

# Sistemi di pagamento elettronico



Moreno Marzolla  
Dipartimento di Informatica  
Università Ca' Foscari di Venezia  
marzolla@dsi.unive.it  
<http://www.dsi.unive.it/~marzolla>

## Ringraziamenti

- prof. Francesco Dalla Libera
  - Corso di Commercio Elettronico, Dipartimento di Informatica, Università Ca' Foscari di Venezia.

## Pagamenti in rete?

- Compensazione per informazioni, beni e servizi forniti attraverso la rete:
  - Accesso a materiale brevettato
    - Software, documenti, ...
  - Ricerche su archivi
  - Utilizzo di risorse
- Forma di pagamento per beni e servizi esterni:
  - Mercanzie consegnate fuori banda
  - Servizi forniti fuori banda

## Definizioni

- Pagamento
  - trasferimento di moneta da un individuo, o entità legale, ad un altro
- Moneta
  - "qualcosa che è di solito accettata come un mezzo di scambio, una misura di valore o un mezzo di pagamento"

## Tipi di moneta

- **Moneta Merce**
  - Mezzo di scambio utilizzato come moneta che ha già un valore di per sé (valore intrinseco)
  - Sono esempi di questo tipo l'oro o le sigarette nei campi di prigionia.
- **Moneta a corso legale**
  - Moneta priva di valore intrinseco che viene riconosciuta ed accettata per decreto legislativo. La banconota da 10€ non ha valore intrinseco, ma la legge dice che vale 10€
  - Con 10€ faccio la spesa, con un biglietto da 10 del monopoli faccio poco

## Tipo di moneta

- **Fiduciaria**
  - Ha la fiducia degli operatori
  - assegni, carte di credito / debito
- **Circolante**
  - Emessa da un istituto (banca) centrale
  - Banconote, monete

## Alcuni mezzi di pagamento

- Banconote o monete
- Assegni bancari / circolari
- Assegni personali
- Carte di credito e di debito
- Bonifico bancario
- Traveller's check
- Buoni sconto, bollini del supermercato, buoni pasto

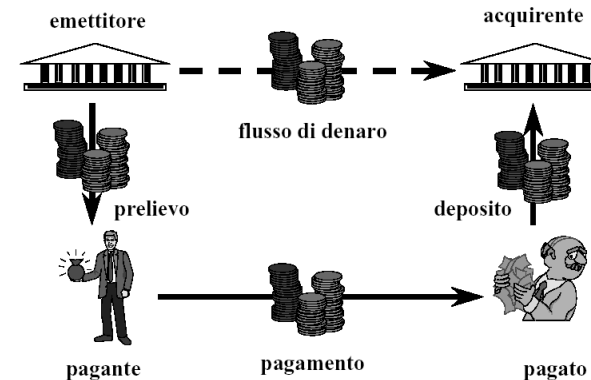
## Attori

- **Pagante**
  - Ottiene beni e/o servizi
- **Pagato**
  - Offre beni e/o servizi
- **Istituto emettitore**
  - Finanziaria alla quale il pagante si rivolge per ottenere il mezzo di pagamento
- **Istituto acquirente**
  - Finanziaria alla quale il pagato versa il pagamento

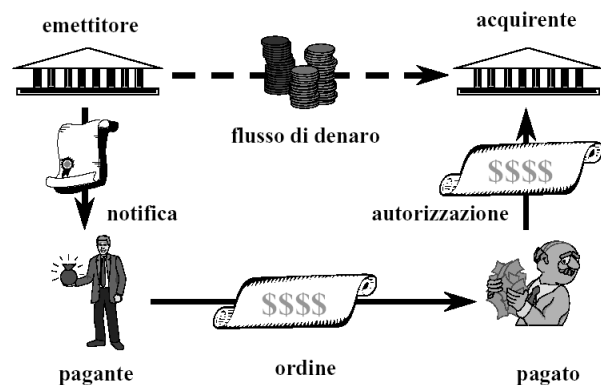
## Finalità del sistema

- Consentire al pagato di ottenere il denaro
  - Di solito nel suo conto bancario
  - Il pagamento in contanti è raro; solo per scambi di basso valore e in situazioni di faccia-a-faccia
  - Si pensi alla carta di credito. Chi dà al mercante la moneta vera?
- La maggior parte dei pagamenti non viene “eseguito” individualmente
  - Ad esempio: assegni – troppo piccoli per giustificare trasferimenti separati di fondi; vengono riuniti in blocchi (*batch*) per efficienza

