Pagamenti elettronici

Gianluca Dini

Dipartimento di Ingegneria dell'Informazione: Elettronica, Informatica, Telecomunicazioni

University of Pisa

gianluca.dini@ing.unipi.it

Concetti Generali

Pagamenti elettronici

- Il momento del pagamento è il cuore del commercio
- Nel commercio elettronico anche il pagamento deve avvenire "in rete"
- La sicurezza di una transazione di pagamento elettronico è un problema centrale

Costo di una transazione

costo di una transazione

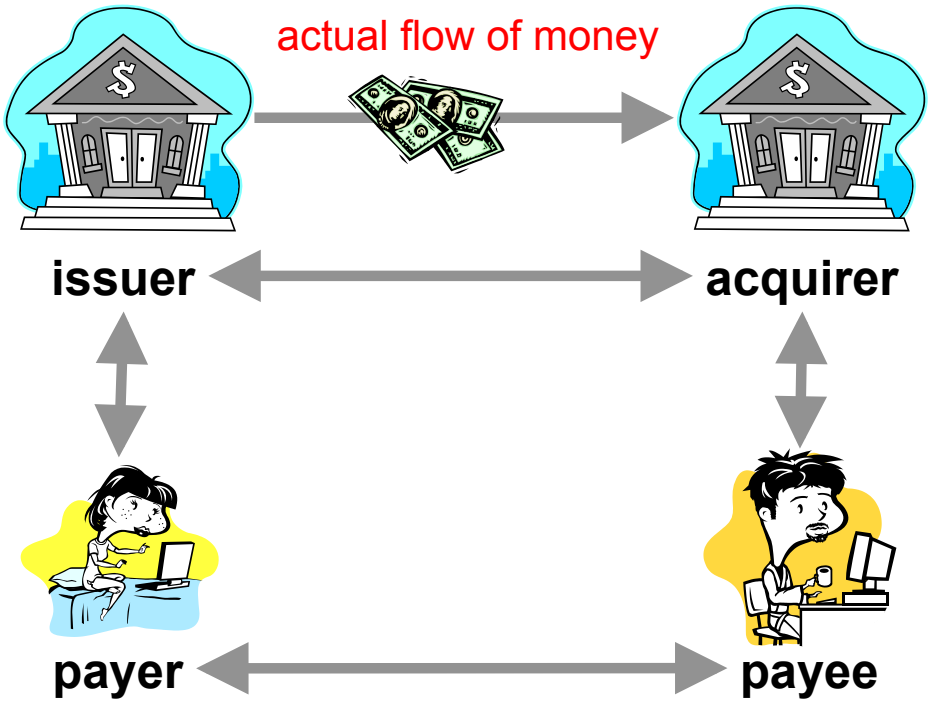
Branch	**$1.07**
Telephone	**$0.52**
Automated Teller Machine	**$0.27**
PC banking	**$0.015**
Internet banking	**$0.01**

Booz-Allen & Hamilton, "Survey of North American financial institutions," *The Emerging Digital Economy*, U.S. Dept. of Commerce, 1998

- interessi più alti nei conti on-line: la pressione del mercato spinge le banche a dividere con i clienti i risparmi di gestione
- né i clienti né i media prestano attenzione all'allocazione del rischio che si ha passando da un conto tradizionale ad Internet banking

Sistema di pagamento

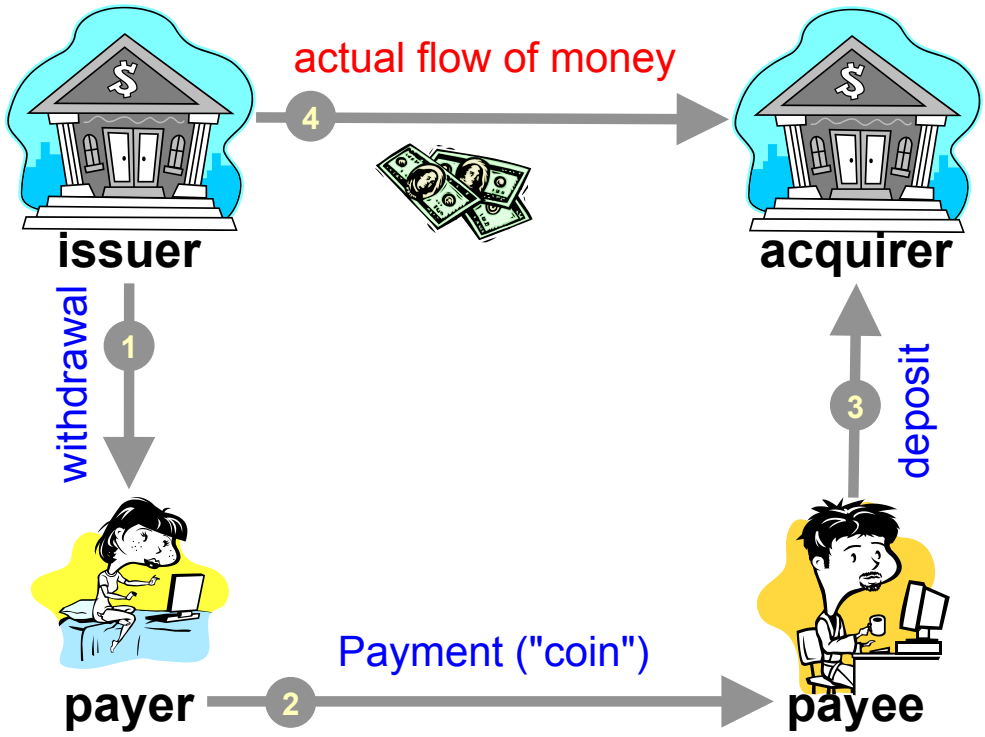
Concetti Generali



Sistemi di pagamento

- **Sistemi di pagamento diretti**
  - Un pagamento richiede un'interazione diretta tra payer e payee
  - Moneta, carta di credito, bancomat
- **Sistema di pagamento indiretto**
  - Un pagamento non richiede un'interazione diretta tra payer e payee
  - **Electronic Funds Transfer**
- I sistemi EFT sono basati su **reti proprietarie**
- I sistemi di pagamenti su Internet sono basati su **reti aperte**

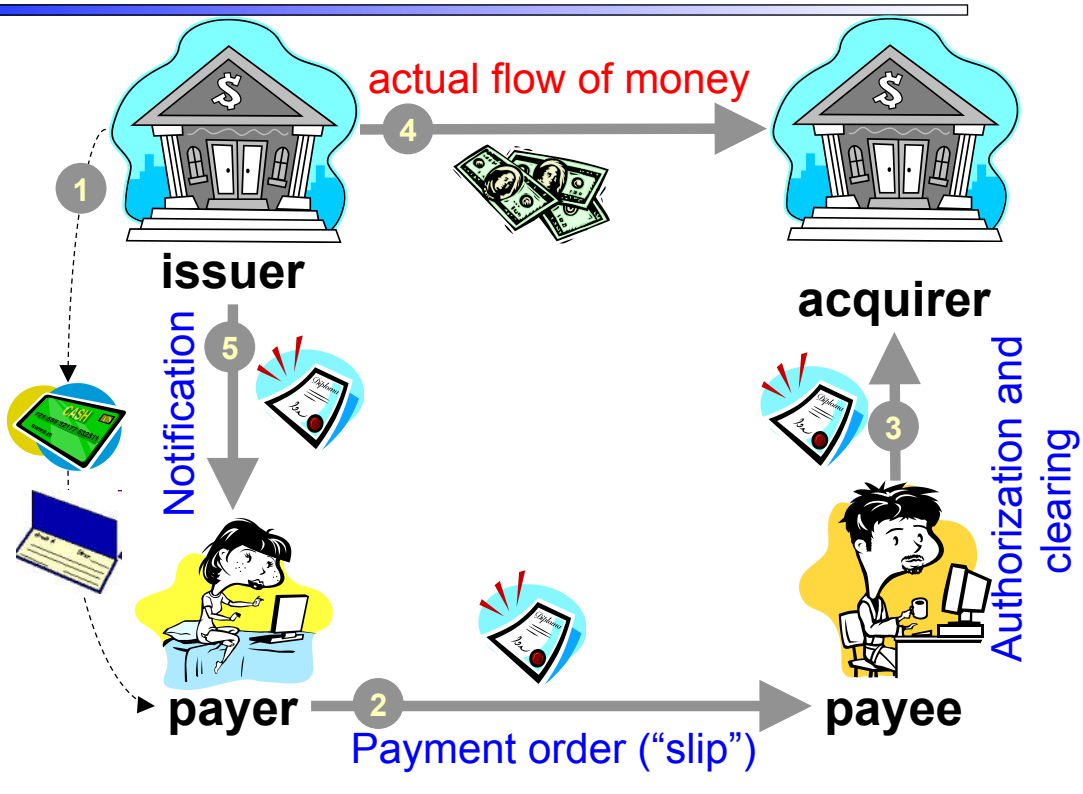
Sistema di pagamento "cash-like"



Sistemi di pagamento cash-like

- Borsellini elettronici basati su smart card
- Moneta elettronica
- Certified checks

Sistema di pagamento “check-like”



Sistemi di pagamento “check-like”

- **Pay-now system**
  - L’addebito al payer viene eseguito al momento del pagamento
    - ✓ **Bancomat (Automatic Teller Machine)**
- **Pay-later system**
  - L’accredito al payee viene eseguito prima dell’addebito al payer
    - ✓ **Carte di credito**

Requisiti

- Disponibilità
- Affidabilità
- Economicità
- Ubiquità/accettabilità
- Facilità d’uso
- Efficienza
- Sicurezza

Requisiti di sicurezza

Concetti Generali

- Autenticazione ed integrità del pagamento
- Autorizzazione del pagamento
- Non-ripudio del pagamento
- Privacy del pagamento
- Audit-ability del pagamento

Requisiti di sicurezza

Concetti Generali

- Autenticazione ed integrità
  - autenticazione dei partecipanti (non sempre necessaria)
  - integrità dei dati e dei messaggi
- Autorizzazione

  Nessuno può addebitare (accreditare!) del denaro ad un utente senza un'autorizzazione esplicita dell'utente
  - Out-of-band authorisation (carta di credito)
  - Password authorisation
  - Signature authorization
- Audit-ability
  - provare la correttezza del sistema
  - risoluzione delle dispute
    - ✓ tecniche di logging

Requisiti di sicurezza

Concetti Generali

- **Non-ripudio**
  - Capacità di provare ad **una terza parte fidata** e disinteressata che una transazione è effettivamente avvenuta, rendendo impossibile, per ciascuna parte, il ripudio o la negazione della validità o dell'esistenza della transazione stessa.
- **La firma digitale è il meccanismo base per garantire il non-ripudio**

Requisiti di sicurezza

Concetti Generali

- **Privacy del pagamento**
  - **Confidenzialità**.

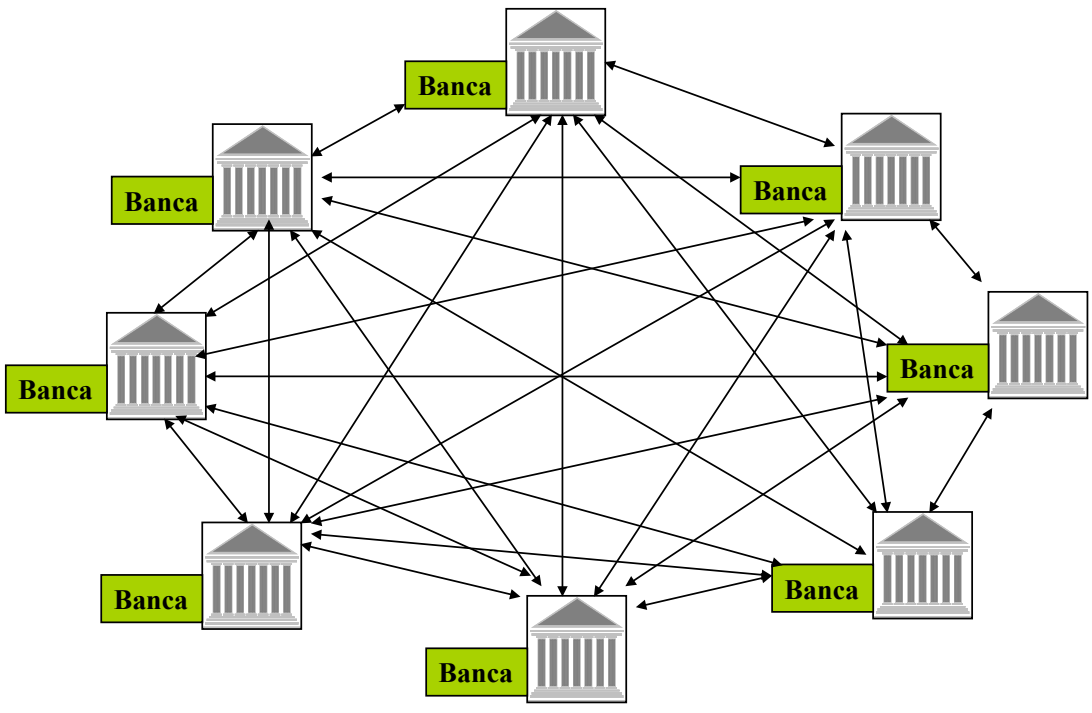
    I dettagli del pagamento (payer, payee, account numbers, amounts, date, and time, payment subject, etc.) non devono essere noti ad un outsider
  - **Anonimato**
    - ✓ **Payer anonimity**. non è possibile conoscere l'identità del payer (pseudonimi)
    - ✓ **Payer untraceability**. non è possibile ricollegare due pagamenti dello stesso payer
    - ✓ **Livello di anonimato.** Anonimity/untraceability può essere rispetto a: una terza parte (outsider), il payee, l'issuer, …

Sistemi di pagamento elettronico

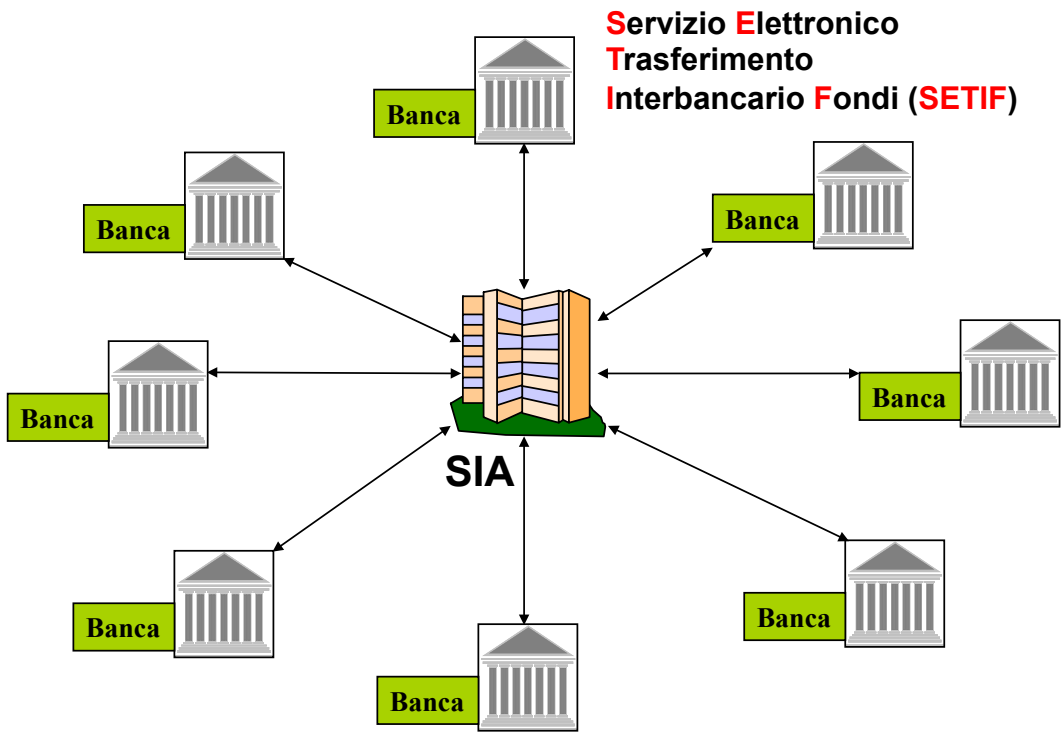
- ✓ **inquadramento storico**
- ✓ **bancomat, POS e carta di credito**

La situazione prima del 1977

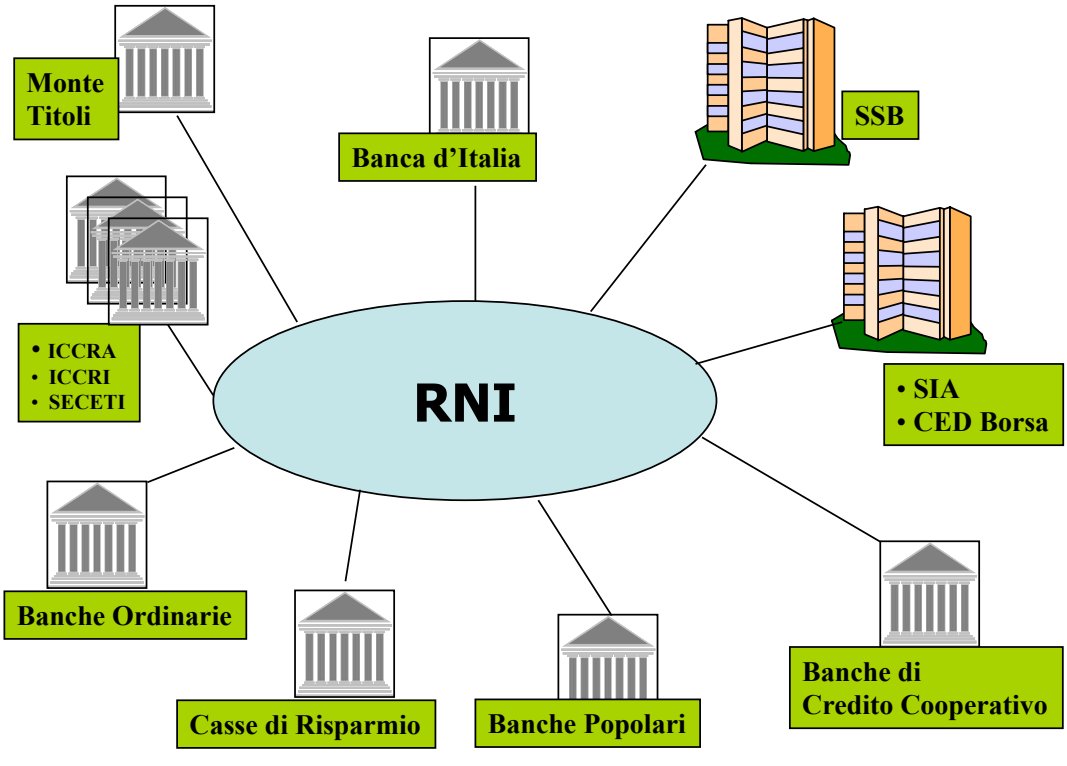
Inquadramento storico



Società Interbancaria per l'Automazione



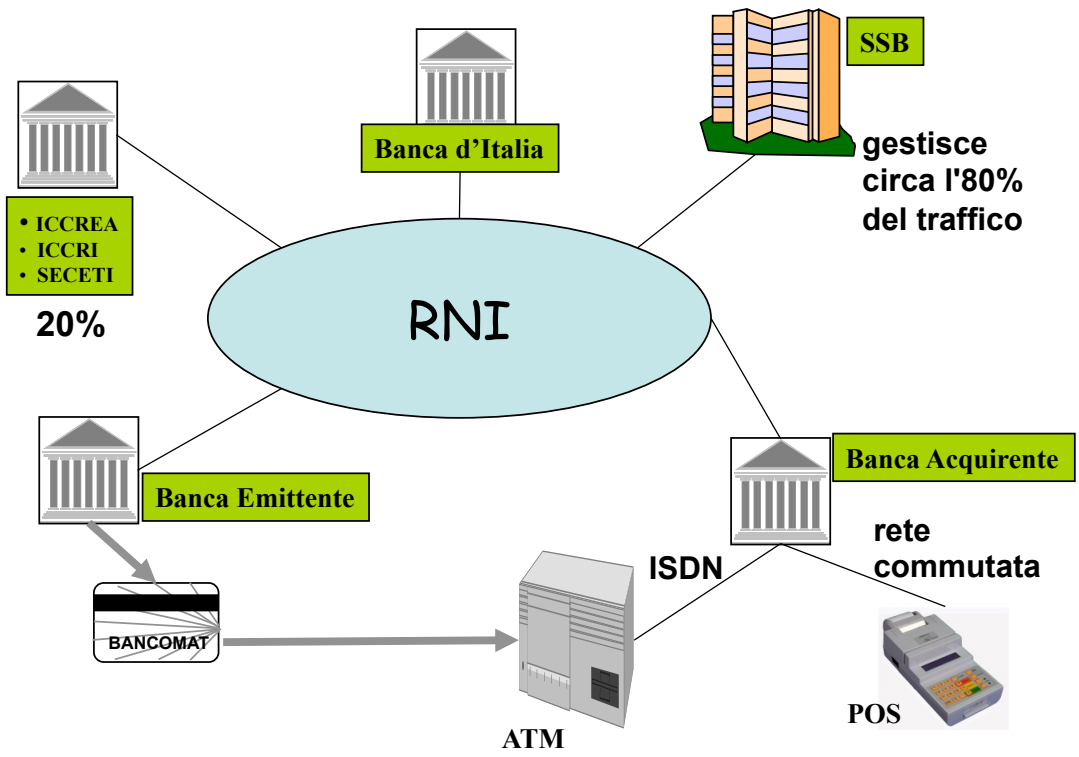
La Rete Nazionale Interbancaria



Il bancomat: obiettivi

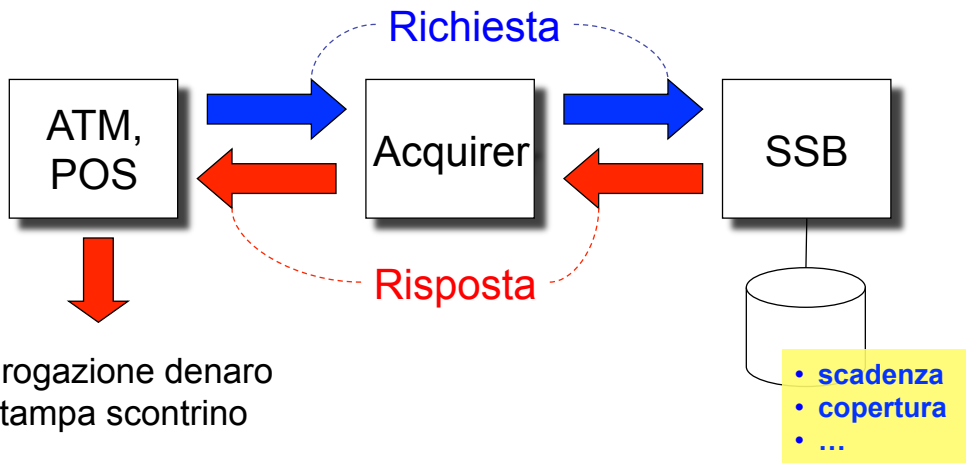
- Abituare la clientela ad operazioni self-service
- Evitare il contante
- Fornire un servizio di prelievo a basso costo
- Sostituire lo “sportellista” con il “consulente”

