Paiement sécurisé sur internet

CHAIGNEAU Delphine
DANTE Alexandra
GARNODIER Karine

RICM3
25 janvier 2002

Plan

Introduction
1. Présentation
2. Les techniques actuelles
3. Les principaux courants
Conclusion
Questions
Liens

Plan

Introduction
1. Présentation
2. Les techniques actuelles
3. Les principaux courants
Conclusion
Questions
Liens

1. Présentation

1.1 Internet et commerce
1.2 Modes de paiement
1.3 Qualités d'un procédé

1.1 Internet et commerce

1.1.1 Commerce traditionnel
1.1.2 Commerce électronique

1.1 Internet et commerce

1.1.1 Commerce traditionnel :

- Livraison de biens/services matériels
- Avantages
  - visibilité permanente, bon marché, mondiale
  - économie de personnel

1.1 Internet et commerce

1.1.2 Commerce électronique :

- Livraison de substance sur le réseau
- Avantages
  - faible coût de distribution
  - faculté d'automatiser les transactions

1.2 Modes de paiement

- Crédit
  - Cartes de crédit
  - Chèques
  - Réseaux à valeur ajoutée
- Débit
  - Porte-monnaie électronique

1.3 Qualités d'un procédé

- Rapidité d'adoption
- Fiabilité
- Garanties de recours
  - Identité du commerçant
  - Traçabilité de la commande
- Confidentialité
  - Confidentialité de la commande
  - Anonymat de l'acheteur
  - Confidentialité des renseignements bancaires

1.3 Qualités d'un procédé

- Authentification
  - De l'argent électronique
  - Des messages
- Divisibilité
- Disponibilité
- Non-répudiation

Plan

Introduction
1. Présentation
2. Les techniques actuelles
3. Les principaux courants
Conclusion
Questions
Liens

2. Techniques actuelles

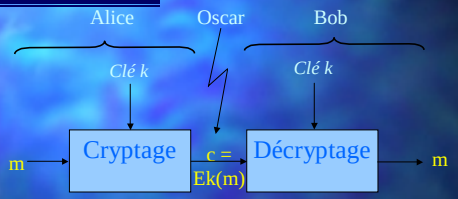
2.1 Procédés de cryptage
2.2 Signature électronique
2.3 Certificats électroniques
2.4 Identification
2.5 Datation

2.1 Procédés de cryptage

2.1.1 Algorithmes symétriques

2.1.2 Algorithmes asymétriques

2.1.1 Algorithmes symétriques



Avantage : Simplicité

Problèmes : - Transmission de la clé

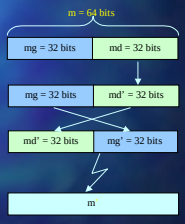
- Une clé différente par paire d'utilisateurs

Exemple : *Data Encryption Standard*

- Développé en 1976 par IBM
- Chiffrement par blocs de 64 bits
- Clé de 56 bits

16 fois avec plusieurs parties de la clé

- md est crypté par 1 **permutation** et 1 **substitution** en utilisant une partie de la clé.
- On « mélange » mg et md.

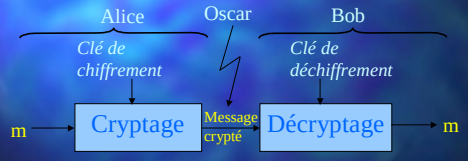


Exemple : *Data Encryption Standard*

- Fiabilité : facile à casser
- Performance : vitesse de chiffrement et de déchiffrement élevées
- Domaines d'utilisation :
  - domaine commercial
  - banques

2.1.2 Algorithmes asymétriques

- Clé publique, clé privée

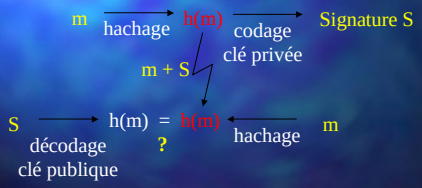


Exemple : *Rivest Shamir Adlemann*

- p et q 2 nombres premiers :p=11 et q=17
  entier d = 7
- entier e = 23
  (e x d –1) est multiple de (p-1)(q-1) et e < n
  n = p x q = 187
- Clé = clé secrète = (p,q,d) + clé publique = (n,e)
- $c = m^e$ modulo n => $m' = c^d$ modulo n
- Domaines d'utilisation : logiciels, industries, télécommunications

