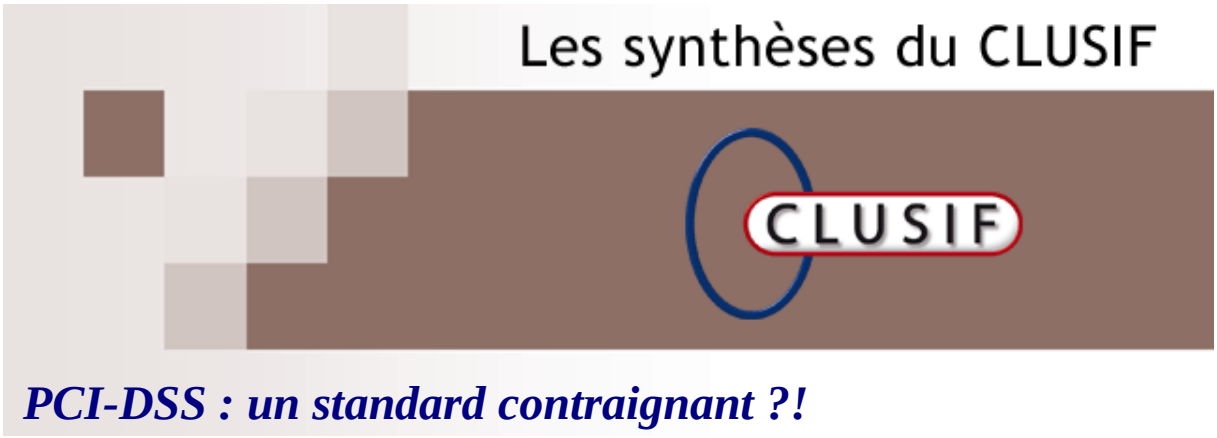

PCI-DSS : un standard contraignant ?!

Synthèse de la conférence thématique du CLUSIF du 7 avril 2011 à Paris

Devant l'augmentation des fraudes et des incidents liés à la carte bancaire, les cinq grands émetteurs de cartes bancaires ont souhaité réunir les exigences de sécurité qui devront être respectées par les différentes parties qui manipulent, stockent, traitent ou conservent des informations liées à la carte bancaire. Or, mettre en place les exigences du standard est difficile et coûteux. La question posée aujourd'hui est donc « PCI DSS, un standard contraignant !? ».

Thierry Autret, Groupement des cartes bancaires

Thierry Autret rappelle que PCI a presque 7 ans. Les premières initiatives de Visa avec AIS et de Masterd Card avec les programmes SDP ont été les prémices de ce qui est devenu en 2005 le standard commun : PCI DSS (Payment Card Industry Data Security Standards). La responsabilité du maintien et des évolutions du standard est assurée par le PCI SSC (PCI Security Standards Council).

Il différencie, parmi les données « carte », celles qui sont sensibles des autres en précisant que les sensibles ne doivent en aucun cas être stockées sur les systèmes d'information. Plus particulièrement le PAN et la date de fin de validité doivent faire l'objet d'une protection particulière.

Les 12 exigences sont un dérivé du référentiel ISO 27002 à quelques différences près.

Au-delà du respect des exigences du standard, la législation française s'impose à tout organisme qui manipule des données de la carte bancaire (ex : la loi informatique et liberté et la perte ou divulgations des données nominatives).

Le GIE CB représente les établissements de paiement et de crédit. Il est l'une des 625 organisations participantes au PCI SSC (dont 75 % sont américaines). Cette situation limite actuellement son influence au sein de cette organisation. Afin de remédier à cette situation, le GIE a posé sa candidature en tant qu' « advisor » (*membre du bureau*).

Les membres du GIE ont demandé un référencement des QSA par le PCI SSC. Les auditeurs étaient quasi exclusivement d'origine anglo-saxonne et les membres du GIE ont souhaité que les auditeurs en charge des évaluations soient de langue française et possède une réelle connaissance de la monétique française. A ce jour 4 QSA sont référencés par le GIE carte bancaire (Elitt, Provadys, Trustwave et Verizon Business). D'autres structures en France ont la qualité de QSA mais n'ont pas demandé à être référencées.

