte ISO/IEC 14443 e opzionalmente con il protocollo ISO/IEC 15693.

Lo standard NFC affonda le sue radici nella tecnologia RFID, ed ha dovuto attraversare un lungo processo di testing e standardizzazione, del quale si riportano alcuni punti salienti:

- 1983 Il primo brevetto a essere associato con l'abbreviazione RFID è stata concesso a Charles Walton
- 2004 Nokia, Philips e Sony stabiliscono la Near Field Communication (NFC) Forum
- 2006 Vengono definite le specifiche iniziali per i tag NFC
- 2006 vengono definite le specifiche per "SmartPoster" Records
- 2006 il Nokia 6131 è il primo telefono che integra la tecnologia NFC (nella sua variante 6131 NFC)

- 2009 Nel mese di gennaio, NFC rilascia lo standard Peer-to-Peer per trasferire i contatti, URL, avviare Bluetooth, ecc
- 2010 Samsung Nexus S, viene mostrato come il primo telefono Android con NFC
- 2011 al Google I/O viene mostrato "How to NFC", che dimostra come l'NFC possa essere usato per avviare un gioco e condividere un contatto, URL, app, video, ecc.
- 2011 la RIM è la prima compagnia che per i suoi dispositivi ottiene la certificazione di MasterCard Worldwide, per le funzionalità di PayPass; successivamente nel gennaio del 2012 Visa certifica sia gli smartphone BlackBerry sia Android per i pagamenti "Visa payWave"
- 2012 Sony introduce gli “Smart Tags”, che fanno uso della tecnologia NFC per cambiare modalità e profilo di utilizzo di uno smartphone Sony a stretto contatto. Tali tag vengono inclusi nella confezione del Sony Xperia P, uscito lo stesso anno
- 2013 Samsung e Visa annunciano una partnership per lo sviluppo di sistemi di pagamento elettronici
- 2013 Il gruppo di ricerca di IBM a Zurigo, nel tentativo di combattere frodi e problemi di sicurezza, sviluppa un nuovo sistema di autenticazione per sistemi mobili basato su NFC.
- 2014 La Apple annuncia Apple Pay, un sistema di pagamento NFC per i nuovi iPhone 6, iPhone 6 Plus e Apple Watch

2.2 Differenze e affinità

Nel capitolo 1 si è svolta una panoramica sul background tecnologico dell’NFC. Ora si vogliono elencare le differenze e le analogie tra RFID e NFC:

- 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. In NFC, invece, gli applicativi funzionano sempre nel cosiddetto campo vicino dove avviene solo accoppiamento induttivo.
- Come si è discusso nella sezione 1.3, 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 10 cm, 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.

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.
- 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.

2.3 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.

Per Hamilton e Pelly l'NFC è una tecnologia di comunicazione wireless a corto raggio simile al Bluetooth e al Wi-Fi ma che si differenzia da queste sostanzialmente per la distanza alla quale avviene la comunicazione, che in queste due tecnologie è molto maggiore. Inoltre, Wi-Fi e Bluetooth a livello di rete 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.

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 Wi-Fi. 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 Wi-Fi 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 Wi-Fi 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.

2.4 Modalità 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. Se ad esempio si utilizza uno smartphone che utilizza un sistema operativo Android, 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.

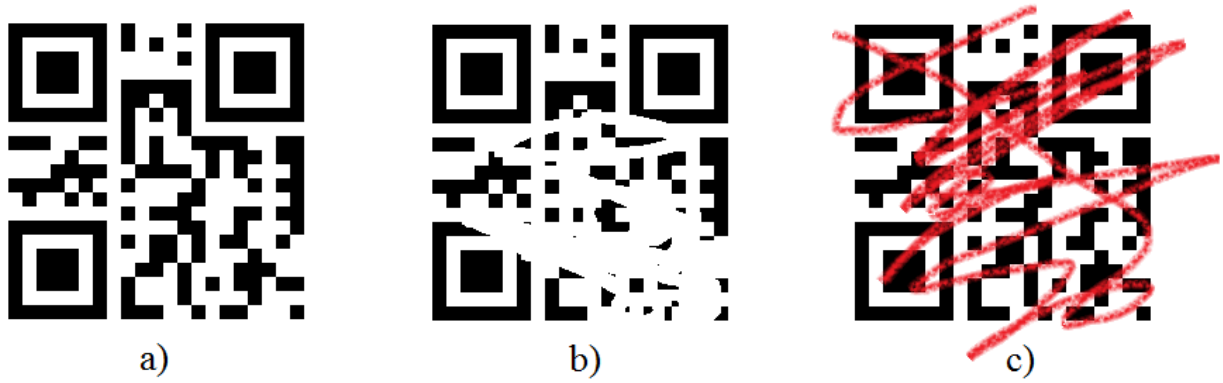


Figura 6. a) QR Code codificati con l'url: http://www.poliba.it in figura b) il QR Code originale, in figura b) esempio di QR Code non leggibile a causa della superficie rovinata, in figura c) QR Code compromesso a causa di una macchia.

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. 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.

2.5 NFC Data Exchange Format: NDEF

2.5.1 Struttura dei messaggi

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. Ogni messaggio NDEF è il costrutto fondamentale definito dalla specifica NDEF, che deve essere scambiato in modalità *read* o *peer-to-peer*. E' composto di uno o più record NDEF come si vede in figura 3.2.

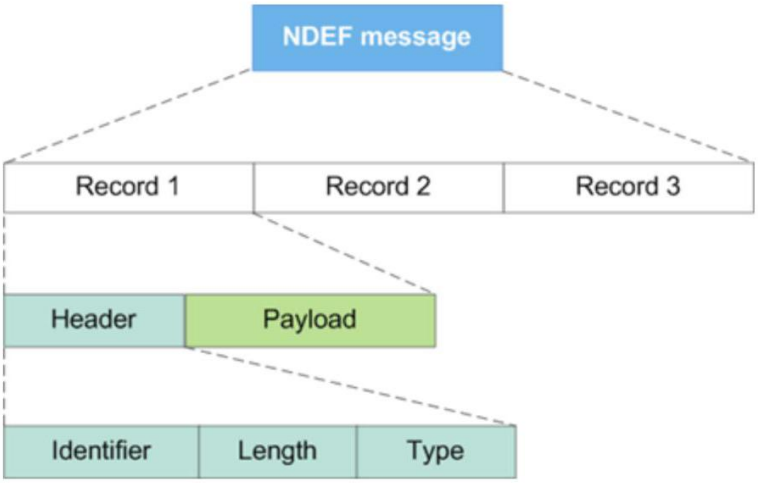


Figura 7. Composizione di un messaggio NDEF

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 8. Struttura di un record NDEF

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

1. Un byte che contiene i flag di stato del record NDEF, che possono essere:
    - MB: flag Message Begin, che indica il record del primo messaggio
    - ME: flag Message End, che ne indica la fine
    - 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
    - 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, come mostrato in figura 9. 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.	

Figura 9. Possibili valori del campo TNF

2. Un campo TYPE_LENGTH che indica la lunghezza in byte del campo TYPE
3. Un campo ID_LENGTH che indica la lunghezza in byte del campo ID, presente solo se è stato settato il flag ID_LENGTH
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.