Il bancomat: architettura di rete



Il bancomat: autorizzazione

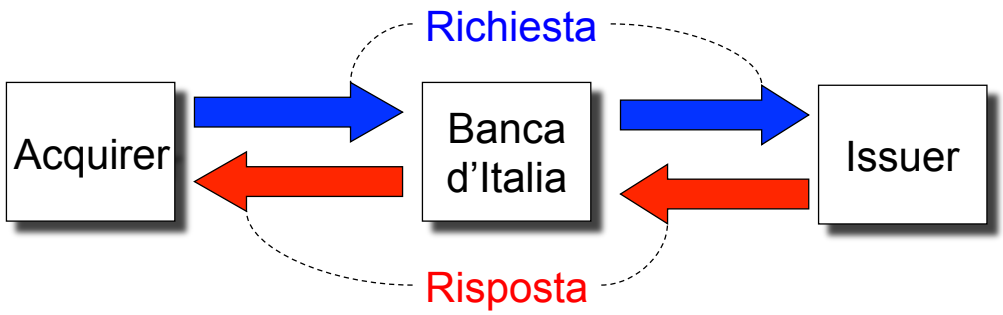
Caso generale: Issuer ¥ Acquirer



- SSB verifica che la carta non sia scaduta, che ci sia la copertura,…

Il bancomat: compensazione

Caso generale: Issuer ≠ Acquirer



- Attraverso la Banca d'Italia l'Acquirer invia all'Issuer una richiesta di accredito ed il conseguente addebito sul conto del titolare

Il bancomat: note

Il bancomat

- Le banche operano il proprio bancomat in locale
  - Due plafond per ogni carta
- La SIA gestisce la centrale allarme nazionale
  - L'utente fa una segnalazione a SIA e questa informa SSB e l'Issuer
- Gli enti autorizzatori
  - CEDACRI, SECETI, SETEFI, SITEBA, MULTITEL, SSB, … gestiscono il traffico POS per conto delle banche

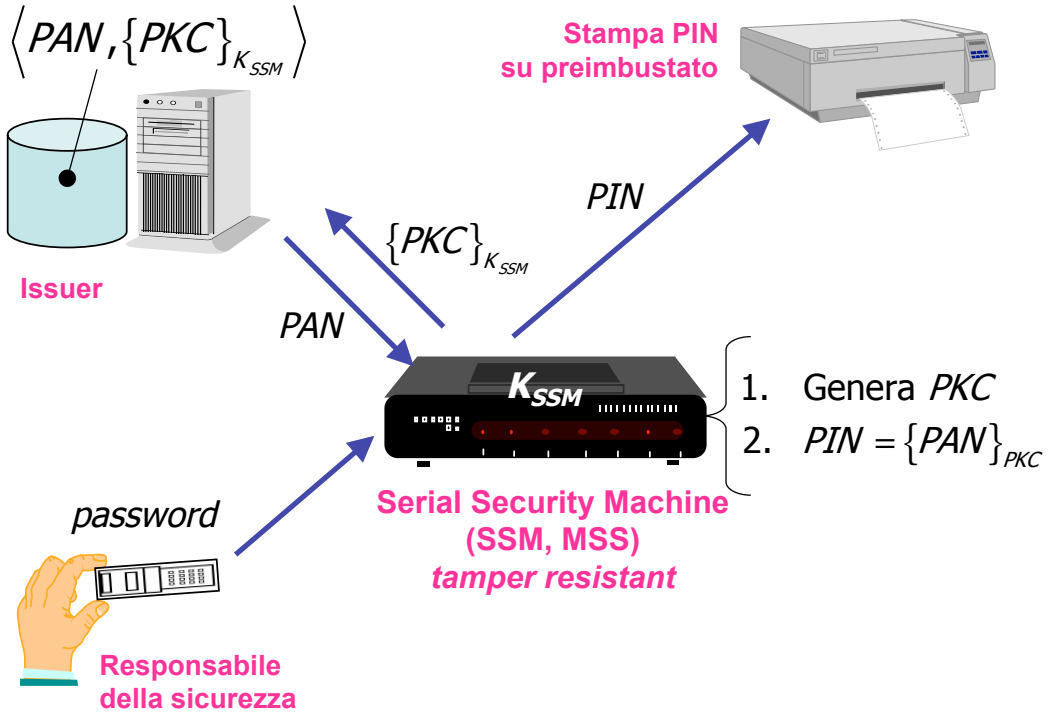
Le quantità di sicurezza

Il bancomat

- Primary Authentication Number (PAN)
  - costituito da 18 caratteri e posto sulla carta
    - ✓ABI (5 char)
    - ✓Codice (12 char)
    - ✓Check digit (1 char)
- Personal Identification Number (PIN)
- Pin Key Card (PKC)
  - **chiave di cifratura** utilizzata **per generare il PIN** e **memorizzata presso l'emittente**
  - **ogni carta ha la propria PKC**
  - **PKC è memorizzata nel DB dell'issuer** accanto al PAN

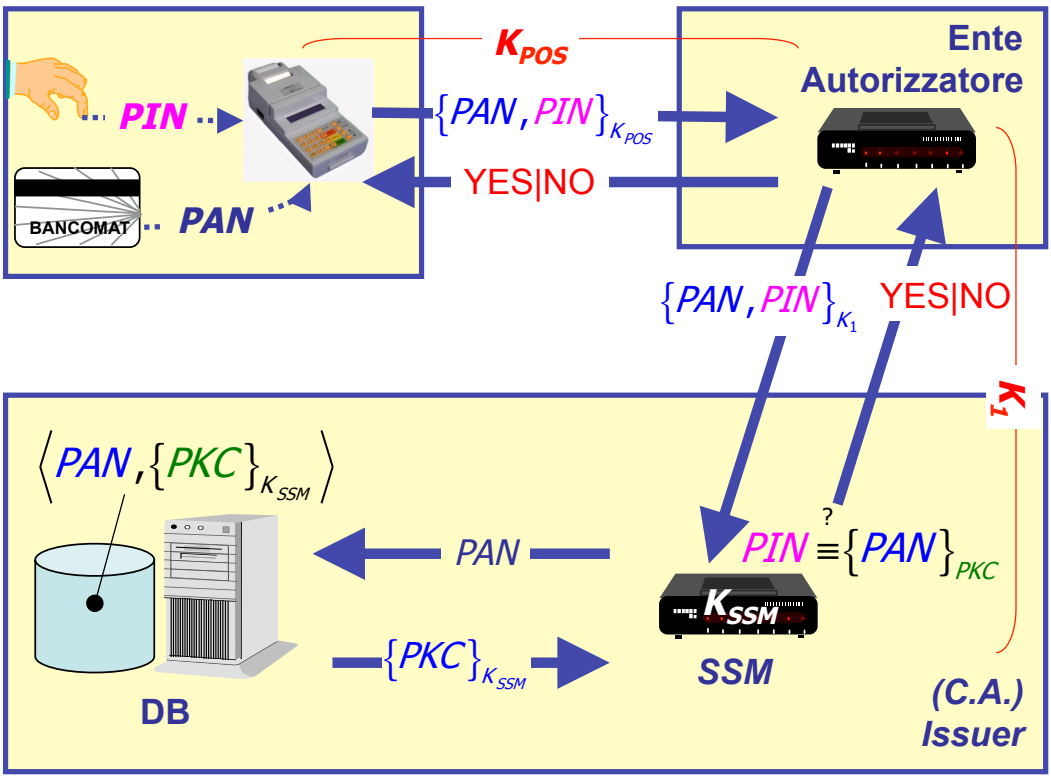
Emissione (schema concettuale)

Il bancomat



Autorizzazione POS (schema concettuale)

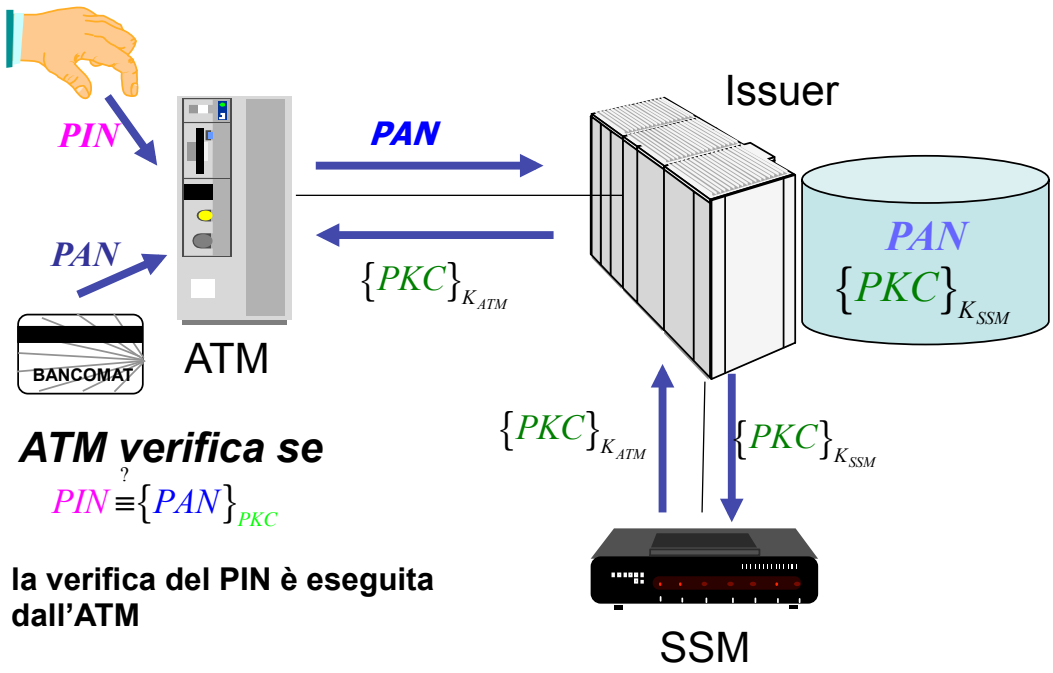
Il bancomat



Il bancomat

Autorizzazione ATM (schema concettuale)

Nel caso che issuer ed acquirer coincidano



ATM verifica se

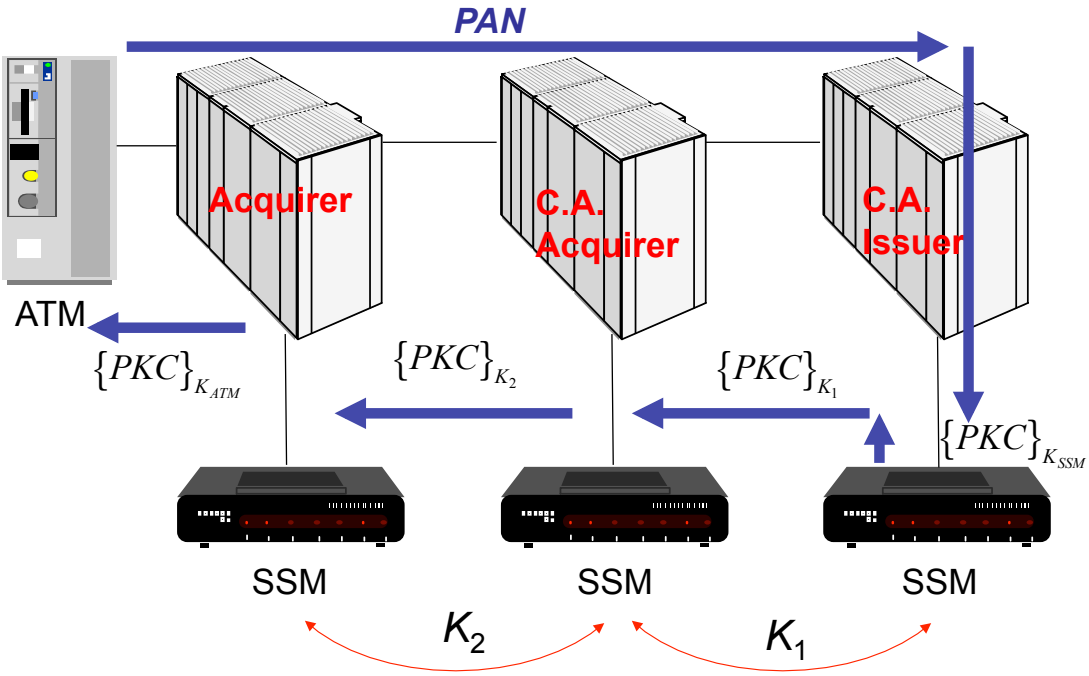
$$PIN \stackrel{?}{\equiv} \{PAN\}_{PKC}$$

la verifica del PIN è eseguita dall'ATM

Il bancomat

Autorizzazione ATM (schema di principio)

Nel caso che issuer ed acquirer non coincidano



Le quantità di sicurezza

- Numero random
  - **Ad ogni prelievo da un ATM**
    - ✓ Issuer/SSB/… genera un numero random ***r*** e lo memorizza sia localmente sia sulla carta (terza pista)
  - **Al prelievo successivo da un ATM**
    - ✓ Issuer/SSB/… verifica la freshness della transazione verificando che il numero random sulla carta ***r*** sia uguale a quello memorizzato localmente ***r***
- Ogni carta ha due numeri random
  - uno per i prelievi su sportelli della banca
  - uno per i prelievi in circolarità

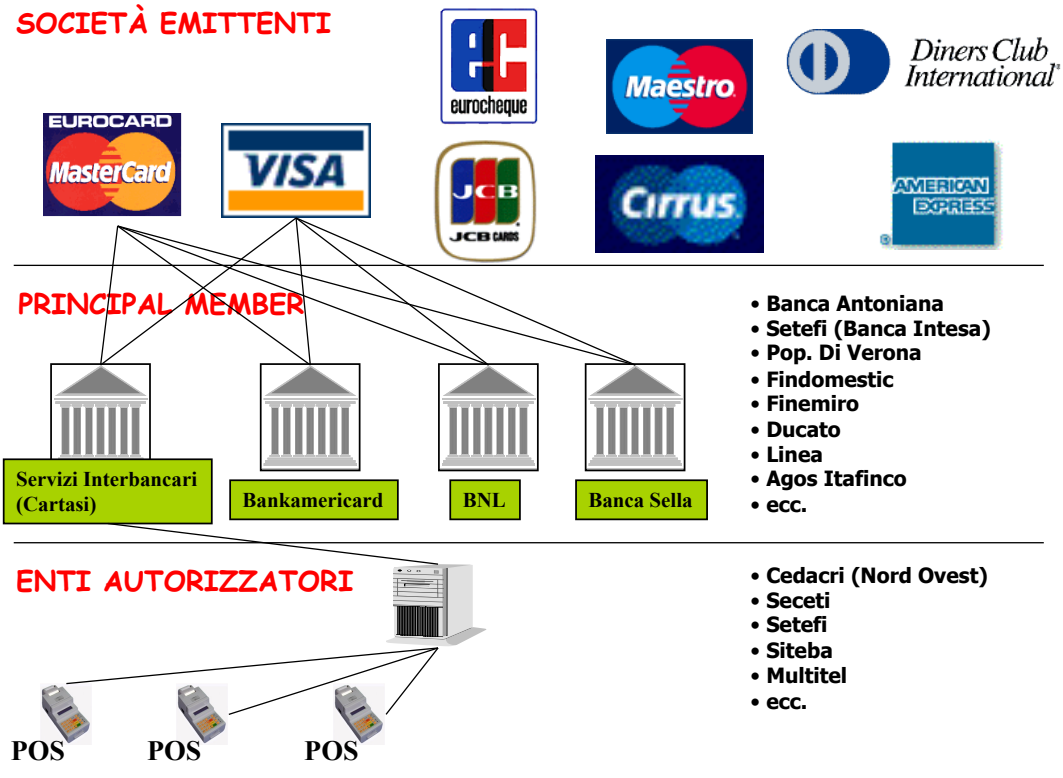
Storia

- **Le carte di credito nascono nel 1920 negli USA**
  - sono emesse da catene alberghiere e compagnie petrolifere
- L'utilizzo incrementa dopo WW II
- La prima **carta universale** viene emessa da **Diners Club Inc.** nel **1958**
- **American Express** nasce nel **1958**
- Nel 1959 nascono i primi circuiti supportati dalle banche
- Nel **1959 Bank of America** lancia **BankAmericard** in California
- Nel **1976** BankAmericard viene rinominata **Visa**
- Successivamente arrivano altri circuiti importanti come **MasterCard**
- Nel **1985** nasca **Carta Si** con il nome Servizi Interbancari

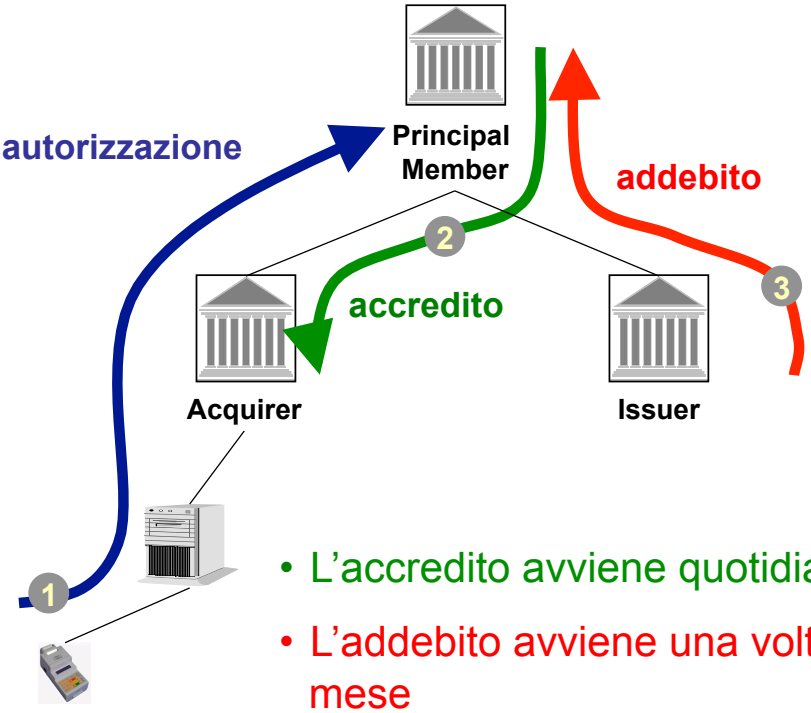
Struttura organizzativa

- Il “mondo” delle carte di credito può essere idealmente suddiviso in tre livelli
- Il livello degli **Enti emittenti** costituiti dai grandi circuiti mondiali (VISA, MC ecc.)
- Il livello dei **Principal member** che hanno il compito di emettere carte e di convogliare le autorizzazioni
- Il livello degli **Enti autorizzatori** rappresentati dai soggetti che connettono fisicamente i terminali POS e tutte le apparecchiature in grado di leggere carte magnetiche e/o a microprocessore

