Industrie des cartes de paiement (PCI)
Norme de sécurité des données (DSS)
Questionnaire d'auto-évaluation

Instructions et conseils

Version 3.2.1

Juin 2018

Modifications apportées au document

Date	Version	Description
1er octobre 2008	1.2	Aligner le contenu sur la nouvelle version v1.2 de la norme PCI DSS et appliquer les changements mineurs relevés par rapport à la version v1.1.
28 octobre 2010	2.0	Aligner le contenu sur la nouvelle version v2.0 de la norme PCI DSS et préciser les types d'environnements du questionnaire d'auto-évaluation (SAQ - Self-Assessment Questionnaire) ainsi que les critères d'éligibilité. Ajout du SAQ C-VT pour les commerçants utilisant un terminal virtuel connecté au Web
Juin 2012	2.1	Ajout du SAQ P2PE-HW pour les commerçants qui traitent les données des titulaires de carte uniquement par le biais de terminaux de paiement physiques compris dans une solution de chiffrement point à point (ou P2PE) validée et répertoriée par le PCI SSC. Ce document doit être utilisé avec la version 2.0 de la norme PCI DSS.
Avril 2015	3.1	Aligner le contenu avec la version v3.1 de la norme PCI DSS, notamment l'ajout des SAQ A-EP et B-IP, et préciser les critères d'éligibilité pour les SAQ actuels.
Mai 2016	3.2	Actualisé pour s'aligner sur la version v3.2 de la norme PCI DSS et pour préciser les critères d'éligibilité des SAQ actuels.
Juin 2018	3.2.1	Mises à jour mineures pour s'aligner sur la version v3.2.1 de la norme PCI DSS.

REMERCIEMENTS: La version anglaise de ce document, telle que mise à disposition sur le site Internet du PCI SSC, à toutes fins, est considérée comme la version officielle de ces documents et, dans la mesure où il existe des ambiguïtés ou des incohérences entre la rédaction de ce texte et du texte anglais, la version anglaise disponible à l'endroit mentionné prévaudra.

Table des matières

À propos de ce document

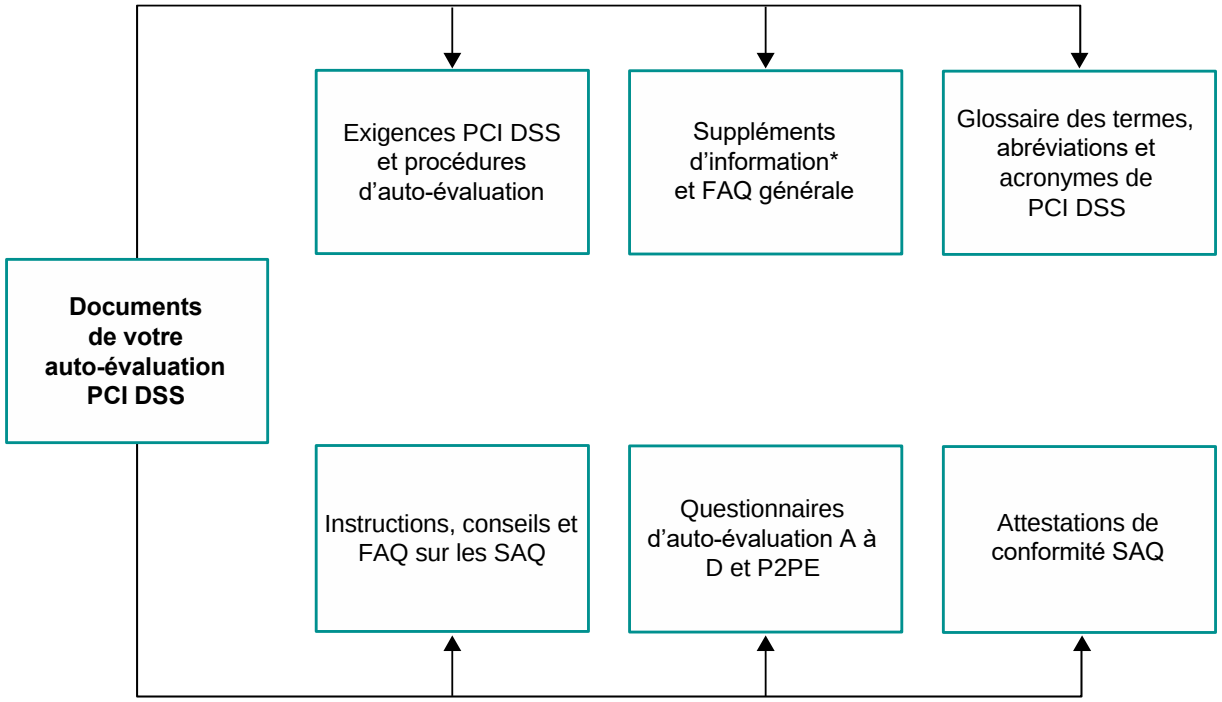
Ce document a été conçu pour aider les commerçants et les prestataires de services à comprendre les questionnaires d'auto-évaluation (SAQ) de la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) Pour comprendre pourquoi la norme PCI DSS est importante pour votre entreprise, les stratégies qu'elle peut mettre en œuvre pour valider sa conformité et si elle est éligible pour remplir un des SAQ abrégés, nous vous conseillons de lire attentivement et intégralement les Instructions et conseils.

