



# Conférence CLUSIF PCI-DSS

L'externalisation : une échappatoire à PCI-DSS?

## Introduction en quelques chiffres

Fraudes à la carte bancaire en hausse de **9,8%\*** par an en France pour un montant de **342,5M€\*** en 2009

\* Rapport d'activité annuel 2009 de l'Observatoire de la sécurité des cartes de paiement publié en Juillet 2010

**9,8%**

**342,5M€**

Pour tenter de limiter ces fraudes, la norme PCI-DSS a été définie en **2006** par **5** sociétés émettrices de cartes

Une mise en conformité pouvant coûter plusieurs millions d'Euro...

**12 M€**

**6 M€**

La stratégie de mise en conformité gagnante...



... réduire le périmètre d'application de la norme

## Pour réduire le périmètre d'application de PCI-DSS : supprimer la donnée CB lorsque c'est possible

*Les endroits où il faut chercher la donnée CB...*

**Collecte des données de cartes bancaires**

*Site Web, Points de vente, Call Centre, TPE, SVI, ...*

**Lutte anti-fraude**

*Contrôles automatiques & manuels*

**Gestion des paiements**

*Demandes d'autorisation, remboursements, recouvrements, ...*

**Reporting**

*Résultats transactions, factures, ...*

**Bases de données clients**

*Information personnelle, clé de référence, programme de fidélité*

**Parmi ces activités** quelles sont les données dont à besoin l'entreprise ?



« On conserve les données des années... pour des raisons de fraude je suppose... enfin je crois »

## Pour réduire le périmètre d'application de PCI-DSS : désensibiliser la donnée CB 1/2

### La troncature / Le masquage

*Dédiée à une identification visuelle : page Web, frontal applicatif, factures, ...*

1234 5678 9012 3456 → 3456

1234 5678 9012 3456 → 1234 56\*\* \*\*\*\* 3456

### Le hash

*Dédié à un besoin de comparaison unique (ex: contrôles anti-fraude) ou sauvegarde dans les bases*

1234 5678 9012 3456 → ac814bbb4f38abeca3df6ab61f

## Pour réduire le périmètre d'application de PCI-DSS : désensibiliser la donnée CB 2/2

### La tokenisation

*Identifiant unique, non réversible, permettant de remplacer la donnée carte bancaire dans les systèmes*