## Pagamento per contanti



## Pagamento per assegno



## Carta di credito

### Definizione

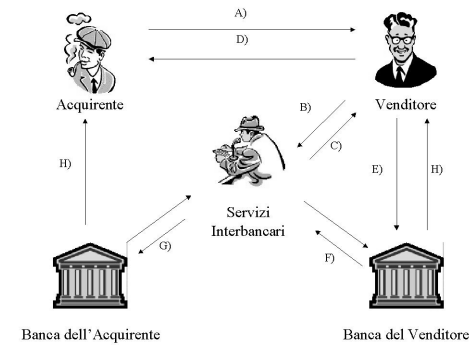
- Documento che abilita il titolare, in base a un rapporto contrattuale con l'emittente, a effettuare acquisti di beni / servizi presso esercizi convenzionati con l'emittente stesso, con pagamento differito
- Il regolamento da parte del titolare avviene a scadenze predefinite, effettuato con l'addebito in un conto bancario o tramite assegno o vaglia

## Carta di credito

### Caratteristiche

- Emessa da un istituto emittente, non da una banca
  - VISA, Mastercard, American Express, Diners, ...
- A favore di un individuo
  - Autenticazione con nome, cognome e firma
- Pagamenti solitamente appoggiati su conto corrente bancario
- *Ora anche prepagate e ricaricabili*

## Pagamento con carta di credito



## Fasi del pagamento

- l'acquirente presenta la carta di credito al venditore (non sempre: ad esempio ordini telefonici o via Internet)
- il venditore utilizza la carta di credito per richiedere l'autorizzazione a procedere
- la Rete Interbancaria autorizza la transazione
- il venditore produce una nota di vendita contenente tutte le informazioni di rilievo sulla transazione e ne consegna una copia al cliente
- il venditore invia una seconda copia della nota di vendita alla propria banca (in genere, aspetta di aver raccolto un certo numero di note di vendita e le invia in blocco)
- la banca del venditore accredita sul conto corrente del venditore l'importo relativo alla transazione e notifica i servizi interbancari,
- i servizi interbancari notificano la banca dell'acquirente, che detrae l'importo della transazione dal conto corrente intestato all'acquirente (i servizi interbancari regolano le transazioni tra le due banche),
- ciascuna banca invia al proprio cliente un estratto conto che indica il completamento della transazione

## Carta di debito

### Definizione

- Documento che consente al titolare di effettuare operazioni presso sportelli automatici (Bancomat) e/o su terminali ai punti di vendita (Pos) installati presso esercizi commerciali;
- La carta prevede l'addebito in tempo reale di ogni transazione sul c/c bancario a essa collegato.

## Carta di debito

### Caratteristiche

- Emessa da una banca
  - Appoggiata ad un conto corrente
  - Autenticata dalla presentazione simultanea di un token (la carta di plastica) e di un PIN
  - Scopo: autorizzare un trasferimento (immediato) di denaro dal c/c in oggetto a quello del mercante

## Alcuni esempi di sistemi di pagamento elettronici

- Trasferimento interbancario (EFT)
- Carta di credito (Visa, Mastercard, ...)
- Smart card (Mondex)
- Accumulazione (Qpass)
  - Ora anche sul mercato wireless
- Intermediari (PayPal)
- Micropagamenti (e.g. Millicent)
  - Progetto sospeso
- Gettoni (Flooz, Beenz)
  - Falliti in agosto 2001
- Electronic cash (eCash)

## Proprietà attese

- Universalmente accettato
- Transferibile, portabile
- Sicura
  - non falsificabile
- Privacy
  - nessuno, eccettuato le parti in causa, conosce l'ammontare
- Anonimo
  - nessuno può identificare il pagante
- Funziona off-line
  - nessuna verifica necessaria on-line
- Divisibile in pezzi
  - si paga con pezzi da 10 € un totale da 100 €
- Valori arbitrari (325.14 €, 1.000.000 €)

## Rischi per il cliente

- Credenziali e password rubate
- Mercanti disonesti
- Dispute sulla qualità del servizio
- Fornitori di servizi finanziari disonesti
- Uso non corretto dei dettagli della transazione
  - Privacy

## Rischi per il mercante

- Mezzi di pagamento copiati o non originali
- Dispute sulle commissioni
- Fondi insufficienti nel conto del cliente
- Ridistribuzione illecita dei beni acquistati
- Fornitori di servizi finanziari disonesti
- Pagamenti lenti da parte del fornitore di servizi finanziari