Le groupement travaille activement sur la lisibilité du standard PCI et les conditions de sa mise en œuvre :

- dans la relation des établissements avec les commerçants, il a été demandé de rajouter une mention explicite dans le contrat CB du respect du référentiel PCI DSS.
- Au niveau des systèmes d'échanges Les numéros de carte dès lors qu'elles ne servent plus doivent être supprimés.
- Les comités de direction du groupement votent des « bulletins » qui sont des exigences destinées à faire évoluer soit les protocoles soit les applications sur les terminaux de paiement ou distributeurs. Le « bulletin 10 » par exemple a fait évoluer le masquage de la zone discrétionnaire.
- Le bulletin du 13 d'avril 2010 définit l'affichage du numéro de carte sur le ticket porteur, celui du commerçant. Aujourd'hui il est obligatoire de garder le numéro complet sur ce ticket puisqu'il permet au commerçant d'avoir une preuve en cas de litige. L'objectif est de faire disparaître ce ticket commerçant, disparition sans doute liée au « End-to-End Encryption ».

Concernant l'externalisation, une mention dans le contrat commerçant dit que l'accepteur (c'est le commerçant) doit s'assurer que les tiers tels que les prestataires de services techniques ou sous traitants intervenant dans le traitement ou le stockage des données respectent le référentiel PCI DSS. En 2011, le GIE a décidé de se focaliser sur le secteur du T&E (agences de voyages, hôtels, loueurs de voiture, compagnies aériennes…). Il s'agit d'un secteur d'activité où les nombreux prestataires de services travaillent souvent en cascade et dans des pays différents avec leurs contrats propres.

Le CVX2 (ou cryptogramme visuel). Cette donnée, largement en vigueur dans le e-commerce, est parfois utilisée de façon dangereuse voire illicite (photocopie recto-verso de la CB, fourniture par téléphone,..). Des évolutions sont en cours qui devraient permettre d'avoir des CVX différents selon le canal, ou d'avoir des I CVV dans la puce

Une autre approche est d'utiliser des PAN multiples selon les types d'application. Avoir un PAN pour le chip & PIN, un PAN pour le sans contact, un PAN pour la VAD ou le E-commerce. Cette évolution permettrait d'éviter le cumul des types de fraude en empêchant une même donnée, obtenue frauduleusement, d'être utilisée sur plusieurs canaux.

Le groupement carte bancaire est également très actif sur la réduction du périmètre. Un nouveau système de protection des clés de chiffrement va être introduit avec le « End-to-End Encryption ». Le problème de sécurité va être déporté vers les clés, couvert par la partie PTS de PCI. Il sera nécessaire de mettre en place de la cryptographie asymétrique et désigner les autorités de certification en charge de vérifier l'authenticité des clés. Thierry Autret souligne que depuis 2005, avant l'arrivée de PCI DSS, les terminalistes ont l'obligation de chiffrer via SSL les échanges. Le GIE a mis en place une autorité de certification avec les constructeurs et les systèmes d'acquisition au sein d'une infrastructure qui s'appelle STCA (Secure Transactions Certification Authority) qui permet de certifier les clés qui sont dans les terminaux. Ce système pourrait être utilisé dans le cadre de « End-to-End Encryption ».

La mise en œuvre sera délicate pour les commerçants qui sont « multi-acquéreurs ». En effet les systèmes « End-to-End Encryption » fonctionneront-ils avec plusieurs banques ou constructeurs et ceci en dépit des solutions techniques que pourront mettre au point les spécialistes.

Un groupe de travail du Clusif, animé par Rodolphe Simonetti, a produit sur le thème « PCI DSS » plusieurs documents :

- « PCI DSS une présentation » qui a connu un vif succès.
- Un deuxième document est sorti l'année dernière à l'occasion de la version 2 de PCI DSS pour expliquer quelles étaient les différences avec la première version.

