

ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

---

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI  
Corso di Laurea in Scienze di Internet

## Sistemi per il pagamento elettronico

Tesi di Laurea in Algoritmi e Strutture Dati

Relatore:  
Chiar.mo Prof.  
Moreno Marzolla

Presentata da:  
Francesco Varanelli  
Mat. 0000247821

I

2009-2010

*Alla mia famiglia...*



# Sommario

In questa tesi verranno descritti i principali metodi di pagamento online attualmente presenti nel mercato elettronico. Successivamente, verranno paragonati tra loro, evidenziando i vantaggi e gli svantaggi legati ad ognuno di essi. Questi confronti saranno basati su sei principali caratteristiche che ogni metodo di pagamento online possiede. L'obiettivo principale è, dunque, far capire all'utente quale sistema di pagamento sia a lui più conveniente, attraverso una tabella riepilogativa che denoterà pregi e difetti legati alle varie forme di pagamento. Nella tesi si parlerà principalmente dei sistemi di pagamento online, che saranno introdotti da una breve descrizione sull'e-commerce, dove verranno identificati gli attori delle compravendite online e le varie forme di e-business. Molta importanza verrà data alla sicurezza legata alle transazioni via Web; il fattore sicurezza è il principale limite frenante dell'e-commerce, poichè gli utenti sono piuttosto frenati dalla possibilità che i propri dati vengano intercettati da terze parti per scopi fraudolenti. Verranno quindi descritti i principali rischi e le principali forme di sicurezza da intraprendere, si parlerà dei principali protocolli di sicurezza e dei sistemi di crittografia ad essi associati. Nell'ultimo capitolo questi sistemi di pagamento online verranno confrontati tra loro, questi confronti verranno visualizzati in una tabella riepilogativa che permetterà di identificare uno specifico metodo di pagamento online adatto alle proprie esigenze.



# Indice

<b>INDICE</b>	<b>i</b>
<b>1 Il commercio elettronico</b>	<b>2</b>
1.1 Introduzione . . . . .	2
1.2 Il commercio elettronico: concetto generale	3
1.3 Problematiche del commercio elettronico .	5
1.4 Le varie forme di Commercio Elettronico .	8
1.4.1 Business-to-business (B2B) . . . . .	8
1.4.2 Business-to-consumer (B2C) . . . . .	9
1.4.3 Consumer-to-consumer (C2C) . . . . .	9
1.4.4 Consumer-to-business (C2B) . . . . .	10
<b>2 Tipologie di metodi di pagamento online</b>	<b>11</b>
2.1 Introduzione . . . . .	11
2.2 Carta di credito . . . . .	15
2.3 Carte ricaricabili . . . . .	20
2.4 Paypal . . . . .	23
2.5 BankPass Web (“pagamentionline” Si-servizi)	29
2.6 Bonifico bancario online . . . . .	32
2.7 Sistemi di pagamento emergenti . . . . .	36
2.7.1 Square . . . . .	36
2.7.2 Google Check-out . . . . .	39
<b>3 Rischi e forme di sicurezza nei pagamenti online</b>	<b>41</b>
3.1 I rischi . . . . .	41
3.2 Forme di sicurezza . . . . .	43
3.2.1 Sistemi di crittografia . . . . .	47
3.2.1.1 Crittografia simmetrica . . . . .	47

3.2.1.2	Crittografia asimmetrica . . . . .	49
3.2.2	Il protocollo HTTPS . . . . .	51
3.2.3	Protocollo SET . . . . .	51
<b>4</b>	<b>Sistemi di pagamento online a confronto</b>	<b>54</b>
4.1	Introduzione . . . . .	54
4.2	Riservatezza . . . . .	56
4.3	Accettazione . . . . .	57
4.4	Costi . . . . .	58
4.5	Sicurezza . . . . .	59
4.6	Tempi . . . . .	61
4.7	Facilità d'uso . . . . .	61
4.8	Tabella riepilogativa . . . . .	63

# Elenco delle figure

2.1	Funzionamento Carta di credito/Carta ricaricabile . . . . .	20
2.2	Funzionamento Paypal . . . . .	27
2.3	Funzionamento Sis-Bankpass . . . . .	31
2.4	Funzionamento bonifico bancario online . . . . .	35
2.5	Funzionamento Square . . . . .	38
2.6	Funzionamento Google Check-out . . . . .	40
3.1	Schema SET . . . . .	53

# Elenco delle tabelle

1.1	Attori nel commercio elettronico . . . . .	4
1.2	Motivazioni scarso successo dell'e-commerce . . . . .	7
2.1	Tariffe transazioni Paypal . . . . .	28
2.2	Costi di Square . . . . .	36
4.1	Tabella riepilogativa . . . . .	63

# Capitolo 1

## Il commercio elettronico

### 1.1 Introduzione

Con lo sviluppo delle tecnologie digitali e con la maggiore diffusione di Internet, si è verificato un vero e proprio mutamento all'interno della società e di conseguenza del singolo individuo. Internet, sfruttando la possibilità di mettere in comunicazione tra loro persone da ogni angolo del pianeta, ha creato un nuovo mercato innovativo.

Con l'evolversi di questa nuova frontiera commerciale online, ed il crescente interesse da parte degli utilizzatori verso gli strumenti offerti dalla rete, questi ultimi assumono una rilevante importanza sia da un punto di vista economico che da un punto di vista sociologico: il principale fattore per il successo dell'e-commerce è la reazione, positiva o negativa che sia, dei singoli utilizzatori, analizzata in maniera aggregata. La possibilità di effettuare transazioni commerciali utilizzando Internet è diventata una realtà concreta e in continua evoluzione; tuttavia, vi è ancora una generalizzata paura del nuovo, di ciò che ancora non si conosce e non si comprende del tutto, ed infatti fattori psicologici, quali la diffidenza e la sfiducia, rappresentano i principali ostacoli all'avvicinamento ai mercati elettronici da parte di nuovi utilizzatori.

## 1.2 Il commercio elettronico: concetto generale

Il commercio elettronico si può definire come l'attività di vendita e acquisto di beni e servizi svolta con l'ausilio e tramite sistemi di comunicazione informatica.

Il commercio elettronico (detto anche E-Commerce da Electronic Commerce) oltre ad essere una valida alternativa al commercio tradizionale è considerato la nuova frontiera del business. Il Ministero dell'Industria, del Commercio e dell'Artigianato lo definisce in questo modo[1]:

*“L'E-Commerce consiste nello svolgimento di attività commerciali e di transazioni per via elettronica e comprende attività diverse quali: la commercializzazione di beni e servizi per via elettronica, la distribuzione online di contenuti digitali, l'effettuazione per via elettronica di operazioni finanziarie e di borsa, gli appalti pubblici per via elettronica ed altre procedure di tipo transitorio della pubblica Amministrazione”.*

E' possibile acquistare un bene via internet con diverse modalità: un utente può acquistare un prodotto immediatamente, con il semplice “scaricamento” da un sito Web dopo aver pagato un prezzo stabilito (esempio può essere l'acquisto di un file musicale MP3), oppure può acquistare un bene in maniera tradizionale, il che necessita di una forma di consegna e che quindi non prevede una contestualità tra acquisto e consegna.

In questo elaborato l'utilizzo del termine commercio elettronico individuerà principalmente le transazioni ed i modelli di business riferibili ad Internet, ed in particolare saranno trattate le modalità di pagamento delle merci acquistate dai consumatori finali attraverso

la rete. Comprare e vendere su Internet è la tendenza del futuro e offre vantaggi sia per le aziende che per i consumatori.

Gran parte delle aziende che utilizzano il commercio elettronico hanno la possibilità di ridurre i costi di marketing e di vendita, di migliorare il rapporto con i clienti e i fornitori e raggiungere nuovi mercati.

Il consumatore ha invece la possibilità di ottenere informazioni dettagliate sui prodotti o sui servizi richiesti, comparare rapidamente le offerte di fornitori diversi risparmiando sui costi di acquisto e risparmiando tempo.

Il significato del termine “commercio elettronico” è mutato col passare del tempo. All’inizio indicava il supporto alle transazioni commerciali in forma elettronica, generalmente ricorrendo a una tecnologia denominata Electronic Data Interchange (EDI, introdotta alla fine degli anni settanta) per inviare documenti commerciali come ordini d’acquisto o fatture in formato elettronico.

Gli attori del commercio elettronico sono mostrati nella tabella 1.1:

Nome	Descrizione
Merchant	Gestore del sito di e-commerce
Merchant system	La soluzione hw/sw adottata dal Merchant
Payment Gateway	Società incaricata di eseguire le transazioni nei circuiti bancari degli attori
Certificati digitali	File che certificano l’identità dell’attore (Merchant/cliente)
Wallet	Software add-on del browser che effettua la codifica/decodifica delle informazioni da scambiare nella transazione

Tabella 1.1: Attori nel commercio elettronico

In questa tabella vengono elencati gli attori del commercio elettronico, tra questi figurano: il Merchant, il Merchant system, il Payment Gateway, i certificati digitali e il Wallet.

### 1.3 Problematiche del commercio elettronico

Il successo del commercio elettronico è strettamente collegato alla possibilità di effettuare transazioni sicure sulla rete. Questo comporta maggiore fiducia del consumatore finale. Il principale ostacolo per la crescita del commercio elettronico è, quindi, rappresentato dalla diffidenza e dalla mancanza di sicurezza che gli utenti hanno nei confronti del commercio elettronico.

Questa diffidenza è dovuta a vari aspetti:

- Diffidenza verso le varie forme di pagamento online.
- Timore che il prodotto acquistato non sia conforme a quello che ci si aspettava.
- Sfiducia nei confronti del venditore (solitamente avviene per le compravendite tra privati)

La perplessità principale da sfatare sembra essere quella della sicurezza nei pagamenti - è rischioso pagare online? - la risposta sembra essere di no, tuttavia i rischi ci sono comunque, gli stessi rischi che si affrontano acquistando offline, nella vita di tutti i giorni: i malintenzionati esistono tanto nel web quanto per strada.

Un'altra delle principali problematiche connesse al commercio elettronico è quella relativa alla tutela della privacy delle parti coinvolte nei pagamenti online, nonché della sicurezza dei dati personali richiesti al fine di eseguire le varie operazioni negoziali e, più in generale, dei dati che viaggiano sulla rete. La regolamentazione dei rapporti che intercorrono tra gli operatori delle reti telematiche nel

momento della loro utilizzazione è un punto fondamentale per uno sviluppo equilibrato del settore. Occorre, poi, tener presente che Internet non ha solo una dimensione visibile. Esiste, infatti, anche un gran numero di trattamenti che avvengono del tutto all'insaputa dell'individuo. Si pensi, ad esempio, ai problemi connessi all'utilizzo dei cookie [2]. I cookie HTTP [3] (più comunemente denominati Web cookies, tracking cookies o semplicemente cookie) sono frammenti di testo inviati da un server ad un Web client (di solito un browser) e poi rimandati indietro dal client al server - senza subire modifiche - ogni volta che il client accede allo stesso server. I cookie HTTP sono usati per eseguire autenticazioni e tracking di sessioni e memorizzare informazioni specifiche riguardanti gli utenti che accedono al server, come ad esempio i siti preferiti o, in caso di acquisti on-line, il contenuto dei loro "carrelli della spesa" (shopping cart). Il termine "cookie" - letteralmente "biscotto" - deriva da magic cookie, concetto ben noto in ambiente UNIX che ha ispirato sia l'idea che il nome dei cookie HTTP.

In generale, tutte le attività svolte su internet possono essere facilmente “spiate” attraverso l’utilizzo di software: i web bug (cimici web), etichette elettroniche che aiutano i siti web e le imprese di pubblicità a tracciare gli spostamenti dei visitatori della rete e che spesso si nascondono all’interno di banner pubblicitari; gli spyware, programmi in grado di raccogliere dati ed inviarli al produttore del software oppure a società che si occupano di telemarketing (generalmente informazioni relative a tipologie e licenze del software installato); la cosiddetta Persistence Internet Explorer, tecnologia pensata per ridurre le comunicazioni tra sito web e browser agevolando la navigazione all’utente ed alleggerendo il carico di lavoro del server web ma che fanno ciò archiviando le ricerche effettuate dall’utente sui motori di ricerca; gli adware (software advertising supported), software gratuiti in cui sono inserite pubblicità, di solito banner, che rallentano la navigazione.

Quali sono le motivazioni che rallentano gli acquisti online nel nostro paese? Dalle ricerche effettuate da istituti economici italiani, i dati rilevati dalle motivazioni si possono riassumere in tabella 1.2:

Motivazione	Percentuale
E’ troppo complicato	5%
E’ più veloce acquistare in negozio	9%
Non è sicuro	19%
E’ difficile verificare la qualità	7%
Non sono a mio agio	7%
Non sono titolare di carta di credito	7%
Preferisco il rapporto face-to-face	16%
E’ difficile trovare siti di mio interesse	2%
I siti non vendono online	2%
Non trovo nulla di mio interesse	24%
E’ difficile avere assistenza	2%

Tabella 1.2: Motivazioni scarso successo dell’e-commerce  
 fonte: Osservatorio e-commerce SDA Bocconi

## 1.4 Le varie forme di Commercio Elettronico

In base al fatto che la transazione coinvolga aziende piuttosto che singoli individui, si possono distinguere quattro forme di commercio elettronico: business to business, business to consumer, consumer to consumer e consumer to business. Il maggiore volume d'affari è prodotto dal business-to-business, il primo ad essere nato, ma anche il business-to-consumer sta prendendo piede.