Auto-évaluation PCI DSS : les interactions

La norme PCI DSS et les documents qui s'y rapportent sont un ensemble d'outils communs qui garantit un traitement sécurisé des données de titulaire de carte. La norme fournit un cadre d'actions permettant de développer un processus de sécurité solide, notamment par la prévention, la détection et la réaction aux incidents de sécurité. Pour réduire le risque de compromission des données et atténuer son éventuel impact, il est impératif que toutes les entités stockant, traitant ou transmettant des données de titulaire de carte s'y conforment.

Le graphique ci-dessous décrit les outils mis en place pour aider les entreprises à être conformes à la norme PCI DSS et à s'auto-évaluer.

Vous trouverez ces documents ainsi que d'autres sur www.pcisecuritystandards.org.



* *Attention : les suppléments d'information n'apport ent que des informations supplémentaires et des conseils. Ils ne remplacent pas ni ne prévalent sur les exige nces PCI DSS.*

* ***Remarque :*** *les suppléments d'information apportent des renseignements et des conseils qui viennent compléter et qui ne remplacent en aucun cas ni ne prévalent sur les exigences de la norme PCI DSS.*

Présentation du questionnaire d'auto-évaluation

Les *Questionnaires d'auto-évaluation PCI DSS* (SAQ) sont des outils de validation destinés à aider les commerçants et les prestataires de services à auto-évaluer leur conformité à la norme PCI DSS. Il existe plusieurs versions de SAQ PCI DSS correspondant à différents scenarios. Ce document a pour vocation d'aider votre entreprise à déterminer le ou les SAQ qui correspondent le mieux à son environnement.

Les SAQ de PCI DSS sont des outils de validation destinés aux commerçants et aux prestataires de services dont l'acquéreur ou la marque de paiement n'exige pas de rapport de conformité (ROC) à PCI DSS. Veuillez vous adresser à votre acquéreur ou à votre marque de paiement pour plus de détails sur les exigences de validation de la norme PCI DSS.

Chaque SAQ de PCI DSS se compose des éléments suivants :

1. Des questions relatives aux exigences de la norme PCI DSS, selon les différents environnements : lire « Choisir le SAQ et l'attestation les plus adaptés à votre entreprise » dans le présent document. Cette partie comprend également une colonne « Tests attendus » qui correspond aux procédures de tests de la norme PCI DSS.
2. Attestation de conformité : l'attestation inclut votre déclaration d'éligibilité à remplir le SAQ applicable ainsi que les résultats de l'auto-évaluation PCI DSS.

L'importance de la norme PCI DSS

Les membres fondateurs du Conseil des normes de sécurité PCI (American Express, Discover, JCB, Mastercard et Visa) surveillent en permanence les cas de compromission des données. Ces cas de compromission de données concernent tous les commerçants et prestataires de services, des plus petits aux plus grands.

Les conséquences d'une faille de sécurité et la compromission des données des cartes de paiement qu'elle entraîne sont de grande ampleur pour les entreprises touchées. Il peut s'agir :

1. d'une obligation de signalement aux organismes réglementaires,
2. d'une perte de réputation,
3. d'une perte de clients,
4. de pertes financières potentielles (par ex. des amendes et pénalités de la part des autorités), et
5. de litiges.

L'analyse « post-mortem » des compromissions a montré que les points faibles courants en matière de sécurité, qui sont traités par les dispositifs de contrôle PCI DSS, sont souvent exploités soit parce que les mesures de sécurité PCI DSS n'étaient pas mises en œuvre soit parce qu'elles étaient mal appliquées lorsque la compromission est survenue. La norme PCI DSS a été conçue, et comprend des exigences détaillées, exactement pour cette raison : réduire la probabilité d'une compromission de données et ses effets.

Parmi les exemples de défaillance courante en matière de dispositifs de sécurité PCI DSS, on peut citer, sans limitation :

- Le stockage de données d'authentification sensibles (DAS), comme les données de pistage, à l'issue de l'autorisation (exigence 3.2). Bon nombre d'entités compromises ignoraient que leurs systèmes stockaient ces données.
- Des contrôles d'accès inadéquats en raison de systèmes de point de vente (POS) mal installés, permettant ainsi aux utilisateurs malveillants d'y pénétrer au moyen de parcours normalement réservés aux fournisseurs du POS (exigences 7.1, 7.2, 8.2 et 8.3).
- Des configurations et des mots de passe système par défaut qui n'ont pas été modifiés lors de l'installation (exigence 2.1).
- Des services inutiles et non sécurisés qui n'ont pas été supprimés ni sécurisés au moment de l'installation du système (Exigences 2.2.2 et 2.2.3).
- Des applications Web mal codées, entraînant une injection SQL et d'autres vulnérabilités qui permettent d'accéder à la base de données contenant les données de titulaire de carte, directement depuis le site Web (Exigence 6.5).
- Des correctifs de sécurité non appliqués et obsolètes (Exigence 6.2).
- L'absence de journaux (Exigence 10).
- L'absence de surveillance (via l'examen des journaux, la détection/le blocage des intrusions, l'analyse des vulnérabilités trimestrielle et des mécanismes de détection des changements) (Exigences 10.6, 11.2, 11.4 et 11.5).

