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

SET: un protocollo per transazioni elettroniche sicure su Internet

M. Bruschi, L. Delgrossi
e-mail: m.bruschi@agonet.it,
ldgrossi@pc.unicatt.it

Quaderni del CRATOS

Serie di Economia
CTR-E98-003

Università Cattolica del Sacro Cuore – Piacenza, Italia

Contenuti

Per favorire lo sviluppo su scala globale del commercio elettronico è necessario garantire che le transazioni su Internet siano caratterizzate da un adeguato livello di sicurezza. A questo proposito, sono stati proposti negli ultimi anni una serie di metodi di pagamento sicuri. Questo articolo illustra le principali caratteristiche di uno di questi metodi, il protocollo Secure Electronic Transactions (SET), progettato con l'obiettivo di garantire la sicurezza delle transazioni elettroniche basate sull'utilizzo di carte di credito e di debito.

1. Introduzione

Il commercio elettronico è ritenuto da molti una delle potenziali *killer-application* di Internet, cioè una di quelle applicazioni che da sole possono motivare un fortissimo utilizzo della rete su scala globale. Dato il numero di utenti della rete, in forte e costante crescita, il commercio e la distribuzione di beni e servizi tramite Internet potrebbe nei prossimi anni costituire una alternativa valida ed efficiente ai tradizionali canali della grande distribuzione organizzata. Per poter raggiungere questo obiettivo, è però necessario da un lato creare i presupposti culturali necessari per sostenere questo tipo di evoluzione, dall'altro garantire che le comunicazioni su Internet siano caratterizzate da un adeguato livello di sicurezza, tale da permettere agli utenti di utilizzare con fiducia le risorse e le opportunità offerte dalla rete.

A questo proposito, sono stati proposti negli ultimi anni una serie di metodi di pagamento sicuri. Il ruolo di un metodo di pagamento è quello di garantire la riservatezza rispetto a terzi delle comunicazioni associate alle transazioni, di autenticare ciascuna delle parti coinvolte rendendo impossibile l'impersonazione da parte di estranei e di garantire l'integrità delle istruzioni di pagamento. Questo articolo illustra le principali caratteristiche di uno di questi metodi di pagamento, il protocollo Secure Electronic Transactions (SET), progettato con l'obiettivo di garantire la sicurezza delle transazioni elettroniche basate sull'utilizzo di carte di credito e di debito. La discussione evidenzia i diversi meccanismi utilizzati da SET per raggiungere gli obiettivi legati ai problemi di sicurezza.

Nel seguito, la Sezione 2 introduce gli elementi fondamentali di SET; la Sezione 3 descrive i meccanismi di sicurezza utilizzati da SET; la Sezione 3.5 illustra le principali operazioni consentite dal protocollo: registrazione degli utenti, ordine di acquisto, istruzione di pagamento e pagamento; la Sezione 5, infine, conclude la presentazione.

2. Secure Electronic Transactions (SET)

Il protocollo SET è il risultato di un accordo di collaborazione tra Visa, Mastercard, GTE, IBM, Microsoft, Netscape, Saic, Terisa, VeriSign, Verifone, Tandem, SAIC e RSA. Le prime specifiche di questo protocollo sono state rilasciate nel Settembre 1995 e sono state rese disponibili su Internet perché tutti potessero verificare gli eventuali punti deboli e contribuire alla loro correzione. Con tale metodo e grazie alla collaborazione offerta sono state raccolte oltre 3000 proposte di modifica, molte delle quali sono state accettate per giungere alle attuali specifiche [5]. Il protocollo si basa su schemi di crittografia asimmetrica RSA [2] e adotta certificati digitali secondo lo standard X.509 [1].

SET è stato pensato come soluzione specifica per il commercio elettronico ed in particolare per facilitare i pagamenti mediante carte di credito o di debito. Esso non si pone quindi l'obiettivo di stabilire una connessione dati sicura, come, ad esempio, i protocolli SSL [3] , AH [8] o ESP [9]. SET non opera a livello di pacchetto IP, ma tutte le operazioni vengono compiute a livello applicativo e cioè sui dati che vengono scambiati tra le parti coinvolte nelle transazioni elettroniche.

