

Le paiement sur Internet



F.-Y. Villemin (f-yv@cnam.fr)

<http://dept25.cnam.fr/ITCE>

Types de paiement

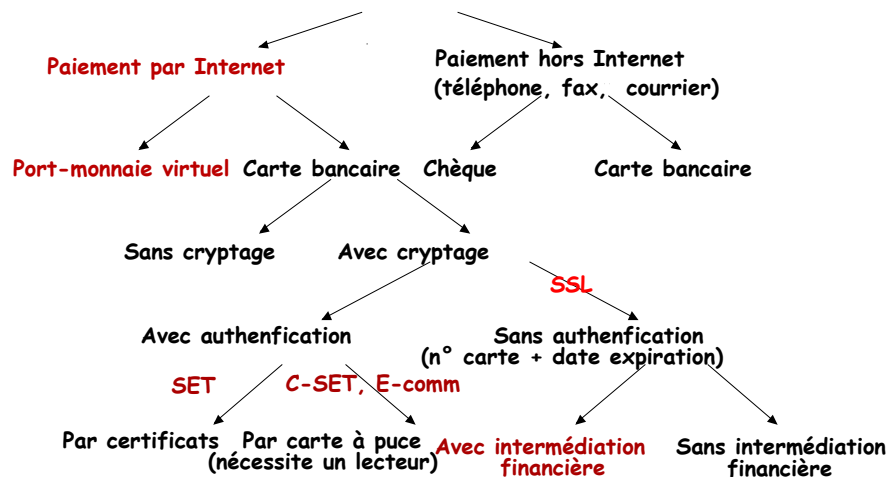
- Paiement à la livraison
- Paiement par virement / facture
- Paiement par virement automatique
- Paiement par cartes de crédits
 - Transmis par Fax
 - Transmis par l'Internet (SSL)
- Futur: par protocole sécurisé
- Paiement par micropaiement, ou par GSM

© F.-Y. Villemin 2012

2

Types de paiement

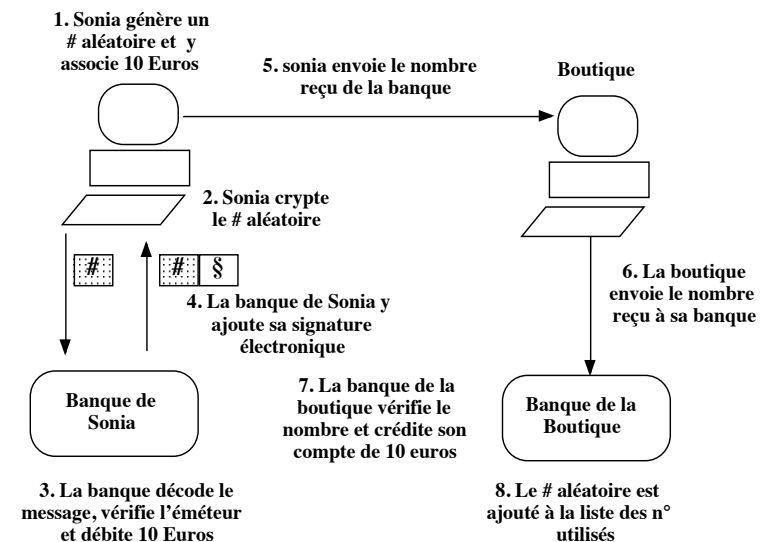
Moyens de paiement



© F.-Y. Villemin 2012

3

Porte-monnaie électronique



© F.-Y. Villemin 2012

4

Porte-monnaie électronique

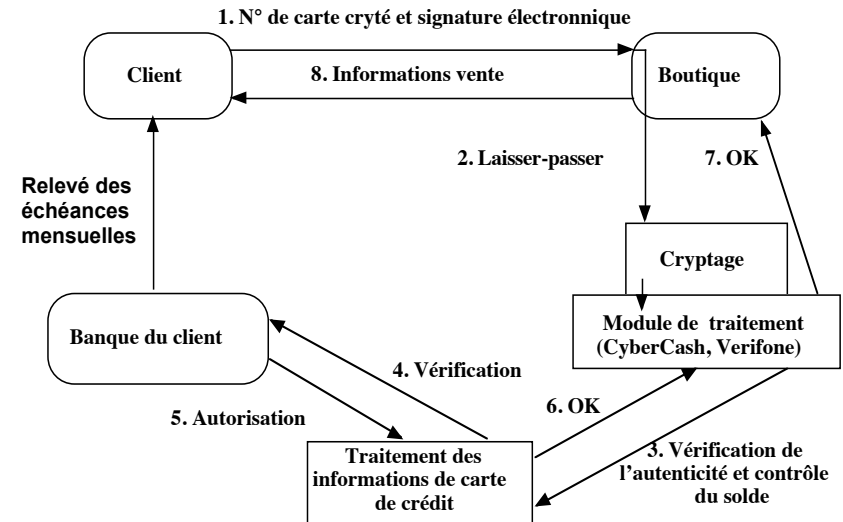
Avantages :