La creazione delle aste on line ha generato due nuovi termini: consumer-to-consumer e consumer-to-business.

Cerchiamo di analizzare le quattro forme più nel dettaglio, partendo da quella più matura:

### 1.4.1 Business-to-business (B2B)

Business to Business, molto spesso indicato con l'acronico B2B, è un termine comunemente usato per descrivere le attività di compravendita tra aziende. Il commercio business to business riguarda tutte le transazioni commerciali che intercorrono tra due aziende, quindi è solitamente caratterizzato fra aziende che acquistano beni e servizi da altre aziende per la produzione di altri beni e servizi da trasferire a terzi.

La maggior parte delle transazioni avviene online, solitamente vengono acquistate grandi quantità di beni e gli importi sono mediamente elevati.

Oltre alla possibilità di risparmiare denaro, la migliore caratteristica del B2B è la possibilità di risparmiare tempo, ciò significa maggiore velocità nella vendita, rapido accesso ai nuovi fornitori e acquirenti e una nuova e più facile entrata nei mercati. Una nuova frontiera del B2B, è il B2B online, in particolare alcuni siti statunitensi gestiscono aste online, dove vengono commercializzati surplus di prodotti messi a disposizione dalle aziende.

### 1.4.2 Business-to-consumer (B2C)

Business to Consumer, spesso abbreviato in B2C, è quella forma di commercio che riguarda le transazioni commerciali tra l'azienda e il consumatore. E' un modello che si è sviluppato soprattutto grazie alla diffusione di Internet negli uffici, nelle case e nelle scuole.

Il principale fattore di successo del B2C è che attraverso la rete, i consumatori sono entrati in contatto con aziende, fino a quel momento irraggiungibili, stando comodamente seduti davanti al pc.

Amazon<sup>1</sup>, una compagnia di commercio elettronico statunitense, è stata la prima a vendere merci su Internet, è il tipico esempio, nonché il primo caso di maggiore successo nel marketing B2C. Amazon.com iniziò come libreria online, sebbene presto allargò la gamma di prodotti venduti a DVD, CD musicali, software, videogiochi ecc.

### 1.4.3 Consumer-to-consumer (C2C)

La forma più recente di commercio elettronico è la C2C (Consumer to Consumer); diventata popolare negli ultimi anni grazie ai numerosi siti che gestiscono aste online, e che quindi, permettono a semplici consumatori di contattarsi tra loro e vendere direttamente o tramite il supporto di aste online vari prodotti.

Le modalità di vendita sono stabilite dall'acquirente e dal venditore, solitamente viene venduto un oggetto per volta e gli importi sono mediamente contenuti.

Il sito di aste online per eccellenza è eBay<sup>2</sup> che, oltre ad affermarsi come brand, è una delle poche società leader in Internet ad ottenere un profitto economico. Questo profitto deriva da una tariffa applicata alle compravendite, varia tra l'1,5% e il 5% del prezzo di vendita finale, quindi più alto è il valore di vendita dell'articolo, maggiore sarà il guadagno per eBay.

---

<sup>1</sup>www.amazon.com

<sup>2</sup>www.ebay.com

La strategia di eBay è quindi lasciar fare agli utenti gran parte del lavoro, investendo quindi un capitale esiguo; deve gestire un'infrastruttura web, ma non deve tenere quindi, un inventario, spedire prodotti o trasferire pagamenti, sono gli utenti a fare tutto.

#### **1.4.4 Consumer-to-business (C2B)**

E' una forma di commercio elettronico non ancora sviluppato. La principale caratteristica sta nel fatto che sono i consumatori finali a fare il prezzo, ovvero comunicano all'azienda l'importo che sono disposti a pagare, e l'azienda in seguito decide se accettare o meno l'offerta.

L'esempio più classico è quello di priceline.com, in questo sito i clienti propongono un prezzo per il biglietto aereo che intendono acquistare. Il meccanismo funziona in questo modo: il potenziale cliente sceglie su priceline una destinazione, una data, quant'è disposto a spendere e, come garanzia, il numero di carta di credito. Priceline non fa altro che agire da intermediario e smista le richieste alle linee aeree con cui è in contatto. Se una di loro è interessata a vendere quel viaggio, si conclude la transazione e priceline ne ricava una percentuale.

Il vantaggio per i consumatori è che riescono ad acquistare a prezzi vantaggiosi, per le compagnie aeree invece, il vantaggio consiste nel riempire i voli, dato che ogni posto vuoto comporterebbe una perdita.

## Capitolo 2

# Tipologie di metodi di pagamento online

### 2.1 Introduzione

Il commercio online deve il suo sviluppo all'implementazione di nuovi sistemi di pagamento che determinano il passaggio dalla banconota al contante digitale. Questo fenomeno estremizza una delle caratteristiche di Internet, cioè la dematerializzazione degli strumenti reali e giuridici di cui l'uomo si serve nella vita quotidiana [4].

Negli ultimi anni sono stati creati numerosi strumenti per i pagamenti in Internet. Molti di questi richiedono l'intervento di una terza parte che funga da intermediario della transazione. A seconda del tipo di strumento utilizzato, l'intermediario può risultare legato da un rapporto contrattuale al compratore, al venditore o ad entrambi [5]. I fondamentali vantaggi connessi all'utilizzo dei metodi di pagamento online sono rappresentati dalla convenienza e dall'efficienza degli stessi, e dal fatto che le due controparti non debbano incontrarsi di persona per trattare. Alcuni di questi impongono una commissione comparabile a quella che viene addebitata con l'utiliz-

zo delle carte di credito, ma altri sono meno costosi, quando non completamente gratuiti; un venditore che desideri accettare i pagamenti con carte di credito (vedi sezione 2.2) sarà anche tenuto a sopportare notevoli costi sia iniziali che periodici. I costi generici da sostenere per le transazioni mediante carta di credito sono relativamente bassi, ma per i venditori con un basso volume d'affari questi possono apparire proibitivi. Poiché i pagamenti online restano per molti aspetti non disciplinati, assistiamo ad una sorta di contrattualizzazione dei diritti di compratori e venditori [6]. Le modalità di pagamento utilizzabili nella rete sono sostanzialmente suddivisibili in tre gruppi [7]: credit-based, debit-based e token-based.

Innanzitutto, lo strumento sicuramente più utilizzato è rappresentato dalle transazioni che avvengono attraverso l'invio dei dati della carta di credito (i cosiddetti sistemi credit based). A dispetto dei tanti dubbi esistenti sulla sicurezza degli acquisti online, le carte di credito coprono, secondo gli ultimi dati, l'88% della spesa virtuale mondiale, assicurando un importantissimo beneficio all'e-commerce. Il sistema su cui si basa tale tipo di pagamento è semplice da descrivere: il compratore, dopo aver concluso il contratto online, digita sul proprio computer i dati della sua carta di credito, che vengono criptati ed inviati al venditore. A seguito di tale invio, il venditore chiederà l'autorizzazione alla propria banca, la quale attraverso il controllo e la verifica dei dati in questione, darà il via all'operazione. I rischi per l'acquirente sono legati alla sicurezza dei dati che viaggiano sulla rete e alla possibilità che questi vengano intercettati e clonati abusivamente da terzi. Il venditore, dal canto suo, non avendo elementi certi sull'identità e sulla reale solvibilità del compratore, corre il rischio di vedersi costretto a restituire l'importo ricevuto, qualora il cliente neghi, in seguito, di aver autorizzato il pagamento. Di particolare importanza in questo ambito è quindi, l'adozione di sistemi di sicurezza avanzati che garantiscono l'identità

del codice della carta digitato.

Esistono poi, i cosiddetti sistemi debit based che si fondano su meccanismi tipici del sistema bancario. Qui il cliente, dopo aver stipulato una convenzione con una banca ed aver quindi aperto un conto corrente, emette a favore del venditore un assegno che viene convalidato dall'istituto di credito. Il funzionamento in breve è questo: l'acquirente apre un conto corrente online; la banca autorizza l'utente ad installare nel proprio hard disk una sorta di libretto di assegni digitale; al momento della transazione l'acquirente appone all'assegno la propria firma digitale e lo spedisce al venditore che infine, si rivolge alla banca emittente per incassare la somma.

Troviamo da ultimo, il cosiddetto sistema token based: si tratta di un metodo che, come gli altri, completamente svincolato dalla fisicità ma con rischiosi aspetti di incontrollabilità. La moneta elettronica (in senso stretto, anche detta e-cash) è un valore monetario rappresentato da un credito nei confronti dell'emittente, memorizzato su un dispositivo elettronico dietro ricezione di fondi il cui valore non sia inferiore al valore monetario emesso, accettato come mezzo di pagamento da imprese diverse dall'emittente. L'introduzione di un mezzo di pagamento assimilabile al contante ripropone la questione relativa all'identificazione della moneta rilevante ex art. 1277 c.c. ai fini dell'adempimento delle obbligazioni pecuniarie<sup>1</sup>. Per altro verso, la circolazione di moneta non emessa dalla banca centrale, solleva delicate questioni di politica monetaria e di vigilanza.

Si assiste infine, alla diffusione di un supporto per i pagamenti che offre notevoli vantaggi per la garanzia dell'anonimato e della sicurezza: le smart card.

---

<sup>1</sup>Problema che appare, oramai, superato dalla Direttiva 2000/46/CE

Queste rappresentano, in sostanza, un'evoluzione delle tradizionali carte di pagamento prepagate: a differenza di queste ultime, che consistono di un supporto laminato su cui è installata una banda magnetica contenente un numero limitato di informazioni, le smart card contengono al loro interno un microprocessore che permette alla carta di memorizzare una quantità notevolmente superiore a quella di una normale carta a banda magnetica [8]. Queste particolari carte si suddividono in due tipi: monouso, che consentono di effettuare pagamenti nei confronti di un unico soggetto, che spesso coincide con l'emittente; multiuso, che consentono di effettuare pagamenti presso un numero più o meno ampio di esercenti convenzionati. Da quando nel 1989 l'ISO (International standard organization) ha diffuso il documento 7816 (valido in tutto il mondo) riguardante le specifiche tecniche ed il protocollo di comunicazione delle smart card, ufficialmente queste sono state riconosciute e universalmente definite tanto da far ormai parte della nostra quotidianità. L'implementazione di questo tipo di carte per i pagamenti online ha garantito un salto di qualità nello sviluppo dell'e-commerce grazie alla loro relativa sicurezza ed agli esigui rischi derivanti da un'illecita clonazione della carte [9].

## 2.2 Carta di credito

L'uomo ha sempre cercato uno strumento attraverso il quale poter effettuare scambi di beni. Con il passare del tempo si è avvertita l'esigenza di uno strumento più pratico e leggero rispetto al denaro contante o ad un libretto di assegni. In seguito alle guerre del secolo scorso ed alle relative svalutazioni monetarie, si avverte l'esigenza di creare un nuovo sistema di pagamento che coniughi la praticità, la garanzia e l'immediatezza del riscontro da parte del cedente e dell'accettante.

Proprio in questo periodo, dopo la seconda guerra mondiale, le banche cominciano a progettare delle carte di pagamento: personali, garantite, pratiche, che permettono all'utilizzatore di effettuare transazioni senza avere con sé del denaro contante. La prima carta di credito nacque nel 1950 negli Stati Uniti per pagare al ristorante. L'intero sistema di pagamento tramite carta di credito si è sviluppato in quarant'anni, anche se ha assunto forme e modalità a cui siamo abituati noi, solo negli ultimi venti anni.

Furono l'American Express e la Bank of America le prime ad investire ed a credere in questo rivoluzionario sistema di pagamento. Bank of America lancia la sua prima carta di pagamento nel 1958, il cui utilizzo è limitato alla California. Non è un caso che le carte di pagamento trovino la loro genesi in un contesto economico vivace, con enormi potenzialità, ed in costante sviluppo come si presenta la California negli anni '50: un ambito in cui si incrociano tutte le esigenze a cui le carte di credito vanno incontro. Prima fra tutte l'impossibilità e la limitata sicurezza di trasportare e far circolare ingenti somme di denaro. In seconda battuta la necessità di concludere affari e transazioni in tempo reale, in un'economia in cui è necessario approfittare anche del momento per realizzare guadagni e cogliere occasioni.

Dieci anni più tardi, frutto del commercio, quattro banche della California entrano in competizione con la Bank of America fondando il circuito MasterCharge.

La grande diffusione delle carte di credito negli Usa arriva però negli anni '60 e '70, quando cioè tali strumenti cominciano a giocare un ruolo di fondamentale importanza anche nel settore dei servizi. Ciò, oltre a provocare un repentino aumento delle transazioni effettuate mediante le carte di pagamento, coinvolge nell'utilizzo delle stesse non più solo i ceti alti della grande industria e del commercio, ma anche il ceto medio.

Alla fine degli anni '70 la maggior parte delle carte di credito create e rimaste fino ad allora indipendenti vengono inglobate nei due circuiti principali. Nel 1970 viene fondata la National BankAmericard Corporation (NABANCO), che riunisce Bank of America ed altre banche che emettono carte di pagamento su sua licenza, per fornire ai soci vari servizi tra cui l'autorizzazione, la compensazione e il controllo delle frodi.

Nel 1974 viene fondata un'organizzazione internazionale, la International BankAmericard Corporation (IBANCO), per creare ed appoggiare un programma mondiale di carte bancarie. Vengono lanciate negli Stati Uniti e in altri 15 paesi, le carte BankAmericard blu, bianche e oro. Nel 1977 NABANCO diventa Visa USA e IBANCO diventa Visa International, e gli istituti finanziari soci iniziano ad emettere le prime carte Visa.

