Industrie des cartes de paiement (PCI)

Norme de sécurité des données

Condition d'application de la norme PCI DSS dans un environnement EMV

Document de directives

Version 1.0

Publication : 14 septembre 2010

Table des matières

1 Résumé

Ce document compare les capacités de réduction de la fraude actuelles des EMV dans le cadre de la Norme de sécurité de l'industrie des cartes de paiement (PCI DSS) (PCI DSS) et examine les raisons pour lesquelles il reste nécessaire de mettre en œuvre la norme PCI DSS dans les environnements EMV qui existent aujourd'hui.

1.1 Le rôle de l'EMV

Les cartes à puces EMV ont été conçues et introduites pour réduire la fraude survenant dans le contexte d'utilisation des bandes magnétiques en personne, à l'aide de cartes à circuit intégré (CI) qui utilisent des clés cryptographiques secrètes pour générer des données d'identification et d'autorisation. En tant que telles, l'application robuste des spécifications de la norme EMV peut atténuer le risque de compromettre les données de cartes utilisées pour commettre une fraude lors d'une transaction individuelle. La mise en application de l'EMV qui utilise des valeurs de vérification de carte conservées dans la puce, différentes de celles conservées sur l'image d'une bande magnétique, constitue une barrière efficace contre la création de contrefaçons de cartes à bande magnétique à partir de données d'image sur bande magnétique EMV compromises. En outre, lorsqu'elle est mise en application conjointement avec un code PIN pour la vérification du titulaire de la carte, l'EMV limite l'impact des fraudes à la carte perdue/volée/jamais reçue. Il a été clairement démontré que dans les pays où a été déployé le système EMV, il existe une baisse mesurable et significative de la fraude lors des transactions individuelles.[1].

Toutefois, le système EMV en lui-même n'empêche pas l'accès inapproprié aux, ni ne protège la confidentialité des, données du titulaire et/ou d'identification sensibles. Les environnements d'acceptation EMV et de traitement actuels peuvent traiter à la fois les transactions EMV et non EMV (comme une bande magnétique, ou une clé d'entrée de numéro de compte primaire [PAN] lorsque des raisons techniques l'exigent). Ces transactions non EMV n'ont pas la même capacité de réduire la fraude que les transactions EMV, et, par conséquent, requièrent une protection supplémentaire. En outre, il est important de noter que dans des environnements EMV, la confidentialité du PAN n'est pas conservée à tous les points de la transaction ; en effet, il est nécessaire de traiter le PAN en clair sur le terminal du point de vente pour compléter les étapes essentielles du processus de transaction EMV. La date d'expiration et les autres données du titulaire sont également transmises en texte clair.

Les possibilités que ces types de transaction et/ou éléments de données soient exposés et utilisés de manière frauduleuse au sein des réseaux traditionnels et en carte absente sont les raisons pour lesquelles il est nécessaire de mettre en œuvre la norme PCI DSS dans le ou les environnements d'acceptation EMV d'aujourd'hui.

[1] Financial Fraud Action UK and the UK Cards Association. « Fraud The Facts 2010 – The Definitive Overview of Payment Industry Fraud and Measures to Prevent it ». Disponible en ligne : http://www.theukcardsassociation.org.uk/files/ukca/fraud_the_facts_2010.pdf

1.2 Le rôle de la norme PCI DSS

La norme de sécurité de l'industrie des cartes de paiement (PCI DSS) contient 12 conditions opérationnelles et techniques essentielles, définies par le Conseil des normes de sécurité PCI (PCI SSC). Plutôt que de se concentrer sur une catégorie de fraude spécifique, la norme PCI DSS cherche à protéger les données d'identification sensibles et celles du titulaire, partout où ces données sont présentes dans l'écosystème de paiement, limitant ainsi la disponibilité de ces données pour les fraudeurs. La norme PCI DSS atteint ses objectifs de sécurité de deux manières :

- En garantissant l'intégrité des composantes du système, qui conduisent aux données d'identification sensibles et à celles du titulaire de carte, contre des attaques physiques et logiques.