2.2 Signature électronique

- Introduite par Diffie et Hellman en 1992
- Empreinte électronique
  - Fonctions de hachage



2.3 Certificat électronique

- Document d'identité électronique attestant du lien entre une identité et une clé publique = identification
- Signé par l'autorité émettrice
- Mentionne :
  - Identité
  - Clé publique
  - Date d'expiration
  - Numéro de série

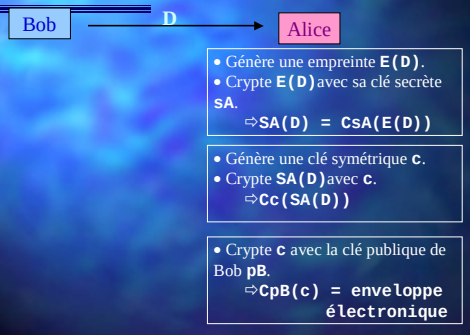
2.3 Certificat électronique

2.4 Identification

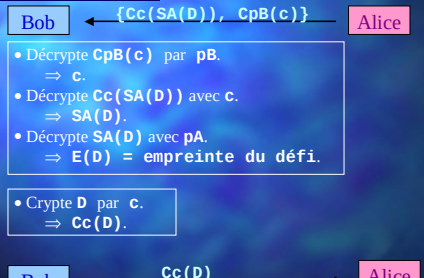
2.4.1 Identité certifiée

2.4.2 Identification par le réseau

2.4.1 Identité certifiée



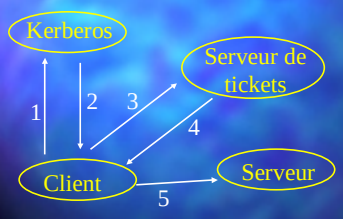
2.4.1 Identité certifiée



2.4.2 Identification par le réseau : Kerberos

- Développé au MIT en 1978
- Basé sur un protocole à clé secrète
- Service central de distribution de clés
- Base de données des identités

2.4.2 Kerberos



1 – demande du ticket d'accès au serveur de tickets (st)

2 – envoi du ticket (st)

3 – demande du ticket d'accès au serveur

4 – envoi du ticket de session

5 – demande d'utilisation d'un service

2.5 Datation

- Signature en aveugle : le signataire n'a pas accès au contenu du document
- Cryptage de l'empreinte du document
- Service de datation
  - Cryptage aléatoire
  - Clés publiques notoires et archivées

Plan

Introduction
1. Présentation
2. Les techniques actuelles
3. Les principaux courants
Conclusion
Questions
Liens

3. Les principaux courants

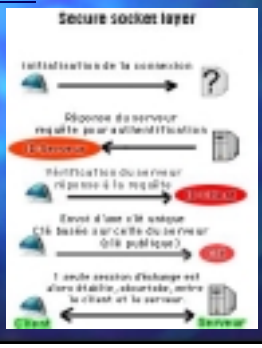
3.1 Approche transport sécurisé
3.2 Approche indépendante du transport

3.1 Transport sécurisé : SSL

3.1.1 Présentation
- SSL Record Protocol
- SSL Handshake Protocol

3.1.2 Fonctionnement
- Lancement d'une session SSL
- Utilisation de clés de session

3.1 Transport sécurisé : SSL



3.2 Approche indépendante du transport : SET

3.2.1 Présentation
3.2.2 Objectifs
3.2.3 Les différentes parties d'un paiement SET
3.2.4 Déroulement d'un paiement SET

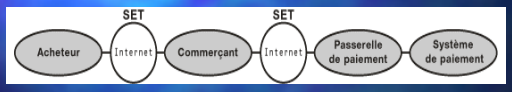
3.2 Approche indépendante du transport : SET