- les banques ne savent pas qui a dépensé quoi et où (anonymat)
- système de "monnaie en ligne" : vérification de l'authenticité en temps réel par la banque émettrice
- possibilité de Clearing interbancaire des monnaies électroniques
- utilisation de la cryptographie à clé publique et de signatures numériques authentifiant les utilisateurs et garantissant contre les risques de répudiation

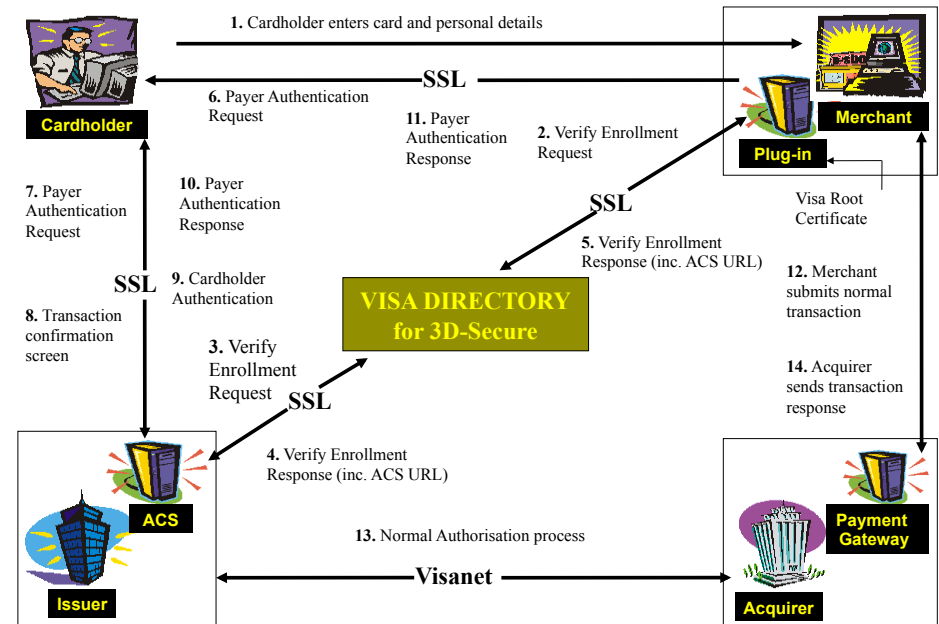
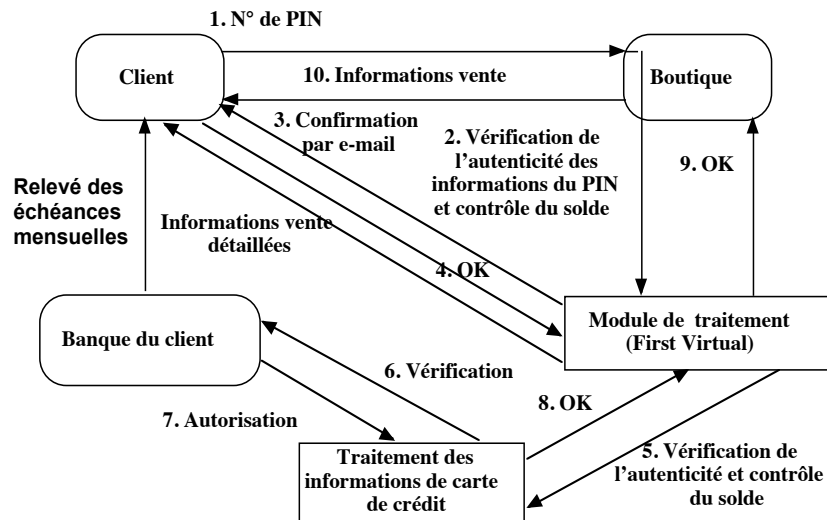
Limites :