- De mauvaises décisions quant au champ d'application—par exemple, exclure une partie du réseau du champ d'application de PCI DSS en raison d'une segmentation dudit réseau inadéquate qui n'a pas prouvé son efficacité (Exigence 11.3.4). Cela a pour conséquence d'exposer sans le savoir l'environnement des données de titulaire de carte aux faiblesses des autres parties du réseau qui n'ont pas été sécurisées selon la norme PCI DSS (par ex. des points d'accès sans fil non sécurisés et des vulnérabilités introduites via les e-mails d'employés et leur navigation sur le Web) (Exigences 1.2, 1.3 et 1.4).

Comprendre la différence entre conformité et sécurité

Il faut bien faire la distinction entre conformité et sécurité. Être conforme à la norme PCI DSS à un moment donné n'empêche pas votre environnement d'évoluer, ce qui pourrait impacter votre sécurité si les contrôles appropriés ne sont pas appliqués. Par conséquent, vous devez faire en sorte que les dispositifs de contrôle de PCI DSS soient correctement appliqués en permanence dans le cadre des activités d'affaires courantes (BAU) et tel que défini par votre stratégie globale de sécurité. Ainsi, vous pourrez contrôler l'efficacité des mesures de sécurité de votre entreprise en continu et maintenir votre environnement conforme à la norme PCI DSS entre chaque évaluation PCI DSS. Le chapitre « Bonnes pratiques de mise en œuvre PCI DSS dans les affaires courantes » de la norme PCI DSS offre des exemples d'intégration de la norme dans les activités BAU.

De plus, les exigences de sécurité PCI DSS sont destinées à protéger les données des cartes de paiement, et votre entreprise peut posséder d'autres données et actifs sensibles qui ont eux aussi besoin d'être protégés, même s'ils sortent du champ d'application de la norme. Par conséquent, même si la conformité à la norme PCI DSS, si elle est correctement maintenue, contribue certainement à la sécurité globale, elle ne remplace pas un programme de sécurité plus robuste à l'échelle de toute l'entreprise.

Conseils et stratégies d'ordre général pour être conforme à la norme PCI DSS

Ci-dessous sont présentés des conseils et des stratégies pour débuter vos efforts de conformité à la norme PCI DSS. Ces conseils peuvent vous aider à cesser de stocker les données de titulaire de carte dont vous n'avez pas besoin, à isoler les données réellement utiles dans des zones bien définies, contrôlées et centralisées et à restreindre le champ d'application de vos efforts de validation de la conformité à la norme PCI DSS. Par exemple, en éliminant les données de titulaire de carte dont vous n'avez pas besoin et/ou en isolant les données dont vous avez réellement besoin dans des zones définies et contrôlées, vous pouvez supprimer les systèmes et les réseaux qui ne stockent pas, ne traitent pas et ne transmettent pas les données de titulaire de carte (et qui ne se connectent pas aux systèmes qui le font) du champ d'application de votre auto-évaluation.

1. **Les données d'authentification sensibles (incluant le contenu complet de la bande magnétique ou des données équivalentes sur une puce, les codes et valeurs de vérification de la carte, les codes PIN et les blocs PIN) :**

   ➢ Assurez-vous de ***ne jamais stocker ces données*** après l'autorisation :

2. **Interroger le fournisseur du terminal POS sur la sécurité de votre système, en lui posant les questions suivantes par exemple :**

   a. La configuration et les mots de passe par défaut ont-ils été modifiés sur les systèmes et les bases de données utilisés par le système du POS ?

   b. Avez-vous accès au système de mon terminal POS à distance ? Si oui, avez-vous mis en place les contrôles appropriés pour empêcher d'autres personnes d'accéder à mon système POS, comme par exemple un accès à distance sécurisé et ne pas utiliser de mots de passe trop courants ou par défaut ? À quelle fréquence accédez-vous à distance à mon terminal POS et pour quelle raison ? Qui est autorisé à accéder à mon terminal POS à distance ?

   c. Tous les services inutiles et non sécurisés ont-il bien été supprimés des systèmes et bases de données qui font partie du système POS ?

   d. Le logiciel de mon terminal POS est-il conforme à la norme de sécurité des données de l'application de paiement (PA-DSS) ? Consulter la liste PCI DSS des Applications de paiement agréées.

e. Mon logiciel POS stocke-t-il des données d'authentification sensibles, comme les données de bande magnétique ou les blocs PIN ? Si oui, c'est interdit : pouvez-vous m'aider à les supprimer rapidement ?

f. Le logiciel de mon terminal POS stocke-t-il des numéros de compte primaire (PAN) ? Si oui, ils doivent être protégés : comment le sont-ils ?

g. Documentez-vous la liste des fichiers créés par l'application, avec un résumé du contenu de chaque fichier, afin de vérifier que les données susmentionnées, qui sont interdites, ne sont pas stockées ?