2.5.2 Tipologie di record: 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.

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.

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.

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.

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. Il concetto di "Smart" indica capacità di rendere interattivo un messaggio NDEF. 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.

2.6 Sicurezza e attacchi

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 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.

2.6.1 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 esposte 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 il DES, il 3DES (Triple Data Encryption Standard) e la AES (Advanced Encryption Standard). D'altra parte, è anche possibile utilizzare i medesimi algoritmi per cifrare i dati da scrivere su un tag. In tal caso il livello di sicurezza non è più nel canale ma insito nei dati stessi. Il reader autorizzato dovrà però ovviamente disporre della chiave.

2.6.2 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.

2.6.3 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.

2.6.4 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.

2.6.5 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 3

La ricetta medica digitale: NFC & Android

3.1 La ricetta medica Italiana

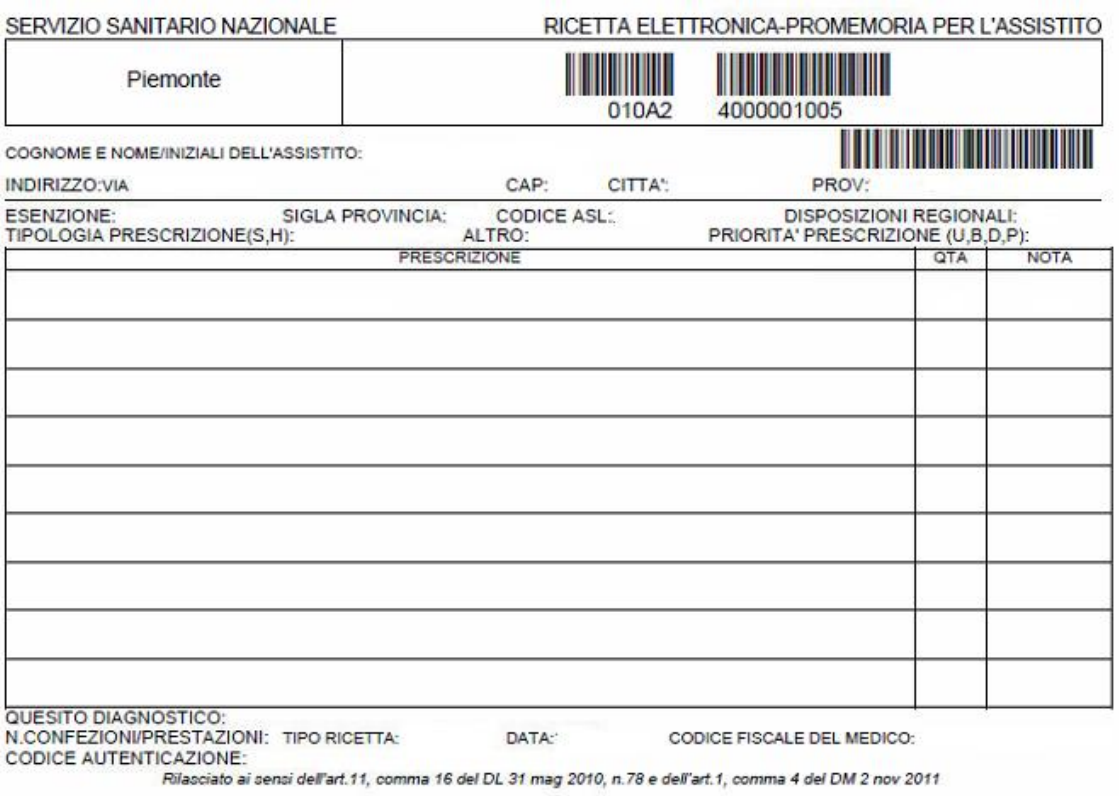
In questo lavoro, è stata analizzata la possibilità di utilizzare NFC a supporto della digitalizzazione della ricetta medica nel formato italiano. E' facile comprendere come l'emissione di un documento cartaceo per ogni prescrizione dei medici italiani sia uno spreco sia in termini economici, quantificato in circa 1 milione di euro al giorno.

Il Governo Italiano ha introdotto per la prima volta il concetto di ricetta medica digitale nel piano e-Gov 2012[1], prevedendo con D.M. del 21 febbraio 2011, il processo di entrata a regime della trasmissione per via telematica dei dati delle ricette da parte dei medici prescrittori, con la conseguente riduzione, teorica, del quantitativo di carta necessaria all'emissione. Purtroppo, ad oggi la cosiddetta ricetta "dematerializzata" è in fase di prima sperimentazione e presenta alcuni punti piuttosto equivoci.

Nel modello previsto, I medici non ricevono più blocchi di ricette cartacee, ma una serie di numeri. Quando devono prescrivere un farmaco si connettono al sistema sanitario via computer e inseriscono il codice fiscale dell'assistito, a cui possono quindi associare uno dei numeri-ricetta. Il sistema analizzerà il codice fiscale e tutte le informazioni di esenzione (per reddito e/o per patologia). Il medico compilerà quindi la ricetta sul computer e consegnerà al paziente un semplice promemoria su carta bianca, da usare solo se nella farmacia manca la linea al momento della consegna del farmaco o è presente un malfunzionamento nei server dedicati. Altrimenti, al farmacista basta inserire il numero della ricetta e il codice fiscale per visualizzare la prescrizione, con gli eventuali sconti ed esenzioni previsti per quel paziente. Si potrà usare lo stesso sistema anche per la prescrizione, da parte del medico di famiglia, di analisi nei laboratori o visite specialistiche. Un sistema di questo tipo introdurrebbe un risparmio economico notevole riguardante l'emissione da parte della Zecca dello stato delle "ricette rosse", che costano 40 centesimi ciascuna. Inoltre, eviterebbe gli errori di lettura degli erogatori, che

Questa visione si scontra con alcune criticità ancora da sciogliere. Innanzitutto, è ancora prevista la stampa di un promemoria (Figura 10), per permettere ai pazienti di poter usufruire della prescrizione anche in caso di malfunzionamento del sistema centrale. Ciò significa che, almeno al momento, lo spreco di carta è tutt'altro che ridotto, sebbene vi sia un netto risparmio economico precedentemente analizzato. In secondo luogo, almeno nella prima fase sul promemoria sarà stampato un codice a barre che identificherà la prescrizione effettuata, in quanto il sistema centralizzato entrerà in funzionamento soltanto in una seconda fase. Ovviamente, il codice a barre si presta a tutti i problemi di leggibilità analizzati nel precedente capitolo, come il deterioramento o la compromissione in seguito a una macchia.