In una transazione SET sono presenti cinque figure:

- il *possessore di carta di credito* (il compratore),
- il *venditore*,

- una *autorità di certificazione*, che ha il compito di certificare l'identità delle parti coinvolte,
- un *payment gateway* che svolge la funzione di intermediario per lo svolgimento di determinate operazioni, e
- la *rete di pagamento* delle istituzioni finanziarie.

Ogni utente di SET, qualunque sia il suo ruolo, deve disporre di un certificato elettronico che provi la sua identità agli altri utenti coinvolti nella transazione. Il protocollo SET prevede la possibilità di poter intrattenere rapporti commerciali cifrati ed autenticati solo tra entità in possesso di un certificato valido. Ogni attore ha la possibilità di poter decifrare solo i messaggi a lui destinati. Ogni potenziale abuso può essere scoperto grazie agli strumenti che verranno descritti in seguito.

SET non definisce in dettaglio le operazioni relative al rilascio dei certificati, ma semplicemente assume che esistano una o più autorità di certificazione in grado di compiere queste operazioni in modo sicuro. Diversi problemi legati alla certificazione elettronica non sono trattati da SET e rimangono aperti: intendiamo discutere questi problemi un prossimo lavoro.

3. Meccanismi per la Sicurezza Elettronica

Prima di esaminare in dettaglio le diverse operazioni di cui SET consiste, è opportuno introdurre alcuni elementi legati alla sicurezza elettronica e, più in particolare, ai meccanismi che possono essere utilizzati per raggiungere un adeguato livello di protezione. I meccanismi utilizzati da SET sono essenzialmente rivolti a garantire:

a) la confidenzialità dei messaggi rispetto a terzi,
b) l'integrità dei messaggi stessi e
c) l'autenticità del mittente.

3.1 Crittografia a chiavi asimmetriche

La confidenzialità dei messaggi rispetto a terzi può essere ottenuta tramite la codifica dei messaggi con algoritmi di crittografia basati su chiavi asimmetriche. Nei sistemi crittografici a chiave asimmetrica, ad ogni utente sono associate due chiavi: la prima chiave, detta *chiave pubblica*, è resa disponibile a tutti gli utenti; la seconda, detta *chiave privata*, è nota esclusivamente al proprietario.

Le due chiavi vengono generate con un particolare procedimento matematico in modo che abbiano le seguenti proprietà: a) conoscendo una qualsiasi delle due chiavi, non è possibile risalire all'altra; b) i messaggi codificati con qualsiasi delle due chiavi possono essere decodificati esclusivamente con l'altra chiave. Con questo tipo di sistema, per inviare ad un utente un messaggio confidenziale è sufficiente codificare il messaggio con la sua chiave pubblica. L'utente potrà decifrare il messaggio utilizzando la propria chiave privata, essendo certo che nessun altro potrà fare altrettanto.

In SET, la distribuzione delle chiavi pubbliche avviene in modo semplice ed efficace: esse vengono inserite nel certificato di cui ciascun utente deve disporre. Quando un utente riceve il certificato del suo interlocutore per verificarne l'identità, automaticamente entra in possesso anche della chiave pubblica da utilizzare per comunicare con lui in modo protetto. L'uso dei certificati elettronici in SET viene descritto in maggior dettaglio nella Sezione 3.5.

3.2 Crittografia a chiave simmetrica

I sistemi a chiavi asimmetriche hanno il grande vantaggio di non richiedere alcuno scambio di chiavi iniziale tra il mittente e il destinatario del messaggio. La loro implementazione è però piuttosto complessa e l'esecuzione dei relativi algoritmi di codifica e decodifica richiede elevati tempi di esecuzione. Per ovviare a questo inconveniente, SET adotta, ove possibile, la crittografia a chiave simmetrica, più efficiente dal punto di vista delle prestazioni, ma che richiede uno scambio iniziale delle chiavi. Per rendere sicuro questo scambio, viene utilizzato il meccanismo di busta elettronica descritto nella Sezione 3.4.