3.2.2 Objectifs

- Intégrité des données
- Authentification du titulaire de la carte
- Authentification du commerçant
- Confidentialité des données

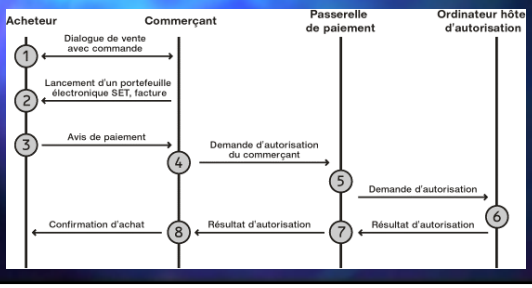
3.2 Approche indépendante du transport : SET

3.2.3 Les différentes parties d'un paiement SET



3.2 Approche indépendante du transport : SET

3.2.4 Déroulement d'un paiement SET



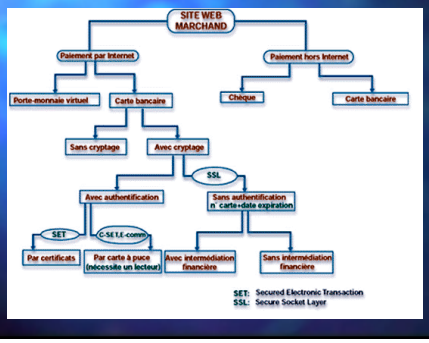
Plan

Introduction
1. Présentation
2. Les techniques actuelles
3. Les principaux courants
Conclusion
Questions
Liens

Conclusion

- Fonctions d'un système de paiement
  - Authentifier marchands et consommateurs
  - Sécuriser la transaction
  - Traiter l'intégrité de la transaction
  - Autoriser l'utilisation de plusieurs devises
  - Réaliser des transactions de tout montant

Conclusion



Plan

Introduction
1. Présentation
2. Les techniques actuelles
3. Les principaux courants

Conclusion
Questions
Liens

Questions ...

Plan

Introduction
1. Présentation
2. Les techniques actuelles
3. Les principaux courants

Conclusion
Questions
Liens

Liens

- http://www.er.uqam.ca/nobel/m237636/paiement/intro.html
  Dossier sur le paiement sur Internet
- http://www.withoutcard.com/
  Enquête sur le commerce électronique et les moyens de paiements, les problèmes de sécurité sur Internet
- http://www.rambit.qc.ca/plamondon/ecashind.htm
  Le paiement électronique sur Internet : recensement et analyse des différentes méthodes
- http://www.w3.org/Ecommerce/
  Le commerce électronique

Liens

- http://www.chez.com/nopb/crypto.html
  Chiffrement et cryptographie : Technologies, aspect technique du chiffrement, le chiffrement en France
- http://www.osidler.multimania.com/authentification/
  - Kerberos.htm : Le système Kerberos : description et fonctionnement
  - Ssl.htm : Fonctionnement du protocole SSL et authentification avec SSL
- http://www.guill.net/reseaux/Authentification.html
  Description du système d'authentification avec Kerberos
- http://www.pourlascience.com/numeros/pls-260/internet.htm
  Ce lien donne accès à 4 dossiers sur le thème du e-commerce

Liens

- http://www.set.ch/basics/basics-fr.html
  Présentation de SET avec définitions, objectifs, parties et déroulement
- http://actualite.free.fr/dossier/ecom
  Dossier sur le e-commerce : état des lieux : paiement sécurisé, formes de paiement, dans quels cas utiliser le paiement sécurisé, description de 4 normes
- http://nicogold.free.fr/pages/ssl.html
  Présentation du protocole SSL (Secure Socket Layer)
- http://www.idf.net/articles/paiements.html
  Moyens de sécurisation (SSL et SET), paiements sur Internet, portefeuille virtuel.