CRATOS
Centro di Ricerca sulle Applicazioni della Telematica
alle Organizzazioni e alla Società

Introduzione all'utilizzo di carte di credito nei pagamenti su Internet

L. Delgrossi
e-mail: ldgrossi@pc.unicatt.it

Quaderni del CRATOS

Serie di Economia
CTR-E98-002

Università Cattolica del Sacro Cuore – Piacenza, Italia

Contenuti

Uno dei fattori critici per la crescita e la diffusione del commercio elettronico su Internet nei prossimi anni è l'adozione di un appropriato metodo di pagamento. A questo proposito, sembra naturale tentare di sfruttare metodi già sperimentati e diffusi nella pratica comune e definirne una versione elettronica che ne estenda l'utilizzo agli utenti della rete. In questo documento, discutiamo le caratteristiche fondamentali delle transazioni con carta di credito e presentiamo alcuni metodi di pagamento elettronico basati sull'uso della carta di credito tra quelli recentemente proposti.

1. Introduzione

Uno dei fattori critici per la crescita e la diffusione del commercio elettronico su Internet nei prossimi anni è l'adozione di un appropriato metodo di pagamento. A questo proposito, sembra naturale tentare di sfruttare metodi già sperimentati e diffusi nella pratica comune per definirne una versione elettronica che ne estenda l'utilizzo agli utenti della rete. In questa ottica, sono stati proposti negli ultimi due anni una serie di metodi di pagamento on-line basati sull'utilizzo della carta di credito [1] [2] [4].

Quando si traduce uno schema di pagamento progettato per il mondo reale nel suo corrispondente elettronico, è necessario considerare una serie di problemi non convenzionali, determinati in gran parte dall'assenza di contatto fisico tra i diversi soggetti coinvolti. Ad esempio, durante la vendita di un prodotto su Internet, non c'è contatto visivo tra l'acquirente e il venditore[1] e questo fatto può tendenzialmente favorire simulazioni da parte di individui non autorizzati e frodi ripetute. Su Internet, cioè, non possiamo essere in generale certi dell'identità della persona con cui stiamo comunicando. Inoltre, le informazioni che viaggiano sulle reti telematiche pubbliche come Internet sono potenzialmente esposte a sofisticati attacchi automatizzati, come l'utilizzo di filtri software per estrarre da tutti i messaggi elettronici che attraversano una dato nodo della rete i numeri di carta di credito che vi sono contenuti, e come i sottili e difficilmente controllabili attacchi operati dagli hacker [2]. Questi fattori portano gli utenti della rete a diffidare dal suo utilizzo in un ambito critico come quello dei pagamenti. E' quindi necessario assicurare alle transazioni on-line un adeguato livello di protezione e sicurezza.

Un altro aspetto da considerare riguarda la natura stessa delle transazioni on-line. Per quanto ogni previsione possa oggi essere incerta, la natura del commercio su Internet sembra essere orientata per una parte significativa ad un numero elevatissimo di transazioni di importo molto basso, anche frazioni di centesimo di dollaro statunitense[2]. Per denotare questo tipo di transazioni, è diventato di uso comune il termine *micropagamenti*. Sotto il profilo dei micropagamenti, l'utilizzo della carta di credito non sembra particolarmente attraente, dato l'alto costo per transazione che questo sistema comporta. Si pone cioè il rischio che il costo delle procedure di completamento di una transazione sia troppo elevato rispetto all'importo della transazione stessa[3]. Tuttavia, esistono altri importanti fattori che giustificano gli attuali sforzi dei ricercatori e degli istituti di credito per realizzare uno schema di pagamento on-line basato sull'uso della carta di credito, a cominciare dalla larga diffusione su scala mondiale di questo metodo che può potenzialmente garantire un elevatissimo numero di utenti. Inoltre, dato che il sistema della carta di credito è diventato ormai di uso comune, gli istituti di credito possono trarre vantaggio dal fatto che non saranno necessari investimenti specifici per la formazione degli utenti. Infine, il sistema della carta di credito aiuta a risolvere il problema della registrazione degli

[1] L'utilizzo di video digitale su Internet è tuttora limitato da fattori tecnici. In futuro, la disponibilità di canali di comunicazione a larga banda e di dispostivi multimediali su tutti i personal computer potrebbero richiedere una modifica di questa affermazione.

[2] Varian anticipa alcuni problemi legati all'economia dell'informazione e si chiede quanto potrebbero valere due bit nel cybermercato [7].