- En protégeant la confidentialité des données du titulaire lorsqu'elles sont stockées au sein d'un environnement donné, ou celle des données du titulaire et d'identification sensibles lorsqu'elles sont transmises sur un réseau ouvert ou public.

1.3 Conclusions

Les environnements d'acceptation qui utilisent efficacement le système EMV peuvent réduire considérablement la fraude dans les environnements de transaction individuelle, mais, comme nous l'avons mentionné en détail ci-dessus, un environnement EMV, tel qu'il est mis en place aujourd'hui, ne remplit pas automatiquement les conditions de la norme PCI DSS ni ne protège la confidentialité des données du titulaire et d'identification sensibles. Ajoutons à cela la capacité des commerçants à traiter à la fois les transactions EMV et non EMV, et il devient évident qu'il est essentiel de protéger la confidentialité des données d'identification sensibles et de celles du titulaire.

Par sa conception, la norme PCI DSS ne fait pas de distinction entre les mécanismes de sécurité de transaction sous-jacents, mais cherche plutôt à protéger le PAN et d'autres données d'identification sensibles comme un but en soi, sans examiner le risque de fraude sous-jacent si la sécurité de ces données était compromise. À l'avenir, si le système EMV devait devenir le seul moyen de paiement dans un réseau de transaction individuelle donné, couplé à un processus d'identification robuste adopté au niveau international pour les transactions en carte absente, le besoin de maintenir la confidentialité du PAN et celle d'autres données d'identification sensibles devrait être considérablement réduit. En conséquence, la norme PCI DSS serait mise à jour pour la mettre en conformité avec le contexte de menaces qui existerait alors, et ses conditions d'application en relation avec l'EMV réduites en conséquence. Jusqu'à aujourd'hui, l'EMV et la norme PCI DSS créent ensemble une puissante approche en deux volets dans le cadre des objectifs de réduction de la fraude et du renforcement de la sécurité.

Par conséquent, dans la sécurisation de l'environnement d'acceptation des transactions individuelles actuel, il ne faut pas considérer qu'il s'agit des normes EMV ou PCI DSS, mais plutôt des normes EMV et PCI DSS. Les deux éléments sont essentiels dans la lutte contre la fraude et l'exposition des données. Ensemble, ils fournissent le meilleur niveau de sécurité pour les données du titulaire sur la totalité du processus de transaction.

2 Portée

Ce document est destiné aux personnes adoptant la technologie EMV, y compris, mais sans s'y limiter, les détaillants, acquéreurs, processeurs, et émetteurs, ou ceux qui valident les environnements PCI DSS comme les QSA (Qualified Security Assessors – évaluateurs de sécurité qualifiés) et les ISA (Internal Security Assessors – évaluateurs de sécurité internes).

Il est entendu et accepté que le stade de déploiement et de maturité EMV sur les différents marchés dans les diverses régions du monde varie. Ces marchés, qui ne sont pas encore acquis la maturité, travailleront à réaliser les recommandations des marques de cartes de crédit et de l'EMVCo.

Le document ne fournit pas de détails techniques concernant les normes EMV et PCI DSS, ni d'instructions sur la manière de les mettre en œuvre, mais suppose que le lecteur est familiarisé avec ces deux normes. Il suppose également que les fabricants de cartes CI et de terminaux ont intégré les dernières directives EMV à leurs produits. Il est entendu que la meilleure sécurité est fournie par les terminaux approuvés aux termes de la dernière version du programme de test de sécurité des transactions par PIN PCI.

Pour le lecteur intéressé, les détails des normes EMV et PCI ainsi que les spécifications se trouvent sur les sites Web concernés *www.emvco.com et www.pcisecuritystandards.org* ainsi que dans les directives et documents spécifiques de chaque marque.

Il est rappelé au lecteur que le rôle du Conseil des normes de sécurité PCI est d'élaborer des normes de sécurité et d'autres documents de directives à l'appui. Tous les aspects relatifs à la conformité, à l'application et à l'adoption de ces normes, notamment tous les problèmes relatifs aux risques, sont de la responsabilité des systèmes de carte individuels. Les questions que les lecteurs peuvent avoir à cet égard doivent être adressées à leur contact PCI DSS.

