

**UNIVERSITÀ DEGLI STUDI DI PERUGIA**  
**FACOLTÀ DI SCIENZE MATEMATICHE FISICHE E NATURALI**

*Sicurezza Informatica*



**S.E.T.**  
**(SECURE ELECTRONIC TRANSACTION)**

**Andrea Valentini Albanelli**

**Fabrizio Cardellini**

# Introduzione

Esiste il problema di comunicare dati privati sulla carta di credito in maniera sicura per poter effettuare acquisti e guadagnare fiducia sugli utenti. Inoltre il commerciante, generalmente, accetta più tipi di carte di credito, ma potrebbe risultargli scomodo il fatto di dover trattare con più banche emittenti. Per questo nasce il protocollo **SET** (Secure Electronic Transaction) sviluppato nel 1997 principalmente da Visa e Mastercard con la collaborazione di altre compagnie quali GTE, IBM, Microsoft, Netscape, RSA, Safelayer e VeriSign utilizzato nell'ambito della sicurezza delle transazioni su reti definite insicure come internet. SET non è da solo un sistema di pagamento, ma un insieme di protocolli di sicurezza (SHA-1, DES, RSA, X.509) che consentono agli utenti di utilizzare le attuali modalità di pagamento con carta di credito in maniera sicura.

## DES

Ideato da IBM è divenuto Standard nel 1976 grazie al Federal Information Processing Standard (FIPS). DES è un algoritmo di cifratura a chiave simmetrica a SOLI 56 bit. DES oggi è considerato insicuro per moltissime applicazioni a causa della lunghezza della chiave. Infatti al giorno d'oggi con i moderni sistemi L'algoritmo DES può essere violato in poche ore. Per tale motivo SET utilizza una sua versione sicura: TripleDES.

## RSA

Algoritmo di Crittografia Asimmetrica a chiave pubblica. Ci sono due chiavi utilizzate per la criptazione e la decriptazione del messaggio. Se una viene utilizzata per la criptazione solo l'altra può essere utilizzata per la decriptazione e viceversa. L'utente crea le due chiavi e ne rende pubblica solamente una. E' sicuro! Ancora oggi risulta essere inviolabile. TripleDES unito con RSA creano uno strumento davvero potente ed affidabile.

## SHA-1

La sigla SHA sta per **Secure Hash Algorithm**. Come ogni algoritmo di *hash*, l'SHA produce un *message digest*, o "impronta del messaggio", di lunghezza fissa partendo da un messaggio di

lunghezza variabile. La sicurezza di un algoritmo di *hash* risiede nel fatto che la funzione non sia reversibile (non sia cioè possibile risalire al messaggio originale conoscendo il suo *digest*) e che non deve essere mai possibile che si riesca a creare *intenzionalmente* da due messaggi diversi lo stesso *digest*.

## **X.509**

E' un formato che definisce lo standard di certificati a chiave pubblica. Viene rilasciato da una Certification Authority (CA).

# Protocollo S.E.T.

## Attori

- **Cardholder:** Il titolare della carta è un soggetto autorizzato ad utilizzare una carta di credito, come MasterCard o Visa emessa da un emittente (discusso in seguito).
- **Commerciante:** Un commerciante è una persona o un'organizzazione che vuole vendere beni o servizi ai titolari di carte di credito. Un commerciante deve mantenere una relazione con un acquirente (discusso in seguito) per accettare pagamenti su Internet.
- **Emittente:** L'emittente è un istituto finanziario (come ad esempio una banca) che fornisce una carta di credito per il titolare, ed è responsabile dei pagamenti effettuati dagli stessi.
- **Acquirente:** Questo è un istituto finanziario che ha un rapporto con i commercianti per l'autorizzazione di carte di credito e dei pagamenti. Perciò, l'acquirente si occupa di fornire al commerciante un'autorizzazione che attesti che la carta di credito è attiva e che la proposta di acquisto non superi il limite di credito e trasferisce poi il denaro elettronico nell'account del commerciante. Infine, l'emittente rimborsa l'acquirente.
- **Payment Gateway:** Questo ruolo può essere assunto dall'acquirente stesso o affidato ad una terza parte dedicata. Il Payment Gateway elabora i messaggi di pagamento per conto del commerciante. In particolare, nel SET, il Payment Gateway funge da interfaccia tra SET e le reti di pagamento con carte bancarie. Il commerciante scambia messaggi utilizzando il protocollo SET con il Payment Gateway che a sua volta è connesso con il sistema di elaborazione dell'acquirente.
- **Certification Authority:** E' un entità atta a rilasciare certificati a chiave pubblica di tipo X.509 per titolari, commercianti e payment gateway.