h. Le logiciel de mon terminal POS utilise-t-il des mots de passe uniques et complexes pour tous les accès par des utilisateurs ?

i. Pouvez-vous confirmer que vous n'utilisez pas des mots de passe courants ou par défaut pour accéder à mon système et aux systèmes d'autres commerçants que vous prenez en charge ?

j. Les systèmes et bases de données contenus dans le système du terminal POS ont-ils bien été actualisés avec toutes les mises à jour de sécurité applicables ?

k. La fonction de génération de journaux est-elle bien activée pour les systèmes et bases de données qui font partie du système du terminal POS?

l. Si les versions précédentes du logiciel de mon terminal POS stockaient des données d'authentification sensibles, cette fonction a-t-elle été supprimée lors des mises à jour récentes du logiciel ? Un utilitaire d'effacement sécurisé a-t-il été utilisé pour supprimer ces données ?

3. Données de titulaire de carte : si vous n'en avez pas besoin, ne les stockez pas !

a. Les règles applicables aux marques de paiement autorisent le stockage des numéros de compte primaire (PAN), de la date d'expiration, du nom du titulaire de la carte et du code de service.

b. Répertoriez toutes les raisons justifiant ce stockage ainsi que tous les endroits où sont stockées ces données. Si ces données ne correspondent pas à un but légitime, mieux vaut les supprimer.

c. Déterminez si le stockage de ces données et le processus métier qui les utilise compensent ce qui suit :

i. Le risque que les données soient compromises.

ii. Les contrôles PCI DSS supplémentaires qui devront s'appliquer pour protéger les données.

iii. Les futurs efforts continus de maintenance pour rester conforme à la norme PCI DSS.

4. Données de titulaire de carte : si vous en avez besoin, consolidez-les et isolez-les.

Vous pouvez limiter le champ d'application d'une évaluation PCI DSS en regroupant le stockage des données dans un environnement défini et en isolant les données grâce à une segmentation appropriée du réseau. Par exemple, si vos employés naviguent sur le Web et reçoivent des e-mails sur l'appareil ou le segment du réseau où sont stockées les données de titulaire de carte, vous devez envisager de segmenter (isoler) ces données sur un appareil ou segment du réseau réservé à cet effet (par ex. via des routeurs ou des pare-feux). Si vous avez la possibilité d'isoler les données de titulaire de carte de manière efficace, vous pourrez concentrer vos efforts de conformité à la norme PCI DSS précisément sur cette partie et non pas sur tous les appareils.

5. Contrôles compensatoires

Des contrôles compensatoires peuvent être envisagés pour la plupart des exigences PCI DSS lorsqu'une entreprise n'est pas en mesure de respecter la spécification technique d'une exigence, mais a suffisamment atténué le risque associé par le biais d'autres dispositifs de contrôle. Si votre entreprise n'applique pas exactement le dispositif de contrôle indiqué par la norme PCI DSS mais que d'autres méthodes de contrôle, correspondant à la définition des contrôles compensatoires, sont mis en œuvre (cf « Contrôles compensatoires » à l'Annexe B de la norme PCI DSS et *Glossaire des termes, abréviations et acronymes des normes PCI DSS et PA-DSS*), votre entreprise doit procéder comme suit :

a. Suivre la procédure relative aux contrôles compensatoires décrite à l'Annexe B de la norme PCI DSS.

b. Répondre à la question du SAQ concerné dans la colonne « OUI pour CCW » pour toutes les exigences satisfaites au moyen de contrôles compensatoires.

c. Documenter chaque contrôle compensatoire en complétant une Fiche de contrôle compensatoire dans l'Annexe B du SAQ.

> Une Fiche de contrôle compensatoire doit être remplie pour chaque exigence satisfaite au moyen d'un contrôle compensatoire.

d. Envoyer toutes les Fiches de contrôle compensatoire dûment remplies, ainsi que le SAQ et/ou l'Attestation de conformité complétés, conformément aux instructions de votre acquéreur ou marque de paiement.

6. Aide d'un professionnel et formation

a. Si vous souhaitez engager un professionnel de la sécurité pour vous aider à effectuer votre auto-évaluation, nous vous conseillons vivement de contacter un évaluateur de sécurité qualifié (QSA). Les QSA ont été formés par le PCI SSC pour mener des évaluations PCI DSS et ils sont répertoriés sur son site Web.

b. Le site Web de PCI SSC propose des ressources supplémentaires, comme :

- Le*glossaire des termes, abréviations et acronymes de la norme PCI*
- Foire aux questions (FAQ)
- Webinaires
- Des informations supplémentaires et directives
- Formulaires SAQ et Attestations de conformité

c. Le PCI SSC fournit également des formations pour sensibiliser le personnel d'une entreprise. On peut citer comme exemple les formations Sensibilisation à la norme PCI, Professionnel PCI (PPCI) et Évaluateur de sécurité interne (ISA).

Consultez le site www.pcisecuritystandards.org pour obtenir plus d'informations.