3 Sécurité EMV et PCI DSS

Pour comprendre comment les environnements d'acceptation et de traitement EMV actuels sont liés à la norme PCI DSS, il faut examiner les éléments de données présents dans les transactions EMV et comprendre comment ces informations peuvent être utilisées de manière frauduleuse. En outre, il est important de comprendre la protection limitée inhérente aux transactions non EMV et la manière dont ces informations sont susceptibles d'être utilisées de façon frauduleuse si elles venaient à être divulguées.

Le tableau ci-dessous présente les éléments de données présents dans une carte à puce EMV et/ou disponibles durant le traitement d'une transaction EMV, ainsi que les raisons justifiant leur présence. Ce faisant, il est important de souligner que les données conservées sur une carte à puce EMV, ainsi que les données envoyées lors d'une transaction EMV, contiennent des éléments du titulaire de carte et d'identification sensibles que la norme PCI DSS cherche à protéger.

	Élément de données	Argumentaire
Données de titulaire de carte	Numéro de compte primaire (PAN)	Nécessaire en texte clair pour les transactions EMV pour : • identifier le titulaire de carte et effectuer la transaction ; • faciliter l'acheminement de la transaction ; • procéder à l'identification des données au point de vente ; • autoriser la dérivation de clé par l'émetteur.
	Nom du titulaire de la carte	Présent sur une puce EMV. Sa transmission dans un message d'autorisation n'est pas nécessaire.
	Code service	Présent dans les données équivalentes aux données de piste 2 sur une puce. Son but dans une transaction EMV est de permettre à l'émetteur de valider le code ou la valeur de vérification de la carte s'ils sont également inclus dans les données équivalentes aux données de piste 2.
	Date d'expiration	Toujours disponible en clair sur des cartes EMV, avec une balise de date d'expiration spécifique. En cas d'autorisation en ligne, la date d'expiration incluse dans les données équivalentes aux données de piste 2 sera indiquée dans le message d'autorisation. Ces données sont disponibles en texte clair.

	Élément de données	Argumentaire
Données d'identification sensibles	Données complètes de la bande magnétique	Une carte EMV peut contenir des données équivalentes aux données de piste 1 ou 2, qui contiennent les mêmes champs qu'une bande magnétique. En raison des systèmes existants, les données équivalentes aux données de piste 2 sont généralement incluses dans les demandes d'autorisation en ligne EMV. Ces données sont disponibles en texte clair. Pour l'utilisation d'un code ou une valeur de vérification de carte à puce unique ; cependant, les données équivalentes aux données de piste 2 sont maintenant différentes des données de piste 2 de la bande magnétique, et ne peuvent donc pas être utilisées pour créer des cartes à bande magnétique frauduleuses. Dans ce cas, seuls les éléments de données du titulaire, tels qu'ils sont décrits ci-dessus, restent sensibles.
	CAV2/CVC2/CVV2/CID	Ne fait pas partie de la spécification EMV. Les puces EMV ne contiennent pas ces informations. Ce code est uniquement imprimé sur la carte elle-même.
	Code/bloc PIN	La spécification EMV permet une vérification hors ligne du titulaire de carte grâce à l'utilisation du PIN dans la puce elle-même de sorte que le bloc PIN ne quitte jamais l'environnement de point de vente. D'autres méthodes de vérification de carte sont également prises en charge, notamment le code PIN en ligne.

3.1 L'environnement de carte de paiement

La plupart des environnements traitant des transactions EMV aujourd'hui sont des environnements hybrides, gérant à la fois des transactions EMV et non EMV. Dans de telles circonstances, la protection de la confidentialité des données du titulaire et d'identification sensibles reste essentielle pour garantir l'intégrité de la chaîne de paiement.