[3] La pratica comune indica che attualmente, negli Stati Uniti, l'importo medio di una transazione è di circa 60 dollari [2].

utenti, che, come vedremo in seguito, è uno dei principali problemi da considerare nell'ambito dei metodi di pagamento elettronici.

In questo breve articolo, discutiamo le caratteristiche fondamentali delle transazioni con carta di credito (Sezione 2) e presentiamo alcuni metodi di pagamento on-line tra quelli recentemente proposti (Sezioni 4, 5, 6). Dato che la maggior parte dei metodi di pagamento utilizzano tecniche crittografiche per assicurare un determinato livello di sicurezza, illustriamo sinteticamente alcuni elementi di crittografia (Sezione 3). Alcune conclusioni sono presentate nella Sezione 7.

2. Transazioni con carta di credito

Il completamento di una transazione con carta di credito coinvolge i seguenti soggetti:

- Un acquirente
- Un venditore
- I rispettivi istituti di credito
- Una rete di autorizzazione dei pagamenti
- Un sistema di pagamento tra istituti di credito

La rete di autorizzazione dei pagamenti collega venditori e istituti di credito. Ciascun venditore possiede un dispositivo in grado di leggere le informazioni registrate sulla banda magnetica posta sul retro della carta di credito ed inviarle alla rete di autorizzazione[4]. La rete di autorizzazione, a fronte della richiesta del venditore, invia un segnale di risposta, concedendo o negando l'autorizzazione.

Il sistema di pagamento interbancario ha il compito di risolvere le posizioni debitorie tra gli istituti di credito. Naturalmente, se l'acquirente e il venditore sono clienti del medesimo istituto di credito, il passaggio tramite il sistema di pagamento interbancario non è necessario.

I soggetti coinvolti in una generica transazione sono rappresentati nella Figura 1. Per semplificare la figura, sono stati indicati con *servizi interbancari* sia la rete di autorizzazione di pagamento che il sistema di risoluzione dei pagamenti tra banche[5].

[4] Se il venditore non dispone della carta di credito, egli può comunque immettere i dati relativi alla carta tramite una tastiera numerica.

[5] Questo riflette la situazione italiana, nella quale le due funzioni sono svolte dalla Società di Servizi Interbancari di Milano.

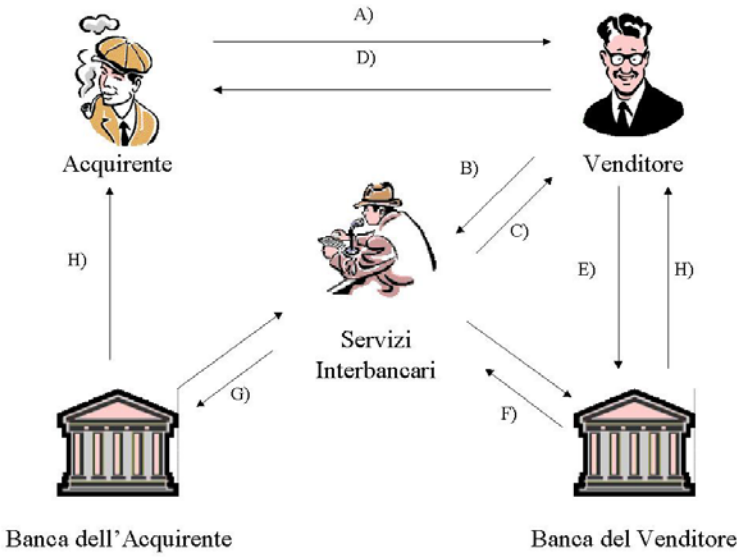

Figura 1: Schema di transazione con carta di credito

2.1 Schema di pagamento

Esaminiamo ora in maggiore dettaglio i passaggi che sono necessari per il corretto completamento di una transazione con carta di credito:

a) l'acquirente, al momento del pagamento, presenta la carta di credito al venditore,

b) il venditore utilizza la carta di credito per richiedere l'autorizzazione a procedere,

c) la rete 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, egli 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.