3.3 Firma digitale

La firma digitale è un meccanismo in base al quale si garantisce l'autenticazione del mittente. L'integrità dei messaggi può essere ottenuta applicando un algoritmo di *hash* al messaggio. Gli algoritmi di hash generano un estratto del messaggio (*message digest*) che dipende dal contenuto del messaggio stesso. Se il contenuto di un messaggio venisse alterato o manipolato da terzi, anche il risultato dell'applicazione dell'algoritmo di hash risulterebbe alterato. Confrontando il risultato dell'algoritmo di hash eseguito alla sorgente del messaggio (ed inserito dal mittente nel messaggio stesso), con quello calcolato alla destinazione sul messaggio ricevuto, il ricevente è in grado di capire se il messaggio ricevuto è integro. Gli algoritmi di hash sono realizzati in modo che sia estremamente improbabile che due messaggi differenti generino message digest identici.

L'autenticazione del mittente può essere ottenuta cifrando il digest del messaggio con la chiave privata del mittente. In questo modo, si possono garantire sia l'autenticità del mittente che l'integrità del messaggio. Questo metodo è la base sulla quale vengono realizzati i meccanismi di firma digitale (*digital signature*).

3.4 Buste elettroniche

Veniamo ora alla busta elettronica (*digital envelop*): essa è il mezzo con il quale le parti coinvolte si scambiano la chiave simmetrica segreta. Come abbiamo già detto, la busta elettronica viene utilizzata per limitare l'impiego dello schema a chiave pubblica, piuttosto oneroso dal punto di vista di vista computazionale.

La busta elettronica viene generata nel seguente modo: il testo del messaggio viene cifrato con una chiave simmetrica, che viene poi "posta" in una busta elettronica, e cioè cifrata utilizzando la chiave pubblica del destinatario. Questi, quando riceve il messaggio, "apre" innanzitutto la busta elettronica decifrandola con la propria chiave privata e, ottenuta la chiave simmetrica, è in grado di decifrare il testo del messaggio. In questo modo, la codifica con chiave asimmetrica (onerosa in termini di tempo computazionale) viene utilizzata solo per una quantità limitata di informazioni, mentre il testo del messaggio, che si presume lungo, è codificato con la chiave simmetrica.

3.5 Certificati Elettronici

Per poter partecipare ad una transazione con SET, ciascun utente deve disporre di un certificato elettronico che ne attesti l'identità e che permetta di risalire alla chiave pubblica dell'utente considerato. Il certificato del compratore è simile ad una rappresentazione elettronica della sua carta di credito. Esso è firmato digitalmente dall'autorità di certificazione in modo da non poter essere alterato. Il certificato non contiene alcuna informazione relativa al numero della carta di credito o alla sua data di scadenza, per cui, leggendo il contenuto del certificato, non si ha accesso ad alcuna

informazione riservata. Il certificato viene rilasciato all'acquirente solo con il consenso dell'istituto finanziario e la richiesta di un certificato indica, da parte dell'acquirente, la volontà di acquistare beni o servizi tramite transazioni elettroniche. Un venditore che riceve il certificato di un potenziale compratore può essere certo che il cliente dispone di una carta di credito valida.

I certificati di un venditore indicano che egli è in grado di accettare pagamenti tramite carta di credito. SET richiede che, per ogni tipo di carta di credito accettata, il venditore disponga di una coppia di certificati (Sezione 4.1). Per evitare alterazioni o falsificazioni, anche nel caso del venditore ciascun certificato viene firmato elettronicamente dalla corrispondente autorità di certificazione.