1234 5678 9012 3456 → 1234 56Ab CDef 3456

#### Quelques points d'attention

- Taille du token
- Format du token
- Existence de digits

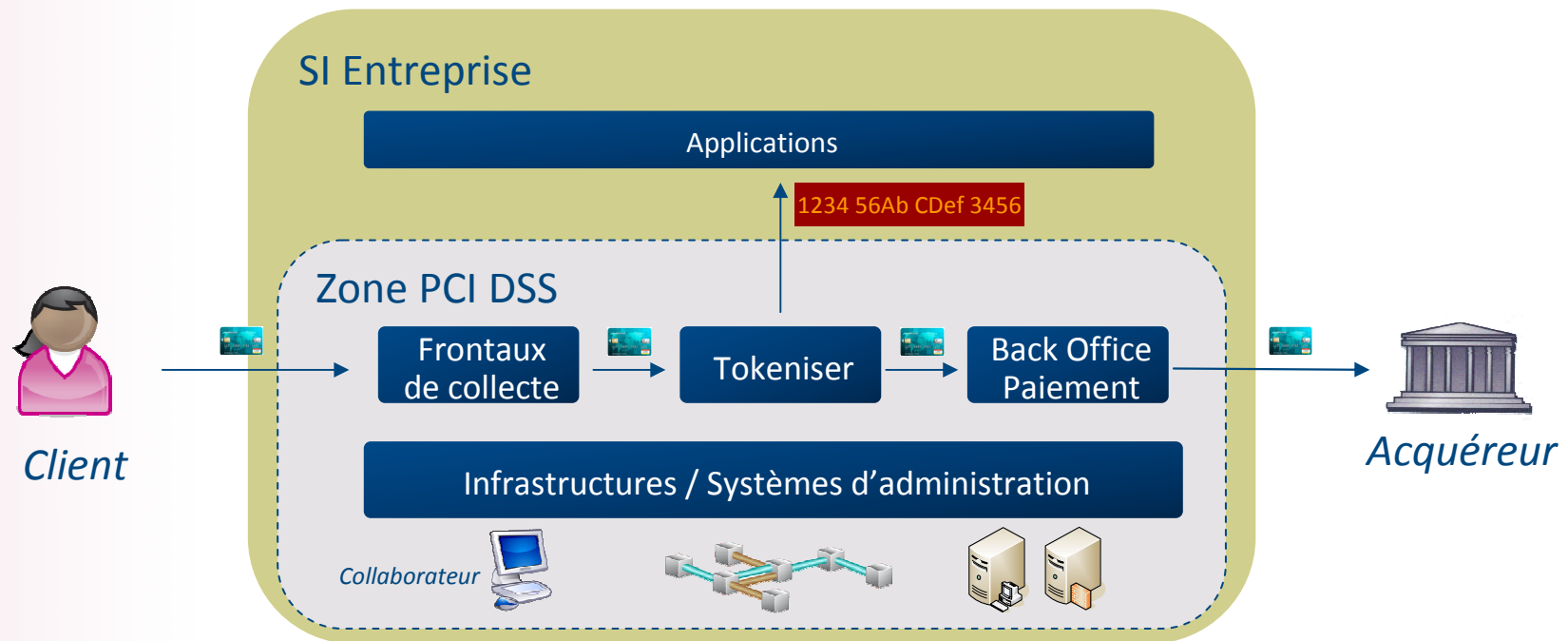


#### Solutions de tokenisation

- Marché actuel offrant des *solutions matures* conformes avec les exigences PCI DSS



Malgré la suppression et la désensibilisation des données bancaires, une zone PCI-DSS subsiste !



Suppression et désensibilisation des données CB



Des coûts de mise en conformité réduits mais qui peuvent  
toute fois s'avérer très importants

→ L'externalisation du paiement auprès d'un PSP peut-elle  
permettre de réduire ces coûts?

## A quoi sert un PSP ?

Les PSP (*Payment Service Provider*) proposent

- Externalisation complète de solutions de paiement,
  - Offres certifiées PCI DSS,
  - Offres standards et personnalisables, ...
- ... pour la réalisation de plusieurs centaines de millions de transactions par an



11 des 15 premiers\* sites de vente en ligne entièrement externalisés auprès d'un PSP (\*classement défini par la FEVAD)

## Fonctionnalités proposées par les PSP (1/2)

### Offres multicanal

- Sites Web et Call Centre par une redirection du client vers une **page web personnalisée**  
(Format navigateur, smartphone, tablette)
- **Serveur Vocal Interactif**
- Vente en magasin par **TPE**



### Multi moyens de paiement

- Carte bancaires
- Cartes privatives
- Offres de crédit
- ...



### Contrôles avancés de lutte anti-fraude

- Contrôles sur la carte
- Contrôles 3D Secure
- Scoring sur le profil du client



### Outil de tokenisation

- Format paramétrable
- Identifiant unique de la carte
- Communiqué à la demande d'autorisation

## Fonctionnalités proposées par les PSP (2/2)

### Connexions acquéreurs



Connexions à des centaines d'acquéreurs dans le monde pour réaliser

- Paiements à l'unité ou par lot
- Paiements récurrents
- Remboursements
- ...