Le groupe travaille actuellement sur un troisième document. Il s'adressera plus particulièrement aux entités en charge d'implémenter le standard. Il devrait apporter une meilleure compréhension des exigences et des concepts tels que la tokénisation, le End-to-End Encryption, la réduction du périmètre.

Sébastien Mazas, Verizon Business

Sébastien Mazas insiste, dès l'introduction de son intervention, sur l'importance de la relation qui existe entre les différents acteurs et le PCI SSC.

Les banques et les PSP (fournisseurs de services de paiements) sont en relation directe et de type contractuel avec les réseaux.

Les marchands sont en relation directe avec leur banque. Cette dernière définit le niveau de la conformité à PCI DSS, qu'on appelle le niveau de marchand, et est également responsable du maintien, dans le temps, de cette conformité. La conformité représente une contrainte et un coût pour les marchands.

Les autres acteurs (Hébergeurs, fournisseurs d'applications ou de matériels,…) qui interviennent dans les paiements d'une manière directe ou indirecte sont aussi concernés. Ils n'ont pas nécessairement une relation contractuelle mais connaissent une pression commerciale pour prendre en compte PCI DSS dans leur activité et être certifiés ou non.

Sébastien Mazas décrit la mise en conformité, pour les marchands, comme :

- Une obligation compte tenu du contrat qui les lie à leur banque ;
- Un levier pour obtenir des budgets et se faire se rapprocher les équipes IT et métiers.

Toutefois il différencie conformité et sécurité. Un audit est avant tout l'évaluation d'une conformité par rapport à un standard. L'audit ne juge pas la sécurité, il évalue la conformité de l'infrastructure par rapport à des règles qui ont été édictées par les réseaux

PCI DSS cible plus précisément certains acteurs sur le marché :

- Le e-commerce est aujourd'hui le domaine le plus sensible en termes de paiement ; c'est aussi un domaine d'activité assez nouveau et pour lequel la sécurité IT est assez bien développée.
- L'hôtellerie en raison des conditions de gestion des réservations.
- Les sociétés des autoroutes qui ont des contraintes spécifiques en raison du très grand nombre de transactions de faibles montants qu'elles gèrent quotidiennement.

L'exercice a donné lieu à un regroupement de l'ensemble des acteurs que sont les autoroutes, les équipementiers, les réseaux et les banques, pour trouver une solution qui soit viable et qui réponde aux exigences de PCI DSS.

De nombreuses structures de marchands coexistent et certaines ont des organisations complexes : franchises, filiales ou multi-acquéreurs. Elles rendent parfois complexe la question de la conformité à PCI DSS. Le QSA les aide alors, dans leur relation avec les banques, à identifier qui doit faire quoi pour répondre à cette problématique.

Les PSP (Payment Service Provider) sont aussi des acteurs fondamentaux. Il est aujourd'hui interdit de contractualiser avec un PSP s'il n'est pas certifié PCI DSS.

Les PSP rencontrent, dans leur mise en conformité, plusieurs difficultés :

- Diversité des services offerts.
- Les systèmes mis en œuvre sont fractionnés et posent un problème à la vision globale qu'impose le standard.
- Un nombre importants de transactions.
- Les architectures sont souvent complexes et doivent répondre à des exigences importantes de disponibilité et de temps de réponse.

Les banques n'ont pas d'obligation de certification mais une obligation morale de conformité. Toutefois la Banque de France impose aux banques des vérifications sur ce sujet. Le PCI Council ne leur imposant rien directement, certaines banques ont analysé leurs écarts avec les exigences de PCI DSS et d'autres ont mis en place des grands plans de conformité pour lesquels elles sont accompagnées par des QSA.

La contrainte principale des banques est la présence du numéro de carte bancaire comme donnée de référence dans la quasi-totalité des applications métier. De fait, le périmètre d'application du standard est important. Enfin les systèmes d'informations sont souvent constitués de matériels et de systèmes anciens : Mainframe, systèmes à haute disponibilité, vieux langages de programmation (Cobol).

Les banques ont intégré la sécurité dans leur processus depuis longtemps mais les QSA peuvent les aider à appliquer ce standard récent dans le domaine de l'IT.