## Rischi per il fornitore di servizi finanziari

- Dispute sulle commissioni per i conti esterni
- Dispute sulle commissioni con il mercante
- Mercanti che “svaniscono”
- Mezzi di pagamento copiati o non originali

## Soluzioni tecniche

- Sicurezza della transazione e autenticazione delle parti
- Protezione delle credenziali di pagamento
  - Carte magnetiche
  - Smart cards
- Autorizzazioni on-line
  - Individuare le doppie spese
  - Controllare l'esistenza di fondi sufficienti
  - Validare modelli e comportamenti di spesa

## Classificazione

- Evoluzione sistemi tradizionali
  - Invio dettagli di carte di credito/debito
    - e-mail, connessione Out-Of-Band (First Virtual)
    - e-mail cifrata, HTTPS (HTTP + TLS), SET
- Sistemi a token
  - Utilizzo di “contante elettronico” (eCash)
  - Micropagamenti (Minipay)
  - Note di pagamento elettronico
- Smart-card
  - Borsellino elettronico hardware (Mondex)

## Proprietà Integrità

- Perfetta coincidenza tra:
  - Operazione richiesta dalle parti
  - Operazione eseguita dal sistema
- Integrità per pagante / pagato / sistema

## Proprietà Autorizzazione

- Nessuna operazione può avvenire senza il consenso esplicito delle parti
- Tutte le operazioni eseguite possono essere provate
  - Ciascuna operazione lascia una traccia
  - Non-operazioni non lasciano tracce
- Le regole per risolvere i casi controversi sono parte del sistema

## Proprietà Autorizzazione

- La parte autorizzante usa un canale fidato esterno al sistema per autorizzare l'operazione
- Es: carta di credito per ordini telefonici
  - l'istituto di credito notifica un addebito
  - l'utente autorizza implicitamente l'operazione
    - ... ma può bloccarla comunicandolo entro 90 gg out-of-band

## Proprietà Autorizzazione e password

- Ogni messaggio di autorizzazione contiene un controllo crittografico costituito da un segreto condiviso
- Se il segreto condiviso è semplice
  - Facilmente attaccabile
  - Può essere utilizzato per proteggere un dispositivo che supporta strumenti crittografici complessi (smart card)

## Proprietà Autorizzazione e firma elettronica

- L'operazione viene eseguita solo se è firmata elettronicamente
  - La firma garantisce il non-ripudio
  - Richiede l'utilizzo di algoritmi crittografici complessi

## Proprietà Riservatezza

- **Confidenzialità**
  - I dettagli dell'operazione non devono essere resi pubblici
    - Identità del pagante/pagato, l'importo, il bene acquistato
- **Anonimato**
  - **Pagante anonimo**
    - Il pagante agisce usando uno pseudonimo
  - **Pagamenti non collegabili**
    - Il pagato non riconosce pagamenti diversi provenienti dalla stessa persona
- **Non tracciabilità del pagante**
  - il sistema di pagamento non consente di risalire all'identità pagante

## Proprietà Affidabilità

- **Transazioni atomiche**
  - Il sistema deve impedire perdite dovute ad interruzioni o malfunzionamenti
- **Recupero da situazioni critiche**
- **Supporto di comunicazione affidabile**

## Proprietà Equità

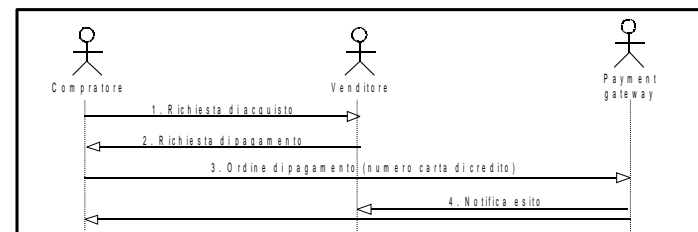
- **Non-ripudio per**
  - Ordine di acquisto
  - Invio di un bene
  - Ricevuta
- **Pagamenti per ricevuta o beni on-line**
- **Firma di contratti**
- **Obiettivi**
  - Minimizzare l'uso di terze parti
  - Semplicità
  - Indipendenza dal bene scambiato