### Gestion clients

- Fonction de « portefeuille client » pour l'enregistrement de carte
- Paiements « un click »

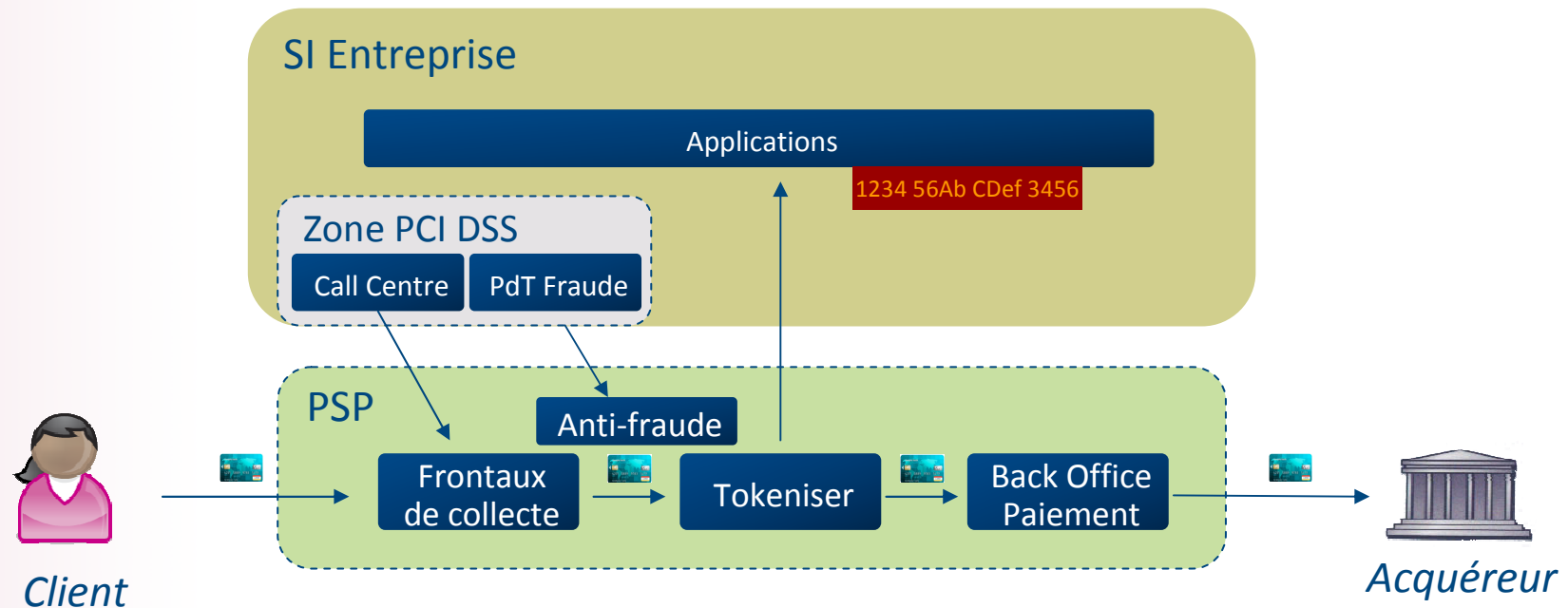
### Reporting

- Suivi des transactions
- Rapprochement bancaire
- Par fichier ou interface Web



Ensemble de fonctionnalités pour un coût unitaire récurrent à la transaction

Après externalisation, une zone PCI-DSS très réduite, mais toujours présente



Une externalisation qui nécessite tout de même certains coûts internes pour des modifications applicatives

## L'externalisation : une échappatoire à PCI-DSS?

- L'externalisation ne permet pas d'échapper à PCI-DSS...
  - C'est un facteur de réduction de périmètre PCI-DSS
  - Une zone interne PCI-DSS persiste généralement
- ... mais contribue à apporter de la valeur au-delà d'une mise en conformité PCI-DSS
  - Apport de nouvelles fonctionnalités (fraude, moyens de paiement...)
  - Harmonisation et simplification des processus de paiement

L'externalisation : une opportunité pour justifier les coûts PCI-DSS et impliquer la Direction Financière