Remarque : *les compléments d'information complètent la norme PCI DSS et identifient des considérations et des recommandations supplémentaires pour satisfaire à ses exigences. En revanche, ils ne modifient pas, n'éliminent pas ni ne remplacent la norme PCI DSS ou une de ses exigences.*

d. Des programmes et des ressources de formation sur les paiements peuvent également être proposés par les marques de paiement et/ou votre acquéreur.

Choisir le SAQ et l'attestation les plus adaptés à votre entreprise

Tous les commerçants et prestataires de services doivent respecter en permanence la norme PCI DSS selon leur environnement. Il existe différents types de SAQ, présentés synthétiquement dans le tableau ci-dessous et détaillés dans les pages qui suivent. Servez-vous du tableau pour déterminer quel SAQ correspond à votre entreprise, puis lisez la description détaillée pour vous assurer de bien satisfaire à toutes ses exigences.

Remarque applicable à tous les SAQ, excepté le D : Ces SAQ comportent des questions qui correspondent à un type précis d'environnement commercial, tel que défini dans les critères d'éligibilité du SAQ concerné. Si des exigences PCI DSS s'appliquent à votre environnement mais ne sont pas traitées par un SAQ donné, c'est probablement que ledit SAQ n'est pas adapté à votre environnement. De plus, vous devez respecter toutes les exigences PCI DSS applicables pour être considéré comme conforme à la norme.

SAQ	Description
A	Les commerçants « carte non présente » (e-commerce ou vente à distance) qui ont entièrement sous-traité toutes les fonctions liées aux données de titulaire de carte à un prestataire de services tiers conforme à PCI DSS, et qui ne stockent pas, ne traitent pas ni ne transmettent électroniquement les données de titulaire de carte sur les systèmes ou dans les locaux du commerçant. *Ne s'applique pas à la vente en face-à-face.*
A-EP	Les e-commerçants qui sous-traitent tout le processus de traitement des paiements à des tiers agréés par la norme PCI DSS, et qui possèdent un site Web ne recevant pas directement les données de titulaire de carte mais néanmoins susceptibles d'affecter la sécurité des transactions. Aucun stockage, traitement ni aucune transmission électronique de données de titulaire de carte sur les systèmes du commerçant ou dans ses locaux. *Ne s'applique qu'à l'e-commerce.*
B	Commerçants utilisant uniquement : ▪ des terminaux à empreinte sans stockage électronique de données de titulaire de carte et/ou ▪ des terminaux autonomes de connexion sortante (dial-out), sans stockage électronique de données de titulaire de carte. *Ne s'applique pas à l'e-commerce.*
B-IP	Commerçants utilisant uniquement un terminal de paiement autonome compatible avec la norme PTS, équipé d'une connexion IP avec le processeur de paiement, sans stockage électronique de données de titulaire de carte. *Ne s'applique pas à l'e-commerce.*
C-VT	Commerçants qui saisissent manuellement chaque transaction sur le clavier d'une solution de terminal de paiement virtuelle sur Internet, fournie et hébergée par un prestataire de services tiers agréé par la norme PCI DSS. Aucun stockage électronique de données de titulaire de carte. *Ne s'applique pas à l'e-commerce.*

SAQ	Description
C	Commerçants équipés de systèmes d'applications de paiement connectés à Internet, sans stockage électronique de données de titulaire de carte. *Ne s'applique pas à l'e-commerce.*
P2PE	Commerçants utilisant uniquement des terminaux de paiement physiques, compris et gérés par une solution de chiffrement point à point (P2PE) agréée par la norme PCI DSS, sans stockage électronique de données de titulaire de carte. *Ne s'applique pas à l'e-commerce.*
D	***QAE SAQ D pour commerçants :*** tous les commerçants non concernés par les descriptions des SAQ ci-dessus.
	SAQ D pour les prestataires de services : tous les prestataires de services considérés par une marque de paiement comme éligibles pour remplir un SAQ.

SAQ A – commerçants « carte non présente », toutes les fonctions relatives aux données de titulaire de carte sont entièrement sous-traitées

Le SAQ A a été conçu pour répondre aux exigences applicables aux commerçants dont les fonctions de gestion des données de titulaire de carte sont complètement sous-traitées à des tiers agréés et qui ne conservent que les formats papier des factures ou reçus contenant les données de titulaire de carte.

Pour choisir un type de SAQ à l'aide d'un graphique, allez à la page 20 « Quel SAQ correspond le plus à mon environnement ? ».

Les commerçants concernés par le SAQ A relèvent soit de l'e-commerce, soit de la vente à distance (carte non présente), et ils ne stockent pas, ne traitent pas ni ne transmettent de données de titulaire de carte sous forme électronique dans leurs systèmes ou leurs locaux.

Lesdits commerçants confirment qu'ils remplissent les critères d'éligibilité suivants pour ce mode de paiement :

- Votre entreprise accepte uniquement les transactions « carte non présente » (e-commerce ou vente à distance) ;
- L'intégralité du traitement des données de titulaire de carte est sous-traité à des prestataires de services tiers agréés par la norme PCI DSS ;
- Votre entreprise ne stocke pas, ne traite pas ni ne transmet de données de titulaire de carte sur vos systèmes ou dans vos locaux car c'est un tiers qui se charge entièrement de toutes ces fonctions ;
- Votre entreprise a vérifié que tous les tiers chargés du stockage, du traitement et/ou de la transmission des données de titulaire de carte sont conformes à la norme PCI DSS ; **et**
- Les données de titulaire de carte détenues par votre entreprise sont sous forme papier (par ex. factures imprimées ou reçus), et ces documents ne sont pas reçus par voie électronique.