La carta di credito

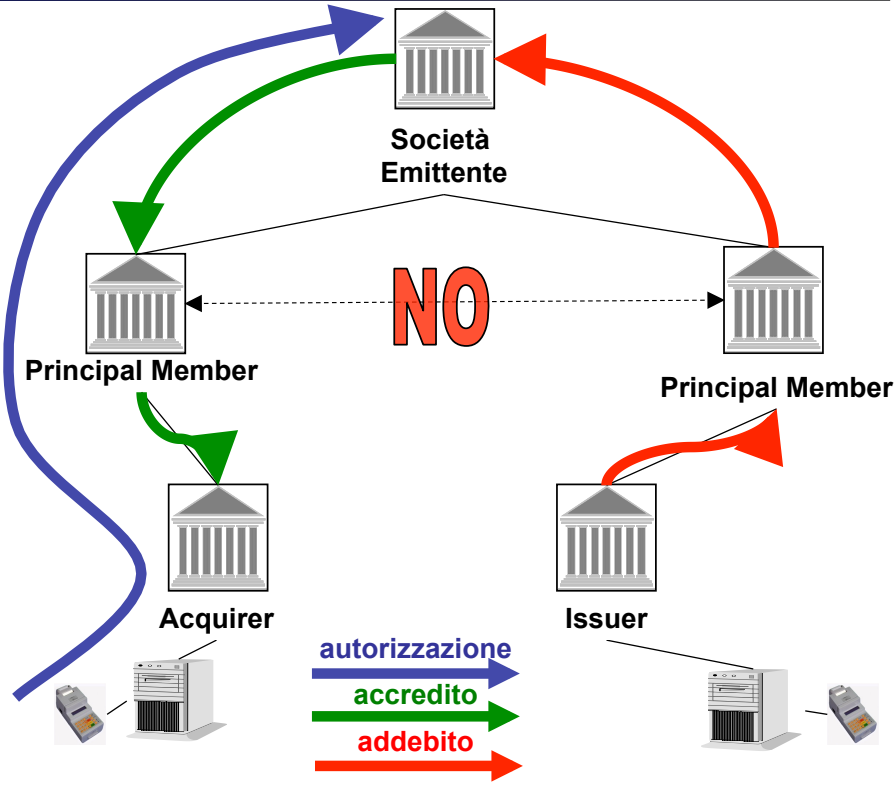


La carta di credito



- L'accredito avviene quotidianamente
- L'addebito avviene una volta al mese

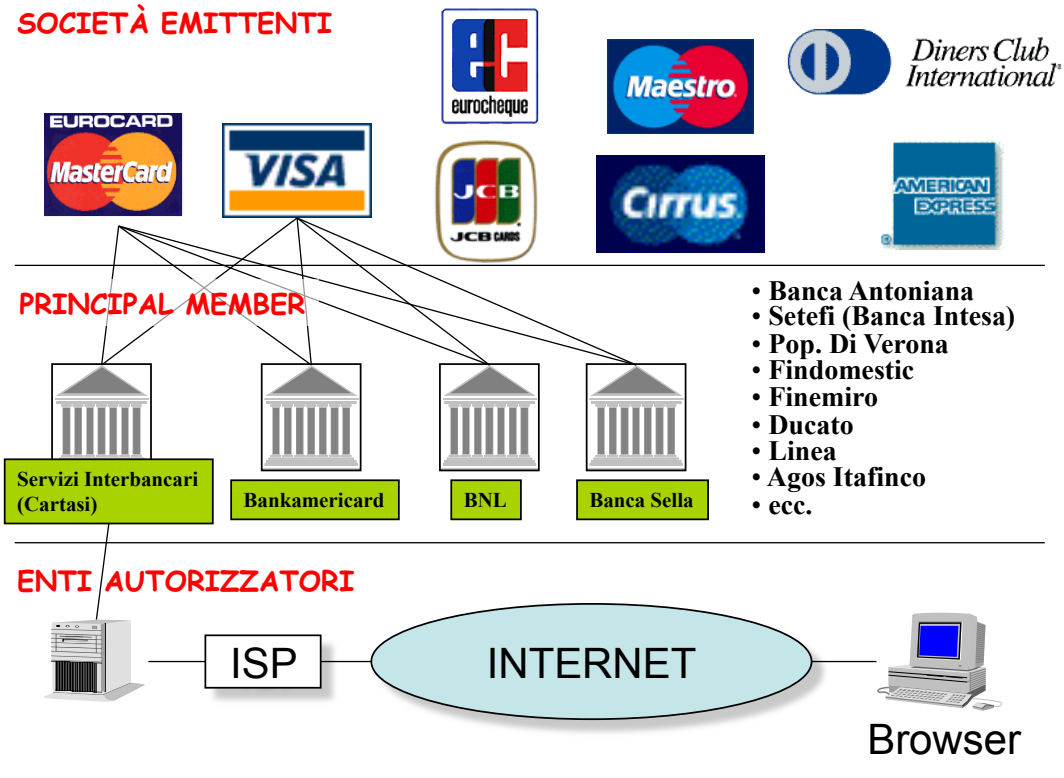
La carta di credito



Spese e guadagni

- **Il titolare della carta**
  - tipicamente non paga commissioni e l'addebito non è immediato (mensile)
  - paga una quota annuale al principal member
  - paga le spese di estratto conto e bolli
- **Il principal member**
  - riceve una commissione dall'esercente per ogni transazione
  - riceve le quote annuali dei titolari
- **L'esercente**
  - paga una commissione al principal member per ogni transazione

La carta di credito in Internet



Il numero della carta di credito

La carta di credito

- **P**rimary **A**ccount **N**umber
- La numerazione delle carte di credito è standardizzata da

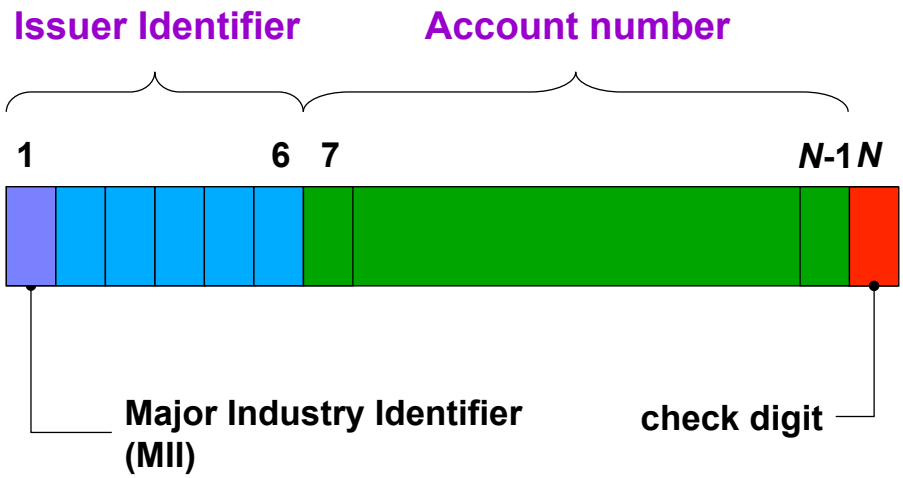
  ISO (ISO/IEC 7812-1: 1993) e da

  ANSI (ANSI X4.13)
  - Queste organizzazioni non distribuiscono le loro pubblicazioni gratuitamente

Il PAN

La carta di credito

- **Il numero di carta di credito è costituito da *N* (< 20) cifre decimali (digit)**



Il PAN: MII

MII	Issuer Category
0	ISO/TC 68 and other industry assignments
1	Airlines
2	Airlines and other industry assignments
3	Travel and entertainment
4	Banking and financial
5	Banking and financial
6	Merchandizing and banking
7	Petroleum
8	Telecommunications and other industry assignments
9	National assignments

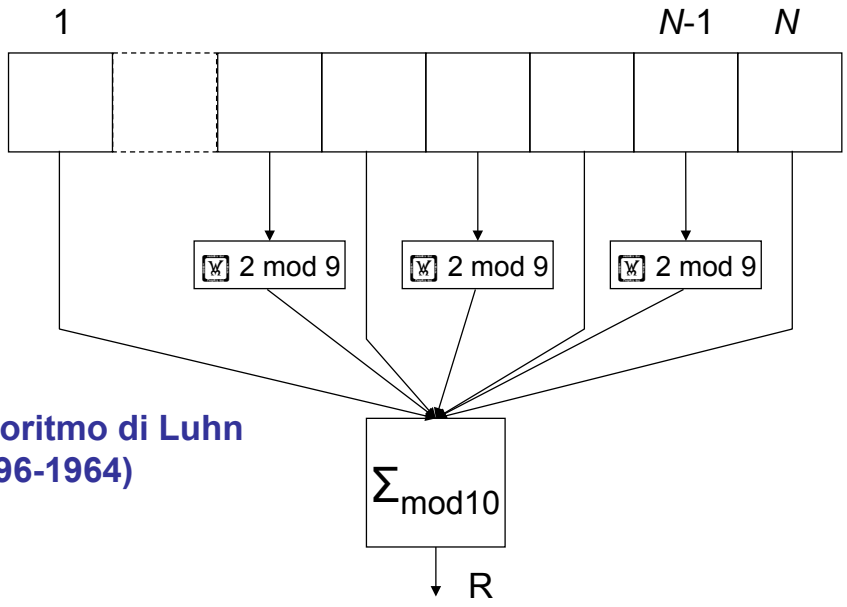
- American Express, Diner's Club sono nella "categoria travel and entertainment"
- VISA, Mastercard e Discover sono nella categoria "banking and financial"

Il PAN: issuer identifier

Issuer	Identifier	Card Number Length
Diner's Club/Carte Blanche	300xxx; 305xxx; 36xxxx; 38xxxx	14
American Express	34xxxx; 37xxxx	15
VISA	4xxxxx	13, 16
MasterCard	51xxxx; 55xxxx	16
Discover	6011xx	16

- Sono possibili, al più,10^6 emettitori e 10^{12} account number
- Se MII = 9, allora l'identifier ha il seguente formato 9CCCNN, con
  - CCC il codice della nazione (ISO 3166)
  - NN il codice dell'issuer secondo gli standard nazionali

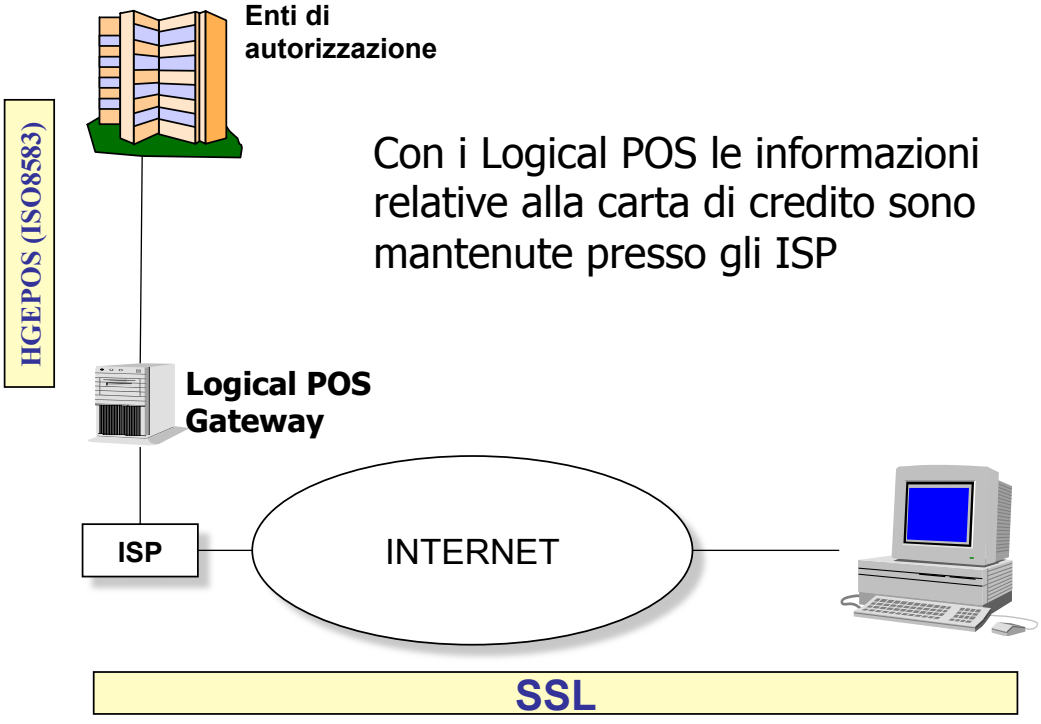
Il PAN: check digit



Algoritmo di Luhn (1896-1964)

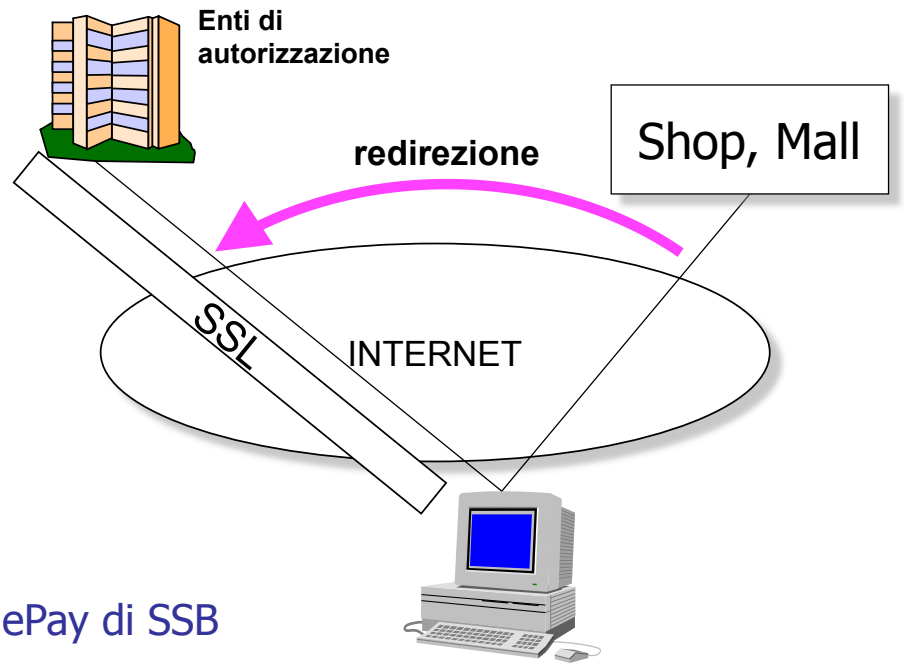
se R == 0, allora il numero è valido

I logical POS



Con i Logical POS le informazioni relative alla carta di credito sono mantenute presso gli ISP

I Gateway

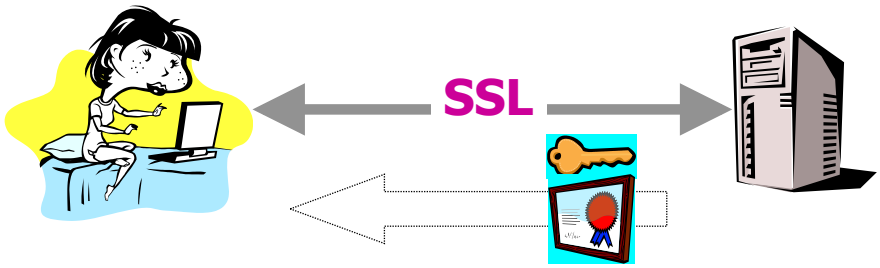


TelePay di SSB

Sistemi di pagamento elettronico

✓ **Casi di studio: SSL**

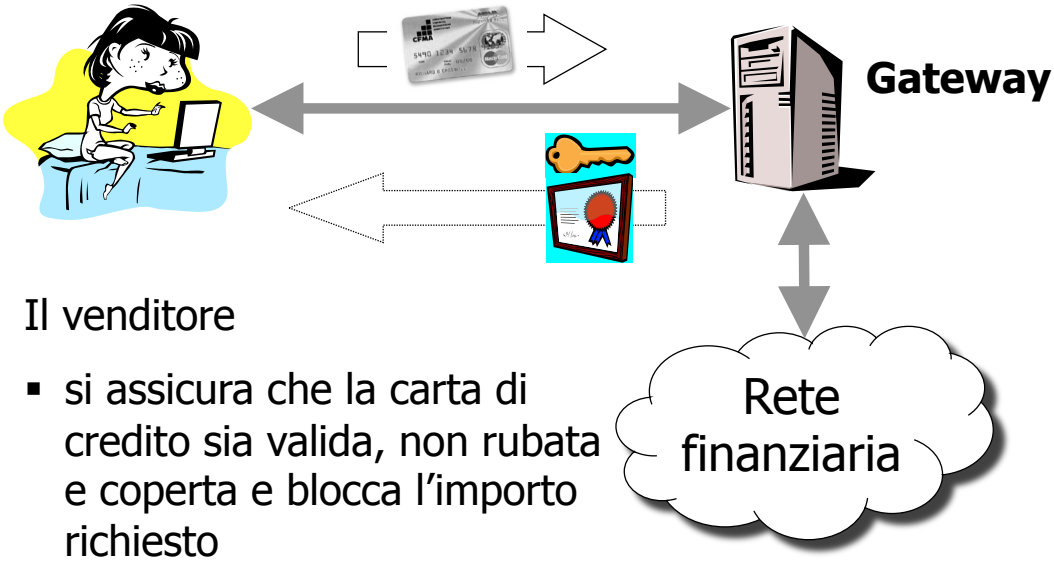
SSL



SSL

- SSL permette di stabilire un **canale sicuro** (**confidenzialità** ed **integrità**) tra il **browser** ed il **server**
- **Tipicamente**
- Il **server** viene autenticato attraverso un **certificato** (**protocollo handshake**)
- L'**utente** viene autenticato per mezzo di **password**, numero di **carta di credito**,…(**livello applicativo**)

Schema di pagamento



SSL

Il venditore

- si assicura che la carta di credito sia valida, non rubata e coperta e blocca l'importo richiesto
- eroga il servizio o consegna la merce
- procede all'addebito

Autorizzazione dal cliente

SSL

- Una transazione con carta di credito viene autorizzata dal titolare attraverso una **firma autografa**
- Il venditore deve accertarsi che la firma sia **"ragionevolmente" simile** al campione presente sul retro della carta
- L'istituto emittente **garantisce** il pagamento al venditore ed eventualmente il riaccredito al titolare
- In un acquisto su Internet via SSL, la firma autografa **non è più presente** …

Acquisti in rete con SSL

SSL

SSL non permette di (autenticare cliente) accertarsi che il titolare del pagamento sia il possessore della carta di credito

Acquisti in rete mediante carta di credito

SSL

Decreto legislativo 22 maggio 1999, n. 185, di attuazione della direttiva 97/7/CE

Art. 8 - Pagamento mediante carta

1. Il consumatore può effettuare il pagamento mediante carta ove ciò sia previsto tra le modalità di pagamento, da comunicare al consumatore al sensi dell'articolo 3, comma 1, lettera e), del presente decreto legislativo.

2. *L'istituto di emissione della carta di pagamento* ***riaccredita al consumatore*** *i pagamenti dei quali questi dimostri l'eccedenza rispetto al prezzo pattuito ovvero l'effettuazione mediante l'uso fraudolento della propria carta di pagamento da parte del fornitore o di un terzo*, fatta salva l'applicazione dell'articolo 12 del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197. *L'istituto di emissione della carta di pagamento* ***ha diritto di addebitare al fornitore*** *le somme riaccreditate al consumatore*.