L'istituto di credito che concede una carta di credito ad un proprio cliente, se ne assume allo stesso tempo i relativi rischi. Il commerciante che accetta un pagamento con carta di credito e ottiene una regolare autorizzazione dalla rete di autorizzazione dei pagamenti è sicuro di venire comunque pagato dall'istituto di credito, il quale si fa carico della riscossione del pagamento dall'acquirente. Come controparte, il commerciante rinuncia ad una piccola percentuale[6] sugli importi delle transazioni. Anche l'acquirente che utilizza una carta di credito per il pagamento gode di alcuni benefici: ad esempio, se il commerciante fallisce prima di avere consegnato il prodotto o fornito il servizio oggetto della transazione, l'acquirente può ottenere

[6] In genere, si tratta di una percentuale vicina al 4%.

immediato risarcimento dalla banca, al contrario di quanto avviene per gli assegni bancari.

Nella pratica comune, esistono diversi casi in cui il commerciante accetta un pagamento anche se la carta di credito non è presente. Ad esempio, questo succede spesso per prenotazioni telefoniche di camere di albergo. Nelle transazioni con carta assente, il venditore non ha la possibilità di verificare che la firma del cliente sia corretta. In questo caso, il venditore si assume i rischi di frode, mentre il rischio di mancato pagamento grava sempre sull'istituto di credito.

2.2 Meccanismi di Sicurezza

Lo schema di pagamento descritto contiene una serie di meccanismi volti a garantire la sicurezza delle transazioni: il numero della carta di credito è scolpito in rilievo in modo da non poter essere alterato; la firma autografa dell'acquirente deve essere confrontata con la firma apposta sul retro della carta a garanzia della corretta identificazione dell'acquirente; le copie della nota di vendita generate dall'apposito dispositivo tutelano l'integrità della transazione; infine, il commerciante ottiene immediata conferma del pagamento dalla rete di autorizzazione.

In generale, possiamo distinguere i seguenti requisiti di sicurezza per i metodi di pagamento elettronici:

- *Identificazione*: la carta di credito deve essere associata ad un conto corrente bancario in modo certo ed univoco,
- *Autenticazione*: il venditore deve poter essere certo che il latore della carta è effettivamente la persona autorizzata ad utilizzarla,
- *Integrità*: i soggetti coinvolti nella transazione devono avere tutti una visione unica della natura della transazione,
- *Confidenzialità*: le informazioni associate alla transazione non devono essere accessibili a terzi,
- *Conferma*: il venditore deve avere la certezza del pagamento al momento della consegna della merce.

Ottenere un adeguato livello di sicurezza significa poter assicurare che ciascuno di questi requisiti venga osservato. A questo scopo, nell'ambito delle comunicazioni su reti telematiche vengono in genere utilizzate tecniche crittografiche; nella prossima sezione, presentiamo in breve sintesi alcune delle tecniche più comuni.

3. Sicurezza

Per proteggere le comunicazioni da una serie di possibili attacchi da parte di individui non autorizzati, è possibile utilizzare tecniche crittografiche. Queste tecniche sono basate sulla cifratura di un testo in chiaro per renderlo illeggibile. Il testo cifrato viene ottenuto tramite l'applicazione di un algoritmo di cifratura basato su una chiave segreta. Il messaggio cifrato viene poi trasmesso alla destinazione, che possiede la chiave necessaria per la decodifica (Figura 2). Anche nel caso in cui il messaggio venisse intercettato durante il trasferimento dalla sorgente alla destinazione, esso rimarrebbe comunque illeggibile per l'intruso a meno che questi non sia in possesso della chiave di decodifica. Si noti come la segretezza delle comunicazioni risieda interamente nella chiave, mentre l'algoritmo di cifratura può anche essere reso noto.

Quando si utilizza la medesima chiave per cifrare e decifrare, diciamo che si tratta di un sistema di cifratura simmetrico. Questo tipo di sistema, che è il più

tradizionale, è particolarmente efficiente ma presenta alcuni inconvenienti: 1) la chiave segreta deve essere comunicata in precedenza tramite un canale sicuro; 2) per ogni coppia di interlocutori, è necessario disporre di una chiave: questo conduce ad un numero di chiavi da utilizzare molto elevato[7]. Per ovviare a questi inconvenienti, sono stati ideati sistemi di crittografia asimmetrici, in cui le chiavi utilizzate per cifrare e decifrare sono differenti.

