

*Les détaillants, les établissements financiers, les processeurs de données et tous les autres fournisseurs qui gèrent des données de détenteurs de cartes de crédit doivent aujourd'hui respecter des politiques strictes pour s'assurer que les données sont sécurisées en permanence. En collaborant avec American Express, Discover, MasterCard, Visa, ou tout autre émetteur de carte de crédit, ces entreprises pâtissent considérablement des vols de données, en particulier en subissant des amendes et un manque à gagner. SafeNet peut aider à relever un grand nombre de défis critiques de sécurité pour respecter les politiques des émetteurs de cartes de crédit en ce qui concerne la confidentialité des données au sein de l'entreprise.*

Mise à jour en septembre 2006, la norme de sécurité des données de l'industrie des cartes de paiement (PCI - Payment Card Industry) est appliquée par tous les grands émetteurs de cartes de crédit, y compris American Express, Discover Financial Services, JCB, MasterCard Worldwide et Visa International. Bien que cette norme s'étende du changement régulier des mots de passe d'employés au déploiement de pare-feu, de nombreuses règles portent sur la sécurité des données pendant leur stockage au sein de l'entreprise.

SafeNet peut aider à relever un grand nombre des défis critiques pour assurer la sécurité des données sensibles au sein de l'entreprise et pour respecter les politiques des émetteurs de cartes de crédit.

Dans les pages qui suivent, nous allons présenter certaines exigences spécifiques de la norme PCI et nous allons illustrer comment SafeNet peut vous aider à répondre à ces exigences.

Réglementations	Réponses de SafeNet
<p><b>Exigence 3 : Protéger les données stockées des détenteurs de cartes</b></p> <p>Le chiffrement joue un rôle essentiel dans la protection des données des détenteurs de cartes. Si un intrus réussit à passer tous les contrôles de sécurité de réseau pour accéder à des données chiffrées, sans les clés cryptographiques appropriées, les données sont illisibles et inutilisables par cette personne.</p>	<p>SafeNet apporte des capacités de chiffrement assurant la sécurité des données sensibles en appliquant des algorithmes de chiffrement standard et robustes.</p>
<p><b>Exigence 3.4</b></p> <p>Rendre le numéro de compte principal PAN [Primary Account Number] au minimum illisible quel que soit l'endroit où il est stocké (y compris les données sur le support numérique portable, le support de stockage, les journaux et les données reçues de réseaux sans fil ou stockées sur ceux-ci) en utilisant n'importe laquelle des approches suivantes :</p> <ul style="list-style-type: none"> <li>• Fonctions de hachage unidirectionnel fort (indices hachés)</li> <li>• Troncation</li> <li>• Jetons et tampons d'indices (les tampons doivent être stockés en toute sécurité)</li> <li>• Cryptographie forte associée à des processus et des procédures de gestion de clés.</li> </ul>	<p>SafeNet prend en charge des algorithmes de chiffrement de cryptographie forte, y compris 3DES et AES 256 bits. SafeNet prend également en charge DES, AES 128 bits et 192 bits, RC4 (40 bits et 128 bits) et RSA (DES et RC4 ne sont pas généralement recommandés pour la protection des données au repos dans des environnements de production.) SafeNet prend également en charge les hachages HmacSHA-1.</p> <p>En outre, SafeNet assure la génération de clés sécurisées, le stockage de clés sécurisées et la gestion de clés sécurisées par le biais d'une plate-forme matérielle renforcée. L'architecture de sécurité et de gestion de clés de SafeNet comprend des composants matériels et logiciels qui assurent la gestion de clés sécurisées et la conformité à PCI.</p>

**Exigence 3.5.1**

Restreindre l'accès aux clés au plus petit nombre de responsables nécessaires.

SafeNet centralise le stockage et la gestion des clés sur un appareil de sécurité dédié unique, où toutes les clés sont stockées, cryptées et contrôlées pour garantir leur intégrité au sein de la plate-forme, et elles ne sont jamais disponibles en texte clair pour qui que ce soit.

L'accès aux clés peut être restreint à des propriétaires de clés désignés ou à des groupes d'utilisateurs de SafeNet. Des niveaux plus granulaires de permission peuvent également être octroyés sur la base d'opérations de clés (chiffrement/déchiffrement, signature/vérification de signature, et MAC/vérification de MAC) et de l'accès aux clés (sur la base du temps et sur la base du taux) par le biais des capacités de gestion de politiques centralisées de SafeNet.

**Exigence 3.5.2**

Stocker les clés en toute sécurité dans le plus petit nombre possible d'emplacements et de formes.