Acquisti in rete mediante carta di credito

SSL

- Il fornitore di beni o servizi on-line ***è tenuto ad accollarsi il rischio*** della rivalsa degli istituti di emissione qualora, in caso di uso fraudolento delle carta, questi riaccreditano le corrispondenti somme al legittimo titolare.
- La legge ***non consente*** al fornitore di liberarsi dall'obbligo della restituzione delle somme agli istituti di emissione qualora dimostri
  1. di avere usato tutte le cautele necessarie e possibili ad evitare l'uso fraudolento della carta di credito
  2. che il fatto è stato causato dal caso fortuito.
- **I fornitori dovranno usare tutte le cautele del caso per potere**, nel caso di uso fraudolento di carte di credito, **perlomeno rintracciare l'illegittimo utilizzatore e rivalersi su questo**
- **Le conseguenze derivanti dall'addebito** delle somme riaccreditate al titolare della carta **potrebbero poi essere annullate contraendo una assicurazione** a copertura dei danni (economici) derivanti da tale circostanza.

Acquisti in rete con SSL

SSL

FOGLIO INFORMATIVO SULLE OPERAZIONI E SERVIZI OFFERTI ALLA CLIENTELA (CARIPRATO)

Caratteristiche e rischi tipici

Struttura e funzione economica

CARTE DI DEBITO e CARTE DI CREDITO

Strumenti di pagamento rilasciabili a clienti della Banca che consentono:
- Acquisto di beni;
- Prestazione di servizio presso esercenti convenzionati.
- Ottenimento di contante presso sistemi automatici o sportelli bancari convenzionati.

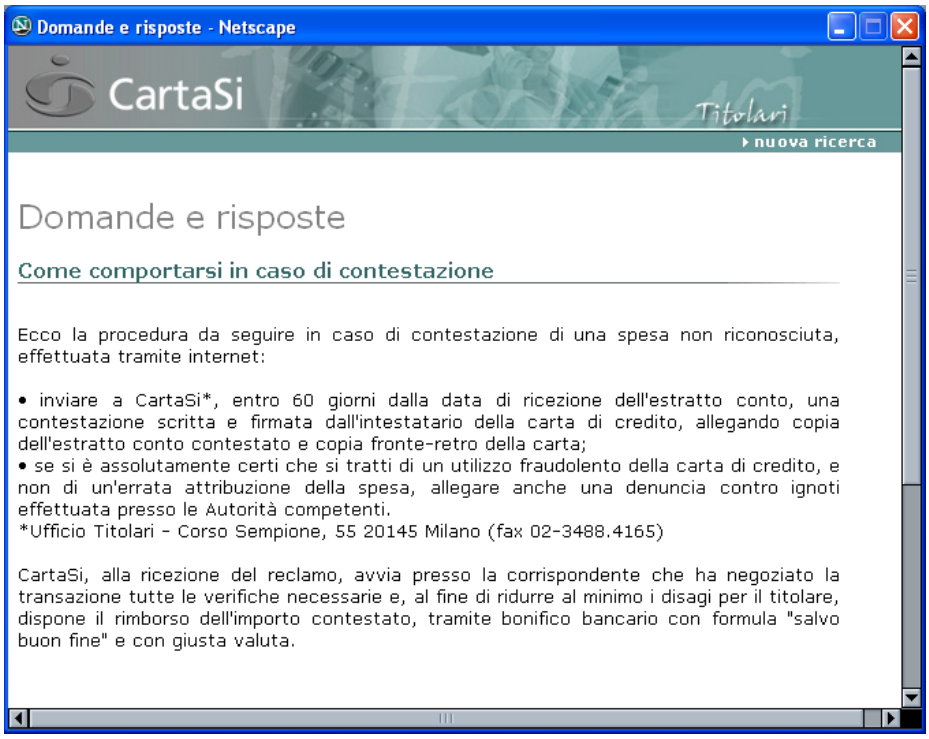
Funzione Bancomat: è il servizio in forza del quale la banca (emittente), attraverso il rilascio di una Carta, consente al correntista (c.d. "titolare") di effettuare prelievi di denaro — entro massimali di utilizzo stabiliti dal contratto - presso sportelli automatici (ATM) contraddistinti dal marchio Bancomat, digitando un codice segreto (c.d. P.I.N., "Personal Identification Number").
Funzione PagoBANCOMAT: è il servizio in forza del quale il correntista può compiere acquisti di beni e servizi presso esercizi commerciali convenzionati che espongono il marchio "PagoBANCOMAT", digitando il citato codice segreto.
L'utilizzo del sistema di pagamento è consentito nei limiti giornaliero e mensile, entro limiti di importo contrattualmente previsti, determinato dal momento dell'emissione e dalla capienza di conto corrente al momento dell'addebito.

Principali rischi (generici e specifici)

Il rischio relativo ad eventuali utilizzi fraudolenti effettuati con le Carte di Pagamento è limitato a 150 € per evento se il Titolare ha ottemperato e rispettato quanto indicato dalla "Raccomandazione della Commissione Europea del 30 giugno 1997 n. 97/489"
In sintesi il titolare è tenuto a:
- Firmare la carta nel caso che la stessa sia munita di apposita banda di scrittura;
- Osservare la massima attenzione nella custodia della carta e PIN e la massima riservatezza nell'uso del medesimo;
- Bloccare la carta nel caso di furto, smarrimento o uso fraudolento della medesima, confermando l'evento con denuncia o dichiarazione di smarrimento.

Acquisti in rete con SSL

SSL



Acquisti in rete mediante carta di credito

SSL

- ***Gli istituti di emissione***, cui compete l'autorizzazione dell'operazione di pagamento, nonché i soggetti che rendono tecnicamente possibile la transazione on-line, ***sono tenuti a controllare la correttezza del numero della carta e la data della sua scadenza ma non anche la corrispondenza tra il numero fornito e l'effettivo titolare***
- ***Gli istituti di emissione verificano la corrispondenza tra numero della carta di credito*** **comunicato per effettuare una transazione on-line** ***ed il nominativo fornito da colui che la effettua***

  Address Verification Service (AVS): **si verifica che l'indirizzo di consegna sia quello con cui il possessore della carta è registrato**

- In Europa il grado di sicurezza nelle transazioni on-line è minore e quindi il commercio elettronico è destinato ad incontrare resistenze anche da parte dei fornitori di che sopportano rischi elevati

Devo credere al certificato?

SSL

- **Un certificato costituisce una base solida per fidarmi di un server?**
  - **CertPap.com** afferma che la chiave pubblica della **Banca di Paperopoli** è **K**
  - Quanti utenti **leggono** il certificato?
  - Quanti utenti **capiscono** il certificato?
  - CertPap.com **è autorizzata a parlare per** la Banca di Paperopoli?

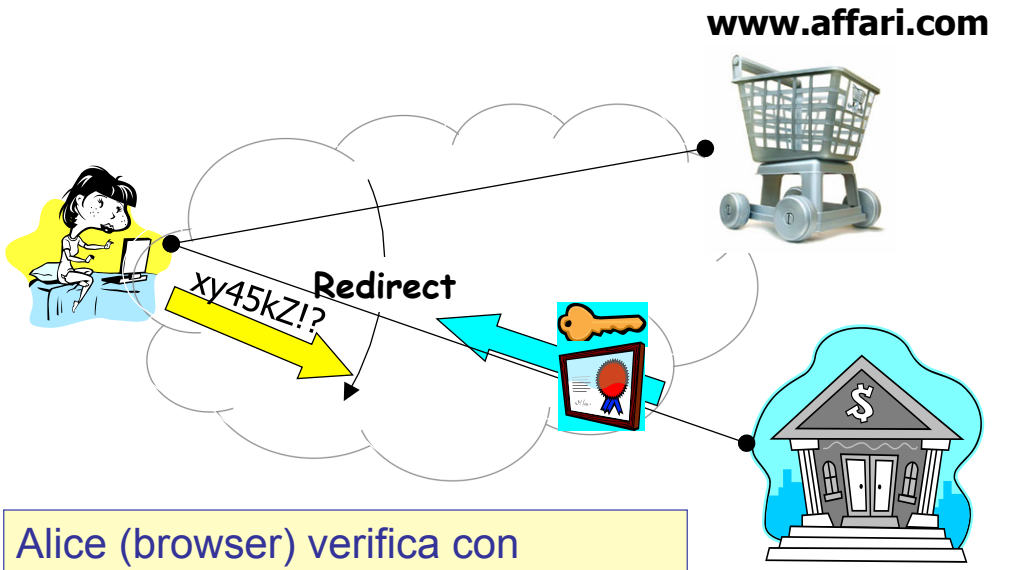
Devo credere al browser?

SSL

- **Dall'URL riesco a capire a chi mi sto effettivamente collegando?**
- **Fancy URL**
- Nel 1999, Gary D. Hoke riuscì a spoof-are il sito bloomberg.com facendo rialzare il valore delle azioni
- http://www.loucipher.com/biz2/headlines/topfin.html
- http://204.238.155.37/biz2/headlines/topfin.html
- http://bloomberg.com:biz@3438189349/biz2/headlines/topfin.html
- **Typejacking**
- PayPal.com scamming
  - "**paypal**" e "**paypai**"

Devo credere al browser?

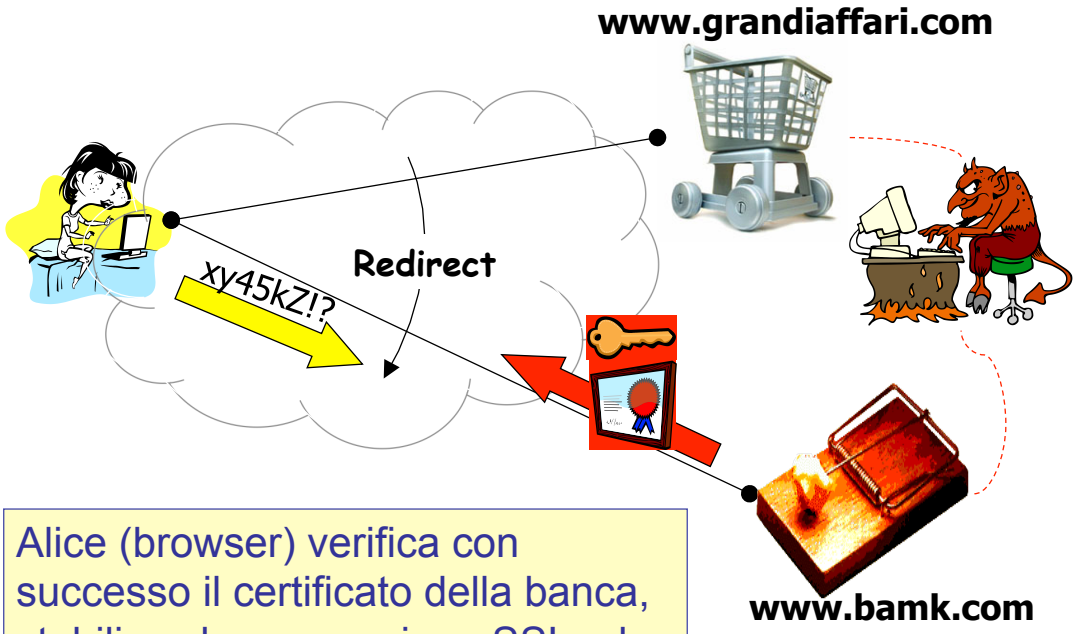
SSL



Alice (browser) verifica con successo il certificato della banca, stabilisce la connessione SSL ed invia la propria PWD alla banca

Devo credere al browser?

SSL



Alice (browser) verifica con successo il certificato della banca, stabilisce la connessione SSL ed invia la propria PWD alla banca

Devo credere al browser?

SSL

- **Il problema è che SSL opera al livello trasporto** mentre

➔ dovrebbe essere l'applicazione a (indurre l'utente a) verificare che il nome richiesto sia uguale al nome contenuto nel certificato verificato

- ESEMPIO: Netscape
  - Il browser *notifica* all'utente se l'URL specificato dal browser e quello contenuto nel certificato del server sono diversi
  - L'utente decide se proseguire la connessione oppure no (interfaccia utente!!!)
  - In linea di principio non è detto che il controllo eseguito dal browser Netscape sia sufficiente per ogni tipo di applicazione Web-based

Sistemi di pagamento elettronico

✓ **Secure Electronic Transactions (SET)**

Secure Electronic Transactions

SET

- SET è un sistema di tipo check-like che permette di effettuare pagamenti con carte di debito/credito (pay-now/-later)
  - "carta di credito virtuale"
- SET è stato sviluppato da MasterCard e Visa
- SET non è adatto ai micropagamenti a causa dei cost-overhead di elaborazione delle transazioni
- SET simula il “paper world”

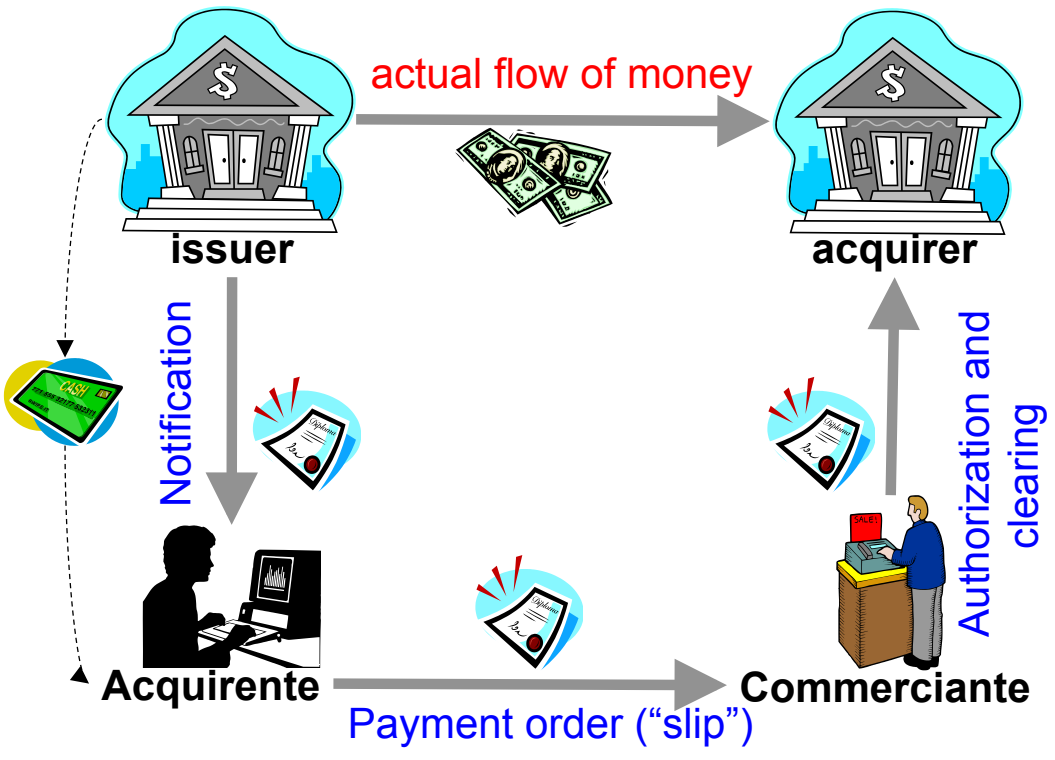
SET

Storia

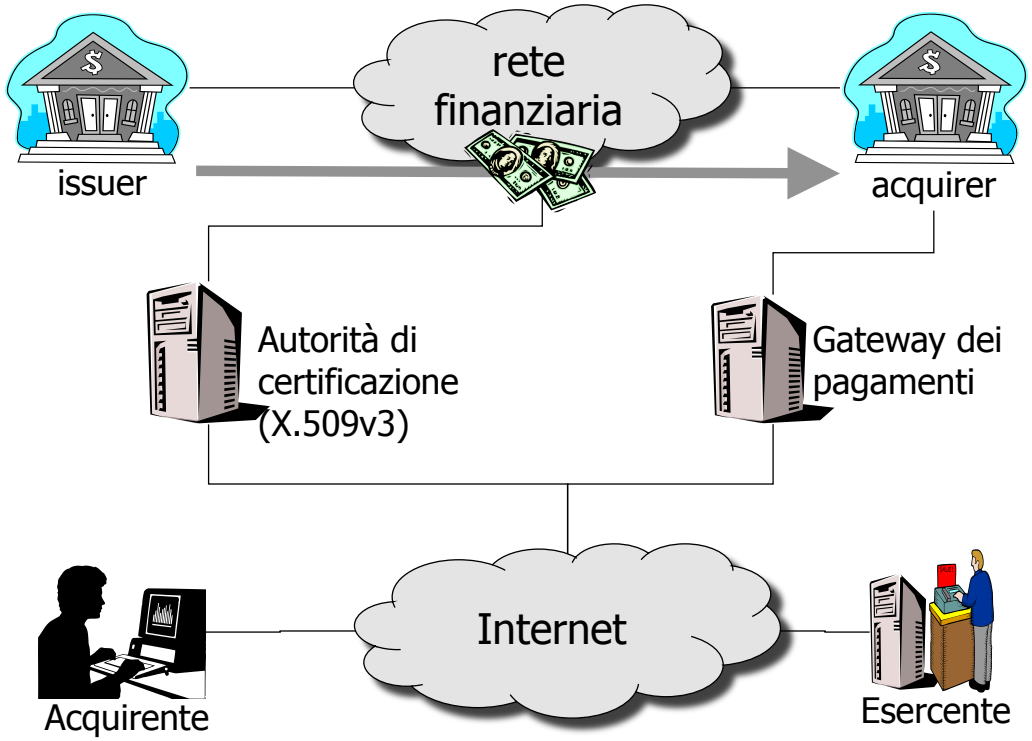
- Febbraio 1996
  - MasterCard e Visa richiedono uno standard di sicurezza
  - Lo sviluppo della specifica coinvolge IBM, Microsoft, Netscape, RSA Data Security, Terisa, Verisign
- 1998
  - escono i primi prodotti basati sulle specifiche SETv1
  - La specifica SET sta su 3 volumi per un totale di 971 pagine

SET

Check-like



Architettura



SET

Partecipanti

- Titolare di una carta di credito (cardholder)
- Commerciante (merchant)
  - accetta carte di credito ed ha un rapporto con un istituto acquirente
- Istituto emittente (issuer)
- Istituto acquirente (acquirer)
- Gateway dei pagamenti
  - costituisce l'interfaccia tra SET e la rete finanziaria dei pagamenti
- Autorità di certificazione

SET

Certificati

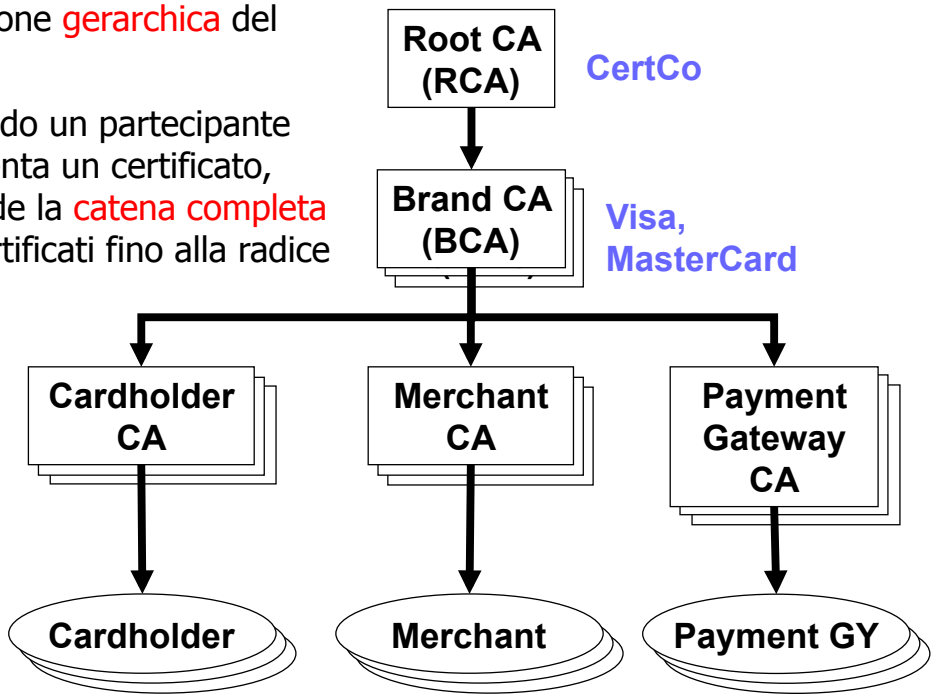
SET

- Cardholder Certificate
  - lega il possessore della carta di credito ad un conto bancario (numero e scadenza)
  - per privacy le informazioni sul conto bancario (*payment instruction*) presenti nel certificato non sono in chiaro
- Merchant Certificate
  - testimonia una relazione valida tra il venditore ed una istituzione finanziaria acquirente (brand)
  - il merchant ha due coppie di chiavi: una per la firma digitale ed una per lo scambio di chiavi
  - Una coppia di certificati per ogni brand
- Gateway Certificate
  - è rilasciato dall'istituto acquirer