## Doppia Firma (DS)

Lo scopo della *doppia firma* (dual signature) oltre a garantire i goal di autenticazione e di integrità, è quello di creare una relazione tra le informazioni di pagamento (PI) e le informazioni dell'ordine (OI). Se non ci fosse una relazione tra le due informazioni avremmo che il cliente invia i due messaggi (PI - OI) al commerciante in modo separato: un OI firmato e PI firmato. Se il commerciante è in grado di catturare un altro ordine OI dallo stesso Cardholder, il commerciante potrebbe sostenere che tale OI vada con la prima PI ricevuta piuttosto che con la PI relativa truffando il cliente. Quindi la *doppia firma* è fondamentale per creare una sorta di relazione tra le due istanze. Andiamo a vedere come si costruisce tale **dual signature (Figura 1)**: il Cardholder prende le informazioni di pagamento (PI) e crea tramite l'hash (SHA-1) il digest (Payment Information Message Digest). Allo stesso modo, viene creato il digest delle informazioni dell'ordine (Order Information Message Digest). Il Cardholder successivamente concatena PIMD e OIMD ed applica l'hash alla concatenazione (Payment Order Message Digest) poi cripta il POMD con la sua chiave privata. L'output di questo processo è la doppia firma (Dual Signature). La convalida dell'ordine da parte del Commerciante è eseguita confrontando due tipi di POMD (Figura 2). Il POMD1 viene ricavato decriptando la doppia firma con la chiave pubblica del Cardholder, mentre il POMD2 viene costruito dallo stesso Commerciante. Dal *message request*, infatti, il Commerciante prende l'OI e il PIMD che sono trasmessi in chiaro. Dall'OI crea l'OIMD tramite la funzione hash, lo concatena al PIMD preso dal request message e forma il POMD2. La convalida da parte del Payment Gateway è analoga a quella del Commerciante. Anche esso fa una verifica tra due POMD. POMD1 lo ricava alla stessa maniera, mentre il POMD2 lo ricava in modo analogo con la differenza che non si ricava l'OIMD ma il PIMD.