[1] http://www.funzionepubblica.gov.it/media/872560/aggiornamento%20piano%20e-gov.pdf



SERVIZIO SANITARIO NAZIONALE — RICETTA ELETTRONICA-PROMEMORIA PER L'ASSISTITO

Piemonte — 010A2 — 4000001005

COGNOME E NOME/INIZIALI DELL'ASSISTITO:

INDIRIZZO:VIA CAP: CITTA': PROV:

ESENZIONE: SIGLA PROVINCIA: CODICE ASL: DISPOSIZIONI REGIONALI:
TIPOLOGIA PRESCRIZIONE(S,H): ALTRO: PRIORITA' PRESCRIZIONE (U,B,D,P):

PRESCRIZIONE	QTA	NOTA

QUESITO DIAGNOSTICO:
N.CONFEZIONI/PRESTAZIONI: TIPO RICETTA: DATA: CODICE FISCALE DEL MEDICO:
CODICE AUTENTICAZIONE:

Rilasciato ai sensi dell'art.11, comma 16 del DL 31 mag 2010, n.78 e dell'art.1, comma 4 del DM 2 nov 2011

Figura 10. Il promemoria rilasciato ai pazienti ad ogni prescrizione

In questo scenario, l'eliminazione completa del supporto cartaceo, anche in caso di utilizzo del sistema telematico appena descritto si rende doverosa. E' però tenere bene in mente che l'urgenza di alcune prescrizioni non può tollerare alcun malfunzionamento del sistema, né una mancanza di connessione a internet sia per il prescrittore (medico) che per l'erogatore (farmacista). L'utilizzo della tecnologia NFC si presterebbe bene a questo ruolo, introducendo peraltro tutti i vantaggi esposti nel precedente capitolo, legati alla sicurezza e alla maggiore robustezza del dato digitale in quanto non deteriorabile facilmente come nel caso di codici a barre o QR.

Nel presente lavoro è stato sviluppato un sistema che fa uso di Tag NFC per la memorizzazione di una prescrizione medica, nel formato attualmente previsto per la ricetta rossa. In particolare, sono state sviluppate due applicazioni: la prima simula il software posseduto dal medico per la prescrizione, dal quale può selezionare il paziente dal suo database, prescrivere una serie di farmaci previsti dal Sistema Sanitario Nazionale e al termine salvare la ricetta completa in un Tag NFC, dopo opportuna cifratura; la seconda funge da Reader NFC, in grado di decrittare i dati salvati, parsarli e infine visualizzare la ricetta ivi contenuta.

I farmaci prescrivibili sono stati ottenuti attraverso gli Open Data[2] messi a disposizione dall'*Agenzia Italiana del Farmaco* (AIFA). La licenza di distribuzione dei dati utilizzata da AIFA è la CC-BY (attribuzione) nella versione 4.0. Questa licenza permette a terzi di distribuire, modificare, ottimizzare ed utilizzare i dati, anche commercialmente, con l'obbligo di citare la fonte. IFA rende disponibili i dati per facilitarne la consultazione, il riutilizzo e la distribuzione in diversi

[2] http://www.agenziafarmaco.gov.it/it/content/open-data

formati (xml, csv, pdf). Il file csv (*comma separated value*) è un formato testuale che consente di distribuire dati in formato tabellare: possono essere letti con software open (calc di OpenOffice) o con software proprietari come Excel di Microsoft o semplicemente con editor testuale (NotePad).

In particolare, è stato utilizzato il file csv con le tabelle contenenti l'elenco dei farmaci di fascia A, dispensati dal Servizio sanitario Nazionale, ordinati per principio attivo e per nome commerciale, al fine di consentire, per tutti gli Operatori sanitari, la prescrizione per principio attivo disposta dall'articolo 15, comma 11-bis, del decreto legge 6 luglio 2012 n.95, convertito con modificazioni dalla Legge 7 agosto 2012 n. 135.

Per quanto riguarda la sicurezza, NFC utilizza algoritmi di cifratura della comunicazione tra dispositivi. Nel caso della ricetta medica digitale è però fondamentale, per questioni di privacy, salvare dati crittografati nei Tag, in modo che il contenuto non sia leggibile in caso di smarrimento o furto. Nel presente lavoro è stata prevista la possibilità di utilizzare due algoritmi di cifratura simmetrica: il DES (Data Encryption Standard) e il 3DES (Triple Data Encryption Standard). In questo modo solo le applicazioni autorizzate (che dovrebbero essere, nell'implementazione ufficiale, quelle del Servizio Sanitario Nazionale) potrebbero decodificare i dati, essendo a conoscenza della chiave di cifratura.

3.2 Utilizzo di NFC in Android

Figura 11. Pagamenti NFC con Android

Il sistema operativo Android, di proprietà di Google Inc., è stato uno dei primi sistemi operativi a supportare la tecnologia NFC in maniera completa, consentendo lo sviluppo di diversi applicativi che ne sfruttano le potenzialità. Android supporta attraverso le sue API l'utilizzo di messaggi

NDEF, facilitandone le operazioni di lettura e scrittura. Inoltre, Android Developers[3] fornisce un completo tutorial che descrive le modalità di funzionamento e le convenzioni adottate.

L'utilizzo dello standard NDEF è fortemente consigliato, in quanto utilizzando le librerie messe a disposizione, è possibile evitare errori nella composizione dei messaggi, nella scrittura dei flag e nella lettura dei byte ad essi associati. Nel caso di utilizzo di NDEF, Android prevede due casi d'uso principali:

- Lettura di dati NDEF da un Tag NFC
- Invio di messaggi NDEF da un dispositivo ad un altro utilizzando Android Beam™

La lettura di dati NDEF da un Tag NFC viene effettuata dal cosiddetto Tag Dispatch System, che analizza i Tag rilevati, ne categorizza i dati contenuti, ed avvia un' applicazione in grado di processare tali informazioni. Un'applicazione interessata a un certo tipo di dati deve dichiarare un intent filter per comunicare tale intenzione al sistema operativo.

La funzionalità denominata Android Beam™ permette invece ad un dispositivo di inviare un messaggio NDEF ad un altro semplicemente avvicinando il retro di entrambi. Questa interazione fornisce uno strumento molto intuitivo per inviare dati rispetto ad altri come Bluetooth, in quanto come già analizzato in precedenza, non è richiesta alcuna procedura di discovery o pairing. La connessione viene avviata automaticamente quando due dispositivi vengono avvicinati. Ad esempio, la rubrica, il browser e Youtube utilizzano Android Beam per condividere contatti, pagine web e video con altri dispositivi.

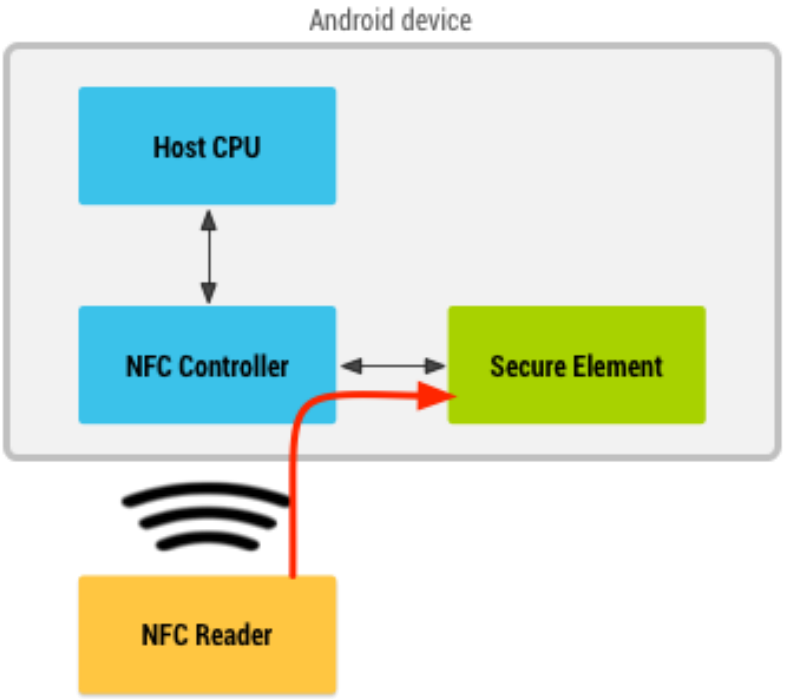


Figura 12. NFC Card Emulation con il secure element.