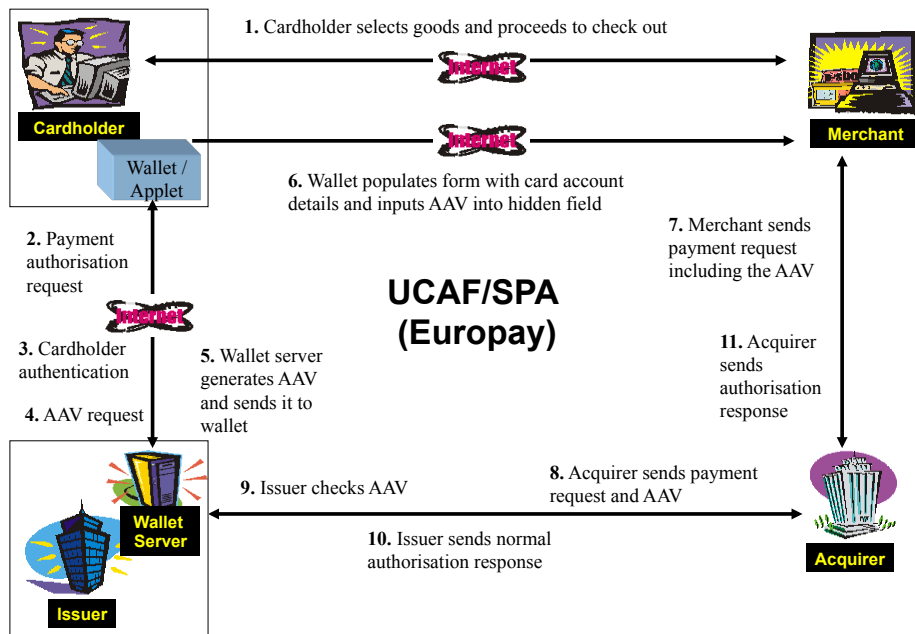
- contrôle des pouvoirs publics sur la création monétaire
- gestion de la bibliothèque des clés publiques

Cartes et intermédiaires



Cartes et intermédiaires





Cartes et intermédiaires

Autre intermédiaires :

- Authorize.Net
- CyberCash,
- DataCash
- Lloyds TSB CardNet
- NetBanx
- PayPal
- Planet Payment Systems
- Protix
- SECPay
- Secure Trading
- Trivnet
- Verisign Payment System
- WorldPay...
- PicoPay : micropaiement par les bandeaux publicitaires

© F.-Y. Villemin 2012

10

Cartes et intermédiaires



Cas de PayPal :

Action	Informations transmises
1. Nick se connecte à PayPal.com et s'enregistre	. nom de Nick . adresse de Nick . e-mail de Nick
2. Nick déclare donner 50 € à Sonia en entrant ses données de carte de crédit, l'e-mail de Sonia et le montant (30c + 2.2% du montant)	. numéro et date de la carte de Nick . montant de la transaction . e-mail de Sonia
3. La carte de Nick est débitée de 50 € et un compte au nom de Sonia est créé et crédité de 50 €	
4. Sonia reçoit un e-mail de notification et un lien	
5. Sonia se connecte à ce lien et s'enregistre	. nom de Sonia . adresse de Sonia
6. Sonia peut transférer cet argent sur son compte bancaire ou sur un autre compte PayPal ou demander un chèque à PayPal (30c + 1.6% du montant)	

© F.-Y. Villemin 2012

11

Cartes et intermédiaires

	
Chiffrement (128 bits) communication entre client et POS serveur.	Contrôles moins précis que sur un terminal réel (CVV non contrôlé)
Pas de numéros de carte de crédit chez le commerçant (POS server).	Identité du porteur non contrôlée. Pas d'authentification. Anonymat lié à Internet.
Contrôle validité du PAN, disponible, date de validité et liste noire.	Répudiation des transactions par le porteur aux frais du commerçant jusqu'au Liability Shift.

© F.-Y. Villemin 2012

12

Cartes et intermédiaires

Avantages :

- sécurité pour l'acheteur
- minimisation des risques de faux numéros de cartes de crédit pour les fournisseurs
- acceptation de la transaction après autorisation bancaire, donc en limitant les risques de cartes de crédit refusées.

