

Commerce Electronique sur Internet (Approche SET)

I – Schéma SET : Secure Electronic Transaction :

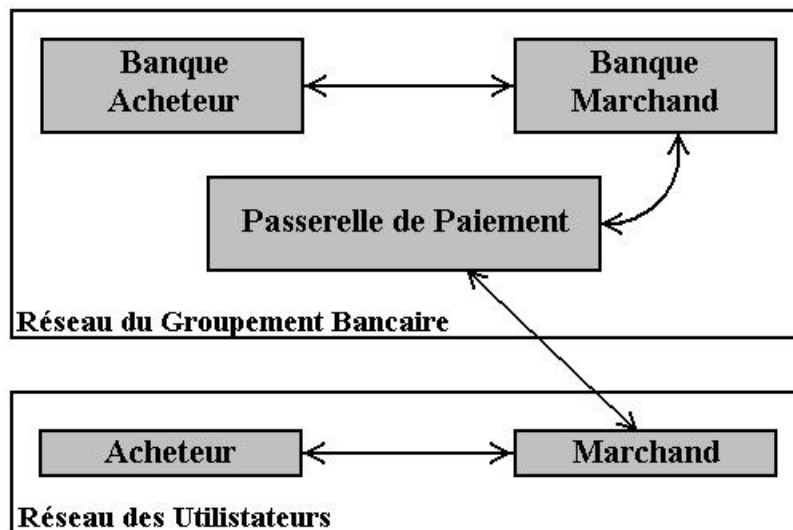
C'est un standard créé en 1996/1997, soutenu par les grands groupements bancaires : VISA, MASTERCARD, AMERICAN EXPRESS et les fournisseurs : IBM, MICROSOFT ...

Il est constitué par un ensemble de protocoles de sécurité applicatifs, pour le paiement par carte bancaire sur Internet :

- Le protocole d'achat.
- Le protocole d'autorisation de paiement.
- Le protocole de paiement.

Ces protocoles utilisent des techniques de cryptologie telles que RSA, DES et les fonctions de hachage.

→ Schéma simplifié :



→ Principe :

Acteur :	Acheteur	Marchand
Tâches :	<ul style="list-style-type: none"> - Connecter sur le serveur marchand. - Consulter le service. - Passer la commande. - Autoriser paiement. 	<ul style="list-style-type: none"> - Accepter et réaliser la commande. - Adresser l'autorisation de paiement de l'acheteur, à sa banque via la passerelle de paiement.

I.1 – Règles de sécurité de base :

- **Authentification** : L'acheteur et la passerelle de paiement, doivent pouvoir vérifier que le marchand est bien celui qu'il prétend être.
- **Intégrité** : Une personne non autorisée ne doit pas pouvoir modifier les messages qui circulent entre le marchand et la passerelle de paiement.
- **Confidentialité** : Le marchand ne doit pas accéder au numéro de la carte bleu de l'acheteur.
- **Confidentialité** : Le banquier n'a pas à connaître la nature de la commande passé par l'acheteur.

I.2 – Modélisation :

I.2.1 – Les Rôles dans SET :

Les différents intervenants dans SET sont :

- Le banquier.
- L'acheteur.
- Le marchand.
- Les autres.

I.2.1 – Les classes :

→ Objets :

1. La carte bleue.
2. Le PIN code de la carte bleue.
3. Le numéro de la carte bleue.
4. L'identifiant de la commande.
5. Le contenu descriptif de la commande.
6. Le prix de la commande.

→ Les méthodes :

- A. Créer.
- B. Lire ou connaître.
- C. Accepter ou signer.
- D. Détenir.

→ Correspondance Objets – Méthodes :

	1	2	3	4	5	6
A						
B						
C						
D						

→ **Matrice des Droits :**

	1A	1D	2A	2B	3A	3B	4A	4B	5A	5B	5C	6A	6B	6C
Banquier														
Acheteur														
Marchand														
Autres														

I.3 – Opération achat :

I.3.1 – Phase d’accréditation préalable :

Les différents intervenants dans SET, doivent être accrédité – par la délivrance d’un certificat d’authentification – par une autorité tierce, digne de confiance : l’autorité d’accréditation.

→ **Le certificat d’authentification :**

Un certificat regroupe un ensemble d’informations caractéristiques de l’usager et de l’autorité. Il comporte :

- Un Identificateur précis de l’usager (Nom, Adresse, Raison Sociale etc.)
- La clef publique de l’usager.
- La date limite de validité du certificat.
- Le numéro du certificat.

En outre le certificat doit respecter ces conditions :

- Le certificat étant délivré pour être utilisé sur le réseau, on doit vérifier qu’il n’a pas été réalisé par un fraudeur.
- L’autorité de certification doit être reconnue et authentifiable : en appliquant une signature numérique infalsifiable, aux certificats.

I.3.2 – Aspect cryptographique :

→ **Algorithme :**

SET, utilise l’algorithme DES, pour les échanges effectifs et RSA pour la distribution des clefs du DES. La longueur de la clef est de 1024 Bits car un système à clef de 512 Bits a déjà été cryptanalysé.

L’intérêt d’un tel système hybride, réside dans la solidité de RSA, qui assure la confidentialité de la clef et la rapidité du DES (1000 fois plus rapide que RSA), qui assure la fluidité des échanges.

→ **La signature numérique :**

Elle est basée sur SHA : Secure Hash Algorithm. (RSA Based)

La fonction de hachage utilisée est publique à sens unique : text → Digest.

I.3.3 – Processus d'achat:

Il est constitué de deux échanges du type : Requête / Réponse.

→ 1^{er} Echange :

- Le marchand envoie le bon de commande signé à l'acheteur, avec son certificat.
- A l'aide de la signature numérique et du certificat du marchand, l'acheteur vérifie l'intégrité du bon de commande et l'identité du marchand.

→ 2^{ème} Echange :

- Envoi de la requête d'achat :
 1. L'acheteur construit la structure de données OI (Order Information), concernant la commande et envoie au marchand : (OI , SHA(OI))
 2. L'acheteur construit la structure de données PI (Payement Information), concernant la commande et envoie à la passerelle de paiement le message suivant:
DES (PI , SHA(OI) , SHA(CONCAT(SHA(OI), SHA(PI)))).
Le dernier terme de ce triplet est appelé *Signature Duale*, dans la norme SET.
C'est entre autre un moyen de relier le paiement à la commande, sans pour autant donner l'occasion à la passerelle de découvrir le contenu de la commande.
Il envoie aussi la clef DES, chiffrée avec la clef publique RSA de la passerelle.
- Réponse du Marchand :
 1. Le marchand construit le message – accusé de réception – , signé numériquement comme suit :
DES (Accusé de Réception , SHA (Accusé de Réception)).

Commentaires :

1. Comment le marchand vérifie-t-il l'intégrité de la commande ?

→ Disposant de OI et de SHA(OI), envoyés par l'acheteur, il n'a qu'à appliquer SHA au premier terme et comparer avec le second.

2. Comment la passerelle vérifie-t-elle l'intégrité de PI ?

→ Disposant de SHA(OI) et de PI, elle applique SHA au second terme, concatène le tout et ré-applique SHA de nouveau. Finalement elle compare le résultat avec la signature duale.