[3] http://developer.android.com/guide/topics/connectivity/nfc/nfc.html

E' importante sottolineare che la maggior parte dei dispositivi Android dotati di tecnologia NFC offrono anche supporto alla NFC card emulation, nella quale la carta viene emulata da un chip separato nel dispositivo, denominato *secure element*. Proprio nell'ultima versione, Android 4.4 KitKat introduce un metodo addizionale di card emulation, che non coinvolge alcun secure element, denominato Host-Based Card Emulation. Questa tecnologia permette a ciascuna applicazione Android di emulare una carta e comunicare direttamente con un reader NFC.

In particolare, quando viene utilizzata la semplice modalità di card emulation, la carta viene emulata dal secure element del dispositivo attraverso un'applicazione Android. Quindi, quando l'utente vuole comunicare con un terminale NFC, l'NFC Controller nel dispositivo guida i dati dal reader verso il secure element (Figura 12).

Quando invece una card NFC viene emulata usando la Host-based card emulation, i dati vengono inviati all'CPU che ospita l'applicazione direttamente, senza utilizzare alcun secure element (Figura 13).

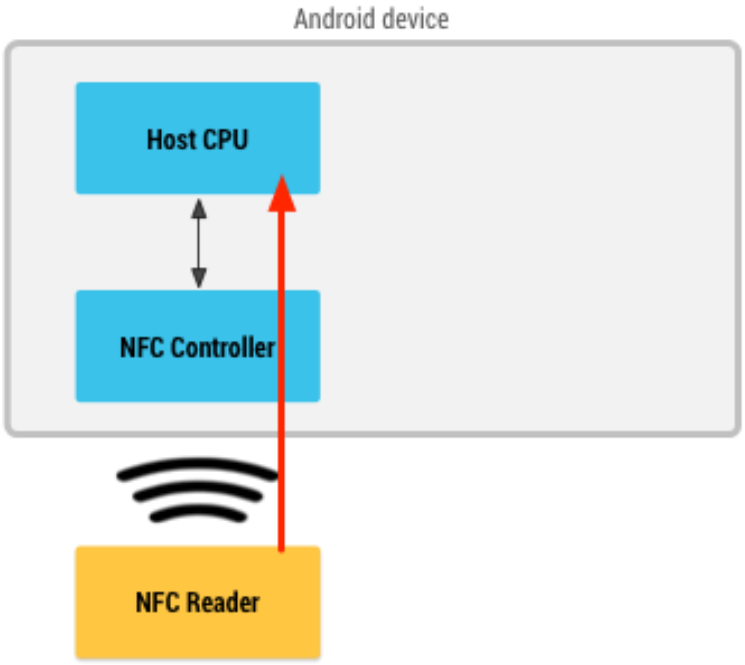


Figura 13. NFC Card Emulation senza il secure element.

Per maggiori dettagli sull'implementazione di operazioni di lettura e scrittura di messaggi NDEF, sia su Tag che tramite Android Beam, si rimanda alla pagina di Android Developers dedicata.

3.3 Prescription Writer

Nel presente lavoro, sono state proposte due applicazioni Android in grado di fornire un'efficace implementazione della ricetta medica digitale. In particolare, la prima applicazione denominata *PrescriptionWriter* simula il software utilizzato dal medico per effettuare le prescrizioni

ai suoi pazienti; la seconda, *PrescriptionReader* rappresenta l'applicativo utilizzato dal farmacista per leggere la prescrizione e consegnare al paziente i farmaci di cui necessita.

Entrambe le applicazioni sono pensate per l'utilizzo di NFC per la memorizzazione e la successiva lettura di Tag NFC e per la trasmissione della ricetta tra dispositivi attraverso Android Beam e sono disponibili in due lingue: italiano e inglese. Nel seguito verranno analizzate entrambe le applicazioni, in particolare quella utilizzata dal prescrittore, descrivendo tutti gli strumenti utilizzati e le funzionalità implementate.

3.3.1 Interfaccia e funzionalità

L'applicazione PrescriptionWriter rappresenta il pannello digitale attraverso il quale il medico compila le prescrizioni per i suoi pazienti. Attualmente, il medico, al termine della compilazione stampa la ricetta in formato cartaceo e la consegna al fruitore. In questo caso invece, la ricetta verrà salvata all'interno di un Tag NFC, evitando l'utilizzo di altri supporti.

PrescriptionWriter presenta 4 schermate principali, selezionabili da un opportuno NavigationDrawer, elemento di design definito dalle specifiche di Android, mostrato in Figura 14.

Figura 14. Navigation Drawer

E' opportuno analizzare innanzitutto le opzioni "Pazienti" e "Profilo medico" per fornire una prima analisi dell'architettura dell'applicazione. L'opzione "Profilo medico" (Figura 15) permette di definire i dati che identificano il prescrittore in maniera univoca: attualmente sulla ricetta medica cartacea vengono indicati nome, cognome, provincia, regione, un codice regionale che identifica il medico all'interno del Sistema Sanitario locale e un codice identificativo dell'ASL di appartenenza. I dati vengono salvati sul dispositivo premendo il pulsante di conferma ed è quindi sufficiente inserirli una sola volta.

Figura 15. Profilo medico

Una volta impostati i dati relativi al prescrittore, è possibile visualizzare o manipolare la lista dei pazienti appartenenti al medico (secondo il SSN, in teoria) attraverso il pannello "Pazienti". In Figura 16a è mostrata la lista dei pazienti in ordine cronologico di inserimento nel database; è possibile eliminare un paziente premendo sul pulsante accanto ai suoi dati o aggiungerne uno nuovo premendo il pulsante in basso a destra: alla pressione, viene mostrata la finestra di Figura 16b, che permette di inserire nome, cognome e codice fiscale (ben formato) del paziente.

