Sistemi di Pagamento Elettronico

Moreno Marzolla
INFN Sezione di Padova
moreno.marzolla@pd.infn.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 sè (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

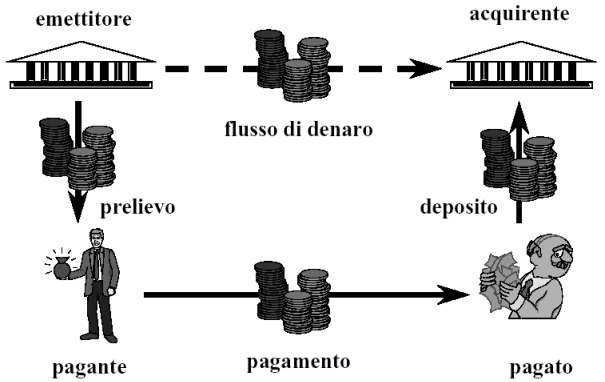
Attori

- 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

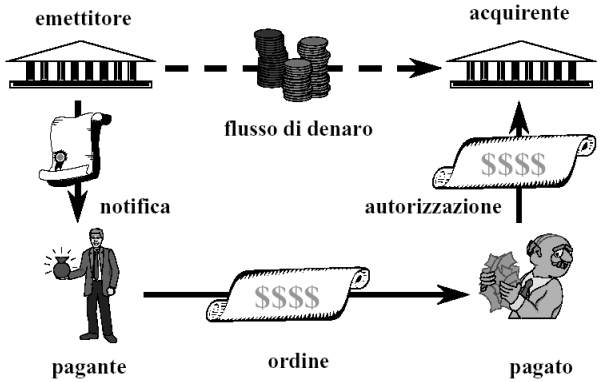
Finalità del sistema

- Consentire al pagato di ottener 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

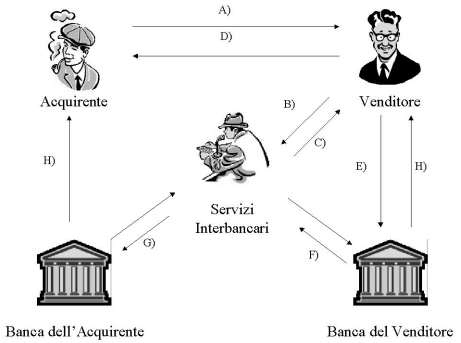
Definizione

- 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 cadenze 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

A) l'acquirente presenta la carta di credito al venditore (non sempre: ad esempio ordini telefonici o via Internet)
B) il venditore utilizza la carta di credito per richiedere l'autorizzazione a procedere
C) la Rete Interbancaria autorizza la transazione
D) il venditore produce una nota di vendita contenente tutte le informazioni di rilievo sulla transazione e ne consegna una copia al cliente
E) 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)
F) la banca del venditore accredita sul conto corrente del venditore l'importo relativo alla transazione e notifica i servizi interbancari,
G) 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),
H) 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

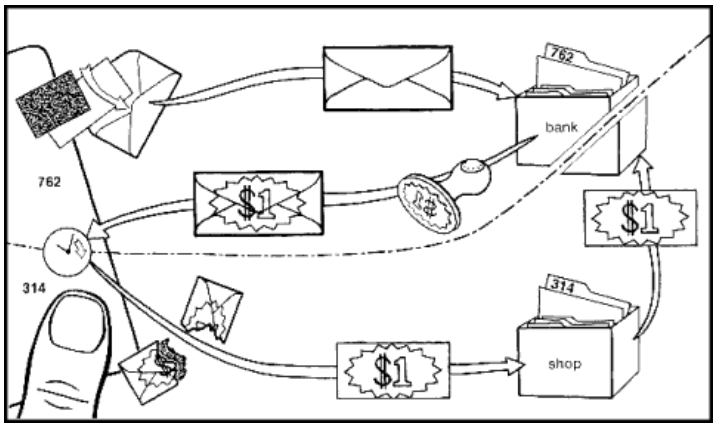
- Transazioni atomiche
  - Il sistema deve impedire perdite dovute ad interruzioni o malfunzionamenti
- Recupero da situazioni critiche
- Supporto di comunicazione affidabile

