Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Informatica per il Management

SISTEMI DI PAGAMENTO : Innovazione e sicurezza tecnologica in costante evoluzione

Relatore:
Chiar.mo Prof.
Davide Sangiorgi

Presentata da:
Marco Bondelmonte
Mat. 0000346471

Sessione II
Anno Accademico 2013-2014

A tutti quelli che hanno sempre creduto in me!

Indice

Capitolo 1

I sistemi di pagamento

1.1 Introduzione

Che cosa sono i sistemi di pagamento? Partendo dalla definizione generale, i sistemi di pagamento sono degli strumenti e procedure diretti a riprodurre gli spostamenti materiali di denaro da un soggetto ad un altro, al fine di regolare le transazioni economiche instaurate[1]. Attraverso i sistemi di pagamento noi possiamo acquistare beni e servizi, erogando una somma di denaro in base ad accordi presi e consegnando tale importo a una controparte creditrice nei nostri confronti. Il settore dei sistemi di pagamento é diventato oggi una parte importante e fondamentale delle attivitá di scambio di ogni paese, con il passare del tempo é divenuto sempre piú complesso, richiedendo una scelta sempre maggiore fra strumenti e soluzioni tecnologiche, idonee per favorire la velocitá e l'efficacia delle modalitá di scambio. Tutto ció ha manifestato un crescente ruolo verso soggetti bancari e soggetti non finanziari, ma specializzati però in natura pienamente tecnologica. Nuove tecnologie e nuove idee hanno quindi portato l'iniziale e semplice transazione, come poteva apparire il pagamento in contanti, alla complessitá degli attuali sistemi di pagamento. Gli scambi monetari avvengono ormai in grande prevalenza attraverso sistemi informatici e i soggetti che li gestiscono sono coinvolti in modo crescente nel controllo di reti telematiche e sistemi di information tecnology. Il pagamento é visto come un processo articolato in differenti differenti fasi complesse o meno, con il compito di trasferire informazioni relative

al pagamento alle diverse parti coinvolte(compratore, venditore, istituzione bancaria che collega la moneta vera e propria), cosí da consentire, una volta verificata la conformitá dell'operazione e la disponibilitá dei fondi, di dar il via al trasferimento fisico della moneta[2].

Il funzionamento del sistema dei pagamenti richiede un quadro normativo: il Payment System Directive(PSD)[1], che regola i diritti e gli obblighi delle diverse parti coinvolte nell'utilizzo degli strumenti di pagamento.

Per quanto concerne l'aspetto legislativo i servizi di pagamento sono regolamentati dal D.Lgs.n.11 del 27 gennaio 2010, che regola appunto l'esercizio dei servizi di pagamento nell'ambito del mercato europeo. Gli obbiettivi primari di questa riforma sono quelli di tutelare la clientela svolgendo un miglioramento della qualità dei servizi di pagamento. Questa normativa viene applicata solamente a strumenti di pagamento di tipo elettronico, che risultano più efficienti, escludendo quindi tutti quelle tipologie di strumenti cartacei. Ricordiamo quindi che l'evoluzione nel tempo degli strumenti di pagamento, va di pari passo a quella del commercio elettronico, ossia del mercato online.

Di seguito troviamo le maggiori tipologie di pagamento online utilizzate al giorno d'oggi:[3]

- Carta di credito
- Carta di debito
- Bonifico bancario
- Addebiti diretti
- Rimesse di denaro (*money transfer*)
- Carte prepagate

[1] www.bancaetica.it/psd-payment-services-directive-direttiva-europea-sui-servizi-pagamento

1.2 Strumenti di pagamento elettronici

Parlando di strumenti di pagamento elettronici bisogna tenere a mente che le principali caratteristiche che un utente solitamente nota quando decide di avvalersene sono quelle di, riservatezza(privacy), sicurezza, facilità di utilizzo, accettazione, costi e tempi di accredito e addebito. Il tema della privacy per l'utente è molto importante, perché uno dei maggiori dubbi che colpisce un utente quando effettua un acquisto online è la paura che le sue informazioni, finiscano in mano ad utenti malintenzionati, che le utilizzeranno per compiere crimini informatici.

1.2.1 Carte di credito

La carta di credito é uno strumento di pagamento elettronico, che può essere rilasciato da una banca o un ente finanziario. La sua struttura é composta da una carta di materiale plastico, che al suo interno possiede un dispositivo per il riconoscimento dei dati relativi al titolare di tale strumento e anche informazioni riguardanti l'istituto che la ha emessa. Questa carta garantisce una disponibilità di fondi che varia in base all'affidabilità del cliente stesso. Grazie al suo volume ridotto e alla riduzione del volume del contante, la carta di credito offre numerosi vantaggi che spingono una moltitudine di persone al suo utilizzo, nonostante questo strumento abbia anche aspetti negativi come piccoli costi di gestione. Il funzionamento di tale carta è dato essenzialmente da un processo di autorizzazione del sistema bancario(da qui derivano appunto i costi di gestione). Questo processo é composto essenzialmente da tre soggetti :

- Ente emittente(issuer): é una azienda , che può essere una banca o un ente finanziaro, la quale si occupa di rilasciare la carta di credito, definendo un contratto di finanziamento con il futuro titolare della carta. Futuro titolare della carta perché i titolari, sono appunto considerati dall'azienda i clienti e sono quelli che spendono il loro denaro attraverso l'utilizzo della carta.

- Ente esercente(merchant) : corrisponde all'esercizio commerciale che, dopo aver aderito ad un circuito di pagamento, permette ai propri

clienti di pagare attraverso il sistema di pagamento convenzionato, differente dal contante. La partecipazione ad un determinato circuito, avviene solamente tramite l'intermediazione di una società che si occupa di gestione terminali (acquirer) che offre appunto dei servizi di vendita o di noleggio di POS[2] (Point of sale), contabilizzazione e rendicontazione dei pagamenti, reportistica e gestione delle controversie (definite dispute), comunicazione flussi informativi da e verso i clienti stessi.

- Circuito di pagamento: si riferisce all'azienda che si occupa di gestire le richieste e le autorizzazioni alla spesa effettuate mediante carta, attraverso una rete propria. La rete si espande, grazie alle autorizzazioni che vengono date agli acquirer per l'installazione dei POS, come punti terminali della rete, dai commercianti. Il circuito si occupa anche di operazioni di tipo settlement, ovvero di contabilizzazione e pareggio delle partite contabili sulle posizioni dei singoli titolari ed esercenti. Le informazioni vengono inviate all'ente emittente e alla società di gestione terminali, i quali mantengono aggiornati i loro rapporti con titolari e negozianti. I principali circuiti mondiali sono Visa, MasterCard, Diners, American Express, JCB e China Union Pay.

Sulla carta sono presenti informazioni riguardanti le generalità del titolare, il numero della carta e la sua scadenza. Con la carta é possibile effettuare il pagamento subito dopo l'acquisto, tale importo verrà addebitato direttamente sul conto corrente. Dietro alla carta il proprietario deve porre la propria firma all'interno dello spazio predisposto. I soggetti che vengono coinvolti, quando viene effettuata una transazione, sono tre, ognuno con il rispettivo compito:

- il titolare della carta, il quale si impegna a restituire all'emittente della carta l'importo della transazione effettuata, nei tempi e nei modi prestabiliti dal contratto sottoscritto.

[2]Il POS è un dispositivo elettronico indipendente che non ha bisogno di interfacciarsi con un PC, ed è spesso dotato di un sistema operativo. Questo lettore, in un punto vendita, consente a un creditore di accettare e incassare, direttamente sul proprio conto corrente, i pagamenti mediante moneta elettronica. (http://it.wikipedia.org/wiki/Point_of_sale)

- Il fornitore eroga i beni o servizi richiesti dal cliente.
- L'istituto emittente si impegna a pagare al posto del cliente quanto dovuto, eventualmente al netto di commissioni prestabilite.

La carta di credito é quindi ritenuta un metodo di pagamento efficiente in quanto il cliente può effettuare acquisti, senza l'utilizzo del contante, il fornitore non incorre in un rischio di non pagamento, dovuto alla mancanza di fondi, e l'istituto che si occupa di erogare il servizio, percepisce per tutto ciò una commissione. É un particolare strumento che mi consente anche non soltanto di pagare alla cassa, ma di prelevare in uno sportello automatico, tramite un codice segreto consegnato insieme alla carta.

1.2.2 Carte di debito

La carta di debito, chiamata impropriamente, ma diffusamente, carta Bancomat, è una carta di pagamento, che consente di addebitare importi monetari sul conto del titolare, a fronte di operazioni di transazioni effettuate. Generalmente questo strumento è collegato ad un conto corrente bancario, dove i fondi che vengono spesi, per mezzo di questa carta all'interno di esercizi commerciali o per prelievi presso sportelli bancomat, vengono addebitati appunto sul conto corrente del titolare; da qui deriva il termine "*Debito*" .

1.2.3 Money transfer

Il money transfer è il mezzo più utilizzato per inviare i soldi all'estero da parte di cittadini privati, come ad esempio i lavoratori immigrati provenienti da paesi esteri, fuori dall'area dell'Euro, che utilizzano i money transfer per inviare soldi ai loro famigliari rimasti nel paese di origine. Per questo motivo le agenzie money transfer sono la forma di trasferimento di denaro più utilizzate in Italia e nel Mondo. Per l'invio di denaro mediante queste agenzie, occorre solamente un documento di identità valido, e per importi di denaro superiori a 2000 euro, un documento che certifichi la provenienza di quei soldi. Come documento si può utilizzare ad esempio una ricevuta bancaria oppure una busta paga, per garantire che quei soldi non derivino da fonti illecite di guadagno. Per la riscossione del denaro, bisogna essere in

possesso di una carta d'identità, come per l'invio, ed avere un codice identificativo della transazione, che il mittente del denaro avrà spedito. Riguardo i tempi di trasferimento di norma il denaro è spedito intorno alle 48 ore, che possono diminuire in caso di invio urgente a 24 ore. Altrimenti, se invece di richiedere il ritiro in contanti, si è possessori di un conto corrente, e si dispone per accreditare tale somma sul conto, i tempi sono ancora più brevi, solitamente il giorno stesso. I maggiori operatori del settore per le agenzie money transfer sono, Western Union, Ria e MoneyGram, reperibili solitamente spesso presso uffici di cambio, aereoporti, stazioni autobus, Internet point e agenzie di viaggio.

1.2.4 Bonifico bancario

Il bonifico bancario è uno strumento di pagamento utilizzabile sia online sia tramite uno sportello bancario. Grazie all'ampia diffusione di Internet, il bonifico bancario online è oggi uno degli strumenti di pagamento più utilizzati vista la sua semplicità e comodità per l'invio di denaro direttamente dal proprio computer. Molte banche, consentono l'invio di bonifici a spese zero. Come per ogni altra operazione bancaria tramite Internet, per ragioni di sicurezza, si utilizza un dispositivo particolare, che viene chiamato Token, solitamente consegnato dalla banca. Questo dispositivo, è una sorta di chiavetta che genera una password differente ogni 60 secondi per evitare le frodi online. La prima cosa da fare per accedere al conto corrente online, è collegarsi al sito della banca in cui si dispone di un conto corrente online, inserire username e password, ed effettuare l'accesso, procedendo successivamente alla compilazione di un form, con il relativo inserimento dei dettagli di pagamento, dando conferma una volta avvenuta la compilazione.

1.2.5 Addebito diretto in conto corrente

Il servizio di domiciliazione (RID), è stato sostituito da l'attuale debito diretto SEPA[3] (o SSD), il quale è definito come uno strumento di incasso a livello europeo, fondato su un accordo, detto "*mandato*" e concluso tra

[3] www.sepaitalia.eu/welcome.asp

debitore e beneficiario, dove il primo soggetto autorizza il secondo a disporre di addebiti sul proprio conto corrente per effettuare tipologie di pagamenti ricorrenti (ad esempio rate di un prestito).

1.2.6 Carte prepagate

La carta prepagata, è una particolare carta elettronica di pagamento che mi consente di effettuare pagamenti con le stesse modalità delle carte di credito tradizionali, con l'unica differenza che la prepagata non è necessariamente collegata ad un conto corrente e che tale carta deve essere ricaricata prima del suo utilizzo, perché le spese effettuate non possono superare l'importo massimo caricato al suo interno. La carta può venire caricata attraverso bonifici o deposito di contante. Per richiederla non è necessario dimostrare l'affidabilità creditizia come nelle carte di credito, ma può tuttavia appartenere comunque a circuiti Visa, MasterCard, Visa Electron, ed è utilizzabile sia dal titolare e sia da un'altra persona. Sono divise in due categorie, le prime sono, *carte prepagate ricaricabili*, le quali possono essere ricaricate più di una volta fino alla scadenza, ed avere un fondo di ricarica elevato ma che non supera massimali stabiliti. Mentre le seconde sono *carte prepagate usa e getta*, le quali contengono un importo prefissato, spesso raggiungono un fondo massimo di 500 euro, che non è possibile ricaricare, perciò una volta terminato tale importo le carte diventano inutilizzabili. Si possono ulteriormente distinguere queste carte in carte nominativa o al portatore. Le *carte nominative*, che possono essere di tipo ricaricabile, senza limiti sull'importo massimo caricabile, e le*carte al portatore*, che non richiedono la registrazione del titolare e sono di tipo usa e getta con un importo caricabile stabilito.[4] Questo strumento di pagamento è molto facile da utilizzare e sicuro rispetto ai contanti e in caso d furto può essere bloccata come una carta di credito, trasferendo però il saldo dell'importo in un'altra carta sostitutiva.

1.3 New digital payment

L'evoluzione dell'era informatica ha portato sempre più un maggiore sviluppo e cambiamento nel settore delle tecnologie e di conseguenza anche in quello dei pagamenti, i mezzi di pagamento classici che conosciamo o conoscevamo, alcuni dei quali elencati precedentemente, nel corso della storia hanno subito diverse mutazioni e continuano tutt'ora a essere soggetti a trasformazioni. Lo sviluppo hardware, software, di comunicazione e gestione dei sistemi, hanno portato i mezzi tradizionali di pagamento a effettuare una estensione della loro funzione, creando appunto nuovi modi di pagare. Questa specializzazione ha quindi condotto l'era moderna a sviluppare pagamenti di tipo non convenzionale, raggruppabili concettualmente in tre tipologie differenti, denominati anche come "**NEW DIGITAL PAYMENT**", che includono una varietà di prodotti nuovi, ma che comunque si basano su prodotti di pagamento tradizionale. Le tre categorie sono:[5][6]

- M-Payments
- E-Payments
- C-less Payments

Prima di poter procedere nel conosce le tipologie di pagamento bisogna avere anche chiaro che ogni modalità di pagamento, gira comunque attraverso differenti circuiti e ognuno di essi deve avere una accettazione, ovvero un processo mediante il quale vengono acquisite le transazioni, attraverso una rete che li convalidi li verifichi e li accetti; ed un circuito emittente, cioè un processo di emissione dello strumento di pagamento, con cui è possibile pagare le somme dovute. Bisogna inoltre conoscere un'altro tipo di figura, quella di Intermediario di pagamento, ovvero un soggetto che è coinvolto in maniera attiva nel processo di intermediazione di pagamento, gestendo un conto vero e proprio in cui viene regolato il trasferimento di fondi da un debitore a un creditore. Questi particolari soggetti possono essere ad esempio banche oppure figure non bancarie, ma che comunque esercitano attività imprenditoriale sempre legata al concetto di intermediario di pagamento, un esempio attuale e molto odierno è dato dai Digital Wallet, ovvero portafogli

digitali (comunemente borsellini digitali), oppure da operatori telefonici che gestiscono somme di moneta elettronica, in appositi conti intestati a clienti, i quali possono caricare e spendere il loro denaro per effettuare acquisti di servizi telefonici o beni.

1.3.1 Mobile payments

Nei mobile payments rientrano quelle tipologie di pagamenti, differenti dai tradizionali, che utilizzano dei dispositivi mobili come, Smartphone (ovvero cellulari di nuova generazione),Tablet, o altri apparecchi tecnologici, per poter acquistare o vendere, beni e servizi, abilitando i trasferimenti di moneta elettronica tramite una rete di telecomunicazione mobile, saldando così l'importo dovuto. I mobile payments, possono essere considerati come uno sviluppo del concetto di e-commerce, dato dal fatto che, questi dispositivi di ultima generazione sono costantemente connessi alla rete Internet. Data la definizione è possibile fare una ulteriore distinzione in base alle modalità di pagamento:

- Mobile remote payment
- Mobile proximity payment

Mobile remote payment: nei sistemi di pagamento da mobile remoto, la transazione viene effettuata a distanza utilizzando la rete del telefono smartphone (o altro dispositivo dotato di rete mobile). Vi è una situazione d'uso in cui due persone che possono essere per esempio cliente ed esercente sono distanti fra loro, ma però tramite la tecnologia di una rete cellulare, riescono a effettuare svariate operazioni finanziarie. I canali utilizzati per dar via alle transazioni nonostante siano molteplici, possono essere rappresentati per esempio da: SMS, rete mobile (LTE, HSPA,ecc), applicazioni per smartphone (o altri dispositivi mobili), e la connessione Internet (WAP) attraverso Browser mobile.

Mobile proximity payment: nei sistemi di pagamento da mobile in prossimità, le transazioni avvengono sempre per acquistare beni o servizi, ma avvengono appunto in prossimità di dispositivi che utilizzano delle particolari connessioni per lo scambio di dati ma in maniera ravvicinata senza però

il bisogno di contatto fra un dispositivo e un altro, ma solo grazie all'avvicinamento. Questa trasmissione sfrutta una rete wireless a corto raggio senza dunque aver bisogno di quella mobile. Fra le tecnologie che possono aiutare questo tipo di pagamento possiamo trovare NFC, il QR-code e applicazioni per smartphone.[7]

Il pagamento da parte dei dispositivi mobili può essere associato ad alcune possibili soluzioni come, conti telefonici, Wallet, carte di pagamento(carte di credito e prepagate).

1.3.2 Che cosa sono i Wallet ?

I borsellini elettronici chiamati alcune volte anche con il nome di e-Wallet, servono a ricreare delle funzioni simili quasi uguali a quelle di un portafoglio fisico; all'interno degli e-Wallet vengono contenute delle informazioni che possono essere, il numero di carta di credito che si utilizza per effettuare transazioni(le quali possono essere più di una e si può scegliere quale utilizzare), del denaro elettronico ed alcuni dati che identificano il proprietario (nome, cognome, indirizzo, ecc). Quindi i borsellini elettronici danno la possibilità a una persona che è intenzionata a eseguire delle transazioni online, di inserire solamente una volta le informazioni riguardanti il proprio profilo, senza dovere ogni volta ripetere nuovamente tutti i dati richiesti per il pagamento, consentendo perciò di ottimizzare il processo verso la fase finale di checkout. Questa tipologia di tecnologia rende così, qualsiasi tipo di acquisto, molto più veloce rispetto agli altri sistemi di pagamento; ed avendo già memorizzato tutti i dati necessari per l'acquisto, al cliente, non resta che collegarsi online ed effettuare la transazione. La memorizzazione delle informazioni dei Wallet può avvenire attraverso due modi, i dati possono essere salvati nella parte Server-side e cioè conservati in un server remoto di proprietà di un particolare commerciante (esempio sito di E-commerce), oppure in quello di un Intermediario di pagamnto, che gestisce il portafoglio. L'inconveniente di questa soluzione, è che la debolezza di questi sistemi di memorizzazione potrebbe portare, nel caso in cui ci sia una violazione nella sicurezza, alla rivelazione di parecchie informazioni, come numeri di carte di credito di differenti utenti. È per questo motivo quindi che i dati memorizzati in maniera Server-side,

hanno degli standard di protezione molto alti per combattere le intrusioni da parte di utenti non autorizzati. L'altra modalità di memorizzazione è Client-side, ovvero tutte le informazioni riguardanti l'utente, vengono salvate nel computer o sul dispositivo elettronico in possesso della persona. La differenza dal Server-side è che il Wallet client-side, deve scaricare il software del portafoglio digitale sul dispositivo che si utilizza per effettuare transazioni. Questo è un grande inconveniente, perché ogni qual volta si richiederà di utilizzare il servizio di portafoglio su un dispositivo nuovo, diverso da quello usato solitamente, il software dovrà essere scaricato ancora. Questa struttura effettua il salvataggio di tutte le informazioni sensibili all'interno dei dispositivi utilizzati e in maniera analoga ai portafogli server-side, nel caso di una attacco al sistema di sicurezza del dispositivo, cosa abbastanza difficile date le varie applicazioni di sicurezza installate solitamente, i dati conservati sarebbero facilmente reperibili. La differenza sostanziale fra le due modalità di memorizzazione ricade quindi sulla portabilità delle informazioni, la quale non è per niente realizzabile sui dispositivi client-side, visto che per ogni dispositivo nuovo da quello predefinito, bisogna reinstallare il software dall'inizio con il relativo inserimento dei dati.[8] Per riuscire a comprendere meglio il concetto di portafoglio elettronico, consideriamo alcuni esempi di Wallet abbastanza conosciuti nella società odierna:

- Google Wallet
- Paypal
- Apple Pay

1.3.2.1 Google Wallet

Google Wallet, è un'applicazione di pagamento mobile, creato appunto dalla Google, che sfrutta il concetto di portafoglio digitale, ovvero è in grado di effettuare pagamenti, sfruttando degli smartphone di ultima generazione (quindi non compatibile con qualsiasi smartphone). Questo servizio consente di effettuare transazioni in maniera molto più semplice, memorizzando all'interno del cellulare il numero di carte di credito o di debito, coupon per sconti e carte regalo. La nuova applicazione di Google punta quindi a rendere

più efficienti le transazioni, utilizzando solamente un dispositivo che al suo interno contiene informazioni in grado di poter pagare con denaro in forma elettronica, utilizzando la tecnologia NFC. Tale tecnologia consente di saldare l'importo dovuto, semplicemente avvicinando lo smartphone a un sensore di un POS, il quale effettuerà alcune verifiche di sicurezza e autorizzerà il pagamento.[9]

1.3.2.2 Sicurezza Google Wallet

Lo smartphone con Google Wallet è trasformato a tutti gli effetti quindi in una carta di credito virtuale, di cui potremo godere degli aspetti positivi ma anche di quelli negativi, come furto di cellulare con il conseguente utilizzo fraudolento della carta connessa al dispositivo, oppure furto di dati ed informazioni della carta contenute nel dispositivo mobile. Per ovviare a questi problemi di sicurezza, lo smartphone, è stato dotato di alcune caratteristiche che hanno provveduto a renderlo più sicuro; le informazioni vengono salvate all'interno di una particolare memoria, un chipset NFC, che è all'interno del telefono cellulare, ma che però è isolato dalle restanti parti hardware ed è isolato dal sistema operativo, è chiamato Sicure Element, un elemento protetto. Tale Sicure Element, garantisce così l'accesso solamente a determinati protocolli non garantendo quindi l'accessibilità a tutti, proteggendo perciò il dispositivo a livello hardware da alcune tipologie di intrusione come "*snooping* (ascolto)" e "*tamperig* (manomissione)". Di conseguenza solo programmi sviluppati da Google Wallet potranno entrare e effettuare pagamenti. La comunicazione fra il chipset e il sistema operativo, avviene tramite Application Protocol Data Unit, ed il codice scritto per l'elemento chipset, ovvero l'elemento protetto, è sotto forma di JAVA CARD[4], cioè una particolare tecnologia software, basata su linguaggio Java, che consente di fornire un ambiente sicuro per applicazioni che vengono eseguite su smart card e altri dispositivi con memorie molto limitate.[10] Ulteriore forma di sicurezza dei contenuti dell'applicazione, è data dal fatto che, una volta aperta l'applicazione e avviata, viene richiesto l'inserimento di un codice PIN di 4 cifre, protetto da un algoritmo che utilizza una funzione crittografica di hash a sen-