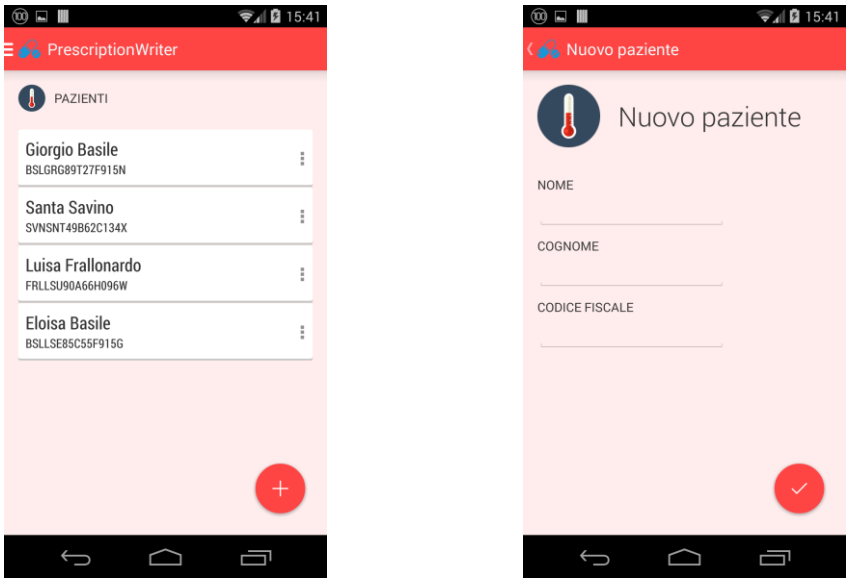


Figura 16. a) Lista dei pazienti e b) pannello di aggiunta

3.3.2 Prescrizione e uso di NFC

A questo punto possiamo analizzare il pannello dedicato alle prescrizioni, che presenta una lista delle ultime prescrizioni effettuate. Al click sul pulsante di aggiunta, viene visualizzata la schermata di Figura X, che permette di selezionare uno dei pazienti presenti nel database: una volta

selezionato, i campi che lo riguardano vengono automaticamente compilati nel form. In seguito, è possibile aggiungere la prescrizione di un determinato farmaco, cliccando sul pulsante dedicato. Nel pannello visualizzato, il medico può selezionare il principio attivo che vuole prescrivere, ricercandolo in base al suo nome o al nome commerciale associato contenuto nel file csv fornito dall'AIFA, e successivamente specificare quantità e modalità di assunzione. Una compilata la prescrizione del farmaco è possibile eliminarla, aggiungerne un'altra o modificare i dati del paziente. Al termine della procedura, cliccando sul tasto di salvataggio, la prescrizione viene memorizzata e listata nell'elenco delle prescrizioni recenti. Il processo fin qui descritto è mostrato nel dettaglio in Figura 17.

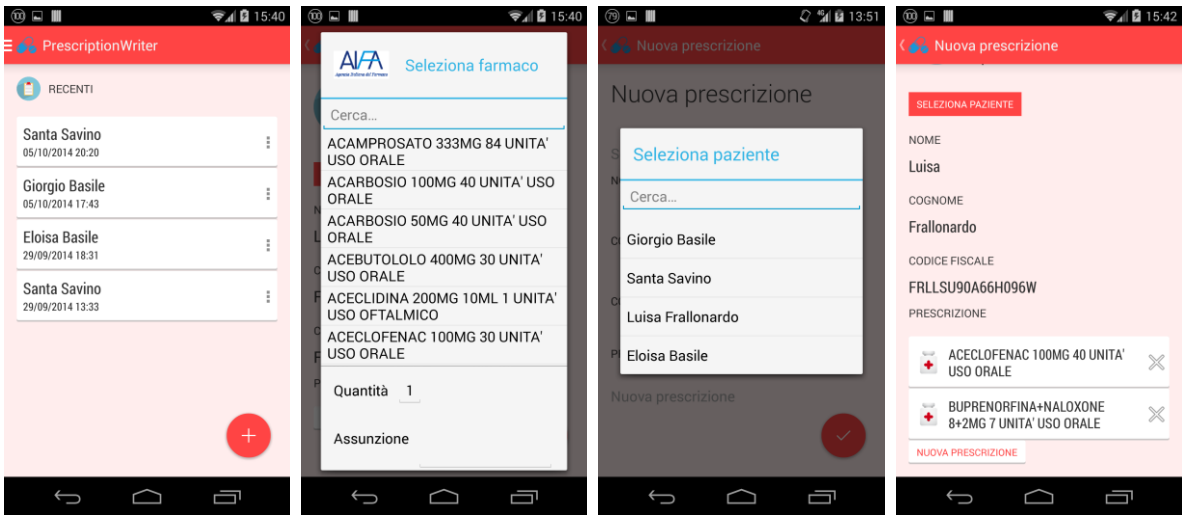


Figura 17. a) Lista delle prescrizioni, b) scelta del paziente, c) prescrizione del farmaco, d) salvataggio della prescrizione

Una volta terminata la procedura di emissione della prescrizione completa, è possibile effettuare la vera e propria scrittura della ricetta su un tag NFC formattato NDEF. Il salvataggio consiste nella composizione di una stringa strutturata contenente tutti i campi da inviare separati da un delimitatore. Successivamente, il messaggio attraversa uno stadio di criptazione prima di venire fisicamente salvato nel Tag. La scrittura vera e propria è data da un messaggio NDEF formato da due record: il primo è un cosiddetto Android Application Record, che permette di specificare l'applicazione destinataria del messaggio appena scritto (nel nostro caso il PrescriptionReader), il secondo è l'effettivo messaggio incapsulato in un record NDEF di tipo plaintext. La modalità di utilizzo del tag è quella read/write, in modo da poter riutilizzare il tag per altre prescrizioni successive.

In questo lavoro sono stati utilizzati tag NXP NTAG 216 con capacità di memoria di 888 byte, che lavorano alla frequenza standard di 13,56 MHz, utilizzando gli standard di comunicazione ISO 14 443-2 A e ISO 14 443-3 (Figura 18a). Avvicinando il tag al retro del telefono, esso viene rilevato dal chip NFC contenuto nella batteria (Figura 18b): premendo il pulsante accanto alla prescrizione scelta è possibile salvare la prescrizione sul tag con successo (Figura 18c). Nel caso in cui dopo la detection il tag venga allontanato, oppure i dati da memorizzare sono in quantità superiore alla memoria disponibile, viene restituito un messaggio di errore.

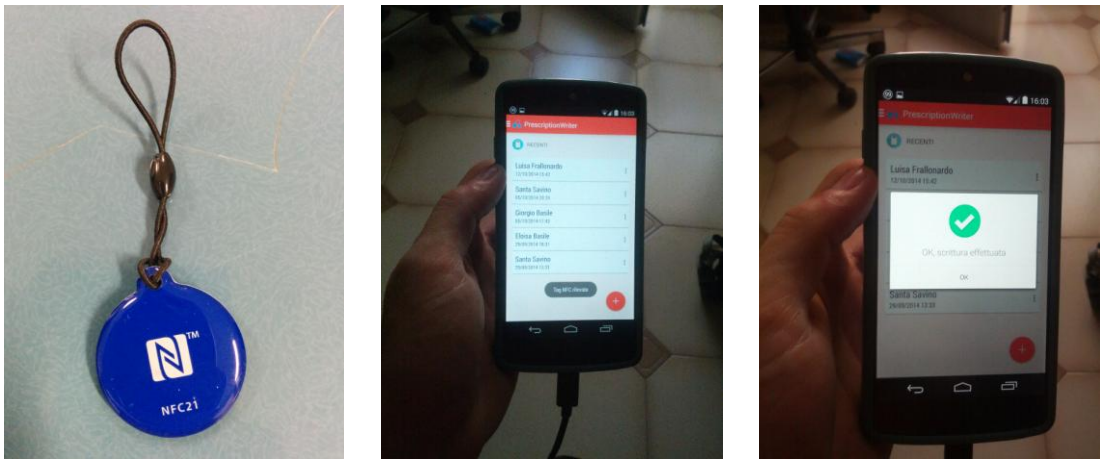


Figura 18. a) Un Tag NFC, b) rilevazione del tag, c) salvataggio della prescrizione.

