

# Sécuriser le e-commerce avec les solutions « Remote Card Authentication » dans l'infrastructure « 3D-Secure »

*Ce livre blanc a été rédigé par XIRING, leader européen des solutions d'authentification bancaire basées sur carte à puce. Il se concentre sur la technologie « remote card authentication » plutôt que sur les offres existantes et a pour but d'éclairer les banques et prestataires de service sur les utilisations et les bénéfices de la technologie RCA pour sécuriser le commerce en ligne.*



## Introduction

Le commerce électronique en France connaît une croissance de plus de 60% par an. Le nombre de transactions des 24 commerçants du panel ACSEL en France (l'Association pour le Commerce et les Services en Ligne) a atteint près de 12 millions de transactions au cours du premier trimestre 2007. Cette croissance est portée par l'accélération de l'équipement des ménages en haut débit. Un facteur essentiel du développement du e-commerce est la confiance des internautes dans la sécurité des paiements en ligne : alors que les e-transactions ne représentent que 5% des transactions, elles totalisent 35% de la fraude totale, cette fraude a progressé de 41% en France (source : Banque de France, Fraud World, 2007).

### e-commerce en France : chiffres clés 2006\*

12 milliards d'euros de CA (x6 en 4 ans)

132 millions de transactions en ligne

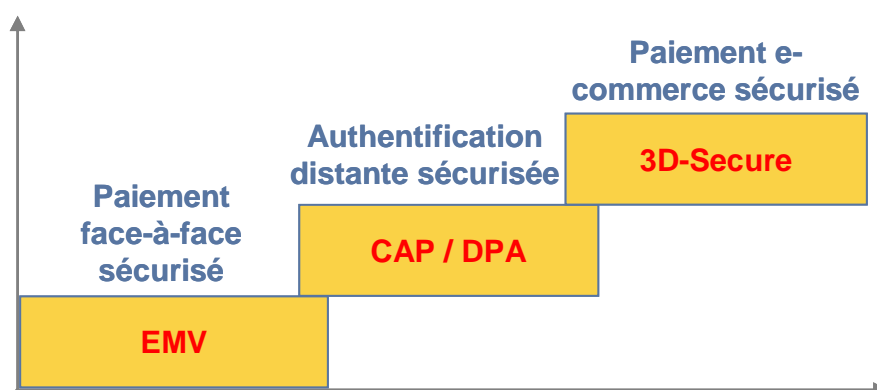
17.6 millions d'acheteurs en ligne (6 internautes sur 10)

80% des paiements en CB

\* source Europay France

Le volume actuel des paiements e-commerce réalisés par carte bancaire justifie l'évolution de la sécurité des transactions à distance pour atteindre le même niveau que celui des transactions en face-à-face basées sur la carte à puce EMV. Il est certain que tout comme le déploiement de la technologie carte à puce en remplacement des cartes à piste magnétique a drastiquement réduit la fraude dans le monde réel, cette mise à niveau aura le même effet dans les transactions à distance.

Pour accompagner cette évolution du commerce en ligne en apportant la sécurité nécessaire, VISA et MasterCard ont lancé en 2001 le modèle « 3D-Secure », dont la mise en place s'inscrit naturellement après le déploiement du standard EMV (pour les cartes de paiement) et du standard CAP/DPA pour l'authentification forte à distance (partie intégrante des programmes MasterCard « SecureCode » et Visa « Verified by Visa »).