[4] www.oracle.com/technetwork/java/embedded/javacard/overview

so unico (one-way). Se vengono effettuati più di 5 tentativi di inserimento del pin, ed ogni volta risultano errati, l'applicazione viene immediatamente bloccata e diventa inutilizzabile.[11] Tuttavia una società americana viaForensics, che si occupa di sicurezza avanzata dei sistemi mobile, ha provato a mettere in pratica alcune tipologie di attacchi informatici solitamente utilizzati, riuscendo così a violare l'impenetrabilità del sistema e facendo giungere a buon fine un parte di questi. L'attacco Man in the Middle, utilizzato in una rete wi-fi, durante una registrazione di un account e in una registrazione di carta di credito, non ha raggiunto l'obbiettivo, Google Wallet è riuscito a proteggere il sistema dall'intrusione. L'analisi Forense dei dati memorizzati su dispositivo e l'esame dei registri di sistema, invece ha mostrato come Google Wallet possieda dei grandi buchi da colmare a livello di sicurezza. I problemi che sono stati riscontrati, sono stati differenti, dalla relazione della società americana è apparso che i dati delle carte di credito erano memorizzati all'interno di database SQLite, assieme a numerose altre informazioni facilmente reperibili, come il saldo della carta, il tipo, la data di scadenza, il nome del proprietario, limite, ultime quattro cifre del conto, e-mail del proprietario, rendendoli perciò facilmente recuperabili e utilizzabili. Quando l'applicazione di Google viene ripristinata e le relative transazioni vengono cancellate, è possibile comunque riuscire a recuperare tutte queste informazioni (pare che questo problema sia stato risolto con il successivi aggiornamenti del software, Risolto nella versione 1.1-R41v8). Un altro problema apparso nell'analisi e nel report dell'azienda, è dovuto al continuo monitoraggio di Google Analytics, che è un servizio di Google in grado di analizzare statistiche sui visitatori di un sito web, al quale vengono fornite esattamente informazioni su quello che realmente sta facendo la mia applicazione Wallet. Sono stati trovati degli URL di Google Analytics che inviano alcuni dati a proposito dell'utente in formato stringa, utilizzando dei metodi get,es: GET http/ 1.1, in modo da poter essere intercettati più facilmente, cosa che sarebbe più difficile rispetto a protocolli SSL più sicuri. Infine ultimo problema riportato (ma pare risolto nella versione 1.0-R33v6]) , è che il portafoglio elettronico di Google, crea un immagine della carta di credito, recuperabile, ed è sufficiente per lanciare un attacco di ingegneria sociale. Nonostante le prime 12 cifre della carta di credito non siano visibili, danno comunque la capacità ad alcuni utenti di poter

lanciare alcuni tipi di attacchi, perchè se si conoscono le restanti informazioni della carta come ad esempio il nome del proprietario della carta,si può risalire a l'indirizzo in cui vive e a tutte le informazioni legate a quell'individuo, ed inoltre è possibile osservare tutti gli usi recenti che ha fatto della sua carta, permettendo alla figura dell'attaccante di poter carpire informazioni molto utili, da poter utilizzare a suo piacimento per commettere crimini.[12]

1.3.2.3 Paypal

Paypal è un'altra versione di portafoglio elettronico che si utilizza per effettuare pagamenti online, comunemente utilizzato sul sito e-commerce ebay e per effettuare pagamenti in altri siti convenzionati. Paypal è una società statunitense, fondata a Palo Alto in California nel 1998, ed è nata inizialmente all'interno del gruppo ebay, cosa non veritiera oggi visto che la società si sta separando dal gruppo, formando due aziende distinte; la separazione è attesa intorno alla metà del 2015.[13] Paypal è uno dei sistemi di pagamento più diffusi al mondo ed è appunto un ente che si occupa di erogare moneta elettronica attraverso la rete, con lo scopo principale di abilitare tutti i sistemi di pagamento non soltanto attraverso via web, ma anche mobile e presso un punto di vendita fisico, attraverso un cloud, ovvero una risorsa Server-side, gestita in maniera sicura. Per poter incominciare a utilizzare paypal, è necessario registrarsi, inserendo tutti i dati necessari, poi, verrà aperto una sorta di conto corrente, nel quale verranno depositati realmente importi monetari tramite carte di credito; l'idea principale è appunto, come suggerisce il concetto di portafoglio elettronico, effettuare transazioni comodamente e semplicemente, senza però far riconoscere i dati della carta a colui che riceverà il nostro pagamento. La registrazione al sito web consentirà, quindi l'accesso, mediante inserimento di e-mail e password, ed una volta entrati nel proprio conto corrente, si potrà ad esempio iniziare a trasferire somme di denaro da/verso altri utenti della rete Paypal. All'interno del conto potremo inserire carte di credito, fino a un massimo di otto, oppure carte prepagate o ancora ricaricare il nostro conto Paypal attraverso un bonifico bancario. Come è possibile associare una carta, con Paypal, e quindi consumare le risorse di quest'ultima, è possibile anche ricaricarla, trasferendo

somme di denaro dal conto alla carta in maniera molto semplice. Inoltre la società mette a disposizione delle carte di credito, a tutte le persone che ne facciano richiesta, le quali girano attraverso un circuito Visa, a differenza invece delle carte prepagate, rilasciate anche quella su richiesta del cliente, che invece girano su circuito MasterCard. In quanto a sicurezza Paypal offre protezione sugli acquisti, ovvero se non arriva o arriva un prodotto che non è uguale alla descrizione che è stata fornita dal venditore, la società provvede al rimborso totale, inclusa spedizione, dell'intero importo. Mentre se si riceve un pagamento di tipo non autorizzato da un account che è stato rubato, da una persona diversa dal proprietario del conto, viene rimborsato anche in questo caso l'importo della vendita. Paypal è una società che punta, come già detto, a effettuare pagamenti Mobile, per garantire così maggiore efficienza e velocità alle transazioni quotidiane, non solo attraverso rete web; ed è per questo motivo che ha sviluppano una soluzione per inviare e ricevere pagamenti attraverso il cellulare, semplicemente utilizzando un applicazione per smartphone.[14]

1.3.2.4 Sicurezza Paypal

Molti siti, come anche Paypal al giorno d'oggi, utilizzano dei protocolli SSL per criptare le informazioni sensibili, di tipo finanziario, inviate su Internet per garantire così una maggiore affidabilità delle operazioni di pagamento. Tuttavia però un azienda informatica americana, Duo Security, ha riscontrato dei buchi, dei difetti, nella sicurezza dell'applicazione mobile di Paypal, trovando un mondo per poter aggirare, l'autenticazione a due fattori dell'utente. L'autenticazione a due fattori, è una funzione in grado di fornire una maggior sicurezza a tutti i processi di login di un qualsiasi account, richiedendo all'utente non solo un fattore di autenticazione come potrebbe essere la password, ma anche secondo fattore, che comprovi effettivamente la nostra identità. Il secondo fattore è dato da un codice univoco di identificazione, utilizzabile solamente una volta, che può essere spedito via Sms o via E-mail, quando si sta effettuando l'accesso a un account; una volta utilizzato questo codice non è più valido, non garantendo così a malintenzionati in ascolto la riusabilità di tale oggetto. L'autenticazione a due fattori è molto

utilizzata, anche soprattutto nel campo dell'Home Banking, per l'accesso a conti correnti online, dove il secondo fattore di autorizzazione è dato da uno strumento fisico, chiamato Token, che è appunto una sorta di chiave elettronica, che genera in maniera casuale a intervalli regolari, un codice univoco di identificazione, che è possibile utilizzare solamente una volta. Esistono anche i Mobile Token, che hanno la stessa funzione dei token normali solamente che permettono di generare le password per l'accesso senza bisogno di avere sempre dietro la chiavetta elettronica o carta (altra tipologia di token, che ha dimensioni di una carta di credito, contenente codici numerici monouso), ma avendo con se solamente il telefono cellulare.[15][16]

Paypal per l'identificazione a due fattori utilizza come secondo fattore di identificazione due tipologie di strumenti, il primo è una Security key, che è un dispositivo a forma di carta di credito, che crea un codice univoco di sicurezza, ogni volta che viene premuto il pulsante sopra di essa, da utilizzare al momento dell'accesso. Il secondo tipo può essere un Security key per Mobile, che consente, una volta effettuato l'accesso all'account con la password, di ricevere un Sms sul proprio cellulare, contenente un codice univoco e monouso, che dovrà essere inserito per procedere all'accesso autorizzato. La società Duo Security è riuscita quindi a bypassare questa sicurezza a due fattori dell'applicazione mobile di Paypal, semplicemente scavalcando la seconda verifica di sicurezza e riuscendo a entrare senza problemi. In questo modo un soggetto malintenzionato avrebbe bisogno solamente di riuscire ad entrare in possesso della e-mail e la password iniziali, attraverso tecniche per esempio di *pishing* o *ingegneria sociale*, per poter accedere direttamente al conto e poter inviare denaro. Il problema scoperto era dato dall'autenticazione ai servizi webAPI (Application Programming Interface) di Paypal. L'api di Paypal(api.paypal.com), utilizza un protocollo di comunicazione open, chiamato OAuth (Open Autorization, compatibile con qualunque applicazione web, mobile, desktop), tramite il quale un applicazione o un servizio web, può gestire l'accesso ai dati in maniera sicura.[17]

Utilizzando Burp Suite, una piattaforma java utilizzata per penetrare le applicazioni web e testare la loro sicurezza; hanno potuto analizzare il traffico HTTP/HTTPS, fra le applicazioni mobili e i servizi web, osservando principalmente il processo di autenticazione e concentrandosi su quale fosse

la differenza fra la risposta di un account abilitato all'autenticazione a due fattori e la risposta a conti senza abilitazione a due fattori. Quindi nella risposta, ritornata sotto formato JSON, per i dispositivi non abilitati, hanno potuto notare che l'attributo "**2fa_enabled**" era settato su TRUE, consentendo quindi all'applicazione Paypal di tornare nuovamente al login subito dopo aver eseguito l'accesso iniziale e aver mostrato il messaggio di errore indicante che l'autenticazione a due fattori non era abilitata. Utilizzando nuovamente la piattaforma Burp, sono così stati in grado di modificare l'attributo "**2fa_enabled**", settandolo a FALSE, riportando così l'applicazione mobile ad avere una sola forma di autenticazione, quella classica con e-mail e password, potendo di conseguenza procedere a trasferimenti di denaro.[18][19]

Un'altra modalità più semplice, scoperta e utilizzata, per eliminare l'autenticazione a due fattori per applicazione mobile (solamente però per applicazioni del sistema operativo iOS), sfrutta il fatto di sapere che l'applicazione una volta effettuato l'accesso iniziale con e-mail e password e mostrato il messaggio di errore di non supporto dell'abilitazione dell'autenticazione a due fattori, si disconnette, ritornando alla schermata di login iniziale. Questa modalità di evitare il secondo fattore di autenticazione si basa appunto sul momento esatto in cui passare con il cellulare alla modalità offline(modalità aereo), appena l'applicazione mostra il messaggio di errore, consentendo così al telefono di disconnettersi dalla rete garantendo un pieno acceso al conto Paypal.[20][21]

1.3.2.5 Apple pay

Apple pay è un nuovissimo, appena uscito, portafoglio elettronico utilizzato per il pagamento attraverso smartphone, creato dalla Apple e compatibile solamente con i suoi dispositivi (iPhone5 e modelli successivi), ed utilizzabile per il momento solamente negli Stati Uniti. Le carte che si possono utilizzare su questa applicazione, essendo appena uscita sul mercato, non sono molteplici, ma è possibile inserire carte MasterCard, Visa e American Express. Per acquisire i dati delle carte di credito con il telefono, bisogna scattare una foto, così facendo il telefono riconosce tutte le informazioni utili e compila un modulo, che dovrà poi essere inviato per una verifica, garantendo che l'utiliz-

zatore della carta sia veramente il proprietario, ed una volta che i dati sono stati verificati, si può procedere a transazioni di vario genere. A differenza di Google Wallet questo tipo di applicazione, una volta verificata l'identità del proprietario delle carte, per autorizzare i pagamenti non richiede l'inserimento di un PIN, ma utilizza un sistema di lettura di impronte digitali, appositamente studiato per iPhone. Quindi una volta avviata l'applicazione, bisogna avvicinare il dispositivo al terminale POS del negozio in cui stiamo effettuando la transazione, e mediante il chip NFC interno al telefono, viene avviata una connessione a corto raggio, che mi consente una volta individuata la carta di credito che voglio utilizzare, di procedere all'autenticazione e al pagamento di ciò che voglio acquistare. Unico inconveniente della modalità di autorizzazione mediante impronta digitale, è data purtroppo dagli acquisti online, perché a differenza di quelli fisici in un negozio vero e proprio dove utilizziamo il lettore di impronte digitali fornito dal telefono, per un negozio online, questa proprietà non è supportata ancora dai browser, costringendo di conseguenza gli utenti a utilizzare specifiche applicazioni per telefono di negozi online, che però, vista la scarsità di quest'ultime in circolazione, rendono l'identificazione uno strumento difficilmente sfruttabile.[22][23]

1.3.2.6 Sicurezza Apple pay

In quanto a sicurezza, anche qui viene utilizzato un chipset NFC, isolato dal resto dei componenti hardware del telefono, e quindi le informazioni possono essere salvate e utilizzate da questo elemento sicuro, che mi garantisce di ottenere un ambiente dinamico in cui posso gestire i dati in maniera completamente privata. L'elemento sicuro, è una memoria appunto, con crittografia ad alta sicurezza, che risiede nel chip NFC (solitamente è un chip smart card). La differenza riscontrata però fra Google Wallet e Apple Pay, è che quest'ultima, una volta effettuata l'autorizzazione di pagamento con l'impronta digitale, il chip NFC, connettendosi con il POS, genera un codice di sicurezza dinamico, univoco e monouso che viene usato per la singola transazione che si sta andando a effettuare, consentendo così di non conservare all'interno del dispositivo, o inviare, informazioni riguardanti la carta di credito, garantendo così una maggiore sicurezza dei dati. La generazione di un codice

univoco per la chiusura di ogni transazione, senza la conservazione fisica dei dati di pagamento, è una forma di sicurezza che consente a utenti malintenzionati che entrano in possesso del dispositivo elettronico o che effettuano attacchi per conoscere le informazioni relative, di non riuscire a riutilizzare tali numeri per commettere ulteriori abusi a discapito della vittima di turno. Introducendo il sistema di autenticazione mediante impronte digitali per il pagamento, in sostituzione al codice PIN, la società americana Apple, era convinta di fornire una maggior forma di sicurezza inattaccabile, che avrebbe garantito un maggior senso di protezione e affidabilità per l'utente utilizzatore dell'applicazione di pagamento. Cosa che però non si è verificata, visto che un'organizzazione di hacker con sede in Germania, chiamata Chaos Computer Club[5], è riuscita nell'intento di aggirare l'ostacolo utilizzando una procedura abbastanza semplice, che prevede l'impiego di alcuni tipi di materiali, reperibili nella vita quotidiana (tecnica descritta nei capitoli successivi). Apple era sicura di aver rilasciato un dispositivo che fosse molto più sicuro e affidabile rispetto alle versioni precedenti di altre tecnologie di identificazione a impronta digitale, cosa che appunto non è stata veritiera, visto che il sensore adibito alla scansione dell'impronta, possedeva solamente una maggiore risoluzione rispetto ad altri sensori. È stato quindi sufficiente creare una falsa impronta, con una risoluzione che garantisse l'elusione del sistema di sicurezza.[24][25]

1.3.3 Electronic payments

Con il termine di E-payment, includiamo tutti quei metodi di pagamento elettronico, che sono considerati sottoinsieme del commercio elettronico(e-commerce), per l'acquisto di beni o servizi attraverso la rete Internet.[26] Il pagamento elettronico è molto più comodo e veloce rispetto al comune pagamento in carta, che invece è molto più dispendioso perché prevede oneri più elevati per la gestione delle banconote. Questa modalità prevede comunque l'utilizzo delle più comuni tipologie di pagamento che utilizzano la moneta elettronica per effettuare le transazioni. Il vantaggio del pagamento elettronico consiste nel dare a ogni piccolo utente la possibilità di restare co-

[5] it.wikipedia.org/wiki/Chaos_Computer_Club

modamente nella propria abitazione, magari davanti a un monitor computer, ed effettuare tutte le operazioni di acquisto o vendita di prodotti o servizi, raggiungendo l'intera rete globale. Definendo la monete elettronica[2], possiamo dire che questa rappresenta un valore monetario memorizzato elettronicamente, ed esprime un credito nei confronti di un ente che ha emesso tale valore, dietro però a un ricevimento di fondi monetari; ed utilizzabile per realizzare pagamenti verso soggetti fisici o giuridici(ad esempio le aziende o commercianti). Gli strumenti di pagamento più comuni utilizzati attraverso la rete sono :[27]

- Carte di credito
- Carte prepagate
- Bonifici
- E-Wallet

All'interno della rete web, esiste anche un'altra tipologia di moneta elettronica , diversa dal concetto di moneta soggetta all'emissione e gestione da parte di un istituto finanziario e da noi conosciuta; questa moneta si avvicina più a un concetto definito con il nome di cripto-moneta data la sua natura. Con il termine di cripto-valuta quindi indichiamo una moneta decentralizzata, cioè che non dipende da nessuna autorità centrale o banca, la cui implementazione è basata sul concetto di crittografia.

1.3.3.1 I bitcoin

I bitcoin, sono una particolare moneta elettronica creata da Satoshi Nagamoto, nel 2009; questa moneta sfrutta una rete chiamata Bitcoin che usa una tecnologia di tipo peer-to-peer per gestire l'emissione e le transazioni della moneta attraverso la rete Internet. Bisogna fare una semplice distinzione tra bitcoin in minuscolo, che indica la moneta, e Bitcoin in maiuscolo che invece indica la rete open-source utilizzata per lo scambio, alla quale ognuno può prendere parte. Come già accennato la differenza principale fra le altre valute e bitcoin, è che quest'ultima, non fa uso di nessuna autorità centrale o banca, ma utilizza un database distribuito, cioè un database che non si trova

su un solo computer connesso, ma bensì ripartito fra diversi nodi all'interno della rete (da qui la tecnologia peer-to-peer), che tengono traccia di tutte le transazioni effettuate. Gli utenti della rete sono quindi in grado di conservare il proprio denaro virtuale sul nodo di proprietà e scambiarlo quando si ritiene necessario da un terminale ad un altro. Questo tipo di moneta sfrutta il concetto di crittografia, perchè utilizza la crittografia a chiave pubblica e a chiave privata, per potere gestire tutti gli aspetti riguardanti l'assegnazione della proprietà o la creazione di nuovi bitcoin. All'interno della rete Bitcoin, è consentito il possesso delle monete, mediante un Wallet elettronico che contiene chiavi e indirizzi per effettuare tranzazioni, tutto ciò in maniera molto anonima date le chiavi di criptazione, anche perchè gli indirizzi forniti, non contengono nessuna informazione riguardante il proprietario del portafoglio. Essendo il sistema completamente pubblico e quindi trasparente, per il trasferimento di bitcoin da un terminale ad un altro, occorre avere conoscenza di un "indirizzo pubblico", che ogni utente della rete possiede appunto nel proprio portafoglio per consentire così il passaggio di moneta verso quel determinato nodo. All'interno dei portafogli possiamo quindi trovare una coppia di chiavi crittografate, come già detto, la chiave crittografata pubblica, chiamata anche indirizzo pubblico, la quale serve dunque come un punto di riferimento per lo scambio, invio e ricezione, dei pagamenti. Mentre la chiave crittografata privata, è una chiave che non è visualizzabile da nessun'altro utente all'interno della rete, se non dal proprietario stesso del Wallet, che garantisce l'autorizzazione di un pagamento da parte di un utente in maniera del tutto univoca, garantendo quindi la proprietà della moneta di quell'individuo. Gli indirizzi utilizzati, sono delle sequenze alfanumeriche casuali di caratteri a 33 cifre, che iniziano sempre con il numero 1, aventi ad esempio la seguente forma: 175tWpb8K1S7NmH4Zx6rewF9WQrcZv245W. Tutti gli utenti possono avere, senza nessun tipo di vincolo, un numero qualsiasi di indirizzi, permettendo così ad ogni individuo di avere una nuova coppia di chiavi per ogni transazione e garantendo di conseguenza un maggiore anonimato. Il funzionamento delle transazioni è abbastanza semplice, visto che i bitcoin contengono l'indirizzo, ovvero la chiave pubblica del proprietario, quando un qualsiasi utente che chiameremo A, trasferisce un bitcoin a un altro utente, che chiameremo B, rinuncia alla proprietà della moneta, aggiungendo l'in-

dirizzo pubblico(chiave pubblica) di B alla moneta in questione e firmando l'autorizzazione con la chiave privata di A. Per evitare frodi, come ad esempio rispendere una moneta bitcoin già utilizzata in precedenza, il sistema Bitcoin conserva all'interno della rete un apposito registro crittografato riguardante tutte le transazioni effettuate, ed ogni volta che viene praticato un nuovo scambio, viene utilizzato per controllare la validità del gettone in questione. La transazione dei bitcoin viene inserita in un apposito messaggio, contente indirizzo e importo che si vuole trasferire, ed ogni nodo della rete che riceve il messaggio ed aggiorna la propria copia del registro contenente tutte le transazioni, per poi passare il messaggio alla rete. Una nuova firma digitale viene generata da un messaggio di transazione e la chiave privata. Il resto dei nodi, per sapere poi se l'operazione effettuata è veritiera, controllano se le firme crittografiche generate dal messaggio sono valide, in maniera quindi da dimostrare che la firma digitale generata con la chiave privata corrisponda alla chiave pubblica; considerando che la firma digitale sarà diversa da ogni messaggio, quindi non riutilizzabile per una transazione diversa. Lo svantaggio di questa moneta però è dato dal fatto che sia impossibile da tracciare, rendendola quindi di fatto una moneta usata come strumento utile per tutte quelle tipologie di transazioni illegali, come la compravendita di armi o droga.[28][29][30][31] I bitcoin sono un sistema di pagamento che sta prendendo sempre più piede nel mondo, anche in Italia, al giorno d'oggi ci si può pagare praticamente di tutto e sempre più commercianti stanno iniziando ad accettarli. Esistono già dei particolari ATM, conosciuti comunemente come sportelli bancomat, che prendono in ingresso una valuta, che può ad esempio essere Euro, e la scambiano con i bitcoin, consentendo a chiunque anche a chi non se ne intente di utilizzare questa moneta. In Italia queste macchinette avrebbero raggiunto il numero di 5, una delle quali appunto in Emilia-Romagna, in un negozio che vende scarpe da tennis, skateboard e abbigliamento. In questo negozio appunto, sarebbe possibile effettuare acquisti utilizzando bitcoin, ma anche convertire euro in quest'ultimi, data la presenza di uno sportello ATM.[32]