Infine, nel pannello Impostazioni, è possibile selezionare l'algoritmo con il quale si vogliono cifrare i dati relativi alla ricetta medica da salvare su tag NFC. Gli algoritmi supportati sono, come accennato, il DES (Data Encryption Standard) e il Triplo DES, due algoritmi di cifratura simmetrica. Nel paragrafo 3.5 verranno descritti tutti i dettagli di funzionamento di questi cifrari.

3.4 Prescription Reader

Una volta salvata la prescrizione sul Tag NFC, il potenziale paziente può recarsi dal farmacista per ottenere i farmaci di cui ha bisogno: è necessario prevedere l'utilizzo di un software in grado di leggere i dati memorizzati nel tag, decrittarli, effettuarne il parsing e infine visualizzare la ricetta completa. Per fare queste operazioni è stata scritta l'applicazione PrescriptionReader, in grado di effettuare esattamente i compiti descritti in precedenza. Non è necessario effettuare alcun tipo di avvio manuale: avvicinando il dispositivo al Tag NFC il Tag Dispatch System di Android legge il primo record e lancia l'applicazione, inviandogli il messaggio contenuto nel Tag. Tale messaggio verrà descrittato e parsato, fino alla definitiva visualizzazione della ricetta, mostrando tutti i campi di cui è composta. In Figura 19 un esempio di lettura da un Tag NFC.

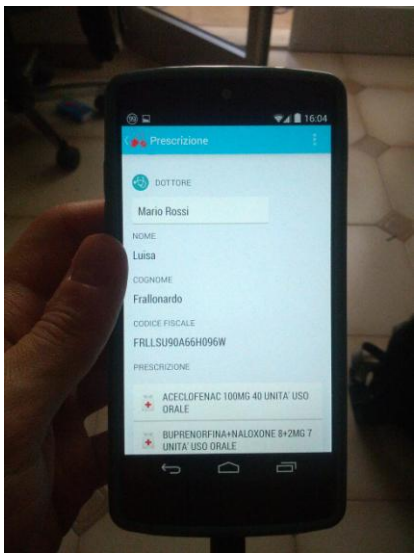


Figura 19. Lettura da Tag NFC e visualizzazione della ricetta

Inoltre, in aggiunta alla lettura da Tag, l'applicazione supporta l'utilizzo di Android Beam, rendendo possibile il trasferimento della ricetta verso un altro dispositivo dotato anch'esso di PrescriptionReader: in questo modo, è possibile inviare la ricetta con un semplice "beam" (Figura 20). Sebbene ad un primo approccio possa sembrare un'operazione priva di utilità, in realtà la verifica della funzionalità di tal sistema potrebbe abilitare il salvataggio della ricetta direttamente su un dispositivo, senza dover necessariamente utilizzare un Tag NFC, che rappresenterebbe comunque un costo evitabile.

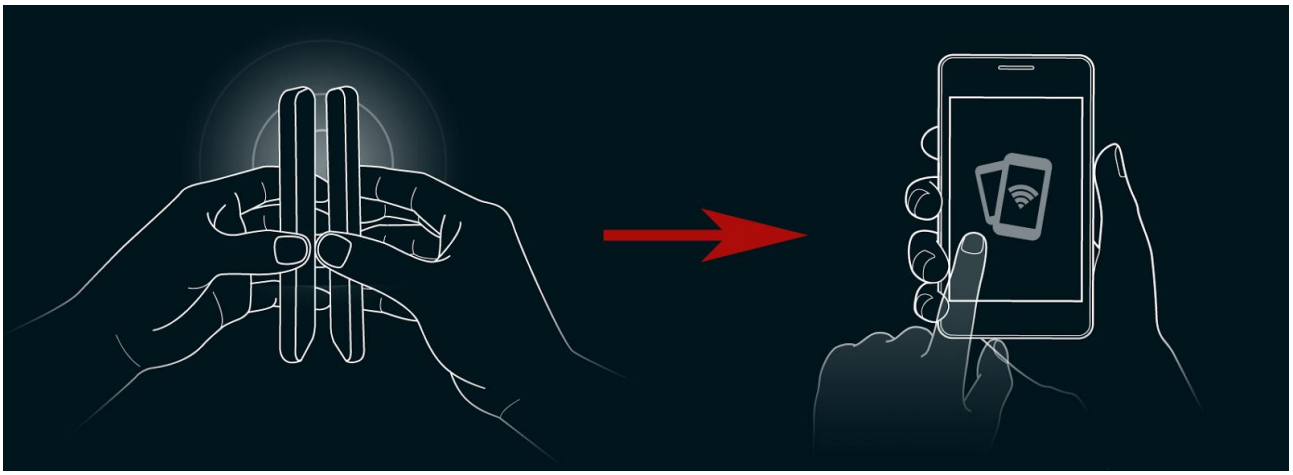


Figura 20. Trasferimento di una ricetta tramite Android Beam

3.5 Algoritmi di crittografia: DES e 3DES

Il sistema crittografico D.E.S. nasce nel 1973 dall'IBM come evoluzione di un crittosistema più obsoleto, LUCIFER, su richiesta della NBS (National Bureau of Standards). E' un cifrario simmetrico che effettua una codifica a blocchi. Risulta quindi necessario che l'intero messaggio in chiaro venga suddiviso in blocchi (stringhe di plaintext), di 64 bit ciascuno.

Usando una chiave di 64 bit (di cui 8 sono i bit di parità, quindi effettivamente la chiave è di 56 bit), si ottiene un testo cifrato rappresentato da una stringa di 64 bit.

3.5.1 Encryption

Cifratura e decifratura seguono diverse fasi (che nel DES sono 16) e in ogni fase viene usata una particolare sottochiave derivata da k. L'algoritmo di cifratura si compone di 3 passi fondamentali (schematizzati in Figura 21):

1. Dato il plaintext x, si costruisce una stringa x_0 permutando (ordinando in successione) i bit di x secondo una permutazione iniziale fissata PI. In particolare:

   $x_0=PI(x)=L_0*R_0$

   dove, L_0 comprende i primi 32 bit di , x_0 e R_0 gli ultimi 32 bit.