De plus, pour l'e-commerce :

- Tous les éléments de toutes les pages de paiement affichées par le navigateur des clients proviennent uniquement et directement d'un prestataire de services tiers agréé par la norme PCI DSS.

Ce SAQ ne s'applique pas à la vente en face-à-face.

SAQ A-EP – E-commerce partiellement sous-traité à un site Web tiers pour les paiements

Le SAQ A-EP a été conçu pour répondre aux exigences applicables aux e-commerçants possédant un site Web qui ne reçoit pas de données de titulaire de carte en tant que tel mais qui a néanmoins un impact sur la sécurité des transactions et/ou l'intégrité de la page recevant les données de titulaire de carte du client.

Les commerçants concernés par le SAQ A-EP sont des e-commerçants qui sous-traitent partiellement le canal de paiement à des tiers agréés par la norme PCI DSS. Ils ne stockent pas, ne traitent pas et ne transmettent pas électroniquement de données de titulaire de carte sur leurs systèmes ou dans leurs locaux.

Pour choisir un type de SAQ à l'aide d'un graphique, allez à la page 20 « Quel SAQ correspond le plus à mon environnement ? ».

Lesdits commerçants confirment qu'ils remplissent les critères d'éligibilité suivants pour ce canal de paiement :

- Votre entreprise accepte uniquement les transactions d'e-commerce ;
- Tout traitement des données de titulaire de carte, à l'exception de la page de paiement, est entièrement sous-traité à un processeur de paiement tiers agréé par la norme PCI DSS ;
- Votre site Web d'e-commerce ne reçoit pas de données de titulaire de carte mais il décide de rediriger vos clients, ou leurs données de titulaire de carte, vers un processeur de paiement tiers agréé par la norme PCI DSS ;
- Si le site Web du commerçant est hébergé par un fournisseur tiers, ce dernier est certifié conforme à toutes les exigences de la norme PCI DSS applicables (notamment à l'Annexe A s'il s'agit d'un fournisseur d'hébergement partagé) ;
- Chaque élément des pages de paiement affiché dans le navigateur du client provient soit du site Web du commerçant, soit du prestataire de services conforme à PCI DSS ;
- Votre entreprise ne stocke pas, ne traite pas ni ne transmet électroniquement de données de titulaire de carte sur vos systèmes ou dans vos locaux car c'est un tiers qui se charge entièrement de toutes ces fonctions ;
- Votre entreprise a vérifié que tous les tiers chargés du stockage, du traitement et/ou de la transmission des données de titulaire de carte sont conformes à la norme PCI DSS ; **et**
- Les données de titulaire de carte détenues par votre entreprise sont sous forme papier (par ex. factures imprimées ou reçus), et ces documents ne sont pas reçus par voie électronique.

Ce SAQ ne s'applique qu'à l'e-commerce.

Remarque : *Aux fins du SAQ A-EP, les exigences PCI DSS relatives à l'« environnement de données des titulaires de carte » sont applicables aux sites Web du commerçant. En effet, le site Web d'un commerçant a un impact direct sur la manière dont les données de la carte de paiement sont transmises, même s'il ne reçoit pas de données de titulaire de carte en tant que tel.*

SAQ B – Commerçants équipés de terminaux à empreinte uniquement ou de terminaux autonomes de connexion sortante (dial-out) uniquement. Pas de stockage électronique des données de titulaire de carte

Le SAQ B a été conçu pour répondre aux exigences applicables aux commerçants qui traitent les données de titulaire de carte uniquement au moyen de terminaux à empreinte ou de terminaux autonomes à connexion sortante.

Les commerçants du SAQ B peuvent être soit des magasins physiques (carte présente) soit des enseignes de vente à distance (carte non présente), et ils ne stockent pas de données de titulaire de carte dans leur système informatique. Lesdits commerçants confirment qu'ils remplissent les critères d'éligibilité suivants pour ce canal de paiement :

Pour choisir un type de SAQ à l'aide d'un graphique, allez à la page 20 « Quel SAQ correspond le plus à mon environnement ? ».

- Votre entreprise utilise exclusivement un terminal à empreinte et/ou un terminal autonome à connexion sortante (connecté au processeur via une ligne téléphonique) pour relever les informations de la carte de paiement du client ;
- Les terminaux autonomes à connexion sortante ne sont pas connectés à un autre système de votre environnement ;
- Les terminaux autonomes à connexion sortante ne sont pas connectés à Internet ;
- Votre entreprise ne transmet pas les données de titulaire de carte sur un quelconque réseau (Intranet ou Internet) ;
- Les données de titulaire de carte détenues par votre entreprise sont sous forme papier (par ex. factures imprimées ou reçus), et ces documents ne sont pas reçus par voie électronique ; **et**
- Votre entreprise ne stocke pas les données de titulaire de carte sous forme électronique.