La validità dei certificati viene verificata attraverso una catena di fiducia. Seguendo la catena di fiducia fino a quando viene raggiunta un'autorità di cui egli si fida, un utente può verificare la validità di un certificato. L'origine della catena di fiducia (*root*) è ritenuta fidata per tutti gli utenti di SET ed ha una chiave pubblica che può essere usata per verificare qualsiasi certificato. La chiave pubblica di root è nota a tutti gli utenti di SET. La Figura 1 rappresenta un esempio di catena di fiducia.

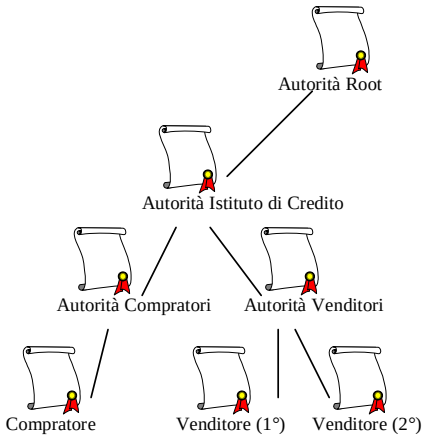

Figura 1: Piramide di Certificazione

Il protocollo SET prevede la possibilità di poter intrattenere rapporti commerciali solo tra entità in possesso di un certificato valido. SET non definisce in dettaglio le operazioni relative al rilascio dei certificati, ma semplicemente assume che esistano una o più autorità di certificazione in grado di compiere queste operazioni in modo sicuro.

4. Come opera SET

Questa sezione illustra le diverse operazioni svolte da SET. Secondo le specifiche del protocollo, il procedimento viene suddiviso in diverse fasi, ciascuna delle quali è destinata ad assolvere un compito preciso. Le fasi principali sono:

- *user registration*: ciascun utente registra la propria identità presso una autorità di certificazione che rilascia il corrispondente certificato elettronico.
- *purchase request*: il compratore genera un messaggio nel quale vengono riassunte le condizioni di acquisto e lo invia al venditore.

- *payment authorization*: il venditore richiede al payment gateway l'autorizzazione di pagamento e, una volta ricevuta l'autorizzazione, provvede alla consegna della merce all'acquirente.
- *payment capture*: il pagamento si concretizza ed una somma appropriata viene detratta dal conto corrente dell'acquirente e depositata su quello intestato al venditore.

4.1 Registrazione dell'utente

In SET, esistono due tipi di richieste di registrazione: quella inoltrata da un acquirente possessore di carta di credito e quella effettuata da un venditore. Le due richieste sono differenti in quanto sono differenti i fabbisogni informativi di cui necessita l'autorità di certificazione. Mentre per il compratore è sufficiente un solo certificato per la firma elettronica dei messaggi, il protocollo SET impone che ciascun merchant abbia due certificati, il primo per firmare elettronicamente i messaggi, il secondo per creare le buste digitali per lo scambio sicuro di chiavi simmetriche. La presenza di due certificati è una ulteriore misura di sicurezza perché un eventuale malintenzionato, per impersonare un venditore, è tenuto conoscere entrambe le chiavi private del merchant, operazione difficile tenendo conto anche del fatto che i certificati elettronici hanno una durata temporale limitata[1].

Secondo l'attuale definizione del protocollo SET, la registrazione del compratore possessore di carta di credito avviene in 6 passi:

1) Il compratore che intende registrarsi invia un messaggio all'autorità di certificazione (*initiate request*). Questo messaggio, che non è protetto da alcun meccanismo di sicurezza, è semplicemente un'espressione, da parte dell'utente, della propria volontà di ottenere la registrazione.
2) l'autorità di certificazione, ricevuta la richiesta dell'utente, genera un messaggio di risposta nel quale inserisce il proprio certificato (*initiate response*). L'autorità autentica il messaggio apponendovi la propria firma digitale e lo invia al richiedente.
3) il richiedente verifica la validità del certificato ricevuto attraverso la piramide di autorizzazione; successivamente, egli utilizza la chiave pubblica dell'autorità[2] per decifrare la firma elettronica assicurandosi così di interagire con un'autorità di certificazione fidata. Il possessore di carta di credito verifica a questo punto l'integrità del messaggio, calcolando il digest relativo al messaggio ricevuto e confrontandolo con quello contenuto nel messaggio stesso. Compiute queste verifiche, egli crea un nuovo messaggio in cui inserisce le informazioni relative al proprio conto corrente e alla carta di credito che egli intende utilizzare per i pagamenti e richiede che gli venga inviata la registration form (*registration form request*).
4) L'autorità di certificazione, ricevuto il messaggio lo decifra e ne verifica l'autenticità e l'integrità nei modi già descritti. Quindi, seleziona l'appropriata registration form (esiste un tipo di registration form differente a seconda del tipo di carta di credito che si ha intenzione di utilizzare) e la invia all'utente (*registration form*).

