



Sécurité des données cartes bancaires PCI DSS et le système CB

Thierry Autret
Groupement des Cartes Bancaires CB

Comment faire passer PCI DSS

Version américaine



Source : <http://www.youtube.com/watch?v=xpfCr4By71U>

Comment faire passer PCI DSS

Version française

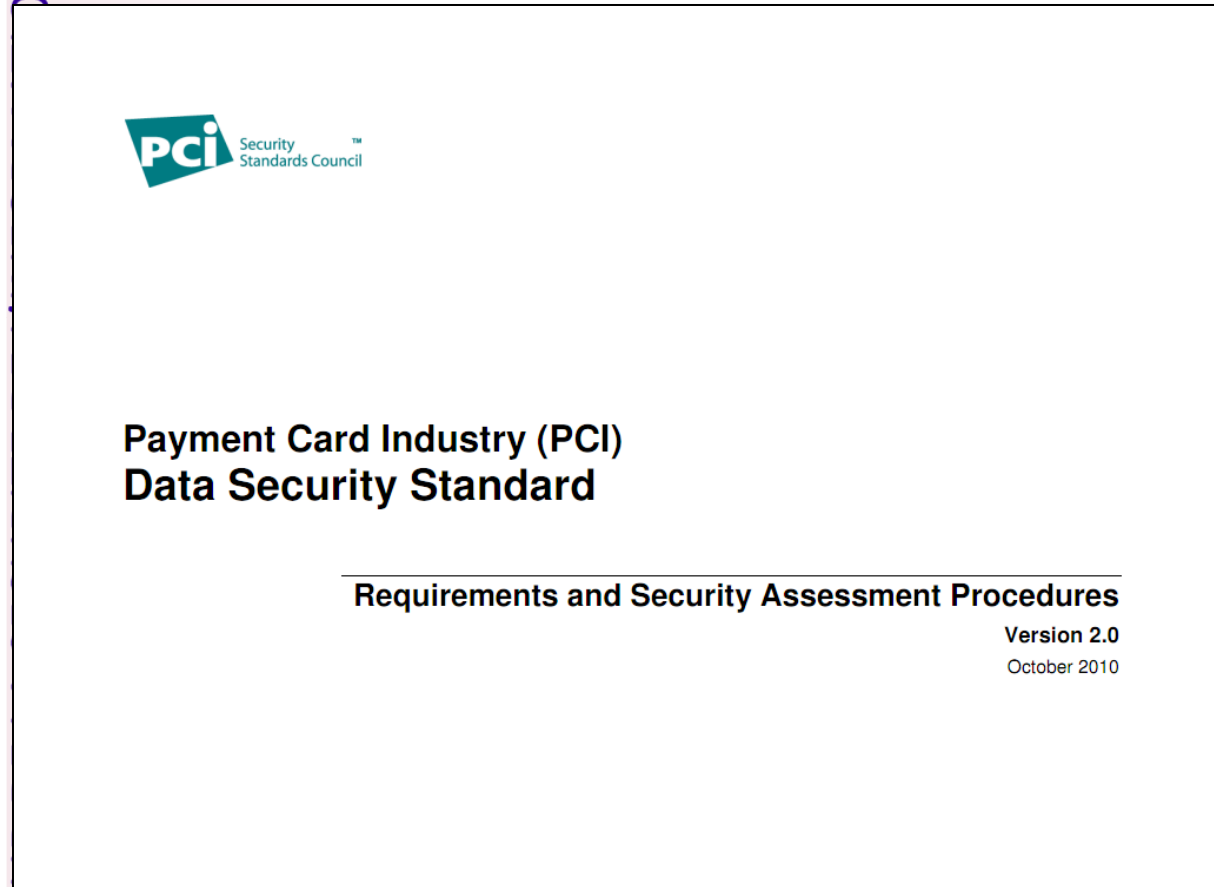


La Valse de PCI

Les illusions perdues ...