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

Transazioni economiche anonime

http://www.chaum.com/articles/Security_Wthout_Identification.htm



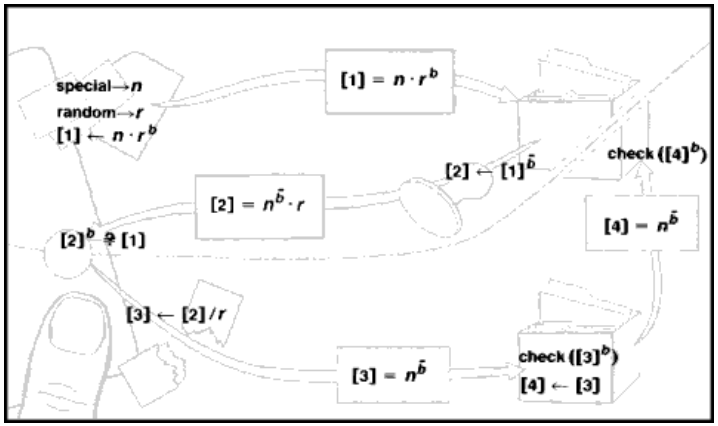
Transazioni economiche anonime

http://www.chaum.com/articles/Security_Wthout_Identification.htm

- *"UNTRACEABLE PAYMENTS are illustrated by an analogy to envelopes and carbon paper. The individual (or, in the computerized analogue, the card) seals a blank slip of paper and a facing piece of carbon paper in an envelope, and supplies it to the bank. The bank deducts one dollar from the individual's account, applies a "worth one dollar" signature (stamp) to the outside of the envelope, and returns the unopened envelope to the individual. Upon receiving this, the individual verifies the bank's validating signature. Before making payment sometime later, the individual removes the envelope and carbon, leaving only the signed slip of paper. When the shop receives the slip, it verifies the carbon image of the validating signature on the slip, and supplies it to the bank for deposit. After also verifying the slip's validating signature, the bank honours the deposit, since it knows the slip must have been in an envelope it signed. The bank does not, however, know which of the many envelopes that it signed contained the slip, and thus the bank cannot trace the slip to the Individual's account. In actual computerized systems, unless the individual allows tracing, withdrawals on one side of the dashed boundary line and payments on the other side of it are unconditionally untraceable to each other-even if the bank and all other organizations collude."*

Transazioni economiche anonime

http://www.chaum.com/articles/Security_Wthout_Identification.htm



Transazioni economiche anonime

http://www.chaum.com/articles/Security_Wthout_Identification.htm

- UNTRACEABLE PAYMENTS WITH NUMBERS are made much as in the paper analogy. First the individual's card computer chooses half the digits of n by a physical random process, and repeats these digits (actually in a scrambled form) to create the note number n with this special repeated-halves property (corresponding to choosing a suitable slip of paper at random in the analogy). The card also creates a totally random number r (like choosing an envelope and carbon). The card then raises the random number r to the bank's "worth one dollar" public power b, multiplies this by the note number n (like sealing the slip in the envelope), and supplies the result to the bank in transmission [1]. The bank deducts from the account uses the corresponding private power b' to sign the transmission, and returns the result to the card in [2]. The card verifies that the bank returned exactly the right thing, and obtains the signed note by dividing out the random r (like removing the envelope and carbon). When a payment is made, the shop checks that transmission [3] is a signed special number, and then forwards a copy [4] to the bank for deposit. The bank checks the signature just as the shop did, and accepts the deposit if the valid note has not already been deposited. If Individuals do not divulge the random r's their cards create, then the [1]'s are unconditionally untraceable to the [4]'s, since there is exactly one r that would make any [2] correspond with any [4].

SET
Secure Electronic Transaction

- Standard per il pagamento elettronico con carte di credito
- Obbiettivi di SET
  - Cifrare informazioni critiche inviate su Internet
  - Separare il venditore dalle informazioni sulla carta di credito
  - Collegare le informazioni sul pagamento con quelle relative all'acquisto

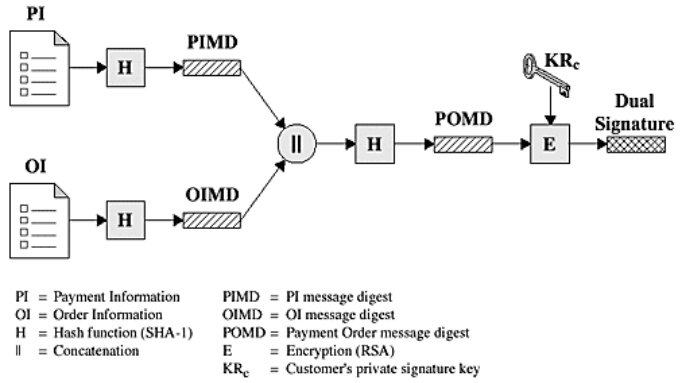
SET

- 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: esempio

- Alice: colei che deve pagare (il cliente)
- Bob: colui che deve essere pagato (il venditore)
- PG: Payment Gateway