2. Li*Ri, per $1\leq i\leq 16$, viene calcolato come:

   $L_i=R_{i-1}$

$R_i=L_{i-1} \oplus f(R_{i-1},k_{i-1})$

dove $\oplus$ è l'operatore di XOR, f è una funzione e verranno descritti meglio nel seguito, e $k_0,k_1,\ldots,k_{15}$ si chiamano ***sottochiavi*** e sono composte da 48 bit calcolati in funzione della chiave k di 56 bit*;*

3. Si applica la ***permutazione finale*** (fissata) PF alla stringa di bit $R_{16}*L_{16}$, ottenendo il testo cifrato *c*, cioè $c = PF(R_{16}*L_{16})$

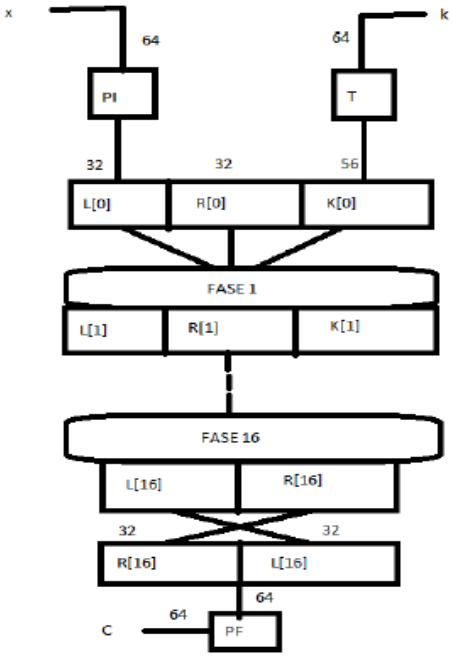


Figura 21. Schematizzazione dell'algoritmo DES

3.5.2 Analisi di una singola fase di codifica

Nei tre passi appena analizzati, le incognite principali riguardano la funzione f e il calcolo delle sottochiavi, utilizzate al passo 2. La funzione ***f*** (Figura 22) ha come primo argomento la stringa $\mathbf{R_{i-1}}$ di 32 bit, come secondo argomento la stringa $\mathbf{K'_{i-1}}$ di 48 bit, e produce in output una stringa di 32 bit di lunghezza:

1. $\mathbf{R_{i-1}}$ viene "espanso" in una stringa di 48 bit in base ad una funzione di espansione **EP** fissata. $\mathbf{EP(R_{i-1})}$ consiste dei 32 bit di $\mathbf{R_{i-1}}$ permutati, 16 dei quali compaiono due volte;

2. Si calcola $\mathbf{EP(R_{i-1}) \oplus K'_{i-1}}$;

3. Il risultato del punto 2 viene "compresso" in una stringa di 32 bit generata da una funzione di compressione **S** fissata. Ciò avviene nei cosiddetti **S-box**, che sono il cuore del DES;

4. La stringa di 32 bit in uscita agli **S-box** viene permutata in accordo ad una permutazione **P** fissata. La stringa risultante è $\boldsymbol{f(R_{i-1},K'_{i-1})}$.

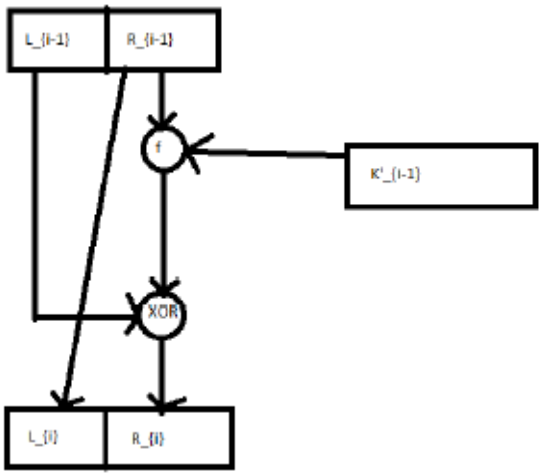


Figura 22. Una fase di codifica

Il risultato della funzione f viene messa in EX-OR con L_{i-1}. L'EX-OR è un operatore binario largamente diffuso in quanto disponibile su tutte le CPU, che viene definito come l'operatore di **confusione** ideale perchè, se l'input è casuale allora anche l'output godrà della stessa casualità. Il suo funzionamento è definito dalla seguente tabella delle verità:

A	B	⊕
0	0	0
0	1	1
1	0	1
1	1	1

In Figura 23 è mostrata una schematizzazione della funzione f.

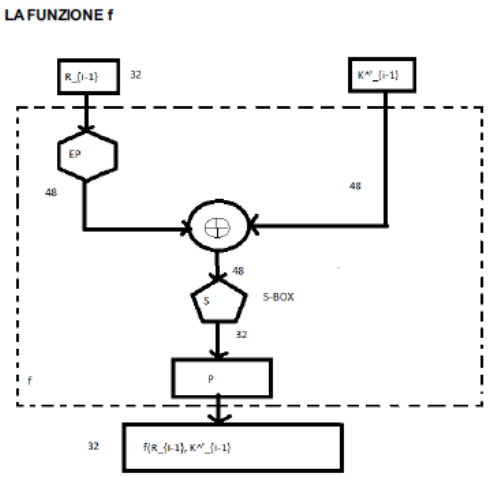


Figura 23. La funzione f

3.5.3 S-Box

Il calcolo degli S-Box segue i passaggi elencati di seguito (Figura 24):

- Si calcola EP(Ri-1) ⊕ **K'i-1** e si scrive il risultato come la concatenazione di otto stringhe di 6 bit $B=B_1B_2B_3B_4B_5B_6B_7B_8$

- Si utilizzano gli Si, $1\leq i\leq 8$, che sono tabelle 4×16 i cui elementi sono interi compresi fra 0 e 15. Data una stringa di 6 bit $B_j=b_1b_2b_3b_4b_5b_6$, $S_j(B_j)$ viene calcolata come segue:

  - i due bit b_1 e b_6 determinano la rappresentazione binaria di una riga r di S_j ($0\leq r\leq 3$),
  - i quattro bit $b_2b_3b_4b_5$ determinano la rappresentazione binaria di una colonna c di S_j ($0\leq c\leq 15$).
  - Pertanto $S_j(B_j)$ è l'elemento $S_j(r,c)$, scritto in binario sotto forma di stringa di 4 bit $\Rightarrow C_j = S_j(B_j)$, $1\leq j\leq 8$

- La stringa di 32 bit $C = C_1C_2C_3C_4C_5C_6C_7C_8$ viene permutata in accordo ad una permutazione P fissata. La stringa risultante P(C) è $f(R_{i-1},K'_{i-1})$.

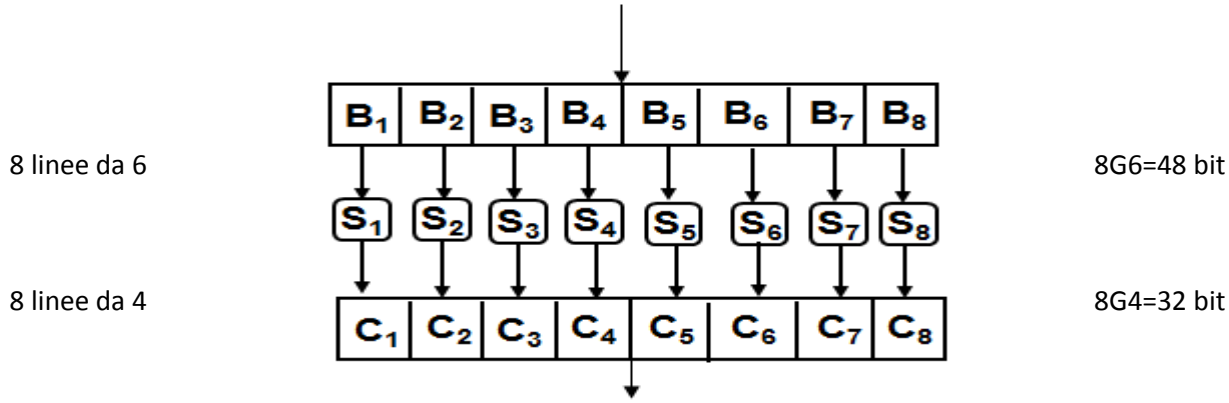


Figura 24. Calcolo S-Box

3.5.4 Calcolo delle sottochiavi

- k è una stringa di 64 bit, di cui 56 costituiscono la chiave vera e propria, mentre i rimanenti 8 sono bit di parità (per il rilevamento di errori);

- I bit di parità occupano le posizioni 8,16,…,64 (multiple di 8)ed assumono valore tale che ogni byte abbia un numero dispari di bit a 1. Il bit di parità può servire a rilevare errori su un singolo bit del byte relativo;

- I bit di parità non vengono utilizzati nel calcolo delle sottochiavi.