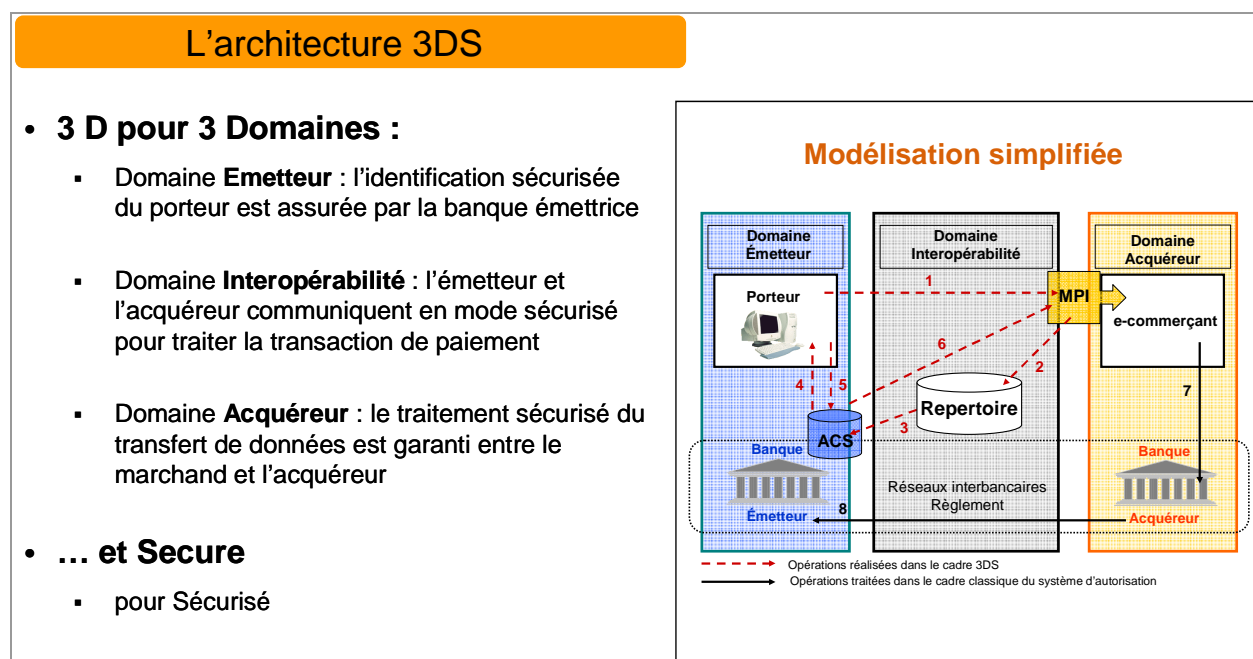


## L'infrastructure 3D-Secure

Aujourd'hui, lorsque l'internaute passe à l'étape « paiement » dans un achat en ligne, le plus souvent, il est redirigé vers un site externe (une banque ou un opérateur spécialisé). A cette étape, la sécurité visible est assurée par la mise en œuvre du protocole SSL/TLS (Secure Socket Layer / Transport Layer Security – matérialisé par le « cadenas » apparaissant en bas du navigateur web). Cette mesure de sécurité porte sur la confidentialité, en chiffrant les informations échangées, mais ne porte pas sur le contenu.

Lorsqu'il choisit de payer par carte bancaire, moyen de paiement largement privilégié, l'internaute donne trois informations : le numéro de sa carte, la date d'expiration et le code de sécurité (les trois chiffres au dos de la carte). Ces informations statiques sont insuffisantes pour garantir que l'internaute est bien le détenteur de la carte, ni même qu'il la détient physiquement (il suffit de quelques secondes à une personne malveillante pour copier ces informations, pour ensuite les « rejouer » tant que la carte n'est pas mise en opposition).

L'appellation « 3D-Secure » est la contraction de « Trois Domaines de Sécurité » : le domaine acquéreur, le domaine émetteur et le domaine interbancaire. Lancée en 2001 par Visa et MasterCard, 3D-Secure adapte aux transactions réalisées à distance le modèle de paiement des transactions par carte en face à face, en définissant les rôles et responsabilité de chaque intervenant (ou domaine).



Les acteurs d'une transaction type sont : le client (porteur de la carte), le commerçant, la banque du client, la banque du commerçant. Le système 3D-Secure donne à la banque émettrice (celle du client) la responsabilité d'identifier et d'authentifier le porteur de carte. Il leur faut donc un moyen sûr d'authentifier leurs clients.

Le recours à un mot de passe statique étant de plus en plus controversé, un code à usage unique généré par un lecteur personnel et une carte à puce apparaît comme une réponse idéale pour l'internaute : En utilisant une solution CAP/DPA, la banque est assurée que la carte à puce a été physiquement utilisée et introduite dans le lecteur de carte au moment de l'achat en ligne.

Ainsi, la mise en œuvre d'une solution CAP/DPA dans l'architecture 3D-Secure permet de garantir que l'internaute est bien le détenteur légitime de la carte et que c'est bien lui qui l'utilise au moment du paiement.

Les services de banque en ligne étaient confrontés à la même problématique avec l'utilisation de mots de passe statiques. De très nombreuses banques européennes ont renforcé l'authentification de leurs utilisateurs par le déploiement de solutions CAP/DPA, en bénéficiant de l'infrastructure EMV déjà déployée. L'association EMV+CAP/DPA s'intègre parfaitement dans l'infrastructure 3D-Secure et s'impose comme la meilleure solution technico-économique pour sécuriser le commerce en ligne.

## Les enjeux en France

En France, le « transfert de responsabilité » interviendra en octobre 2008 pour les paiements à distance nationaux (c.à.d. les transactions pour lesquelles le porteur de la carte et le commerçant sont tous deux situés en France). Dès lors, le commerçant bénéficiera de la garantie de paiement pour les transactions réalisées par carte.