Contemporaneamente la strada dell'internazionalizzazione viene imboccata anche dal circuito MasterCharge che modifica il suo nome in MasterCard. E' questo il periodo della svolta anche da un punto di vista tecnologico: sulle carte viene apposta una banda magnetica, che ne aumenta esponenzialmente la rapidità e facilità di riconoscimento e di accettazione della parte dell'esercente. Al giorno d'oggi la carta di credito è uno strumento di pagamento, costituito da

una carta plastificata con dispositivo per il riconoscimento dei dati identificativi del titolare e dell'istituto bancario o finanziario dell'emittente. Le sue dimensioni sono definite nello standard ISO/IEC 7810 ID01: 85,60 x 53,98 mm ed uno spessore di 0,76 mm.

Il primo dispositivo applicato sulla carta è, come abbiamo già detto, una banda magnetica; per far fronte ai bisogni crescenti di sicurezza e all'avanzare del fenomeno delle frodi, dal 1993 è stato applicato alla carta anche un microchip, rendendola una smart card. Rispetto alle carte con la sola banda magnetica, che non possono conservare i dati relativi al proprietario della carta in modo sicuro e hanno una capacità di memoria limitata, le smart card memorizzano le informazioni in modo sicuro per poi utilizzarle durante la transazione. Grazie ad una maggiore capacità di memoria e al microprocessore interno, le smart card possono essere utilizzate per accedere a più servizi, potendo essere memorizzati sulla stessa carta un maggior numero di dati (identificativi, di accesso, concorsi a punti ecc.); questa caratteristica propria della smart card è chiamata "multi-applicazione". Invece, le carte con la sola banda magnetica, permettono in genere solo una o due funzioni di pagamento, quali l'accesso diretto al conto (carta di debito, bancomat) e/o l'accesso ad una linea di credito (carta di credito).

La carta di credito viene rilasciata da una banca o da un ente finanziario presso il quale un cliente detiene un conto corrente. L'utilizzo della disponibilità della carta varia quindi in funzione dell'affidabilità del cliente stesso.

Il sistema di funzionamento delle carte di credito è un processo di autorizzazione del sistema bancario. Questo processo si articola in tre soggetti:

- Ente emittente (issuer): è l'azienda che provvede ad emettere la carta di credito. Questa può essere una banca oppure un ente finanziario. L'azienda emittente definisce un contratto di finanziamento con il titolare della carta. I titolari di carta sono considerati clienti della società emittente e sono coloro che spendono denaro attraverso l'utilizzo della carta.
- Ente esercente (merchant): è l'esercizio commerciale che, aderendo ad un circuito di pagamento, permette ai propri clienti di pagare attraverso il mezzo di pagamento convenzionato, alternativo al contante. L'adesione al circuito avviene solitamente tramite l'intermediazione di una società di gestione terminali (acquirer) che offre servizi di vendita o noleggio POS (Point of Sale), contabilizzazione e rendicontazione dei pagamenti, reportistica e gestione delle controversie (solitamente definite dispute), comunicazione e flussi informativi da e verso i circuiti stessi.
- Circuito di pagamento: è l'azienda che si occupa di veicolare, attraverso una rete di comunicazione, le richieste e le corrispondenti autorizzazioni alla spesa. La rete del circuito si allarga attraverso l'installazione dei POS, rappresentabili come terminazioni della rete, presso nuovi esercenti. Il circuito si occupa anche delle operazioni di settlement, cioè di contabilizzazione e pareggio delle partite contabili sulle posizioni dei singoli titolari ed esercenti. I principali circuiti mondiali sono Visa, MasterCard, Diners, American Express, JCB e China Union Pay (CUP).

La carta di credito è uno strumento che consente di regolare il pagamento successivamente all'acquisto. Sulla carta sono riportati le generalità del titolare, il numero della carta e la sua scadenza. Il titolare è tenuto a porre la propria firma nello spazio predisposto.

La transazione di vendita coinvolge tre attori con i rispettivi rapporti, ovvero:

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

L'utilizzo è molto semplice (vedi figura 2.1): l'utente sceglie un prodotto sul sito web del venditore (1), al momento del pagamento il sito del merchant richiede alla banca (del merchant) un gateway per il pagamento (2), nel quale sono inseriti i dati da comunicare alla banca (3), la quale provvederà ad incassare i soldi dalla banca dell'acquirente.

Quindi, il cliente può acquistare senza l'uso di contanti, il fornitore non è soggetto al rischio di un pagamento tramite assegno e quindi all'eventuale insolvenza dello stesso, e l'istituto eroga un servizio percependo per questo, una commissione. Oltre che come strumento di pagamento, la carta può essere utilizzata come strumento di prelievo allo sportello automatico (similmente ad una carta Bancomat) mediante il codice segreto consegnato insieme alla carta.

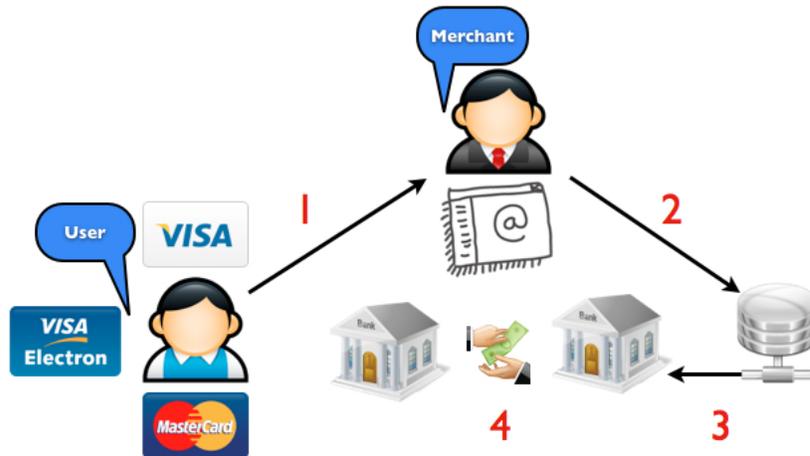


Figura 2.1: Funzionamento Carta di credito/Carta ricaricabile

## 2.3 Carte ricaricabili

Le carte di credito ricaricabili sono delle carte che possono essere acquistate come prodotto a se stante, senza la necessita che siano associate ad un conto corrente. Al momento della stipula del contratto, si carica la carta prepagata con l'importo desiderato; in seguito si potrà spendere tale importo effettuando acquisti sia online che nei negozi, per un importo mai superiore alla somma versata, la quale verrà scalata man mano che l'utente effettuerà pagamenti.

L'utente che acquista attraverso una carta prepagata, solitamente lo fa attraverso circuiti Visa o MasterCard, anche se ultimamente sta emergendo anche il circuito Visa Electron. Le carte di credito ricaricabili sono oggi utilizzate da moltissimi utenti come efficaci mezzi di pagamento sul web. Sono facili da usare ed offrono un'adeguata sicurezza.

Ci sono due categorie di carte prepagate: quelle che necessitano dell'abbinamento con un conto, e quelle per le quali, invece, non è necessario associare un deposito tradizionale. Di quest'ultime fanno parte anche delle carte prepagate che hanno un vero e proprio Iban dedicato che nel caso degli accrediti o degli ordini di pagamento, consentono di funzionare come un vero e proprio conto corrente.

Le carte di credito ricaricabili presentano numerosi vantaggi; come abbiamo detto possono essere del tutto indipendenti dal conto corrente, quindi l'utente non corre il rischio di vedersi il proprio conto corrente bancario prosciugato. Non prevedono alcun tasso di interesse verso la banca e possono essere possedute da chiunque, anche dai minorenni (viene spesso utilizzata da studenti fuori sede).

Sono semplicissime da ottenere, basta recarsi in banca o in posta per averne una, i costi di attivazione vanno dai €5,00 ad un massimo di €20,00, solitamente i costi di ricarica si aggirano tra 0 e €2,50 e i prelievi da €1,00 a €5,00 (solitamente per i prelievi dall'estero).

Il procedimento di acquisto risulta sicuro e la spesa è continuamente monitorabile in quanto il tetto della cifra disponibile è limitato dalla quantità di ricarica effettuata. Le carte prepagate, come già detto, sono la soluzione più appropriata per coloro che non possiedono un conto corrente bancario, infatti, proprio per questo motivo sono molto diffuse tra i più giovani, che costituiscono la quota più significativa del mercato online.

Da una ricerca effettuata dalla SSB[12](Società per o Servizi Bancari delle Banche Italiane), società leader nel mercato dei sistemi

di pagamento, si evince che i picchi più elevati relativi all'utilizzo e alle ricariche delle carte prepagate avviene nel periodo estivo, tradizionale momento di forte impatto dei giovani sul mercato[15].

Tuttavia, le carte ricaricabili presentano degli svantaggi, legati principalmente alla scomodità delle operazioni. Si tratta della ricarica, che viene fatta prevalentemente presso gli sportelli della banca emittitrice (ad eccezione delle carte legate al conto corrente, che possono essere ricaricate online). Bisogna quindi recarsi fisicamente lì per ricaricare la carta; inoltre per le ricariche, a volte, sono previsti dei costi leggermente alti, è quindi buona norma informarsi presso le banche prima di scegliere la carta più conveniente sotto questo aspetto[14].

Per quanto riguarda i servizi di protezione, non essendo una carta di credito vera e propria, essa non è tutelata come queste in caso di smarrimento o furto.

## 2.4 Paypal

Paypal è un sistema di pagamento online, comunemente utilizzato su eBay o presso numerosi negozi online. E' uno dei più diffusi sistemi di pagamento online ed è principalmente un metodo alternativo alla carta di credito.

Paypal è una società statunitense fondata a Palo Alto nel 1998 da Peter Thiel e Max Levchin, fa parte del gruppo eBay ed ha come sede la città di San Jose (California). Il boom di Paypal è avvenuto negli ultimi 5 anni, a seguito della sempre più ampia diffusione delle carte di credito e delle carte prepagate. Paypal è un ente che emette moneta elettronica online, attraverso il quale l'utente che si registra aprirà una sorta di conto corrente, nel quale si depositano soldi veri tramite una carta di credito; questo conto verrà usato per effettuare pagamenti verso/da altri utenti Paypal[16].

Aprire un conto Paypal è molto semplice, la registrazione è gratuita, basta fornire il proprio indirizzo e-mail, una password ed associare al proprio account una carta di credito, fino ad un massimo di otto, oppure una carta prepagata, oppure si può anche ricaricare senza spese dal proprio conto corrente bancario. Paypal accetta pagamenti in 24 valute.

Paypal ha 84 milioni di conti attivi ed è disponibile in 190 paesi e territori (dati al 31 Marzo 2010) [10]. Paypal non è una banca, perciò non offre le stesse garanzie legali di una banca. Formalmente è un "istituto per l'emissione di moneta elettronica".

E' possibile infatti spedire e ricevere denaro in tutta sicurezza non fornendo i numeri di carta di credito, basta l'indirizzo e-mail. Ricevere ed inviare pagamenti è molto semplice, colui che riceve denaro deve indicare il proprio indirizzo di posta a colui che effettua il pagamento, che invece dovrà recarsi nella propria pagina Paypal e indicare l'indirizzo dell'utente che riceverà il pagamento.

Con Paypal non solo si invia denaro in sicurezza, ma si gode anche

di una certa tutela nella transazione. Paypal infatti offre strumenti a difesa dell'acquisto fatto a garanzia del possibile recupero delle somme versate a causa di comportamenti fraudolenti. Naturalmente, il sito è affidato a connessioni sicure del tipo HTTPS (di cui parleremo nel capitolo 3) e il numero della carta di credito si specifica solo all'atto dell'iscrizione. Gli aspetti della sicurezza online sono molto curati, alla scelta della password di accesso viene data molta importanza in modo tale da evitare manomissioni, i responsabili per la sicurezza di Paypal, inoltre, invitano gli utenti con frequenti messaggi a cambiare spesso le proprie credenziali di accesso.

Gli stessi ideatori hanno persino previsto un sistema di affidabilità e reputazione sugli iscritti che vengono sovente invitati a controlli per accertarne l'indirizzo. Per ogni transazione Paypal impiega circa tre o quattro giorni per aggiornare il saldo della carta di credito. Ai clienti vengono offerti due programmi di protezione, un programma per chi acquista tramite Paypal oggetti su eBay, e un programma offerto per quei beni acquistati al di fuori di eBay.

Il secondo tipo di programma di tutela si applica solo in caso di reclami per oggetto non ricevuto. Il primo tipo di tutela, offre all'utente una protezione molto alta, infatti, prevede rimborsi anche nel caso in cui l'oggetto arrivi a destinazione, ma l'utente ritenga che non sia conforme alla descrizione. Un oggetto non conforme alla descrizione è sostanzialmente diverso dalla descrizione riportata nell'inserzione.

Ad esempio: l'oggetto ricevuto è completamente diverso, l'oggetto dichiarato nuovo è in realtà usato, l'oggetto non è originale, non vengono ricevute parti o caratteristiche importanti, l'utente ha ricevuto una quantità inferiore di oggetti rispetto alle quantità dichiarate nell'inserzione, l'oggetto risulta danneggiato durante la spedizione[11].