Trust management

SET

- Gestione gerarchica del trust
- Quando un partecipante presenta un certificato, include la catena completa di certificati fino alla radice



Certificato per lo scambio delle chiavi

SET

- Generalmente è buona norma utilizzare chiavi diverse per la firma digitale e per lo scambio chiavi (più in generale per la cifratura)
- Certificato per la firma digitale: C_A
- Certificato per la lo scambio delle chiavi: C_A^{kex}

L'involucro digitale (digital envelope)

SET

Notazione

$A \rightarrow B: \ \{x\}_{\{K_{ab}\}_{K_b^{ex}}}$ è equivalente a

$A \rightarrow B: \ \{x\}_{K_{ab}}, \{K_{ab}\}_{K_b^{ex}}$

con:

- K_{ab} una chiave simmetrica temporanea generata "al volo" da Alice per comunicare con Bob
- K_b^{ex} la chiave pubblica di Bob per lo scambio delle chiavi

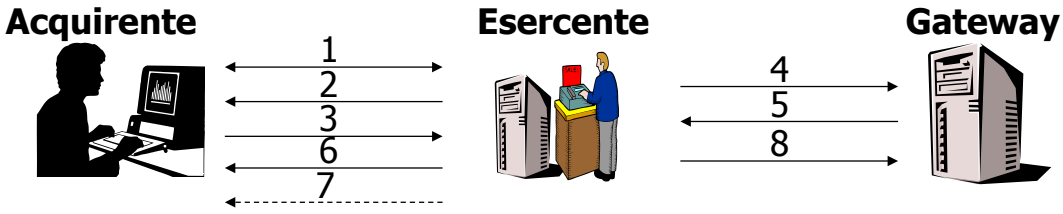
SET

Obiettivi

- Riservatezza
  - ✓ **delle informazioni relative agli ordini ed al pagamento (DES)**
- Integrità dei dati
  - ✓ **Firma digitale (RSA, SHA-1; HMAC SHA-1)**
- Autenticazione del titolare
  - ✓ **Il commerciante può verificare che il titolare della carta di credito è anche titolare di un conto valido (certificati X.590v3)**
- Autenticazione del commerciante
  - ✓ **I titolare può verificare che il commerciante può accettare carte di credito (certificati X.590v3)**
- Interoperabilità
  - ✓ **indipendenza dalla piattaforma**

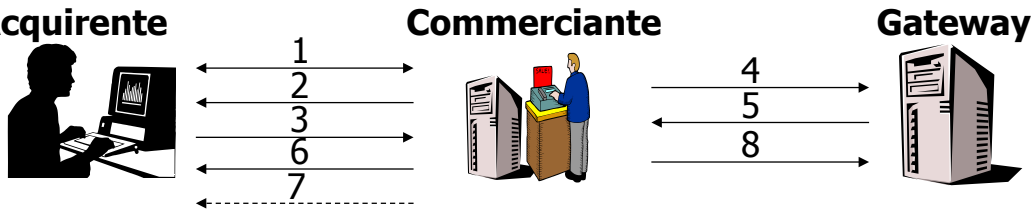
SET

Interazioni



- L'acquirente naviga sul sito dell'esercente, sceglie gli articoli da acquistare ed invia la lista all'esercente (**1**)
- L'esercente invia all'acquirente un **modulo d'ordine** compilato, contenente la lista degli articoli, il loro prezzo, il prezzo totale, la data ed un numero d'ordine, ed il suo certificato (**2**)
- L'acquirente valida l'esercente e gli invia **l'ordine**, il **pagamento** ed il suo **certificato** (**3**)

Interazioni



- L'esercente autentica l'acquirente, richiede al gateway l'autorizzazione al pagamento (**4**)
- Il gateway autorizza il pagamento (**5**)
- L'esercente invia una **conferma d'ordine** al cliente (**6**)
- L'esercente fornisce i prodotti/servizi all'acquirente (**7**) e richiede il pagamento (**8**) al GW*

* **L'ordine delle azioni 7 e 8 è stabilito per legge**

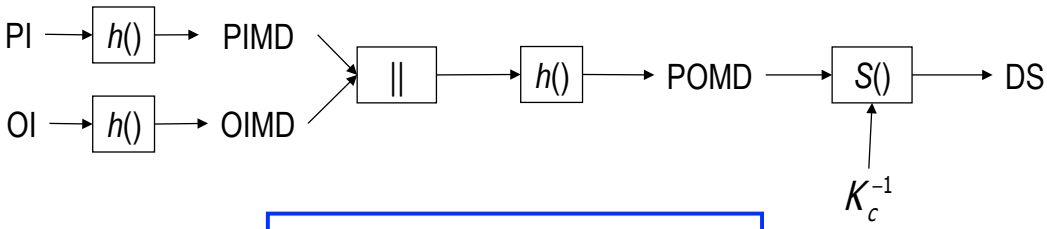
SET

La doppia firma

- **Il cliente invia due tipi di informazioni a due diversi destinatari:**
  - **l'ordine** (***order information***, ***OI***) **al commerciante**
  - il **pagamento** (***payment information***, ***PI***) **alla banca**
- **Per garantire la riservatezza del pagamento**
  - **il commerciante non deve conoscere le informazioni sul pagamento**
  - **la banca non deve conoscere le informazioni sull'ordine**
- **Per garantire l'integrità del pagamento**
  - **le informazioni sul pagamento e le informazioni sull'ordine devono essere legate le une alle altre**
- **In caso di disputa (non-ripudio)**
  - **si deve poter provare che le due informazioni sono legate**
- La **doppia firma (dual signature)** permette di soddisfare questi requisiti

SET

La doppia firma (dual signature)



$$DS = S_{K_c^{-1}}\left(h\left(h(PI)\|h(OI)\right)\right)$$

- DS permette di provare che OI e PI sono legate
- Il commerciante riceve OI e PIMD nell'**ordine**, K_c nel **certificato** del cliente e può quindi verificare DS
- La banca riceve PI e OIMD nel **pagamento**, K_c nel **certificato** del cliente e può quindi verificare DS

SET

Elaborazione del pagamento

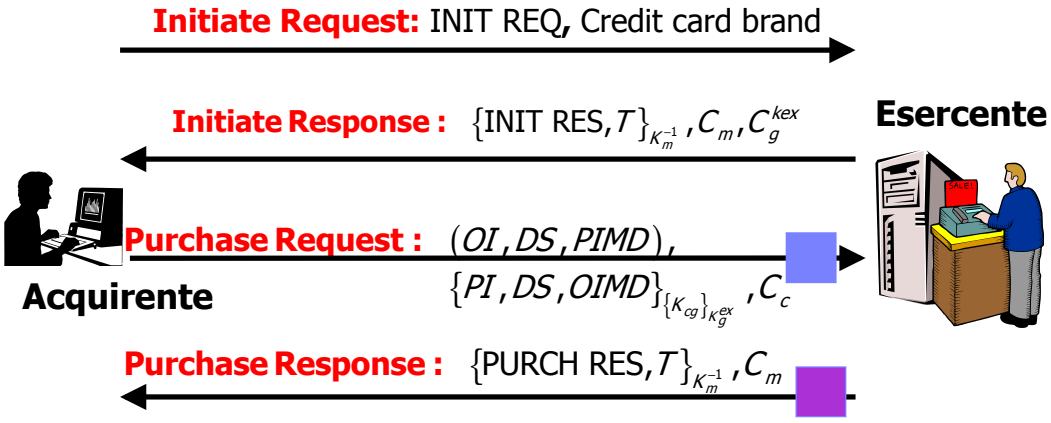
TRE FASI

- **Richiesta di acquisto**
- **Autorizzazione del pagamento**
- **Rilevazione del pagamento**

SET

Richiesta di acquisto

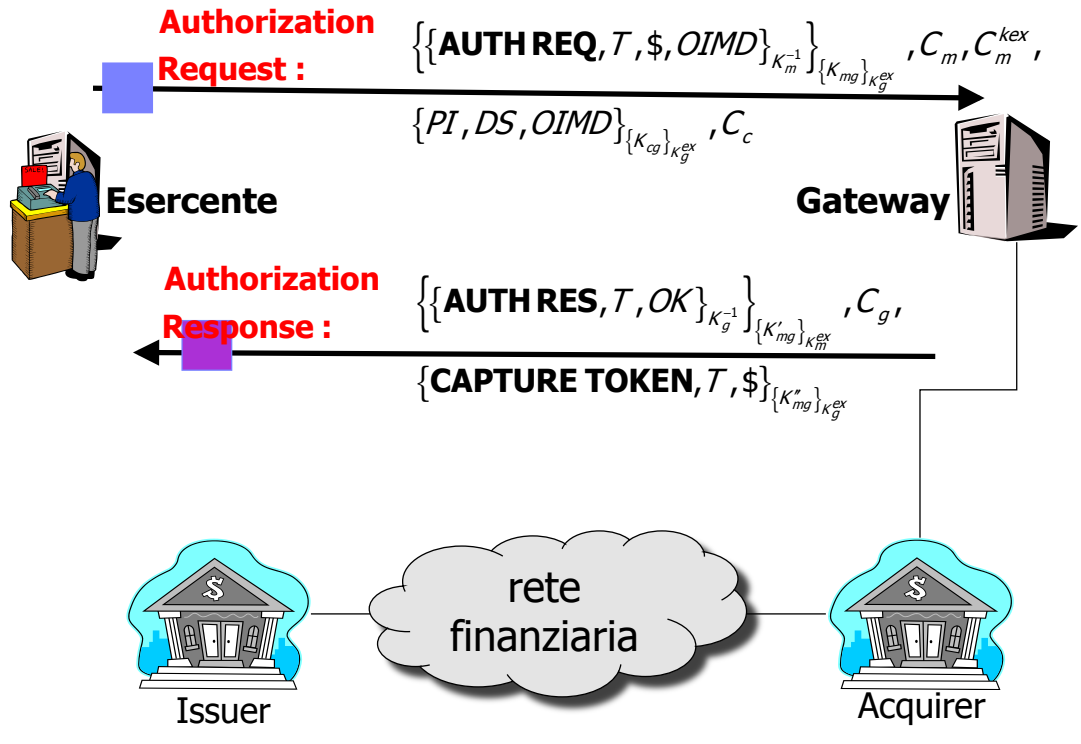
SET



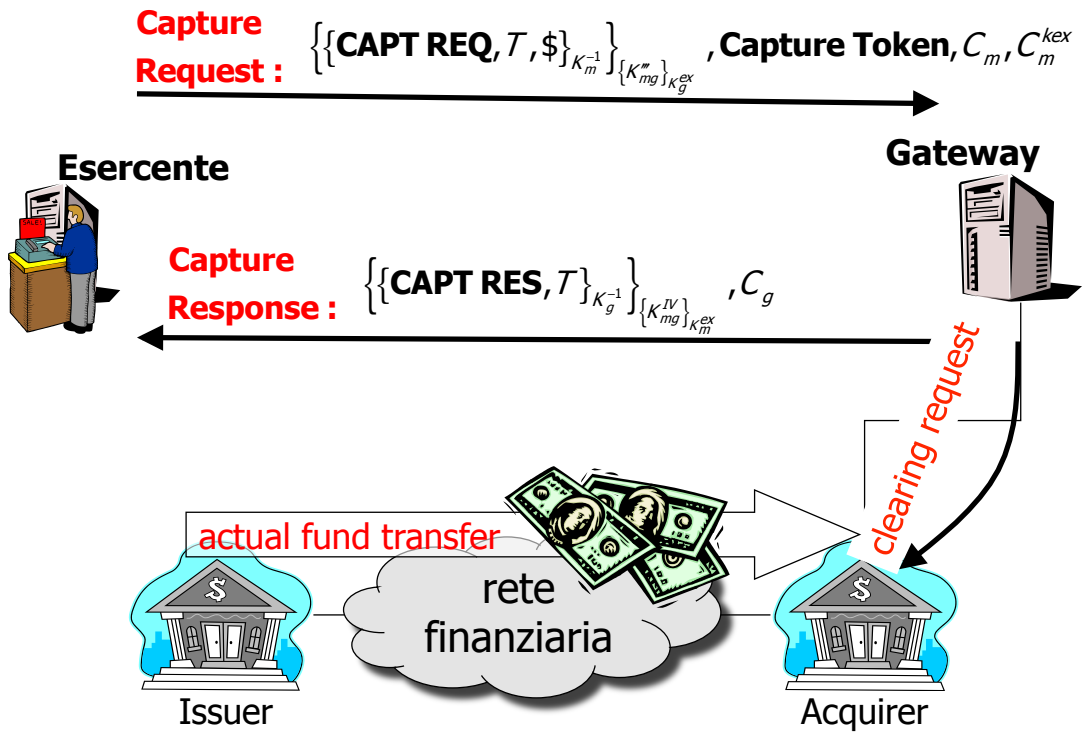
- OI fa riferimento all'identificatore di transazione *T*
- Il messaggio Purchase Response conferma all'acquirente che il commerciante ha ricevuto l'ordine

Autorizzazione del pagamento

SET



Rilevazione del pagamento



SET

Pro e contro

- **Pro**
  - **Standard**
  - **Basato sulla firma digitale**
    - ✓ **meccanismo di base per la gestione delle dispute**
  - **Sfrutta l'infrastruttura bancaria esistente**
- **Contro**
  - **Servizio on-line: il gateway può diventare un collo di bottiglia**
  - **Troppo "grosso" per le smart card**
  - **Costoso (crittografia costosa, molti messaggi)**
  - **Assume che i computer siano sicuri (!!)**
    - ✓ **le chiavi private devono essere protette**

SET

Allocazione del rischio

- **tende a spostare il rischio sul cliente**
  - l'utente è considerato presente alla transazione
  - l'utente non può ripudiare quello che ha firmato
- **ma il rischio per il cliente di perdere i mezzi per autorizzare una transazione SET (la chiave privata) sono ben diversi da quello di perdere la carta di plastica**

…ma un PC è sicuro?

Considerazione

- **malicious payload**
  - una volta installato, non c'è limite ai danni che un programma malizioso può causare
  - c'è da aspettarsi che l'utente medio non sia in grado di rilevare la presenza di un programma malizioso
- **delivery mechanism**
  - physical installation
  - remote automated delivery
    - ✓ Email virus & worms (Code Red, Nimda, Bubbleboy)
      - – si diffondono rapidamente ed installano software sull'host vittima
    - ✓ Bug nel SO e ne SW applicativo (buffer overflow)
    - ✓ ActiveX o altra applicazione scaricata consciamente
      - – che installa un Trojan Horse

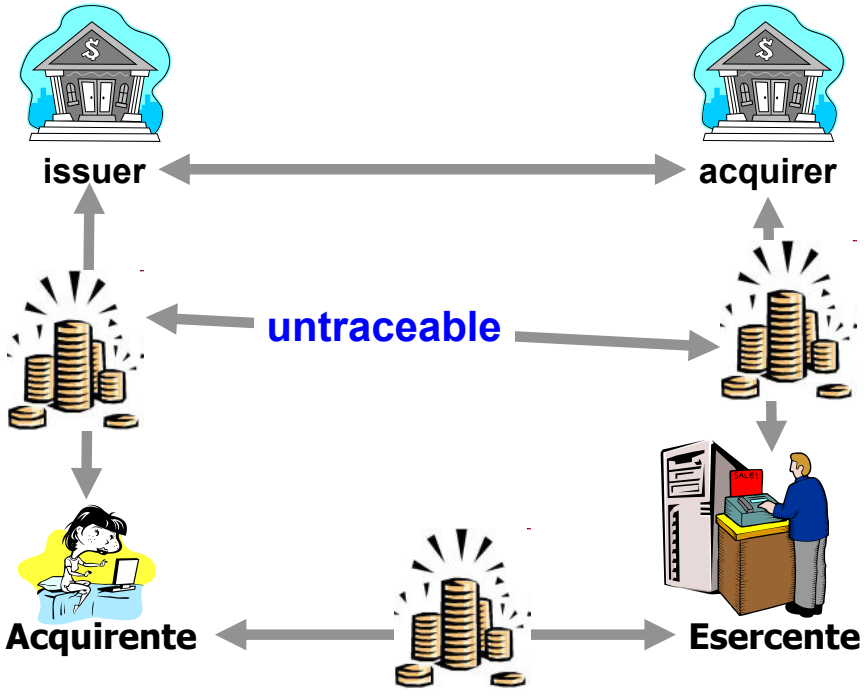
Pagamenti elettronici

- ✓ Moneta elettronica (senza supporto fisico): eCash™

Requisito fondamentale: non-tracciabilità

Digital Cash

- ♦ **ecash™**



RSA

- L'algoritmo di firma digitale (cifratura) è costituito da:
- algoritmo di generazione delle chiavi
- algoritmo di generazione della firma (cifratura)
- algoritmo di verifica della firma (decifratura)

RSA

Generazione delle chiavi

- Siano p e q due numeri primi grandi
- Sia $n = p \times q$ (modulo)
- Sia $\Phi = (p-1) \times (q-1)$
- Sia $1 < e < n$ tale che MCD$(e, \Phi) = 1$
- Determinare d tale che $e \times d = 1$ (**mod** Φ)
- **chiave pubblica: (e, n)**
- **chiave privata: (d, n)**
- Distruggere i valori p e q

RSA

Generazione della firma digitale

- Siano ***m*** un messaggio
- La firma digitale $s = m^d \pmod n$
- (m, s)

Verifica della firma digitale

- $m' = s^e \pmod n$
- **return** $(m' == m)$

Dimostrazione (bozza)

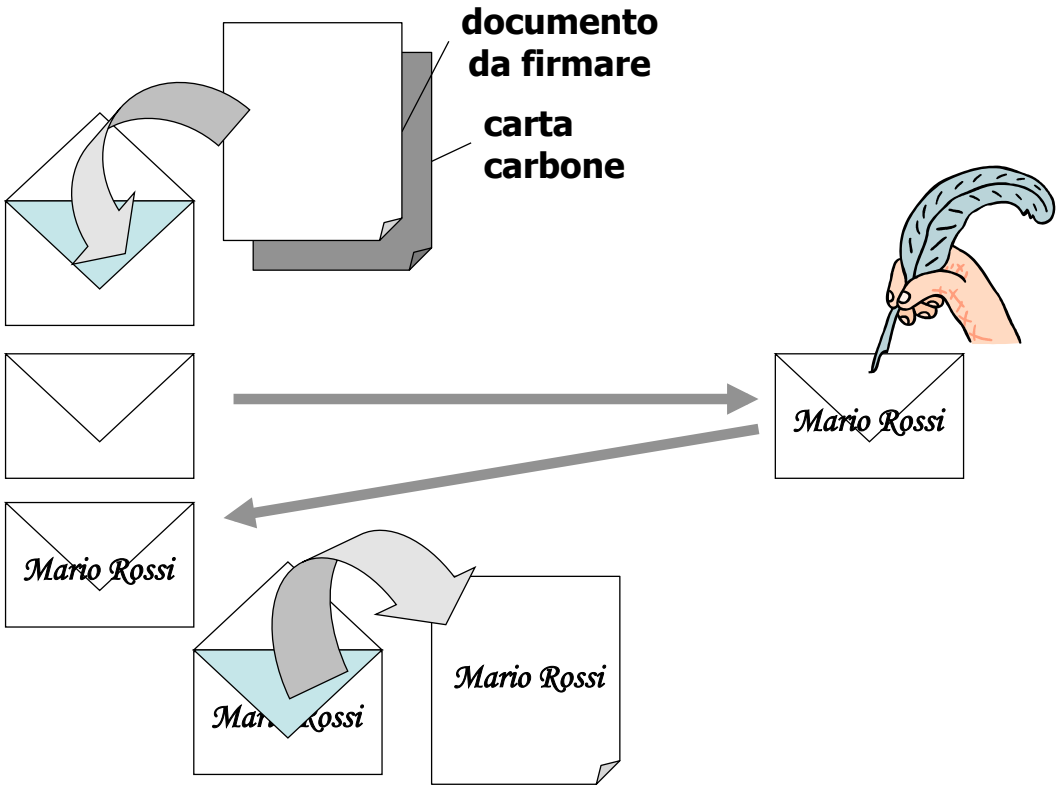
- $s^e = (m^d)^e = m^{de} = m \pmod n$

Blind signature

Proprietà

- In un sistema di blind signature, l'entità che firma
- non vede cosa firma
- non è in grado di ricollegare la firma all'atto di firma (**untraceability**)