3.1.1 Transactions par bande magnétique

Dans une transaction par bande magnétique, les données du titulaire et d'identification sensibles sont lues depuis des données statiques encodées sur la bande magnétique de la carte et transmises à l'émetteur (généralement en clair) pour autorisation. Étant donné la nature statique de ces données, elles peuvent facilement être copiées, soit directement depuis la carte, soit par interception lors du traitement d'une transaction. Les données de bande magnétique capturées peuvent ensuite être utilisées pour créer des cartes à bande magnétique contrefaites pour une utilisation lors d'une transaction individuelle ou d'une fraude au GAB. En outre, le PAN et la date d'expiration peuvent être extraits des données de bande magnétique pour une utilisation frauduleuse en carte absente, où le réseau carte

absente n'utilise pas de données d'identification supplémentaires au-delà de ce qui est disponible dans le réseau de transaction en personne.

3.1.2 Repli technique

La plupart des cartes EMV contiennent une bande magnétique, soit pour une rétrocompatibilité dans des environnements non EMV, soit pour prendre en charge un repli technique si la carte à puce EMV est illisible. « Repli technique » décrit un processus d'exception dans lequel un dispositif compatible EMV lit la bande magnétique, au lieu des données de la puce sur une carte EMV. Dans de telles situations, les mécanismes de sécurité fournis par l'EMV sont effectivement contournés, et la sécurité de la transaction revient à celle d'une bande magnétique. Dans de nombreux marchés EMV matures cependant, un repli technique est généralement limité et contrôlé, limitant ce type de fraude.

3.1.3 Entrée de clé PAN

Une entrée de clé PAN se produit en guise de mécanisme de repli lorsqu'il est impossible de lire une bande magnétique ou une puce. Pour terminer une transaction d'entrée de clé PAN, seuls le PAN, la date d'expiration et la signature du client sont nécessaires, rendant cette technique plus sensible à la fraude à partir de données de titulaire compromises dans un quelconque réseau d'acceptation. Alors qu'une entrée de clé PAN requiert la falsification de la signature du titulaire de carte, cette méthode de vérification du titulaire est potentiellement moins fiable car elle peut être soit correctement vérifiée par un commerçant, soit tout simplement pas vérifiée. Cette méthode d'entrée de données est restreinte, contrôlée et peu utilisée dans un environnement EMV mature, ce qui limite ainsi la fraude d'entrée de clé PAN.

3.1.4 Transactions de commande postale ou téléphonique

Les commerçants utilisent parfois cette méthode pour accepter des transactions à distance dans leurs environnements d'acceptation EMV. Comme entrée de clé PAN, le détaillant saisit manuellement le PAN et la date d'expiration ; cependant, en plus de ces données, le détaillant entre souvent le code de sécurité de la carte (code à trois chiffres imprimé sur la carte) dans le cadre de l'autorisation de la transaction.

3.1.5 Transactions EMV

Dans des environnements d'acceptation EMV, la transaction EMV contient des données précieuses pour un fraudeur. Les scénarios dans lesquels ces données sont exposées au risque, peuvent être classés comme suit :

- Manque de puce unique CVV/CVC : si une carte EMV conserve le même CVV/CVC que la bande magnétique, les données équivalentes de piste 2 saisies peuvent être utilisées pour créer des cartes à bande magnétique pour une utilisation frauduleuse en transaction individuelle et au GAB.

- Lecture « en profondeur » : lorsque la carte est complètement insérée dans un lecteur, comme dans un GAB, la bande magnétique réelle peut être lue et les données capturées utilisées pour créer des cartes à bande magnétique.

- Exposition du PAN et de la date d'expiration : EMVCo n'exige pas de conserver la confidentialité du PAN et de la date d'expiration lors du traitement d'une transaction EMV. Dans l'infrastructure d'acceptation de paiement d'aujourd'hui, il est possible que les transactions de paiement puissent être présentées pour approbation et autorisées uniquement grâce au PAN et à la date d'expiration. Ces informations sont généralement disponibles en texte clair dans le cadre des transactions EMV et par bande magnétique, et peuvent être utilisées de manière frauduleuse dans d'autres

réseaux d'acceptation de paiement, notamment en carte absente, qui n'utilisent pas de données d'identification supplémentaires au-delà de ce qui est disponible dans le réseau de transaction en personne.

En conséquence de ces menaces, les données natives d'une transaction EMV requièrent une protection au-delà de ce qui est intrinsèquement fourni par la transaction EMV elle-même.

