

Protocollo E-cash ed algoritmo RSA

Carlo Manasse

Giulio Baldantoni

Corso di laurea in Informatica

May 10, 2012

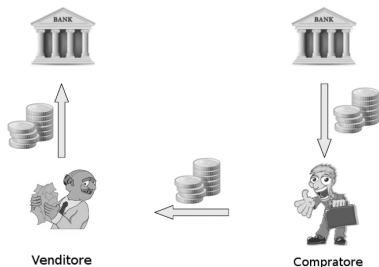
- **Moneta elettronica**
 - Introduzione
 - E-Cash
 - Esempi
- **Algoritmo RSA**
 - Cifratura - Decifratura
 - Esempio numerico
 - Firma
 - Firma Cieca

I sistemi di pagamento elettronico riguardano il commercio elettronico e quindi lo svolgimento di attività commerciali e di transizioni per via elettronica quali:

- commercializzazione di beni e servizi
- effettuazioni di operazioni finanziarie e di borsa
- l'utilizzo di apparecchiature che consentono lo svolgimento di alcune operazioni, senza interazione diretta tra le parti (carte di credito)

Gli acquisti effettuati attraverso questo sistema prevedono ovviamente un pagamento elettronico, cioè un pagamento virtuale senza passaggio fisico di denaro, per questo entra in gioco la moneta elettronica.

Perché i pagamenti elettronici stanno diventando di uso sempre più comune?



Per le Aziende : aumentare la competitività, ridurre i costi

Per il Cliente : servizi personalizzati, prezzi convenienti

Le caratteristiche principali che un sistema Digital Cash deve possedere, sono :

- SICUREZZA
- ANONIMATO
- SCALABILITA'
- ACCETTABILITA'
- TRASFERIBILITA'
- INDIPENDENZA DELL'HARDWARE
- TIPOLOGIE DI PAGAMENTO
- COSTI DI GESTIONE

Ricordiamo tra questi i più conosciuti : E-cash e CAFE.

E-cash (Electronic Cash Payment Protocol) è un sistema di pagamenti sicuri per Internet elaborato da Digicash, introdotto nel 1993;

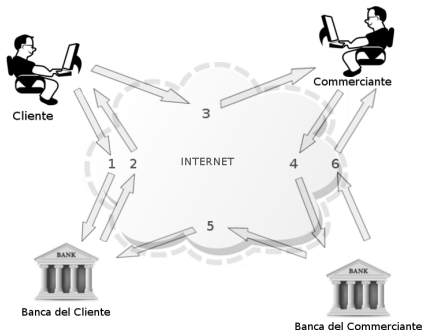
Utilizza RSA crittografia a chiave pubblica, il funzionamento chiave di E-cash è l'uso della 'Firma cieca' che garantisce anonimato e privacy, solo da chi effettua il pagamento.

La banca che per prima ha creduto e ha dato un contributo al progetto è stata la Mark Twain Bank, Saint Louis (Missouri), nel 1995.

Tre partecipanti sono coinvolti nel modello Ecash:

- 1 Clienti:
 - Hanno il software Ecash (cyberwellet) sui propri dispositivi.
 - Possono usare E-coins del loro portafoglio per fare acquisti dai commercianti.
 - Ritirano le monete dai loro conti presso le banche associate.
 - Memorizzano e gestiscono tutte le proprie transazioni.
- 2 Commercianti:
 - Accettano ed elaborano i pagamenti.
 - Interagiscono con una banca associata per eseguire la convalida e l'autenticazione.
 - Vendono oggetti e generano entrate.
- 3 Banche:
 - Dove i clienti e i commercianti hanno conti presso una banca associata.
 - Gestiscono i conti dei clienti e commercianti.

Procedura di pagamento con Ecash



- 1 Il Cliente invia la moneta codificata con il numero di serie per la Banca.
- 2 La Banca rimanda indietro al Cliente la moneta firmata.
- 3 Il Cliente decodifica il numero di serie ed usa la moneta per pagare.
- 4 Il Commerciante manda questa moneta alla propria Banca.
- 5 Le due Banche effettuano la verifica sulla moneta.
- 6 Il Commerciante riceve la conferma e l'accredito.

Demo

Enrico
Francesco
Giulio
Carlo

Carlo
Manasse
Giulio
Baldantoni

DEMO

Conclusioni

Carlo
Manasse
Giulio
Baldantoni

PRO	CONTRO
Permette pagamenti su Internet Peer-to-peer Anonimo Adatto per micro-pagamenti Gratuito Non c'è bisogno di terzi Leggero	Non è adatto per grandi quantità Non è Internazionale

Anche se tutto quello che il sistema offre sembrava essere molto promettente, il suo successo non si è evoluto come ci si aspettava.

Conclusioni

Alcuni imputano il fallimento al modo in cui i sistemi sono stati implementati :
richiedendo troppi step durante la configurazione del software client-server,
per un utente medio.

Altri attribuiscono il fallimento alla mancata definizione di uno standard, data
la molteplicità di implementazioni concorrenti.