De nombreux acteurs interviennent dans la gestion de la carte bancaire, depuis la supervision jusqu'à l'archivage. Les exigences formulées dans le chapitre 12.8 qui décrivent la relation contractuelle entre les différents acteurs qui manipulent les données de la carte bancaire prennent toute leur importance dans ce domaine où le phénomène de cascade rend le transfert des responsabilités délicat. Ces entités n'ont pas l'obligation de certification mais c'est un argument commercial dont elles peuvent avoir besoin.

L'audit porte sur le respect de 280 exigences, se déclinant en environ 900 points de contrôle. Il suffit qu'un seul ne soit pas conforme pour ne pas être certifié.

Sébastien Mazas insiste sur le point suivant : le QSA est en charge de l'évaluation, c'est le réseau qui certifie. Le rôle du QSA est de faire le lien entre la réalité du métier et les exigences des réseaux. Il est également le meilleur avocat pour défendre son client auprès de son réseau s'il s'agit d'un PSP, ou auprès de sa banque s'il s'agit d'un marchand. Si le QSA, par exemple, accepte une mesure compensatoire, c'est lui qui doit la défendre auprès du destinataire du rapport.

Pour bien choisir son QSA il faut opter pour un accompagnement depuis l'initialisation du projet jusqu'à l'audit de conformité. PCI DSS autorise le QSA qui accompagne un client d'assurer aussi l'audit d'évaluation. Le rôle du QSA va être fondamental lors de la validation de la réduction du périmètre même si celle-ci n'est pas nécessairement la meilleure solution. Selon Sébastien Mazas, le QSA va « démystifier » PCI DSS en prenant les exigences les unes après les autres et en montrant au client que bien souvent il fait déjà naturellement 90 % de ce qui est demandé. La partie la plus importante va consister à formaliser les processus existants.

Le QSA, de par son expérience, aide son client à travailler sur sa stratégie de mise en conformité. Il peut d'ailleurs conseiller à son client d'évaluer sa conformité et de se mettre aux normes sans forcément aller jusqu'à la certification.

Matthieu Garin, Solucom.

Mathieu Garin pose la question de l'externalisation comme stratégie de mise en conformité à PCI DSS.

Il rappelle que c'est l'augmentation des fraudes qui a motivé les sociétés de carte bancaire à créer PCI DSS. Le standard existant depuis 2006, les coûts d'une mise en conformité commencent à être connus. Les chiffres annoncés vont de 6 à 15 millions d'euros. Une mise en conformité PCI DSS est donc un projet ambitieux. Se pose alors la question du périmètre d'application du standard. La définition communément acceptée est de dire que PCI DSS s'applique à tous les composants qui manipulent ou qui permettent l'accès aux données bancaires.

C'est ce « permettent l'accès » que Mathieu Garin détaille :

- Tous les composants manipulant ou stockant des données CB en clair (systèmes, applications, DB…)
- Les environnements manipulant des données CB qui sont autour de ces systèmes sans aucun filtrage réseau
- Et enfin, tous les environnements qui assurent la sécurité du contrôle d'accès sur les systèmes bancaires,

C'est sur ce périmètre là qu'il faut travailler. La stratégie gagnante est de réduire le périmètre d'application.

- Réduire le périmètre d'application consiste à supprimer la donnée carte bancaire partout où c'est possible.
- C'est impossible sur les applications qui la collectent (sites web, points de vente, centres d'appel, TPE…).
- C'est impossible également sur les systèmes anti-fraudes et les systèmes de gestion des paiements (demandes d'autorisation, remboursements, recouvrements qui nécessitent des envois de numéros de carte bancaire).

En revanche, les marges de réduction sont plus importantes sur les systèmes de reporting et les bases de données clients (informations personnelles, programme de fidélité).

La première étape consiste à supprimer la donnée carte partout où elle n'est pas absolument nécessaire.

Une deuxième solution pour réduire le périmètre est de désensibiliser la donnée carte bancaire (troncature ou masquage de la donnée).