Limites :

- aucun chiffrement n'est "incassable"

Perspectives :

- accords avec des institutions bancaires et SET

SET

L'incapacité à identifier formellement l'acheteur est l'un des principaux points faibles des solutions SSL

Visa, Eurocard/Mastercard, IBM, Microsoft et Netscape ont développés un **standard mondial** pour le paiement sûr par carte de crédit sur Internet, le protocole Secured Electronic Transaction (**SET** : www.setco.org) :

- intégrant des fonctions d'
 - identification de l'acheteur
 - identification du marchand
 - identification de la banque
- utilisant des certificats numériques pour identifier les parties en présence

SET

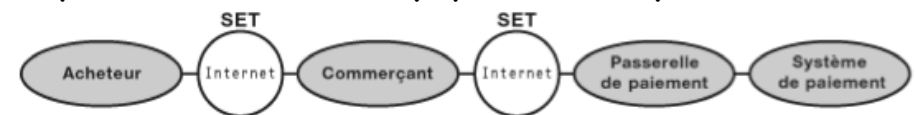
La carte du porteur doit être certifiée par un serveur SET et l'acheteur doit disposer d'un logiciel de paiement SET sur son ordinateur

SET satisfait aux exigences suivantes, :

- Intégrité des données (signature numérique)
- Authentification du titulaire de la carte
- Authentification du commerçant
- Confidentialité des données

SET

Les parties suivantes sont impliquées dans un paiement SET :



Acheteur:	navigateur Web	Portefeuille électronique SET avec code privé et certificat SET
Commerçant :	serveur Web	logiciel POS SET pour commerçants avec code privé et certificat SET
Passerelle de paiement :		passerelle de paiement SET avec code privé et certificat SET

SET

Portefeuille électronique SET (SET Wallet) est le logiciel dont a besoin le titulaire de carte pour participer à SET. Il exécute le protocole SET du côté du titulaire de carte et mémorise le code et le certificat d'une ou plusieurs cartes

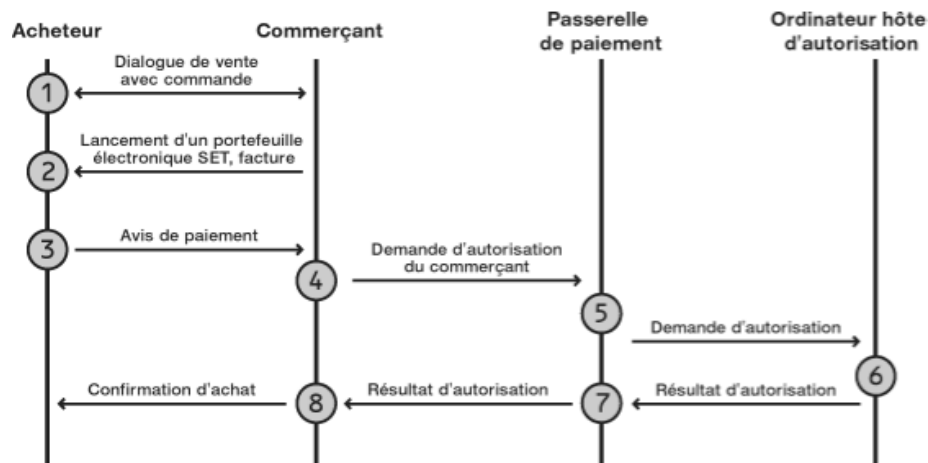
Logiciel POS (SET) pour commerçants est le logiciel dont a besoin le commerçant pour participer à SET. Il exécute le protocole SET du côté du commerçant

SET

Certificat (SET) est une sorte de pièce d'identité qui permet aux principales parties impliquées dans SET (titulaire de carte, commerçant) de décliner leur identité. Dans le certificat SET du titulaire de carte, l'émetteur de carte atteste avoir fourni une carte de crédit au titulaire et engage sa responsabilité pour le titulaire. Dans le certificat SET du commerçant, le responsable du traitement des paiements par carte de crédit engage sa responsabilité pour le commerçant

Passerelle de paiement (SET) est le logiciel dont a besoin le responsable du traitement des paiements par carte de crédit pour participer à SET. Il exécute le protocole SET du côté du responsable du traitement

SET



SET

2. Lancement du portefeuille électronique SET et présentation de la facture. L'acheteur débloque le portefeuille électronique en indiquant son identification d'utilisateur et son mot de passe. La facture lui est alors présentée dans le portefeuille électronique SET