1.3.3.2 Person to person payments (P2P)

Con questa tipologia di pagamento, si intende definire, tutti quei trasferimenti di denaro che avvengono da una persona, verso un'altra. Basti pensare a quelle transazioni che possono avvenire per pagare una baby-sitter, oppure trasferimenti di fondi che un immigrato può dare alla famiglia che si trova ancora nel proprio paese d'origine. Tutte queste categorie, rappresentano proprio dei sistemi di pagamento che una persona effettua verso un'altra, utilizzando determinati mezzi che consentano di mobilitare somme di moneta elettronica con facilità. Nei New Digital Payment, avrei dovuto quindi aggiungere un'ulteriore tipologia di sistema di pagamento, appunto i pagamenti P2P, i quali però inserirò all'interno dei metodi di pagamento elettronico per il semplice motivo, che per pagamenti diversi dal contante, gli strumenti utilizzati dal P2P fanno comunque parte degli strumenti utilizzati per il pagamento elettronico, dato che le transazioni devono avvenire attraverso una rete. In conclusione si può quindi assumere che l'utilizzo dei mezzi di pagamento P2P, comporta gli stessi rischi di sicurezza, vantaggi/svantaggi dei sistemi utilizzati per il pagamento elettronico. Ad esempio una persona potrà aver aperto un conto corrente online presso una banca, che utilizzerà per l'invio di denaro verso un'altra persona per il pagamento di un servizio, incorrendo nei problemi di sicurezza che la gestione di un conto online comporta.[33]

1.3.4 Contactless payments

Con il termine di pagamenti contectless, si intendono tutti quei sistemi di pagamento che utilizzano particolari strumenti elettronici, come ad esempio carte/smartcard, orologi, portachiavi, ecc; forniti di una particolare tecnologia chiamata RFID (Radio Frequency Identification), sono in grado di effettuare il pagamento in maniera efficiente e sicura, senza utilizzare contatto diretto o inserimento. Sono sistemi rapidi per il pagamento di piccole spese quotidiane. Per questo tipo di pagamenti, è sufficiente avvicinare il dispositivo elettronico a un lettore in maniera da permettere a quest'ultimo di leggere tutte le informazioni relative alla transazione che si sta andando a compiere. Sicuramente i tempi di attesa rispetto agli altri metodi di

pagamento sono molto ridotti, il conctactless, consente non solo, una volta avvicinato il dispositivo al lettore, di autentificarsi in maniera rapida e sicura, ma consente anche la manipolazione dei dati in lettura ed in scrittura. In quanto a sicurezza viene utilizzata una tecnologia che non necessita di un inserimento di un PIN, per l'autenticazione, anche perché gli acquisti che possiamo effettuare tramite avvicinamento, riguardano spese di denaro che non possono superare dei limiti stabiliti, che sono all'incirca di 25 euro.[34] Alcune tipologie particolari di dispositivi utilizzati per il pagamento contactless sono:

- Carte di credito paypass
- Watch2pay
- Telepass

Carte di credito paypass: Le carte di credito paypass, sono delle particolari carte di credito o prepagate, che sfruttano la tecnologia conctactless e consentono di effettuare acquisti sicuri e tranquilli, che non superino però importi di 25 euro, perché altrimenti si procederà in maniera classica, con firma di ricevuta o inserimento PIN. Come per le altre tecnologie conctactless, basterà avvicinare questa carta a un lettore POS, il quale autorizzerà e consentirà il pagamento dell'importo dovuto, senza la firma di nessuna ricevuta e senza l'inserimento di nessuna chiave di sicurezza.[35]

Watch2pay: È un particolare orologio utilizzato per effettuare pagamenti conctactless, il quale attraverso una speciale sim card Mastercard paypass, si comporta come una normale carta di credito a cui viene associato un conto corrente dove è possibile depositare e prelevare fondi monetari. La piccola sim va inserita all'interno dell'orologio, per poi iniziare a godere di tutti i vantaggi di una normale carta MasterCard, effettuando gli acquisti semplicemente avvicinando l'orologio a un lettore, per poter procedere con il pagamento.[36]

Telepass: Il telepass è un dispositivo utilizzato per i pagamenti conctactless per la riscossione automatica del pedaggio nelle autostrade. È composto da una particolare unità, generalmente chiamato appunto Telepass, che risiede all'interno di un'automobile (solitamente tenuto sul parabrezza), ed un componente che invece deve risiedere a terra, sui caselli autostradali, al quale

spetterà il compito di lettore del Telepass. Questo particolare strumento che utilizza la tecnologia RFID, è alimentato in maniera indipendente da una batteria, permette di trasmettere i dati contenuti al suo interno solo quando interrogato dal lettore, consentendo all'automobilista, la riscossione automatica del pedaggio grazie appunto alla tecnologia DSRC (Dedicated Short Range Communication). La trasmissione fra il lettore e il Telepass avviene a una frequenza di 5,8 Ghz, dando così al lettore la possibilità di poter leggere i dati e verificarli, consentendo quindi a un automobilista in prossimità di un casello di poter passare una volta che la sbarra si sarà sollevata.[37]

Capitolo 2

Evoluzione della moneta

Questo capitolo punta a spiegare i vari sviluppi, vantaggi e svantaggi intercorsi nella storia, riguardanti i sistemi di pagamento in tutte le sue forme, partendo da quella primitiva (il baratto) ed arrivando a quella odierna. In ogni epoca storica con la nascita di nuovi sistemi di pagamento, si è sempre cercata una tecnologia che fosse in grado di supportare le nuove forme di moneta. Anche le tecnologie di conseguenza, hanno avuto nel corso della storia, un evoluzione sempre maggiore, fino ad arrivare alle forme di innovazione conosciute oggi.

2.1 Prime forme di pagamento

Il denaro, ha sempre subito processi di sviluppo degni di nota, che hanno condizionato in gran parte i comportamenti socio-economici di ogni comunità. A partire dalla forma di scambio più primitiva conosciuta, il baratto. Il baratto è la prima forma di pagamento accettata nella storia, esso impone una scambio diretto di un bene o servizio fra due o più persone, senza l'utilizzo della moneta.[38] La nascita del baratto risale a quando ancora le persone vivevano riunite in piccoli gruppi, in cui ognuno svolgeva le attività che gli garantissero la sopravvivenza. In questo periodo nacquero così le prime forme di pagamento caratterizzate dallo scambio di beni; nasceva così la prima tipologia di pagamento definita come **MONETA-MERCE**.[2]

I limiti del baratto erano dati dalla difficoltà di riuscire a incontrare qualcuno che fosse in possesso di un bene desiderato e che accettasse di scambiarlo per un bene offerto. Gli svantaggi erano comunque numerosi, vi era il vincolo della durevolezza, perché non tutti i beni conservavano il loro valore per lo stesso tempo, il problema dalla trasportabilità, ovvero, non tutte le merci potevano essere mobilitate con facilità e perciò risultava difficile uno scambio veloce e pratico. Un ulteriore problema era dato dalla qualità difficilmente verificabile della merce, cioè non si poteva dare un giusto valore di cambio ad alcuni prodotti, ed infine cosa molto importante, la complicazione derivante dalla divisibilità, la quale non consentiva di effettuare delle divisioni eque per alcuni beni, per intenderci ad esempio era difficile dare un uovo a metà, o lo si dava intero oppure non lo si dava affatto. Questo sistema non garantiva inoltre nessuna sicurezza o tutela, perché le merci una volta effettuato lo scambio, erano comunque soggette a rischio di furti oltre che agli svantaggi elencati precedentemente. Naturalmente si abbandonò questo sistema di pagamento MONETA-MERCE e si passò ad un altro sistema di pagamento più evoluto , cioè la moneta coniata con metalli preziosi.

Il baratto però al giorno d'oggi non è svanito del tutto come strumento di pagamento, ma sta tornando come nuova forma di pagamento, conosciuta con il nome di *Bartering* , ovvero una pratica commerciale che consente di scambiare beni e servizi tra le imprese in maniera da avere una compensazione. È uno strumento di pagamento che consente di acquisire beni e servizi senza risorse liquide, ad esempio una azienda che opera in certo settore e che vende alcuni tipi di beni, può vendere a un'azienda che pagherà il corrispettivo importo monetario dei beni acquistati, mediante cessione di servizi o prodotti che fanno parte di quel settore (ad esempio fornirà un valore di pubblicità sul mercato, equivalente al valore dei prodotti acquistati).[39]

2.2 La moneta

Visti i vari svantaggi a cui il pagamento tramite baratto conduceva, si decise appunto di passare a una nuova forma di pagamento, quella che ricorreva all'uso di una moneta che veniva coniata da metalli preziosi. L'utilizzo di questi metalli preziosi (ad esempio barre di oro ed argento), garantiva

appunto alcuni vantaggi, fra i quali: i metalli impiegati erano solitamente formati da materiali rari, non subivano un deperimento attraverso il tempo, ed erano facilmente trasportabili, consentendo di avere un valore elevato in poco spazio. Ulteriore caratteristica vantaggiosa era data dalla possibilità di poter dividere in maniera semplice questi materiali, consentendo così di poter perfezionare lo scambio raggiungendo con precisione l'ammontare della transazione. Le prime monete furono il frutto della fusione di questi metalli preziosi ed i Greci, intorno al 700 a.c furono la prima popolazione a coniare monete d'argento, le quali attesero diversi anni prima di poter essere largamente diffuse in tutto il mondo, da Romani e Greci stessi, i quali promossero anche conoscenze di tecniche per la coniazione. La moneta si sviluppo velocemente attraverso gli anni perché era un sistema di pagamento rapido e semplice, che facilitava lo scambio, molto più complesso con il baratto, consentendo di pagare un giusto valore per un determinato bene o servizio. Tuttavia come accadeva per il baratto se queste somme di moneta non erano conservate o gestite in maniera sicura, potevano essere soggette a furti o truffe. Le monete però presentavano comunque alcuni svantaggi riguardanti di fatto i metalli preziosi, che come tali, una volta che venivano utilizzati in grandi quantità erano difficilmente reperibili, ed inoltre il trasferimento d'importanti somme di denaro era molto più faticoso ed anche rischioso. Dati i vari difetti si pensò quindi di introdurre una nuova forma di pagamento, una *"moneta cartacea"*, che non fosse vincolata alla limitata disponibilità di metalli preziosi e a tutte le problematiche inerenti.[2]

2.3 Moneta cartacea

Le prime forme di sistemi di pagamento basate su moneta cartacea, furono usate a partire dall'anno 800 d.c, da le popolazioni cinesi che iniziarono a emettere questa banconota, la quale era una moneta del tutto inutile, perché priva di ogni valore intrinseco, ma che godeva di fiducia, perché il potere d'uso e d'accettazione derivava da un decreto imperiale.

Iniziò così ad emergere successivamente il fenomeno di emissione, da parte di mercanti e industriali, di lettere di credito, che provavano, che un soggetto aveva versato del denaro a questi soggetti, ricevendo in cambio un corri-

spettivo documento che garantisse appunto, la conversione dell'ammontare equivalente in moneta metallica. Questo processo, impegnava perciò l'emittente della lettera di credito, a riconoscere al portatore di questo documento, un valore nominale in moneta metallica, che poteva essere passato di mano in mano, verso soggetti differenti dal portatore iniziale, potendo così ottenere grandi vantaggi per le operazioni di transazione in termini di efficienza. Fu così aperta la strada alla banconota convertibile, con cui chiunque avesse voluto effettuare acquisti di beni o servizi in una piazza di commercio poteva utilizzare queste lettere di cambio per poter effettuare pagamenti riducendo i rischi legati al trasporto della moneta, limitando perciò i rischi di furto. Nacquero di conseguenza le attività di deposito, con cui i mercanti-banchieri, garantivano la custodia dei fondi monetari, in cambio di commissioni. Questi soggetti si trovarono così a dover gestire ingenti fonti di denaro, che iniziarono anche a prestare, in cambio di una remunerazione dei rischi a cui andavano incontro, facendo così nascere il concetto di *attività creditizia* e creando una nuova figura di intermediario finanziario chiamato banca di emissione, che si occupava appunto di emettere monete e concedere prestiti. La prima banca, il Banco di San Giorgio, nacque nel 1407 a Genova e fu la prima banca moderna che si occupava della gestione del debito pubblico.[40]

Alcune banche successivamente, dopo lo sviluppo della banconota, operavano in maniera meno prudente, rilasciando sul mercato, grandi quantità carta, superiori ai depositi effettivi di metalli preziosi, rischiando perciò di non essere in grado di garantire la totale copertura del titolo nel caso avessero dovuto far fronte alla richiesta di conversione. Vista questa carenza di cautela e per ovviare a ciò i vari Stati, resero prerogativa, l'emissione della banconota, solamente a una tipologia di banca: la *banca centrale*. Fatto sta che comunque si assistette alla nascita di un nuovo sistema di pagamento, quello appunto della moneta cartacea con corso legale, la quale godeva appunto della possibilità di semplificare le transazioni, creando un titolo che fosse facilmente trasportabile e scambiabile ovunque, che venisse accettato da tutti, perché appunto in suo valore corrispondeva a una quantità depositata di metalli preziosi e la legge gli aveva conferito un potere liberatorio, garantendo l'accettabilità obbligatoria in caso di pagamento. Tuttavia, anche se questa moneta cartacea poteva portare numerosi vantaggi, come sistema di

pagamento, per gli scambi di merci o servizi, era comunque sempre soggetta a rischi di smarrimento o addirittura di furto, non garantendo nessuna forma di tutela per il soggetto utilizzatore.[41][42]

2.4 Moneta bancaria

Lo sviluppo delle banconote e la relativa emissione, portò la nascita di un altro sistema di pagamento, riguardante una forma di moneta basata su conti gestiti ed organizzati presso banche commerciali e prendeva appunto il nome di moneta bancaria. In maniera diversa rispetto a quanto accadeva per le banconote, il pagamento di transazioni veniva svolto in questo caso richiedendo procedure che consentissero al titolare del conto, di dare l'ordine alla propria banca il trasferimento di moneta verso il beneficiario del pagamento. Tali procedure garantirono la formazione di nuovi strumenti per effettuare i pagamenti che presero la forma di assegni bancari, bonifici e giroconti. Il primo assegno bancario nella storia fu emesso da *"Hoare's Bank"* di Londra nel 1763.[43]

Per garantire comunque, nello stesso tempo i pagamenti fra clienti di differenti banche, vennero realizzati sistemi e procedure di trasferimenti monetari che si basavano sull'impiego di un intermediario, ovvero le banca centrale, che deteneva al suo interno conti su cui erano scritti i movimenti di pagamento fra le banche commerciali. Queste nuove procedura di pagamento, delineava almeno quattro aspetti positivi importanti: La sicurezza, perché il rischio di smarrimento e furto era diminuito notevolmente. La certezza, perché la circolazione di moneta bancaria è vincolata da procedure riservate, strettamente personali e inflessibili. Legalità, perché la gestione di ogni pagamento, limitava di molto le attività illecite. Praticità, perché permetteva di effettuare acquisti senza doversi preoccupare anticipatamente del contante. Nonostante l'evoluzione storica avesse portato lo sviluppo e l'innovazione della moneta fino a un punto, in cui si iniziavano a riscontrare vantaggi notevoli e una maggior sicurezza di utilizzo, rispetto ai metodi di pagamento iniziali, la nascita delle banche e della relativa moneta bancaria diede un maggiore impulso ad uno sviluppo tecnologico che avrebbe continuato a portare cambiamenti nel corso della storia. Questo sviluppo vide la nascita e la

crescita di alcuni strumenti di pagamento, che garantivano ancora di più una maggiore praticità, garanzia ed una velocità di riscontro migliore da parte del soggetto debitore e creditore. Di fatto verso la metà del Novecento, la nascita dell'informatica e della telematica, portarono un vero e proprio cambiamento per i sistemi di pagamento, veniva data da quel momento la possibilità di poter memorizzare le informazioni e i dati in maniera digitale e successivamente, poterli scambiare attraverso la rete. Realmente si era entrati in una nuova epoca, che vedeva l'inizio dello sviluppo di un nuovo concetto di pagamento, l'elettronic-payments. Uno primo risultato scaturito da questa nuova rivoluzione, è conosciuto oggi con il nome di carta di credito. [2]

2.5 Carta di credito

Il concetto di carta di credito va fatta risalire all'epoca storica del 1730 dove un commerciante di mobili di pregio, un certo Christopher Thomson, ebbe un idea: far pagare ai propri clienti, che non potevano saldare l'intero importo subito, delle piccole rate mensili fino al raggiungimento del prezzo concordato. Questo sistema venne utilizzato da alcuni mercanti fino a quando, nel 1914 la società Western Union creò e distribuì ai propri clienti una carta metallica, in grado di dilazionare pagamenti per i servizi utilizzati. Anche altre società successivamente rilasciarono le proprie carte di credito per consentire agli utenti utilizzatori dei servizi di queste aziende, il pagamento rateale. Dopo la seconda guerra mondiale, grazie ad un aumento di domanda dei beni di consumo di massa, nacque la prima e vera carta di credito. L'anno di nascita della carta risale al 1950, dove la Diners Club inc., società ideatrice, aveva concepito questo strumento per poter essere utile a uomini d'affari, concedendogli fino a 60 giorni di credito per riuscire a regolare il pagamento di beni acquistati. La carta fu utilizzata soprattutto nei settori di turismo e divertimento. In seguito anche altre banche capirono le potenzialità di questi strumenti di pagamento e così nel 1958 anche la American Express mise in circolo la sua carta. Nel 1967 quattro banche della California, crearono il programma MasterCharge, per poter competere con il sistema introdotto da Bank of America, che aveva creato la prima carta di credito revolver la quale sfruttava un circuito chiamato BankAmericard. Verso metà degli anni set-

tanta il settore delle carte di credito cercò di espandersi oltre che in America in altri stati e visto che il nome BankAmericard avrebbe potuto creare problemi, fu sostituito con il nome VISA e anche MasterCharge, fu rinominato MasterCard.[44] Nel 1958, in Italia, fu emessa la prima carta di credito della Diners club e successivamente BankAmericard nel 1968. Inizialmente vennero distribuite carte composte da un strato di PVC (polimero del cloruro di vinile, una sorta di materiale plastico) con una semplice colorazione con nome del cliente e numero di conto impressi in rilievo.[45] Successivamente con lo sviluppo della tecnologia nel 1969 la prima banda magnetica, venne applicata sul retro di una carta di credito, consentendo a chiunque effettuasse acquisti con tale strumento di passare semplicemente la carta in un terminale di un commerciante, il quale effettuava la lettura dei dati identificativi impressi sulla banda e autorizzava così il procedimento d'acquisto del relativo bene. La banda magnetica è uno strumento molto simile al nastro di un audiocassetta, è caratterizzato da un sottile strato di materiale composto da particelle in resina magnetizzabili, ed è sostanzialmente suddivisa in tre tracce, dove vengono contenuti i dati per l'utilizzo della carta. Nelle prime due tracce troviamo i dati preregistrati da utilizzare solamente per la lettura mentre nella terza parte possiamo effettuare operazioni di scrittura. La capacità totale della banda è composta da 226 caratteri alfanumerici. Per imprimere i dati all'interno viene utilizzato un campo magnetico in prossimità della banda, dove le particelle contenute vengono polarizzate in una precisa direzione. Per la lettura in maniera uguale, il passaggio di una testina sulla banda, provoca dei picchi di corrente indotti dalla polarizzazione della carta, codificandone il contenuto in base a valori 0 e 1. La maggior parte delle carte di credito a banda magnetica utilizzano standard ISO (International Organization for Standardization) 7811, che specificano la posizione dei dati sulla carta.[46] Tuttavia questo sistema di pagamento fosse molto utilizzato sul mercato, presentava svantaggi notevoli, ovvero, una scarsa capacità di memorizzazione dei dati, inoltre essendo la banda magnetica uno strumento molto delicato, il continuo sfregamento per la lettura dei dati, poteva portare all'usura di questo materiale, con il relativo rischio di cancellazione o corruzione dei dati. Anche il contatto con superfici o oggetti magnetizzati poteva causare la smagnetizzazione totale o parziale delle informazioni contenute.

Per ovviare a questi inconvenienti, furono introdotti successivamente, nuovi materiali, high-coercivity (Hi-co), che consentivano l'alterazione della banda magnetica solamente da campi magnetici molto superiori a quelli generati dai comuni magneti. Tuttavia, il continuo bisogno di sicurezza e la conseguente tutela verso le frodi, fece sviluppare nuove tecnologie che prevedevano l'impiego di particolari microchip all'interno della carta di credito, rendendola perciò uno strumento molto più sicuro ed affidabile rispetto ai primi strumenti inventati. Nel corso del tempo le carte di credito a banda magnetica, furono sostituite dalle carte a microchip e dalle carte ibride (banda magnetica e microchip).[45] Di fatto le prime tipologie di carte di credito, che possedevano solamente la banda magnetica erano limitate in quanto a fattori di sicurezza, visto che le informazioni incise sulla banda magnetica potevano facilmente essere duplicate e riutilizzate, grazie alla procedura che noi conosciamo oggi come skimming, ovvero la copia di dati contenuti nella banda magnetica, su una carta falsa, utilizzata successivamente all'insaputa del proprietario.[47]

2.6 Nascita Home Banking

Un ulteriore effetto dello sviluppo dei pagamenti elettronici, fu introdotto dalla nascita dell'Home Banking[48], quando i primi veri e propri servizi bancari, iniziarono a operare nel 1981 a New York. In questi anni, quattro delle principali banche di questa città, garantivano servizi bancari online, utilizzabili attraverso il sistema Videotex[6], ovvero un sistema che permetteva di trasmettere dati e messaggi (solitamente pagine di testo), attraverso una rete telematica, ed in grado di visualizzare le informazioni sul televisore. Questo sistema fu successivamente abbandonato da tutti, ad eccezione del Regno Unito, che apportò diversi cambiamenti e miglioramenti, fino a quando nel 1983, prese vita il primo Istituto in grado di fornire servizi bancari online restando comodamente a casa. Il Nottingham Building Society, si basava su un tipologia di sistema chiamato Prestel[49], anche questo un sistema telematico, basato sul concetto di Videotex, che però vide la sua scomparsa con

[6] it.wikipedia.org/wiki/Videotex

l'avvento di Internet. Semplicemente utilizzando una connessione alla rete, con un computer o un televisore e una tastiera, era possibile per l'utente effettuare operazioni online, che gli consentissero di controllare ad esempio il saldo del suo conto corrente o effettuare trasferimenti di denaro per pagamenti di bollette. La nascita di una nuova rete, Internet, vide la scomparsa di tutte le altri reti telematiche utilizzate precedentemente e l'inizio del concetto di Internet Banking. La prima banca a utilizzare questo servizio fu la Stanford Federal Credit Union, che nell'ottobre del 1994 rese disponibile per la prima volta ai propria clienti la banca online. Attraverso l'Internet Banking, come suggerisce la parola, è possibile effettuare sul sito della banca online, delle operazioni di transazione in maniera elettronica senza dovere fisicamente recarsi presso il proprio istituto di credito. Il sistema Prestel, possedeva alcuni svantaggi, ed è anche per questo che venne abbandonato, la sua rete non garantiva effettivamente un grande grado di sicurezza. Ogni abbonato alla rete possedeva un codice personale e l'accesso a ogni servizio richiedeva l'immissione di un secondo codice segreto.[50] Un hacker di nome Robert Schifreen, fu in grado di violare la rete telematica di Prestel, riuscendo a scoprire semplicemente un ID e una password e ricavando così l'ammissione al sistema senza pagare. Con queste credenziali, fu in grado di accedere a zone, all'interno della rete, solitamente non accessibili a chiunque, riuscendo ad ottenere l'intera gestione del sistema, e la conseguente possibilità di modifica ed alterazione di qualsiasi pagina presente su Prestel.[51] La nascita di Internet e l'incessante sviluppo dei metodi di pagamento elettronico, portarono un conseguente aumento e perfezionamento dei protocolli di sicurezza; le reti obsolete che non erano in grado di poter fornire un livello di protezione adeguato, vennero eliminate e sostituite da sistemi che fossero in grado di fronteggiare frodi future.