Le référentiel PCI DSS



- Dès 2004 ,VISA, Mastercard, Amex, Discover et JCB développent des programmes de « *sensibilisation* » à la protection des données cartes
- Début 2005, convergence vers le référentiel « *PCI DSS* »
- En 2006, création du PCI Standard Security Council, organisme de maintenance des standards de conformité PCI
- Version courante : 2.0
- Chaque système de paiement définit ses propres règles d'application du standard PCI DSS

Les données à protéger

<i>Cardholder Data includes:</i>	<i>Sensitive Authentication Data includes:</i>
<ul style="list-style-type: none"> Primary Account Number (PAN) Cardholder Name Expiration Date Service Code 	<ul style="list-style-type: none"> Full magnetic stripe data or equivalent on a chip CAV2/CVC2/CVV2/CID PINs/PIN blocks

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data ¹	Full Magnetic Stripe Data ²	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2



Un référentiel dérivé du standard ISO 27002

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes.
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security for all personnel.

Systeme "CB" : chiffres 2010

Le Groupement "CB" est le GIE de 130 membres

A fin 2010, nombre de :

- cartes "CB" : 59,771 Millions
- DAB "CB" : 56 243
- Contrats commerçants "CB" : 1 226 000

Activité sur l'année 2010:

- 7,063 milliards d'opérations de paiement (336 M€)
+ 1,509 milliard de retraits DAB (115 M€)

Loi Informatique & Libertés

L'article 34 de la Loi Informatique & Libertés dispose :

« Les responsables de traitement doivent prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès. »

Loi Informatique & Libertés

Le non respect des dispositions de la loi Informatique & Libertés est pénalement sanctionné.

Le responsable du traitement est l'Accepteur (commerçant): c'est lui qui risque d'être incriminé devant les juridictions pénales

CB n'est que l'une des... 625 'organisations participantes' de PCI SSC (dont 75% sont aux USA)



PCI-DSS et le système "CB"

La Communauté Bancaire et le Groupement des Cartes Bancaires "CB" **partagent les objectifs** du référentiel PCI-DSS, déclinaison appliquée à la monétique de la norme [ISO 27002](#).

La Communauté considère que les objectifs de sécurité définis par le référentiel PCI-DSS correspondent à l'état de l'art de ce que recommandent aujourd'hui les experts en sécurité des systèmes d'information pour sécuriser les bases de données, les échanges, pour protéger les contrôles d'accès,....

Type de communication "CB"

(site web)

Tous les acteurs responsables travaillent ensemble à protéger les données sensibles des cartes de paiement

La communauté bancaire et le Groupement CB partagent les objectifs du standard PCI-DSS, eux-mêmes déclinés à partir des standards ISO de sécurité des systèmes d'information, et visant un haut niveau de protection des données sensibles des cartes. La communauté considère que les objectifs de sécurité définis par le référentiel PCI DSS correspondent à l'état de l'art de ce que recommandent aujourd'hui les experts pour sécuriser les bases de données, les échanges d'informations, pour protéger les contrôles d'accès,....

Bientôt une FAQ dédiée

Un lien spécifique PCI DSS depuis la page d'accueil du site Web

Un accès rapide aux « QSA référencés CB »

Une page de foire aux questions

- PCI DSS s'applique-t-il à mon commerce ?
- Dois je faire l'objet d'un audit sur site ?
- Etc. etc.

Référencement "CB" de QSA

« A la demande de ses membres, le Groupement des Cartes Bancaires "CB" référence, sur une base volontaire et après analyse, des sociétés déjà accréditées QSA chez PCI SSC qui souhaitent réaliser des audits PCI DSS en France.

Le référencement "CB" garantit aux commerçants et aux acquéreurs "CB", l'existence d'une offre en langue française, adaptée au marché national ainsi que la confidentialité des données recueillies pendant ces audits. »

A ce jour 4 sociétés QSA sont référencées par le Groupement:

- Elitt, Provadys, Trustwave, Verizon Business
Les coordonnées des contacts sont sur notre site web

Les actions du Groupement

Règles contractuelles

- Mention explicite « PCI DSS » dans le contrat CB , article 3.14:
 - `L'accepteur doit respecter les exigences du référentiel de sécurité PCI DSS (à la demande de l'acquéreur, selon les volumes d'opérations cartes acceptées)

Systèmes d'échanges

- Mise à niveau des systèmes d'échanges `CB' en matière de transport d'informations `sensibles ` (Bulletin 10)

Problématique de l'externalisation

Mention explicite à la sous traitance dans les contrat d'acceptation "CB"

- Article 3.12 : L'accepteur "CB" doit s'assurer que les tiers tels que les prestataires de services techniques ou sous-traitants intervenant dans le traitement et le stockage des données liées à l'utilisation des cartes, respectent le référentiel de sécurité PCI DSS.