3. L'acheteur vérifie la facture, sélectionne l'une des cartes de crédit disponibles dans le portefeuille électronique et confirme le paiement. Le certificat du commerçant et celui de la passerelle de paiement SET sont vérifiés dans un premier temps. Un message est établi avec une valeur hash portant sur la facture, ainsi que la monnaie et le montant. Le message est ensuite signé par le titulaire de la carte (au moyen de son code secret), crypté et envoyé au commerçant avec le certificat du titulaire de la carte

SET

6. Le commerçant commence par vérifier le certificat du titulaire de la carte (client) afin d'être certain qu'il a affaire à un titulaire de carte autorisé. Il fait une demande d'autorisation à la passerelle de paiement SET: Il envoie le message de l'acheteur avec son certificat (client), un message analogue de sa part (valeur hash, monnaie, montant) qui est ensuite signé par le commerçant (au moyen de son code secret SET), crypté et complété par son certificat (commerçant)
5. La passerelle de paiement SET contrôle les points suivants:
signature du titulaire de la carte
signature du commerçant
concordance des informations des deux messages (valeur hash de la facture, monnaie et montant). Si résultats positifs, la passerelle de paiement SET transmet alors la monnaie, le montant et le numéro de la carte de l'acheteur (numéro tiré du certificat) à l'ordinateur hôte d'autorisation, afin que ce dernier traite ces données

SET

6. L'ordinateur hôte d'autorisation de l'émetteur des cartes de crédit s'assure qu'il existe un contrat valable avec le commerçant, que la carte n'est pas bloquée et que le plafond de la carte n'est pas dépassé
7. Le résultat de l'autorisation est renvoyé à la passerelle de paiement SET qui communique à son tour le résultat au serveur du commerçant
8. Lorsque la passerelle de paiement SET a autorisé l'achat, l'acheteur reçoit confirmation du bon déroulement de l'achat. Si l'achat est refusé, l'acheteur est informé du motif du refus

SET

Points forts de SET

- Protocole harmonisé Visa - Mastercard défini en 1996.
- Réduction des Charge-backs.
- Amélioration de la sécurité liée aux transactions sur Internet.
- Amène un climat de confiance concernant le business sur Internet.

Raisons de l'échec de SET

- Déploiement trop lent
- Sous-estimation de l'effort d'intégration dans le magasin virtuel du commerçant .
- Licence d'utilisation non adaptée au marché (trop cher pour le petit commerçant).
- Pas de solutions intégrées pour les clients (non portable).
- Pas de marketing.
- Pas de support Visa aux USA.
- Pas d'avantage financier offert par Visa / Eurocard

SET et Cyber-Comm

En France, le certificat SET n'est pas une preuve absolue de paiement. Le GIE Cartes bancaires et les banques ont donc eu l'idée d'utiliser la puce au lieu des certificats SET pour authentifier de façon forte les paiements

C-SET (Chip-Secure Electronique Transaction), est un dispositif de paiement sur Internet sécurisé par carte à puce

C-SET permet donc d'effectuer des paiements en France comme à l'étranger

Pour les paiements internationaux, le système reste compatible avec les logiciels SET à travers une passerelle logicielle

SET et Cyber-Comm

Groupeement Cyber-Comm inclut Banques Populaires, BNP, Caisses d'épargne, CCF, Crédit agricole, Crédit Lyonnais, Crédit mutuel, La Poste, Société générale, Europay, Visa, Gemplus, France Télécom, Alcatel et Bull

La solution garantit une sécurité absolue tant du côté du marchand que de celui de l'acheteur, mais elle requiert un lecteur de carte à puce (environ 25 €) et l'installation d'un logiciel de paiement SET sur le poste client