Ce SAQ ne s'applique pas à l'e-commerce.

SAQ B-IP – Commerçants disposant de terminaux de point d'interaction (POI) autonomes, connectés via IP et conformes à la norme PTS, pas de stockage électronique de données de titulaire de carte

Le SAQ B-IP a été conçu pour répondre aux exigences applicables aux commerçants qui traitent les données de titulaire de carte exclusivement au moyen d'un dispositif de point d'interaction (POI) autonome et conforme à la norme PTS, connecté via IP au processeur de paiement.

Pour choisir un type de SAQ à l'aide d'un graphique, allez à la page 20 « Quel SAQ correspond le plus à mon environnement ? ».

Les commerçants du SAQ B-IP peuvent être soit des magasins physiques (carte présente) soit des enseignes de vente à distance (carte non présente), et ils ne stockent pas de données de titulaire de carte dans leur système informatique.

Lesdits commerçants confirment qu'ils remplissent les critères d'éligibilité suivants pour ce canal de paiement :

- Votre entreprise utilise uniquement des dispositifs de point d'interaction (POI) approuvés par la norme PTS et autonomes (hormis SCR), connecté via IP au processeur de paiement dans le but de relever les informations de la carte de paiement du client ;
- Les dispositifs de point d'interaction (POI) autonomes et connectés via IP sont certifiés conformes à la norme PTS, tel qu'indiqué sur le site Web de PCI SSC (hormis SCR) ;
- Les dispositifs POI connectés via IP et autonomes ne sont connectés à aucun autre système de votre environnement (grâce à la segmentation du réseau qui permet d'isoler les dispositifs POI des autres systèmes) ;
- Les seules transmissions de données de titulaire de carte possibles sont celles des dispositifs POI conformes à la norme PTS à destination du processeur de paiement ;
- Le dispositif POI ne dépend d'aucun autre appareil (comme un ordinateur, un téléphone mobile, une tablette, etc.) pour se connecter au processeur de paiement ;
- Les données de titulaire de carte détenues par votre entreprise sont sous forme papier (par ex. factures imprimées ou reçus), et ces documents ne sont pas reçus par voie électronique ; **et**
- Votre entreprise ne stocke pas les données de titulaire de carte sous forme électronique.

Ce SAQ ne s'applique pas à l'e-commerce.

SAQ C-VT – Commerçants équipés de terminaux virtuels connectés au Web, sans stockage électronique des données des titulaires de carte

Le SAQ C-VT a été conçu pour répondre aux exigences applicables aux commerçants qui traitent les données de titulaire de carte uniquement au moyen de terminaux de paiement virtuels isolés sur un ordinateur connecté à Internet.

Un terminal de paiement virtuel procure un accès par navigateur Web au site Web d'un acquéreur, un processeur ou un prestataire de services tiers afin d'autoriser les transactions par carte de paiement. Le commerçant saisit manuellement les données de la carte de paiement via un navigateur Web connecté et sécurisé. Contrairement aux terminaux physiques, les terminaux virtuels ne lisent pas les données directement sur la carte. En effet, les transactions par carte sont saisies manuellement.

Pour choisir un type de SAQ à l'aide d'un graphique, allez à la page 20 « Quel SAQ correspond le plus à mon environnement ? ».

Les commerçants du SAQ C-VT traitent les données de titulaire de carte uniquement par le biais d'un terminal de paiement virtuel et ils ne les stockent pas sur un système informatique. Ces terminaux virtuels sont connectés à Internet pour accéder à un tiers hébergeant la fonction de traitement du paiement par terminal virtuel. Ce tiers peut être un processeur, un acquéreur ou un prestataire de services tiers qui stocke, traite et/ou transmet les données de titulaire de carte afin d'autoriser et/ou de régler les transactions de paiement au moyen du terminal virtuel du commerçant.

Cette version du SAQ ne s'applique qu'aux commerçants qui saisissent manuellement chaque transaction sur un clavier dans une solution de terminal virtuel sur Internet. Les commerçants du SAQ C-VT peuvent être des magasins physiques (carte présente) ou des enseignes de vente à distance (carte non présente).

Lesdits commerçants confirment qu'ils remplissent les critères d'éligibilité suivants pour ce canal de paiement :

- Votre entreprise ne traite les paiements que via un terminal de paiement virtuel accessible depuis un navigateur Web connecté à Internet ;
- La solution du terminal de paiement virtuel de votre entreprise est fournie et hébergée par un prestataire de services tiers agréé par PCI DSS ;
- Votre entreprise accède à la solution du terminal de paiement virtuel conforme à la norme PCI DSS via un ordinateur isolé dans un endroit prévu à cet effet. Ce dernier n'est pas connecté à d'autres lieux ou systèmes de votre environnement (grâce à un pare-feu ou la segmentation du réseau qui isole l'ordinateur en question des autres systèmes) ;
- L'ordinateur de votre entreprise ne contient pas de logiciel stockant des données de titulaire de carte (par ex. aucun logiciel de traitement par lot ou de stockage et transmission en différé n'est installé) ;
- L'ordinateur de votre entreprise ne comporte aucun matériel périphérique destiné à relever ou stocker les données de titulaire de carte (par ex. aucun lecteur de carte relié) ;
- Votre entreprise ne reçoit ni ne transmet d'aucune autre manière les données de titulaire de carte par voie électronique via n'importe quel canal (par ex. via un intranet ou Internet) ;

- Les données de titulaire de carte détenues par votre entreprise sont sous forme papier (par ex. factures imprimées ou reçus), et ces documents ne sont pas reçus par voie électronique ; **et**
- Votre entreprise ne stocke pas les données de titulaire de carte sous forme électronique.