2011 – Le secteur du T & E

Cartographie des acteurs du secteur

- Agences de voyage
- Hôtels
- Loueurs de voitures
- Compagnies aériennes
- Offreurs de « packages »

Recensement des canaux de distribution

- Paiement de proximité
- E-commerce
- Centres d'appel (MOTO)

Analyse des risques liés à la sous traitance

Un monde complexe avec de multiples intervenants dans le secteur T&E

- Plusieurs niveaux de 'sous traitants en cascade'
- Localisation géographique
 - Hébergeur pays A, serveurs et applicatifs pays B, centres d'appel pays C,D,...)
- Type de contrats en place: quel(s) droit(s), clauses d'audit
- Type d'hébergement serveurs (mutualisé ou spécifique)
- Mode de développement des applications
- Niveau d'étanchéité application(s) de paiement
- Type de 'données cartes' échangées, et quelle sécurisation des échanges
- Stockage : modalités , durée, politique d'apurement,...

Problématique spécifique du cryptogramme visuel CVX2

Le CVX2 est obligatoire en e-commerce
(et seulement pour les paiements 'en une fois', non récurrents)

Interdiction systématique de stockage

Le CVX2 n'est pas impératif pour la VAD 'classique'

Extension 'VAD' sur un TPE agréé 'CB' : CVX2 non obligatoire
(et en tout état de cause, la transaction n'est pas garantie)

Recensement des procédures 'commerciales' en place-hors CB-
inutiles pour un paiement 'CB' et dangereuses:

- Photocopies cartes recto/verso, stockage de bons de commande 'papier',
- Archivage CVX2 pour le cas où le porteur ayant réservé ne se présente pas,
- Centres d'appels, etc.

Évolutions et études en cours

Identifiants CVX distincts selon le mode opératoire

- Principe : une donnée utilisée sur un mode d'acceptation ne peut être utilisée dans un autre mode pour éviter ce que l'EPC appelle la 'cross chanel contamination' (Ex:CVV1 magnétique /CVV2 imprimé/iCVV dans le chip EMV)
- Freins: exige une qualité/fiabilité des données échangées pas toujours effective globalement
- Conceptions différentes USA/Europe dans le secteur VAD: (aux USA ,un PAN seul suffit à générer une transaction et un émetteur est libre de répondre positivement à une demande d'autorisation avec CVV faux.....)

Évolutions et études en cours

Etude faisabilité gestion de 'PAN' multiples selon l'application

- Chip & PIN / sans contact / VAD / e-commerce

Étude pour la dématérialisation du ticket porteur

- Nécessite de générer un identifiant unique
 - Recours en cas de litige
 - Lié au E2EE

Chiffrement bout en bout

Chiffrement E2EE ou P2PE

- Les données chiffrées sortent du périmètre de certification PCI DSS, dès lors que l'entité qui stocke celles-ci ne possède pas la clé pour les déchiffrer
- x2xE facilite et diminue le coût de la conformité par la réduction du périmètre à certifier
- x2xE ne supprime pas les autres points de conformité à PCI DSS

Le PCI SSC publiera prochainement les exigences x2xE

.....Mais ce n'est pas sans impacts

Impact des solutions x2xE

Impératif d'interopérabilité : solutions multi-acquéreurs, multi-fournisseurs

En cohérence avec les référentiels à venir du PCI SSC

- Nécessité d'un niveau de protection très élevé pour les clés de chiffrement/authentification
- Exigences sur l'environnement de chiffrement : protection physique et logique (PTS)
- Gestion des clés, algorithmes
- Infrastructures de gestion des clés : quelle racine ? STCA ?
- Procédures de sauvegarde, distribution, expiration, révocation des clés
- Environnement (HSM) du système acquéreur banque, procédures d'accès, contrôles,...
- Impacts pour les back-offices bancaires : Impact pour acquéreur vis à vis de la fourniture d'un identifiant standardisé 'non sensible' de la transaction (besoins de back office commerçant)

Le CLUSIF et PCI DSS

Création en 2008 d'un groupe de travail PCI DSS au sein du CLUSIF, animé par Rodolphe Simonetti

- Première production en novembre 2009: « PCI DSS: une présentation »
- Deuxième production en décembre 2010 « Brève info sur la version 2.0 »
- Travail en cours: un document plus opérationnel sur la mise en œuvre des exigences