Se non è possibile risolvere la contestazione direttamente con il

venditore, l'utente dovrà aprire una contestazione entro 45 giorni. Se la contestazione non viene risolta, l'utente dovrà convertirla in reclamo entro 20 giorni dalla data della contestazione. L'utente dovrà attendere almeno 7 giorni dalla data del pagamento prima di convertire la contestazione in reclamo, a meno che l'importo non sia superiore di 2500 USD (o importo equivalente in un'altra valuta).

Nel caso in cui Paypal prenda in esame il reclamo, potrà richiedere all'utente di fornire documentazioni a sostegno della propria posizione. A questo punto, Paypal potrebbe richiedere all'utente di restituire l'oggetto al venditore, a Paypal o a terzi, a spese dell'acquirente. Una volta preso in considerazione il reclamo, Paypal prenderà la decisione finale a favore dell'acquirente o del venditore. La decisione finale a favore del cliente o del venditore è a completa discrezione di Paypal e viene presa in base a qualsiasi criterio appropriato da Paypal, questa decisione dovrà essere irrimediabilmente rispettata dagli utenti[11].

Infine, se Paypal accetta il reclamo, il venditore dovrà fornire per intero la somma pagata per quell'oggetto più le spese di spedizione pagate per rispedire l'oggetto al venditore. Il reclamo dei fondi tuttavia, non è garantito, infatti è limitato solo agli importi che Paypal recupera dal conto dei venditori. Sotto questo aspetto, Paypal si tutela bloccando sul conto del venditore, l'importo ricevuto per l'oggetto, non rendendo tale somma prelevabile. Questo blocco viene fatto solo agli utenti che hanno meno di 50 feedback[17]. L'importo viene sbloccato quindi, dopo 21 giorni, oppure quando l'acquirente rilascia un feedback positivo.

Il feedback è un meccanismo di scambio di valutazioni sulla transazione che avviene tra compratore e venditore. Ne esistono di 3 tipi: Positivo, transazione conclusa con successo, ognuno ha fatto il suo dovere; punto positivo Neutro, transazione non conclusa e rimborso da parte del venditore; negativo, mancato ricevimento della

merce, merce contraffatta e/o non corrispondente alla descrizione. I 2 punteggi attribuiti in base al tipo di feedback ricevuto determinano una percentuale (ad esempio se sono tutti positivi 100%) che a colpo d'occhio, permette subito di capire l'affidabilità del venditore. A partire dal 20 maggio 2008, i venditori possono rilasciare agli acquirenti solo feedback positivi (o non rilasciarne) in modo che gli acquirenti si sentano liberi di rilasciare giudizi oggettivi sull'esperienza d'acquisto senza temere feedback negativi di ritorsione da parte del venditore. D'altro canto verranno rimossi tutti i feedback negativi o neutri rilasciati da utenti, acquirenti o venditori, sospesi o che non hanno risposto alle controversie. Al raggiungimento di un determinato numero di feedback negativi eBay può decidere la sospensione, il blocco o la chiusura definitiva dell'account del venditore. Il meccanismo dei feedback può essere travisato da utenti che dispongono di più account o si accordano con altri, e simulano delle finte vendite di oggetti (a sé stessi o a terzi) per scambiarsi e aumentare rapidamente il proprio numero di feedback. L'unica verifica sui dati di iscrizione, che sarebbe a garanzia dell'univocità dell'account (una persona=un account), consiste nel calcolo del codice fiscale, facilmente falsificabile con i programmi disponibili in rete.

Utilizzare Paypal è abbastanza intuitivo (vedi figura 2.2): l'utente carica il conto Paypal con una delle sue carte di credito o direttamente dal conto corrente bancario (1), sceglie sul sito del venditore quale prodotto acquistare (2), inserisce nel sito paypal.com l'indirizzo e-mail e l'importo da pagare (3), Paypal verifica la disponibilità finanziaria dell'utente, se ci sono abbastanza fondi addebita l'importo nel conto Paypal dell'acquirente e lo accredita in quello del merchant.

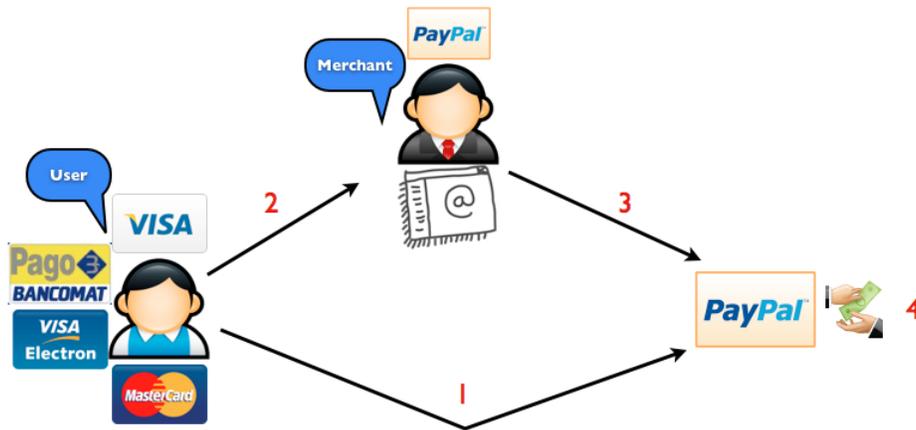


Figura 2.2: Funzionamento Paypal

Ultima cosa da dire è che Paypal, non è la soluzione ai problemi di sicurezza su Internet, in primo luogo perché non è un sistema universalmente accettato, non riceve le stesse forme di tutela che hanno tutte le banche, e poi ricevere denaro ha un costo a percentuale fissa che va dall'1,8% al 3,4% (tabella 2.1) in base agli importi dei pagamenti, per cui il sito non è affatto gratuito.

Pagamenti ricevuti (al mese)	Tariffa per transazione
€0,00 - €2.500,00 EUR	3,4% + €0,35 EUR
€2.500,01 EUR - €10.000,00 EUR	2,7% + €0,35 EUR
€10.000,01 EUR - € 100.000,00 EUR	2,2% + €0,35 EUR
>€100.000,00 EUR	1,8% + €0,35 EUR

Tabella 2.1: Tariffe transazioni Paypal

## 2.5 BankPass Web (“pagamentionline” Si-servizi)

Dal 31/12/2009 BankPass web non è più utilizzabile, ma non totalmente, tra le principali novità c'è la sospensione per i pagamenti con PagoBANCOMAT, ma continua ad essere erogata la soluzione POS virtuale con operatività inalterata per quanto riguarda i pagamenti con carte di credito. Cambiano quindi, nome, logo e soggetto erogatore del servizio che passerà interamente a Si-servizi del gruppo Cartasì e il nome del prodotto sarà “pagamentionline”.

Questo servizio consente al cliente di effettuare acquisti online in massima sicurezza. E' uno strumento di pagamento messo a punto dal circuito interbancario SSB[12] (Società per i Servizi Bancari delle Banche Italiane, è una società interamente ad azionariato bancario nata per sviluppare e gestire servizi informatici per le Banche, fra i principali servizi gestiti da SSB sono i prelievi con carte Bancomat in circolarità e i pagamenti su POS), e viene fornito da un circuito di istituti di credito aderenti all'iniziativa. Per aderire al servizio è necessario sottoscrivere un contratto di adesione presso una banca aderente al servizio.

Una volta sottoscritto il contratto si può creare un “portafoglio virtuale” detto anche wallet. Al wallet si possono associare più di una carta di credito. Quando si deciderà di pagare online con questo circuito, l'utente sceglierà con quale carta effettuare il pagamento.

Al momento di effettuare il pagamento online, il cliente convenzionato al servizio dovrà semplicemente accedere al suo wallet, tramite il sito [www.sis-bankpass.it](http://www.sis-bankpass.it), inserendo la suo “user id” e la sua “password”; per ogni transazione effettuata attraverso il wallet verrà ricevuta una mail di conferma. La procedura restituisce immediatamente un numero ed una scadenza virtuali, utilizzabili esclusivamente per la transazione indicata dal cliente, gli importi vengono addebitati con i tempi, le modalità e le condizioni previste dalla banca.

Quando un consumatore deve effettuare un pagamento presso un esercente non convenzionato al sistema, accede al sito *sis-bankpass*, e, attraverso il proprio wallet genera un PAN virtuale (con scadenza e CVC2/CVV2) che ha validità limitata a quella determinata transazione. Il PAN virtuale è appunto, un numero di carta di credito virtuale, da utilizzare al posto del vero numero della carta di credito per pagare in piena sicurezza anche presso esercenti non aderenti. Nessun istituto in particolare gestisce questo sistema di pagamento online; i sistemi di pagamento come *sis-bankpass* sono procedure dell'intero sistema bancario ed operano con modalità uniformi e standard. In generale le procedure di pagamento vengono elaborate in gruppi di lavoro presso la CIPA (Convenzione Interbancaria per i Problemi dell'Automazione) o presso l'ABI (Associazione Bancaria Italiana), con la partecipazione di rappresentanti delle banche e dei centri applicativi della RNI (Rete Nazionale Interbancaria).

In questi gruppi di lavoro vengono stabilite sia le regole di scambio e trattamento dei flussi tra banche, sia i protocolli di comunicazione che vengono adottati da tutte le banche. Tra i principali rischi va tenuto presente che: il cliente è tenuto ad utilizzare e custodire con la massima cura la user id e la password di accesso al servizio evitando in modo assoluto la divulgazione a terzi. Il cliente è responsabile di ogni conseguenza dannosa che possa derivare dall'abuso o dall'uso illecito di esse; le operazioni di pagamento tramite *sis-bankpass* devono essere considerate a tutti gli effetti indipendenti dalla merce e/o dai servizi acquistati. Come tale la banca non è responsabile per eventuali contestazioni in merito a quanto acquistato e non potrà procedere con storni addebitati al cliente.

La figura 2.3 mostra il funzionamento di pagamento online di Si-Servizi: l'acquirente si iscrive al sito Si-Servizi e crea un wallet digitale nel quale iscriverà una o più carte di credito (1), successivamente sceglierà un prodotto dal sito del merchant (2) che dovrà essere tassativamente iscritto al circuito di pagamenti di Si-Servizi, l'operazione verrà poi presa in considerazione dal circuito Si-Servizi (3), la quale si occuperà della transazione di denaro addebitando l'importo nel wallet del compratore.

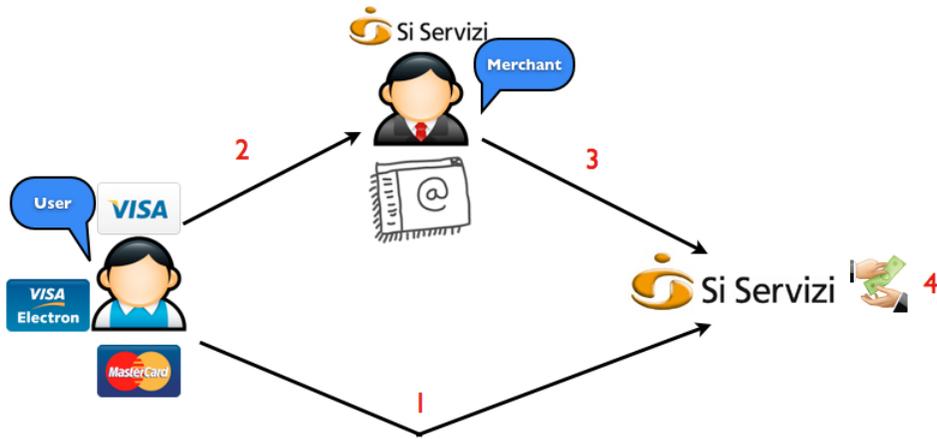


Figura 2.3: Funzionamento Sis-Bankpass

Le condizioni economiche, per l'apertura e la tenuta di sis-bankpass, non sono tuttavia, delle migliori. Infatti, i costi d'attivazione e di tenuta annua per ogni singolo wallet sono entrambe di €10,00 a cui si aggiungono spese di ricerca e copia documentazione di €7,00 e spese di informativa precontrattuale di €10,00.

## 2.6 Bonifico bancario online

Il bonifico è un'operazione che permette di trasferire denaro da una persona fisica o giuridica (ordinante) ad un'altra (beneficiario). Il bonifico bancario online è attualmente il modo più sicuro e flessibile per far circolare elettronicamente addebiti ed accrediti. All'utente non è richiesta alcuna firma, nè tantomeno nessun assegno o modulo da compilare in forma cartacea, gli importi tendono a circolare meno rapidamente rispetto alle soluzioni tradizionali (carte di credito o denaro contante), ma certamente in modalità più sicure. Questo sistema di pagamento può essere effettuato da una qualsiasi banca, ed è particolarmente conveniente se l'utente ordinante o beneficiario ha già un conto corrente aperto presso una banca. La ricezione di questo tipo di pagamento è generalmente di 3-4 giorni lavorativi. Il costo di un bonifico varia dai €0,50 a €6,00, ed è funzione in genere della tipologia di conto corrente e convenzioni che si hanno con la banca.

Il trasferimento dei fondi può avvenire principalmente in due modi, il primo è addebitando ed accreditando direttamente dai conti correnti delle rispettive controparti, l'altro metodo è recarsi personalmente allo sportello e depositare il corrispettivo in contanti presso la banca ricevente.

E' un metodo raccomandabile per importi elevati di pagamento e, grazie alla possibilità di inserire la causale di pagamento non ci sono di solito problemi nel riconoscimento da parte del venditore del pagamento che riceve.

Quando si paga con questo metodo, è importante inserire nella causale di pagamento sempre il numero dell'asta (se si acquista su eBay), e il nome utente, oppure il codice dell'ordine se si acquista da un negozio online. Queste informazioni aiuteranno il venditore a rintracciare subito la transazione e quindi potrà provvedere subito alla spedizione della merce ordinata.