Le sottochiavi k_i, $1\leq i\leq 16$, sono così determinate:

1. Data la chiave k a 64 bit, si tralasciano gli 8 bit di parità, mentre si permutano (si ordinano in successione) i rimanenti 56 bit, in base alla permutazione T, fissata a priori. Sia $T(k)=G_0*D_0$, dove G_0 comprende i primi 28 bit di T(k) e D_0 gli ultimi 28 bit

2. Per i compreso fra 1 e 16 si calcolano:

Infine, otteniamo $G_i=SH_i(G_{i-1})$ e $D_i=SH_i(D_{i-1})$ da cui $k_i=G_{i-1}D_{i-1}$ e $K'_i=CT(G_iD_i)$ dove SH_i è uno shift ciclico a sinistra, di una o due posizioni in funzione del valore di i: si scorre di una posizione per i=1,2,9,16, di due in tutti gli altri casi. CT è una permutazione fissata di compressione. In Figura 23 è mostrata una schematizzazione dell'algoritmo fin qui descritto.

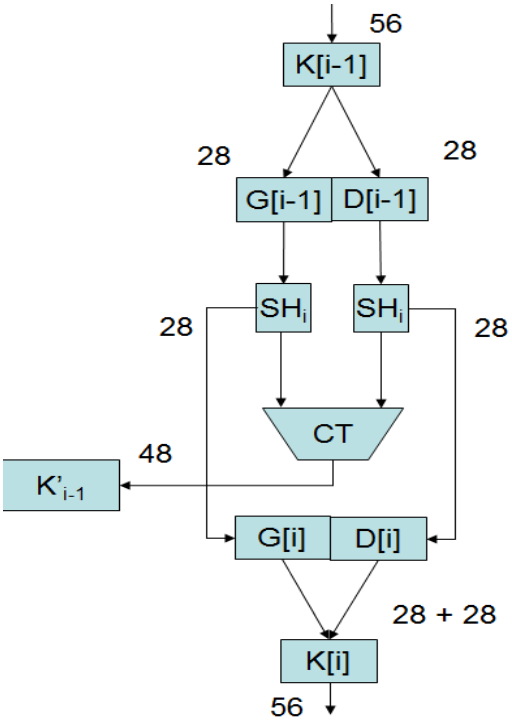


Figura 25. Calcolo delle sottochiavi

3.5.5 3DES

Il Triple DES (DES triplo) è un cifrario a blocchi basato sulla ripetizione del Data Encryption Standard (DES) per tre volte. Quando si scoprì che la chiave a 56 bit del DES non era abbastanza lunga da garantire la sicurezza contro attacchi a forza bruta, il TDES fu scelto come modo semplice per aumentare la lunghezza della chiave senza bisogno di cambiare algoritmo. L'uso di tre passaggi è essenziale per prevenire attacchi di tipo man-in-the-middle che funzionano contro la doppia crittazione DES. Si noti che il DES non è un gruppo; se lo fosse, il TDES sarebbe equivalente al singolo DES, e non sarebbe più sicuro.

Date tre chiavi a 56 bit, K_A, K_B, K_C, detta e_K la funzione di encryption dell'algoritmo DES, allora un messaggio m viene criptato con il Triplo DES eseguendo:

$$c=e_{KC}(d_{KB}(e_{KA}(m)))$$

Siccome TDES utilizza tre passaggi, esso permette l'utilizzo di una, due o tre chiavi di criptazione. L'utilizzo di un'unica chiave è il modo meno sicuro di implementare l'algoritmo in particolare se si utilizza la sequenza criptazione-decriptazione-criptazione (DES-EDE1) che, in realtà, si riduce ad un singolo ordine di criptazione perché i primi due passaggi si elidono a vicenda. L'utilizzo di tre chiavi differenti garantisce la migliore protezione.

Conclusioni

In questo lavoro, è stata proposta una valida implementazione della ricetta medica digitale. Utilizzando la tecnologia NFC è possibile ridurre al minimo l'utilizzo di materiale cartaceo, salvando i dati necessari su un'opportuno Tag con sufficiente capacità di memorizzazione. Le informazioni ivi contenute vengono successivamente lette da un applicazione che sfrutta un reader NFC: esso è in grado di leggere i dati presenti sul supporto, che vengono successivamente decrittate e parsate, restituendo all'utente i campi di cui si compone la ricetta. E' inoltre possibile trasferire la ricetta da un dispositivo Android ad un altro con in semplice tocco dei due apparecchi attraverso l'utilizzo della tecnologia Android Beam.

Le informazioni relative alla ricetta sono efficacemente protette sia da uno stadio di crittografia applicata al canale wireless di comunicazione utilizzato da NFC, sia da un secondo stadio applicato ai dati veri e propri prima del salvataggio sul supporto, che può essere effettuato tramite gli algoritmi DES o Triplo DES. Chi non dispone della chiave di cifratura, generata partendo da un seed hardcodato nei software sviluppati, non è in grado di leggere la ricetta in caso di smarrimento o furto del Tag, preservando la sicurezza e la privacy dell'utente.

In un'implementazione migliorata, si potrebbe utilizzare Android Beam per trasferire la ricetta senza la necessità di salvarla su un Tag: questo presupporrebbe un sistema remoto di memorizzazione della ricetta stessa, appartenente al Sistema Sanitario Nazionale, che permetterebbe di utilizzare lo smartphone solo come depositario della ricetta in caso di malfunzionamento o indisponibilità di connessione al Web.

Bibliografia

[1] K. Finkenzeller, *RFID Hanbook: fundamentals and Application in contactless Smart Cards and Identification*, Munich, Wiley, 2003.

[2] NFC FORUM, *NFC Record Type Definition (RTD)*, technical specification, 2006

[3] NFC FORUM, *NFC Data Exchange Format (NDEF)*, technical specification, 2006.

[4] 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

[5] Android Developers, *Near Field Communication*, http://developer.android.com/guide/topics/connectivity/nfc/index.html

[6] Android Developers, *Host-Based Card Emulation*, http://developer.android.com/guide/topics/connectivity/nfc/hce.html

[7] La sanità digitale – eHealth, http://leg16.camera.it/561?appro=257