Nei sistemi asimmetrici ciascun individuo dispone di una coppia di chiavi, una pubblica e l'altra privata. Le due chiavi hanno la proprietà che ciascuna di esse decifra quanto cifrato con l'altra. Mentre la chiave pubblica è resa nota e disponibile a tutti, quella privata è segreta. L'utilizzo di una coppia di chiavi asimmetriche consente di ottenere diversi risultati dal punto di vista della sicurezza. Ad esempio, per inviare un messaggio riservato ad un interlocutore è sufficiente cifrare il messaggio con la sua chiave pubblica (disponibile a tutti). Solo l'interlocutore, che dispone della propria chiave privata, è in grado di decifrare il messaggio. Allo stesso modo, per garantire l'autenticità di un messaggio, è sufficiente cifrarlo con la propria chiave privata. In questo modo il messaggio sarà leggibile per tutti e certamente autentico. Con la crittografia asimmetrica si riduce il numero delle chiavi da utilizzare (per N individui sono necessarie solo 2*N chiavi) e si evita che mittente e destinazione debbano scambiarsi la chiave prima di poter effettuare una comunicazione sicura. D'altra parte, le chiavi asimmetriche, a causa delle loro proprietà, sono più complesse da generare e richiedono alti costi in termini di tempo di esecuzione delle operazioni di cifratura e decifratura.

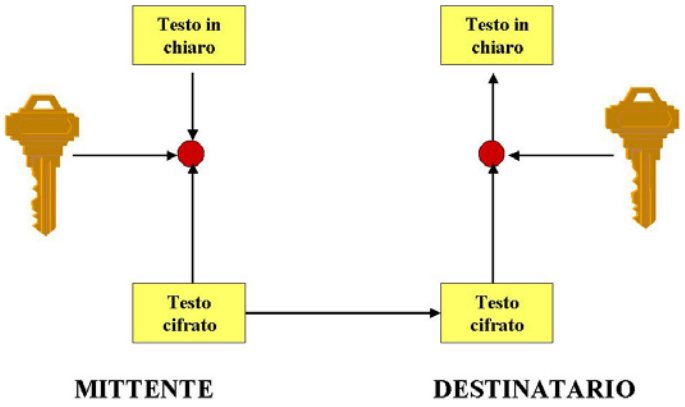

Figura 2: Codifica e decodifica tramite chiavi crittografiche

Nel seguito, illustreremo alcuni metodi di pagamento elettronici. Mentre il metodo realizzato da First Virtual (Sezione 4) non fa uso di tecniche crittografiche, i metodi CyberCash e SET (Sezioni 5 e 6 rispettivamente) sfruttano tecniche di crittografia asimmetrica. Per approfondimenti sulla crittografia si rimanda a [3], [4] e per una discussione completa dell'argomento alla lettura di [11].

4. Il metodo First Virtual

First Virtual è una azienda creata nel 1994 per offrire servizi di tipo commerciale su Internet. Il carattere virtuale dell'azienda, fondata da quattro partner residenti in diversi stati degli Stati Uniti e priva di una sede fisica, è molto interessante ed illustrato in dettaglio in [5]. Il sito web di First Virtual (http://www.fv.com) mette a

[7] Un gruppo di N interlocutori necessita di N * (N - 1) / 2 chiavi simmetriche.

disposizione informazioni sia sulla società che sul sistema di pagamento adottato, singolare in quanto non basato sull'utilizzo di tecniche di crittografia [8] [9]. Questo schema di pagamento è denominato *modello verde* (*green model*).

First Virtual si propone come intermediario tra Internet, dove acquirenti e commercianti si incontrano e si accordano sulla natura ed entità degli scambi, e le reti di pagamento interbancarie. Lo schema di pagamento adottato è misto in quanto prevede sia l'utilizzo di Internet che quello di canali di comunicazione off-line. Per poter usufruire dei servizi offerti da First Virtual è sufficiente disporre di un indirizzo di posta elettronica; questo fatto ha facilitato molto la diffusione di questo sistema e ha dato, nei primi anni di attività, un immediato vantaggio competitivo a First Virtual rispetto ai suoi diretti concorrenti.

Il metodo di pagamento *modello verde* è basato sulla identificazione dell'utente tramite un codice personale segreto (*virtual PIN*) e su un meccanismo di conferma mediante posta elettronica. Se un utente desidera fare un acquisto tramite First Virtual, egli deve innanzitutto registrarsi comunicando i propri dati anagrafici, le informazioni relative alla carta di credito che desidera utilizzare ed il proprio indirizzo di posta elettronica. Queste informazioni vengono comunicate a First Virtual attraverso un canale sicuro off-line, in genere mediante telefono o per posta. In questo modo, le informazioni critiche non vengono mai trasmesse su Internet. In seguito alla registrazione, First Virtual fornisce all'utente un codice personale (virtual PIN) segreto.