2.7 Smartcard : evoluzione bandamagnetica

Come accennato in precedenza, la tecnologia nata e sviluppata con la carta di credito inizialmente era rappresentata dalla banda magnetica, che fu tuttavia successivamente sostituita dalla smart card, per differenti motivi legati alla sicurezza. La smart card è un termine che indica una carta di cre-

dito, che è dotata di un microprocessore, in grado di dare maggior sicurezza e riservatezza dei dati memorizzati al suo interno. Queste particolari carte fecero il loro ingresso nel 1970, quando Kunitaka Arinura in Giappone, ne depositò il brevetto. In seguito tra il 1974 ed il 1976, Roland Morèno, in Francia, costruì una smart card più evoluta rispetto a quella del giapponese e con funzionalità più elevate. Queste nuove tipologie di smart card vennero adottate in sostituzione a quelle con banda magnetica per il semplice fatto che avevano una caratteristica che le rendeva più evolute rispetto alle altre, ovvero al suo interno la scheda, possedeva un sistema di controllo dell'accesso alla memoria della carta, che era basato su password. Il formato delle nuove carte era esattamente identico a quelle con banda magnetica, l'unica differenza era data appunto dal chip che si trovava al suo interno, che gli consentiva di memorizzare le informazioni in maniera più sicura, che sarebbero in seguito state utilizzate per effettuare transazioni. In aggiunta la nuova e più grande capacità di memorizzazione del microchip aumentava di fatto le funzionalità della carta rendendola una tipologia di smart-card "multi-applicazione", in grado cioè di contenere al suo interno non soltanto i dati riguardanti il proprietario, le informazioni di accesso e autenticazione, ma dando la possibilità di raccogliere punti di campagne promozionali e di lavorare direttamente sui dati, prendendo decisioni autonome sulle variazioni di nuove azioni richieste. Grazie a queste nuove tecnologie, si assistì nel 1993, alla nascita di uno standard chiamato EMV, ossia una raccolta di specifiche (basate su ISO 7816[7]), voluta appunto dai maggiori gestori di carte di credito (Europay, Mastercard e Visa) in grado di regolare e standardizzare in maniera migliore, con maggior dettaglio, le applicazioni di pagamento elettronico basate su carte di credito con microprocessore. Una sorta di regole per garantire alle smart card e ai terminali di pagamento la possibilità di interazione fra loro.[45] Queste specifiche riguardano :[52]

- Requisiti di carattere fisico ed elettronico

[7]ISO 7816: è l'estensione degli ISO 7810-7813, nati per carte di credito a banda magnetica usate per applicazioni bancarie. Con ISO 7816, vengono definiti i parametri dei contatti elettrici per carte a microprocessore in funzione della sostituzione di tutte le carte bancarie.

- Modalità con cui condurre transazioni
- Struttura dal punto di vista della sicurezza
- Interoperabilità fra carte e terminali a livello globale
- Linea guida e tempi per il passaggio da banda magnetica a nuovi sistemi.

I vantaggi subentrati a livello di sicurezza, vengono definiti da EMV secondo quattro elementi principali, ossia, autenticazione carta offline, dove viene stabilita se la carta è autentica o meno da un terminale POS, parametri di gestione del rischio, in cui la carta effettua la registrazione di ogni transazione eseguita avvisando se si verificano certe condizioni, offline-pin, dove il PIN(Personal Identification Number) essendo conservato in maniera sicura all'interno della carta può essere verificato facilmente in ogni momento, ed infine autenticazione carta on-line, dove la carta può essere appunto autenticata tramite la connessione alla rete. L'introduzione dello standard EMV puntò alla realizzazione di sistemi di pagamento che fossero in grado di ottenere una sicurezza maggiore, rispetto ai precedenti (vedi carte banda magnetica), garantendo una riduzione delle frodi e delle attività di falsificazione, inoltre che potessero far fronte a un numero sempre più crescente di transazioni, visto che per le carte a banda magnetica ogni volta veniva richiesta la connessione on-line per poter ottenere le autorizzazioni bancarie, con il conseguente svantaggio della perdita di tempo per il collegamento, cosa differente invece per le smart card, dove la possibilità di poter eseguire operazioni off-line, senza aver necessariamente bisogno di una rete attiva, garantiva la possibilità di effettuare pagamenti in qualsiasi condizione o momento. Infine l'obbiettivo di tale standard era quello di sviluppare a livello globale le tecnologie a microprocessori, facilitando così le operazioni di transazione e la comunicazione fra le diverse banche e circuiti di pagamento , ed ultimo punto, si poneva il fine di riuscire ad accorpare tutti i sistemi di pagamento sotto un unica struttura EMV. [53]

2.8 Nascita conctactless

Lo sviluppo dei microprocessori cambiò il nostro modo di utilizzare gli strumenti di pagamento e portò successivamente alla nascita e lo sviluppo di ulteriori mezzi che consentissero appunto di effettuare transazioni in maniera semplice e comoda. Il 1997 vide la nascita di un nuovo metodo di pagamento, quello conctactless, dove una società petrolifera, la Mobil Oil Corp, la prima nel suo genere, offrì un servizio chiamato Speedpass, che consentiva di poter pagare il rifornimento di carburante, utilizzando un semplicemente un portachiavi in plastica. Questo strumento, era dotato di una particolare tecnologia DST(Digital Signal Trasponder) RFID (radio frequency identification) , che consentiva all'utente utilizzatore, di poter pagare l'acquisto di benzina, solamente avvicinando il portachiavi alla pompa, dove era appositamente indicato. Il portachiavi possedeva un chip RFID(un Trasponder passivo) crittografato, che utilizzava in fase di autenticazione, ed un'antenna. La pompa di benzina invece conteneva un lettore in grado di poter codificare il segnale ed autorizzare il pagamento, controllando il codice univoco di identificazione (ID number) che era contenuto nel chip (del portachiavi) e che veniva trasmesso in fase di avvicinamento, tramite un particolare algoritmo di crittografia a blocchi. Una volta che l'autorizzazione era stata concessa, le pompe di benzina si accendevano automaticamente consentendo a l'utilizzatore di poter concludere l'operazione di rifornimento dell'automobile. Il pagamento veniva fatto corrispondere ad una carta di credito che il consumatore possedeva ed aveva inserito all'interno di un conto online apposito del servizio Speedpass e quindi nessuna tipologia di informazione legata alla carta era conservata o gestita fisicamente all'interno del dispositivo portatile, in modo tale da garantire una maggior sicurezza ed affidabilità. Come tutti i sistemi di pagamento non garantivano un grado elevato di protezione, anche questa tipologia, che sembrava essere abbastanza affidabile, non fu immune da attacchi che riuscirono a violare la sicurezza. Nel 2005 appunto, RSA Laboratories e un gruppo di studenti della Jhons Hopkins University, riuscirono a rompere l'algoritmo di cifratura utilizzato per i portachiavi e furono così in grado di riprodurre esattamente una Speedpass, che utilizzarono, in un distributore per poter far rifornimento di benzina.[54][55]

2.9 Mobile commerce

La rivoluzione informatica, avvenuta dalla metà del XX secolo, aveva introdotto grandi cambiamenti nella società moderna, aveva visto la nascita di nuove tecnologie e l'inizio di nuove forme di pagamento. L'evoluzione però di questi concetti non era per niente giunta al termine, anzi la loro esponenziale e rapida crescita, aveva appena portato anche alla formazione di un ulteriore sistema di pagamento, che prevedeva l'impiego di una nuova tecnologia inventata nell'anno 1973, il telefono cellulare. Circa quarantun anni fa, Martin Cooper, un ingegnere della Motorola, inventò il primo telefono che non richiedeva l'ausilio di una rete fissa per poter effettuare una chiamata, ed ebbe così il privilegio di poter effettuare la prima telefonata senza fili della storia. A dire la verità la prima chiamata fu sbagliata, perché l'ingegnere per l'emozione, sbagliò il numero di telefono, mentre la seconda andò a buon fine. Successivamente il 6 marzo del 1983, fu messo in vendita il primo modello di cellulare, il DynaTac 8000X, che era composto da una lunga antenna di gomma, ventuno enormi tasti e si poteva telefonare solamente per trenta minuti, perché una volta trascorsi, bisognava rimetterlo in carica per dieci ore. Questa nuova tecnologia ebbe uno sviluppo ed un utilizzo impressionante, molto più rapido di tutti gli altri strumenti inventati precedentemente.[56] Nel 1993 ad esempio venne infatti inviato il primo SMS (Short Message Service), cioè messaggio di tipo testuale lungo al massimo 160 caratteri, da un cellulare verso un altro, mandato da uno stagista dell'azienda Nokia. Successivamente nel 1999, sempre la Nokia, lanciò il primo telefono con all'interno un browser che consentiva la navigazione in Internet grazie all'implementazione di un protocollo WAP (Wireless Application Protocol). Lo sviluppo di questo protocollo, aiutò ad aumentare le funzionalità dei telefoni cellulari, avendo così permesso a tale strumento di poter dare il via a nuove forme di transazioni economiche, attraverso appunto la rete Internet. Questi nuovi progetti diedero l'idea di poter accrescere il commercio elettronico attraverso l'utilizzo di un semplice telefono cellulare. Già nel 1997, in Finlandia, ci furono i primi casi di Mobile Commerce, dove furono montati dei distributori automatici di CocaCola, che richiedevano il pagamento tramite l'invio di SMS. Dallo stesso anno in poi il concetto di Mobile Commerce fu concepito come un vero e pro-

prio mercato in cui era possibile effettuare transazioni riguardanti prodotti e servizi digitali, ed effettuare pagamenti tramite dispositivi mobili. Dal 1999, si iniziò ad avere i primi tentativi di commercio mobile in particolar modo in Europa, in Norvegia, dove si iniziarono a pagare i parcheggi tramite l'invio di SMS, ed nell'Estremo Oriente, in Giappone, dove una compagnia telefonica, la DoCoMo, attraverso siti i-mode, dava la possibilità di poter acquistare dei biglietti aerei comodamente dal telefono cellulare. Grazie a queste esperienze il telefono cellulare iniziò ad essere concepito come uno strumento utile e semplice per effettuare pagamenti, dando vita, di fatto, ad un concetto di pagamento totalmente nuovo, che tutt'ora si evolve in maniera molto elevata, il Mobile Payments.[57] Il telefono cellulare si sta affermando in tutto il mondo come strumento di pagamento, grazie anche alla trasformazione continua e sbalorditiva che ha subito nel corso della storia e sta subendo tuttora. Oggi il progresso dei sistemi di pagamento non si è di certo arrestato, anzi è in continua crescita ed in costante cambiamento, è un incessante sviluppo di idee tecnologiche in grado di dare l'opportunità a tutti gli utilizzatori, di poter usufruire non soltanto di una semplice modalità di pagamento ma bensì di una moltitudine di servizi che consentano di soddisfare le numerose esigenze di transazione, di ogni singolo individuo.

Capitolo 3

Tecnologia e sicurezza sistemi di pagamento

Come abbiamo visto nel capitolo precedente, l'evoluzione storica ha giocato un ruolo importante per lo sviluppo della moneta, infatti nel corso del tempo, a seconda dei bisogni creati dalla società ed in concomitanza alla nascita di nuove tecnologie, si è sempre assistito ad un cambiamento in grado di poter migliore la facilità di utilizzo e la sicurezza dei sistemi di pagamento. Sono dunque queste, le caratteristiche che ogni giorno dovrebbero spingere una persone ad utilizzare i nuovi metodi di pagamento, ma nonostante ciò alcuni soggetti continuano tuttora a mostrare un certo grado di insicurezza e diffidenza nei confronti di questi sistemi, dovuti ad una parziale disinformazione. Questo capitolo, cercherà di descrivere e spiegare le tecnologie e i sistemi di sicurezza che stanno dietro ai mezzi di pagamento, permettendo magari di capire se, effettivamente è possibile o meno effettuare attacchi che violino la riservatezza dei dati dell'utente.

3.1 Tecnologia mobile

Come già spiegato in precedenza i mobile payments, sono quei particolari sistemi che utilizzano dei dispositivi mobili per effettuare transazioni sfruttando a seconda delle modalità di pagamento, che sia in prossimità o in remoto, una rete di comunicazione. Partendo dalle modalità di Remote

Payments, le reti mobili utilizzate sono diverse e forniscono un supporto per il traffico dei dati in maniera differente e a seconda della velocità, vengono suddivise in base alla generazione di appartenenza. Ma prima di partire ad elencare ciò, è bene capire come funziona una rete cellulare. Ogni area geografica del pianeta, è suddivisa in celle, ognuna delle quali possiede una zona di copertura, dovuta alla presenza di una stazione base. Ogni stazione fissa che si trova all'interno di una determinata cella, scambia il proprio segnale, in base alla potenza di trasmissione, con una stazione di tipo mobile (nel nostro caso un dispositivo cellulare). Le stazioni base, rappresentate da grandi antenne fisse in grado di coprire una zona fino ad un certo limite dato dalla potenza del segnale, sono collegate ad una rete telefonica pubblica commutata (PSTN, Public Switched Telephone Network) o ad un altro centro mobile di commutazione, che gestisce le telefonate. Per avere un idea di che cos'è un centro mobile di commutazione, si può pensare ad una sorta di centralino che si occupa di coordinare tutte le chiamate dall'inizio alla fine e con la capacità di seguire gli spostamenti delle persone. All'interno di una cella di una stazione base, possono esserci svariate chiamate in ogni istante, conseguentemente lo spettro radio, garantito da ogni fornitore di servizi telefonici, deve essere suddiviso dai sistemi cellulari secondo due approcci:

- Multiplexing a divisione di tempo (TDM, Time Division Multiplexing), è una tecnica, che consente di dividere il tempo in frame suddivisi a sua volta in più slot temporali, ognuno dei quali dedicato a una chiamata.

- Multiplexing a divisione di frequenza (FDM, Frequency Division Multiplexing), è una tecnica di trasmissione, dove a ciascuna chiamata viene dedicata una banda di frequenza, per poter evitare l'interferenza, all'interno appunto di un unico mezzo fisico.

Considerato il funzionamento delle reti telefoniche mobili, si può passare quindi ad elencare le generazioni a cui appartengono:

- **GSM** (Global system for mobile communication) : questa tecnologia appartiene alla categoria del 2G, ovvero, della seconda generazione. In Europa fu adottata nei primi anni '90 e fino ad oggi è stato uno

degli standard più diffusi al mondo. Il sistema GSM utilizza un mix dei due approcci visti precedentemente FDM/TDM, che consiste nel dividere il canale in sottobande di frequenza disgiunte dentro le quali il tempo viene diviso in frame e slot. Questa tipologia di rete non era sufficientemente adatta al trasferimento di dati, ma era stata concepita per effettuare chiamate vocali, utilizzando algoritmi di compressione di dati vocali ed in grado di codificare le chiamate a 13 e a 12.2 Kbps, garantendo solamente una buona qualità audio.

- **GPRS** (General packet radio service) : è uno standard successivo al GSM che permette, a differenza di quest'ultimo, di effettuare il trasferimento di dati attraverso la rete cellulare oltre a essere ottimizzato per le chiamate telefoniche. Questo servizio di comunicazione è appartenente al 2,5G, cioè alla generazione che va dalla seconda alla terza. Per quanto riguarda il trasferimento dei dati, nel GPRS, viene fornito un servizio un po' più efficiente, che consente di effettuare trasferimenti di dati ad un tasso compreso generalmente tra i 40 Kbps e 60 Kbps, rispetto al GSM che invece supporta solamente tassi trasmissivi a 9,6 Kbps. Il valore che di trasmissione di questo standard può essere paragonato a un modem di tipo dial-up di una linea telefonica fissa, utilizzato solitamente per la connessione di un computer alla rete Internet.

- **EDGE** (Enhanced data rate for global evolution) : la tecnologia EDGE è stata creata con l'obbiettivo di poter aumentare ulteriormente la capacità di trasferimento delle reti precedenti, sfruttando in maniera migliore il canale di trasmissione utilizzato dal GSM. Questo standard, appartiene sempre alla generazione 2,5G, che va dalla seconda alla terza e permette in teoria un miglioramento rispetto alle reti GSM/GPRS di velocità di trasferimento di dati, a circa 348 Kbps.

- **UMTS** (Universal mobile telecomunication service) : Con questo standard, si entra di fatto nella terza generazione (3G), in cui i nuovi dispositivi mobili sono concepiti per poter offrire servizi di telefonici in grado di poter trasmettere i dati a velocità molto più elevate rispetto ai precedenti sistemi 2G e 2,5G. Questo standard deriva da quello GSM,

però al contrario, non fa più uso dello schema FDMA/TDMA, ma utilizza una tecnica completamente diversa, ovvero il WCDMA (wideband CDMA) e grazie a questo sistema, si è in grado di poter effettuare un trasferimento di dati a una velocità promessa di, 3 Mbps. Il sistema UMTS, perciò consente di avere un potenziamento delle prestazioni di invio voce e dati, rispetto al GSM/GPRS, ed è per questo fattore che questo standard ha assistito ad un enorme crescita e sviluppo prima in Europa e poi in tutto il mondo.[58]

- **HSPA** (High Speed Packet Access) : è un evoluzione della rete UMTS, che appartiene alla generazione intermedia fra la terza e la quarta, in cui i protocolli sviluppati consentono di ottimizzare ancora di più le prestazioni degli standard precedenti, in quanto a velocità di dati trasmessi. Già con questa nuova tecnologia si può iniziare quindi, a parlare di banda larga[59], dove lo scopo è di fornire una maggiore velocità di trasmissione, connessione a Internet e una maggior copertura di segnale, garantendo perciò una buona mobilità. Si divide in due tipologie:

  - **HSDPA**(High Speed Downlink Packet Access), in cui si la trasmissione di dati avviene in downlink (scaricamento), verso l'utente, ad una velocità promessa di circa 14,4 Mbps.
  - **HSUPA**(High Speed Uplink Packet Access), dove la trasmissione di dati avviene in uplink (caricamento), verso la rete, con una velocità promessa di 5,76 Mbps.

- **LTE** (Long Term Evolution) : questo nuovo standard va a collocarsi in una posizione che precede quella della quarta generazione (4G), di fatto questo protocollo di trasmissione è considerato come un Pre - 4G ma è stato effettivamente classificato dalla ITU come un 4G.[60] LTE è un evoluzione degli standard precedenti e si basa su un insieme di protocolli in grado di fornire una connessione a banda larga alla rete Internet e non solo, permette inoltre non soltanto di effettuare chiamate come gli standard precedenti, ma consente di poter chiamare sfruttando appunto il collegamento ad una rete che utilizza il protocollo

IP(Internet Protocol), questa tecnologia è chiamata VoIP (Voice over IP). La rete LTE, per il trasferimento dei dati, dovrebbe garantire una velocità di 100 Mbps per quanto riguarda il download, mentre 50 Mbps, per l'upload.[61]

3.2 Remote payment

Una volta descritte e capite le reti presenti in ogni dispositivo mobile, si può passare a cercare di conoscere le tecnologie che consentono appunto di effettuare i pagamenti, sfruttando le connessioni appena elencate. Fra i diversi strumenti utilizzati per il Remote Payment, troviamo gli SMS, applicazioni per dispositivi mobili e pagamenti on-line tramite Mobile Browser.

3.2.1 Pagamento SMS

Sms è l'abbreviazione di Short Message Service e rappresenta una tecnologia che consente di ricevere ed inviare brevi messaggi, sfruttando l'utilizzo delle reti telefoniche. È un mezzo molto comodo e sfruttato, in grado di inviare molte informazioni utili che non richiedono grandi elaborazioni, ma un semplice invio di testo, ad esempio per invitare a cena qualcuno, per ricevere informazioni di lavoro, per notizie dell'ultima ora, o ancora per le notifiche e-mail e tanto altro; tutto ciò, avviene tramite un normale telefono cellulare o computer connesso a Internet. Ogni SMS, è in grado di contenere un massimo di 160 caratteri di testo, per le lingue che utilizzano l'alfabeto latino, ed invece 70 caratteri per lingue tipo il cinese, russo o giapponese, in maniera da ottenere una dimensione fissa del messaggio di 140 byte (1120 bit). I messaggi, vengono inviati ad un Centro servizi, il Short Message Service Center (SMSC), a cui spetta il compito di dover gestire l'instradamento e la consegna degli SMS, utilizzando un approccio di tipo *store-and-forward* (cioè immagazzina e rimanda), in cui il messaggio inviato viene ricevuto interamente e memorizzato temporaneamente fino a quando, il dispositivo ricevente non diventa disponibile per la rete, rendendo perciò possibile l'inoltro. Il messaggio inviato inizialmente, può attraversare uno o più centri servizi SMSC, realizzando una sorta di ponte, da stazione a stazione, in gra-

do di raggiungere appunto il destinatario finale. Nel caso in cui appunto il dispositivo destinatario non sia raggiungibile per vari motivi, il centro servizi, conserverà il messaggio per un certo periodo di tempo, dopo di che provvederà alla sua eliminazione. Le tecniche di protezione e riservatezza dei messaggi però, si limitano solamente alla sicurezza della rete di comunicazione su cui sono trasmessi, ed inoltre il SMSC può in qualsiasi momento interrompere la disponibilità del servizio, non garantendo perciò l'integrità del messaggio spedito. In pratica gli SMS non utilizzano misure di sicurezza, generalmente utilizzate da altri protocolli, che prevedono l'impiego di una crittografia durante la trasmissione, in modo da rendere le informazioni leggibili solamente al possessore della chiave di decodifica del messaggio cifrato. Per questa tecnologia è previsto invece un cyclic redundancy check, ossia un controllo di ridondanza ciclico che permette di rilevare modifiche involontarie su dati grezzi, consentendo ai messaggi brevi in transito sul canale di trasmissione di poter arrivare a destinazione senza essere danneggiati. Come accennato in precedenza, ogni messaggio spedito, è conservato all'interno del SMSC per un intervallo di tempo limitato se non è subito possibile l'inoltro del testo, al destinatario. L'inconveniente di questo sistema è dato dal fatto che, nel caso purtroppo il dispositivo ricevente non ritorni raggiungibile in un quel lasso di tempo, non sarà più possibile consegnare SMS perché sarà eliminato dal centro servizi; solitamente questo può accadere quando il destinatario del messaggio si trova in una zona non coperta dal segnale del SMS. Un altro svantaggio importante derivante dall'utilizzo di questa tecnologia è dato dal fatto che il messaggio una volta inviato, potrebbe attraversare diversi centri servizi collegati fra loro, che purtroppo provvederanno all'inoltro del testo non appena le condizioni opportune saranno soddisfatte, con lo svantaggio quindi di non riuscire a garantire una tempestività di consegna. Si può dire in conclusione che gli SMS offrono un servizio in modalità *"Best-effort"*, cioè non forniscono di fatto nessuna garanzia sulla consegna effettiva dei dati e sulla velocità di consegna, che può variare anche in base al traffico di rete. Visto che gli SMS non possiedono nessuna forma di crittografia per poter proteggere il contenuto, possono essere intercettati e spiati durante la trasmissione, anche perché i messaggi vengono memorizzati all'interno dei SMSC sotto forma di normale testo, prima di essere conse-

gnati al destinatario, permettendo quindi a gli utenti del centro servizi, che hanno accesso al sistema, di poterli leggere e modificare. Esistono appunto, anche dei programmi spia che consentono di poter registrare tutti gli SMS inviati e ricevuti, memorizzandoli su un file copiato su un server remoto, in maniera da garantire successivamente la visualizzazione.[62] Un esempio di questo è dato da Flexispy[8], un software in grado di poter spiare alcune applicazioni di messaggistica. Bisogna quindi stare molto attenti ad utilizzare gli SMS, soprattutto quando vi è il bisogno di effettuare pagamenti di vario genere. A questo proposito si sta cercando di introdurre un nuovo protocollo chiamato SSMS[63] (secure short message service) in grado di garantire la giusta protezione soprattutto per i pagamenti di tipo mobile, questa soluzione, fornisce un modo sicuro, grazie alla generazione di una crittografia a chiave asimmetrica (ovvero chiave doppia, pubblica e privata) ed emette un certificato per la chiave pubblica di ogni utente.[64] Un esempio attuale di questa modalità di pagamento è offerta dal servizio Cash-Mobile, brevettato da l'azienda milanese 4Tech+, che si occupa di telecomunicazioni e sicurezza. Questo sistema si basa su un'architettura client-server, dove il client è una applicazione che risiede fisicamente sul dispositivo utilizzato, che si occupa di gestire l'interfaccia e la criptazione dei dati, mentre il server si occupa della comunicazione con la struttura di pagamento (Banca, Pos, società carta di credito, PayPal). Il soggetto che vuole utilizzare questo servizio, deve registrarsi su Cash-Mobile, inviando, tramite tramite Internet, informazioni personali ed indicando oltre al numero del cellulare, le strutture di pagamento di cui vuole servirsi. Successivamente questa persona riceverà un SMS contenente un link che gli consentirà di scaricare l'applicazione ed installarla, ed una volta effettuato il primo accesso sarà possibile terminare la registrazione, impostando un codice PIN (Personal Identification Number) scelto appositamente dall'utente. Per gli acquisti, basterà che il negoziante invii i dati necessari per la transazione a Cash-Mobile, tramite un cellulare o qualsiasi altro dispositivo mobile. Cash-Mobile provvederà ad inviare a sua volta il messaggio di richiesta al cliente, sul numero di cellulare scelto precedentemente, con le informazioni dell'acquisto, ed a questo punto l'utente potrà dare conferma, inserendo il proprio codice PIN. Questo nuovo servizio