SET in pratica / 1



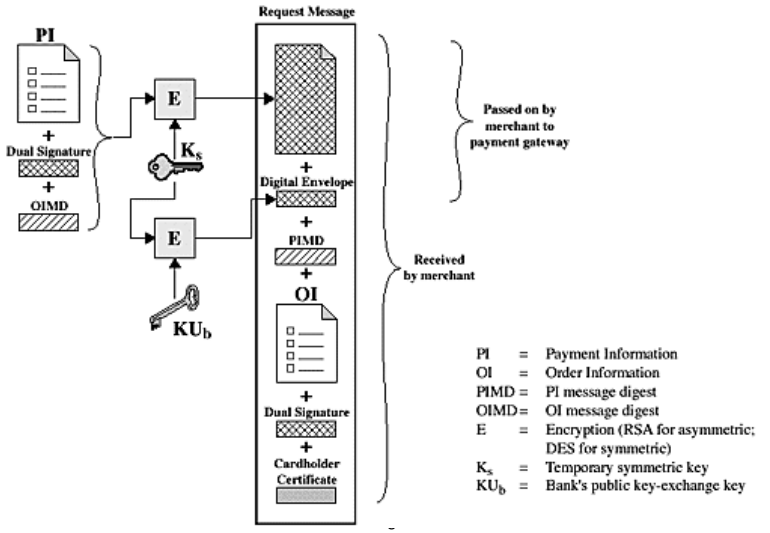
A che serve la “dual signature”?

- Bob può dimostrare che Alice ha pagato proprio per il prodotto X e non Y
- Bob conosce:
  - OI (Order Information)
  - Dual Signature = Krc[H(H(PI) || H(OI))]
  - PIMD
  - Chiave pubblica di Alice
- Krc[H(H(PI) || H(OI))]
  - Decifrando con la chiave pubblica di Alice ottiene H(H(PI) || H(OI))
  - Conosce già PIMD = H(PI)
  - Può calcolare H(OI) perché conosce OI

A che serve la “dual signature”?

- Dimostra al PG che Alice ha pagato Bob
- PG conosce
  - PI (Payment Information)
  - Dual Signature = Krc[H(H(PI) || H(OI))]
  - OIMD
  - Chiave pubblica di Alice
- Krc[H(H(PI) || H(OI))]
  - Decifrando con la chiave pubblica di Alice ottiene H(H(PI) || H(OI))
  - Conosce già OIMD = H(OI)
  - Può calcolare H(PI) perché conosce PI

SET in pratica / 2



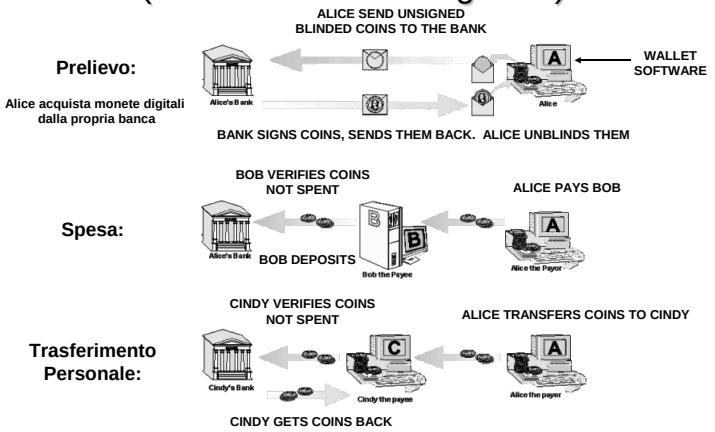
Electronic Cash

- 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

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)

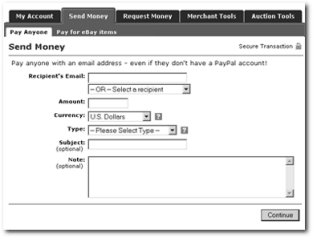


Pagamenti peer-to-peer

- 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

PayPal: funzionamento / 1

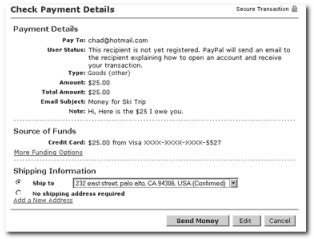
- 1. L'utente seleziona l'opzione per inviare denaro