SafeNet centralise le stockage et la gestion des clés de chiffrement sur un appareil unique (ou plus typiquement une grappe intégrée d'appareils de sécurité dédiés), où toutes les clés sont stockées, cryptées et contrôlées pour garantir leur intégrité au sein de la plate-forme, et elles ne sont jamais disponibles en texte clair pour qui que ce soit. Les clés sont cryptées en utilisant une hiérarchie multicouche de clés de chiffrement de clés. De plus, SafeNet propose une option FIPS 140-2 Niveau 3 répondant aux exigences du gouvernement des États-Unis pour garantir la protection contre les manipulations illicites de la gestion des clés.

Les clés de chiffrement sont également traitées en toute sécurité dans une perspective opérationnelle. Par exemple, lorsque des clés sont copiées sur plusieurs dispositifs SafeNet en grappes ou avec des dispositifs SafeNet distants configurés pour une reprise après accident, les clés sont toujours cryptées. Lorsque les clés sont sauvegardées, les clés (et toutes les autres informations de configuration de SafeNet) sont de surcroît cryptées dans le fichier de configuration de sauvegarde.

**Exigence 3.6**

Complètement documenter et mettre en œuvre tous les processus et toutes les procédures de gestion de clés pour les clés utilisées pour le chiffrement des données de détenteurs de cartes, y compris :

3.6.1 Génération de clés fortes

3.6.2 Distribution de clés sécurisées

3.6.3 Stockage de clés sécurisées

3.6.4 Changement périodique de clés

- D'après les besoins de l'application associée (par exemple, recodage de clé) ; de préférence automatiquement
- Au moins manuellement.

3.6.5 Destruction des anciennes clés

3.6.6 Connaissances divisées et établissement d'un double contrôle des clés (deux ou trois personnes ne connaissant que leur partie de la clé pour reconstruire toute la clé)

3.6.7 Prévention de la substitution sans autorisation de clés

3.6.8 Remplacement de clés compromises connues ou suspectées

3.6.9 Révocation des clés anciennes ou invalides

3.6.10 Les responsables de clés doivent signer un formulaire stipulant qu'ils comprennent et acceptent leurs responsabilités.

Avec la solution de SafeNet, les clés cryptographiques ne quittent jamais la plate-forme DataSecure. La seule manière d'accéder à la plate-forme DataSecure est au niveau administrateur, par le biais de la console de gestion sécurisée sur le Web, une interface de ligne de commande sur SSH, ou une connexion de console directe. La plate-forme peut être configurée pour que les administrateurs individuels n'aient accès qu'à leur sphère de responsabilité.

SafeNet propose un module de sécurité matériel conforme à FIPS 140-2 Niveau 3, répondant aux exigences du gouvernement des États-Unis garantissant que la gestion de clé est protégée contre les manipulations illicites. Voici comment SafeNet répond aux exigences spécifiques :

3.6.1—Des clés fortes sont générées sous forme matérielle en utilisant une capacité matérielle de génération de nombres aléatoires fournie par les accélérateurs cryptographiques sur le dispositif SafeNet en utilisant les outils d'administration de SafeNet, soit CLI soit Admin GUI. Les étapes et les procédures impliquées peuvent être facilement incluses dans des procédures de politique de sécurité.

3.6.2—Avec la solution de SafeNet, les clés cryptographiques ne quittent jamais l'appareil. Les clés de chiffrement sont générées et résident toujours sur l'appareil renforcé. Puisque les opérations cryptographiques sont effectuées sur l'appareil, les clés n'ont pas besoin d'être distribuées ou stockées sur des serveurs Web, d'application ou de base de données. SafeNet fournit des mécanismes sécurisés de copie et de sauvegarde pour que les clés ne quittent pas la plate-forme SafeNet en clair à des fins de support opérationnel.

3.6.3—Les clés sont toujours stockées en toute sécurité sur la plate-forme SafeNet. Les clés de cryptage sont cryptées en utilisant une hiérarchie multicouche de clés de chiffrement de clés. De plus, SafeNet propose une option FIPS 140-2 Niveau 3 permettant de stocker les clés de cryptage dans un module de sécurité matérielle résistant aux manipulations illicites.

# Conformité à la sécurité des données PCI

3.6.4—SafeNet fournit un mécanisme de rotation de clés permettant aux clients de faire tourner efficacement les clés selon leur politique de sécurité.

3.6.5—Les clés sont toujours stockées sur le dispositif SafeNet sous forme cryptée. La clé cryptée est supprimée du disque lorsque la clé est enlevée du dispositif SafeNet.

3.6.6—La connaissance divisée de la création et la suppression/l'accès de clé est prise en charge par le biais de plus de 20 de nos ACL d'administration. Vous pouvez exiger que deux personnes approuvent certains types d'actions, comme la création de clé.