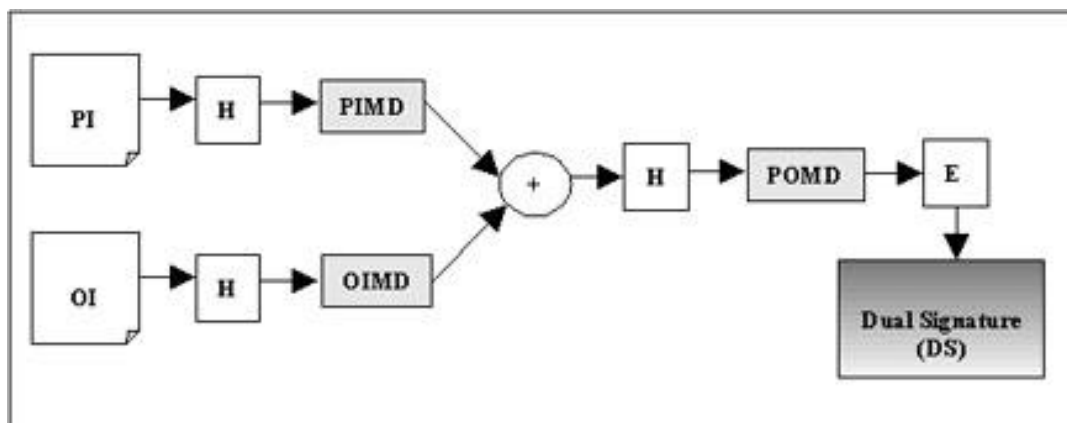
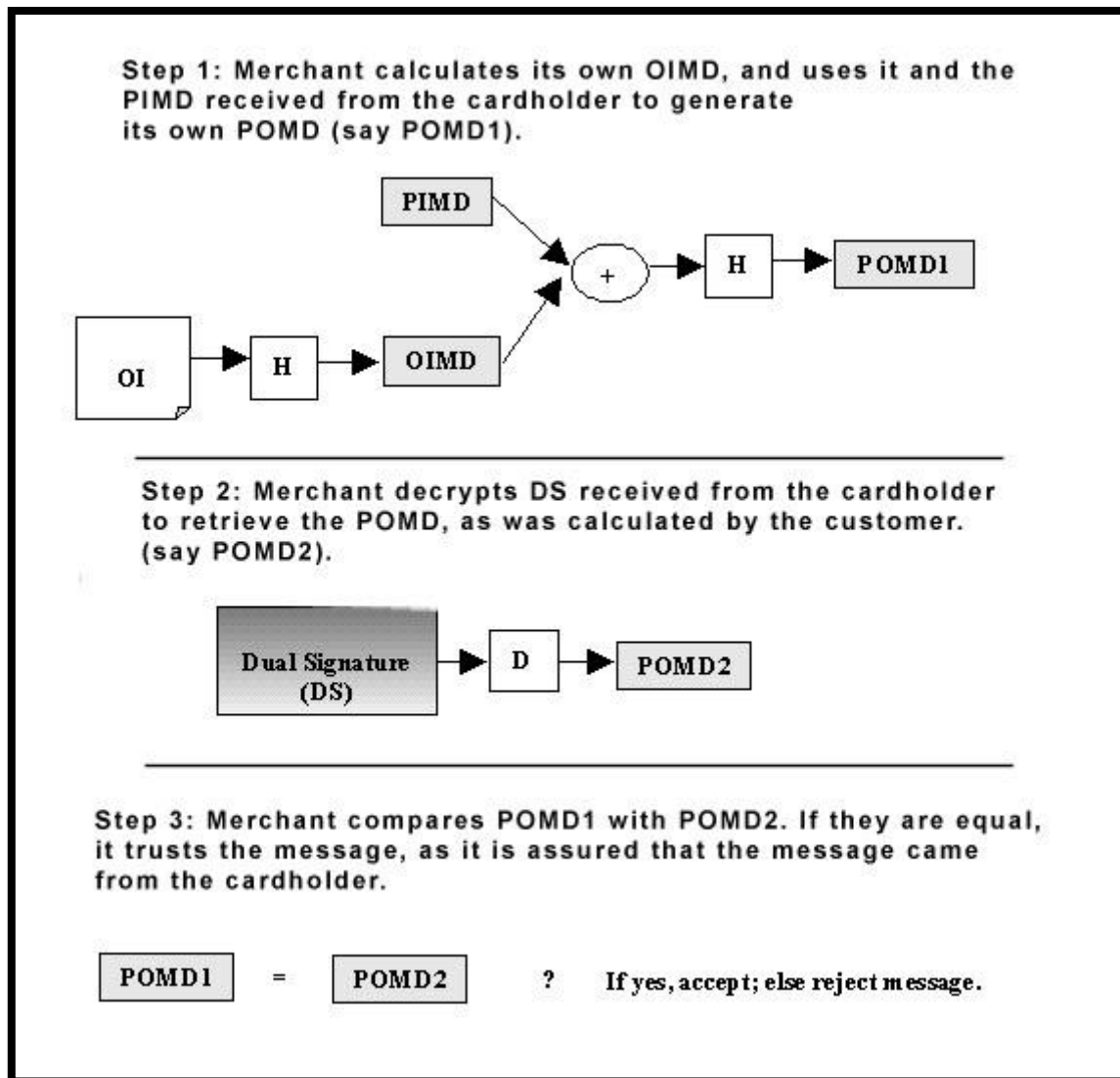


Figura 1



*Figura 2*

## S.E.T. in azione

Le fasi previste dallo standard sono:

1. Registrazione del possessore della carta di credito
2. Registrazione del commerciante
3. Sottomissione di un ordine

4. Autorizzazione del pagamento
5. Adempimento delle due parti (Deve essere effettuato l'addebito sulla carta di credito del cardholder ed il commerciante deve fornire il bene e/o servizio acquistato)

Le prime due fasi sono eseguite una volta sola ed indipendentemente dalle due parti.