Blind signature



Blind signature: esempio con RSA

Client

- Scegliere un numero random b tale che $MCD(b, n) = 1$
- Calcolare $m' = m \times b^e \pmod n$
- Inviare m' al signer
- Ricevere s' dal signer
- Calcolare $s = s' \times b^{-1} \pmod n$

- Siano (d, n) ed (e, n), rispettivamente, la chiave privata e la chiave pubblica del server
- Sia m il messaggio da firmare

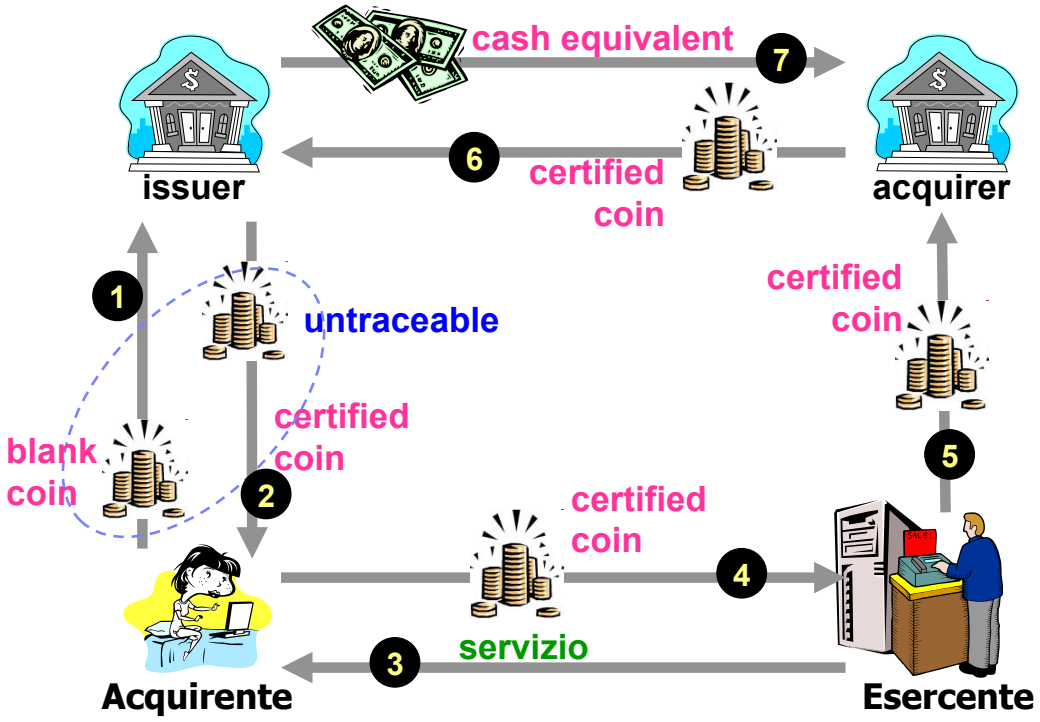
Server (signer)

- Ricevere m' dal client
- Calcolare $s' = (m')^d \pmod n$
- Inviare s' al client

Dimostrazione (bozza). $s' \times b^{-1} = (m')^d \times b^{-1} = (m' b^e)^d \times b^{-1} = m^d \times b^{ed} \times b^{-1} = m^d \times b \times b^{-1} = m^d = s \pmod n$

Blind signature for untracebaility

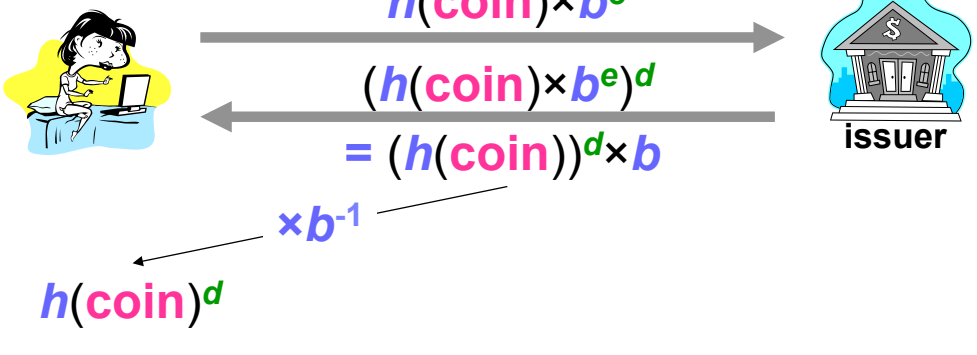
Digital Cash



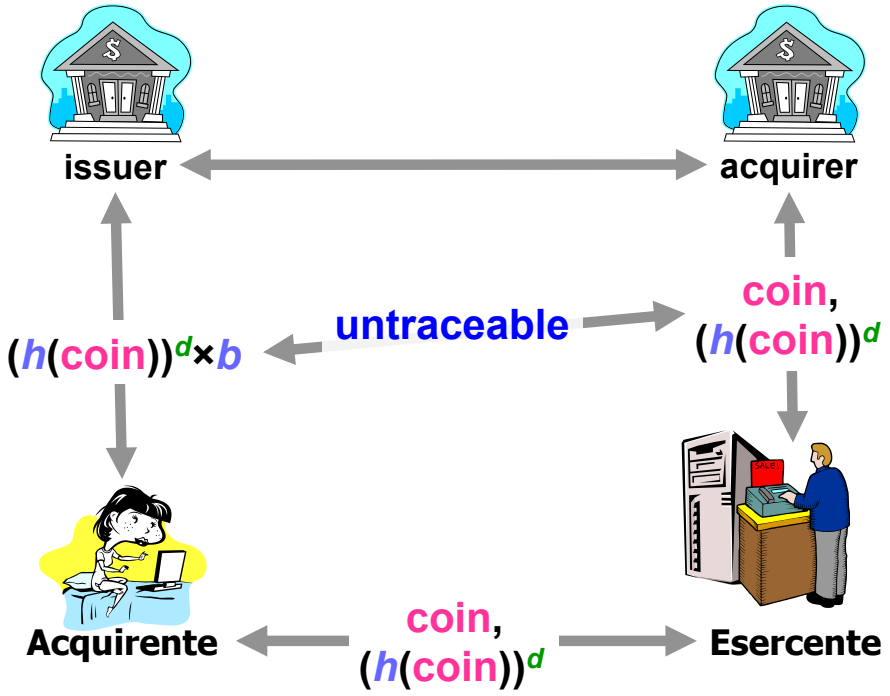
Blind signature for untraceability

Digital Cash

- **Blind Signatures based on RSA**
  - One-way function ***h***
  - La coppia di chiavi RSA (***e, n***), (*d*, *n*) scelta dall'**Issuer** definisce una denominazione
  - Coin: (**coin**, ***h***(**coin**)^{d}), **coin** = numero random
- **Prelievo**



Blind signature for untraceability



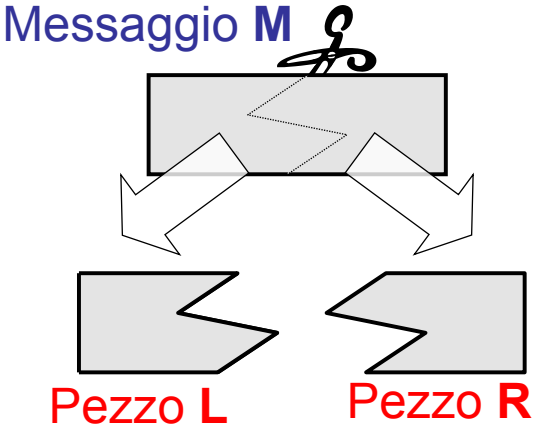
Digital Cash

Double-spending attack

- Il precedente protocollo non impedisce
  - all'**Acquirente** di **spendere il digital coin due o più volte** o
  - all'**Esercente** di **depositare il digital coin due o più volte**
- La banca mantiene la **lista dei digital coin spesi**
  - Questo **protegge la banca dalle frodi**, ma
  - **non permette di identificare il frodatore**
- ci aiuta la crittografia…

Digital Cash

Secret splitting



ESEMPIO

Messaggio **M**

Quantità random **R**

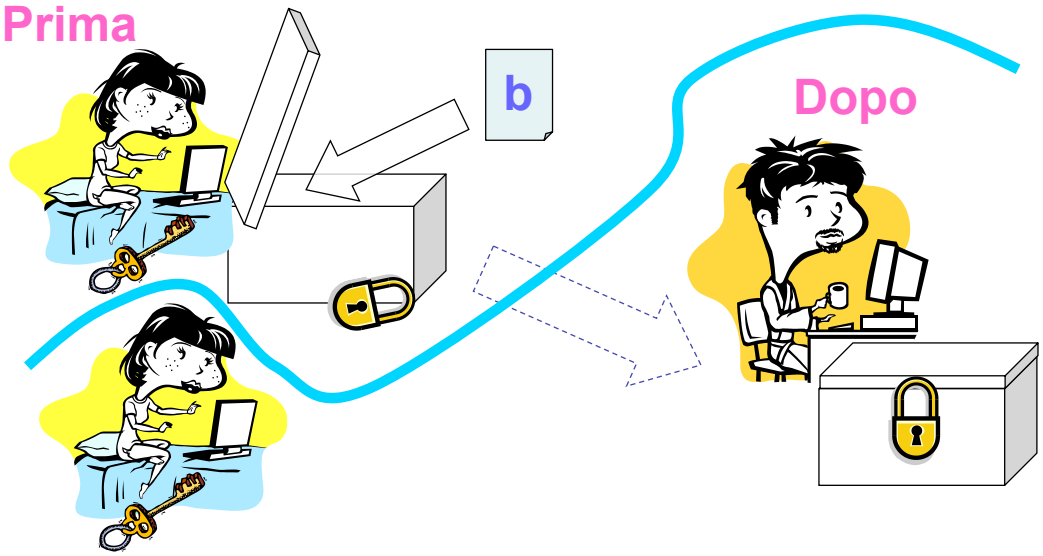
L = M xor R

Ricostruzione di **M**

M = L xor R

- Ciascun pezzo da solo non dà alcuna informazione sul messaggio
- I due pezzi insieme permettono di ricostruire il messaggio

Bit commitment



- Alice **si impegna** con Bob sul valore ***b*** di un bit senza rivelare tale bit ma in modo tale che, **più tardi**, tale valore può essere **rivelato** (o **"aperto")** da Alice e **verificato** da Bob
- **perfectly binding**, **perfectly concealing**

Bit commitment

ESEMPIO (*perfectly binding*)

p primo, ***g*** generatore

Alice

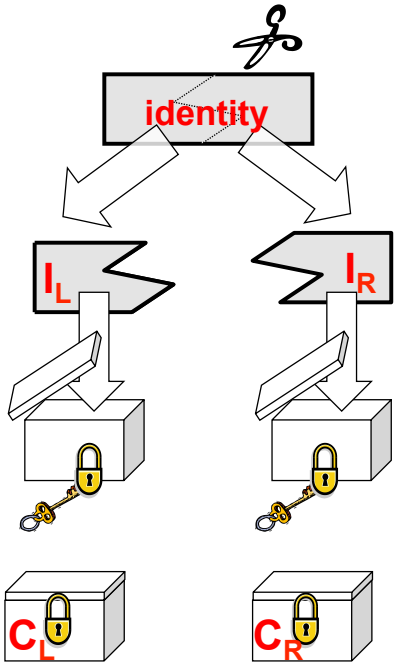
sceglie ***b*** (0<***b***<***p***-1)

calcola $c = g^b \bmod p$

pubblica ***c***

- Non è perfectly concealing perché è possibile determinare ***b*** risolvendo il DLP $b = \log_g c \bmod p$

Double-spending prevention



Secret splitting

Bit commitment

Double-spending prevention

- **Coin**

  (coin, identity string, h(coin, identity string)^d)

- **Uniqueness bit string**
  - coin
- **Identity bit strings**
  - (C_{1L}, C_{1R}), (C_{2L}, C_{2R}), …, (C_{100L}, C_{100R})

    Le coppie sono diverse tra loro
- **Setup**
  - Alice prepara **100 blank coin (money order)**

Cut-and-choose

$h(\text{coin}_i, \text{identity string}_i) \times b_i^e$, $1 \le i \le 100$

unblind 99 (random)

$h(\text{coin}_i, \text{identity string}_i)$, $1 \le i \le 99$

apri le 99 identity strings

$((I_{jL}, I_{jR})_i, 1 \le j \le 100), 1 \le i \le 99$

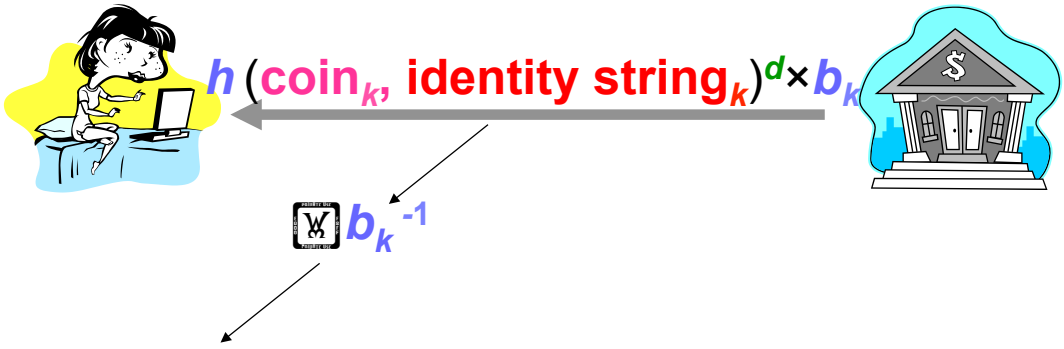
- Al termine del protocollo **cut-and-choose** la banca è convinta al **99%** che il commitment non rivelato contiene l'identità di Alice

Double spending prevention

Digital Cash

Prelievo

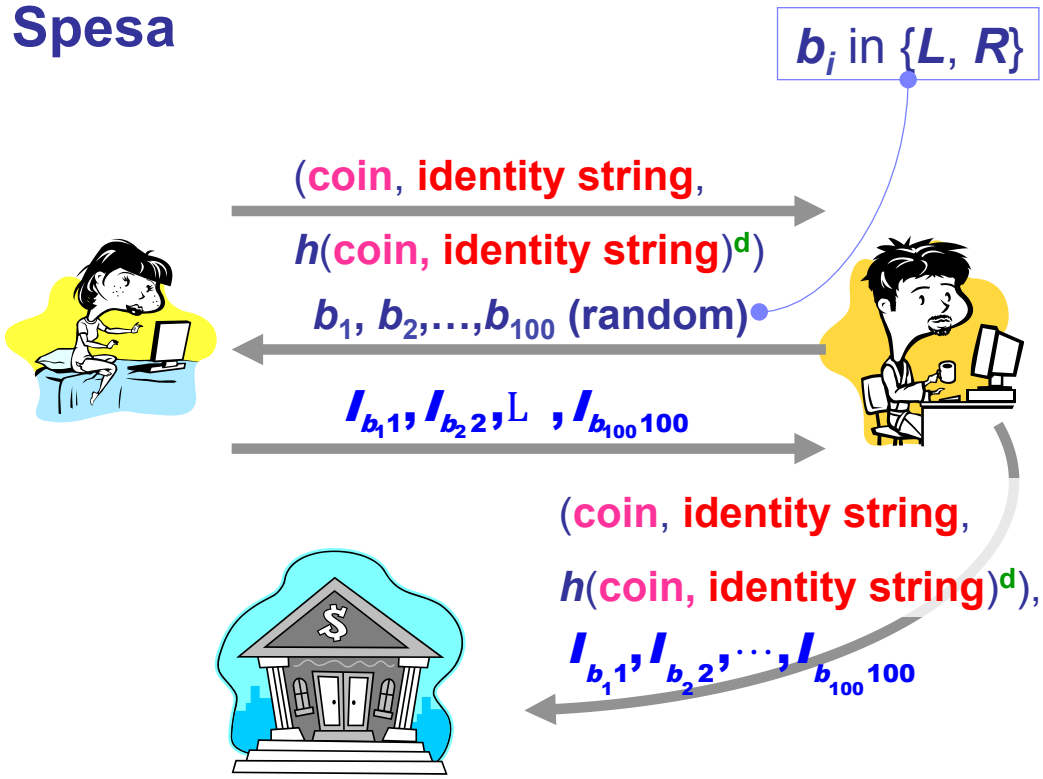
La banca “firma” il “blank” coin che avanza (ad es., il ***k***-esimo)



Double spending prevention

Digital Cash

Spesa



Double spending prevention

Digital Cash

Controlli della banca

- La banca verifica la firma digitale
- Se il **coin** non è stato ancora speso
  - la banca accredita un importo pari alla denominazione a Bob
- Se **coin** è stato già speso,
  - se le **identity string sono uguali**, allora il frodatore è **Bob**, altrimenti
  - se le **identity string sono diverse**, allora il frodatore è **Alice**

Double spending prevention

Digital Cash

In caso di frode la banca rileva il frodatore

- Se **coin** è già stato speso
  - se le **identity string sono uguali**, allora il frodatore è **Bob**, altrimenti
  - se le **identity string sono diverse**, allora il frodatore è **Alice**
    - La banca trova una posizione nelle identity string in cui Alice ha rivelato il pezzo destro ed il pezzo sinistro della sua identità **con probabilità 1- $(½)^{100}$**
    - Dai due pezzi la banca determina l'identità di Alice

Pagamenti elettronici

- ✓ Moneta elettronica (con supporto fisico)

Pagamenti elettronici

- ✓ Le smart card

Cos'è una smart card?

- Una **smart card** ("carta a microprocessore") è una scheda plastificata con un microprocessore o un chip di memoria integrato

Supporto in PVC o polietilene

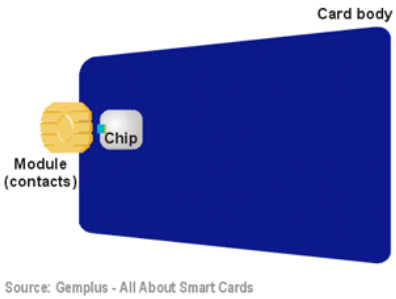
microprocessore o chip di memoria

Una smart card interagisce con un sistema di elaborazione attraverso un **lettore di smart card**

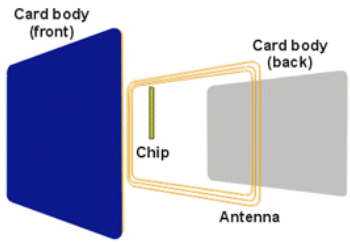
dimensioni standard: 25×15 mm, 33×64 mm, 54×85 mm,

Tipi di smart card?

- **smart card con e senza contatti**

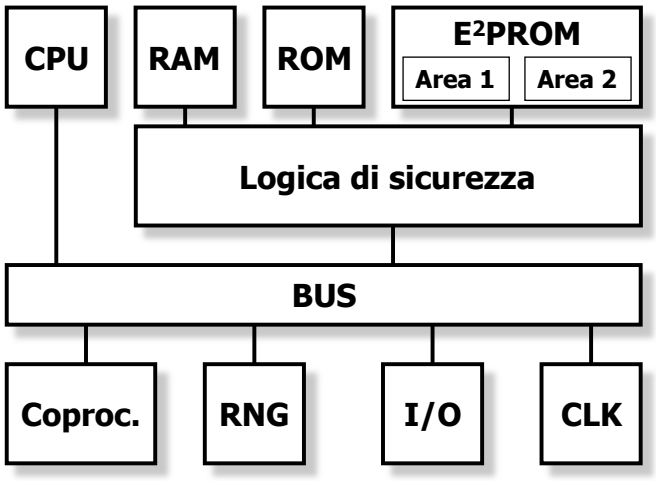


Source: Gemplus - All About Smart Cards



Source: Gemplus - All About Smart Cards

Architettura di una smart card



- **CPU**: **tecnologia CMOS a bassa potenza** (processore a 8 bit, Intel o Motorola, 5MHZ)
- Il **coprocessore** ed il **generatore di numeri random** (**RNG**) permettono la realizzazione di **algoritmi crittografici (DES, RSA, MD5,...)**
- **I/O seriale**
- **ROM**: il SO e le applicazioni all'origine
- **RAM**: dati temporanei

- **E²PROM** contiene le **applicazioni aggiuntive** e/o i **dati**. I dati sensibili sono memorizzati nella in **aree a livello di sicurezza differente** accessibili per mezzo di un **PIN**
- Una **logica di sicurezza** rende la smart card **tamper resistant**

Smart card

Tipi di smart card?