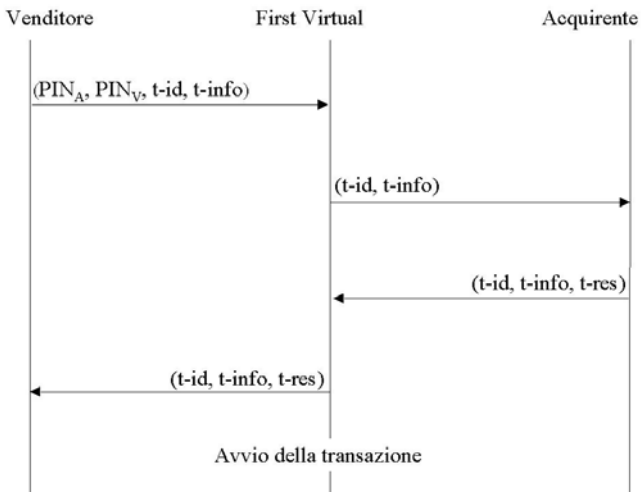

Figura 3: Modello Verde di First Virtual

Quando l'utente vuole autorizzare un pagamento, egli comunica il proprio virtual PIN al venditore in modo non definito da First Virtual. Ad esempio, egli potrebbe inviarlo tramite posta elettronica oppure come password di ingresso ad un server ftp, o ancora in altri modi. Il venditore invia un messaggio al server di First Virtual con una descrizione della transazione ed i due virtual PIN. Il server di First Virtual, usa il virtual PIN dell'acquirente per eseguire una ricerca all'interno della propria base dati utenti. In questo modo, si risale alle informazioni dell'utente ed in particolare al suo indirizzo di posta elettronica. Il server spedisce allora un messaggio di posta elettronica a questo indirizzo chiedendo conferma per l'autorizzazione di pagamento. L'utente che riceve questo messaggio deve rispondere (tramite posta elettronica) con *sì*, *no* oppure *frode*. La risposta *no* indica che l'utente ha cambiato idea e non intende perfezionare l'acquisto. La risposta *frode* indica che l'utente non aveva inviato alcuna

richiesta di acquisto e che qualcun altro sta tentando di utilizzare illecitamente il suo virtual PIN. Solo se l'utente risponde *sì*, la transazione viene avviata. Lo schema è rappresentato in Figura 3. Nella figura, il campo *t-id* contiene un identificatore di transazione, *t-info* le informazioni relative alla transazione e *t-res* la risposta (sì, no, o frode) dell'acquirente. Il modello verde prevede l'utilizzo di altri messaggi ad esempio per richiedere informazioni sui servizi offerti dal server di un venditore, ottenere una storia delle transazioni effettuate, o verificare che un virtual PIN sia attivo.

Nel modello, non è possibile escludere che il virtual PIN cada nelle mani di persone non autorizzate (infatti, esso non è protetto in alcun modo ed è leggibile in chiaro). Tuttavia, anche se questo dovesse accadere, il PIN non potrebbe comunque essere utilizzato al di fuori di Internet e senza disporre di accesso alla posta elettronica dell'utente[8]. Impadronirsi di un virtual PIN risulta quindi più semplice per un malintenzionato, ma i vantaggi che se ne possono trarre sono molto ridotti. Per poter utilizzare il virtual PIN, il truffatore dovrebbe avere accesso al computer dell'utente ed in particolare conoscere la password di accesso alla sua casella di posta elettronica, ma, in simili circostanze, neppure i metodi crittografici più sicuri risultano utili.

5. Il metodo CyberCash

Nel 1995, CyberCash ha realizzato un sistema per collegare in modo sicuro Internet e le reti di autorizzazione di pagamento degli istituti di credito. Tramite questo sistema, un utente di Internet può acquistare beni dal negozio virtuale di un commerciante e utilizzare la propria carta di credito per effettuare pagamenti on-line. Il sistema consiste di un apposito pacchetto software per commercianti ed acquirenti e di un gateway (cioè un computer che opera come collegamento tra due reti telematiche) che collega Internet alle reti di autorizzazione degli istituti di credito.