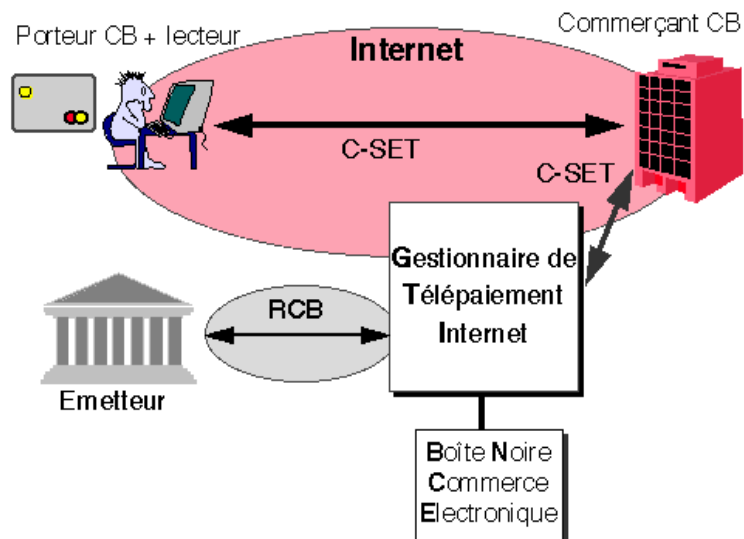
SET et Cyber-Comm

Les **Boîtes Noires Commerce Electronique** (BNCE) sont des matériels sécurisés de cryptographie

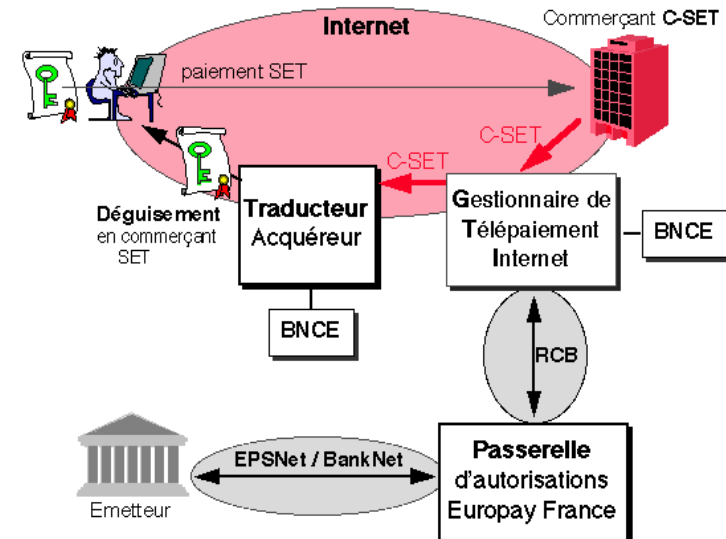
Les **Gestionnaires de Télépaiement Internet** gèrent les paiements nationaux pour le compte des banques des commerçants, et permettent d'offrir un service de délégation, sous certains montants, pour le compte des banques émettrices de cartes

Les **Traducteurs** assurent la gestion des flux internationaux en jouant le rôle de Passerelles de Sécurité entre la France et l'International

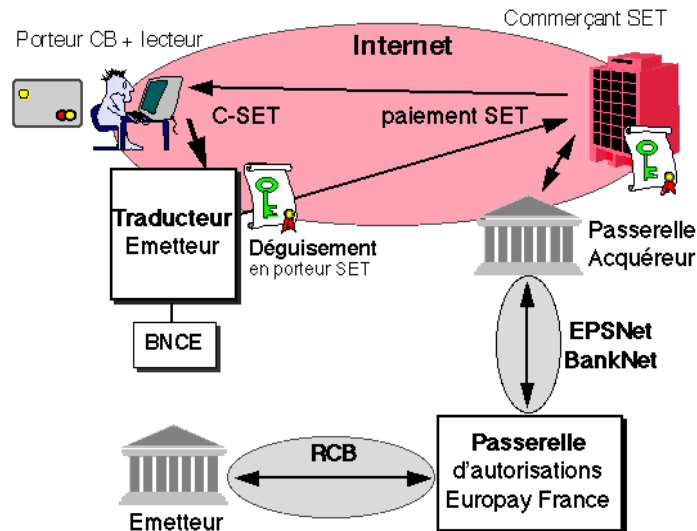
SET et Cyber-Comm



SET et Cyber-Comm



SET et Cyber-Comm



Yescard

La **yescard** est une carte à puce programmable qui permettait de faire des transactions d'achats sur quelques types d'automates de paiement électronique (Diffusion de clés sur Usenet)

Fraude très localisée sur quelques sites :

- En dessous d'un seuil de transaction d'achat, l'authentification de la carte et de son porteur sont faits en local
- Seuls les automates (carburant, titre de transport, location vidéo, etc.) sont concernés :
 - ◆ Les DAB/GAB requièrent une demande d'autorisation en ligne
 - ◆ Les TPE chez les commerçants nécessiteraient la contre-façon visuelle de la carte ou une collusion