Cette opération permet de sortir ces applications du périmètre. Les systèmes environnants dans lesquels il n'y a pas de filtrage réseau et tous les systèmes qui permettent d'accéder à ce système, seront également retirés.

Pour les besoins de comparaison unique comme les contrôles anti-fraude, une deuxième technique, le hash, évite de travailler avec des numéros de carte bancaire.

Une troisième solution pour réduire le périmètre est la tokénisation qui permet de remplacer la donnée carte bancaire par une donnée qui est un jeton.

Au lieu de travailler avec des numéros de carte bancaire le back office travaille avec des jetons qui permettent de retirer l'application du périmètre PCI DSS. Toutefois, le tokeniser, l'outil qui permet de faire la traduction entre le numéro de carte bancaire et le jeton, reste dans le périmètre PCI DSS.

Une fois le périmètre réduit, trois types d'applications, ainsi que leurs infrastructures sous-jacentes, restent dans le périmètre PCI DSS : les frontaux de collecte, le tokeniser et le back office de paiement. Les chiffres annoncés par Mathieu Garin au début de son intervention s'appliquent le plus souvent sur un périmètre réduit proche de celui-ci. Pour réduire encore ces montants conséquents se pose la question de l'externalisation.

Une première approche est l'externalisation de l'infrastructure du périmètre résiduel tout en gardant les applications.

C'est un marché jeune et des hébergeurs commencent à fournir des offres certifiées PCI DSS. Elles peuvent être intéressantes mais il faut veiller aux exigences qui vont s'appliquer sur le périmètre dont on garde la responsabilité en fonction du degré d'externalisation.

La seconde approche c'est l'externalisation des trois applications résiduelles chez des PSP (Payment Service Providers). Il s'agit d'acteurs historiques dont les offres sont déjà pour le plus grand nombre certifiées et largement sollicitées par les plus grandes entreprises ainsi que les sites de ventes en ligne.

Les PSP proposent des solutions qui :

- couvrent la totalité des besoins attendus dans le traitement des données carte bancaire et du commerce en ligne ;
- assurent la relation avec les différents acquéreurs

L'externalisation auprès d'un PSP permet rarement de s'affranchir complètement de PCI DSS parce qu'il reste toujours des systèmes qui doivent manipuler des cartes bancaires :

- l'offre call center des PSP,
- des postes de travail sur les services anti-fraudes qui ont besoin des numéros de cartes bancaires
- certaines multinationales ont des agences dans le monde dans lesquelles des téléconseillers continuent de rentrer directement le numéro de carte des clients dans le système.

L'externalisation n'est pas une échappatoire à PCI DSS mais c'est un facteur de réduction de périmètre PCI DSS complémentaire à toutes les autres solutions de réduction de périmètre évoquées.

Laurent Beaussart, directeur adjoint des systèmes opérationnels et RSSI de Cofiroute,

Laurent Beaussart présente la démarche mise au point par l'ASFA (Association des sociétés françaises d'autoroute et d'ouvrages à péages) pour la mise en conformité PCI DSS.

Les spécificités du métier de gestionnaire des autoroutes ont un impact fort quant au respect des exigences du standard :

- **le nombre de transactions** : 1,3 milliards de transactions tous modes de paiement confondus dont 500 millions de transactions par carte bancaire.
- **Le montant moyen** est faible, 6 euros en moyenne.
- **La disponibilité des équipements.** Les paiements doivent se faire rapidement pour éviter l'attente. l'exploitation doit fonctionner 24/24 h, 365 jours par an. Les lecteurs de carte doivent supporter des cadences très élevées, ils sont multi épaisseurs pour s'adapter aux différents formats de carte et ils doivent subir des contraintes climatiques fortes.
- **Les réseaux sont maillés** entre les différents concessionnaires
- **Le parc matériel** de plus de 4000 lecteurs n'est pas suffisamment important pour négocier avec les fabricants la mise en place de normes spécifiques.

Cofiroute, comme les autres concessionnaires, est exposé, dans gestion de la donnée carte bancaire, à plusieurs menaces :

- **la compromission** de numéros de cartes bancaires, aggravée par le nombre de cartes bancaires qui circulent dans ses réseaux.
- **la fraude.** Des systèmes d'autorisation en ligne ont été mis en place dès 2005 ainsi que des listes d'exclusion.