Il pacchetto software consiste essenzialmente in un portafoglio elettronico e può essere scaricato gratuitamente dal sito web di CyberCash (http://www.cybercash.com). In questo modo, chiunque disponga di un Internet browser può scaricare ed installare il software sul proprio Personal Computer nelle modalità e tempi più convenienti.

CyberCash garantisce agli acquirenti la confidenzialità dei messaggi elettronici in cui essi forniscono informazioni riservate relative alla propria carta di credito. Inoltre, CyberCash garantisce l'autenticità dei messaggi elettronici che commercianti e clienti si scambiano durante le diverse fasi della vendita on-line. Il metodo CyberCash costituisce un esempio pratico di come sia possibile utilizzare tecniche di crittografia a chiave asimmetrica per ottenere protezione per le transazioni on-line.

5.1 Il Portafoglio Elettronico

La vendita on-line necessita di una fase preliminare durante la quale vengono registrate le informazioni fondamentali relative a clienti e commercianti e vengono predisposti i meccanismi di sicurezza. Come primo passo, commercianti ed acquirenti devono dotarsi del pacchetto software fornito da CyberCash, che consiste essenzialmente in un portafoglio elettronico.

Dopo aver installato il portafoglio elettronico sul proprio PC, il cliente può registrarvi i dati relativi a una o più carte di credito con le quali intende pagare la

[8] Se invece si trattasse di un numero di carta di credito, questo potrebbe essere utilizzato per una serie di frodi che non comportano l'utilizzo di Internet.

merce acquistata. Il portafoglio è in grado di memorizzare queste informazioni e mantenere la contabilità aggiornata delle transazioni effettuate dall'acquirente con ciascuna delle carte di credito. Ad esempio, dopo il perfezionamento di un acquisto on-line, il portafoglio elettronico memorizzerà il tipo di prodotto acquistato, le sue caratteristiche, l'importo versato, l'identità del venditore ed altre informazioni di questo genere. I venditori dispongono di un software simile.

La funzione più importante che il software di portafoglio elettronico svolge è relativa alla sicurezza ed in particolare alla generazione e gestione di chiavi asimmetriche. Il software contiene, codificata internamente, la chiave pubblica di CyberCash. Questa chiave viene utilizzata per cifrare i messaggi o le porzioni di messaggio che si desidera solo CyberCash possa decifrare. Inoltre, durante la propria fase di inizializzazione, il software del portafoglio elettronico genera una coppia di chiavi asimmetriche per l'acquirente. Delle due chiavi generate, quella privata viene conservata dall'acquirente e mantenuta segreta, mentre quella pubblica viene inviata a CyberCash con un messaggio cifrato con la chiave pubblica di CyberCash.

Al termine della fase di registrazione, ciascun acquirente e ciascun venditore è in grado di comunicare in modo sicuro con CyberCash e viceversa. Notiamo come questo schema presupponga che acquirenti e venditori ritengano CyberCash un partner affidabile: infatti, anche se le chiavi private sono segrete, esse sono state generate mediante il software distribuito da CyberCash. Questa osservazione pone un problema interessante e cioè come può CyberCash, o più in generale chiunque distribuisca software per generare coppie di chiavi asimmetriche, dimostrare che il software distribuito garantisce la segretezza delle chiavi generate anche nei confronti di chi lo ha programmato?

Infine, osserviamo che lo schema non consente a clienti e venditori di comunicare tra loro in modo confidenziale e pertanto queste comunicazioni dovranno avvenire tramite messaggi in chiaro.

5.2 Meccanismi di Sicurezza

Analizziamo adesso in maggiore dettaglio le diverse fasi di cui il metodo di pagamento CyberCash è composto: immaginiamo ad esempio che l'acquirente "A" intenda acquistare un prodotto offerto dal venditore "V". Sia A che V hanno registrato in precedenza i propri dati presso CyberCash e, come risultato di questa registrazione, sia A che V dispongono ora di una coppia di chiavi, l'una pubblica e l'altra privata. Indicheremo con D_A (D_V) ed E_A (E_V) rispettivamente la chiave privata e la chiave pubblica di A (V). Sia A che V conoscono la chiave pubblica E_{CC} di CyberCash, mentre CyberCash conosce le chiavi pubbliche E_A ed E_V.

In questo scenario, A e V sono in grado di comunicare con CyberCash in modo riservato: infatti, è sufficiente che essi codifichino i loro messaggi utilizzando la chiave E_{CC}. Osserviamo come CyberCash non renda nota a V la chiave pubblica di A né viceversa. Questo significa che la comunicazione tra A e V dovrà avere luogo tramite una serie di messaggi in chiaro.