De plus, la connaissance divisée des clés est souvent employée dans des situations dans lesquelles des bits de clés bruts sont stockés, exposés ou accédés en clair. SafeNet fournit un mécanisme de stockage de clés plus sécurisé car les bits de clés bruts ne peuvent jamais être stockés, exposés ou accédés en clair. Avec la solution SafeNet, les utilisateurs autorisés de clés de cryptage ont accès à des opérations cryptographiques, mais pas aux bits de clés bruts. Les opérations cryptographiques sont effectuées uniquement avec les clés auxquelles un utilisateur SafeNet a accès.

Enfin, il existe des manières d'imposer que les informations partagées entre de multiples administrateurs soient nécessaires avant d'effectuer des opérations administratives spécifiques aux clés. Il y a également des manières d'imposer de multiples niveaux d'authentification avant d'effectuer des opérations cryptographiques avec des clés de chiffrement spécifiques.

## Exigence 4.1

Utiliser des protocoles de cryptographie forte et de sécurité comme SSL (Secure Sockets Layer) / TLS (Transport Layer Security) et IPSEC (Internet Protocol Security) pour protéger les données sensibles des détenteurs de cartes pendant la transmission sur des réseaux publics ouverts.

SafeNet prend en charge SSL pour le chiffrement de transport entre les serveurs de bases de données (ou les serveurs d'applications) et l'appareil SafeNet. L'ordre de préférence des chiffrements SSL et des tailles de clés acceptables peut être configuré sur l'appareil SafeNet comme l'autorisation uniquement des clés de 128 bits ou de tailles supérieures. SafeNet recommande généralement dans le cadre de nos meilleures pratiques d'utiliser SSL pour le chiffrement de transport. Néanmoins, puisque la connexion de réseau entre l'appareil SafeNet et le serveur de base de données (ou le serveur d'application) est typiquement sur le réseau privé du client et non pas sur un réseau public, tous les clients ne mettent pas forcément en œuvre SSL.

## Exigence 8.2

En plus de l'attribution d'un identifiant unique, employer au moins l'une des méthodes suivantes pour authentifier tous les utilisateurs :

- Mot de passe
- Dispositifs à jetons (par exemple, SecureID, certificats, ou clés publiques)
- Biométrie

La seule manière d'accéder à la plate-forme SafeNet est au niveau de l'administrateur, via une console de gestion sur le Web sécurisée, une interface de ligne de commande sur SSH, ou une connexion de console directe. La plate-forme peut être configurée pour que les administrateurs individuels n'aient accès qu'aux zones relevant de leur responsabilité. Les activités administratives sont enregistrées et signées numériquement dans un journal d'analyse rétrospective.

Les administrateurs peuvent obtenir des permissions dans 16 catégories différentes en fonction de leur rôle et de leurs responsabilités, ce qui permet un contrôle administratif de fine granularité. L'authentification à deux facteurs pour l'accès administratif peut être activée et appliquée en utilisant des certificats numériques en conjonction avec des mots de passe. Tous les mots de passe d'administrateurs sont hachés et n'existent jamais sur le dispositif SafeNet en clair.

Les administrateurs SafeNet étant distincts des utilisateurs, c'est-à-dire des applications ou des bases de données ou des utilisateurs finaux ayant besoin de chiffrement/déchiffrement, une séparation opérationnelle intégrée des responsabilités est réalisée entre les personnes (administrateurs) gérant le dispositif et établissant les politiques cryptographiques et les entités (utilisateurs) ayant besoin de crypter ou de décrypter des données.

