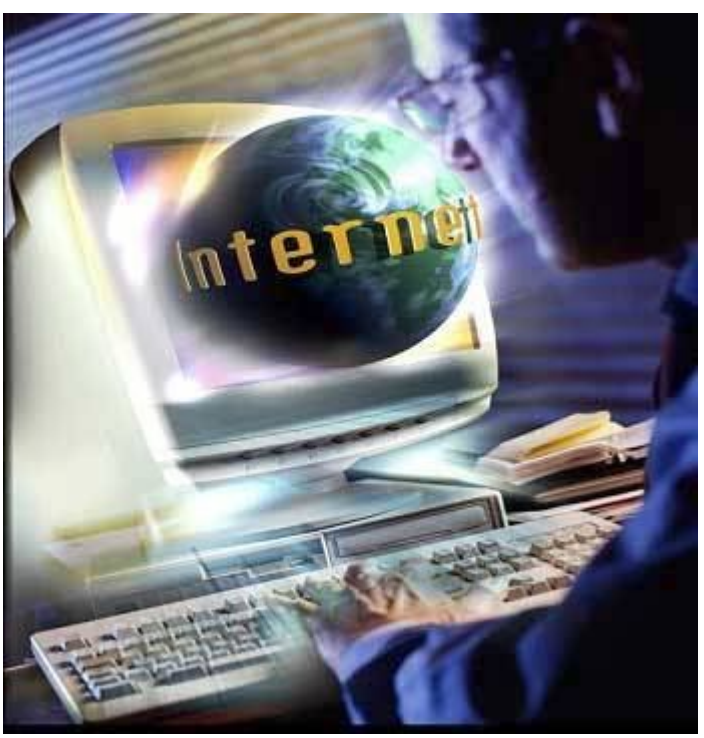
I protocolli per la sicurezza delle transazioni monetarie

L'usuale pagamento a mezzo carta di credito, nato negli anni '60, e, quindi, in un'epoca sicuramente antecedente alla diffusione di Internet, è criticato a causa della sua intrinseca pericolosità relativamente al buon fine della transazione. Si teme, infatti, che allorquando l'acquirente trasmetta al fornitore i propri dati (numero di carta, identità del titolare, scadenza) attraverso Internet, gli stessi possano essere intercettati da terzi e utilizzati abusivamente. In realtà, il problema sopra esposto potrebbe astrattamente porsi anche al di fuori di Internet, mediante il normale utilizzo della carta di credito: nella ricevuta che rimane in mano al negoziante sono infatti presenti gli estremi della nostra carta di credito.



A differenza di quanto potrebbe sembrare, la parte che corre i rischi maggiori dall'effettuazione di un pagamento a distanza mediante carta di credito è il venditore: questi, infatti, accettando il pagamento senza verificare l'identità tra il titolare della carta di credito e l'acquirente, si trova in una posizione giuridicamente molto debole. L'acquirente, per contro, potrà validamente fruire di una tutela abbastanza forte: potrà proporre azione di nullità del contratto nei confronti del venditore visto che può sostenere, non avendo firmato nulla, di non avere espresso la propria volontà formativa del contratto; potrà, altresì, ottenere dall'istituto di credito emittente il risarcimento della somma fraudolentemente pagata (in forza del disposto di cui all'art. 8, comma. 2, del D.Lgs. 22 maggio 1999, n. 185). La banca, peraltro, non potrà sollevare un'ipotetica responsabilità del titolare per ritardo nella comunicazione di smarrimento, visto e considerato che un uso illecito della propria carta può essere fatto da terzi, anche se il titolare rimane nell'effettiva disponibilità della stessa. Acquisti falliti, paure sulla sicurezza dei trasferimenti e insoddisfazione nei confronti degli strumenti utilizzabili sono ostacoli con i quali confrontarsi per garantire lo sviluppo del commercio su Internet. Da qui l'esigenza di implementare uno standard di sicurezza per le transazioni che avvengono nella rete al fine di costruire la necessaria fiducia tra gli utenti della rete per stabilire un canale di comunicazione sicuro.

Al fine di migliorare la sicurezza dei pagamenti a mezzo carta di credito, nel febbraio 1996 è stato sviluppato uno specifico protocollo denominato SET.

Questo sistema garantisce la confidenzialità delle informazioni trattate, l'integrità dei messaggi e la certificazione di autenticità delle parti coinvolte nella transazione. Esso funziona nel modo seguente: il titolare della carta di credito SET riceve dalla banca emittente un certificato criptato in forza del quale egli è identificato univocamente dall'istituto di credito. Il titolare registra sul suo computer il certificato e, nel momento in cui effettua un pagamento via Internet, dà la possibilità alla banca di certificare al venditore se chi sta utilizzando la carta sia l'effettivo titolare della stessa. Così facendo, la banca si sostituisce al venditore nell'onere di verificare la corrispondenza tra la firma di chi effettua il pagamento e la firma apposta sul retro della carta di credito, onere che, ovviamente, nelle transazioni via Internet, risulterebbe impossibile da assolvere.

In questo modo, chi riceve il pagamento risulta essere maggiormente garantito visto che, in caso di problemi, potrà tutelarsi sia nei confronti dell'acquirente, che ha negligentemente permesso che altri utilizzassero per lui la carta SET, sia nei confronti dell'istituto emittente che, alla prova dei fatti, non ha saputo garantire un sistema sicuro e inviolabile. I nuovi contratti delle carte di credito SET impongono, inoltre, in capo al titolare un rigoroso onere di custodia del certificato. Nel caso in cui si verifichi che qualcuno sia venuto a conoscenza del certificato e del numero della carta di credito, il titolare non può contestare l'eventuale esborso addebitatogli fintantoché non abbia provveduto a denunciare all'istituto di credito emittente la violazione di sicurezza. Il SET, per garantire la confidenzialità delle informazioni, assicurare l'integrità dei messaggi, e autenticare l'identità degli utenti, utilizza la crittografia: sia la *Symmetric cryptography* (anche conosciuta come *Secret key cryptography*) che la *Asymmetric cryptography* (*Public key cryptography*).

Mettiamo ora a confronto i due protocolli maggiormente diffusi sulla rete per la sicurezza dei pagamenti on-line. Innanzitutto il SET protegge l'identità di tutte le parti coinvolte nella transazione attraverso la firma digitale; l'SSL non è, invece, predisposto per porre in essere un tale tipo di operazione. Il SET è un protocollo end-to-end, cioè da utente a utente; il SSL, invece, si dice point-to-point, cioè una connessione da un server a un client. Il SET, infine, diversamente dal SSL, non solo definisce tutti i necessari protocolli per lo scambio dei dati al fine del trasferimento pecuniario tra il consumatore e il commerciante, ma anche garantisce che questi dati siano trasferiti alla banca del commerciante.

(*Adattato da http://eprints.biblio.unitn.it*)