Quando A decide di acquistare un prodotto commerciale offerto da V, seleziona il prodotto tramite il proprio browser e invia una *richiesta di acquisto* al server del venditore. Il server produce una *richiesta di pagamento* (cioè un messaggio che descrive la natura della merce, le condizioni di vendita e il tipo di carta di credito che il venditore accetta per il pagamento) e lo spedisce all'acquirente. Il messaggio inviato dal server è in chiaro ed autenticato con D_V.

Se A desidera completare la transazione, egli seleziona la carta di credito che intende utilizzare e approva l'acquisto. Il software del portafoglio elettronico genera un *ordine di pagamento* che contiene una descrizione della transazione e i dati relativi alla carta di credito da utilizzare e lo invia al server del venditore. Questo messaggio viene autenticato mediante l'apposizione di una firma digitale ottenuta con D_A e la porzione che contiene informazioni critiche viene cifrata con E_{CC} in modo che esse siano leggibili solo da CyberCash. Il server del venditore, quando riceve questo messaggio, ne produce uno analogo contenente la propria descrizione della transazione cifrata con E_{CC} ed autenticata con D_V ed invia entrambi i messaggi al gateway di CyberCash.

Il gateway, dopo avere verificato l'autenticità dei due messaggi, confronta le due descrizioni ottenute e, se esse risultano identiche, richiede l'autorizzazione a completare la transazione tramite la rete di autorizzazione. Qualora l'autorizzazione venga concessa, il gateway notifica il server del venditore che a sua volta invia un messaggio di *conferma di pagamento* all'acquirente. La transazione viene completata come una qualsiasi transazione convenzionale. La Figura 4 illustra i diversi messaggi scambiati on-line.

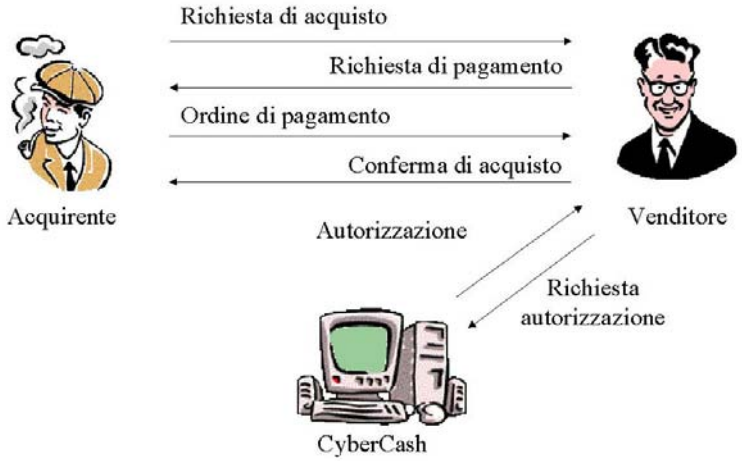

Figura 4: Il Gateway di CyberCash

In questo schema il venditore non viene mai a conoscenza delle informazioni riservate del cliente, ad esempio del suo numero di carta di credito. Questo fatto costituisce un livello di sicurezza aggiuntiva, perché il numero della carta di credito viene rivelato solo a CyberCash e non a ciascuno dei commercianti presso i quali sono stati effettuati degli acquisti. In realtà, nella pratica comune, i venditori usano il numero di carta di credito del cliente come codice di identificazione del cliente all'interno della propria base dati e i clienti sono spesso disposti a rilasciare questo tipo di informazioni [1].

6. Secure Electronic Transactions (SET)

Negli ultimi due anni, Visa, Mastercard ed altri tra i maggiori istituti finanziari interessati dai pagamenti tramite carta di credito hanno compiuto uno sforzo comune per arrivare ad una standardizzazione delle procedure elettroniche. I lavori, che dovrebbero essere conclusi nel 1998, porteranno alla definizione del protocollo Secure Electronic Transactions (SET) [10]. Descrivere le caratteristiche del metodo SET va oltre gli obiettivi di questo breve articolo, ma possiamo comunque anticipare

che SET utilizza tecniche crittografiche in modo simile a CyberCash. Le principali differenze note attualmente all'autore sono le seguenti:

- Per motivi di maggior efficienza dal punto di vista delle prestazioni, il metodo SET utilizza una combinazione di crittografia con chiavi asimmetriche e simmetriche; le chiavi asimmetriche vengono cioè utilizzate dove strettamente necessario, mentre per le altre situazioni vengono usate chiavi simmetriche il cui scambio è protetto dalle chiavi asimmetriche.
- Il SET prevede alcuni meccanismi per la certificazione dell'utente ed in particolare certificati associati al cliente ed al venditore che vengono scambiati durante la fase di pagamento per garantire le reciproche identità dei soggetti coinvolti nelle diverse operazioni.