[1] La durata temporale dei certificati dipende dalla politica di sicurezza adottata dall'autorità di certificazione. Generalmente, i certificati elettronici hanno una validità che può variare dai sei mesi ad un anno.

[2] La chiave pubblica è contenuta nel certificato stesso, come spiegato nella Sezione 3.1.

5) il richiedente, ricevuta la comunicazione da parte dell'autorità, ne verifica l'autenticità e l'integrità e controlla la validità del certificato. Il software utente crea quindi una coppia di chiavi asimmetriche per il richiedente, se questi non ne dispone ancora. L'utente compila la registration form, immettendo tutte le informazioni richieste ed inoltra un messaggio di richiesta di invio del certificato (*cardholder certificate request*). La registration form compilata viene cifrata con una chiave simmetrica. La chiave simmetrica viene posta in una busta elettronica sigillata con la chiave privata dell'autorità.
6) L'autorità apre la busta e ottiene la chiave per decifrare il testo del messaggio. Essa ha ora in proprio possesso tutte le informazioni che occorrono per certificare l'utente. Dopo aver controllato la permanenza di tutte le caratteristiche viste in precedenza (autenticità ed integrità) decide se concedere o meno la certificazione all'utente. In genere, se le informazioni relative alla situazione finanziaria del cliente sono giudicate soddisfacenti si concederà il certificato. L'autorità genera quindi il certificato elettronico e lo firma digitalmente. Include poi il certificato in un messaggio protetto inviato all'utente (*cardholder certificate*).

L'utente riceve il messaggio, esegue gli opportuni controlli, quindi registra il certificato per uso futuro.

Le operazioni esaminate si riferiscono all'iscrizione di un compratore possessore di carta di credito e sono riassunte nella Figura 2. Il venditore, che accetta pagamenti on-line mediante carta di credito dovrà effettuare operazioni un poco differenti, che porteranno alla generazione di due certificati. Ciascun venditore avrà quindi due coppie di chiavi, una per firmare i documenti, l'altra viene per creare la busta digitale.