[8] www.flexispy.com

a differenza di altri, è basato su crittografia a doppia chiave (asimmetrica), che consente di avere un grado di protezione elevato, ed inoltre le comunicazioni riguardanti le transazioni avvengono attraverso SMS cifrati.[65] I vantaggi che contraddistinguono questo sistema di pagamento sono dati da fattori che consentono l'avvio della transazione da parte del venditore e mai da parte del compratore, dalla comunicazione tra client e server che avviene esclusivamente tramite SMS push cifrati, dalla possibilità di decisione del PIN da parte del cliente, senza quindi la possibilità che qualcuno diverso dal proprietario ne entri in possesso. È dato inoltre dal fattore dalla trasparenza del servizio per venditore e cliente, visto che è quest'ultimo il soggetto a cui spetta la decisione di inserire il PIN o meno per poter procedere all'acquisto, ed infine dal fattore di adattamento all'ambiente circostante, visto che il pagamento richiede solamente l'utilizzo di un dispositivo mobile, è più semplice utilizzarlo per vendite che richiedono una disponibilità di spazio limitato.[66]

3.2.2 Sicurezza SMS

Come abbiamo visto quindi i pagamenti via SMS, se non implementati secondo determinati criteri di sicurezza, possono essere pericolosi. Cercare di conoscere il funzionamento degli SMS, può metterci in condizione di poter capire e prevenire alcune tipologie di minacce, derivate dalla vulnerabilità di questa tecnologia:

- **SPOOFING**: è una tecnica di falsificazione di pacchetti, che permette di far apparire una trasmissione di dati ritenuta sicura, perché proveniente da una fonte attendibile, una comunicazione falsificata, perché proveniente invece da un soggetto che punta a violare la sicurezza del destinatario. Lo spoofing consente di stabilire una connessione fra due utenti, su una stessa rete, in cui l'unico modo sicuro per bloccare un messaggio falsificato è dato dal verificare la corretta l'autenticità del soggetto mittente e controllare che le informazioni contenute nel SMS provengano effettivamente da un percorso veritiero ed affidabile.

- **DOS** (Denial of Service) : è un attacco che prova ad impedire agli utenti proprietari dei dispositivi mobili di poter accedere ai servizi di

rete. Questa tecnica è realizzabile perché la debolezza del protocollo SMS, consentirebbe ad un utente malintenzionato di attaccare il telefono utilizzando l'invio di messaggi ripetuti, inondando così tanto la rete da non poter più rendere accessibile il dispositivo mobile. Visto che appunto i messaggi e le chiamate vocali vengono trasmessi all'interno del medesimo canale, l'inondazione di questo, ad esempio con SMS, non darebbe la possibilità di poter utilizzare il servizio opposto, ovvero le chiamate. È stato possibile assistere ad un attacco di questo genere, nell'isola di Manhattan, dove l'invio di 165 messaggi di testo al secondo fu sufficiente per rendere inutilizzabili tutti i telefoni.[67]

- **SMISHING**(SMS Phishing): è dato dall'unione del termine SMS e phishing, da qui il termine Smishing, ed è un attacco in cui il soggetto malintenzionato invia un SMS contenente un link fasullo che rimanda, o all'apertura di una pagina web, simile a quella di un sito conosciuto, ma prontamente contraffatto , oppure al download di una applicazione malware (applicazione software malevola) sul proprio dispositivo mobile. Grazie a questa falsificazione riescono a spingere l'utente ignaro, garantendogli ovviamente un qualsiasi vantaggio, ad inserire informazioni personali in grado di poter essere utilizzate dagli attaccanti, per poter commettere successivamente truffe informatiche, come per esempio attivare un servizio di abbonamento non richiesto dalla vittima ed iniziando così purtroppo, a sottrargli ingenti somme di denaro dal credito telefonico o da altri strumenti di pagamento collegati.[68]

In conclusione possiamo affermare che, anche se gli attacchi possibili possono essere molteplici, bisogna tuttavia prestare un attenzione maggiore verso i messaggi ricevuti, valutando accuratamente il mittente del SMS ed il contenuto, in maniera tale da riconoscere se effettivamente questi provengano senza alcun dubbio da una fonte certa ed affidabile.

3.2.3 Applicazioni Mobile

L'applicazione mobile, non è altro che un software pensato e studiato appositamente per dispositivi mobili di ultima generazione, questa struttura,

a differenza delle applicazioni informatiche tradizionali, consente di ottenere maggiori vantaggi riguardanti velocità e leggerezza del programma, dovuti appunto alla semplificazione ed eliminazione di parti superflue presenti invece nei semplici software informatici. Per intenderci un'applicazione mobile è una sorta di programma di piccole dimensioni e semplice da utilizzare. Possiamo avere due categorie di applicazioni, quelle native e quelle web:

- Le applicazioni native, sono effettivamente installate su dispositivi mobili e non sono altro che un insieme di istruzioni informatiche scritte seguendo determinati linguaggi di programmazione che rendono possibile utilizzare specifici servizi.

- Le applicazioni web, a differenza delle precedenti, non sono installate fisicamente all'interno del dispositivo mobile ma, utilizzano un collegamento verso una pagina web appositamente semplificata per poter utilizzare i servizi.

La differenza tra queste due tipologie è data dal fatto che le applicazioni native non richiedono necessariamente una connessione costante ad Internet, mentre le applicazioni web non influiscono in alcun modo sulla capacità di memoria di un dispositivo.[69] Ogni applicazione, fornisce una compatibilità ed è vincolata al sistema operativo su cui è possibile eseguirla e per facilitarne la ricerca ad utenti meno informati, si ricorre all'utilizzo di un market, che è una sorta di distributore digitale, anche esso vincolato ad un sistema operativo specifico, che si occupa appunto di gestire la loro diffusione. I principali sistemi operativi conosciuti oggi sono: [70]

- Android (google)
- iOS (Apple)
- Windows Phone (Microsoft)
- BlackBerry OS (RIM/BlackBerry)
- Symbian OS (Nokia)
- Bada OS (Samsung)

Per ogni sistema operativo, è possibile utilizzare determinate istruzioni informatiche, che utilizzano diversi linguaggi di programmazione, in grado di poter sviluppare e creare le varie applicazioni mobili. Data la dinamicità del mondo delle applicazioni, è difficile quindi poter trovare un linguaggio di programmazione unico in grado di poter garantire compatibilità con qualsiasi piattaforma. Principalmente i linguaggi più utilizzati sono:

- **JAVA**: nato il 23 maggio del 1995, era stato creato principalmente per due motivi: per garantire una maggior semplicità di scrittura e gestione del codice rispetto a C++ e per permettere la creazione di programmi che non fossero legati ad una architettura precisa. Java è un linguaggio di programmazione orientato ad oggetti ed eredita questa sua caratteristica da C++. Le applicazioni mobili create con questo linguaggio vengono principalmente eseguite su sistemi operativi Android, ma possono essere anche supportate da altri come per esempio Symbian.[71]

- **C++**: è un linguaggio adatto alla programmazione orientata ad oggetti, per poter sviluppare software che utilizzano i più moderni pattern di progettazione. Nato nel 1983, ideato da Bjarne Stroustrup, è oggi considerato uno dei primi 5 linguaggi più utilizzati al mondo. Il suo utilizzo viene applicato in differenti campi, tra i quali troviamo anche quello delle applicazioni mobili, per sistemi operativi come Symbian e Windows Phone. C++ era nato con l'idea di poter mantenere una piena compatibilità con C, conservando molte librerie e strumenti di sviluppo.[72]

- **Objective-C**: è un linguaggio necessario per poter sviluppare applicazioni compatibili con sistemi operativi iOS, è un linguaggio orientato agli oggetti e rappresenta anche questo un estensione di C, con il quale conserva la compatibilitè, consentendo di fatto di poter utilizzare tutti i metodi e le funzioni native di quest'ultimo. Nato da un idea di Brad Cox e Tim Love a metà degli anni '80, questo linguaggio era stato concepito per aggiungere a C le caratteristiche di Small Talk (il primo linguaggio a oggetti).[73][74]

Per quanto riguarda i sistemi di pagamento, sappiamo che esistono alcune tipologie di applicazioni mobili comunemente utilizzate per effettuare trasferimenti di moneta elettronica. Queste, descritte nei capitoli precedenti riguardavano appunto la categoria dei Wallet, o portafogli elettronici, di cui sono state scoperte ed esposte alcune problematiche legate alla sicurezza.

3.2.4 Mobile browser

I browser sono programmi creati per garantire un punto di accesso alla rete Internet, sono presenti all'interno dei dispositivi mobili sotto forma di microbrowser o mobile browser, cioè software ottimizzati, in grado di consentire l'interazione con i contenuti delle pagine web in maniera efficiente ed una visualizzazione corretta a seconda delle dimensioni degli schermi. Al giorno d'oggi, questi strumenti, a differenza dei loro predecessori, sono in grado di poter comunicare attraverso protocolli più classici, che garantiscono maggior interoperabilità, come TCP/IP, in maniera da poter utilizzare il supporto dato da i protocolli HTTP e garantire così la possibilità di poter sviluppare i contenuti delle pagine web utilizzando semplicemente il linguaggio HTML.[75] Come abbiamo visto in precedenza il primo protocollo che consentiva la connessione e la navigazione di dispositivi mobili su pagine Internet, era il WAP (Wireless Access Point), introdotto, nel 97, ma poi successivamente accantonato e sostituito da una forma più evoluta, il WAP 2.0. Dunque il fallimento di questo protocollo era stato dettato da la mancanza di un numero elevato di siti Web che utilizzassero il linguaggio di markup prescelto, ossia il WML (Wireless Markup Language). Questo linguaggio, oggi decisamente obsoleto, era basato su una versione analoga all'HTML (HyperText Markup Language), molto semplice e leggero, che si adeguava facilmente ai problemi di banda di trasmissione ed alluso di memorie limitate dei dispositivi di allora.[76] L'entrata in campo del nuovo protocollo WAP 2.0 ha introdotto alcune differenze tecniche, innanzitutto, il linguaggio precedentemente utilizzato, il WML, è stato sostituito da una sua evoluzione, XHTML Basic (Extensible HTML), uno standard che combina XML (Extensible Markup Language) e HTML, in grado però di garantire minor flessibilità rispetto al semplice HTML, ed impiegato per poter creare pagi-

ne web per dispositivi più contenuti, con meno variazioni di codice. Inoltre una caratteristica importante per il 2.0, è data dall'introduzione di protocolli Internet nell'ambiente WAP, per poter supportare i dispositivi wireless direttamente con l'architettura IP (tabella 3.1):[77]

- **Wireless Profiled HTTP** (WP - HTTP) : Questa specifica, riguarda gli ambienti wireless e garantisce un elevata interoperabilità con il protocollo HTTP /1.1. L'interazione tra, il dispositivo WAP e il WAP Proxy/ WAP Server avviene tramite il modello base di richiesta e risposta HTTP. WP- HTTP, può stabilire tunnel sicuri e supporta la compressione di message body (corpo del messaggio, dove solitamente sono contenuti i dati associati al messaggio) delle risposte.

- **Transport Layer Security** (TLS) : Questo protocollo può essere utilizzato per effettuare transazioni sicure, anche nel campo di dispositivi wireless (senza fili). TLS contiene dei protocolli crittografici in grado di fornire integrità dei dati, visto che sono inclusi algoritmi di firma elettronica; autenticazione, perché sono contenuti i formati dei certificati e cifratura/decifratura su una rete TCP/IP. Questo protocollo permette perciò una sicurezza di comunicazione da una sorgente ad un destinatario (end-to-end) operando al livello di trasporto.

- **Wireless Profiled TCP** (WP-TCP) : è un protocollo che fornisce servizi connection-oriented, cioè orientati alla connessione, ovvero consistono in una modalità di trasmissione dati, attraverso la quale protocolli di comunicazione stabiliscono una connessione fra i dispositivi presenti all'interno di una rete, provvedono alla trasmissione e ricezione di pacchetti dati secondo un ordine stabilito, solitamente quello di invio, rilevando errori dovuti a informazioni perse o mancanti; ed infine terminano il collegamento. WP-TCP è ottimizzato per le reti wireless ed è completamente compatibile con il protocollo standard TCP presente in Internet.[78]

Grazie quindi alla funzionalità dei browser è possibile, tramite i nuovi canali di accesso al web (Smartphones, Tablet, PDA o palmari, RIM BlackBerry, i più conosciuti [79]), poter assistere a un nuovo fenomeno di shopping

Protocollo WAP	
WAP 1.0	**WAP 2.0**
WSP	HTTP
WTP	TLS
WTLS	TCP
WDP	IP
Strato di supporto o bearer	Strato di supporto o bearer

Tabella 3.1: Differenza stack protocolli

online, chiamato mobile commerce. Questo commercio elettronico mobile, da la possibilità agli utenti di collegarsi, tramite browser, ai maggiori siti on-line e procedere così all'acquisto di beni e servizi in tutta semplicità e utilizzando strumenti di pagamento preferiti, precedentemente descritti. Lo sviluppo dei microbrowser e la relativa introduzione dei protocolli Internet, hanno portato questo strumento ad essere considerato un modo pratico e veloce con cui poter fare acquisti in pochi secondi. Inoltre i mobile browser garantiscono lo stesso livello di sicurezza derivante da operazioni condotte via computer, dando però la possibilità di avere anche una maggiore mobilità.[80] Tuttavia però questi software mobile, come i browser stessi, sono soggetti a problemi di sicurezza riguardanti i malware (software maligno creato per danneggiare un sistema informatico), che oggi giorno, prendono di mira sopratutto gli utenti che utilizzano dispositivi mobili per connettersi ed effettuare transazioni online. Il browser dei dispositivi mobili, data la grandezza non eccessiva dello schermo, non consentono di poter visualizzare chiaramente gli indicatori di un normale sito sicuro. Nonostante i protocolli di sicurezza presenti, bisogna fare attenzione a cercare l'icona del lucchetto presente sulla barra degli indirizzi, il quale indica appunto che la connessione è sicura ed affidabile. Ed infine quando si naviga su un web browser, bisogna sempre prestare attenzione di essere indirizzati su link di siti attendibili e non contraffatti, per evitare eventuali problemi di sicurezza legati alla visualizzazione di siti web falsificati, ma simili agli originali.[81]

3.3 Proximity payment

Per le tecnologie che aiutano a effettuare pagamenti sfruttando connessioni a breve distanza, ovvero in prossimità, troviamo alcuni strumenti come NFC (Near Field Communication) e QR-Code.

3.3.1 Pagamento NFC

Il pagamento tramite NFC è un servizio di pagamento che avviene semplicemente avvicinando il dispositivo mobile, dotato della tecnologia NFC, ad un POS conctactless. Come descritto in precedenza al dispositivo deve essere associato uno strumento di pagamento elettronico (esempio carta di debito o credito o prepagata) legato ovviamente a circuiti di pagamento comunemente utilizzati come Visa o Mastercard. Le informazioni riguardanti le credenziali di pagamento si trovano all'interno di un posto "sicuro", chiamato Secure Element, che corrisponde ad un hardware fisico, separato dal resto dei componenti del dispositivo, a cui possono accedere solamente alcune tipologie di applicazioni certificate e dotate di determinati privilegi.

3.3.1.1 Che cos'è NFC ?

Near Field Communication, è una tecnologia a radiofrequenza che fornisce una connettivit'a wireless bidirezionale, tra due dispositivi, a breve distanza, fino ad un massimo di 10 cm, consentendo lo scambio di informazioni o la possibilità di pagamenti sicuri. Questa tecnologia è nata dall'evoluzione del RFID (Radio Frequency Identification), ma a differenza di questa, NFC garantisce la possibilità di comunicazione bidirezionale, consentendo a Initiator e Target (cioè chi esegue la connessione e chi la riceve), quando vengono avvicinati entro un raggio di 4 centimetri, di riuscire realmente a mettersi in contatto, in maniera tale da creare una rete peer-to-peer fra i due dispositivi. La frequenza a cui questa tecnologia lavora è di 13.56 MHz ed è in grado di raggiungere una velocitè massima di 424 kbit/s. È possibile inserire la tecnologia NFC semplicemente integrando un chip all'interno di un dispositivo mobile, oppure utilizzando una scheda esterna che dia la possibilità di sfruttare le porte delle schede SD o mini SD.[82]

3.3.1.2 Architettura NFC

L'architettura di uno smartphone o altro dispositivo mobile abilitato alla tecnologia NFC, deve possedere i seguenti elementi (figura 3.1) :

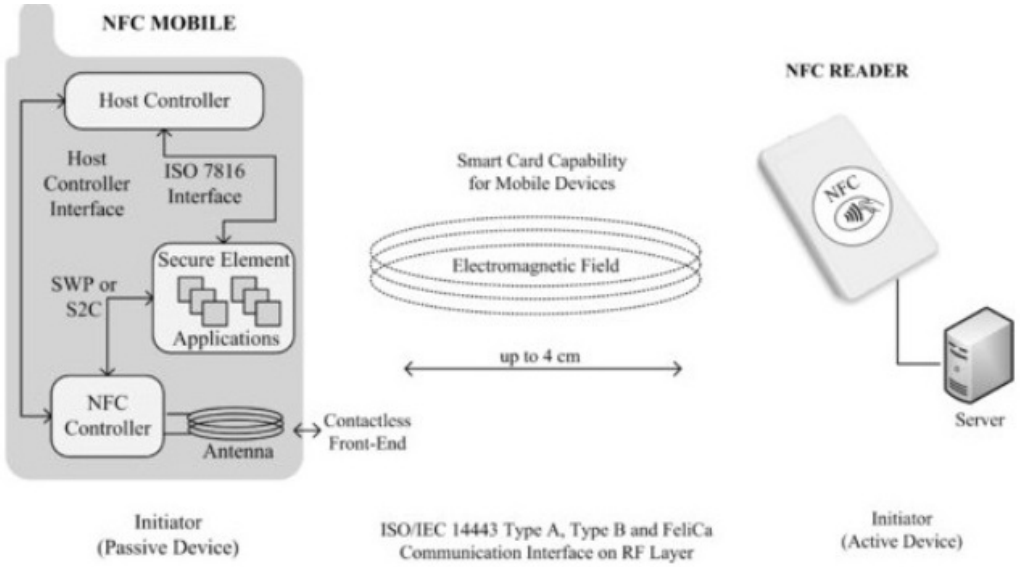

Figura 3.1: Architettura NFC

- Un'antenna RFID, che sia in grado di ricevere comunicazioni con l'esterno.
- NFC Controller per le transazioni NFC, è in grado di ricevere i dati provenienti dall'antenna.
- Un Secure Element, permette la memorizzazione sicura, all'interno di un chip, delle informazioni private, come ad esempio dati della carta di credito di un utente e consente la relativa esecuzione dei servizi di pagamento conctactless.

L'antenna RFID e NFC Controller compongono NFC Contactless Front-End[9] (CLF), il quale è responsabile dell'acquisizione dei dati di ingresso e l'elaborazione di tali con modalità conformi a specifiche predefinite, in maniera

[9] it.wikipedia.org/wiki/Front-end_e_back-end

da renderli utilizzabili in uscita. Il Secure Element è connesso e comunica con NFC Controller, utilizzando dei protocolli per lo scambio di dati, chiamati SWP (Single Wire Protocol) e NFC-WI(NFC Wired Interface). Host Controller è il centro di qualsiasi dispositivo mobile, questo può controllare o accedere al Secure Element. Dall'Host Controller all NFC Controller, viene creato un ponte, denominato HCI (Host Controller Interface), attraverso il quale Host Controller setta le modalità operative dell NFC Controller, elabora i dati inviati e ricevuti e stabilisce la connessione fra NFC Controller e il Secure Element. I dispositivi mobili a cui viene solitamente associato uno strumento di pagamento elettronico, sono generalmente gli smartphone (o cellulari). I dispositivi tecnologi che utilizzano NFC, entrano in modalità di Card Emulator, in maniera da poter così consentire la simulazione di una Smart Card conctactless basata su specifiche ISO/IEC 14443, utilizzando anche, a livello fisico, gli stessi protocolli previsti da quest'ultima. La Smart Card, può contenere come già detto in precedenza delle applicazioni per il pagamento, delle applicazioni di ticketing per trasporto pubblico e molto altro. Inoltre queste applicazioni utilizzano un proprio protocollo (ad esempio EMV per carte di credito) e speciali funzioni di sicurezza. La simulazione della carta non viene effettuata dal processore NFC interno al dispositivo ma dal Secure Element. Questo elemento può essere inserito all'interno dell NFC Controller oppure in una speciale SIM card, denominata UICC (Universal Integrated Circuit Card), in grado di supportare il protocollo SWP, che permette appunto la comunicazione fra il Controller e la SIM. In conclusione nel Secure Element, considerato luogo protetto, è obbligatorio avere l'autorizzazione del produttore del sistema operativo o del dispositivo per poter installare applicazioni; ad esempio nelle SIM card (UICC), è l'operatore telefonico che può decidere chi può avere l'accesso oppure no.[83]

3.3.2 Sicurezza NFC

Nonostante la comunicazione NFC a corto raggio possa fornire una forma di sicurezza intrinseca da alcuni tipi di attacchi, tuttavia non tutela completamente questa tecnologia, visto che è comunque possibile poter attuare alcune tecniche efficaci di intrusione. È possibile per esempio intercettare la

comunicazione tra uno smartphone e un POS, avendo a disposizione di un attaccante, un antenna in grado di intercettare la comunicazione non criptata fra i due dispositivi. Vi è inoltre la possibilità di modificare i dati scambiati tra POS e smartphone tramite un RFID jammer, ovvero un dispositivo in grado di disturbare le comunicazioni in radiofrequenza, permettendo di non ricevere ne trasmettere segnali da telefoni cellulari, inceppando quindi la trasmissione. Un altro attacco attuabile è denominato Relay Attack[10], in cui bisogna posizionare un lettore NFC nelle vicinanze di un POS, oppure di uno smartphone di un cliente ignaro, così da poter leggere i dati, ed inviare il flusso delle informazioni su un altro dispositivo che si trova nelle vicinanze e in possesso del malintenzionato, consentendo così in questo modo di riuscire a simulare il funzionamento della carta di pagamento e procedendo all'utilizzo di questa. Questo tipo di tecnica a differenza di un attacco Man-in-the-Middle, consente semplicemente di inoltrare i messaggi intercettati tra le parti, senza necessariamente manipolarli o leggerli. Un'altra tecnica per poter violare la sicurezza di questa tecnologia consiste nell'effettuare uno "spoofing", riuscendo a falsificare una reale comunicazione, compromettendo un tag NFC e forzando questo a dover eseguire un malware. Questo approccio è di facile attuazione visto che per alcuni dispositivi mobili i comandi ricevuti dal tag NFC sono eseguiti automaticamente. Ed infine è possibile attaccare l'intero stack di protocolli NFC, analizzando il software e sfruttando i bug dello sviluppo, oppure quelli legati al sistema operativo che viene utilizzato per il supporto.[84] Relativamente agli attacchi citati in precedenza, l'Osservatorio NFC & Payment della School of Management del Politecnico di Milano, fornisce un approfondimento su alcune risposte per poter chiarire meglio alcuni dubbi legati agli aspetti della sicurezza del pagamento NFC. Questo approfondimento risponde ad una serie di domande tra le quali: 1) Un malintenzionato, in possesso di un antenna, un amplificatore di segnale e un ricevitore, è in grado di intercettare i dati di pagamento NFC in un raggio di 10 metri? 2) I pagamenti NFC sono davvero al sicuro da attacchi di tipo Man in the Middle? 3) Se un malintenzionato attivasse il proprio ricevitore NFC in luoghi affollati, dove si è molto vicini, potrebbe impossessarsi di informazioni di telefoni NFC? 4) È possibile che il telefono venga clonato? 5)

[10] en.wikipedia.org/wiki/Relay_attack

Se vi sono intercettazioni sulla rete telefonica è possibile che un malintenzionato possa rubare i dati dello strumento di pagamento? E se durante una transazione con Mobile Payment si riceve un SMS o una chiamata è possibile che si verifichino errori o problemi? ed infine, 6) È possibile che il Pos di un esercente venga compromesso, generando pagamenti verso terzi senza il consenso dell'acquirente o venditore?