	Les utilisateurs n'ont pas d'accès administratif au dispositif SafeNet. Néanmoins, il leur est attribué des privilèges leur permettant de demander des opérations cryptographiques avec des clés spécifiques conformément aux politiques centralisées et personnalisables de SafeNet. Indépendamment de l'authentification à deux facteurs pour l'accès des administrateurs, l'authentification à deux facteurs pour l'accès des utilisateurs (aux opérations cryptographiques) peut également être appliquée.
<b>Exigence 8.4</b> Crypter tous les mots de passe pendant la transmission et le stockage sur tous les composants du système.	Les mots de passe sont cryptés via SSL lorsque l'authentification sur la plate-forme DataSecure est effectuée. Dans la plate-forme, les mots de passe sont hachés pour qu'ils ne soient jamais exposés.
<b>Exigence 8.5</b> S'assurer de la bonne authentification d'utilisateur et de la bonne gestion de mot de passe pour les non-consommateurs et les administrateurs sur tous les composants du système.	SafeNet fournit les meilleures pratiques autour de la gestion des privilèges pour l'authentification sur la plate-forme DataSecure. La plate-forme a également un ensemble évolué d'options de gestion de mot de passe pour l'expiration, l'historique de mot de passe, la longueur de mot de passe et le jeu de caractères.
<b>Exigence 10 : Suivre et surveiller tous les accès aux ressources de réseaux et aux données de détenteurs de cartes</b> Les mécanismes d'enregistrement et les capacités de suivi des activités d'utilisateurs sont essentiels. La présence de journaux dans tous les environnements permet le suivi complet et l'analyse des dysfonctionnements. Il est très difficile de déterminer la cause d'un dysfonctionnement sans des journaux d'activité de système.	SafeNet maintient un ensemble extensif de fichiers de journaux centralisés permettant le suivi des activités d'administrateurs et d'utilisateurs. Les fichiers de journaux sont horodatés et comprennent des informations spécifiques d'identification d'administrateur ou d'utilisateur. Les fichiers de journaux sont signés numériquement pour empêcher leur manipulation illicite.
<b>Exigence 10.2</b> Mettre en œuvre une analyse rétrospective automatisée de tous les composants du système pour reconstruire les événements suivants : 10.2.1 Tous les accès d'utilisateurs individuels aux données de détenteurs de cartes 10.2.2 Toutes les actions effectuées par un individu avec des privilèges de racine ou d'administrateur 10.2.3 Accès à toutes les analyses rétrospectives 10.2.4 Tentatives incorrectes d'accès logique 10.2.5 Usage de mécanismes d'identification et d'authentification 10.2.6 Initialisation de journaux d'analyse rétrospective 10.2.7 Création et suppression d'objets au niveau du système.	Les fichiers de journaux comprennent : journal de système, journal d'analyse rétrospective, journal NAE, journal de chiffrement de base de données, et journaux SQL. Les fichiers de journaux peuvent être individuellement configurés pour un planning de rotation souhaité, le nombre de fichiers de journaux archivés sur le dispositif SafeNet et le transfert automatique de journaux hors dispositif en utilisant la copie sécurisée (SCP) ou FTP. La synchronisation avec d'autres dispositifs comme des serveurs de bases de données ou d'applications peut être réalisée en utilisant NTP (Network Time Protocol). Le dispositif SafeNet peut être configuré pour pointer vers une source NTP, comme un routeur ou un autre dispositif de réseau.
<b>Exigence 10.5</b> Sécuriser les analyses rétrospectives pour empêcher leur altération. 10.5.1 Limiter la visualisation des analyses rétrospectives aux besoins des tâches à effectuer 10.5.2 Protéger les fichiers d'analyse rétrospective contre les modifications sans autorisation 10.5.3 Sauvegarder immédiatement les fichiers d'analyse rétrospective sur un serveur d'enregistrement centralisé ou sur un support difficile à altérer 10.5.4 Copier les journaux de réseaux sans fil sur un serveur d'enregistrement du réseau local interne. 10.5.5 Utiliser des logiciels de surveillance d'intégrité de fichier et de détection de changement sur les journaux pour s'assurer que les données de journaux existants ne puissent pas être modifiées sans générer d'alerte (l'ajout de nouvelles données ne devant pas provoquer d'alerte).	Comme cela a été susmentionné, les fichiers de journaux de SafeNet ont une signature numérique pour empêcher leur manipulation illicite. De plus, dans le cadre de l'ensemble flexible d'options de configuration de journaux, SafeNet permet la rotation automatique des fichiers de journaux sur un serveur de sauvegarde ou d'archivage de journaux. Par conséquent, une analyse rétrospective peut être efficacement maintenue pour répondre aux réglementations juridiques et d'analyse rétrospective.

\* Réglementations de la « Norme de sécurité des données de l'industrie des cartes de paiement (PCI) », version 1.1, septembre 2006.



[www.safenet-inc.com](http://www.safenet-inc.com)

**Siège social :**  
4690 Millennium Drive, Belcamp, Maryland 21017 Etats-Unis  
Tél. : +1 410 931 7500 or 800 533 3958, Fax : +1 410 931 7524, Email : [info@safenet-inc.com](mailto:info@safenet-inc.com)

**Siège EMEA :**  
Tél. : + 44 (0) 1276 608 000,  
Email : [info.emea@safenet-inc.com](mailto:info.emea@safenet-inc.com)

**Siège APAC :**  
Tél. : +852 3157 7111, Email : [info.apac@safenet-inc.com](mailto:info.apac@safenet-inc.com)

Pour toutes les coordonnées de contact et les bureaux, visitez : [www.safenet-inc.com/company/contact.asp](http://www.safenet-inc.com/company/contact.asp)

©2009 SafeNet, Inc. Tous droits réservés. SafeNet et le logo SafeNet sont des marques déposées de SafeNet. Tous les autres noms de produits sont des marques de leurs propriétaires respectifs.  
28.10.09