- **memory card e microprocessor card**
  - Le **memory card** hanno la sola funzionalità di memorizzazione dei dati

    possono essere considerate come dei floppy disk con misure aggiuntive opzionali di sicurezza
  - Le **microprocessor card** svolgono funzionalità di elaborazione dati

    possono essere considerate come dei veri e propri elaboratori in miniatura

Smart card

Benefici

Smart card

Caratteristica	Beneficio
sicurezza	▪ Tamper resistant ▪ Protezione dei dati con PIN e/o in lettura e/o in scrittura ▪ Cryptography-enabled ▪ Numero seriale unico
processing	▪ Capacità di elaborazione e non solo memorizzazione ▪ Caricamento dinamico delle applicazioni
comodità	▪ Tamper resistant ▪ Portabile

Utilizzi

Smart card

- **Information Technology**
  - Secure logon and authentication of users to PCs and networks
  - Storage of digital certificates, credentials and passwords
  - Encryption of sensitive data
  - …
- **Mobile Telecommunications**
  - Secure subscriber authentication
  - Secure mobile value added services
  - …
- **Commercial Applications**
  - Banking/payment,
  - Ticketing
  - Loyalty and promotions
  - Parking and toll collection
  - …

Smart card

Carte di credito con microchip

- Concettualmente le transazioni hanno (±) la stessa struttura ma la carta di credito con microchip ha i seguenti **vantaggi** rispetto a quella con *magstripe*:
  - **sono più difficili da falsificare**
  - **Il microchip permette funzioni aggiuntive**
- **Standard EMV** promosso da Europay, MasterCard, Visa (93, 96, 98)
  - **Part I.** Aspetti elettromeccanici
  - **Part II.** Strutture dati e comandi
  - **Part III.** Elaborazione delle transazioni
- **microchip poco costoso** (produzione di massa)
  - ROM (6 Kb), EEPROM (1 Kb), RAM (128 b)

Smart card

Borsellini elettronici

- Lo standard CEN EN 1546 “Inter-sector Electronic Purse” (IEP)
  - La Commissione Europea ha commissionato lo standard nel 1990; la versione definitiva è stata rilasciata nel 1998
- Sistemi basati su CEN EN 1546
  - Eurocheque debit card (Austria/Germania)
  - Visa Cash system
- Le specifiche sono organizzate in quattro parti
  - Part I. Descrizione generale del sistema
  - Part II. Architettura di sicurezza
  - Part III. Strutture dati e comandi
  - Part IV. Specifica dei protocolli
- **CEN EN 1546 definisce un *framework* piuttosto che una specifica e lascia molta libertà alle implementazioni**

Pagamenti elettronici

✓ Moneta elettronica (con supporto fisico)
il sistema Mondex™

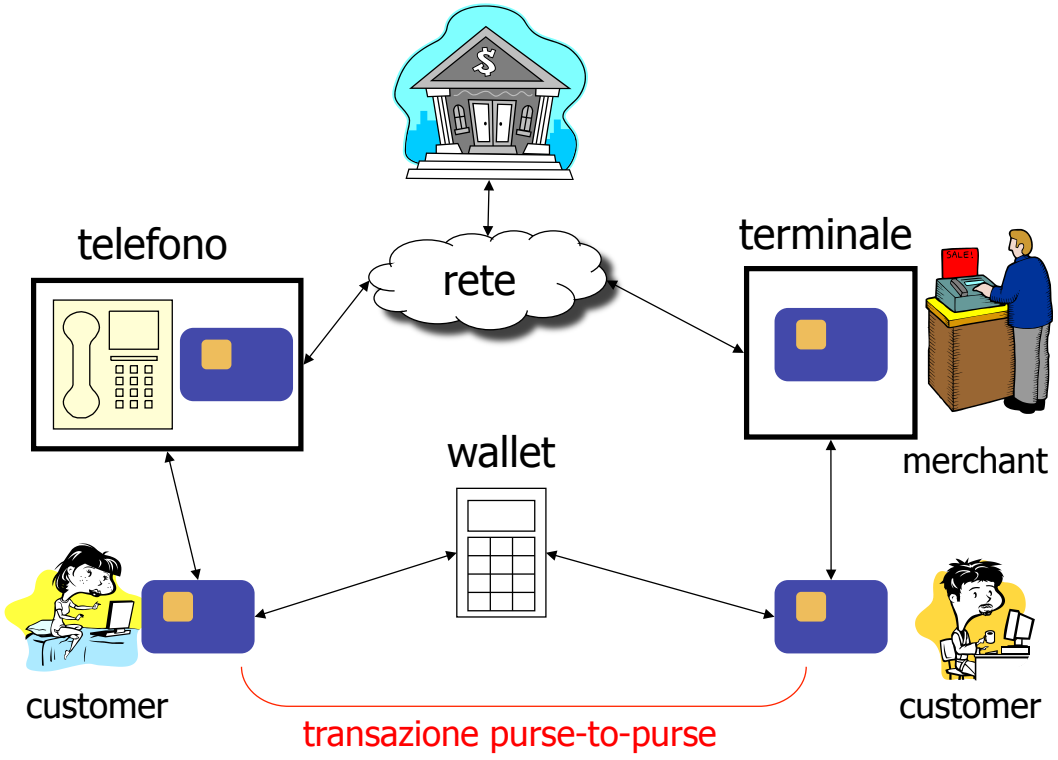
Mondex

- Mondex è un sistema di moneta elettronica con **caratteristiche uniche**
  - è un sistema completamente **aperto** ed **anonimo**
  - è **praticamente l'unico sistema** basato su smart card **in cui**

    il valore monetario è memorizzato nella carta

    le modalità di pagamento corrispondono a quelle con la moneta tradizionale
- **Cenni storici**
  - **1990**: nasce il progetto
  - **1995**: il primo sistema
  - Il consorzio è inglese e composto da British Telecom, National Westminster Bank e Midland Bank

Il sistema



La smart card Mondex

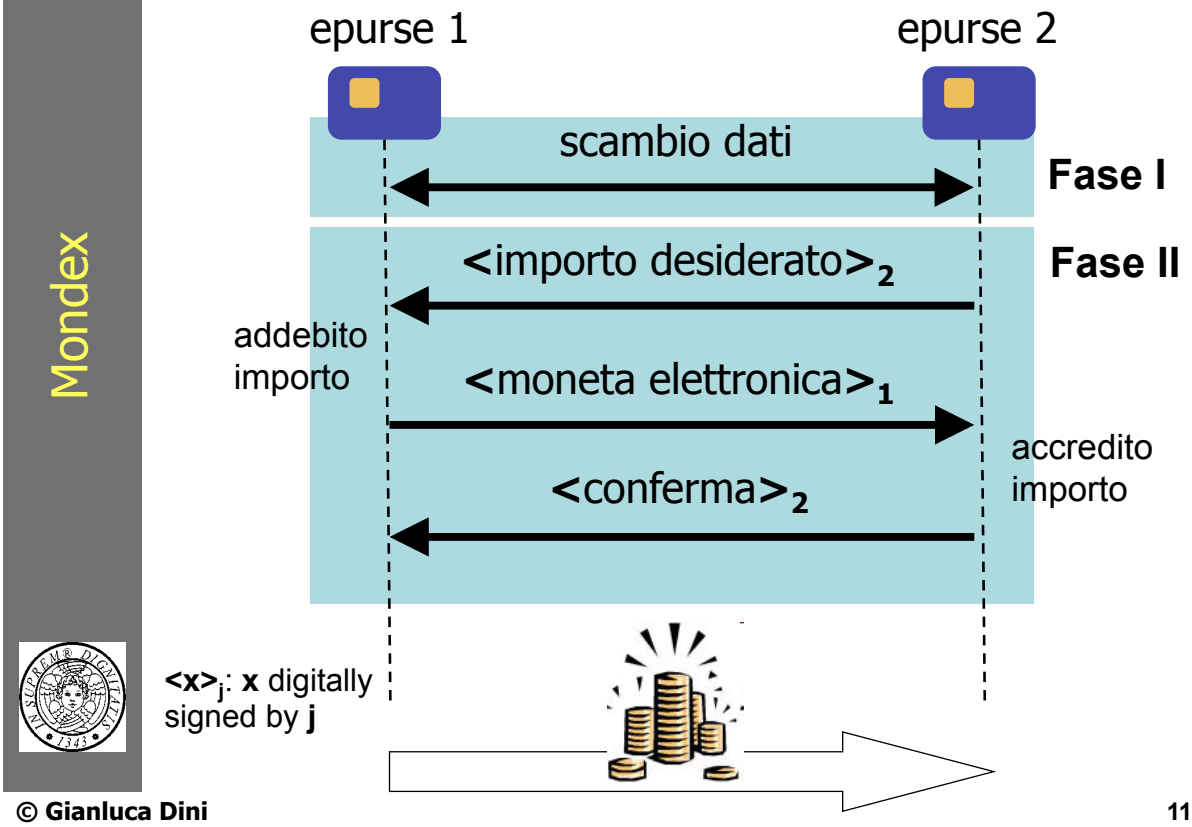
SPECIFICHE FISICHE

- Processore Hitachi H8/3102
- EEPROM: 5 Kbyte
- DES
- Coprocessore (?)
  - RSA (?)

SPECIFICA FUNZIONALE (schema concettuale)

```
class MondexCard  {
    private double saldo = 0.0;
    void credit (double amount) {
       saldo += amount;
    }
    void debit (double amount) {
       saldo -= amount;
    }
}
```

Transazione purse-to-purse (schema)



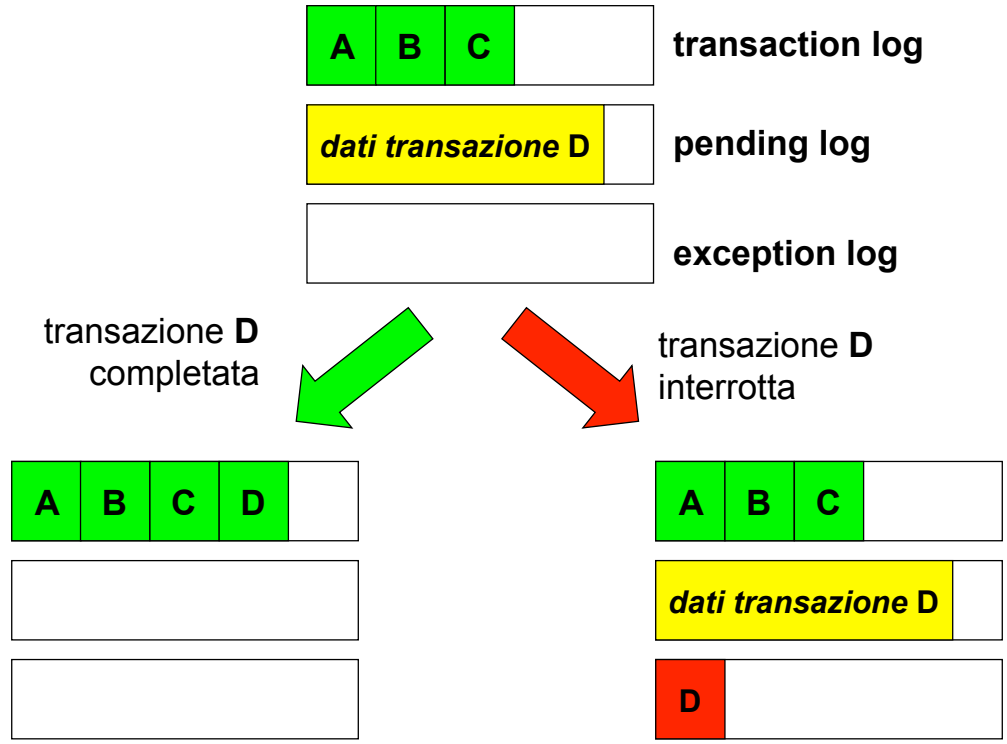
Mondex

Affidabilità della transazione

- Se una transazione viene interrotta, una procedura di **error recovery** permette di farla riprendere e terminare
- Ogni carta Mondex ha **tre log file**:
  - **transaction log**
    specifica le ultime dieci transazioni completate con successo
  - **pending log**
    accumula i dati relativi all'esecuzione di una transazione che sono necessari in caso di error recovery
  - **exception log**
    specifica le transazioni che non sono state completate con successo

Mondex

Affidabilità della transazione



Mondex

Alcuni aspetti di gestione

- **Aggiornamento delle carte**
  - interazione con il background system attraverso il meccanismo "a valanga"
- **Gestione della blacklist**
  - le carte specificate nella black list sono "catturate"
  - le carte specificate nella black list sono "bloccate"
  - dopo un certo numero di transazioni, una carta si blocca automaticamente

    la carta viene sbloccata da un'apposita transazione online che verifica se la carta è elencata bella black list

Mondex

Pro e contro dei borsellini elettronici

- **Vantaggi**
  - **per le banche e l'esercente**
    - ✓ ridotti i costi di gestione del denaro
  - **per l'esercente**
    - ✓ transazioni più veloci ad un costo minore
    - ✓ ridotti i rischi di furto ed atti vandalici
  - **per il consumatore**
    - ✓ transazioni più veloci
    - ✓ contante non è più necessario
- **Svantaggi**
  - **Per il consumatore**
    - ✓ prestito senza interessi al gestore dell'epurse
    - ✓ perdite in caso di fallimento del gestore dell'epurse
    - ✓ perdite in caso di guasto o smarrimento dell'epurse

Pagamenti elettronici

- ✓ **I micropagamenti: CAFE, NetBill, MiniPay, Millicent**

Definizione

- Una qualunque combinazione della nozione di **piccolo valore** (**0.01¥10$**) con quella di
  - **molti pagamenti in breve tempo** e/o
  - pagamenti a **molti esercenti diversi**
  - ad esempio: pay-per-click
- **Problemi**
  - Politica per autorizzazione degli utenti
  - Costi di compensazione dei piccoli pagamenti
- **Soluzioni**
  - alta frequenza / stesso pagante: **CAFE**
  - media frequenza / paganti differenti: **NetBill**, **MiniPay**
- **Non ancora chiaro**
  - alta frequenza / paganti differenti

Hash chain

- *h*: funzione **one-way**, **collision resistant**
- **hash chain**

anchor:	$x_0 = h^n(s) = h(x_1)$
start:	$x_1 = h^{n-1}(s) = h(x_2)$
	...
	$x_{n-1} = h(s) = h(x_n)$
root:	$x_n = h^0(s) = s$

generazione ↑ utilizzo ↓

con $h^k(s) = \underbrace{h(h(\ldots h(s)\ldots))}_{k \text{ volte}}$

CAFE Phone Ticks

commitment

Alice

$<V, h^n(s), 0.1\$>_A$

signed commitment

Vendor

tick payment

Alice

$x_1 = h^{n-1}(s)$ $

$x_2 = h^{n-2}(s)$ $

...

$x_{n-1} = h^1(s)$ $

$x_n = s$ $

Vendor

CAFE Phone Ticks

redemption

$<V, h^n(s), 0.1\$>_A$

+

x_k

massimo tick speso

vendor

acquirer

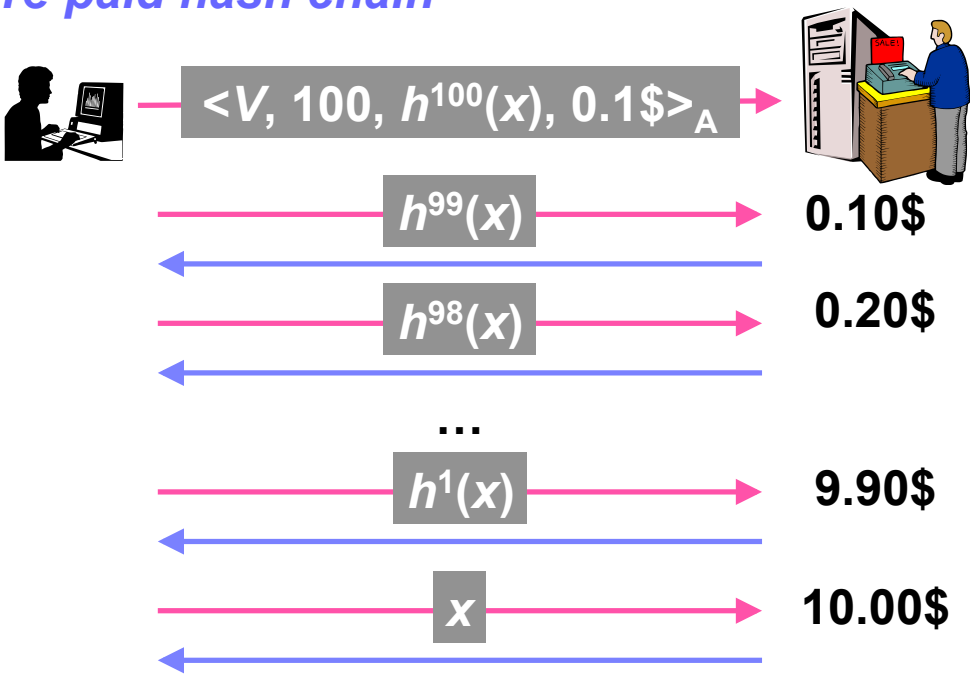
addebito di

k ¥ 0.1$

- Alice paga solo la porzione di catena **effettivamente** spesa
- Il Vendor deve **riporre un certo livello di fiducia** su Alice o fare **frequenti redeemption**

CAFE Phone Ticks

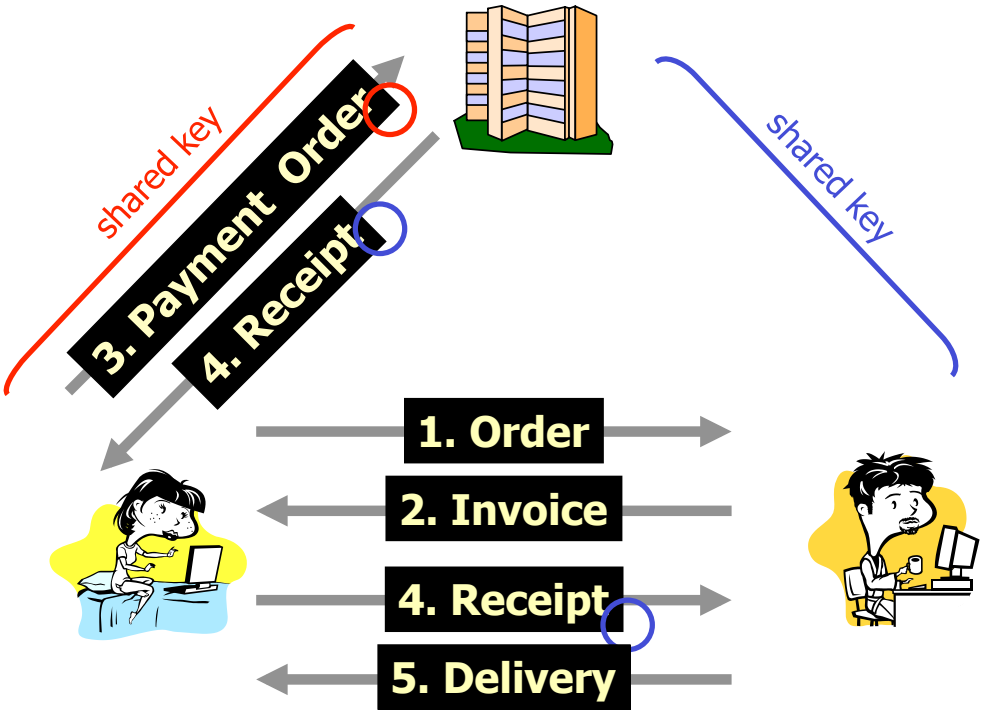
Pre-paid hash chain



CAFE Phone Ticks

- **Pro**
  - **Efficiente: 1 hash per tick**
  - **Approssima il fair exchange di un tick/value**
  - **Può essere integrato con qualunque sistema**
- **Contro**
  - **Adatto solo per pagamenti frequenti allo stesso venditore**