Procedendo in ordine si riesce a rispondere nel modo seguente:

1. conoscendo la frequenza e la potenza operativa dell NFC, la distanza massima per effettuare l'eavesdropping (cioè intercettazione segnali radio e decodifica dati trasmessi) è di 10 metri, solamente se entrambi i dispositivi NFC funzionano in modalità attiva, ovvero trasmettono dati, mentre se uno dei dispositivi è in modalità passiva la distanza massima si riduce ad 1 metro. Pero nei pagamenti NFC, solamente il POS lavora in maniera attiva, mentre il device mobile lavora in modalità passiva, ovvero in modalità card-emulation. Un malintenzionato in questo caso dovrebbe quindi posizionare il suo sistema di intercettazione a meno di 1 metro dal POS, rendendo lo scenario reale inverosimile, dato l'ingombro e la visibilità delle antenne adibite appunto "all'ascolto" delle credenziali scambiate.

2. L'attacco Man in the Middle, è una tecnica in cui un hacker si inserisce in una conversazione tra un client e un server, ed inganna quest'ultimo trasferendogli comunque le informazioni spedite dal client, ma ottenendo nel frattempo le informazioni volute. Grazie alle scelte protocollari e tecniche questi attacchi sono impraticabili nel caso di pagamenti NFC, a meno che non si soddisfino contemporaneamente questi requisiti:

    - Il dispositivo del malintenzionato dovrebbe essere posto fra lo smartphone della vittima e il POS, assicurandosi anche che il POS e il cellulare non riescano a comunicare direttamente, altrimenti si accorgerebbero della ripetizione della conversazione da parte del terzo elemento. Visto quindi che la comunicazione utilizza una distanza di funzionamento di pochi cm, il non notare un dispositivo diverso sarebbe improbabile.

- Il dispositivo del malintenzionato dovrebbe rispondere al POS in maniera tempestiva, non permettendo alla transazione di andare in timeout, e al tempo stesso schermare la comunicazione diretta telefono-POS. Anche questo, poco realizzabile, visto che i dati vengono trasmessi tramite un link Wi-fi, per cui i tempi del dispositivo del malintenzionato sarebbero incompatibili con i tempi di risposta imposti dal protocollo, i quali garantiscono appunto che la comunicazione sia avvenuta per mezzo di canali NFC.

3. La possibilità di riuscire ad ottenere i dati di una carta di pagamento è improbabile, visto che l'applicazione di pagamento che ha i privilegi per accedere al Secure Element, deve essere attivata dall'utente, mantenendo la possibilità di accesso per un dato intervallo di tempo, solitamente 60 secondi, trascorsi i quali è possibile riattivarla solamente con un click. Inoltre solo spese molto piccole, inferiori a 25 euro, possono avvenire senza l'inserimento di un PIN, ed infine tale limite di spesa può essere ulteriormente ridotto, in base alla preferenza dell'utente.

4. Esiste sempre la possibilità che i dati contenuti nel Secure Element vengano estratti e copiati, come nelle carte tradizionali, in cui il chip può essere clonato. Risulta però tutto molto difficoltoso, visto che bisogna violare i sistemi di sicurezza del protocollo come ad esempio il PIN e aggirare i servizi di sicurezza accessori che consentono di avvisare il cliente, come ad esempio servizi di SMS alerting. È quindi evidente che chiunque utilizzi il telefonino come forma di pagamento, essendo un oggetto più intelligente, può innalzare il livello di sicurezza, a differenza invece di una semplice carta di credito, concedendo in conclusione a tale strumento, una maggior fiducia rispetto ad un oggetto plastificato.

5. Quando viene effettuato un pagamento, lo scambio delle informazioni non avviene tramite una rete telefonica, ma attraverso la comunicazione fra POS e smarphone, quindi non è possibile generare una interferenza fra i due canali di trasmissione. Il Single Wire Protocol, permette appunto la comunicazione fra la SIM e il cellulare, consentendo alla

SIM di poter essere utilizzata contemporaneamente sia per effettuare pagamenti e sia per effettuare chiamate.

6. È in teoria possibile, ma difficile, visto che il POS per funzionare devono essere allacciati a un circuito, che li censisce, li identifica, e li autorizza ad operare. Anche in questo caso il rischio è pari a quello che un soggetto incontra quando utilizza uno strumento di pagamento elettronico tradizionale.[85]

3.3.3 QR Code

I QR-Code (abbreviazione di Quick Response Code), sono barcode bidimensionali (o 2D) che rappresentano un evoluzione dei tradizionali codici a barre. È formato da moduli di colore nero disposti all'interno di uno schema di forma quadrata, nel quale vengono memorizzate informazioni destinate ad essere lette da un cellulare di ultima generazione. In un unico simbolo QR-Code possono essere contenuti fino a 7089 caratteri numerici o 4296 caratteri alfanumerici, e 2953 byte di dati binari, rappresentati in ogni punto del simbolo QR.[86] Questa tecnologia nata nel 1994 e sviluppata dalla società giapponese, Denso Wave,[87] a differenza dei semplici codice a barre, è in grado di contenere non solo semplici sequenze di numeri, ma anche formati di dati come ad esempio, biglietti da visita virtuali, posizioni su una mappa, indirizzi pagine web, indirizzi e-mail, numeri di telefono, testi e tanto altro ancora. Come precedentemente accennato, questi simboli QR possono essere letti da dispositivi mobili di ultima generazione che, utilizzando particolari programmi, sono in grado di poter acquisire le informazioni contenute, utilizzando una fotocamera. I QR Code, sono tipicamente indicati quindi per poter fornire servizi aggiuntivi a chi utilizza un dispositivo mobile ed in particolare possono essere una soluzione per effettuare alcune tipologie di pagamento. Prima però sarebbe meglio analizzare e capire alcuni aspetti tecnici di funzionamento di questa tecnologia.[88]

Figura 3.2: QR Code

3.3.3.1 Dettagli tecnici

Si possono notare (figura 3.2) tre grandi quadrati evidenziati in rosso, sono chiamati i segnaposto, questi indicano allo scanner (programma adibito alla lettura) della fotocamera i margini del QR code. Il quadrato piccolo, evidenziato sempre in rosso è di allineamento ed è un punto di riferimento per lo scanner, per essere sicuro di essere allineato. In QR più grandi sono presenti più di uno. Le strisce rosse che evidenziano i quadratini neri e bianchi, definiscono le posizioni di righe e colonne. Le sezioni verdi definiscono il formato e sono in grado di indicare allo scanner se il codice in questione indica un sito web, un SMS, numeri o combinazioni di questi elementi. Le parti evidenziati in blu rappresentano il numero della versione. Più moduli ci sono e più il numero della versione è alto (la massima versione è v40 in grado di contenere 177x177 moduli). Nel caso in cui il codice sia più piccolo di v6, la versione non deve essere definita, perché lo scanner è in grado di contare da solo i moduli.

I moduli che rimangono (Figura 3.3) vengono raggruppati in sezioni di 8 moduli e ciascuno di questi gruppi, chiamati “bytes”, si intrecciano fra di loro come pezzi di un puzzle nelle aree grigie di differenti tonalità. Quando un dispositivo mobile, attraverso uno scanner legge il QR Code, ogni byte viene acquisito come leggibile o illeggibile. Quindi cambiando un singolo modulo (cambiando il colore di un quadratino da bianco a nero) si può causare l’illeggibilità di tutto il byte. Per ovviare a questo, tutti i QR Code

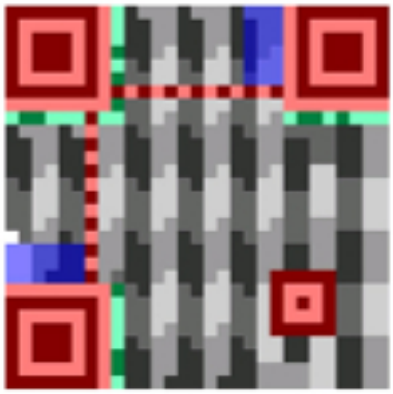

Figura 3.3: QR Code

possiedono un algoritmo in grado di poter correggere gli errori, potendo così rendere leggibile il contenuto, anche se alcuni byte sono stati corrotti (perché mancanti, modificati, macchiati o graffiati). Questo algoritmo è denominato Reed Solomon e consente di ricostruire parti di dati andati persi, ed inoltre la capacità di correzione degli errori può essere stabilita, al momento della creazione di un nuovo codice, su più livelli, L (basso), M (medio), Q(quartile) oppure H(alto).

- Con L possiamo ripristinare circa il 7% dei dati
- Con M possiamo ripristinare circa il 15% dei dati
- Con Q possiamo ripristinare circa il 25% dei dati
- Con H possiamo ripristinare circa il 30% dei dati

La correzione degli errori risulta importante quando si vuole personalizzare il proprio QR, inserendogli all'interno un immagine o un altro elemento, che possa coprire delle parti di codice, senza perdere funzionalità. I codici QR possono essere generati in diverse dimensioni (dalla versione 1 formata da massimo 21x21 moduli, alla 40 formata da massimo 177x177 moduli[89]) e più grande sarà la versione del codice e più byte si riusciranno a coprire, senza perdere alcun contenuto.[90]

3.3.4 Sicurezza e pagamenti QR Code

Per capire meglio dunque l'applicazione dei QR code nel campo dei pagamenti mobili, è possibile citare alcuni esempi che utilizzano questo metodo di pagamento. Nel nostro paese sono in atto alcuni progetti fra i quali: Bemoov, una piattaforma che consente di pagare via smartphone, utilizzando QR Code, per vari servizi come: prodotti in negozi eCommerce, biglietti autobus, del treno, di spettacoli, parcheggi e altro ancora. Un'altra forma di applicazione di questa tecnologia è data da l'applicazione Day Tronic Mobile, mediante la quale è possibile, controllare i propri buoni pasto e vedere quali ristoranti li accettano. Su questa applicazione è presente un buono pasto Day, che può essere letto dall'esercente mediante QR Code. Infine con Pay On Delivery, un servizio lanciato nel 2012 da PayPal e Mondo Convenienza, in cui, grazie alla scansione di un QR Code presente sulla bolla di consegna, è possibile far aprire una pagina di Mondo Convenienza dove viene indicato l'importo da saldare, per poi pagare successivamente tramite PayPal o carta di credito.[91] Nonostante dunque questo strumento sia molto utile per agevolare i pagamenti, bisogna però prestare sempre attenzione ai fattori di sicurezza che caratterizzano l'utilizzo di questa tecnologia. Infatti grazie a questi codici è possibile accedere rapidamente a contenuti digitali dannosi o ricchi di malware. Bisogna prestare molta attenzione a questi strumenti, visto che un utente malintenzionato potrebbe contraffare il codice QR autentico, reperibile presso un luogo pubblico, semplicemente attaccando un adesivo contenente codice maligno, in grado di collegare il dispositivo mobile verso un sito corrotto. Il problema dei codici QR è dato appunto, dalla possibilità di poter nascondere i siti e i contenuti su cui si viene indirizzati. Un ulteriore svantaggio è dato anche dalla facilità con cui è possibile distribuire i codici QR a potenziali vittime ignare. Queste complicazioni possono portare ad attacchi di tipo Drive-by-download, che consentono di installare sul dispositivo utilizzato per la lettura del codice QR maligno, un software malware o applicazioni come key logger, senza che l'utente ne sia realmente a conoscenza. Quindi si potrebbe fornire agli hacker, la possibilità di controllare i dispositivi, ed entrare così nei portafogli mobili (collegati a strumenti di pagamento), consentendogli dunque di poter commettere azioni a danno

del soggetto colpito. È comunque possibile proteggersi da questi attacchi, utilizzando appositi software per la protezione, o applicazioni in grado di verificare l'autenticità del link della pagina web prima che possa essere attivato. In conclusione è quindi consigliato di agire come tutti gli strumenti di pagamento elettronico utilizzati, con molta calma e attenzione.[92] [93]

3.4 Strumenti elettronic payment

L'evoluzione della società e in particolare dell'e-commerce, ha portato all'adozione di sistemi di pagamento che fossero in grado di fornire un elevata sicurezza ed una maggiore facilità di utilizzo, accrescendo in questo modo la fiducia degli utenti nell'impiego di Internet per svolgere i loro affari. Attualmente molti utenti non si avvalgono degli strumenti di pagamento, perché temono in qualche modo di poter essere truffati o aggirati. Per cercare di rimuovere la diffidenza mostrata dagli utenti nei confronti dei sistemi di pagamento, si cercherà di comprendere le tecnologie e i sistemi di sicurezza adottati, per rendere così più chiare le modalità di pagamento.

3.4.1 Caratteristiche tecniche carte di pagamento

Negli Elettronic Payments gli strumenti più utilizzati per effettuare pagamenti, sono le carte di credito e prepagate, ma il loro utilizzo è molto rallentato tutt'oggi perché si teme la possibilità di essere vittime di frodi sempre più sofisticate. In questa parte prenderemo in esame le carte di credito perché comunque possiedono caratteristiche simili a quelle prepagate. Iniziamo con il capire come una carta di credito è riconoscibile rispetto ad un'altra, che potrebbe essere contraffatta. Solitamente la numerazione delle carte di credito, definita anche con il nome di PAN (Primary Account Number) è composta da 16 cifre ed ognuna di queste possiede un particolare significato. La prima cifra iniziale, rappresenta il circuito di appartenenza della carta:

- 3 indica che le carte appartengono al circuito American Express o Diners Club

- 4 viene utilizzato per Visa
- 5 utilizzato per Mastercard
- 6 per le Discover Card

Dalla seconda alla sesta cifra, viene indicato il "bin range", cioè l'identificativo dell'ente emittente, dalla settima alla penultima, avremo il numero del conto che identifica la carta in modo univoco ed infine l'ultimo numero rappresenta una cifra di controllo. Le dimensioni standard delle carte sono definite da lo standard ISO/IEC 7810 ID01e sono di 85,60 x 53,98 mm e uno spessore di 0,76 mm.[94] Tuttavia la sola banda magnetica presente ancora oggi su alcune carte, era considerato uno strumento che non garantiva una piena protezione, visto che era facilmente clonabile con tecniche di skimming. A questo proposito lo sviluppo delle carte di credito ha portato alla nascita di nuove schede, integrate con un microprocessore in grado di fornire una memorizzazione dei dati più sicura. Molte carte di credito, oggi, possiedono sia la banda magnetica e sia il microprocessore. Le smart card, sono appunto le nuove carte di credito munite di microchip, in cui vengono memorizzati in maniera crittografata, le informazioni del titolare.[53] Queste carte permettono di memorizzare una quantità più elevata di dati rispetto alla banda magnetica, il che gli consente di non dover accedere a un database remoto ad ogni transazione, proprio perché possiedono già tutte le funzionalità e informazioni. Nella categoria delle carte a microprocessore è possibile distinguere:

- **Carte a contatto**: in questa tipologia di carte, il circuito stampato, può connettersi e comunicare con il lettore grazie allo scambio di contatti elettrici.
- **Carte a prossimità o conctactless**: Queste carte si differenziano da quelle a contatto, perché lo scambio di informazioni avviene mediante trasmissione in radio frequenza e non tramite il canale fisico realizzato dai contatti della carta e del lettore. Visto che è una carta senza contatto, all'interno, è presente una piccola antenna in grado di ricevere il segnale emesso dall'antenna presente sul dispositivo fisso con cui co-

munica. Infine questa carta consente di ottenere una velocità elevata di lettura e scrittura, ad una data distanza.

3.4.1.1 Architettura smart card

L'architettura interna della smart card è composta da diversi elementi e fra questi possiamo individuare: [95]

- L'unità centrale (CPU): rappresenta il cuore della Smart Card; essa è in grado di eseguire istruzioni, di effettuare calcoli aritmetici, di controllare il flusso di dati che entrano ed escono dalla carta e di gestirne l'archiviazione sulla memoria.

- La Memoria volatile (RAM): rappresenta lo "spazio di lavoro" utilizzato dall'unità centrale per svolgere i propri compiti. Quando l'unità centrale esegue una applicazione utilizza la RAM come appoggio per archiviare temporaneamente i dati e le informazioni necessarie. Tutte le volte che viene tolta l'alimentazione alla Smart Card si perde inevitabilmente il contenuto di questa unità.

- Memoria a sola lettura (ROM): in questa unità risiedono programmi e dati fondamentali per il corretto funzionamento della Smart Card. Queste informazioni sono registrate sulla ROM al momento della costruzione del processore e in alcun modo modificabili o cancellabili una volta rilasciata la Smart Card.

- La Memoria programmabile (EEPROM Electrically Erasable Programmable Read Only Memory): rappresenta la memoria di massa della Smart Card; su questa unità è possibile memorizzare dati ed applicazioni strettamente legati alla Smart Card stessa e dipendenti dal tipo di utilizzo cui è riservata o dall'utente cui appartiene. La EEPROM presente su una Smart Card ha svariate dimensioni tipicamente è di 32Kbyte. I file sulla EEPROM sono organizzati in maniera simile ad un normale disco fisso, ovvero il sistema operativo la suddivide in settori di dimensione fissata.

- Porta di I/O. La carta comunica con l'esterno tramite un'uscita seriale ad un solo bit, con velocità che variano secondo il tipo e le necessità delle specifiche applicazioni. Valori usuali sono 9600 bit/secondo, ma per le carte contactless sono richieste velocità superiori.

- Oltre alle unità appena descritte è possibile trovare un co-processore crittografico specializzato per l'esecuzione di algoritmi crittografici standard quali MD5, SHA-1, RSA, DES, 3-DES, DSA. Il co-processore è molto importante in quanto solleva l'unità centrale dal compito di eseguire gli algoritmi crittografici e garantisce buone prestazioni poiché ottimizzato per effettuare esclusivamente questo tipo di operazioni.

3.4.2 Sicurezza carte di credito

Per quanto riguarda la sicurezza delle carte di credito, entrano in gioco le specifiche EMV, che definiscono i requisiti minimi che le smart card e i terminali, devono possedere per poter interagire fra di loro. Questi requisiti, sono sia di carattere fisico ed elettrico, ed anche di carattere applicativo. Riguardo agli aspetti fisici, vengono definite un insieme di regole chiamate Level 1. Queste regole definiscono i requisiti di base per tutti i terminali e smart card, che vanno da le caratteristiche fisiche ed elettromeccaniche, fino all'interfaccia logica ed i protocolli di trasmissione. Vengono stabiliti quindi una sorta di elementi essenziali che garantiscono la comunicazione e l'invio di informazioni. Per quanto riguarda invece gli aspetti applicativi, vengono specificate un insieme di regole, che indicano le modalità con cui le transazioni di pagamento devono essere eseguite una volta stabilita la connessione fra smart card e terminale. Queste regole, chiamate Level 2, definiscono le specifiche per l'esecuzione delle funzioni associate alle transazioni, che includono la selezione dell'applicazione, la gestione dei dati individuali, i comandi e la sicurezza. Lo standard EMV in definitiva, provvede a definire un linguaggio comune per poter garantire una interoperabilità e l'algoritmo di crittografia prescelto è il DES, cioè un algoritmo in grado di criptare e decriptare dati in blocchi di 64 bit.[45] Un'altra forma di sicurezza presente sulla carta di credito, è data dal codice di verifica CVV, che però può essere utilizzato solamente durante transazioni via web. Le smart card danno inoltre la pos-

sibilità di poter eseguire un autenticazione sia off-line che on-line, attraverso due differenti tecniche. Nella prima, le carte di pagamento, contengono un certificato crittografato da una chiave segreta. Questa forma di autenticazione, chiamata SDA (Static Data Authentication), può essere utilizzata per ogni connessione ad un terminale, tramite una chiave pubblica, non richiedendo un elaborazione crittografica da parte della carta. La carta viene così identificata dal terminale attraverso l'uso della stessa firma digitale per ogni transazione. Mentre la seconda, chiamata DDA (Dynamic Data Authentication), in cui il terminale interroga la carta, la quale risponde sulla base dei della chiave segreta e dei dati contenuti in essa. Questa tecnica crea quindi una firma digitale diversa per ogni transazione. Nel caso la transazione sia on-line, si può effettuare un completo controllo di autenticazione, utilizzando in questo caso una chiave simmetrica.[53] Solitamente sulla carta di pagamento, al fine di incrementare la sicurezza, ed evitare falsificazioni, vengono spesso applicati ologrammi o microstampe, o ancora più semplicemente viene utilizzato uno spazio apposito dove poter inserire la firma dell'utente proprietario.