## Caratteristiche tecnologiche

- Coinvolgimento nella transazione di terze parti autorizzante
- Anonimato della transazione
- Tracciabilità della transazione
- Obiettivi
  - Processare pagamenti autorizzati
  - Impedire pagamenti non autorizzati
  - Impedire doppi pagamenti
  - Assicurare la privacy

## Soluzioni con carta di credito

- Attori:
  - Compratore
  - Venditore
  - Payment gateway: è il ponte tra Internet e i circuiti finanziari autorizzativi (può non essere esplicitamente visibile al compratore)



## Classificazione

- Pagamento diretto
  - Tutti i dati della transazione (dati della Carta di Credito, dati dell'acquisto) sono gestiti direttamente dal mercante che si interfaccia con la rete interbancaria con modalità solo a lui note
- Payment gateway
  - I dati della Carta di Credito vengono dati dal compratore al *payment gateway* (terza parte fidata, che si interfaccia con la rete interbancaria) il quale garantisce presso il mercante
  - I dati dell'acquisto non sono invece comunicati al gateway

## I problemi della sicurezza e le soluzioni adottate

- Intercettazione delle informazioni
  - SSL
- Manomissione delle informazioni
  - Firma digitale, SSL
- Autorizzazione al pagamento
  - Firma digitale, SSL
- Impersonazione del venditore o del payment gateway
  - Certificati, SSL
- Cattiva gestione dei numeri delle carte di credito
  - I numeri delle carte non sono mai comunicati al venditore
- Impersonazione del compratore
  - Certificati
- Frode del compratore (ripudio)
  - Certificati

## Alcune soluzioni in Italia

- Sistemi a pagamento diretto (@Pos)
  - I dati della carta di credito sono comunicati direttamente al venditore
  - Semplicità di integrazione
  - Manca l'autenticazione del compratore
- Sistemi basati su payment gateway (Telepay Light, BankPass, Banca Sella, ... )
  - I dati della carta di credito non sono comunicati al venditore
  - Semplicità di integrazione
  - Manca l'autenticazione del compratore
- Sistemi non ripudiabili (SET)
  - Autenticazione del compratore
  - Transazioni non ripudiabili
  - Necessitano di software specifico per quest'ultimo (digital wallet)
  - Implementazione complessa e costosa

## Condizioni (novembre 2003)

- GestPay di Banca Sella
  - Canone annuale da 100 a 400€, commissione percentuale sull'importo della transazione dal 3 al 4%
- Secur@light di Banca Intesa.
  - Servizio basilare di pagamento offerto a 600€ annui più una trattenuta percentuale sulle transazioni

## Italia

- Bankpass Web
  - consente al cliente di effettuare acquisti on line, utilizzando i propri strumenti di pagamento, carte di credito e PagoBANCOMAT, inseriti in un portafoglio elettronico (wallet)
  - per ogni acquisto sarà sufficiente digitare i codici assegnati al momento dell'adesione al servizio, tramite uno specifico contratto presso una delle banche che partecipano all'iniziativa
  - Il servizio è emesso dall'ABI in collaborazione con E-committee
- Condizioni economiche
  - dal lato cliente: attivazione di un wallet dal costo annuo di 22€, il costo di transazione dipenderà dalla particolari condizioni proprie della carta di credito, bancomat o bonifico.
  - Dal lato esercente: costo di attivazione una tantum di 25€ e un canone annuale di 250€, commissione variabile dal 0,25 al 0,15% in base al numero di transazioni annue

## Soluzioni esistenti: commenti

- In Italia le soluzioni più diffuse sono quelle basate su payment gateway:
  - Garanzia per il compratore: il numero della carta è comunicato solo al payment gateway
  - Per i venditori resta il problema dell'autenticazione del compratore
- SET stenta a decollare
  - Scarso interesse da parte delle banche
  - Costi elevati per il software del merchant
  - Complessità di installazione e aggiornamento del certificato per il compratore

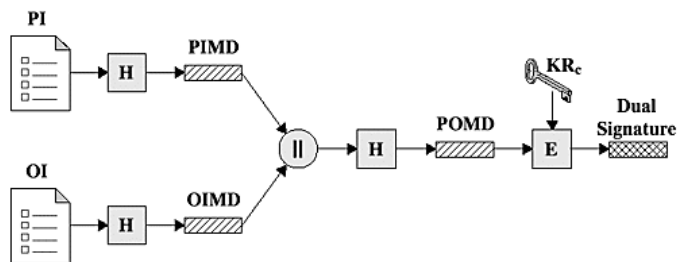
## SET Secure Electronic Transaction

- Standard per il pagamento elettronico con carte di credito
- Basato su una gerarchia di certificati che garantisce la chiave pubblica associata ad una carta di credito o ad un venditore
- La carta di credito deve essere abilitata al commercio elettronico fornendo al proprietario un certificato firmato che ne prova la validità
- Acquirente e Venditore devono acquisire una coppia chiave pubblica/chiave privata dalla banca