Se il pagamento viene effettuato da un'altra persona è sempre consigliabile informare il venditore comunicando il nominativo della persona che ha effettuato il pagamento.

Per eseguire un bonifico bancario, fino al 1 Gennaio 2008 era necessario indicare le coordinate bancarie ABI, CAB, CIN e numero di conto corrente del destinatario; dopo tale data, per inviare un bonifico ad un destinatario si è reso obbligatorio l'uso dell'IBAN<sup>2</sup>, ossia un codice composto da 27 cifre che identifica univocamente il nostro conto corrente dagli altri, al posto delle coordinate bancarie.

Il codice IBAN viene fornito al cliente all'atto dell'apertura di un nuovo conto corrente. Questo dato, insieme al nome dell'intestatario del conto corrente, è sufficiente per ricevere l'accredito generalmente in pochi giorni lavorativi, salvo errori nella compilazione.

Ogni bonifico bancario è identificato univocamente tramite un numero di 11 cifre chiamato CRO<sup>3</sup>. Tale codice viene rilasciato dalla banca al momento dell'avvenuto pagamento tramite bonifico, e consente al destinatario di verificare la corretta ricezione del pagamento presso la sua banca. Effettuare un bonifico bancario online è molto semplice. La banca online offre una particolare sezione nel proprio sito web nella quale l'utente riesce ad accedere ai propri dati personali per effettuare qualsiasi tipo di interrogazione o per inoltrare la richiesta di bonifico. L'utente in questo caso compila un form molto simile al rispettivo cartaceo che viene compilato quando ci si reca fisicamente alla propria banca, con il nome del beneficiario, il suo codice IBAN e la causale di trasferimento.

Il bonifico può essere infine, ordinario, ovvero di un importo non rilevante e non urgente, oppure urgente e/o di importo rilevante. In quest'ultimo caso il perfezionamento del pagamento avviene attraverso circuiti interbancari dedicati, che consentono la ricezione in

---

<sup>2</sup>International Bank Account Number

<sup>3</sup>Codice di Riferimento Operazione

tempi molto ridotti, stesso giorno o giorno lavorativo successivo, ma ovviamente, le commissioni saranno maggiorate.

Non conviene utilizzare un bonifico bancario quando non si è in possesso di un conto corrente bancario, di solito le spese di commissioni per coloro che richiedono un bonifico, non avendo un conto corrente bancario, sono relativamente elevate. In questo caso è consigliabile effettuare un pagamento su conto corrente postale o vaglia postale.

L'ordinante accede utilizzando il proprio IDpass e il proprio PIN alla pagina personale nel sito della propria banca (1), sceglierà la voce "bonifico bancario online", dopodichè si aprirà una pagina della quale inserire codice IBAN e nome e cognome del beneficiario (2). Fatto questo la banca trasferirà la somma desiderata nella banca del beneficiario applicando tariffe e tempi previsti dalla banca dell'ordinante (figura 2.4).

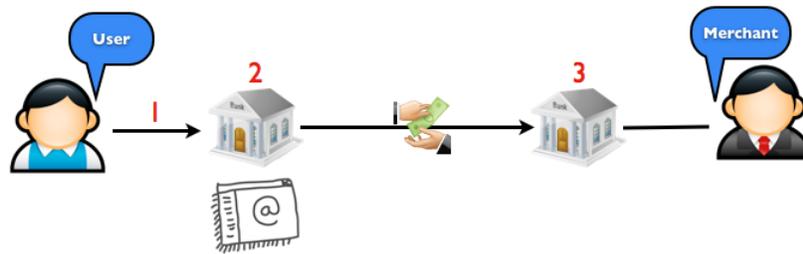


Figura 2.4: Funzionamento bonifico bancario online

## 2.7 Sistemi di pagamento emergenti

### 2.7.1 Square

Square è un nuovo metodo di pagamento realizzato per iPhone e iPad. Ideato dal fondatore di Twitter Jack Dorsey e Kevin Rose, questo servizio permette di eseguire pagamenti direttamente dal dispositivo Apple. Al momento questo servizio è disponibile esclusivamente negli Stati Uniti. Il funzionamento avviene tramite un piccolo accessorio hardware, cioè un lettore di carte di credito che potrà essere inserito nell'uscita jack del dispositivo Apple.

Questo lettore permetterà di processare le carte di credito e in seguito inserire l'importo, il codice di protezione e la firma direttamente sul display, tramite un'interfaccia abbastanza semplice e intuitiva.

Square sarà più economico dei tradizionali POS americani che richiedono 30 centesimi ed il 2,9% della transazione contro i 15 centesimi e 2,75% (vedi tabella 2.2) richiesti dall'utilizzo di Square; inoltre non è previsto un contratto, il venditore non deve fornirsi di un POS (solitamente acquistabile per una cifra tra i 150 e i 900 dollari), non sono previste spese di settaggio, nè varie tasse mensili che i tradizionali POS presentano.

Caratteristica	Square	Altri
Richiesta account commerciante	Non Prevista	Prevista
Contratto	Non Previsto	1-2 Anni
Lettore di Carte	Gratis	\$150-\$900
Setup	Gratis	\$0-\$50
Tasse mensili	Non Previste	\$15-\$25
Minimo mensile	Non Previsto	\$25
Card-present (swiped) rate	2.75% + 15¢	2.9% + 30¢
Card-not-present (keyed-in) rate	3.5% + 15¢	2.9% + 30¢

Tabella 2.2: Costi di Square

Questo nuovo metodo consentirebbe anche ai più piccoli negozi o liberi professionisti di poter far utilizzare la carta di credito come metodo di pagamento e con spese davvero minime.

Per accedere a tale servizio basterà registrarsi al sito SquareUp.com, così da ricevere l'accessorio che permetterà di leggere le carte di credito, l'utente inoltre durante la registrazione dovrà scattarsi una foto che verrà poi mostrata all' esercente al momento dell'acquisto tramite l'applicazione Square, anch'essa da scaricare dal sito precedentemente citato.

Al momento Square è ancora in via sperimentale, come abbiamo già detto, solo negli Stati Uniti: nel periodo di introduzione il sistema verrà utilizzato per effettuare micropagamenti inferiori ai 60 dollari. Al momento del pagamento l'utente striscerà la propria carta di credito nel lettore Square, dopo questa operazione sarà visualizzata la foto dell'utente sul dispositivo, il quale dovrà inserire il proprio codice personale e apporrà tramite il display multitouch Apple la propria firma.

L'applicazione consentirà di effettuare il pagamento se e solo se, entrambe le parti siano in possesso di un account Square, al termine dell'operazione verrà inviata una e-mail di riepilogo con tutti i dati della transazione.

Un sistema piuttosto semplice, che funziona grazie ad un jack audio ed un dispositivo di lettura e che sfruttando le caratteristiche di iPhone e iPad costituisce, senza dubbi, un passo avanti nel sistema dei pagamenti elettronici. Tuttavia, per essere pienamente adottato, richiede tempi lunghi: lo stesso Dorsey, realizzatore di Square, disponibile anche per i device Android, non ha ancora reso nota la data di lancio.

L'utente dovrà registrarsi a Square immettendo i propri dati e fornendo una foto per rendere più facile il riconoscimento (1). L'acquirente si recherà fisicamente presso il negozio del venditore (iscrit-

to a Square), al momento del pagamento dovrà strisciare la propria carta attraverso il dispositivo Square collegato all'iPhone/iPad del venditore(2), successivamente all'acquirente sarà chiesto di apporre la propria firma sul display multitouch Apple (3), che invierà i dati al server Square, il quale avrà il compito di addebitare l'importo sulla carta dell'acquirente (4) (figura 2.5).

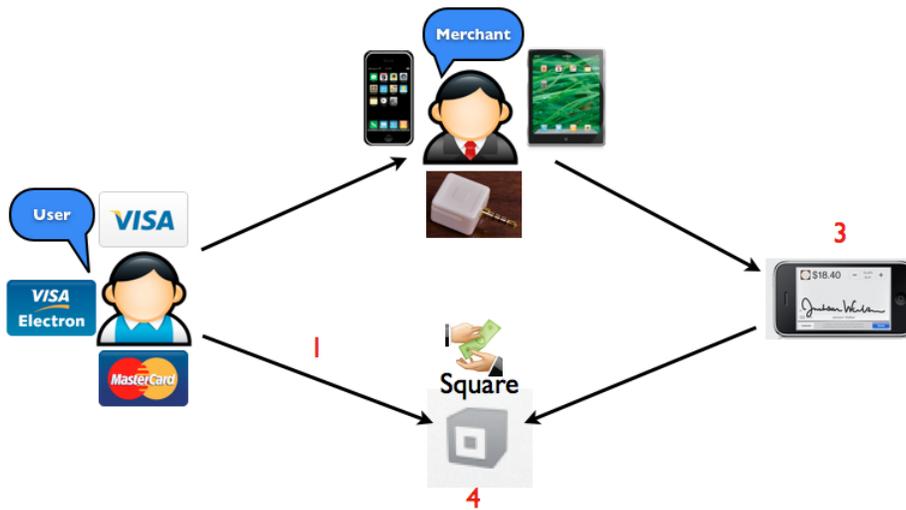


Figura 2.5: Funzionamento Square

### 2.7.2 Google Check-out

Google Check-out è un metodo di pagamento ideato da Google per rendere più facile e veloce lo shopping online. La caratteristica fondamentale di questo metodo di pagamento è che si può acquistare online con pochi e semplici passaggi.

Infatti, con Google Check-out si può evitare di compilare il tipico form che si presenta al momento dell'acquisto di un oggetto online. Google Check-out memorizza tutte le informazioni al momento della registrazione, basterà possedere un account Google, inserire nome, cognome, numero della carta di credito e nome del titolare, un numero di telefono e l'indirizzo per la spedizione.

Tutti i dati necessari per effettuare un acquisto online, con Google Check-out vengono digitati dall'utente una sola volta, nel momento della registrazione; questi dati, tra cui, quelli anagrafici e quelli relativi alla carta di credito (numero carta di credito, nome e cognome del titolare, scadenza e cvv), vengono in seguito ripresi nel momento in cui l'utente acquista un prodotto online, senza bisogno di doverli reinserire nuovamente.

Acquistare con Google Check-out è quindi molto semplice, basta infatti:

- Trovare un articolo che desideriamo acquistare da un negozio che accetta Google Check-out.
- Aggiungere l'articolo al carrello degli acquisti del negozio.
- Fare click sul pulsante Google Check-out e fare il log-in.
- Controllare i dettagli dell'ordine e fare click su "Emetti il tuo ordine ora".

A questo punto l'oggetto è stato acquistato in quattro semplici passaggi. Google Check-out è gratuito, si dovrà solo pagare per

l'acquisto effettuato, più, eventualmente le spese di spedizione; al momento della registrazione viene trattenuto 1 dollaro a titolo di autorizzazione che verrà riaccreditato dopo qualche giorno.

Attualmente Google Check-out non è tra i sistemi di pagamento più usati; il principale difetto è che, nonostante sia molto simile a Paypal, ma molto più giovane, non è molto diffuso, nonostante sia privo di costi, e quindi anche più conveniente del più anziano e celebre Paypal.

Il funzionamento di Google Check-out è molto semplice (vedi figura 2.6): l'acquirente dovrà registrare la propria carta di credito sul sito internet di Google Check-out (1), nel momento dell'acquisto sul sito del merchant gli basterà un click e il log-in in Google Check-out per acquistare il prodotto (2), dopodichè sarà Google Check-out ad addebitare l'importo sulla carta di credito dell'acquirente.

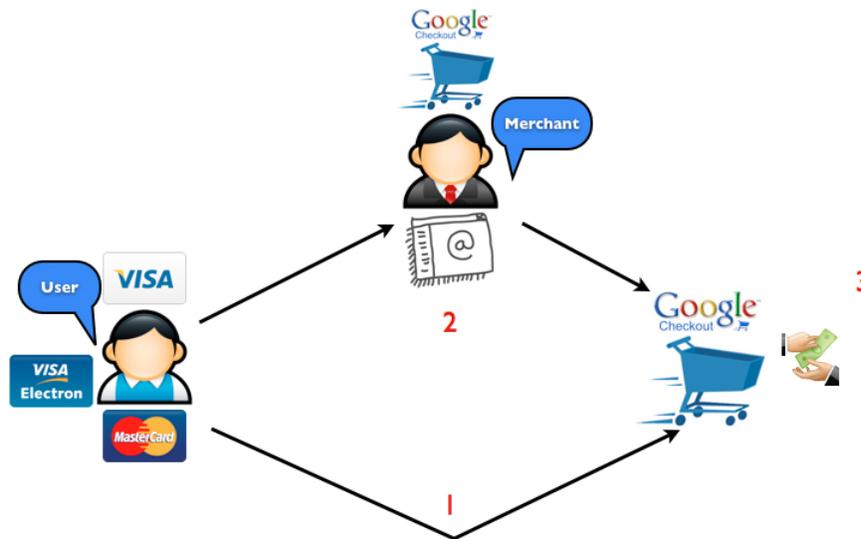


Figura 2.6: Funzionamento Google Check-out

## Capitolo 3

# Rischi e forme di sicurezza nei pagamenti online

### 3.1 I rischi

Acquistare online presenta dei rischi, legati alla possibilità che i dati forniti al momento del pagamento vengano intercettati da terze parti con scopi fraudolenti. Il sistema di pagamento maggiormente a rischio è la carta di credito, poichè, a differenza della carta di debito, il malfattore può effettuare pagamenti in rete e, usare un terminale in modo tale da essere meno esposto.