Le GIE Cartes Bancaires a validé l'adoption de l'architecture 3D-Secure pour les transactions nationales et conseille la mise en place d'un système d'authentification forte par les banques. Plusieurs solutions sont possibles, à chaque banque de choisir son propre système d'authentification.

La Banque de France recommande la mise en place de moyens d'authentification forte dynamiques pour sécuriser les transactions à distance.

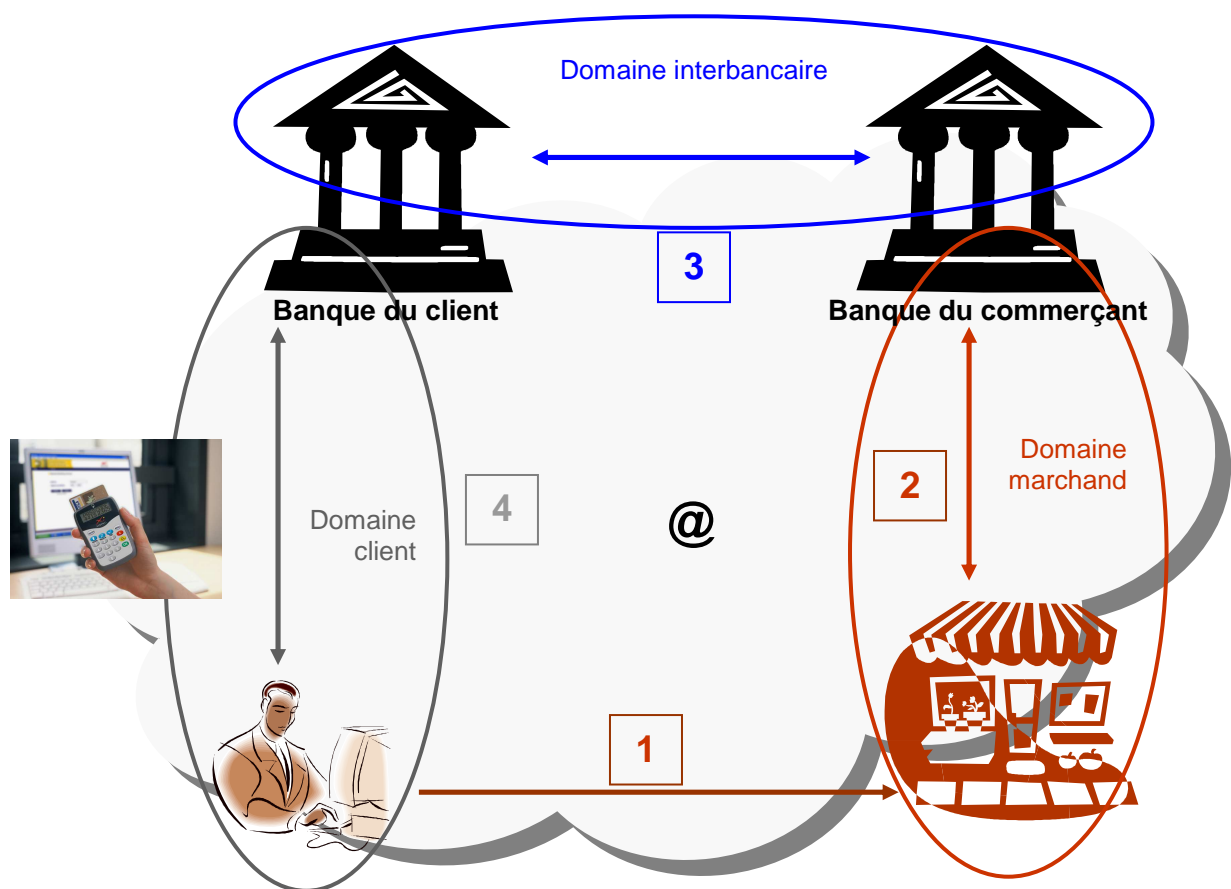
Côté client, tous les déploiements terrain démontrent que les consommateurs augmentent leur utilisation des services en ligne lorsqu'on renforce la sécurité perçue.

Les solutions "Remote Card Authentication" reposent sur l'utilisation conjointe d'une carte de paiement EMV et d'un lecteur d'authentification qui génèrent un mot de passe à usage unique (« one-time password » ou OTP) ou une signature électronique, basés sur les clés secrètes stockées dans la puce de la carte.

Avec cette solution EMV-CAP, vue par les commerçants et les consommateurs comme le programme « SecureCode » de MasterCard ou « Dynamic Passcode Authentication / Verified by Visa » de VISA, un paiement en ligne bénéficie de toute la sécurité de la carte à puce, comme au distributeur de billets ou chez un commerçant.