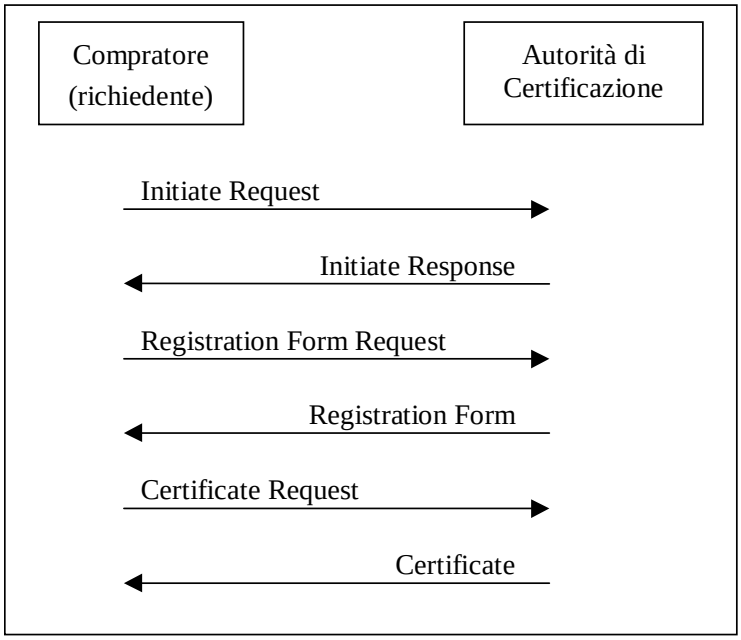

Figura 2: Registrazione del possessore di carta di credito

SET affida all'autorità di certificazione la responsabilità di garantire l'identità dei soggetti coinvolti. In genere, per ottenere un livello di sicurezza adeguato potrebbe essere conveniente che l'autorità di certificazione svolgesse anche un controllo

"fisico", imponendo ad esempio che durante la fase di registrazione l'utente si debba recare da un notaio che controlli le generalità dell'utente stesso. Senza questo tipo di controllo, sarebbe possibile per un malintenzionato a conoscenza di tutte le informazioni necessarie, registrarsi con il nome di un altro utente, compromettendo così la sicurezza dello scambio.

Commento [LB1]:

4.2 Purchase request

Dopo che la fase di registrazione è stata completata ed ogni parte dispone dei certificati necessari, la transazione vera e propria può avere inizio. Il protocollo SET entra in gioco solo quando l'utente ha già effettuato le proprie scelte relativamente alla merce da acquistare ed è stato raggiunto un accordo sulla quantità, qualità e prezzo degli articoli che gli dovranno essere consegnati. Ulteriori accordi potrebbero riguardare il numero di rate ed il tipo di carta di credito da utilizzare.

L'operazione di purchase request è composta da 4 passi:

1) l'acquirente genera un messaggio iniziale non protetto contenente il proprio certificato e lo invia al venditore (*initiate request*).
2) Il venditore, ricevuto il messaggio, assegna alla transazione un identificatore univoco (tipicamente una serie di numeri e cifre) e lo pone in un messaggio insieme ai propri certificati e a quelli del payment gateway. Il messaggio viene firmato digitalmente ed inviato al compratore (*initiate response*).
3) Il compratore verifica la validità dei certificati che gli sono stati inviati e genera un *order information* (OI) ed un *payment instruction*s (PI). Sia OI che PI contengono, oltre alle altre informazioni, l'identificatore della transazione, che servirà al payment gateway per riconoscere la transazione che si sta portando in atto. Dato che l'OI non contiene informazioni riservate, esso non viene cifrato, ed è sufficiente che il compratore firmi digitalmente il documento. Il PI contiene invece informazioni riservate che solo il payment gateway è autorizzato a conoscere. Per questo motivo, il PI viene cifrato con una chiave simmetrica, posta poi in una busta digitale che potrà venire aperta solamente dal payment gateway. Infine, PI, OI e certificato del compratore vengono inviati al venditore (*purchase request*).
4) Il venditore verifica la validità del certificato del compratore e controlla che OI contenga l'esatto identificatore di transazione, quindi invia una richiesta di approvazione della transazione al payment gateway[3]. Una volta ottenuta la risposta dal payment gateway, essa viene inserita in un messaggio firmato digitalmente dal venditore ed inviato al compratore (*purchase response*).

Il possessore di carta di credito può conservare questo messaggio come prova della avvenuta transazione. Le operazioni relative alla fase di purchase request sono riassunte nella Figura 3.

[3] Questa fase viene descritta nella prossima sezione.