Questi rischi per gli utilizzatori di carte di credito (card holder), sono aumentati in questi ultimi anni grazie anche alla diffusione di pagamenti a distanza in modalità elettronica, all'incremento delle soluzioni e-commerce e alla maggiore diffusione delle carte di pagamento (sia di debito sia di credito). Dai dati resi noti dalla polizia postale relativi al periodo 2006-2007[18] emerge un netto calo delle frodi online rispetto agli anni precedenti. Gli utilizzi fraudolenti di carte di credito nel 2007 sono nettamente minori rispetto al 2006, dai 5208 ai 2730 del 2007. Tra il 2008 e il 2009 invece, le truffe hanno registrato un nuovo rialzo nel mercato italiano[19]. Il circuito Cartasì, occupa un quarto del mercato italiano con più di 7 milioni di clienti, e i tentativi di transazione illecita nel 2008 sono stati di

circa 290 mila.

Secondo la polizia postale nel 2009, l'utilizzo illecito e fraudolento di carte bancarie è aumentato del 30%, all'estero non va meglio, in Gran Bretagna ci sono state frodi per un ammontare di 610 milioni di sterline.

Per le carte di credito si distinguono tre principali tipologie di frodi:

- Card ID-theft: avviene quando il truffatore utilizza una carta di credito della quale è in possesso avendola sottratta in precedenza ad un'altra persona la quale ne era titolare. Quindi c'è un totale furto di identità ai danni del titolare della carta di credito da parte del malfattore, il quale, sostituisce totalmente il malcapitato fingendosi titolare.
- Card-present fraud: avviene quando la carta rubata è fisicamente presente al momento dell'acquisto, quindi il truffatore dovrà presentarla al momento del pagamento affinché la transazione abbia buon esito. Questo tipo di truffa avviene solitamente mediante carte di credito smarrite o rubate, contraffazione di carte o utilizzo di blank card.
- Card-non-present fraud: per questo tipo di tecnica non c'è bisogno della presenza fisica della carta, in quanto il truffatore utilizza solo i dati della carta di credito, solitamente per acquisti online i quali non prevedono un face-to-face.

Ci sono diverse tecniche per impossessarsi dei dati delle carte di credito: attraverso lo skimming, dal verbo inglese to skim (strisciare) si cerca di carpire codici o password catturando i dati della carta direttamente dagli ATM mediante l'uso di dispositivi in grado di leggere la banda magnetica della card; con il phishing o pishing, si

cerca di sottrarre i dati attraverso l'uso ingannevole delle e-mail; mediante il trashing invece, si vuol risalire ai dati del possessore della carta di credito mediante la lettura di scontrini o estratti conto facilmente reperibili in prossimità degli ATM, scontrini o estratti conto possono essere una fonte diretta o indiretta per ottenere dati attraverso l'utilizzo di semplici software scaricabili dalla rete.

Per quanto riguarda le carte di debito generalmente, si cerca di rubare i dati direttamente dall'ATM o dai POS attraverso l'utilizzo di dispositivi in grado di leggere e memorizzare i dati dalla banda magnetica della carta. Il principale problema per il truffatore è scoprire il codice PIN, senza il quale non è possibile effettuare alcuna operazione. Solitamente vengono installate piccole telecamere (ben nascoste) nella parte sovrastante l'ATM in modo da registrare la sequenza di numeri digitata direttamente dalla mano dell'ignaro e sfortunato utente.

### **3.2 Forme di sicurezza**

Il timore principale dell'utente che acquista online è vedersi truffato per quanto riguarda l'acquisto di prodotti, o vedersi sottratto dei propri dati e le proprie password delle carte di credito da parte di malintenzionati (vedi sezione 3.1).

Oggi giorno tuttavia, pagare online è diventato piuttosto sicuro e tutelato, basta infatti fare un pò di attenzione per evitare truffe.

La legge italiana tende sempre più a tutelare il consumatore e le banche, colui che principalmente rischia è il commerciante. Nel caso in cui un utente acquisti un prodotto da un negozio online è presente una forma di tutela piuttosto completa. Infatti, se il prodotto venduto viene smarrito o il consumatore non è soddisfatto, quest'ultimo può vantare del diritto di recesso; il venditore dovrà

riaccreditare totalmente l'ammontare speso, sulla carta di credito dell'utente<sup>1</sup>.

Nel caso di appropriazione indebita di codici e/o dati di carte di credito attraverso tecniche di phishing, colui che le effettua rischia pene e sanzioni assai gravi. Rischia infatti da 1 a 5 anni di reclusione e una multa che va da €309 a €1549<sup>2</sup>.

Le principali precauzioni da prendere onde evitare di essere truffati online sono molteplici:

- E' consigliato verificare la presenza e salvare tutti i dati del venditore (nome, cognome, indirizzo, partita IVA, locazione della ditta o società), in modo tale da avere un recapito nel caso in cui il venditore faccia perdere le proprie tracce.
- Inserire i dati della carta di credito solo se nel form di inserimento dei dati è presente una connessione sicura, basti controllare la presenza di un lucchetto nella parte inferiore del browser, e che la pagina sia protetta dal protocollo HTTPS (Secure HyperText Transfer Protocol, di cui parleremo più avanti), ovvero se è presente la scritta https nella barra dove viene inserito il nome del sito.
- Monitorare con frequenza lo stato del proprio conto, in modo da verificare l'eventuale presenza di anomalia che devono al più presto essere contestate.
- Conservare tutte le mail che confermano l'acquisto del prodotto, poiché fungono da ricevute di pagamento.
- Avere sempre sotto mano il numero verde della carta di credito per poterla eventualmente bloccare.

---

<sup>1</sup>articolo 56 del codice del consumo, decreto legislativo 206 del 2005

<sup>2</sup>articolo 12, legge 97 del 1991

Per rendere sicuri gli acquisti effettuati online si è avuta l'esigenza di implementare degli standard di sicurezza al fine di garantire più fiducia tra utente e venditore. SSL (Secure Socket Layer) è un protocollo che stabilisce un canale di comunicazione sicuro tra browser e server. Questo protocollo funge da soluzione crittografica per i dati che vengono trasmessi dal browser al server, e viceversa.

Fu implementato nel 1994 da Netscape Communications, affinché fosse usato con il browser Netscape Navigator (versione 1.0). Dopo la versione 1.0 venne progettata la 2.0, che fu la prima ad essere disponibile agli utenti; nonostante fosse ben progettata emersero piccole imperfezioni che portarono all'implementazione della versione 3.0 nel 1996.

Contemporaneamente, la Microsoft Corporation introdusse una tecnologia simile per il browser Internet Explorer denominata PCT (Private Communication Technology). Successivamente alla nascita dei due protocolli, la IETF (Internet Engineering Task Force) mise insieme questi protocolli per creare uno standard comune per ogni browser, denominato TLS[20](Transfer Layer Security). TLS rappresenta la versione finale e più completa di SSL, poiché si basa in tutto e per tutto su SSL, ma lo integra con alcuni miglioramenti.

La componente fondamentale di una connessione SSL è rappresentata dal cosiddetto SSL Handshake Protocol, ovvero dallo scambio di messaggi che intercorrono tra browser e server, e viceversa. Inizialmente il server deve autenticarsi, per il client non è obbligatorio; una volta terminata l'autenticazione c'è la contrattazione per la sequenza cifrata, viene quindi fornito un parametro crittografico che verrà utilizzato per l'intera durata della sessione e che garantirà la sicurezza negli scambi.

Durante la sessione di pagamento al client sarà chiesto di inserire i propri dati sensibili assieme a tutti i dati della carta di credito. Tutte queste informazioni vengono cifrate ed inviate al server in mo-

do sicuro, viene spedita poi una richiesta per ottenere un punto di transito con conversione dei protocolli (gateway) alla banca dell' esercente, per terminare il pagamento. A questo punto il server SSL ottiene l'autorizzazione o il rifiuto per la transazione, attraverso il gateway per il pagamento, e spedisce il risultato al commerciante ed al consumatore.

Recentemente Banca Sella ha implementato un nuovo gateway per i pagamenti online. GestPay è stato creato per rendere più sicure le transazioni effettuate tra il cliente e il negozio dell' esercente convenzionato con GestPay. L' esercente convenzionato scaricherà dal sito di Banca Sella una classe Java multiplatforma adattabile a qualsiasi sistema, la quale avrà il compito di cifrare i dati forniti dall' acquirente che saranno poi spediti al server Banca Sella mediante un algoritmo a chiave simmetrica (di cui parleremo più avanti). Lo scambio dei messaggi tra browser e server viene tutelato attraverso un trasporto criptato dal protocollo SSL3 a 128 bit.

Inoltre, per garantire maggiore sicurezza il merchant deve comunicare uno o più indirizzi IP che andranno a comunicare col server Banca Sella, che farà una verifica incrociata sull' ID del venditore e sugli indirizzi IP forniti. Infine, grazie ad un tool che gestisce i rischi si potranno impostare dei criteri secondo i quali rifiutare transazioni potenzialmente pericolose.

### 3.2.1 Sistemi di crittografia

Un sistema di crittografia è un algoritmo, che permette di cifrare una serie di dati in modo tale da renderli illeggibili se non si possiede una chiave.

Gli algoritmi di crittografia si possono dividere in due categorie: gli algoritmi a crittografia simmetrica o a chiave privata, e gli algoritmi di crittografia asimmetrica a chiave pubblica.

#### 3.2.1.1 Crittografia simmetrica

La caratteristica fondamentale degli algoritmi di crittografia simmetrica risiede nel fatto di avere un'unica chiave, che permette sia di cifrare i dati, sia di decifrarli. Nonostante le migliori prestazioni (maggiore velocità), rispetto agli algoritmi a crittografia asimmetrica, il principale limite sta proprio nel fatto di avere una sola chiave. Infatti, essendoci un'unica chiave il rischio che qualcuno se ne impossessi, avendo quindi i permessi per leggere e modificare i dati, è molto alto.

Un'altra caratteristica degli algoritmi a chiave privata è che, se un utente deve inviare un messaggio criptato a più parti, adoterà tante chiavi segrete quante sono le controparti; altrimenti ogni utente potrebbe leggere, e quindi anche modificare messaggi non rivolti a se stesso. Un altro problema sta nello scambio delle chiavi, le due parti dovranno vedersi di persona per scambiarsi le chiavi, dato che inviarle via mail non sarebbe una scelta giusta non essendo un canale protetto.

Esistono svariati algoritmi per la crittografia simmetrica:

- DES (Data Encryption Standard, algoritmo di crittografia sviluppato negli Stati Uniti ma usato anche da altri governi e soprattutto nel mondo della finanza. DES è un cifratore a blocchi

con dimensione di 64 bit. Per la cifratura e la decifratura utilizza chiavi di 56 bit che lo rendono vulnerabile ad attacchi di forza bruta data l'attuale potenza di calcolo disponibile. Tuttavia, è abbastanza difficile da attaccare singolarmente, ma può essere facilmente forzato da associazioni, governi o istituzioni militari aventi a disposizione adeguate risorse hardware.

- IDEA (International Data Encryption Algorithm), è un algoritmo sviluppato dalla ETH Zurich in Svizzera, politecnico federale di Zurigo. Ideato nel 1990, è un algoritmo piuttosto recente ed anche uno tra i più conosciuti. Considerato molto sicuro, utilizza una chiave a 128 bit, e, da quando è stato creato nessuno è riuscito ad attaccarlo.
- RC4, algoritmo realizzato dalla RSA Security Inc., società statunitense specializzata in sicurezza informatica. Accetta chiavi di lunghezza arbitraria quindi non banale da attaccare. E' essenzialmente un generatore di numeri pseudo casuali; è molto utilizzato nei protocolli SSL e WEP. L'RC4 crea un flusso di bit pseudo casuali, il quale viene combinato attraverso un'operazione di XOR che utilizza questa sequenza pseudo casuale per ottenere i dati cifrati.

### 3.2.1.2 Crittografia asimmetrica

A differenza degli algoritmi di crittografia a chiave simmetrica, che utilizzano la stessa chiave per cifrare e decifrare il messaggio, negli algoritmi di crittografia a chiave asimmetrica si utilizzano due chiavi distinte. La chiave per il decriptaggio non è ottenibile da quella utilizzata per il crittaggio.

Caratteristica principale di questi algoritmi è che una chiave è pubblica mentre l'altra è privata: la chiave pubblica è nota a tutti i destinatari del messaggio, quella privata invece è a conoscenza solo del proprietario. Quindi la chiave pubblica serve a criptare il messaggio, mentre la chiave privata a decriptarlo.

La crittografia asimmetrica fu ideata da Whitfield Diffie e Martin Hellman per rendere più sicuro lo scambio delle chiavi. Un limite relativo l'uso di questi algoritmi può essere l'invio di un messaggio da parte di un utente che finge di essere il mittente.

Per questo motivo è stata ideata la firma digitale.

A differenza della crittografia simmetrica. in quella asimmetrica non è presente il problema di distribuzione delle chiavi, poiché è necessario scambiarsi solo le chiavi pubbliche. La comodità è quindi che le due parti possono trasmettere dati privati anche quando non c'è modo di concordare una chiave privata.

Solitamente tutti i metodi utilizzati per la crittografia asimmetrica sono abbastanza lenti.