A questo proposito, va però notato che SET non risolve tutte le complicazioni ed i problemi legati alla certificazione, ma ne delega la verifica ad una autorità di certificazione esterna. Lo schema SET prevede che questa autorità possa offrire maggiori garanzie agli utenti tramite una struttura piramidale del processo di verifica in cui è necessario l'intervento di diversi soggetti per stabilire la autenticità dei certificati.

7. Conclusioni

In questo breve articolo abbiamo illustrato le principali caratteristiche dei sistemi di pagamento tramite carta di credito e ne abbiamo analizzato i principali aspetti legati alla sicurezza elettronica. I sistemi che prevedono l'uso di opportune tecniche di crittografia sembrano costituire il metodo più promettente oggi a disposizione. Si tratta di tecniche ampiamente sperimentate e che sono in grado di fornire agli utenti di Internet un livello di sicurezza in molti casi superiore a quello normalmente disponibile nelle transazioni tradizionali.

Tuttavia, per un'ampia diffusione del commercio elettronico nei prossimi anni, sarà necessario accompagnare l'introduzione di questi metodi alla creazione di una serie di condizioni che inducano gli utenti a preferirli ai metodi tradizionali. Ad esempio, l'acquisto di prodotti o servizi su Internet dovrà essere più conveniente economicamente, più rapido in termini di ordine e consegna oppure dovrà essere il risultato di una scelta tra un maggior numero di soluzioni proposte.

Il ruolo dei metodi di pagamento presentati in questo articolo è critico perché dal loro successo dipende in gran parte il grado di accettazione e di fiducia nel commercio elettronico da parte dell'utente nei prossimi anni. In alcuni lavori futuri, intendiamo trattare in maggiore dettaglio le caratteristiche del Secure Electronic Transactions (SET) ed i problemi legati alla certificazione elettronica.

8. Bibliografia

[1] M. A. Sirbu: "*Credits and Debits on the Internet*", IEEE Spectrum, Febbraio 1997.

[2] C. Schmidt, R. Mueller: "*A Framework for Micropayment Evaluation*", Giugno 1997.

[3] R. W. Baldwin, C. V. Chang: "*Locking the E-Safe*", IEEE Spectrum, Febbraio 1997.

[4] A. Bhimani, "*Securing the Commercial Internet*", Communications of the ACM, Vol. 39, N° 6, Giugno 1996.

[5] N. Borenstein et Al.: "*Perils and Pitfalls of Practical Cybercommerce*", Communications of the ACM, Vol. 39, N° 6, Giugno 1996.

[6] P. Panurach*: "Money in Electronic Commerce: Digital Cash, Electronic Fund Transfer, and E-cash*", Communications of the ACM, Vol. 39, N° 6, Giugno 1996.

[7] Varian, Hal R.*; "The Information Economy: How much will two bits be worth in the digital marketplace?*", Scientific American, September 1995, pp. 200-201 [pagina web] <URL: http://www.sims.berkeley.edu/~hal/pages/sciam.html.> [Visitata Febbraio 1998].

[8] N. S. Borenstein et Al.: "*The Green Commerce Model*", Internet Memo, Maggio 1995, [pagina web] <URL: http://www.firstvirtual.com/pubdocs/> [Visitata Febbraio 1998].

[9] N. S. Borenstein et Al.: "*The Lessons of First Virtual First Year*", Frontiers of Electronic Commerce, Maggio 1995, [pagina web] < URL: http://www.firstvirtual.com/pubdocs/ green-model.txt> [Visitata Febbraio 1998].

[10] Secure Electronic Transaction Specification (Version 1.0): "*Book 1: Business Description*", Maggio 1997.

[11] L. Berardi, A. Beutelspacher: "*Crittologia: come proteggere le informazioni riservate*", Franco Angeli Editore, ISBN 88-204-9898-7, 1996.