3.4.2.1 Tipologie frodi carte di pagamento

Le carte di pagamento, nonostante le forme sicurezza citate, possono comunque essere soggette a frodi, che danno la possibilità al truffatore, di entrare in possesso dei dettagli relativi a questo strumento. il soggetto malintenzionato , può quindi in qualche maniera, venire a conoscenza di dati come, nome del titolare, numero di carta, data di scadenza e codice CVV, attraverso svariate tecniche, tra cui:

- Boxing: in cui il truffatore è in grado di acquisire i dati con la sottrazione dell'estratto conto inviato al proprietario stesso della carta.
- Hacking: in questa tecnica i dati delle carte sono reperibili, tramite violazione di database di siti web, che si occupano di vendere beni e servizi e che conservano al loro interno tutti i numeri di svariate carte.
- Sniffing: questo termine viene utilizzato per descrivere l'analisi dei protocolli, cioè l'analisi del contenuto dei pacchetti e la loro visualizzazione,

all'interno di una rete. Gli strumenti adatti a questa tecnica, sono chiamati analizzatori di protocollo o sniffer, i quali sono dunque in grado di catturare password o informazioni su carte e altro ancora. Per cui intercettando le coordinate di pagamento di una transazione effettuata in rete, è possibile riutilizzare questi dati per poter fare ulteriori acquisti in altri siti, senza che la vittima ne sia a conoscenza.

- Phishing: Con questa tecnica, si cerca di spingere le persone, a rivelare le proprie password o altre tipologie di informazioni riservate. I dati possono dunque essere acquisiti attraverso particolari e-mail e siti web contraffatti e creati appositamente, che inducano le persone a fidarsi e le spingano ad inserire informazioni private.

- Trashing: Attraverso questa pratica è possibile poter risalire ai dati delle carte o altre informazioni private, attraverso il setaccio dei rifiuti della vittima, possono ad esempio ricercare scontrini di carte che i titolari solitamente buttano via dopo un acquisto. [53]

3.4.3 Contromisure minacce commercio elettronico

La maggior parte dei pagamenti elettronici oggi, avviene attraverso la rete Internet e di conseguenza un ruolo importante viene assunto dal Commercio Elettronico, le cui le transazioni per la commercializzazione di beni e servizi avvengono attraverso l'impiego di strumenti adatti alla connessione Web (ad esempio Browser). L'enorme sviluppo del Commercio Elettronico, ha portato tuttavia, anche problematiche legate alla sicurezza, visto che attraverso la rete, vengono trattati dati personali e finanziari di vario genere. Anche la mancanza di un contatto diretto con il venditore, oltre alle questioni legate alla sicurezza, non sono fattori incoraggianti per gli utenti che devono servirsi delle applicazioni di acquisto in rete. Solitamente i clienti, sono appunto restii a divulgare informazioni riguardanti ad esempio il numero della carta di credito oppure a rilasciare le opinioni o preferenze. A questo proposito un sito Web, deve mettere in atto misure di sicurezza in grado di garantire la tutela delle informazioni personali dei clienti. Dunque per lo sviluppo di una

applicazione e-commerce, è importante considerare alcuni aspetti legati alla sicurezza, fra cui:

- **Metodo elettronico per l'identificazione del cliente** : è necessario sviluppare strumenti più sofisticati in grado di autenticare in modo univoco l'utente che accede al sito e-commerce, la sola password a tale scopo non è sufficiente.

- **Metodo elettronico per identificazione venditore** : tale sistema, dovrebbe assicurare all'utente, che il venditore da cui sta effettuando l'acquisto sia realmente qualificato e originale. Visto che sarebbe possibile attaccare un sito e-commerce, trasferendo tutte le comunicazioni rivolte ad esso, verso un altro sito contraffatto. Si può tuttavia risolvere questo problema ad esempio tramite azioni di marketing, che puntano a far riconoscere al pubblico e-commerce. Utilizzando per esempio un logo facilmente riconoscibile ed in grado di guadagnarsi la fiducia degli utenti

- **Comunicazione sicura** : In ogni transazione importante, di tipo finanziaria, è necessario riuscire a mantenere i dati segreti e protetti durante la trasmissione, per non rendere possibile un eventuale lettura che possa compromettere le informazioni del cliente

- **Approccio sicuro per i pagamenti** : Le informazioni della carta, non possono essere accessibili a nessuno, a parte il proprietario stesso e l'istituto di credito che si occupa della transazione. Il cliente e il venditore quindi, comunicano solamente con l'istituto finanziario, trasmettendo, il primo, il proprio numero di carta per dar via all'operazione di pagamento mentre il secondo richiede garanzie sulla disponibilità del cliente a saldare l'importo dovuto.

- **Non ripudio e integrità dei dati** : Data l'assenza di un contatto fra venditore e cliente, è necessario attuare meccanismi che evitino situazioni in cui un cliente non riconosca un ordine realmente effettuato o che un venditore non dichiari di non aver mai ricevuto un ordine, che in realtà gli è stato consegnato. Deve essere ugualmente possibile anche,

che la comunicazione fra cliente e venditore non possa in alcun modo essere modificata da un soggetto estraneo.

- **Sicurezza dei sistemi preesistenti** : I computer utilizzati per gestire le società e-commerce, sono spesso collegati ad altre macchine dedicate a differenti scopi, è dunque importante proteggere i dispositivi che fanno da ponte fra la rete locale e Internet. Altrimenti un intruso in queste macchine, potrebbe forzare l'intera infrastruttura della società. Per evitare ciò sarebbe giusto proteggere i dati sensibili con sistemi di archiviazione crittografata.

Ora possiamo quindi passare a capire come avviene una tipica sessione di commercio elettronico via Internet e successivamente come è possibile effettuare transazioni commerciali sicure tramite Web. Gli attori presenti sono quattro:

- **Cliente & Browser** : qui, abbiamo un utente che utilizza un normale Browser, per interfacciarsi alla rete e collegarsi a un sito E-commerce, mediante il quale può osservare i prodotti o servizi di interesse e volendo, acquistarli.

- **Shopping mall** : è il vero e proprio negozio on-line, dove è possibile visualizzare i prodotti e procedere agli acquisti. Molti negozi utilizzano un Merchant Server per le gestioni commerciali vere e proprie.

- **Merchant Server** : si occupa di gestire le transazioni, appoggiandosi a una società di servizi interbancari, attraverso la quale è in grado di poter gestire i diversi tipi di pagamento.

- **Banking System** : tutte le richieste di transazione commerciali provenienti dal merchant server, vengono gestite da una banca, presso la quale è detenuto un conto appartenente a quest'ultimo. Per poter gestire la transazione, è necessario che la banca del merchant, si colleghi alla banca sulla quale si appoggia il cliente, per verificare se il pagamento è effettivamente possibile.

Ogni attore quindi, procede a effettuare i seguenti passi (figura 3.4) :

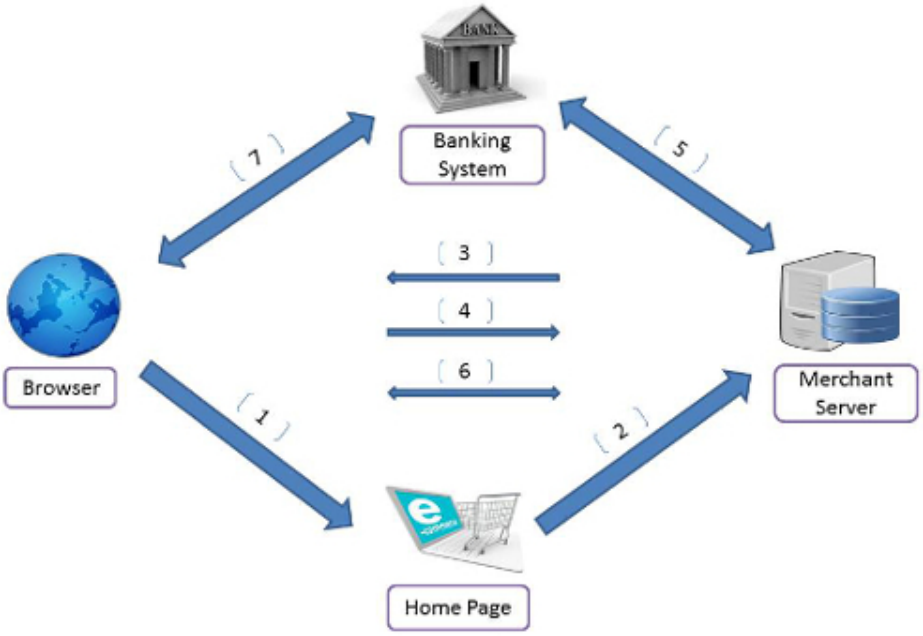

Figura 3.4: Transazioni e-commerce

1. Il cliente, accede dal browser ad una pagina web che fornisce servizi di e-commerce

2. Una volta selezionato il servizio richiesto, il cliente viene collegato al merchant server del sito e-commerce, adatto a trattare le transazioni secondo protocolli di sicurezza.

3. Viene presentata la pagina dei prodotti all'utente

4. Deciso di acquistare un prodotto, il cliente dopo aver scelto la relativa forma di pagamento, conferma l'ordine.

5. Il merchant server contatta la società di servizi interbancari e ottiene l'autorizzazione ad accreditare sul conto del venditore l'importo dovuto dal cliente, per l'ordine effettuato.

6. Il pagamento viene confermato al cliente.

7. La società di servizi interbancari si occupa di contattare la banca del cliente, per richiedere l'addebito della spesa.

Questa transazione, non avviene in modo diretto tra cliente e fornitore, ma attraverso una società di servizi interbancari, la quale successivamente stabilisce un rapporto con la banca di chi ha effettuato l'operazione di pagamento.[45] Per effettuare il pagamento esistono differenti modalità di cui il consumatore può usufruire:[96]

- carta di credito
- carta di debito (carta prepagata)
- bonifico bancario
- Wallet

3.4.4 Protocolli sicurezza web

Come abbiamo visto precedentemente, le transazioni che avvengono attraverso i Browser, nel momento in cui ci si collega a un merchant server facendo richiesta di specifici servizi, prevedono l'impiego di particolari protocolli che garantiscano una protezione per la comunicazione di dati riguardanti il pagamento elettronico. I protocolli più utilizzati sono: SSL/TLS, SET e HTTPS.

3.4.4.1 SSL/TLS

Il protocollo TLS (Transport Layer Security), un evoluzione dello standard SSL (Secure Socket Layer), è un protocollo di crittografia, utilizzato per poter proteggere lo scambio di informazioni e le comunicazioni fra due nodi di una rete Web. Questo protocollo utilizza certificati di crittografia asimmetrici, che per funzionare necessitano della presenza di una o più autorità di certificazione (CA, Certification Authority) e di un infrastruttura a chiave pubblica, che consentano di verificare se la relazione fra il certificato e il suo possessore sia effettivamente valida e non sia fasulla. Oltre che da questi certificati la protezione è garantita dallo scambio di chiavi di sessione simmetriche. Per crittografare i dati della connessione di rete questo

standard, si appoggia al livello di applicazione nel modello ISO/OSI (Open System Interconnection, OSI, è uno standard che stabilisce la struttura logica della rete promosso da International Organization for Standardization, ISO). SSL/TLS, permette alle applicazioni di tipo client di poter comunicare e instaurare con un server, una connessione sicura, per mezzo di una rete, in modo tale da non consentire eavesdropping ("origliare") e tampering ("manomettere, immischiarsi nelle comunicazioni"). Per lo scambio di messaggi fra client e server (handshaking), è necessario che il primo indichi al secondo, di stabilire una connessione protetta per il trasferimento informativo attraverso l'impiego di una porta differente da quella utilizzata comunemente (ad esempio per lo scambio con HTTPS, HTTP supportato da SSL/TLS, la porta utilizzata è 443 mentre per HTTP semplice, è la 80). Durante l'operazione di negoziazione fra client e server per stabilire una connessione affidabile, questi due concordano i diversi parametri necessari per poter effettivamente autorizzare un collegamento affidabile. Nella prima fase, vengono scambiati diversi dati, fra cui la versione del protocollo utilizzata, le impostazioni di cifratura, dati specifici della sessione e altre informazioni. Il client nel caso di navigazione web controlla ad esempio se l'intestatario del certificato crittografico ricevuto, corrisponde effettivamente al server contattato e se la Certification Authority sia affidabile. Il client, crea il pre-master session(in cui viene generata una master session key) e lo crittografa con la chiave pubblica ricevuta dal server e lo invia al server stesso. Nel caso in cui il server lo richieda, il client invia una firma autenticata, ovviamente crittografata, per garantire la propria identità. Il server decodifica poi il pre-master session (ovvero la master session key) e genera il master secret, se ovviamente è avvenuta identificazione del client, altrimenti viene interrotta la sessione. Sia il server che il client utilizzano il master secret per generare la chiave (simmetrica) di sessione, utilizzata nel corso della comunicazione per poter crittografare e decriptare i dati inviati da una parte all'altra e per verificane l'integrità. Alla fine il server terminerà la propria sessione indicando che la procedura di handshaking è terminata e invierà al client una session identifier (un numero univoco generato casualmente) utilizzabile in un'altra sessione ed una ulteriore si potrà instaurare utilizzando la chiave di sessione definita. [97] [45]

3.4.4.2 SET

Secure Electronic Transaction, è un protocollo che rende sicure le transazioni con carte di credito attraverso la rete Internet, ed è stato inizialmente sviluppato da Mastercard e Visa. SET fa uso di tecniche crittografiche come i certificati digitali e la crittografia a chiave pubblica per consentire alle parti di identificarsi reciprocamente e scambiare informazioni con sicurezza.[98] Questo protocollo opera a livello applicativo, consentendo dunque di operare sui dati che effettivamente vengono scambiati tra le parti della transazione economica. In ogni transazione, ogni utente, deve possedere un certificato elettronico che provi la sua identità agli altri soggetti coinvolti, perché questo protocollo da la possibilità di poter condividere rapporti commerciali cifrati e autenticati solo, con soggetti in possesso di certificati validi. Ogni utente dunque, è in grado di decifrare solamente i messaggi che gli appartengono. Per ogni transazione sono presenti 5 soggetti:

- Il possessore della carta di credito(cliente)
- Venditore
- Un autorità di certificazione (CA, Authority Certification), a cui spetta appunto il compito di certificare le parti coinvolte.
- Un Payment Gateway, è quello che si occupa di svolgere le funzioni di intermediario per le operazioni finanziarie.
- Rete di pagamento, delle istituzioni creditizie.

In ogni certificato, firmato elettronicamente dall'Authority Certification, vengono inserite le chiavi pubbliche di ciascun utente. Quando un soggetto riceve il certificato (che consente di verificare l'identità)di un altro, con cui sta intrattenendo una transazione, è in grado di entrare in possesso della sua chiave pubblica da poter utilizzare per comunicare con lui in maniera sicura. Si può considerare il certificato del compratore come una rappresentazione elettronica della sua carta di credito. Questo è firmato dall'autorità in maniera tale da non poter essere alterato, ma non contiene alcuna informazione relativa al numero di carta o altri dati di questa. Il certificato viene rilasciato al compratore solo con un consenso dell'istituto finanziario, perché viene indicata la

volontà di poter acquistare beni e servizi tramite transazioni economiche. Il venditore, che quindi riceve questo certificato, può essere certo che il cliente disponga di una carta di credito valida. Questo standard impone inoltre che per ogni carta di credito accettata dal venditore, si disponga di una coppia di certificati, uno per firmare elettronicamente i messaggi, mentre il secondo per creare le buste digitali per lo scambio sicuro delle chiavi simmetriche.[99] Al momento di una transazione sicura con SET, i dati sono inviati dal client al server del venditore, ma quest'ultimo recupera solo l'ordine. In effetti, il numero di carta di credito è inviato direttamente alla banca del commerciante, che sarà capace di leggere le coordinate bancarie dell'acquirente, e quindi di contattare la sua banca per verificarli in tempo reale. Si può dire quindi che SET è basato sull'uso di una firma elettronica a livello dell'acquirente, ed una transazione in grado di mettere in gioco non soltanto l'acquirente e il venditore, ma anche le loro rispettive banche.[100] In conclusione si può affermare che i requisiti che il protocollo SET punta a soddisfare sono:[45]

- Confidenzialità in tutte le transazioni
- Autenticazione compratore, titolare di un regolare conto bancario
- Autenticazione venditore, in maniera che possa ricevere i pagamenti tramite il sistema bancario su cui si appoggia
- Interoperabilità tra prodotti software di natura diversa e differenti infrastrutture di rete.

3.4.4.3 HTTPS

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS), è un protocollo che integra l'interazione di HTTP attraverso un meccanismo di crittografia di tipo Transport Layer Security (SSL/TLS). Quindi il protocollo HTTP è utilizzato all'interno di un canale realizzato con SSL/TLS. In pratica viene creato un canale di comunicazione criptato tra il client e il server attraverso uno scambio di certificati; una volta stabilito questo canale al suo interno viene utilizzato il protocollo HTTP per la comunicazione. Questo tipo di comunicazione garantisce che solamente il client e il server siano in

grado di conoscere il contenuto della comunicazione. La porta di default per il protocollo HTTPS è la numero 443 (mentre per il protocollo HTTP è la numero 80). Viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti che potrebbero essere effettuati tramite la tecnica di attacco del man in the middle.[101]

3.5 Pagamenti conctactless

I sistemi conctactless come abbiamo descritto nei capitoli precedenti sono quei mezzi di pagamento che prevedono l'impiego di particolari strumenti che utilizzano una tecnologia RFID(Radio Frequency Identification), come ad esempio carte di credito tradizionali, carte prepagate, carte di debito, o altri dispositivi, che consentono di poter effettuare transazioni senza dover introdurre fisicamente questi in un terminale, ma semplicemente utilizzando il passaggio ravvicinato. Questa soluzione permette di pagare in maniera semplice e veloce e senza l'impiego di misure di sicurezza come il PIN (Personal Identification Number), visto che gli istituti finanziari hanno fissato un importo massimo pari a 25 euro, per ciascun pagamento. Tuttavia se questa soglia venisse superata, allora invece bisognerebbe firmare lo scontrino o digitare codice PIN per provvedere ad una tutela maggiore. Effettuare una transazione con carte conctactless è immediato e comporta i seguenti passi:[102]

- l'esercente digita l'importo della transazione sul display del lettore contactless
- il consumatore avvicina la carta al lettore
- il lettore contactless emette un segnale luminoso e acustico a conferma della lettura della carta, ovvero dell'avvenuto pagamento

Diamo ora un occhiata alla tecnologia che utilizziamo per i pagamenti per capire un po' meglio il loro funzionamento.

3.5.1 Tecnologia RFID

Per poter conoscere la tecnologia RFID, diamo prima una definizione di trasponder. Il trasponder o trasponditore, è un ricetrasmettitore in grado di inviare un segnale radio in risposta ad un comando ricevuto da una stazione remota. Il segnale di comando è essenziale per determinare la trasmissione del segnale di ritorno, dal trasponder. Il sistema IFF[11] (provvisto di trasponder), era un sistema sviluppato nella seconda guerra mondiale, già nel 1940, che prevedeva l'istallazione di questa tecnologia all'interno dell'abitacolo degli aerei, per poter comunicare quali veramente facessero parte degli alleati. Con il termine RFID, si intende quindi una tecnologia, in grado di identificare e memorizzare dati riguardanti una persona, oggetti o animali, all'interno di particolari strumenti elettronici chiamati Tag (o trasponder). Questa identificazione avviene tramite un campo elettromagnetico, in cui un lettore statico o portatile (Reader, in grado di comunicare e aggiornare le informazioni contenute internografo di un tag interrogato), manda un segnale generato da un'antenna. Il tag, una volta riconosciuta la correttezza dell'operazione di interrogazione, manda al Reader un segnale che contiene il proprio codice di identificazione univoco, ed altri dati memorizzati. I sistemi RFID, fanno appunto parte della tecnologia Auto-ID, o identificazione automatica, che permette l'acquisizione automatica di dati per l'identificazione e l'introduzione automatica di questi, ed altri dati (senza l'ausilio di tastiere o operazioni manuali), all'interno di programmi di un computer. Questa procedura, consente perciò di limitare gli errori che possono nascere al momento di inserimenti manuali di dati e garantiscono un vantaggio in quanto a tempi e costi inerenti a operazioni manuali. Il sistema RFID è dunque composto da due parti fondamentali : il Tag e il Reader. Il Tag è formato da:

- un chip, cioè il componente elettronico, a cui spetta il compito di dover gestire tutta la parte legata alla comunicazione e identificazione. Questo strumento possiede dunque un codice identificativo univoco e non è in grado di contenere più di 2 Kb di dati[103].

[11] it.wikipedia.org/wiki/Identification_friend_or_foe

- Un'antenna, ovvero l'apparato che permette al chip di poter ricevere e trasmettere le informazioni

- Supporto, cioè il materiale che sostiene e protegge il sistema composto da chip e antenna.

Il Reader, che è il sistema che si occupa di interrogare i tag, inviare e ricevere i dati ed interfacciarsi con i sistemi informativi esistenti, è composto da due parti:

- L'unità di controllo, che è a tutti gli effetti un microcalcolatore in grado di gestire in tempo reale, il collegamento con le antenne (può gestire normalmente da 4 ad 8 antenne diverse), l'interrogazione dei tag (nel raggio dazione dell'antenna), gestione delle collisioni dei messaggi di risposta dei tag, ed infine il collegamento con sistemi informativi aziendali.

- Le antenne, che sono strumenti posti fra unità di controllo e tag, i quali devono generare un campo magnetico per poter attivare un trasponder, dando la possibilità di comunicare fra le parti.[104]

è possibile fare un'ulteriore distinzione, riguardante la classificazione dei Trasponder, questi possono essere: attivi, passivi, ibridi(attivi/passivi).

- **ATTIVI**: sono integrati sia da un trasmettitore radio e sia da una batteria in grado di alimentarlo. Questa batteria consente di poter alimentare il tag ed avere di conseguenza un raggio d'azione, molto più elevato rispetto a le altre tipologie di dispositivi. Gli svantaggi, consistono in un costo più elevato del dispositivo e obbligo di ricarica o sostituzione della batteria una volta esaurita.

- **PASSIVI**: questi dispositivi "riflettono" il segnale trasmesso verso di loro dal Reader o aggiungono informazioni attraverso l'utilizzo del segnale riflesso. Questi tag a differenza dei precedenti non utilizzano nessun tipo di batteria per essere alimentati, di conseguenza il loro raggio di azione è molto pi ù limitato, dell'ordine pochi centimetri o metri e possiedono un costo molto basso.

- **IBRIDI**: In questa versione di Trasponder è contenuta una batteria, utilizzata solamente per poter alimentare il trasmettitore radio, ma per comunicare con il lettore, utilizza lo stesso modo dei tag passivi. Questi dispositivi sono molto più complessi e costosi rispetto ai trasponder passivi.

Una volta descritta la natura dei tag, è possibile passare alla conoscenza delle frequenze con cui questi dispositivi comunicano con i Reader. Queste frequenze, inoltre, sono regolate da organismi internazionali e nazionali in grado di disciplinare da regione a regione, l'utilizzo di queste tecnologie RFID. Lo svantaggio principale di questo sistema è dato dal fatto di non riuscire a garantire l'interoperabilità in tutti i paesi, non permettendo perciò di poter utilizzare alla stessa maniera i dispositivi RFID, in parti differenti del mondo. Le frequenze più utilizzate sono: [105]

- 120-145 MHz (LF, Low Frequencies, valida in tutto il mondo)
- 13,56 MHz (HF, High Frequencies, utilizzata in tutto il mondo, ed impiegata per esempio in, smartcard per controllo accessi, identificazione e pagamenti, nelle etichette associate ad oggetti, quali controllo bagagli, lavanderie, biblioteche e altro ancora).
- 433-435 MHz (UHF, Ultra High Frequencies bassa, solo per tag Attivi, solo in Europa)
- 865 - 870 MHz (UHF, Ultra High Frequencies media, in Europa), 902-928 MHz (UHF, Ultra High Frequencies media, USA), 950 MHz (UHF, Ultra High Frequencies media, Asia).
- 2,4 GHz (UHF, Ultra High Frequencies alta, in tutto il mondo)
- 5,8 GHz (SHF, Super High Frequencies, utilizzato per il dispositivo Telepass).