3.2 La norme PCI DSS et l'environnement EMV actuel

La norme EMV assure une sécurité de transaction et une interopérabilité internationale au sein d'un environnement de transaction EMV. La mise en œuvre de l'EMV, qui utilise des valeurs de vérification de carte différentes de celles conservées sur une bande magnétique, atténue le risque d'utilisation des données de transaction EMV compromises en vue de contrefaire des cartes. De même, une carte EMV empêche activement les attaques par clonage de cartes grâce à l'utilisation de méthodes d'identification de carte améliorées, qui, lorsqu'elles sont appliquées conjointement au PIN comme méthode de vérification du titulaire de la carte, limitent l'impact des catégories de fraude à la carte perdue/volée/jamais reçue. Toutefois, une transaction EMV ne protège pas la confidentialité, ni n'empêche la compromission de certains éléments de données de transaction.

Dans tous les environnements d'acceptation mentionnés dans la section 3.1 ci-dessus, les transactions de paiement présentées pour approbation uniquement fondées sur des données statiques – comme les bandes magnétiques, les données tapées manuellement, les transactions de commandes postales ou téléphoniques, ainsi que les PAN et dates d'expiration – sont intrinsèquement précieuses et peuvent être utilisées pour accomplir des transactions frauduleuses sauf si des mesures appropriées sont prises pour empêcher l'accès à ces données. Pour ces raisons, la norme PCI DSS reste un outil essentiel pour protéger les données statiques.

La norme PCI DSS s'applique à tous les réseaux et moyens de paiement possibles utilisant les données du titulaire pour réaliser une transaction.

3.3 Développements futurs dans la sécurité des transactions

Des changements, des améliorations et de nouvelles opportunités de paiement sont continuellement en développement. En utilisant les méthodes d'identification fournies par une transaction EMV et l'introduction d'une identification supplémentaire dans le réseau carte absente, le PAN et la date d'expiration en eux-mêmes ne seraient pas suffisants pour finaliser une transaction. D'autres changements pourraient voir l'introduction de procédures et processus d'identification améliorés pour tous les réseaux de transactions comme :

- L'EMV est la seule méthode permettant d'effectuer un paiement dans un réseau de transaction individuelle donné. Dans un environnement EMV mature, cela pourrait impliquer une migration à un système à carte uniquement EMV, ce qui permettrait de réduire la menace de l'environnement hybride tout en permettant la transmission du PAN du titulaire de carte et d'autres données sensibles en texte clair.
- Pour des environnements qui ne migrent pas à un système à carte uniquement EMV, mais où l'EMV est la seule méthode de paiement de transaction individuelle, l'utilisation de différentes valeurs de vérification de carte conservées sur la puce et sur la bande magnétique est essentielle.

- Le réseau carte absente utilise des données d'identification supplémentaires pour réaliser une vérification du titulaire de carte, impossibles à obtenir par le biais d'un environnement d'acceptation de transaction individuelle s'il est compromis.

Dans de telles circonstances, le besoin de maintenir la confidentialité du PAN et celle d'autres données d'identification est considérablement réduit. En conséquence, la norme PCI DSS serait mise à jour pour la mettre en conformité avec le contexte de menaces qui existerait alors, et ses conditions d'application en relation avec l'EMV réduites en conséquence.

3.4 Résumé

L'EMV doit être considérée dans le contexte de l'environnement actuel de traitement des transactions où la confidentialité des données du titulaire issues des transactions EMV, ainsi que celle des données d'identification sensibles, reste fondamentale pour garantir l'intégrité du système de paiement.

Bien que l'EMV puisse réduire considérablement la fraude dans des transactions en carte absente, elle ne satisfait pas automatiquement aux conditions PCI DSS pour la protection des données du titulaire et d'identification sensibles. Dans ce contexte des déploiements EMV actuels, le besoin de protéger la confidentialité des données du titulaire et d'identification sensibles, comme le prescrit la norme PCI DSS, reste une part essentielle de l'effort global du secteur pour empêcher l'utilisation de ces données dans des transactions frauduleuses dans d'autres environnements.