- **la radiation du système carte** bancaire en cas de non-conformité notamment par rapport aux règles PCI DSS.
- **les risques financiers** liés aux pertes de recette, aux refus de compensation ou aux amendes en cas de non respect de PCI DSS.
- **Enfin, le risque en termes d'images** lié au statut de société publique que tout le monde connaît**.**

Le projet PCI DSS a démarré en juillet 2006, dès la sortie du standard. Le comité monétique de l'ASFA a coordonné les projets des différentes sociétés d'autoroute. Ce front uni a permis de présenter un plan d'action à l'acquéreur, en l'occurrence le Crédit Mutuel, avec un poids plus important.

A partir de 2008, l'ASFA s'est faite accompagner par Verizon Buisness qui a effectué un certain nombre de travaux dont les audits d'écarts mais également la présentation synthétique de l'avancement de la démarche entre les différentes sociétés à l'acquéreur et aux différents émetteurs de cartes.

Pour répondre à la fois à des préoccupations de sécurité et aux conditions très particulières de règlement par les usagers du péage un standard spécifique de payement pour automate sur autoroute a été élaboré par l'ASFA et validé par le GIE CB.

Cofiroute a conduit en parallèle plusieurs chantiers impactant la donnée carte bancaire et par conséquent le respect des exigences du standard PCI DSS.

L'analyse d'écart menée en 2009 sur les 12 exigences du standard PCI DSS a permis de constater que le périmètre PCI DSS était trop vaste et impliquait un faible niveau d'implémentation des exigences du standard. Par ailleurs, les processus déjà en place n'étaient pas suffisamment formalisés. Pour être conforme il faut documenter la conformité et c'est un travail important souvent négligé.

Laurent Beaussart résume les trois solutions envisagées et non retenues pour la mise en conformité :

- **Le chiffrement** qui nécessite de protéger les clés et de mettre en place une infrastructure contraignante compte tenu du périmètre.
- Verizon a également proposé la solution **du hachage** mais en suggérant de saler le hash (mais si on sale le hash se pose la question de savoir comment on protège le sel).
- **la troncature** qui consiste à ne garder qu'une partie des informations.

Les besoins de Cofiroute sont les suivants :

- **La remise en banque** des transactions bancaires qui nécessitent un déchiffrement de la donnée pour compensation.
- **Les traitements métiers** ont une uniquement besoin d'un identifiant porteur unique et de données carte publiques (Code BIN),

Le choix pour la mise en œuvre de PCI DSS s'est donc porté sur la séparation des flux. Une architecture a été élaborée et mise en œuvre. Elle est constituée par :

- **un silo PCI DSS.** Il permet de conserver la donnée bancaire de façon complètement protégée.
- **Un lecteur de cartes dans un environnement protégé,** qui dialogue avec un serveur monétique de façon sécurisée via un protocole sécurisé qui lui-même va se charger de dialoguer avec la banque et de remettre la transaction dans un format CB2A.
- Concernant la partie transactionnelle, seuls **un numéro tronqué et un ID technique** remontent au back office. Ensuite l'information est tokenisée par rapprochement avec le serveur monétique et c'est le numéro de token qui est conservé dans les transactions et permettre de faire de la réconciliation bancaire, des statistiques ou répondre à des réquisitions.

Pour répondre au besoin documentaire de PCI DSS, Cofiroute a choisi de mettre en place depuis très longtemps un système de management de la sécurité et de l'information basé sur la norme 27001. Il constate que PCI DSS est un sous ensemble du périmètre global.

Questions et Réponses avec l'assistance.

Cette conférence comportait également un débat avec la salle, non retranscrit dans ce document mais disponible en vidéo à l'adresse suivante : https://www.clusif.asso.fr/fr/production/videos/#video110407.

Retrouvez les vidéos de cette conférence et les supports des interventions sur le web CLUSIF
https://www.clusif.asso.fr/fr/infos/event/#conf110407.