3.5.2 Sicurezza pagamenti conctactless

In quanto a sicurezza, queste tipologie, rappresentano un modo sicuro per poter effettuare operazioni di pagamento. Le reti finanziarie sfruttate

per l'elaborazione di informazioni utilizzate per i pagamenti, sono le stesse che vengono impiegate per effettuare le operazioni con carta di credito o bancomat. Che sia un dispositivo di tipo carta, o di qualunque altra tipologia, l'unica differenza consiste nel fatto che le informazioni di pagamento sono inviate ad un Pos, utilizzando la tecnologia a radio frequenza. Questi sistemi, come descritto per NFC, utilizzano una sicurezza intrinseca, visto che la comunicazione avviene a distanze molto brevi, 2-4 cm. Per i pagamenti conctactless l'industria finanziaria ha aggiunto più livelli di sicurezza sia sul dispositivo e sia nella rete adibita all'elaborazione, per poter gestire e prevenire eventuali frodi. Nelle carte conctactless, vengono utilizzate le seguenti tecniche di sicurezza:[106]

- **Crittografia** : a livello della carta, ognuna può avere la sua unica "chiave" che utilizza la tecnologia crittografica standard (AES, Advanced Encryption Standard, specifico standard per la crittografia dei dati elettronici, che utilizza blocchi di 128 bit[107]) per generare un valore unico di verifica della carta, o un codice di autenticazione per identificare esclusivamente ogni singola transazione. La chiave non viene mai trasmessa e non possono esserci due dispositivi in grado di condividere la stessa chiave.

- **Autenticazione** : il codice di autenticazione o crittogramma devono prima essere accettati, dal canale di pagamento, per poter validare la transazione. A livello di sistema è possibile dunque, per il canale di pagamento, poter rilevare e respingere automaticamente, qualunque tentativo di utilizzo delle medesime informazioni per più volte nella stessa transazione.

- **Riservatezza** : i pagamenti effettuati mediante carte conctactless, non richiedono l'utilizzo del nome del titolare della carta per ogni transazione. Anzi il nome del proprietario della carta non è proprio incluso nel chip conctactless.

- **Controllo** : i titolari della carta sono appunto in grado di controllare sia la transazione che stanno andando a effettuare e sia la carta durante

l'operazione. Durante la transazione il proprietario, non deve rilasciare nessuna informazione riguardante il proprio conto di pagamento.

3.5.2.1 Minacce per RFID

Nonostante i sistemi di pagamento contactless siano uno strumento sicuro, bisogna però sapere che, anche per RFID, possono esserci delle minacce in grado di violare la sicurezza di tale tecnologia. Questi attacchi sono essenzialmente raggruppabili in 5 tipologie:[108]

- **Sniffing** : grazie a questa tecnica, è possibile la lettura dei tag RFID, da parte di un soggetto malintenzionato, in qualsiasi momento, tramite dispositivi adatti alla lettura del dispositivo, senza che la vittima ne sia evidentemente a conoscenza.

- **Tracking** : una volta posizionati dei lettori RFID in posizioni strategiche, con questo attacco, è possibile registrare il passaggio di tag identificativi ai quali sono associate identità personali. In questa maniera riusciremmo a tracciare gli effettivi spostamenti di una persona.

- **Spoofing** : consiste nell'alterazione delle informazioni trasmesse dai tag ai reader (ricordiamo il caso della Mobile società petrolifera)

- **Replay attack** : con questo attacco è possibile intercettare e ritrasmettere le credenziali di autenticazione, ingannando i lettori dei sistemi di pagamento conctactless, simulando l'identità dell'emittente.

- **Denial of service** : questo attacco impedisce ai sistemi RFID di poter funzionare correttamente, creando un disturbo del segnale di trasmissione, non permettendo alle onde trasmesse di raggiungere i tag.

Capitolo 4

Biometria

Il continuo bisogno di protezione di dati sensibili nonostante la presenza di sistemi, già in grado di garantire ciò, ha condotto la società ad accrescere le esigenze di pubblica sicurezza, per far fronte alle numerose tipologie di frodi, favorendo l'introduzione e lo sviluppo di tecnologie sempre più sofisticate, che fossero in grado di promettere maggiori livelli di affidabilità ed accuratezza. Questi nuovi sistemi si basano su l'impiego della Biometria per effettuare un ulteriore autenticazione, in aggiunta a quelle tradizionali, aumentando così di fatto la fiducia delle persone, ed eliminando di conseguenza quella naturale diffidenza e insicurezza che ogni soggetto pone negli strumenti di pagamento.

4.1 Autenticazione biometrica

L'autenticazione biometrica, è un metodo attraverso il quale vengono utilizzate della caratteristiche biologiche uniche per identificare in maniera univoca ogni individuo. Queste caratteristiche, possono essere: **Fisiologiche**, cioè si basano su dati statici come ad esempio impronte digitali, disegno dell'iride, sagoma della mano, immagine del volto o riconoscimento DNA. **Comportamentali**, ovvero si riferiscono ad un azione svolta dal soggetto, come ad esempio lo stile di battitura, voce o calligrafia. Solitamente le caratteristiche fisiologiche sono poco variabili nel tempo e costituiscono dunque una componente abbastanza stabile, mentre le caratteristiche comportamentali

possono essere influenzate dalla psicologia dell'individuo. Il riconoscimento biometrico, solitamente si basa su tre tipologie di richieste:

- Un qualcosa che un utente può possedere, come ad esempio un badge
- Qualcosa che un soggetto può conoscere, ad esempio il PIN.
- Un aspetto fisiologico o comportamentale

Per poter acquisire i dati biometrici, all'inizio, nella fase di registrazione, è necessario l'impiego di un meccanismo che sia in grado di poter leggere i tratti caratteristici dell'individuo, come ad esempio uno scanner (lettore). Una volta acquisite le caratteristiche biometriche dallo scanner, un sistema informatico, deve elaborarle, tradurle in un codice binario e successivamente depositarle, il maniera cifrata, in una banca dati che avrà il compito di conservarle. In futuro i nuovi dati, acquisiti dallo scanner, saranno confrontati con quelli inseriti nella banca dati precedentemente, permettendo così di verificare se effettivamente un utente è colui che afferma di essere, ed in caso positivo ottenere il via libera. [109] Oggi i sistemi biometrici più utilizzati sono basati sulle impronte digitali e sono anche quelli maggiormente diffusi perchè i primi a essere utilizzati su larga scala.[110]

4.1.1 Sicurezza biometrica

Già nel mondo odierno esistono dispositivi tecnologici che utilizzano i sistemi biometrici basati su impronte digitali per effettuare pagamenti affidabili, tra cui ricordiamo lo smartphone Galaxy S5, che possiede un sensore in grado di riconoscere le impronte digitali, il quale è collegato all'applicazione di pagamento PayPal, ottenendo, in caso di autenticazione positiva, libero accesso al conto del portafoglio elettronico mobile. Altro strumento conosciuto è l'Iphone 5S, il quale possiede anche lui un sensore, Touch ID, che lo collega ad applicazioni in grado di poter effettuare pagamenti mobili.[111] Vista questa diffusione, è quindi possibile che l'autenticazione biometrica basata su impronte digitali, sia un sistema effettivamente sicuro? La risposta è NO, per il semplice fatto che un organizzazione chiamata Chaos Computer Club, è riuscita di fatto ad aggirare questo sistema di autenticazione, semplicemente utilizzando materiali reperibili ovunque. Per aggirare la sicurezza

dei sensori biometrici, è bastato costruire una falsa impronta digitale secondo questa procedura:[112]

1. Riuscire a reperire un impronta digitale della vittima che si vuole attaccare, una buona fonte possono essere ad esempio bicchieri o maniglie delle porte.

2. Successivamente spruzzare con polvere di grafite (materiale utilizzato per la produzione di matite), che reagendo con il sudore e il grasso lasciato dall'impronta, permetterà di renderla visibile. Oppure un altro metodo alternativo alla graffite, può essere quello di utilizzare una soluzione di Cianocrilato (utilizzato in ambito forense per rilevare le impronte[113]), presente nella colla liquida, ed in grado di formare un calco solido se applicata ad un'impronta.

3. Una volta resa visibile l'impronta, è il momento di procedere alla scansione di questa, tramite una macchina fotografica (ovviamente con una buona risoluzione).

4. Digitalizzata l'impronta, è necessario eseguire una piccola ristrutturazione grafica, con l'obbiettivo di ottenere un immagine uguale ad una impronta digitale.

5. Bisogna poi stampare questa immagine sopra ad una diapositiva trasparente (quella utilizzata solitamente per lavagne luminose) con una stampante al laser. Il toner, forma un rilievo, che sarà poi successivamente utilizzato in maniera simile ad una lettera da stampa.

6. La stampa del manichino uscito deve essere ricoperto da un sottile strato di colla per legna e lasciato asciugare.

7. Una volta asciutta, il foglio della stampa del manichino viene tirato via e viene tagliato un dito su misura.

8. E l'impronta digitale fasulla è pronta per essere utilizzata

L'elusione del blocco delle impronte digitali è stato reso possibile con l'individuazione di una risoluzione appena maggiore di quella impiegata dal

sensore biometrico, che consentisse di fatto di poter creare, con una risoluzione adeguata, la nostra finta impronta. In conclusione si può di certo affermare che anche se il riconoscimento biometrico delle impronte digitali è un mezzo molto utilizzato al giorno d'oggi, non dovrebbe essere impiegato per garantire nulla, proprio perchè le impronte possono essere lasciate facilmente ovunque ed è altrettanto facile poter costruire finte stampe di queste.[114]

Capitolo 5

Conclusioni

Nel corso della storia i sistemi di pagamento hanno sempre avuto una forte evoluzione, dovuta in parte ai bisogni della società di poter disporre di metodi che garantissero una maggior velocità e facilità di transazione e dall'altra di un'affidabilità sempre più elevata. La nascita e la crescita di nuove tecnologie andavano dunque di pari passo con modalità di pagamento innovative. Per questo le tecnologie si sono sempre mosse a favore, anche della tutela di questi mezzi di pagamento, fronteggiando frodi, sempre più complesse e che richiedevano sistemi di sicurezza sempre più elevati. Attualmente siamo certi di esser giunti ad un punto in cui ogni tecnica o modalià di pagamento può essere considerata quasi del tutto protetta, in quanto ogni dato trattato o elaborato, è inviato attraverso canali in grado di garantire una elevata riservatezza e protezione. Sottolineo quasi, per il semplice motivo che qualunque operazione di pagamento, che si andrà a compiere, non garantisce, ne garantirà mai una sicurezza assoluta, la quale, secondo il mio punto di vista, è irraggiungibile, dato che le truffe si muovono di pari passo. Potranno quindi sempre verificarsi truffe, a differenza del contante però, i pagamenti elettronici avranno sempre maggiori strumenti di tutela, visto che solitamente banche ed altri soggetti finanziari, sono in grado di assumersi il rischio di eventuali frodi, risarcendo la vittima. Certamente lo sviluppo di nuovi mezzi di autenticazione, come nel caso della biometria, apporterà naturalmente, notevoli benefici nel campo dell'autenticazione e protezione di identità, ma bisogna essere consapevoli che nonostante i passi mossi della

tecnologia, verso l'innovazione, questi non saranno mai in grado di garantire la totale affidabilità dei metodi di pagamento. Per questo è bene che ogni singolo individuo mostri una maggior attenzione rispetto all'uso che fa del proprio mezzo di pagamento. In conclusione, si può quindi affermare che la componente umana gioca un ruolo fondamentale nel campo della protezione delle proprie informazioni, visto che le azioni dell'individuo possono determinare scelte tattiche che, se compiute in maniera coscienziosa possono andare a supporto delle tecniche di sicurezza, garantendo perciò, una protezione intrinseca superiore.

Bibliografia

[1] http://www.treccani.it/enciclopedia/sistemi-di-pagamento

[2] http://www.bancaditalia.it

[3] http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2014-06-13/servizi-pagamento-elettronico-144309.php

[4] http://www.prepagateonline.com/articoli/carta-prepagata-cosa.htm

[5] http://www.techeconomy.it/2014/02/20/osservatorio-mobile-payment-commerce-nuovi-pagamenti-elettronici-valgono-15-miliardi

[6] http://www.osservatori.net/dati-e-pubblicazioni

[7] http://www.altroconsumo.it/Serp/ShowResults?keyword=mobile+payment

[8] E-business, Gary P. Schneider, Cengage Learning, 2011

[9] http://www.google.com/wallet

[10] http://www.smartcardalliance.org/publications-nfc-frequently-asked-questions/#7

[11] http://cybersecurity.mit.edu/2012/10/google-wallet-overview-threats-and-security-measures

[12] http://viaforensics.com/mobile-security/forensics-security-analysis-google-wallet.html

[13] http://update.ebayinc.com/

[14] http://www.paypal.com/webapps/mpp

[15] http://www.unicredit.it/it/privati/serviziinnovativi/iphone-smartphone/mobiletoken.html

[16] http://www.unicredit.it/it/privati/serviziinnovativi/sicurezzaonline/passwordunicreditpassmo

[17] http://www.html.it/articoli/introduzione-ad-oauth-20-con-java-1

[18] http://portswigger.net/burp/

[19] http://www.duosecurity.com/blog/duo-security-researchers-uncover-bypass-of-paypal-s-two-factor-authentication

[20] http://www.duosecurity.com/blog/the-paypal-2fa-bypass-how-legacy-infrastructure-impacts-modern-security

[21] http://www.ft.com/intl/cms/s/0/d70b9cac-fc83-11e3-98b8-00144feab7de.html

[22] http://www.ilpost.it/2014/10/23/apple-pay

[23] http://www.wired.it/mobile/smartphone/2014/09/10/apple-pay-come-funziona

[24] http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

[25] http://www.forbes.com/sites/davelewis/2014/09/09/apple-pay-in-ios8

[26] http://www1.american.edu/initeb/sm4801a/epayment1.htm

[27] http://www.gdf.gov.it/GdF/it/Servizi-per-il-cittadino/Consigli-utili/info-1163902317.html

[28] http://www.bitcoin-italia.org

[29] http://bitcoin.org/it

[30] http://it.wikipedia.org/wiki/Bitcoin

[31] http://it.bitcoin.it/wiki/Pagina_principale

[32] http://www.repubblica.it/tecnologia/2014/10/20/news/bitcoin_italia-98573671

[33] http://www.fdic.gov/consumers/consumer/news/cnspr14/p2p.html

[34] http://www.kfi.it/it/sistemi-di-pagamento.html

[35] http://www.ilsole24ore.com/art/SoleOnLine4/Tecnologia%20e%20Business/2009/11/paypas
contactless.shtml

[36] http://watch2pay.co.uk/en/product/what-is-watch2pay.html

[37] http://www.autostradetech.it/it/soluzioni/tolling/esazione-automatica-con-dsrc-sistema-telepass.html

[38] http://www.treccani.it/enciclopedia/baratto

[39] http://www.bartex.it/pagina/37/bartering#.VFDVw_mG_IU

[40] http://www.giuseppefelloni.it/img/ASeriesofFirsts.pdf

[41] http://www.skuola.net/economia-ragioneria/moneta-evoluzione.html

[42] http://doc.studenti.it/vedi_tutto/index.php?h=e6f85270&pag=2

[43] http://www.scripofilia.it/news.asp?newsID=747&c=a

[44] Dal Prestito Personale alle Carte di Credito. Come Ottenere un Prestito e Gestire i Tuoi Soldi Senza Rischi per il Portafogli, Roberto Borzellino, Bruno Editore, 01/gen/2014

[45] Sicurezza dei sistemi informatici, M. Grazia Fugini, Fabrizio Maio, Pierluigi Plebani, Apogeo Editore, 2001

[46] La grande storia del computer. Dall'abaco all'intelligenza artificiale, Massimo Bozzo, EDIZIONI DEDALO, 1996

[47] http://www.cartedipagamento.com/banda_magnetica_carta_di_credito.htm

[48] http://www.labancaonline.com/origini_banca_online.html

[49] http://www.i-dome.com/articolo/4523-PRESTEL.html

[50] http://ricerca.repubblica.it/repubblica/archivio/repubblica/1984/11/03/pirati-nella-rete-elettronica-gettano-scompiglio-in.html

[51] http://securitydigest.org/rutgers/mirror/pyrite.rutgers.edu/prestel.hacking

[52] http://www.emvco.com

[53] E-commerce: i sistemi di pagamento via Internet e la moneta elettronica, Antonio Chirico, Esselibri Simone, 2006

[54] RFID Security, Frank Thornton, Chris Lanthem, Syngress, 25/mag/2006

[55] How to Cheat at Deploying and Securing RFID, Frank Thornton, Paul Sanghera, Syngress, 18/apr/2011

[56] http://www.repubblica.it/tecnologia/2013/01/02/news/i_40_anni_della_prima_telefonata_da_ce
49791306

[57] Rivoluzione mobile. I cambiamenti sociali e di marketing introdotti dalle tecnologie mobili, Brognara, FrancoAngeli, 2014

[58] Reti di calcolatori e Internet. Un approccio top-down, James F. Kurose, Keith W. Ross, Pearson, 2008

[59] http://www.ilsole24ore.com/art/tecnologie/2012-04-06/banda-larga-rete-cellulare-185851.shtml?uuid=Ab27y9JF

[60] http://www.itu.int/net/pressoffice/press_releases/2010/48.aspx#.VFuvuPmG_IU

[61] La telefonia mobile e il laboratorio Italia. Primo rapporto sulla telefonia mobile in Italia, Andrea Giuricin, Massimiliano Trovato, IBL Libri, 2009

[62] http://www.infosec.gov.hk/english/technical/files/short.pdf

[63] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=4625610

[64] http://arxiv.org/ftp/arxiv/papers/1002/1002.3171.pdf

[65] http://www.lastampa.it/2014/01/18/blogs/centro-messaggi/anno-del-mobile-payment-gli-esempi-di-tech-e-ipayst-JBCQJ4gT1h2csuDzs6KrHJ/pagina.html

[66] http://www.i-dome.com/articolo/14322-Un-innovativo-sistema-di-pagamento-via-SMS-con-Cash-Mobile.html

[67] http://www.schneier.com/blog/archives/2005/10/sms_denialofser_1.html

[68] http://www.ilsole24ore.com/art/tecnologie/2012-11-30/cose-come-funziona-smishing-113543.shtml

[69] http://www-03.ibm.com/software/products/it/category/mobile-application-development

[70] http://www.altroconsumo.it/hi-tech/cellulari/news/applicazioni-per-smartphone-altroconsumo-244

[71] http://www.html.it/pag/15096/introduzione-a-java

[72] http://www.html.it/guide/guida-c2

[73] http://www.html.it/guide/guida-objective-c

[74] http://www.webnews.it/2008/01/18/panoramica-sui-linguaggi-di-sviluppo-per-mobile-1

[75] http://www.html.it/pag/15338/browser-e-microbrowser

[76] http://www.pcmag.com/encyclopedia/term/54198/wap

[77] Reti di calcolatori, Andrew S. Tanenbaum, Pearson Italia S.p.a., 2003

[78] http://www.wapforum.org/what/wapwhite_paper1.pdf

[79] http://www.html.it/pag/15335/i-nuovi-canali-di-accesso-al-web

[80] http://www.ilsole24ore.com/art/tecnologie/2012-11-16/mobile-commerce-italia-numeri-170003.shtml?uuid=AbtxPY3G

[81] http://www.kaspersky.com/it/internet-security-center/internet-safety/tips-for-mobile-security-smartphone

[82] http://www.nfcitaliaworld.it/cose-nfc-near-field-communication

[83] http://www.rfidglobal.it/tecnologia-nfc-note-tecniche

[84] http://www.malaboadvisoring.it/index.php?option=com_docman&task=doc_download&gid=

[85] http://www.oversecurity.net/2013/05/21/nfc-il-politecnico-di-milano-ci-illustra-la-sicurezza-di-questa-tecnologia

[86] http://www.tec-it.com/en/support/knowbase/symbologies/qrcode/Default.aspx

[87] http://www.qrcode.com/en

[88] http://www.csita.unige.it/manuali/smartphone/qrcode

[89] http://www.qrcode.com/en/about/version.html

[90] http://www.youthedesigner.com/graphic-design-tips/what-is-a-qr-code-and-how-does-it-work

[91] http://www.wireless4innovation.it/approfondimenti/pagamenti-da-smartphone-e-tablet-le-iniziative-in-italia_43672151578.htm

[92] http://www.repubblica.it/tecnologia/2012/05/09/news/se_il_qr_code_nasconde_minacce-34569805

[93] http://www.01net.it/qr-code-comodi-ma-anche-pericolosi/0,1254,3_ART_147164,00.html

[94] http://www.iso.org/iso/catalogue_detail?csnumber=31432

[95] http://www.cs.unibo.it/ margara/page2/page6/page25/assets/Smart

[96] http://www.osservatori.net/dati-e-pubblicazioni/dettaglio/journal_content/56_INSTANCE_VI

[97] http://www.fastweb.it/internet/cosa-sono-i-protocolli-ssl-tls-e-openssl

[98] http://it.wikipedia.org/wiki/Secure_Electronic_Transaction

[99] http://centridiricerca.unicatt.it/cratos_Q_1998_E_Bruschi_Delgrossi.pdf

[100] http://it.kioskea.net/contents/812-criptografia-il-protocollo-set

[101] http://it.wikipedia.org/wiki/HTTPS

[102] http://www.sostariffe.it/news/carta-di-pagamento-contactless-cosa-sapere-e-come-tutelarsi-26609

[103] http://www.fastweb.it/internet/cos-e-la-tecnologia-rfid

[104] RFID. Identificazione automatica a radiofrequenza, Luigi Battezzati, J. L. Hygounet, HOEPLI EDITORE, 2006

[105] http://www.rfid.fub.it/edizione_2/Parte_I.pdf

[106] http://www.smartcardalliance.org/publications-contactless-payment-security-qa/

[107] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[108] http://vitali.web.cs.unibo.it/viewfile/LabInt09/ConsegnaRelazioni?rev=1.2&filename=RF

[109] http://www.di.unisa.it/professori/ads/corso-security/www/CORSO-9900/biometria/index.htm

[110] http://e-learning.dti.unimi.it/Portale/rivista/?p=726

[111] http://www.ilsole24ore.com/art/tecnologie/2014-04-16/galaxy-s5-violato-sensore-impronte-digitali-paypal-nessun-problema-i-pagamenti-185308.shtml?uuid=ABMI8bBB

[112] http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren.en

[113] http://it.wikipedia.org/wiki/Cianoacrilati#Applicazioni

[114] http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

Ringraziamenti

Vorrei ringraziare i miei genitori, mia sorella e i nonni per tutto il sostegno, l'affetto e la pazienza dimostrata in tutti questi anni, che hanno contribuito a poter realizzare questo traguardo importante. Voglio dedicare anche un ringraziamento speciale alla mia ragazza Giulia, che è stata comprensiva e ha saputo incoraggiarmi e darmi buoni consigli in alcuni momenti difficili ed è tuttora ora parte importante nella mia vita. Un ringraziamento va anche a zii, cugini e amici di famiglia per il loro continuo supporto. Ringrazio inoltre tutti gli amici, per l'ausilio datomi in diverse occasioni. Tra questi ringrazio Mattia, che mi ha fornito diversi spunti per la decisione del titolo. Infine, un sentito grazie va a tutta la famiglia della mia ragazza, perché fin dal primo giorno, mi hanno sempre fatto sentire come uno di "casa".