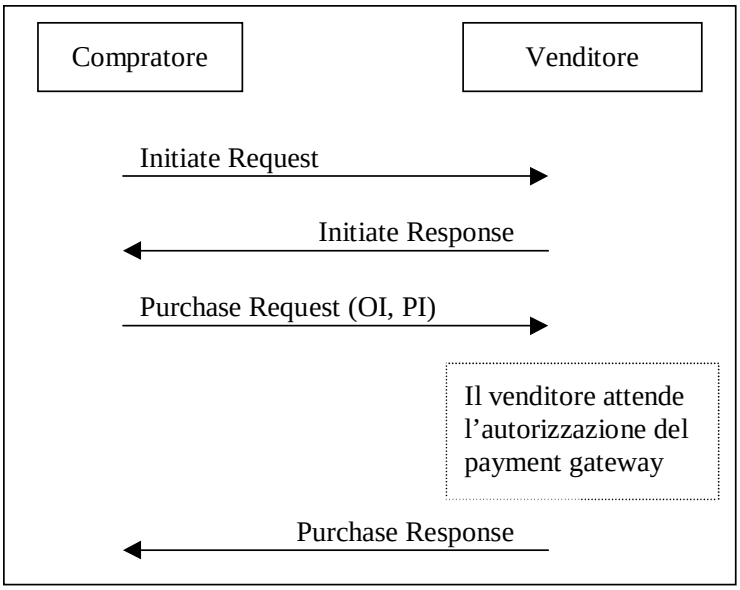

Figura 3: Purchase Request

4.3 Payment authorization

In questa fase, il payment gateway controlla se le informazioni relative alla carta di credito sono valide e se l'importo relativo alla transazione indicato dal venditore coincide con quello indicato dal compratore.

L'operazione di payment authorization si divide in 2 soli step:

1) Il venditore invia un messaggio al payment gateway (authorization request). Questo messaggio contiene una richiesta di autorizzazione al pagamento e tutte le informazioni riguardanti la transazione dettate dal venditore. Queste informazioni vengono cifrate con una chiave simmetrica, posta poi in una busta digitale che solo il payment gateway può aprire. Nello stesso messaggio vengono inclusi sia il PI che contiene le informazioni sulla transazione dettate dal compratore e da lui firmato digitalmente, sia i certificati di venditore e compratore.
2) Il payment gateway, ricevuto il messaggio, controlla la validità dei certificati e procede all'analisi delle informazioni inviate. Aprendo le buste digitali, si ottengono le chiavi simmetriche per decifrare la richiesta di autorizzazione al pagamento ed il PI. Se le informazioni fornite da acquirente e venditore coincidono, il payment gateway invia la richiesta di autorizzazione al pagamento all'istituzione finanziaria che ha emesso la carta di credito del compratore. Questa comunicazione avviene tramite la rete di autorizzazione che collega tutti gli istituti finanziari e le modalità con cui queste comunicazioni avvengono non fanno parte di SET. L'istituto finanziario concede o meno l'autorizzazione ed invia la risposta al payment gateway. Una volta ricevuta la risposta dall'istituzione finanziaria, il payment gateway crea un messaggio di risposta alla richiesta del venditore (authorization response). Questo messaggio ha sostanzialmente il compito di provare che la transazione è stata approvata. Esso viene firmato digitalmente dal payment gateway e contiene un elemento, detto *capture token*.

Se l'authorization request dà esito positivo, il venditore registra il capture token, che verrà utilizzato nella prossima fase per richiedere l'effettuazione del pagamento. A questo punto, il venditore può consegnare la merce senza pericolo di non ottenere il pagamento del corrispettivo dovuto.

4.4 Payment capture

Il payment capture è l'ultima operazione del processo di pagamento. Con questa operazione avviene l'accredito dell'importo della transazione sul conto corrente del venditore.

1) Il venditore crea un messaggio, lo firma elettronicamente e lo cifra utilizzando una chiave simmetrica che viene poi inserita in una busta digitale indirizzata al payment gateway (*capture request*). Al messaggio viene aggiunto il *capture token* descritto nella fase precedente. Il messaggio viene spedito, insieme ai certificati del venditore, al payment gateway.
2) Il payment gateway controlla i certificati, apre la busta digitale a lui indirizzata, decifra le informazioni e controlla la firma digitale. Verificata la consistenza delle informazioni, il payment gateway invia il *capture token*, attraverso un network finanziario, all'istituto del venditore perché effettui il versamento corrispondente. Il payment gateway genera anche un messaggio di risposta, firmato digitalmente, cifrato con una chiave simmetrica apposta in una busta digitale indirizzata al venditore ed inviato quindi, insieme al certificato del payment gateway, al venditore (*capture response*).