### **1. Registrazione del cardholder**

Il cliente acquista una carta di credito da un'emittente certificato da una CA che supporta il pagamento elettronico e SET. L'emittente oltre alla carta di credito rilascia al cliente, dopo aver verificato la sua identità, un certificato di tipo X.509 ed un e-wallet. Un e-wallet (portafoglio elettronico) è una piccola applicazione da installare sul computer del cliente e contiene informazioni sulla carta di credito disponibili e sul certificato acquisito. L'e-wallet inserisce automaticamente i dati del cliente quando questo effettua un ordine in maniera che possano essere trattati dal protocollo SET.

### **2. Registrazione del commerciante**

Il commerciante effettua una registrazione da un'acquirente certificato da una CA che, dopo aver verificato la sua identità, gli fornisce 2 certificati: uno generato all'atto della registrazione contenente la chiave pubblica del commerciante e l'altro di proprietà dell'acquirente contenente la chiave pubblica del payment gateway.

### **3. Sottomissione di un ordine (Figura 3)**

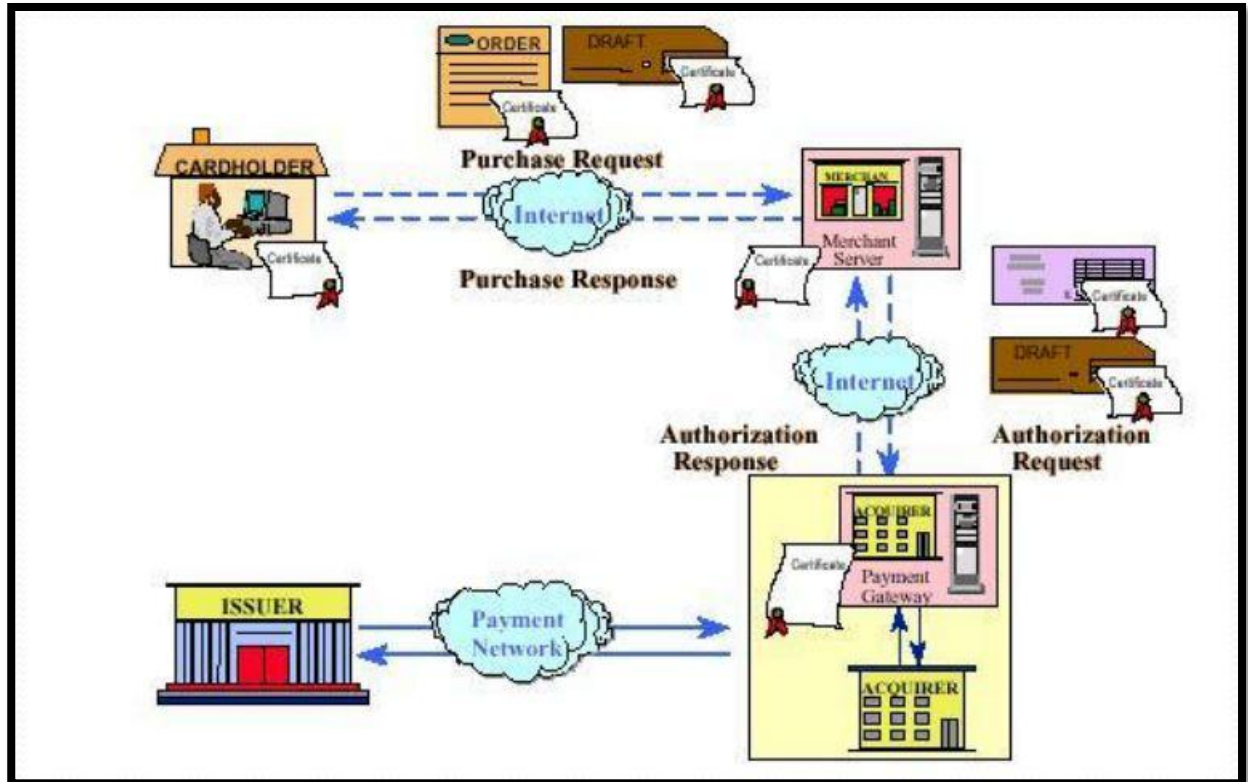
Il cardholder, navigando nel sito web del commerciante, decide di effettuare un ordine ed invia un messaggio denominato *Initiate Request* al commerciante richiedendogli il suo certificato ed il certificato del suo Payment Gateway. Il commerciante risponde con un messaggio di *Initiate Response* contenente i 2 certificati richiesti ed un Transaction ID, ovvero un numero univocamente associato all'ordine criptato con la sua chiave privata. Il cardholder alla ricezione di tale messaggio può verificare l'identità del commerciante e del Payment Gateway e può verificare che il Transaction ID gli sia stato effettivamente inviato dal commerciante decriptandolo con la chiave pubblica dello stesso. A questo punto, il cardholder prepara le informazioni sull'ordine (OI) e sul pagamento (PI). Inoltre crea, con il meccanismo della doppia firma, una firma che contiene sia le PI che le OI in maniera tale che sia il commerciante sia il payment gateway la possano verificare, ma il commerciante vede soltanto le informazioni