Esistono diversi algoritmi a chiave pubblica:

- RSA (Rivest-Shamir-Adelman), è un algoritmo a chiavi asimmetriche creato nel 1978 da tre ricercatori (Rivest-Shamir-Adelman) del MIT (Massachusetts Institute of Technology). E' l'algoritmo a chiave pubblica più diffuso in quanto può essere usato sia per cifrare che per la firma digitale. Molto sicuro se sono usate chiavi abbastanza lunghe: con 512 bit è insicuro, con 786 è mo-

deratamente sicuro e con 1024 è considerato abbastanza sicuro. La sicurezza di questo algoritmo è rappresentata dal fatto che è molto difficile fattorizzare numeri interi molto grandi.

- PGP (Pretty Good Privacy), è un algoritmo di crittografia a chiave pubblica, originariamente sviluppato da Phil Zimmerman nel 1991. E' probabilmente il sistema di crittografia più usato al mondo. PGP è usato principalmente per lo scambio di documenti via Internet e, a differenza di SSL, può anche essere usato per proteggere dati su disco, o dati di backup. PGP utilizza sia la crittografia simmetrica che quella asimmetrica. La crittografia asimmetrica viene utilizzare per creare le due chiavi (pubblica e privata), la chiave pubblica serve al mittente per criptare una chiave segreta, detta anche chiave comune che servirà per un algoritmo di crittografia simmetrica, in pratica questa chiave serve per cifrare il testo in chiaro del messaggio. Il destinatario, una volta ricevuto il messaggio protetto da PGP lo decripta utilizzando la chiave segreta (o chiave di sessione) con l'algoritmo simmetrico. La chiave segreta è allegata nel messaggio ma è criptata, servirà la chiave privata del destinatario a decriptarla.

### 3.2.2 Il protocollo HTTPS

A differenza del più utilizzato protocollo HTTP (HyperText Transfer Protocol), che si occupa del trasferimento dei dati da browser a server tramite l'utilizzo del protocollo TCP (Transfer Control Protocol), il più sicuro protocollo HTTPS (Secure HyperText Transfer Protocol), offre un canale di comunicazione protetto che, oltre ad utilizzare i protocolli HTTP e TCP, utilizza ulteriori protocolli di protezione per rendere possibile il criptaggio dei dati.

HTTPS utilizza il protocollo TLS (Transfer Layer Security) e SSL (Socket Secure Layer), due protocolli utilizzati per cifrare i dati e permettere al browser e al server di scambiarsi questi dati in maniera sicura. Con HTTPS i dati non transitano sulla porta 80, come avviene per le connessioni HTTP, ma vengono trasmessi sulla porta 443. Una connessione HTTPS viene solitamente chiamata connessione sicura, ed è facilmente riconoscibile dal lucchetto chiuso presente nella parte inferiore del browser, e dalla scritta "https://..." sulla barra degli indirizzi.

### 3.2.3 Protocollo SET

SET (Secure Electronic Transaction) è un protocollo di sicurezza ideato da Visa e Mastercard nel 1996, basato sullo standard SSL. SET permette di pagare in modalità sicure su reti aperte, infatti si basa sullo scambio di certificati elettronici fra istituti finanziari.

SET utilizza un algoritmo di crittografia a chiave pubblica (RSA) per criptare i dati, questi dati sono protetti finchè non arrivano all'istituto finanziario. Nel rapporto di compravendita che intercorre tra compratore e venditore, che impiegano la firma digitale per autenticarsi fra loro, nell'utilizzo del protocollo SET figura una terza entità.

L'Autorità di Certificazione (AC), si occupa di fornire certificati che attestino una più alta assicurazione sull'identità delle controparti. Non appena le due parti della compravendita provano la propria identità (con passaporto, carta d'identità, patente), l'Autorità di Certificazione crea due messaggi distinti, per entrambe le parti, contenenti i nomi e le rispettive chiavi pubbliche. Questi messaggi sono firmati digitalmente dall'Autorità di Certificazione, e prendono il nome di certificati.

Nel momento in cui un utente acquista un bene, utilizzando il protocollo SET, tutti i dati utili per perfezionare l'acquisto, sono inviati dal client al server del venditore, che però riceverà solo i dettagli dell'ordine, il numero della carta di credito è inviato direttamente all'istituto bancario.

Acquistare con SET è abbastanza celere, come prima cosa il titolare della carta di credito dovrà ottenere un wallet (1) (vedi sezione 2.5) dalla propria banca, attraverso il quale, tramite l'Autorità di Certificazione sarà possibile memorizzare il certificato digitale riferito a quell'utente (2), anche il merchant dovrà ottenere un certificato digitale (2). Al momento della transazione, il merchant, attraverso un software invia all'acquirente il form nel quale inserire i dati e il certificato digitale criptato (3); invia inoltre il certificato digitale criptato. Simultaneamente il software del wallet dell'acquirente invia le istruzioni per l'ordine e il certificato digitale criptato al merchant (4), così che il venditore non possa vedere le informazioni della carta finché l'istituto di credito non le abbia deciptate. L'ultimo passo spetta alla banca, una volta che, attraverso il protocollo SET vengono inviate le informazioni in modalità sicura alla banca (del merchant) tramite un gateway per il pagamento (5), la banca infine, inoltrerà una richiesta di pagamento alla banca dell'acquirente (6) (vedi figura 3.1[23]).

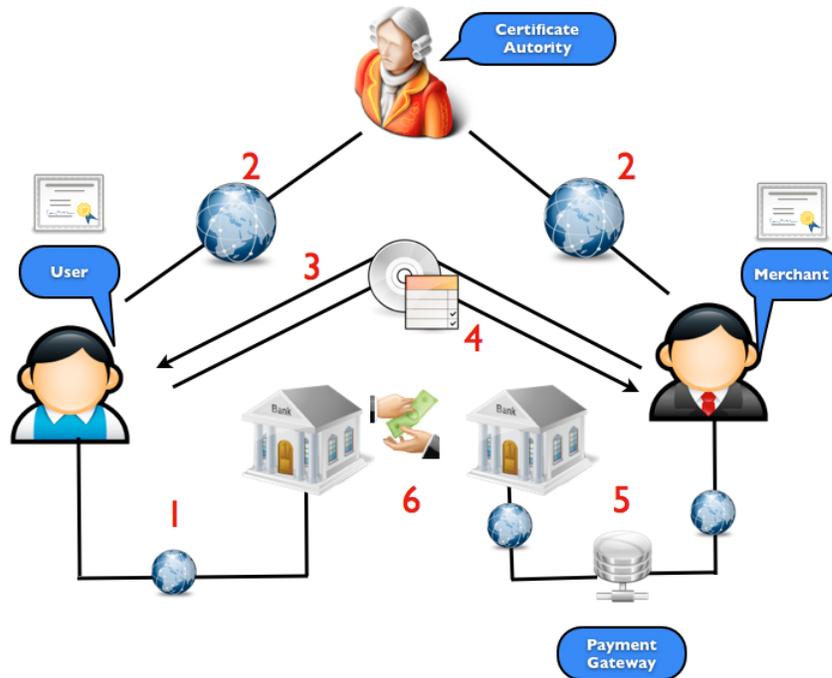


Figura 3.1: Schema SET

Il protocollo SET dunque, richiede quattro distinti software:

- Il software del wallet dell'acquirente
- Il software del venditore
- Il software del server Gateway
- Il software dell'Autorità di Certificazione

Tuttavia, questo protocollo, non ha riscosso molto successo per alcuni motivi: l'installazione del software del client, il costo e la difficoltà riscontrata nei venditori di fornire un supporto ai clienti e le difficoltà logistiche nella distribuzione dei certificati.[21]

## Capitolo 4

# Sistemi di pagamento online a confronto

### 4.1 Introduzione

In questo capitolo si confronteranno tutti i sistemi di pagamento online elencati nel capitolo 2. In particolare, i sistemi di pagamento verranno confrontati sulla base di sei principali attributi:

- Riservatezza
- Accettazione
- Costi
- Sicurezza
- Tempi di accredito/addebito
- Facilità d'uso

La riservatezza è molto importante nei pagamenti online, uno dei dubbi che solitamente tormenta un utente nell'acquistare online è

la paura che i propri dati possano finire nelle mani di utenti malintenzionati. Per ovviare a questi timori, la maggior parte dei siti e-commerce propongono svariati sistemi per il pagamento online utilizzando sistemi mirati a proteggere i dati dell'acquirente, nell'interesse di chi acquista, ma anche di chi vende online. Solitamente i dati personali vengono scambiati solo tra le due parti interessate alla transazione, tuttavia vari sistemi di pagamento prevedono una terza parte fidata, incaricata di gestire la transazione, in modo tale da rendere la compravendita riservata (solitamente i dati sensibili delle controparti vengono utilizzate ai fini della spedizione).

Altro importante fattore per acquistare online è il livello di accettazione, un sistema di pagamento più è accettato, tanto più acquista notorietà tra gli utenti, i quali saranno poi invogliati a preferire un sistema di pagamento maggiormente accettato e diffuso a scapito di quelli meno noti.

I costi invece, costituiscono un importante fattore nella scelta di un metodo di pagamento, minori saranno i costi, maggiori saranno il successo e le adesioni al sistema di pagamento.

Per quanto riguarda la sicurezza, i principali metodi di pagamento assicurano un grado di sicurezza elevato. Tuttavia, se un utente decidesse di intraprendere una trattativa, e scegliesse di pagare al di fuori del sistema di pagamento previsto, la sicurezza non è garantita. In questo caso, la scelta è molto influenzata dai costi, poiché pagando al di fuori dei sistemi di pagamento tradizionali i costi sarebbero relativamente bassi, ma può andare a discapito della sicurezza, perché in questo modo l'acquirente sarebbe esposto a rischi nel momento in cui dovrà fornire i propri dati, compresi quelli della carta di credito, alla controparte.

Altro fattore di scelta per un metodo di pagamento sono i tempi di accreditalmento/addebitamento delle somme versate. Solitamente i tempi necessari per concludere una transazione vanno da un

massimo di sei giorni ad un minimo di pochi secondi.

La facilità d'uso, ultimo attributo, ma non importanza, è determinante nella scelta di un metodo di pagamento. L'interfaccia grafica è molto importante per l'utilizzo di un sistema di pagamento, questa dovrà essere "user friendly", ovvero garantire una certa facilità nell'utilizzo, ma anche una certa efficienza ed efficacia.

## 4.2 Riservatezza

Caratteristica fondamentale in qualsiasi sistema di pagamento online è la riservatezza. Solitamente gli attori di una compravendita richiedono riservatezza nel senso che, solo le due parti coinvolte nella transazione vengono a conoscenza dell'identità del compratore e dell'identità del venditore.

Sovente per garantire maggiore riservatezza i siti internet utilizzano nickname e pseudonimi.

La riservatezza (solo se è presente una terza parte fidata) per chi acquista online a mezzo carta di credito è abbastanza alta, infatti, attraverso l'uso di protocolli (vedi capitolo 3), le informazioni sono accessibili solo alla banca.

Per le carte ricaricabili vale lo stesso discorso, dato che vengono utilizzate in maniera analoga alle carte di credito per acquistare online.

Per quanto riguarda Paypal, la riservatezza è garantita, in quanto al momento del pagamento l'utente fornisce solo ed esclusivamente l'indirizzo e-mail, tramite il quale Paypal procederà con il pagamento, ed attraverso il quale non è possibile risalire ai dati della carta di credito o ricaricabile.

"pagamentionline" di Si-Servizi (ex BankPass Web) funziona in maniera molto simile a Paypal, l'unica pecca si verifica quando si paga verso un esercente non convenzionato al servizio, in quel caso

si utilizza un numero di carta di credito temporaneo da fornire al venditore.

Il bonifico bancario online, per perfezionarsi ha bisogno di nome, cognome e codice IBAN di colui che riceverà il denaro, che a sua volta riceverà via mail nome, cognome e codice IBAN (con alcune cifre oscurate) dell'acquirente. Tuttavia, fornire questi dati per un bonifico è fondamentale (nonostante non assicuri totale riservatezza), poiché il bonifico è solitamente usato per grandi importi di denaro.

Con Square, dato che la carta di credito viene strisciata fisicamente dal venditore, non c'è bisogno nè di scrivere nè di comunicare i dati della carta, ma, al momento del pagamento, dopo che la carta viene letta dal dispositivo, vengono visualizzati tutti i dati sul display, compresa la foto dell'acquirente.

Google Check-out, invece, fornisce tutti i dati del compratore (escluso quelli della carta di credito) al momento dell'acquisto.

### 4.3 Accettazione

Un'altra fondamentale caratteristica per un sistema di pagamento online è il livello di accettazione. Più il sistema di pagamento è diffuso, più è possibile utilizzarlo per acquistare online.

Attualmente, nel mondo e-commerce, il sistema più accettato è Paypal, nonostante vari metodi emergenti che cercano di strappare una fetta di mercato senza grandi risultati.

Le carte di credito sono accettate praticamente ovunque.

Le carte ricaricabili, che stanno col tempo assumendo la stessa importanza delle carte di credito, sono piuttosto accettate, grazie anche al fatto che la maggior parte aderiscono agli stessi circuiti delle carte di credito.

Paypal, come già detto, con i suoi 84 milioni di utenti, è il sistema di pagamento accettato praticamente ovunque nella rete, ba-

sti pensare che grandi piattaforme come eBay.com e Amazon.com utilizzano questo sistema come strumento di pagamento principale.