À l'avenir, si le système EMV devait devenir le seul moyen de paiement dans un réseau de transaction individuelle donné, couplé à un processus d'identification robuste adopté au niveau international pour les transactions en carte absente, le besoin de maintenir la confidentialité du PAN et celle d'autres données d'identification sensibles devrait être considérablement réduit. En conséquence, la norme PCI DSS serait mise à jour pour la mettre en conformité avec le contexte de menaces qui existerait alors, et ses conditions d'application en relation avec l'EMV réduites en conséquence.

Les normes EMV et PCI DSS d'aujourd'hui, ainsi que les normes PA-DSS et PTS, sont complémentaires et importantes car elles fournissent une approche holistique des objectifs de réduction globale de la fraude et en sécurisant les données du titulaire dans le secteur du paiement. Dans les marchés qui ont migré ou sont en train de migrer au système EMV, les intervenants du secteur du paiement doivent utiliser les normes EMV et PCI DSS conjointement pour réduire la fraude et augmenter la sécurité.

4 Référence et glossaire

4.1 Références

1. *EMV 4.2, volume 2, Sécurité* – www.emvco.com
2. *EMV 4.2, volume 3, Spécification d'application* – www.emvco.com
3. *Norme de sécurité des données PCI, v1.2* – www.pcisecuritystandards.org
4. *Émetteur EMV et directives de sécurité d'application, v2.2 mai 2009* – www.emvco.com
5. *EMV 4.2, volume 4, Conditions d'interface du titulaire, du préposé et de l'acquéreur* – www.emvco.com
6. *Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS*
7. *Exigences de sécurité PCI PTS*
8. *Recommandation pour le traitement EMV des types de transactions spécifiques du secteur, décembre 2008, v1.1* – www.emvco.com
9. Financial Fraud Action UK and the UK Cards Association. “Fraud The Facts 2010 – The Definitive Overview of Payment Industry Fraud and Measures to Prevent it.” Disponible en ligne : http://www.theukcardsassociation.org.uk/files/ukca/fraud_the_facts_2010.pdf

4.2 Abréviations et glossaires

Des abréviations et des définitions se trouvent dans le *glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS*

Des abréviations et définitions supplémentaires sont données ci-dessous.

Terme	Définition
CNP	Carte absente
CVM	Méthodes de vérification de la carte
CVR	Résultats de vérification de la carte
DAC	Code d'authentification des données
EMV	Officiellement Europay, MasterCard, Visa – Carte à circuit intégré Spécifications des systèmes de paiement. www.emvco.com
CCI	Carte à circuit intégré
iCVV	Valeur de vérification de la carte CCI
CP/CT	Commande postale/commande par téléphone
POS	Point de vente
SEPA	Single Euro Payments Area, Espace unique de paiement en euros
TRM	Gestion du risque terminal
Carte absente	Type de transaction de paiement, réalisé par exemple par courrier, par téléphone ou par Internet, où le titulaire de carte ne présente pas la carte au commerçant
Carte hybride	Une carte qui contient à la fois une puce EMV et une bande magnétique.
Environnement EMV	Un environnement dans lequel une puce EMV est lue par un terminal de point de vente et utilisée pour réaliser une transaction EMV. Il peut faire partie d'un environnement hybride qui traite également des transactions et données par bande magnétique.
Environnement hybride	Un environnement dans lequel une puce EMV ou une bande magnétique peuvent être lues par le point de vente et utilisées pour traiter des transactions EMV ou par bande magnétique.
Repli technique	État dans lequel une puce ne peut pas être utilisée, un autre type d'entrée comme la lecture de bande magnétique ou une clé PAN, étant utilisé pour finaliser une transaction.

4.3 Remerciements

De nombreuses organisations ont contribué individuellement et collectivement à l'élaboration de ce document, notamment : les membres du conseil PCI, le groupe d'intérêt spécial sur le champ d'application, les membres de la communauté QSA, EMVCo, des banques, des vendeurs, des commerçants et des consultants indépendants. Nous avons grandement apprécié leur précieuse contribution et leur appui.