Logiciel G0lee pour la fabrication de Yescard

Migration EMV 5.1 et 5.2 en cours. A compter de janvier 2002, la clef VA (320 bits) n'est plus utilisée, remplacée par une clef VS (768 bits) avec le durcissement du processus d'authentification et de non répudiation (certificat d'achat)

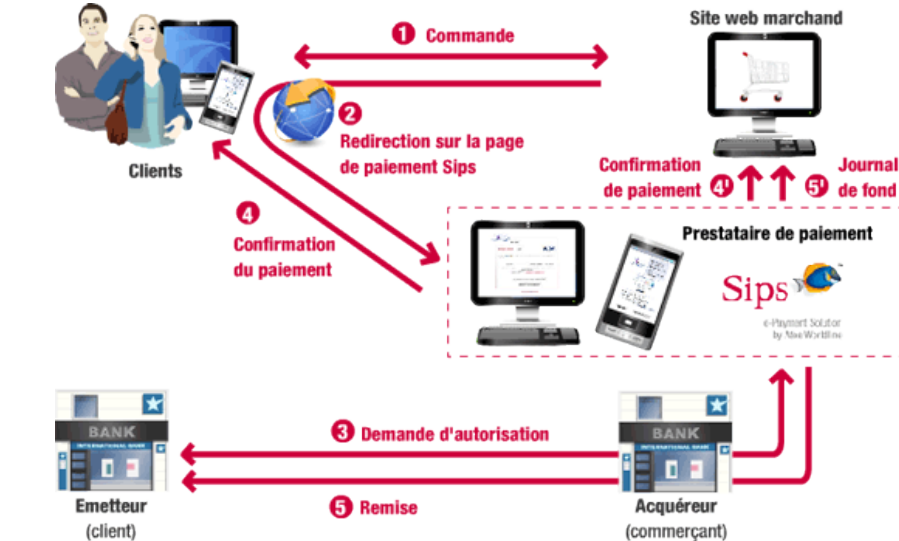
Comparaisons

	En clair	SSL	SET	C-SET
Intégrité des données	☹	☹	☺	☺ ☺
Authentification	☹	☹	☺	☺ ☺
Non-répudiation	☹	☹	☺	☺ ☺
Assurance de paiement pour le commerçant	☹	☹	☺	☺ ☺
Confidentialité	☹	☺	☺	☺ ☺
Simplicité d'utilisation	☺ ☺	☺ ☺	☺	☺
Simplicité de mise en œuvre	☺ ☺	☺ ☺	☹	☺
Performances	☺ ☺	☺ ☺	☹ ☹	☺

3-D Secure

- **3-D Secure** a été développé par Visa pour augmenter le niveau de sécurité des transactions lors du paiement d'achats effectués sur des sites web
- **3-D Secure** a été adopté par Mastercard
- Le protocole de **3-D Secure** permet une meilleure authentification du détenteur de la carte en liant l'autorisation financière avec une authentification en ligne
- Cette authentification est basée sur un modèle comportant 3 domaines (3D) qui sont: le commerçant, la banque et le système de carte bancaire

3-D Secure



© F.-Y. Villemain 2012

33

3-D Secure

Selon la banque émettrice de la carte, pour s'authentifier, le client doit indiquer :

- 1/ son identifiant de banque en ligne, puis indiquer un des codes inscrits sur sa "carte de clés personnelles" (une grille de 64 codes à 4 chiffres dans laquelle il faut piocher le bon code en fonction de la ligne et de la colonne demandée par le site web)
- 2/ sa date de naissance*
- 3/ sa date de naissance et un code est envoyé par sms
- 4/ un mot de passe personnel, crée lors de la première utilisation
- 5/ son nom, le code postal de sa résidence et sa date de naissance

*La validation par la date de naissance présente un risque de fraude reste fort, car la date de naissance est facile à obtenir

© F.-Y. Villemain 2012

34

Sources

- <http://www.setco.org/>
 - <http://www.set.ch/>
 - <http://www.c-set.com/c-set.html>
 - <http://www.e-comm.fr/internet.html>
 - <http://www.ensam.inra.fr/infoservices/1998/liberi/paiement.html>
 - <http://www.decllic.net/francais/savoir/dossier/paiement.htm>
- D. Kosiur "Understanding electronic commerce", Microsoft Press 1997

© F.-Y. Villemain 2012

35