sull'ordine e il payment gateway soltanto quelle sul pagamento. Il cardholder crea una chiave di sessione 3-DES con cui cripta le PI e la doppia firma, poi cripta la chiave di sessione stessa con la chiave pubblica del payment gateway e la aggiunge al messaggio. In questo modo solo il Payment Gateway può leggere la chiave di sessione e recuperare le PI. Le OI verranno invece trasmesse in chiaro insieme alla doppia firma, con la quale il commerciante può verificare la validità delle OI stesse. Il cardholder aggiunge poi il Transaction ID sia alle PI che alle OI. Infine viene anche aggiunto il certificato del cardholder. Tutto ciò costituisce il messaggio di *Purchase Request* e viene trasmesso al commerciante. Il commerciante alla ricezione del messaggio verifica il certificato del cardholder firmato dalla CA e verifica la doppia firma usando la chiave pubblica del cardholder. Questo gli assicura l'integrità dell'ordine e il fatto che l'ordine è stato richiesto effettivamente dal mittente. A questo punto inoltra le informazioni di pagamento criptate precedentemente con il 3-DES al payment gateway, il Transaction ID criptato con la chiave privata del commerciante insieme al suo certificato e a quello del cardholder. Il payment gateway può decriptare le informazioni di pagamento con la sua chiave privata per verificare che non siano state alterate tramite la doppia firma e verifica il commerciante tramite il suo certificato. Ora il protocollo SET da per scontato che esista un canale di comunicazione sicuro tra Payment Gateway e banche emittenti. Uno scenario tipico potrebbe essere l'adozione del protocollo HTTPS da parte degli emittenti o anche semplicemente criptare la richiesta con la chiave pubblica della banca emittente. Sta di fatto che questa parte di comunicazione non è gestita dal protocollo SET. Ammesso che esista tale scenario il payment gateway comunica i dati di pagamento all'emittente che verifica la correttezza degli stessi e la disponibilità della cifra. In caso affermativo fornisce l'autorizzazione al payment gateway. Autorizzazione che poi verrà inviata al commerciante. Il commerciante invia poi un messaggio di *Purchase Response* al cardholder contenente una notifica (ACKnowledge) dell'ordine ed il Transaction ID, il tutto criptato con la sua chiave privata. Inoltre, allega di nuovo il suo certificato per essere verificato nuovamente dal cardholder. Il cardholder può essere sicuro dell'integrità del Purchase Response, in quanto la notifica e il Transaction ID possono essere decriptate soltanto con la chiave pubblica del commerciante.

#### **4. Adempimento delle due parti**

Infine viene effettuato l'addebito sulla carta di credito del cardholder da parte dell'emittente, l'acquirente rimborsa il commerciante ricevendo una percentuale per il servizio ed il commerciante provvede a fornire il bene e/o il servizio acquistato. Il cardholder può utilizzare il messaggio di Purchase Response come prova di pagamento ricevuto ed il commerciante può

utilizzare il messaggio di Purchase Request per testimoniare la volontà di acquisto del cardholder.



