Contraintes réglementaires

PCI DSS

En France, début 2009, les acteurs bancaires ont clairement annoncé leur soutien au standard PCI DSS, tel cet extrait du site Web du Groupement des Cartes Bancaires « CB » :

> *« …La communauté bancaire française et le Groupement Cartes Bancaires CB partagent les objectifs du standard PCI DSS, eux-mêmes déclinés à partir des standards ISO 27001 de sécurité des systèmes d'information, en 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, »… « Depuis plusieurs années, tous les acteurs concernés ont lancé des programmes de sécurisation de ces données sensibles ; à ce jour, de nombreux commerçants et prestataires de services ont déjà terminé ou sont sur le point de finaliser leur mise en conformité PCI DSS. »*

Visa, MasterCard, American Express, Discover et JCB ont fondé en 2006 le Payment Card Industry Security Standards Council (PCI SSC) avec pour objectif de définir un référentiel de sécurisation des données carte bancaires s'appuyant sur des bonnes pratiques : PCI DSS. Ce référentiel s'applique à toute entité qui traite et/ou stocke de la donnée carte.

PCI DSS

CardSystems Solutions Inc (Fournisseur de service de paiements)
Une faille de sécurité a entraîné la compromission de 40 millions de cartes en 2005, cette société a fait faillite depuis.

http://www.ftc.gov/opa/2006/02/cardsystems_r.shtm

TJX : Groupe de distribution (commerce) présent aux Etats-Unis et en Europe.
Une faille concernant un réseau sans fil aurait conduit à la compromission de 45,6 millions de numéros de cartes en 2006.

http://www.securityfocus.com/news/11455

Royal Bank of Scotland WorldPay Inc. : activité fournisseur de services de paiement aux Etats-Unis de la banque anglaise RBS.
Une fraude concernant potentiellement 1,5 million de numéros de cartes a été identifiée en 2008.

http://www.rbslynk.com/RBS_WorldPay_Press_Release_Dec_23.pdf

Heartland Payment Systems Inc. (Fournisseur de service de paiements).
De multiples systèmes d'écoutes ont été trouvés sur les systèmes de la société Heartland en 2008, compromettant ainsi environ 130 millions de cartes.

http://www.2008breach.com

Données porteur

Les données porteur correspondent aux données liées au porteur de la carte de paiement qui sont fournies au commerçant ou récupérées par le commerçant lors d'une transaction de paiement.

Celles-ci sont constituées des informations suivantes :

- Données des porteurs de carte devant faire l'objet d'une protection :
  1. Numéro de compte primaire (PAN, Primary Account Number) ;
  2. Nom du titulaire de la carte de crédit ;
  3. Code de service ;
  4. Date d'expiration.
- Données d'authentification sensibles dont le stockage est interdit après l'autorisation de la transaction :
  5. Données de bandes magnétiques complètes ou leur équivalent stocké sur la puce ;

  6. Le code CAV2/CVC2/CVV2/CID (appelé également cryptogramme visuel): code à 3 chiffres au dos de la carte utilisée pour les transactions à distance, type Internet (le nom diffère selon la marque de la carte) ;
  7. Bloc PIN (qui est une version chiffrée du code PIN).

Données porteur

Les données porteur sont sensibles pour plusieurs raisons :

- Elles peuvent permettre de passer des transactions de paiement (numéro, nom du porteur, date de validité, CVV2, PIN), et donc entraîner des fraudes. Parfois un simple PAN permet de réaliser une transaction ;
- Elles peuvent permettre d'identifier le porteur (nom du porteur, numéro de carte) et sont donc considérées comme des informations indirectement nominatives par la CNIL ;
- Le numéro de carte est parfois utilisé comme identifiant dans des applications, ce qui peut permettre de faire le lien avec des personnes ;
- Elles peuvent permettre de récolter des informations sur les cartes de paiement (type de transactions autorisées, pays émetteur, etc.) et donc de cibler des utilisations malveillantes.

Il est important d'avoir à l'esprit que ces données n'appartiennent ni au porteur ni au commerçant, mais à l'émetteur de la carte conformément au contrat porteur.

PCI Security Standards Council

En 2006, Visa, MasterCard, American Express, Discover et JCB ont fondé le Payment Card Industry Security Standards Council (PCI SSC) afin de maintenir des référentiels communs tels que les référentiels d'exigences des programmes PCI DSS, PCI PA-DSS et PCI PED.