Il venditore può registrare questo messaggio per poterlo confrontare, successivamente, con il pagamento che otterrà dal proprio istituto finanziario.

5. Conclusioni

Nelle sezioni precedenti abbiamo descritto le principali funzioni di SET ed il suo ruolo nel contesto delle transazioni elettroniche. SET non definisce la totalità delle operazioni richieste per completare una transazione in modo sicuro, ma si affida ad una catena di fiducia per la validazione dei certificati elettronici e alla rete di autorizzazione di pagamento interbancaria per l'autorizzazione delle istruzioni di pagamento. Il principale compito svolto da SET è quello di proteggere le comunicazioni tra le parti coinvolte e garantire l'identità degli interlocutori in ogni fase della transazione.

SET cambierà il modo di operare su Internet? A questa domanda non si può dare una risposta semplice e affrettata. Ciò che sembra certo è che Internet ha bisogno di strumenti come SET. SET può contribuire a creare quel livello di fiducia senza il quale il commercio elettronico difficilmente si potrà sviluppare.

Il successo di questo protocollo dipenderà in misura molto stretta dalla praticità ed affidabilità dei meccanismi di sicurezza utilizzati.

SET è ben più di un protocollo per garantire la sicurezza nelle operazioni commerciali. E' il risultato di una alleanza strategica tra colossi ciascuno nel proprio campo d'azione. VISA e Microsoft, leader nei rispettivi "mercati" d'appartenenza, sono due tra i maggiori promotori di questo strumento. Accordi come questi possono creare fiducia per sviluppare il commercio elettronico e dar vita a strumenti il più possibile completi.

I promotori di SET, citati all'inizio, hanno reso disponibile una specifica standard di questo strumento nel tentativo di evitare i problemi legati alla

compatibilità delle varie implementazioni. Durante il 1997 sono stati condotti circa 150 implementazioni pilota di SET, molte delle quali proseguiranno anche durante il 1998. La maggioranza dei progetti sono stati condotti in Europa e Asia, per questo in questi territori ci si trova più pronti per utilizzare questo tipo di strumenti.

David Wiseman, analista della Forrester research sostiene che occorrerà attendere almeno sino al 1999 prima di poter vedere i primi impatti su Internet dati da questo tipo di protocollo [4]. Giga Information Group prevede che solamente il 18% delle transazioni con carte di credito su Internet verranno svolte mediante SET nel 1999, ma tale cifra salirà al 45% entro il 2000. Sono cifre incoraggianti che fanno sperare in un superamento delle limitazioni di Internet rispetto al commercio elettronico entro tempi molto brevi [4].

6. Bibliografia

[1] C. P. Pfleeger: "*Security in Computing*", ISBN 0-13-337486-6, Prentice Hall, 1997.

[2] R. Rivest, A. Shamir, L. Adleman: "*A Method for obtaining Digital Signatures and Public Key Cryptosystems*", Communications of the ACM, Vol. 21, pp: 120-126, 1978.

[3] A. O. Freier, P. Karlton, P. C. Kocher: "*The SSL Protocol Version 3.0*", Transport Layer Security Working Group, Internet Draft <draft-freier-ssl-version3-02.txt>, November 1996.

[4] David Clark, "*SET - it's ready to roll*", IEEE Internet Computing, Dicembre 1997.

[5] AA. VV.: "*Secure Electronic Transaction Specification Version 1.0*", [pagina web] <URL: http://www.visa.com/cgi-bin/vee/nt/ecomm/set/downloads.html>, Maggio 1997.

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

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

[8] R. Atkinson: "*IP Authentication Header*", Internet RFC 1826, Proposed Standard, Agosto 1995.

[9] R. Atkinson: "*IP Encapsulating Security Payload*", Internet RFC 1827, Proposed Standard, Agosto 1995.