*Figura 3*

## Vantaggi

Il protocollo SET offre il vantaggio di garantire diversi goal di sicurezza.

- **Integrità:** Il protocollo assicura la non alterabilità delle informazioni, garantita grazie all'utilizzo della doppia firma.
- **Autenticazione:** Mediante l'utilizzo di certificati X.509 vengono identificate entrambe le parti, insieme all'acquirente e all'emittente. Inoltre viene anche garantita la non ripudiabilità grazie ai messaggi di Purchase Request e Purchase Response.

- **Privacy:** La privacy è garantita sui dati della carta di credito del cardholder, che vengono letti esclusivamente dal Payment Gateway verificato, e dall'emittente che già ne è a conoscenza, in quanto ha rilasciato lui stesso la carta di credito. Il commerciante non riesce in alcun modo a leggerli perché gli arrivano criptati con una chiave 3-DES che solo il Payment Gateway conosce.
- **Confidenzialità:** I dati della carta di credito viaggiano sulla rete in forma criptata con la chiave 3-DES, pertanto nessuno può leggerli in chiaro, se non il Payment Gateway.

Un altro vantaggio è il fatto che SET è immune a molti attacchi. Ad esempio, con un attacco di sniffing non si ricaverebbero informazioni particolarmente interessanti. Le uniche cose catturabili da uno sniffer sono le informazioni sull'ordine, il numero di transazione e i vari certificati. Anche un possibile attacco di replica risulterebbe di poca efficacia. Soltanto il messaggio di Initiate Request può essere replicato ricevendo sempre una Initiate Response, ma la replica di questi 2 messaggi non costituisce scambio di informazioni su ordine o pagamento. Per gli altri messaggi la replica viene sempre identificata, grazie al Transaction ID.

## Svantaggi

Un possibile attacco al protocollo SET è l'utilizzo improprio dell'e-wallet installato nel pc del cardholder nel caso che un attaccante prenda controllo dello stesso mediante un virus. L'e-wallet potrebbe infatti firmare automaticamente transazioni a nome dell'utente proprietario del pc. Questo attacco farebbe crollare tutta l'affidabilità e la sicurezza del protocollo. Tuttavia, negli e-wallet più moderni, la compilazione automatica dei dati viene fatta soltanto dopo la digitazione di una password da parte dell'utente. Un altro fattore che gioca a svantaggio di SET è la sua complessità elevata dovuta all'utilizzo di diversi algoritmi di cifratura e delle lunga fase di scambio messaggi che può fornire tempi di risposta inadeguati. Inoltre, l'installazione dell'e-wallet sia lato client che lato server, potrebbe risultare non banale per clienti e commercianti inesperti e ciò aumenta la complessità del protocollo. Questo è il principale fattore che ha portato all'abbandono di SET e alla scelta da parte dei commercianti di protocolli più leggeri come SSL. Infine, la confidenzialità e la privacy non sono garantite per le informazioni sull'ordine che viaggiano in chiaro ed un attaccante,

con uno sniffing, può capire cosa ha acquistato un utente anche se tali informazioni non hanno un alto grado di sensibilità.

# Conclusioni

In conclusione SET ha delle buone caratteristiche di sicurezza, in alcuni punti anche migliori degli attuali protocolli. Togliendo il principale problema della complessità, che potrebbe anche risultare ininfluente con l'aumentare della potenza di calcolo delle macchine, ci potrebbero essere delle speranze di un riutilizzo di SET per le transazioni on-line.

# Bibliografia

Stalling, William: Cryptography And Network Security 4Th Ed, Prentice-Hall, 2006.

Henry Muccini: Sicurezza: SSL, SHTTP, IPSEC E SET University of L'Aquila

Nikki Goth Itoi. PROMISES, PROMISES What ever happened to SET?  
<http://www.herring.com/mag/issue51/promises.html>

SetCo. SET Secure Electronic Transaction Specification: Business Description, May 1997.  
[http://www.setco.org/set\\_specifications.html](http://www.setco.org/set_specifications.html)