Per quanto riguarda l'ormai ex BankPass Web (pagamentionline Si-Sistemi), questo sistema di pagamento sta avendo un netto calo di popolarità, poichè prima di tutto è accettato solo in Italia, poi anche perché da quando non fornisce più il pagamento mediante carte di debito è diventato un semplice sistema di pagamento che sfrutta un wallet come ce ne sono tanti.

Il bonifico bancario online è abbastanza diffuso, ma non come Paypal, poiché il principale limite è rappresentato dal fatto che oggi sono i giovani che acquistano maggiormente online, e molti di essi non possiedono un conto corrente bancario.

Square, è un metodo di pagamento emergente, tuttavia, è presto stimare un grado di accettazione perché è ancora in prova nei soli Stati Uniti.

Google Check-out, invece, ideato con lo scopo di rivaleggiare con Paypal, non ha riscosso molto successo, è accettato prevalentemente su siti statunitensi e siti convenzionati con Google.

#### 4.4 Costi

I costi nei metodi di pagamento online sono un importante fattore che spinge gli utenti a preferire un sistema anziché un altro.

Essendoci diversi tipi di carte di credito presenti sul mercato, non è facile dire se i costi sono alti o bassi. Su un campione di carte di credito, e una spesa media annua fissa, si evince che i costi vanno da €7,00 annui, fino ad arrivare a €145,00.

Le carte ricaricabili, nonostante il boom di adesioni registrate negli ultimi anni, presentano costi piuttosto alti. I principali fattori che rendono le carte ricaricabili care, sono i costi di prelievo, i costi per operazione e i costi di ricarica.

Paypal, nonostante sia il sistema di pagamento più diffuso, impone anch'esso costi piuttosto alti. Per ogni transazione, infatti Paypal trattiene €0,35 più una percentuale sull'ammontare che va dall' 1,8% al 3,4%.

Il bonifico bancario online, ha dei costi raggiungono anche €6,00, in funzione del tipo di conto corrente e convenzioni che si hanno con la banca.

Le condizioni economiche dell'ormai ex BankPass Web non sono delle migliori, infatti ci vogliono poco meno di €30,00 per usufruire del servizio, più altri costi per operazione.

Oggi giorno, i metodi di pagamento più convenienti sono quelli emergenti. Un pò per promuovere il nuovo sistema, un pò per fare una guerra di prezzi ai sistemi già affermati, Square e Google Check-out, offrono dei prezzi molto bassi e convenienti.

Square negli Stati Uniti ha abbassato le percentuali di trattenuta per operazione, eliminato tasse e costi contrattuali e di setup, mentre Google Check-out è completamente gratuito.

## 4.5 Sicurezza

Come già detto (vedi capitolo 3), il successo del commercio elettronico è strettamente collegato alla possibilità di effettuare transazioni sicure sulla rete. Proprio per questo motivo si tende a tutelare il consumatore il più possibile.

Grazie a svariati protocolli, la sicurezza nei pagamenti online diventa sempre più alta. Tuttavia, i rischi sono sempre presenti (vedi sezione 3.1).

Pagare con carta di credito e con carte prepagate in rete è sempre più sicuro; protocolli e sistemi di crittografia rendono la transazione sicura, fondamentale è quindi, non fornire mai gli estremi della carta

di credito alla controparte a meno che non si è sicuri della buona fede di quest'ultimo.

Con Paypal, invece, la sicurezza e le forme di tutela sono maggiori, infatti oltre ad essere un sistema di pagamento sicuro, prevede varie forme di tutela per il consumatore. Nel caso in cui la merce non arrivi o la merce non sia conforme alla descrizione, Paypal prevede un rimborso. Se un utente presenta un reclamo riguardante un acquisto, Paypal prende in esame l'operazione e decide se procedere con un rimborso oppure no.

A differenza di Paypal, "pagamentonline" di Si-Servizi è meno tutelato, in quanto la banca che fornisce il servizio non è responsabile per eventuali reclami in merito a quanto acquistato e non può procedere con storni addebitati al cliente.

Stesso discorso vale per il bonifico bancario online, indubbiamente molto sicuro, ma non prevede ulteriori forme di tutela come Paypal. La spedizione di un oggetto è regolata e tutelata dal solo Paypal, infatti in una compravendita tra privati, nel caso in cui si riscontrino anomalie, non sono previsti rimborsi in nessuno dei sistemi di pagamento diversi da Paypal. E' bene in questi casi, acquistare solo da negozi online nei quali si ripone una certa fiducia.

La sicurezza con Square è abbastanza alta, infatti al momento del pagamento, sul display viene visualizzata anche la foto dell'acquirente, un ulteriore controllo non previsto dagli altri sistemi.

Google Check-out, invece, come tutti gli altri metodi di pagamento, non comunica in nessun modo gli estremi della carta di credito di colui che effettua l'acquisto.

## 4.6 Tempi

Altro fattore di scelta per un metodo di pagamento sono i tempi di accredito/addebitamento delle somme versate.

Pagando con carta di credito o carta prepagata vengono assicurati tempi minimi. Solitamente quando un utente paga via Internet un bene o servizio utilizzando una carta di credito o prepagata, i tempi di accredito/addebito sono al massimo di qualche ora.

Paypal impiega tre o quattro giorni per aggiornare il saldo della carta di credito; “pagamentonline” di Si-Servizi e Google Check-out, basandosi su carte di credito, impiega fondamentalmente gli stessi tempi delle carte di credito, ovvero massimo un’ora.

Per il bonifico online invece, i tempi sono maggiori, si va da un minimo di un giorno, ad un massimo di sei, a seconda che la transazione avvenga tra la stessa banca o tra banche diverse.

Square invece, essendo un sistema di pagamento “fisico”, nel senso che utilizza la fisicità della carta per terminare la transazione, ha tempi immediati, ovvero la compravendita termina non appena l’utente inserisce il PIN e appone la firma sul display del dispositivo Apple del venditore.

## 4.7 Facilità d’uso

Fattore molto importante per chi acquista online è la facilità nell’utilizzare un determinato sistema di pagamento. L’usabilità è definita dall’ISO (International Organisation for Standardisation), come l’efficacia, l’efficienza e la soddisfazione con le quali determinati utenti raggiungono determinati obiettivi in determinati contesti. In pratica definisce il grado di facilità e soddisfazione con cui l’interazione uomo-strumento si compie[22].

Questo attributo è fondamentale per chi non ha molta esperienza negli acquisti online; nuovi utenti, non particolarmente esperti,

apprezzano molto un'interfaccia comprensibile e facile da utilizzare, ma che allo stesso tempo deve essere efficace ed efficiente.

Pagare con carte di credito o prepagate è piuttosto semplice, basta infatti compilare il tipico form che si presenta al momento del pagamento, dove l'utente andrà ad inserire i propri estremi, il numero la scadenza e il cvv della carta di credito.

Stesso discorso per Paypal, "pagamentonline" di Si-Servizi e Google Check-out, dove l'utente andrà ad inserire tutti i dati al momento della registrazione. Per Paypal sarà sufficiente fornire l'indirizzo e-mail del beneficiario e l'importo da pagare, per "pagamentonline" di Si-Servizi basterà inserire l'importo, mentre per Google Check-out sarà sufficiente un click per completare l'acquisto.

Per Square invece, dopo essersi registrati su squareup.com fornendo una propria foto, sarà molto facile completare l'acquisto; basterà infatti, dopo aver strisciato la carta di credito, inserire il proprio PIN e apporre la propria firma sul dispositivo Apple.

4.8 Tabella riepilogativa

	carta di credito	carta ricaricabile	paypal	sis-bankpass	bonifico bancario online	square	google check-out
riservatezza	alta	alta	alta	alta	media	bassa	alta
accettazione e	molto alta	molto alta	molto alta	bassa	media	bassa	bassa
costi	medi	medi	alti	alti	medi	bassi	bassi
sicurezza	alta	alta	alta	media	molto alta	alta	alta
tempi	bassi	bassi	medi	medi	alti	bassi	medi
facilità d'uso	alta	alta	alta	media	alta	alta	molto alta

Tabella 4.1: Tabella riepilogativa

# Conclusioni

In questa tesi si è trattato l'argomento dei metodi di pagamento online. Dopo aver introdotto brevemente l'e-commerce, nel primo capitolo sono stati elencati gli attori della compravendita online, le varie forme di e-business e sono stati descritti i principali motivi che scoraggiano gli utenti ad avvicinarsi al commercio online. L'obiettivo è stato quello di elencare gli attuali sistemi di pagamento più utilizzati nell'e-commerce, e quelli emergenti, descrivendoli e confrontandoli tra loro sulla base di sei fattori. E' stato molto trattato l'argomento sicurezza, siccome questo attributo è il principale fattore frenante dell'e-commerce, poiché gli utenti che acquistano in rete spesso sono perplessi sotto questo punto di vista. Sono stati descritti quindi, i principali rischi a cui l'utente va incontro acquistando online e i consigli utili per prevenirli; sono state inoltre elencate le principali forme di sicurezza che vengono utilizzate nel momento della transazione, come i protocolli di sicurezza e gli algoritmi di crittografia associati ad essi. Dato che la sfera delle transazioni via Internet sta crescendo di anno in anno, continueranno a nascere nuovi strumenti per pagare online. C'è quindi una vera e propria guerra di idee, proposte e tecnologie in atto, non avremo quindi mai un unico sistema di pagamento telematico, ma una moltitudine di essi, proprio come nel sistema dei pagamenti in vigore nel mondo reale. Tuttavia, si evince che i metodi di pagamento emergenti faranno molta fatica ad arrivare ai risultati raggiunti da metodi di pagamento più vecchi ed affermati. Nella tabella riepilogativa, si è

giunti ad una conclusione che tutti i metodi di pagamento online sono differenti tra loro, sulla base di sicurezza, riservatezza, costi, tempi e facilità d'uso. A mio giudizio il fattore principale che influenza un utente nello scegliere un sistema di pagamento online anziché un altro, è l'accettazione: metodi di pagamento molto diffusi, accettati quindi ovunque nel Web, riscuotono maggiore successo rispetto a nuovi sistemi, magari più convenienti sotto il punto di vista economico.

# Bibliografia

- [1] <http://www.101vetrine.com/servizi/e-commerce/normativa>
- [2] V. B. MACKLIN, E-Commerce at what Price. Privacy Protection in the 'Information Economy', cit., 15-16; I. FAYENSON, Cookies Challenge Meanings of Privacy, 226 N.Y. L. J. 1 (2001); M.S. ROTH, Beware of cookies: do Marketers that Track a User's On-line Activities Threaten Privacy?, 23 The National L. J. PC1 (2001); V. CARIDI, La tutela dei dati personali in Internet: la questione dei logs e dei cookies alla luce delle dinamiche economiche dei dati personali, in Dir. inf., 2001, 763.
- [3] <http://www.ietf.org/rfc/rfc2109.txt>
- [4] V. M.J. RADIN, Information Tangibility, Stanford Law School. Public law research paper n. 48 (2002).
- [5] V. J.K. WINN, Clash of the Titans: Regulating the Competition between Established and Emerging Electronic Payment System, 14 Berkeley Tech. L.J. 675, 691-95 (1999); G.E. MAGGS, Payment Devices and General Principles of Payment Law, 72 Notre Dame L. Rev. 753, 759-763 (1997).
- [6] V. in generale G.E., MAGGS, Payment Devices and General Principles of Payment Law.
- [7] G. PASCUZZI, Il diritto dell'era digitale, 106-110
- [8] V.S. NEWMAN, G.SUTTER, Electronic Payment - the Smart Card, 18 Computer L. & Security Report 307 (2002); J.THEODORE, J.GALATAS, J.SGRO, A Smart Card Revolution in Payment System, 76 Law Institute Journal 76 (2002); E.ALDER, Smart Card Technology - Hong Kong, 18 Computer Law & Security Report 120 (2002); R.CARUSO, Smart card: le nuove tecnologie al servizio del cittadino, in Tributi, 2001, 320; F.SCOPACASA, La natura della transazione negli acquisti con smart card, in Il Corriere Tributario, 2002, 2700;
- [9] V.L. NEROTTI, Aspetti giuridici della sicurezza della firma elettronica e delle smart cards, in Ciberspazio e diritto, 2003, 305.
- [10] <http://www.paypal.com>

- [11] [https://cms.paypal.com/it/cgi-bin/marketingweb?cmd=\\_render-content&content\\_ID=ua/BuyerProtection\\_full&locale.x=it\\_IT](https://cms.paypal.com/it/cgi-bin/marketingweb?cmd=_render-content&content_ID=ua/BuyerProtection_full&locale.x=it_IT)
- [12] [www.ssb.it](http://www.ssb.it)
- [14] <http://www.bancheitalia.it/carte-di-credito/la-carta-prepagata-ricaricabile.htm>
- [15] <http://guide.inrosso.com/prodotti%20finanziari/carte-di-credito/carte-prepagate/vantaggi-uso-possesso.aspx>
- [16] <http://www.shenplanet.net/profiles/blog/show?id=1971767%3ABlogPost%3A37075>
- [17] <http://it.wikipedia.org/wiki/Ebay#Feedback>
- [18] <http://www.anti-phishing.it>
- [19] <http://www.repubblica.it>
- [20] <http://www.ietf.org/rfc/rfc2246.txt>
- [21] [http://it.wikipedia.org/wiki/Secure\\_Electronic\\_Transaction](http://it.wikipedia.org/wiki/Secure_Electronic_Transaction)
- [22] <http://it.wikipedia.org/wiki/Usabilit%C3%A0>
- [23] <http://findicons.com/>