## SET

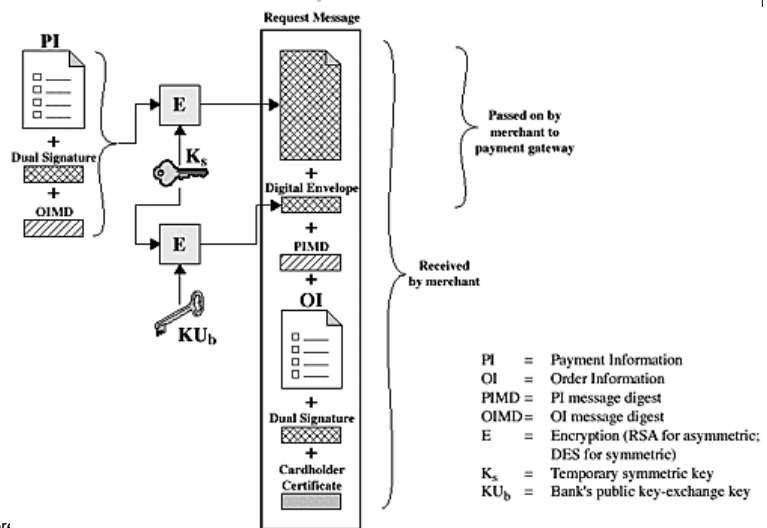
- Il pagante verifica la validità del certificato fornito dal pagato
  - Autenticazione del mercante
- Invia al pagato il proprio certificato insieme agli estremi del contratto
  - Autenticazione del compratore
- Il pagato verifica la validità del certificato del pagante e verifica la copertura della spesa
  - Il venditore non sa il numero di carta di credito
- Se la spesa è coperta la transazione commerciale ha luogo

## SET in pratica / 1



PI = Payment Information      PIMD = PI message digest  
 OI = Order Information        OIMD = OI message digest  
 H = Hash function (SHA-1)    POMD = Payment Order message digest  
 || = Concatenation            E = Encryption (RSA)  
                                          KR<sub>c</sub> = Customer's private signature key

## SET in pratica / 2



PI = Payment Information  
 OI = Order Information  
 PIMD = PI message digest  
 OIMD = OI message digest  
 E = Encryption (RSA for asymmetric;  
       DES for symmetric)  
 K<sub>s</sub> = Temporary symmetric key  
 KU<sub>b</sub> = Bank's public key-exchange key

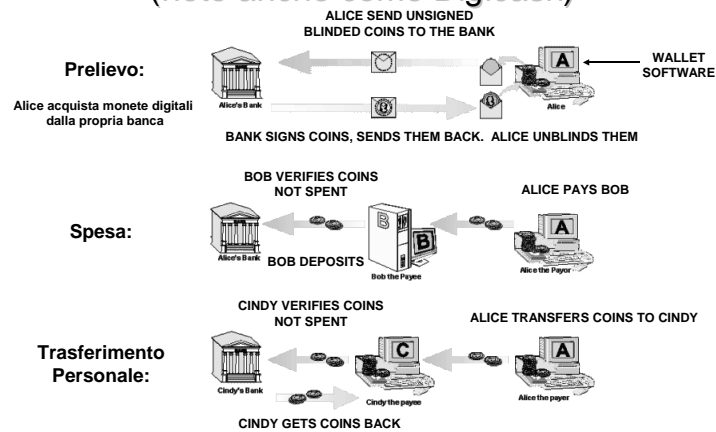
## Electronic Cash

- La moneta elettronica è simile alla moneta circolante:
  - E' in forma digitale
  - Può essere quindi copiata
- Nuovo problema:
  - La copia di una banconota è un reato di falsificazione
  - Ma la copia di una stringa di ecash non è un falso
- Come si emette? come si spende?
- E la falsificazione? e la perdita?
- Frodi, uso in attività criminali, doppia spesa,
- Efficienza (utilizzo offline?)
- Anonimato
- Ad esempio: [www.ecash.com](http://www.ecash.com)

