3D Secure / Verified by Visa / SecureCode: Qu'est-ce que c'est ?

Depuis octobre 2008, les banques et commerçants en ligne ont commencé à adopter le système **3DSecure** pour les paiements sur Internet.

Qu'est-ce que c'est ?

3DSecure est appelé "*Verified by Visa*" chez Visa, et "*SecureCode*" chez Mastercard.
(Les logos ne sont pas recopiés ici pour des raisons légales.)

Ce système a été inventé pour éviter les fraudes de type CNP (Card No Present), c'est-à-dire les paiements frauduleux par carte bancaire sans présence réelle de la carte (numéros de carte volés, par exemple).

Le but est :

- de réduire la fraude pour les commerçants.
- de sécuriser les paiements des clients.

Pourquoi le cryptogramme visuel ne suffit pas

Un paiement par carte sur internet nécessite généralement:

- Le numéro de la carte
- La date d'expiration
- Le cryptogramme visuel

Le cryptogramme visuel, ce sont les 3 nombres au dos de votre ca
qu'on vous demande généralement de saisir lors d'un achat sur int

Or ces informations peuvent être lues visuellement sur la carte et recopiées, permettant ainsi le paiement sans présence de la carte, et donc la fraude.

Avec 3DSecure, des informations complémentaires vous seront demandées pour valider le paiement.
Quelqu'un qui recopierait les informations de votre carte ou même qui vous la volerait ne pourrait pas effectuer des achats chez les marchands utilisant 3DSecure, car il ne connaît pas ces informations complémentaires.

3DSecure ou non

Pour qu'un paiement soit en mode 3DSecure, il faut que votre carte soit 3DSecure **et** que le commerçant supporte 3DSecure.

- La quasi-totalité des cartes bancaires nouvellement fabriquées sont désormais 3DSecure.
- Pour les anciennes, selon les banques, le basculement 3DSecure sera automatique, ou on vous demandera de signer un avenant à votre contrat. Dans tous les cas, cela ne nécessite aucun changement de carte ni de modification de votre carte existante.
- Le passage à 3DSecure ne doit normalement rien vous coûter.

Notez qu'avec une carte 3DSecure, vous pouvez très bien continuer à faire des achats en mode non 3DSecure chez les commerçants qui ne supportent pas 3DSecure. Ces achats ne seront pas sécurisés par 3DSecure.

Si votre carte n'est pas 3DSecure, vous pourrez ou non faire des achats chez les commerçants qui sont 3DSecure (Les commerçants 3DSecure sont libres d'accepter ou non de continuer à accepter les paiements avec des cartes non-3DSecure)

Dans la pratique

Dans la pratique, vous effectuerez vos achats sur internet comme d'habitude.
Vous entrerez toujours votre numéro de carte, expiration et cryptogramme, mais après avoir entré ces informations, **vous serez redirigé vers le site de votre banque** qui vous demandera ces informations supplémentaires.

Une fois les informations fournies, vous reviendrez sur le site du commerçant qui vous confirmera le paiement.

Dans ce scénario, le serveur de votre banque va confirmer au commerçant que vous êtes bien le propriétaire de la carte.

En quoi consiste l'authentification ?

Pendant un paiement 3DSecure, lorsque vous serez sur le site de votre banque, cette dernière vous demandera des informations que vous êtes seul censé connaître, prouvant que vous êtes bien le propriétaire de la carte.

Chaque banque est libre de choisir son moyen d'authentification.

Parmi ceux-ci, on trouve:

- un classique mot de passe (qu'il est possible de changer)
- un système par carte de clé (feuille papier) que votre banque vous a envoyée (style bataille navale : saisissez le nombre à la colonne 5, ligne 3).
- un système par boitier électronique (vous saisissez un code affiché par un boitier électronique)
- votre date de naissance
- et bien d'autres encore...

Notez qu'il est particulièrement lamentable que certaines banques se contentent de votre date de naissance, car cette information est rarement vraiment privée et parfois facile à trouver. Si votre banque est dans ce cas, je vous invite à protester vigoureusement auprès de votre banque pour qu'elle adopte un système d'authentification plus solide.

(Pour information, les joueurs du jeu "*World Of Warcraft*" peuvent sécuriser l'accès à leur jeu avec un boitier qui leur coûte 5€. Il serait honteux que les banques ne puissent pas faire de même.)

Légalement

Lors de tout achat internet normal (non-3DSecure), à aucun moment votre identité n'est prouvée (code PIN ou signature). Cela veut dire qu'il suffit de contester un paiement pour que votre banque vous rembourse.
La responsabilité est du côté de la banque du commerçant, auprès de laquelle votre banque réclamera la somme.

Lors d'un achat en mode 3DSecure, si l'authentification est un succès, il y a un **transfert de responsabilités** vers **votre** banque. (Puisqu'elle a affirmé que c'était bien *vous* qui étiez en train de payer, elle ne peut plus contester et doit transférer l'argent à la banque du commerçant.)

Et bien entendu, votre banque transfèrera cette responsabilité vers vous : Vous ne pourrez plus contester un paiement 3DSecure et vous faire rembourser.
C'est pour cela qu'il est important que votre banque adopte une méthode d'authentification solide.

Notez que **si l'authentification est un échec** et que la banque du commerçant réclame le recouvrement de la somme, votre banque est censée refuser. Si elle l'accepte malgré tout, vous pourrez contester ce débit et vous faire rembourser (puisque rien n'aura prouvé que c'est vous qui avez effectué le paiement).

3DSecure, bien ou mal ?

Dans la théorie, c'est bien :

- Cela réduit la fraude chez les commerçants
- Cela réduit la fraude pour les internautes
- L'adoption grandissante de 3DSecure chez les marchands en ligne rendra la fraude en ligne de plus en plus difficile.
- Les sites marchands adoptant 3DSecure pourront éviter de recourir à des entreprises comme FIA-NET (particulièrement pénible pour les clients.)
- À aucun moment le commerçant n'est en possession de ces informations complémentaires, et ne peut donc pas ses les faire pirater. Vous ne saisissez ces informations que sur le site de votre banque.

Dans la pratique, les systèmes d'authentification faibles mettent l'internaute dans une mauvaise situation en cas de fraude.