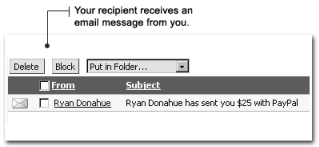
- 2. E' possibile prelevare i fondi da una carta di credito o dal proprio conto bancario

PayPal: funzionamento / 2

- 3. Il pagante verifica gli estremi del pagamento, prima di confermarlo



- 4. Il pagato riceve una mail che lo avvisa che la somma è disponibile



PayPal: funzionamento / 3

- 5. Se il pagato non possiede già un conto PayPal, ne deve aprire uno

- 6. Il pagato può decidere di trasferire i fondi sul proprio CC bancario, ricevere un assegno o girarli a qualcun altro

PayPal: costi (febbraio 2006)

	Personal Account	***Premier/Business Account***
Open an Account	Free	Free
Send Money	Free	Free
Withdraw Funds	Free in US banks	Free US banks
Add Funds	Free	Free
Receive Funds	Free	1.9% to 2.9% + $0.30 USD

Micropagamenti

- Pagamenti di piccolissima entità (0.01$ - 10$)
- Problemi
  - Margine di riscossione molto basso
  - Costo della transazione
  - Problema psicologico. La gente scarica mp3 gratuitamente: occorre convincere la gente che il contenuto vale il prezzo richiesto
  - Problema di valuta: il WEB è globale, che valuta utilizzare?

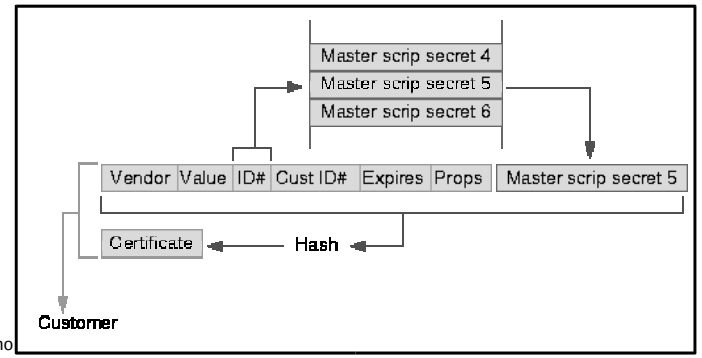
Millicent

http://www.w3.org/Conferences/WWW4/Papers/246/

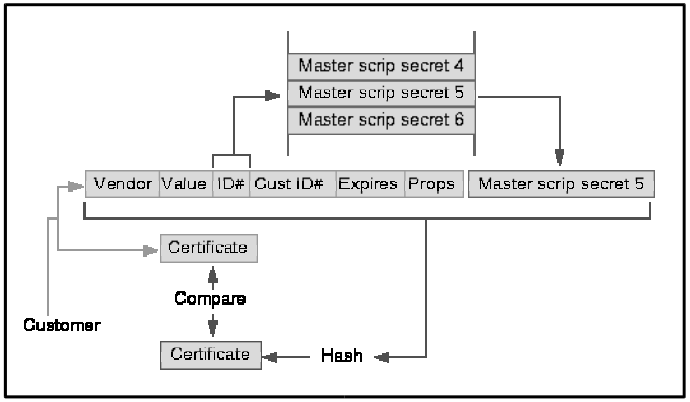
- Scrip: The main properties of scrip are:
  - It has value at a specific vendor.
  - It can be spent only once.
  - It is tamper resistant and hard to counterfeit.
  - It can be spent only by its rightful owner.
  - It can be efficiently produced and validated.
- Basic techniques
  - The text of the scrip gives its value and identifies the vendor.
  - The scrip has a serial number to prevent double spending.
  - There is a digital signature to prevent tampering and counterfeiting.
  - The customer signs each use of scrip with a secret that is associated with the scrip.
  - The signatures can be efficiently created and checked using a fast one-way hash function (like MD5 or SHA).

Scrip / emissione

- Vendor identifies the vendor for the scrip.
- Value gives the value of the scrip.
- ID# is the unique identifier of the scrip. Some portion of it is used to select the master_scrip_secret used for the certificate.
- Cust_ID# is used to produce the customer secret. A portion of Cust_ID# is used to select the master_customer_secret which is also used in producing the customer secret.
- Expires is the expiration time for the scrip.
- Props are extra data describing customer properties (age, state of residence, etc.) to the vendor.
- Certificate is the signature of the scrip.



Scrip / validazione



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
  - non ancora attivo
- 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