## Electronic Cash

- Idea
  - La Banca emette una stringa binaria che contiene:
    - valore della moneta
    - numero di serie
    - ID banca
    - il tutto crittografato
  - La prima persona che restituisce la stringa alla banca incassa il valore
- Problema
  - Non si può usare offline. Bisogna verificare che la moneta non sia già stata spesa
  - Manca l'anonimato, le banche possono registrare il numero di serie.
  - Intercettazione sulla rete

## eCash (noto anche come Digicash)



## Pagamenti peer-to-peer

- Pagamenti "direttamente" tra consumatori che hanno conti accesi presso terze parti fidate
  - PayPal
    - Consente ad un utente di inviare denaro a chiunque abbia un indirizzo e-mail
    - Può essere usato per consentire pagamenti via CC in tempo reale, riducendo quindi il rischio di frode o di sovra-addebito del conto corrente (v. aste)
  - BillPoint
    - Consente ad un compratore di inviare pagamenti elettronici a conti bancari di venditori

## Micropagamenti

- Pagamenti di piccolissima entità (0.01\$ - 10\$)
  - Molti pagamenti in breve sequenza (CAFE)
  - Pagamenti a molti venditori diversi (Minipay)
  - Es. accesso a tempo, pay-per-click, ...
- Problemi
  - Margine di riscossione molto basso
  - Minimo uso di crittografia
  - Utilizzo di funzioni di hash

## Problemi dei micropagamenti

### Costo della transazione online

- Il sistema di pagamento con costo minore (PayPal), addebita un costo per transazione di 30¢, più (in media) il 2% del totale:
  - 32¢ per il primo dollaro
- con PayPal, una transazione di 32¢ darebbe ad un sito un netto di 1¢, generando invece 31¢ per PayPal.
- Amazon Honor System per piccole quantità si comporta meglio:
  - 15¢ per transazione più il 15% del totale.
  - la più piccola transazione in attivo sarebbe di 19¢, generando un attivo di solo 1¢

## Problemi dei micropagamenti

### Problema psicologico

- Gli utenti sono da sempre abituati a scaricare file MP3 e a visitare siti web senza pagare nulla
- Occorre convincere gli utenti che il contenuto proposto vale il prezzo richiesto

## Problemi dei micropagamenti

### Valuta

- Il Web è globale
  - Un qualsiasi sistema di micropagamenti deve lavorare a livello internazionale
- Il sistema deve consentire agli utenti di qualsiasi nazionalità di interagire agevolmente...
  - ...A prescindere dal fatto che i micropagamenti siano espressi in dollari, Euro, o in una valuta Internet creata appositamente (Microbits? WebCents? ePesos? InterPennies?)

## Pagamenti con dispositivi mobili

- Trasferimento di valore monetario da un pagante ad un pagato usando reti mobili
- Mobile Payment Service Providers
  - Banche / Compagnie di Carta di Credito / Dedicated Payment Processors
  - Network Operators
    - Identified Customers
    - Prepaid Customers

## In Italia...

- BankpassMobile
  - È un servizio della famiglia Bankpass che consentirà di trasferire denaro tra 2 utenti di tipo consumer o business attraverso l'invio di un messaggio sms
- Mobilmat
  - Servizio di Banca Sella e Wind
  - Ha un costo di attivazione di 15 euro per il primo anno e di 3 euro per i 2 anni successivi
  - Pagamento Ebay.it, taxi, distributori automatici, ...

## Siemens Pay@Once

- Il cliente si collega al centro di pagamento digitando il numero che compare sul distributore automatico
- Il centro di pagamento contatta il distributore automatico e lo informa che il cliente può acquistare il prodotto
- Una volta selezionato il prodotto, il centro di pagamento viene notificato
- Il cliente paga con la bolletta del telefono un costo fisso (chiamata) più il costo del prodotto



## Conclusioni

- il pagamento tramite Carta di Credito è il più comune
  - Problemi crescenti di frode con lo schema attuale di pagamento (SSL + normale carta di credito)
  - Per il momento le banche non hanno interesse a promuovere schemi alternativi
- La privacy è sempre di più un aspetto chiave
- Paypal sembra dominare nel settore dei pagamenti tra individui
- Presenza di molte transazioni potenziali che cadono al di qua della soglia per le carte di credito
  - micropagamenti?
- Molte soluzioni ad hoc proposte
  - Non c'è per ora un chiaro vincitore