PCI SSC Founders

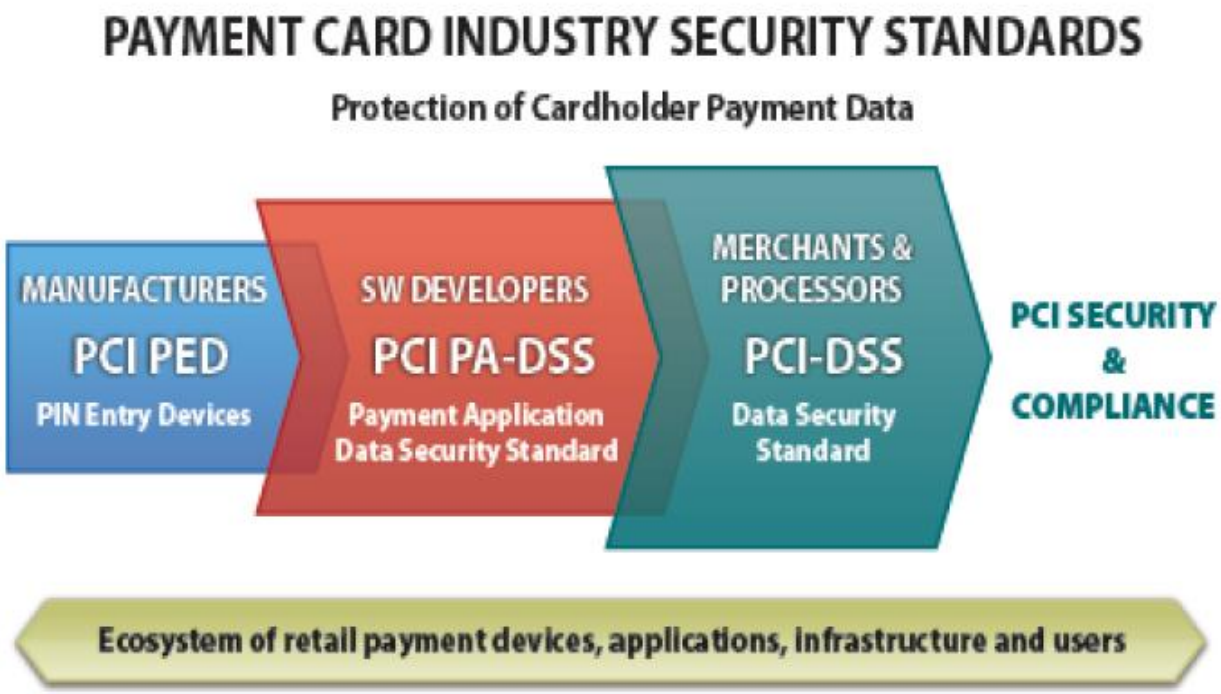
AMERICAN EXPRESS

DISCOVER NETWORK

JCB

MasterCard Worldwide

VISA



Périmètre PCI DSS

Pour les entreprises soumises au standard PCI DSS, le périmètre d'application inclut tous les composants réseaux, systèmes et applicatifs qui traitent, stockent ou supportent les données des porteurs de carte ainsi que les éléments connectés à ceux-ci.

De ce fait, les éléments suivants sont impactés :

- Tous les systèmes, les serveurs, les applications ou les composants réseaux inclus dans, ou reliés à l'environnement de données de détenteurs de carte :
    - Les composants réseau, notamment les firewalls, les commutateurs, les routeurs, les points d'accès sans fil, les équipements de réseau, et les autres équipements de sécurité ;
    - Les serveurs, notamment les serveurs Web, de bases de données, d'authentification, de DNS, de courrier, et de synchronisation horaire (NTP) ;
    - Les applications, que ce soit les applications développées en interne ou les progiciels, qu'elles soient accessibles en interne ou externe.
- Tous les utilisateurs et postes utilisateurs accédant à ces composants, que ce soit pour des besoins métiers ou informatiques, depuis les points de vente, les datacenter ou des bureaux ;
- Tous les raccordements à l'environnement des données de porteur de carte, par exemple : accès à distance des employés, passerelles de paiement, banques, entreprises de cartes de paiement, centres d'appels, accès de tiers pour traitement, et tierce maintenance.

Ce dernier point fait apparaître la notion d'entreprises externes (type fournisseurs, partenaires, mainteneurs réseau/système/applicatif…) qui peuvent accéder logiquement ou physiquement à l'environnement des données des porteurs de cartes et peuvent donc éventuellement en affecter la sécurité en accédant par exemple à des numéros de cartes. Si ces entreprises ne respectaient pas les règles de sécurité demandées par le standard, elles pourraient constituer un maillon faible. Ces entreprises sont donc incluses dans le périmètre PCI DSS sous la notion de « Fournisseurs de Services » décrite plus loin.

12 séries de clauses PCI DSS

Création et gestion d'un réseau sécurisé
1. Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes. 2. Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur.
Protection des données des titulaires de cartes de crédit
3. Protéger les données des titulaires de cartes stockées. 4. Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts.
Mise à jour d'un programme de gestion des vulnérabilités
5. Utiliser des logiciels antivirus et les mettre à jour régulièrement. 6. Développer et gérer des systèmes et des applications sécurisés.
Mise en oeuvre de mesures de contrôle d'accès strictes
7. Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître. 8. Affecter un ID unique à chaque utilisateur d'ordinateur. 9. Restreindre l'accès physique aux données des titulaires de cartes.
Surveillance et test réguliers des réseaux
10. Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes. 11. Tester régulièrement les processus et les systèmes de sécurité.
Gestion d'une politique de sécurité des informations
12. Gérer une politique qui assure la sécurité des informations des employés et des sous-traitants.