

DEA Informatique - Rennes 1 - 2002-2003
SFRC

Sécurité des systèmes informatiques

(Durée : 1h30)

Sécurité du commerce électronique : exemple de SET

Ludovic Mé
janvier 2003

Le protocole SET a été conçu par Mastercard et Visa afin de sécuriser les transactions par carte bancaire sur des réseaux ouverts comme l'internet. Cet examen propose une analyse des mécanismes de protection de base que propose ce protocole.

Note importante : toutes les réponses que vous donnerez doivent être détaillées et motivées.

Les entités qui entrent en jeu (voir Fig. 1) sont l'acheteur, le vendeur, la banque du vendeur (accessible via une passerelle de paiement) et une ou plusieurs autorités de certification. La banque de l'acheteur n'est contactée que via un échange inter-banques classique n'entrant pas dans les spécifications de SET.

Exercice 1 : mécanismes de base

1.1 Certificats

Toute entité (acheteur, vendeur, passerelle de paiement) doit obtenir d'une autorité de certification (AC) un certificat de clé publique.

QUESTION : que contient classiquement un tel certificat ?

Dans le cas de SET, le certificat d'un client contient aussi son numéro de carte bancaire. Cette information ne peut circuler en clair lors de l'émission du certificat vers le client.

QUESTION : donnez la suite des échanges entre client et AC permettant une délivrance sécurisée du certificat client.

Indication : initialement, le client ne possède aucune clé. Il ne connaît que l'adresse électronique de la AC. En outre, il dispose du « logiciel SET », qui sait générer des clés symétriques et asymétriques.

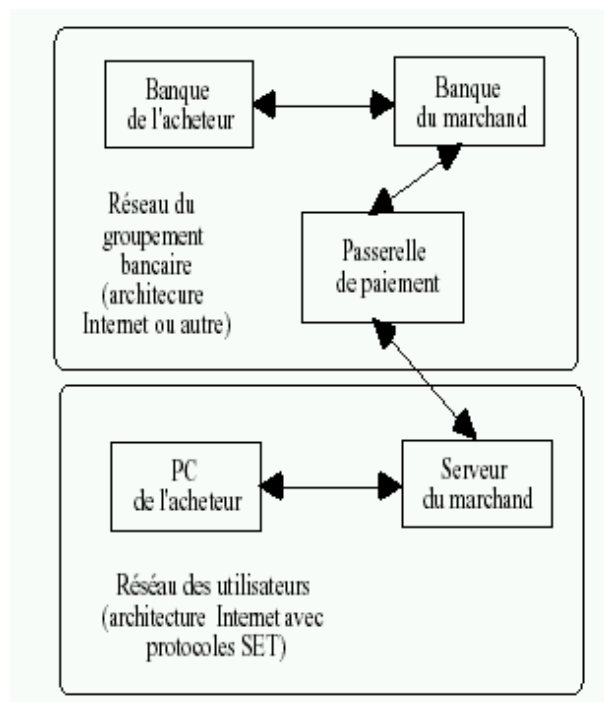


FIG. 1 – Acteurs entrant en jeu dans le protocole SET

1.2 Protection des échanges

Tout message M transmis de l'entité A à l'entité B est de la forme suivante :
 $A \rightarrow B : \{M, C_A, (H(M))_{S_A}\}_{K}, (K)_{P_B}$

QUESTION : que fait B à la réception de ce message? Expliquez d'où proviennent les clés utilisées. Expliquez ce que B vérifie dans C_A . Quels sont les services de sécurité offerts ici?

1.3 Protection supplémentaire lors d'une commande

Un acheteur envoie à un vendeur une demande d'achat ($I_{vendeur}$) et à sa banque une autorisation de transférer l'argent correspondant (I_{banque}). L'acheteur transmet au vendeur le message suivant :

$$\{I_{vendeur}\}_{P_{vendeur}}, \{I_{banque}\}_{P_{banque}}, H(I_{vendeur}), H(I_{banque}), \\ \{H(H(I_{vendeur}) + H(I_{banque}))\}_{S_{acheteur}}$$

QUESTION : $\{H\{H(I_{vendeur}) + H(I_{banque})\}\}_{S_{acheteur}}$ est appelée signature duale. Expliquez son rôle.

Exercice 2 : acte d'achat et autorisation de paiement

2.4 Acte d'achat

L'achat se déroule en deux échanges successifs.

La requête initiale de l'acheteur vers le vendeur passe en clair ; elle indique simplement l'intention de l'acheteur de passer commande. Le vendeur répond par un message contenant :

- un identifiant de commande signé,
- le certificat du vendeur,
- le certificat de la passerelle de paiement.

QUESTION : A la suite de ce premier échange, quelles vérifications doivent être effectuées par l'acheteur ?

Le second échange de l'acte d'achat est constitué par l'envoi par le client de la requête d'achat et par l'envoi par le vendeur d'un accusé réception.

La requête d'achat est constituée d'informations destinées au vendeur ($I_{vendeur}$: identifiant de commande (celui que vient de fournir le vendeur), produits, quantités, prix) et d'informations destinées à la banque via la passerelle (I_{banque} : identifiant de commande, No de carte). Le message émis est conforme à celui étudié en 1.3.

QUESTION :

- **Quels sont les contrôles qui sont fait par le vendeur à la reception de la requête d'achat ?**
- **Comment peut être constitué l'accusé de reception ?**

2.5 Autorisation de paiement

Pour se faire payer, le vendeur envoie à la banque via la passerelle de paiement un message contenant :

- l'identifiant de commande et le prix a payer (chiffré, signé),
- $\{I_{banque}\}_{P_{banque}}$,
- les certificats de l'acheteur et du vendeur.

QUESTION : décrivez les actions de la banque du vendeur avant et après qu'elle se soit mise en rapport avec celle de l'acheteur.