Billing Server

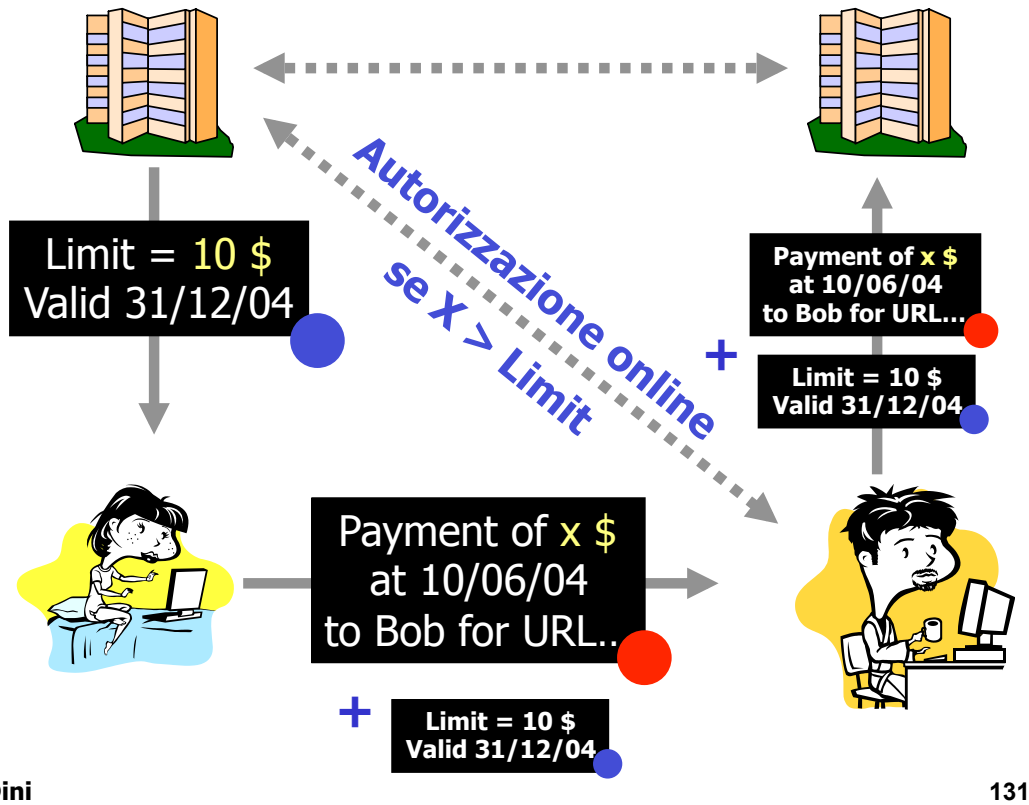


Billing Server

- **Pro**
  - **Efficiente**: MAC-based digital signature
  - **Billing server assicura la fairness**:
    - ✓tiene i soldi fintanto che il servizio non è stato espletato
- **Contro**
  - **Billing server deve essere online**
    - ✓bottleneck
    - ✓deve essere fidato

IBM MiniPay

Micropagamenti



IBM MiniPay

Micropagamenti

- **Pro**
  - **Efficiente**: pochi messaggi
  - **Offline per la maggior parte dei casi**
  - **Basato sulla firma digitale**
    - ✓non ripudio dell'ordine di pagamento
- **Contro**
  - **Basato sulla firma digitale**
    - ✓non adatto per pagamenti frequenti
  - **Le frodi non sono evitate al 100%**

Note

Millicent

- Il sistema **Millicent** è un sistema di micropagamenti (0.1-100 cents)
- progettato a DEC SRC, Palo Alto, California e
- commercializzato da Compaq Corporation (www.millicent.com)

Svantaggi degli altri sistemi

Millicent

- **Carte di credito**
  - Alti costi
- **Account presso un server**
  - Basso overhead di transazione ma un alto overhead iniziale
  - Scoraggia acquisti casuali
  - il server deve mantenere informazioni sui clienti per lunghi periodi di tempo
- **Digital cash**
  - Efficiente ma affetta da double spending

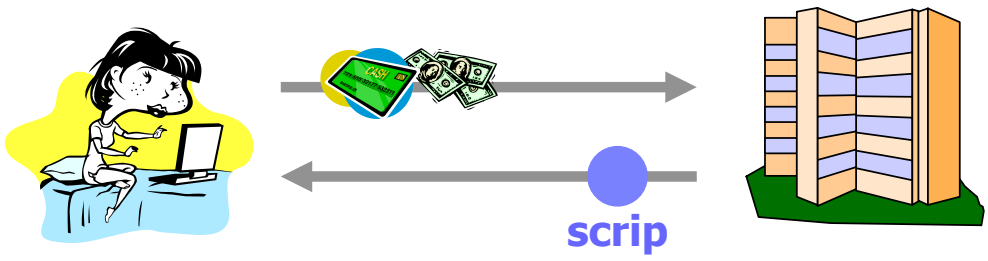
Obiettivi

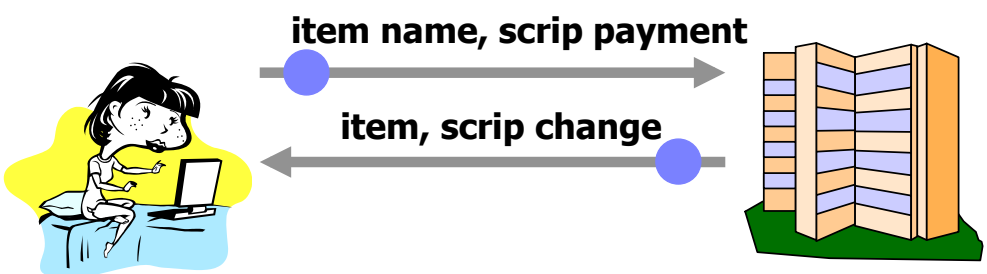
Millicent

- **Efficiente**
  - Sistema distribuito: evita overhead di un sistema concentrato
- **Sicurezza a basso costo**
  - Crittografia non costosa
    - ✓Secret-key cryptography
    - ✓MAC-based signature
- **Free-standing**
  - Non è richiesto un servizio esterno di autenticazione dell'identità degli utenti

Scenario (semplificato)

Millicent





Lo scrip

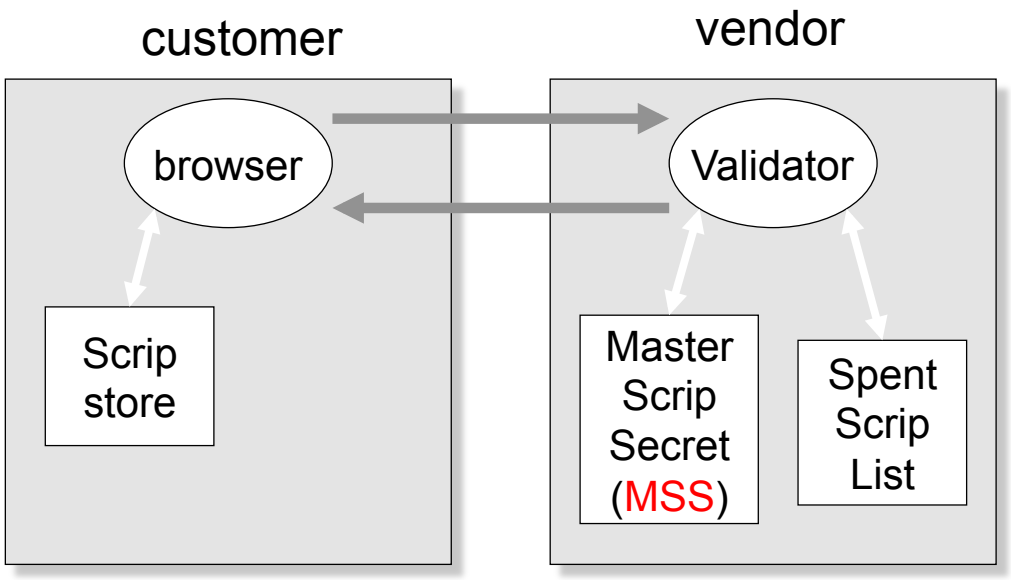
Millicent

Lo scrip è una forma di **digital cash** che

- ha valore solo per uno specifico vendor
- può essere speso una sola volta
- è tamper-resistant e difficile da contraffare
- può essere speso solo dal suo possessore
- può essere prodotto e validato in modo efficiente
- è scalabile
  - ogni vendor valida gli scrip che ha prodotto
- è costituito dai seguenti campi
  - Vendor ID (VID), Value (V), Scrip ID (SID), Customer ID (CID), Expiry date (D), Properties (P), Signature (S)

Il vendor

Millicent



MAC signature method

S = Hash(VID, V, SID, CID, D, P, MSS)

Lo validazione di uno scrip

Millicent

La validazione di uno scrip consiste nei seguenti passi

- Il vendor si accerta che lo scrip non sia stato contraffatto generando una firma a partire dai campi dello scrip e confrontandola con quella contenuta nello scrip (protection against forgery)
- Il vendor si accerta che lo scrip sia sempre valido verificando che non sia ancora spirata la expiry date
- Il vendor si accerta che lo scrip non sia già stato speso verificando che lo Scrip ID non sia presente nella Spent Scrip List(*) (protection against double-spending)

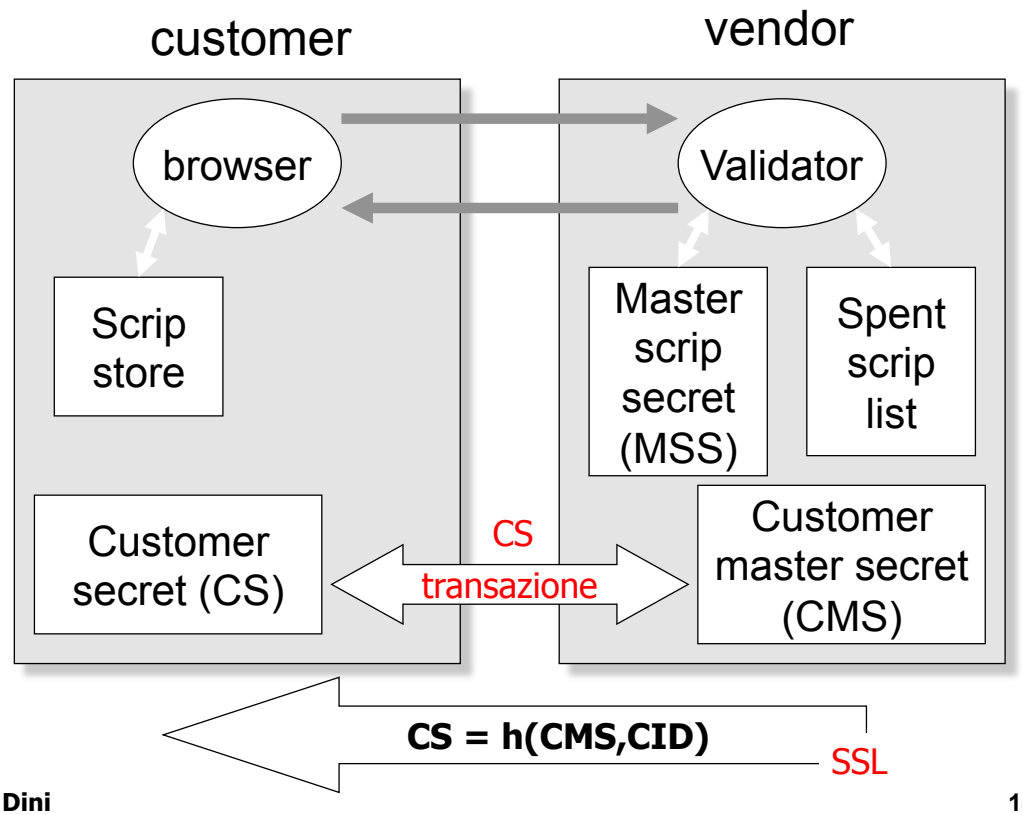
(*) **Gli scrip nella Spent Scrip List la cui Expiry Date è trascorsa vengono rimossi**

Privacy and theft prevention

Millicent

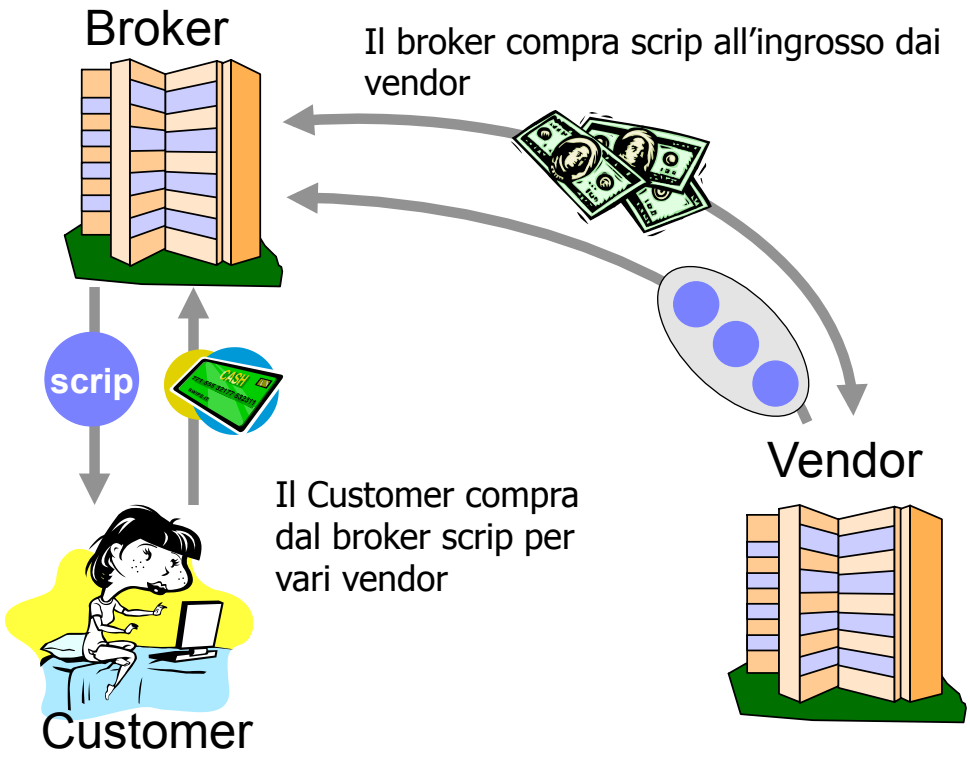
- Il server mantiene il **Customer Master Secret** (**CMS**) e distribuisce al customer CID il **Customer Secret CS** = ***h***(CMS, CID)
- La distribuzione avviene attraverso SSL
- **Per garantire theft prevention** il customer utilizza **CS** per firmare la transazione
- **Per garantire la privacy del customer**, il customer utilizza **CS** per cifrare la transazione

Il vendor



Millicent

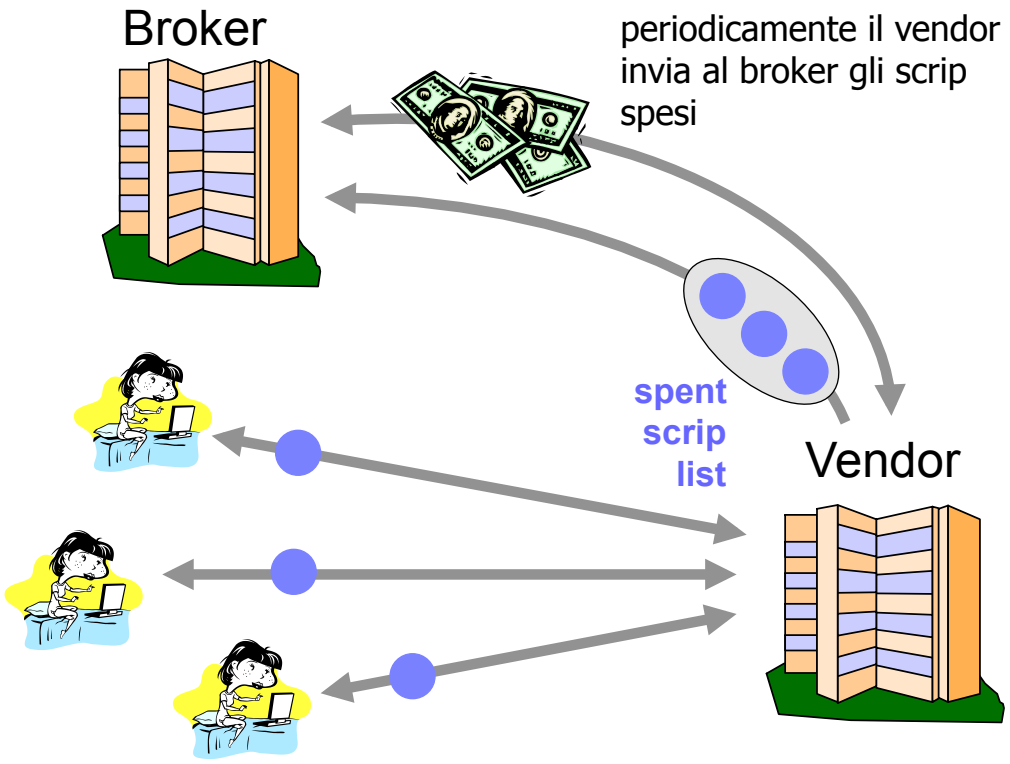
Scenario: broker-based architecture



Millicent

Millicent

Scenario: broker based architecture



Micropagamenti

Situazione dei pagamenti

- "I predict that most sites that are not financed through traditional product sales will move to micropayments in less than two years" (Jakob Nielsen, *The Case for Micropayments*, 1998)
- "You're going to see within the next year an extraordinary movement on the Web of systems for micropayment ... ." (Nicholas Negroponte, 1998)
- "I now finally believe that the first wave of micropayment services will hit in 2000." (Jakob Nielsen, 1999)
- Finora non abbiamo visto i micropagamenti Cosa è successo?

I micropagamenti sono falliti

- **Agli utenti i micro-pagamenti non piacciono**
- **Generano ansietà**
  - Ogni decisione di acquisto causa una certa ansietà;
  - tale ansietà diventa una caratteristica permanente nei micro-pagamenti
  - la transazione vale il livello di ansietà?
- **Generano confusione**
  - Al di sotto di un certo valore, è difficile valutare se una merce o un servizio valgono quel prezzo
- **Sono solo dei sistemi di pagamento**
  - Devono "aiutare i clienti a spendere" il loro denaro e non forzarli a spendere in un certo modo

Come si comprano "small things"?

Soluzioni classiche

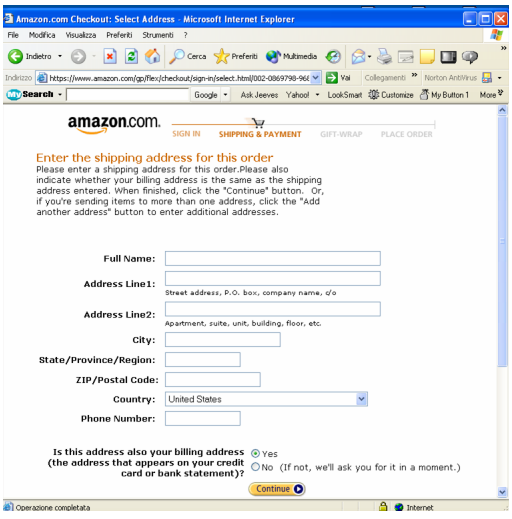
- **Aggregazione (aggregation)**
  - Dysneyland pricing model
  - Esempio: giornale, articoli
- **Abbonamento (subscription)**
  - Aggregazione + predicibilità (100$ adesso sono meglio di 100$ tra un mese) + incentivo rapporto a lungo termine
- **Sovvenzione (subsidy)**
  - Pubblicità
  - Weblog movement

Pagamenti elettronici

- ✓ Borsellini elettronici

Concetti generali

- **Un acquisto online richiede, tipicamente, di compilare una form (operazione noiosa)**



- **Il 65% degli acquirenti online, dopo aver scelto il prodotto di interesse, non porta a termine l'acquisto**

Concetti generali

- Il **borsellino elettronico** (**electronic wallet**) evita all'utente di dover reinserire ad ogni acquisto i dati per la consegna ed i dati relativi al metodo di pagamento
  - Un portafoglio tradizionale contiene carte di credito, assegni, moneta, informazioni sul possessore, …
- Queste informazioni sono memorizzate nel borsellino e sono passate direttamente al server di commercio elettronico al momento dell'acquisto
- Ill borsellino elettronico rende più **efficiente** l'acquisto online (click)

Esempi

- **Agile Wallet** (CyberCash & Agile Wallet Tech.)
  - dati remoti su di un server sicuro
- **eWallet** (LaunchPad Tech.)
  - scaricabile ed installabile gratuitamente
  - dati locali cifrati e protetti da password
  - compatibile con IE e Netscape
- **Microsoft Wallet**
  - compatibile con IE
  - dati locali cifrati e protetti da password

(*continua*)

Esempi

- **Common Markup for Web Micropayment Systems** (W3C)
  - standard
  - interoperabilità
  - espandibilità
- **Electronic Commerce Modeling Language**
  - ECML è un consorzio costituito da AOL, IBM, Microsoft, Visa MasterCard
  - Cerca di affermarsi come standard