## 3D-Secure + CAP/DPA + EMV : Un modèle simple et intuitif

1. Le client se connecte sur le site de vente en ligne, sélectionne ses achats et valide son panier.
2. Au moment de payer, les informations (montant de la transaction, référence, etc.) sont envoyées à la banque du e-commerçant ou à son opérateur de paiement.
3. La banque du commerçant demande à la banque du client de vérifier que le porteur de la carte en est bien son propriétaire, et qu'il est habilité à signer le montant de la transaction.
4. La banque du client procède à son authentification, à l'aide d'une solution « Remote Card Authentication », qui permet à la banque d'être absolument certaine que la carte bancaire du client est physiquement présente au moment de la transaction et que la personne qui détient la carte connaît le code confidentiel. La banque est donc dans la même situation de sécurité que lors d'un paiement en face à face.



## CONCLUSION

Comme décrit dans ce document, les trois standards EMV, CAP/DPA et 3D-Secure sont parfaitement complémentaires :

- Une banque qui a déployé des cartes EMV a tout intérêt à déployer la solution CAP/DPA pour l'authentification aux services de banques en ligne plutôt qu'une solution alternative demandant de dupliquer l'infrastructure de sécurité et sa gestion.
- En déployant des lecteurs CAP/DPA en parallèle de la migration système vers 3D-Secure, une banque bénéficie de la sécurité carte à puce à la source (chez le consommateur) conforme aux recommandations des institutions, et peut réutiliser cette infrastructure de sécurité pour ses services de banque en ligne.

Au-delà des aspects technologiques, il est important de souligner que les solutions de sécurité RCA à base de cartes à puce EMV sont largement déployées en Europe (10M de consommateurs européens équipés d'ici fin 2007). Cette base installée et les retours d'expérience des banques démontrent leur acceptation par les utilisateurs. Concernant l'utilisation pour les services de banque en ligne (authentification forte pour l'accès au site, signature électronique des virements...), on constate que :

- Les utilisateurs perçoivent de manière très positive le fait que leur banque renforce la sécurité par une solution matérielle basée sur la carte bancaire, augmentant ainsi sa valeur d'usage.
- Les banques qui ont lancé des déploiements massifs (sur une base supérieure à 1M) constatent que les nouveaux utilisateurs s'approprient l'outil sans besoin d'assistance.
- Ces technologies permettent des solutions adaptées à des segments de clientèle spécifiques comme les malvoyants ou les personnes âgées (contrairement à d'autres solutions qui rendent les services inutilisables par les personnes aveugles).

Une des motivations des banques anglaises pour les déploiements en 2007 a été l'initiative « *Faster Payment* » dont l'objectif est de raccourcir le délai effectif d'un virement (de quelques jours à quelques heures), nécessitant un renforcement de la sécurité à la source. On retrouve le même besoin de sécurité pour un « Virement SEPA » ou une autorisation préalable à un « Prélèvement SEPA ». Les solutions décrites ici sont parfaitement compatibles avec ces opérations, renforçant encore leur pertinence dans le contexte actuel.

Au Royaume-Uni, les banques ayant massivement déployé en 2007 des solutions RCA pour la banque en ligne, font actuellement évoluer l'utilisation vers le e-commerce, reproduisant ainsi le mode de paiement de proximité dans un contexte distant. Ces banques confirment, sur le terrain, la complémentarité parfaite EMV + CAP/DPA + 3D-Secure et dispose déjà d'une infrastructure de sécurité pour le e-commerce.

## Références

- Technologie Remote Card Authentication : <http://www.remotecardauthentication.info>
- Visa Dynamic Passcode Authentication :  
<http://www.visaeurope.com/aboutvisa/products/dynamicpasscode.jsp>
- MasterCard CAP (programme OneSMART) :  
[https://mol.mastercard.net/mol/molbe/public/login/ebusiness/smart\\_cards/one\\_smart\\_card/biz\\_opportunity/cap/index.jsp](https://mol.mastercard.net/mol/molbe/public/login/ebusiness/smart_cards/one_smart_card/biz_opportunity/cap/index.jsp)

## A propos de XIRING

XIRING est un éditeur de solutions de sécurité pour les transactions à distance. La société propose des solutions logicielles embarquées sur lecteurs de cartes à puce pour l'authentification forte et la signature électronique. Ses solutions adressent aujourd'hui deux principaux marchés : la banque et la Santé. Créée en 1998, XIRING a réalisé en 2006 un chiffre d'affaires de 12.8 M€. XIRING est cotée sur le compartiment Alternext de NYSE-Euronext Paris depuis le 18/09/06. Code ISIN : FR0004155612, mnémonique ALXIR.

Pour plus d'information : [www.xiring.com](http://www.xiring.com).