Ce SAQ ne s'applique pas à l'e-commerce.

SAQ C – Commerçants équipés de systèmes d'applications de paiement connectés à Internet, sans stockage électronique des données de titulaire de carte

Le SAQ C a été conçu pour répondre aux exigences applicables aux commerçants dont les systèmes d'applications de paiement (par ex. les systèmes point de vente) sont connectés à Internet (par ex. via DSL, modem-câble, etc.).

Ces commerçants traitent les données de titulaire de carte via un système de point de vente (POS) ou d'autres systèmes d'applications de paiement connectés à Internet. Ils ne stockent pas les données de titulaire de carte sur un système informatique et peuvent être des magasins physiques (carte présente) ou des enseignes de vente à distance (carte non présente).

Pour choisir un type de SAQ à l'aide d'un graphique, allez à la page 20 « Quel SAQ correspond le plus à mon environnement ? ».

Lesdits commerçants confirment qu'ils remplissent les critères d'éligibilité suivants pour ce canal de paiement :

- Un système d'applications de paiement et une connexion à Internet sont installés sur le même appareil et/ou le même réseau local (LAN) de votre entreprise ;
- Le système d'applications de paiement/appareil Internet n'est connecté à aucun autre système de votre environnement (grâce à la segmentation du réseau qui isole le système d'applications de paiement/l'appareil Internet des autres systèmes) ;
- Le lieu où se trouve l'environnement POS n'est pas connecté à d'autres lieux ou sites, et tout LAN n'est installé que pour un seul magasin ;
- Les données de titulaire de carte détenues par votre entreprise sont sous forme papier (par ex. factures imprimées ou reçus), et ces documents ne sont pas reçus par voie électronique ; **et**
- Votre entreprise ne stocke pas les données de titulaire de carte sous forme électronique.

Ce SAQ ne s'applique pas à l'e-commerce.

SAQ P2PE – Commerçants utilisant des terminaux de paiement uniquement dans le cadre d'une solution P2PE répertoriée par PCI SSC. Pas de stockage électronique de données de titulaire de carte

Le SAQ P2PE a été conçu pour répondre aux exigences applicables aux commerçants qui traitent les données de titulaire de carte uniquement par le biais des terminaux de paiement compris dans une solution de chiffrement point à point (P2PE) validée et répertoriée par le PCI SSC.

Pour choisir un type de SAQ à l'aide d'un graphique, allez à la page 20 « Quel SAQ correspond le plus à mon environnement ? ».

Les commerçants du SAQ P2PE n'ont pas accès aux données de compte en texte clair sur un système informatique ; ils ne saisissent des données de compte qu'au moyen de terminaux de paiement issus d'une solution P2PE agréée par le PCI SSC. Les commerçants du SAQ P2PE peuvent être des magasins physiques (carte présente) ou des enseignes de vente à distance (carte non présente). Par exemple, une enseigne de vente à distance peut être éligible au SAQ P2PE si elle reçoit des données de titulaire de carte sur papier ou par téléphone et qu'elle les saisit directement et exclusivement sur un appareil P2PE agréé.

Lesdits commerçants confirment qu'ils remplissent les critères d'éligibilité suivants pour ce canal de paiement :

- Le traitement des paiements se fait par une solution P2PE conforme à la norme PCI et agréée et répertoriée par le PCI SSC ;
- Les seuls systèmes de l'environnement du commerçant qui stockent, traitent ou transmettent des données de compte sont les appareils point d'interaction (POI) qui sont autorisés à être utilisés avec une solution P2PE validée et répertoriée par le PCI SSC ;
- En aucun cas votre entreprise ne reçoit ni ne transmet par voie électronique les données de titulaire de carte.
- Votre environnement ne stocke pas d'anciennes données de titulaire de carte électroniquement ;
- Les données de titulaire de carte détenues par votre entreprise sont sous forme papier (par ex. factures imprimées ou reçus), et ces documents ne sont pas reçus par voie électronique ; et
- Votre entreprise a mis en œuvre tous les contrôles préconisés dans le *Manuel d'instruction P2PE (PIM)* et délivrés par le fournisseur de solution P2PE.

Ce SAQ ne s'applique pas à l'e-commerce.

SAQ D pour les commerçants – Tous les autres commerçants éligibles à un SAQ

SAQ D pour les commerçants s'applique aux commerçants éligibles au SAQ qui ne correspondent à aucun autre SAQ.

Parmi les exemples d'environnements susceptibles de correspondre au SAQ D, on peut citer, sans limitation :

- les e-commerçants qui acceptent les données de titulaire de carte sur leur site Web ;
- Les commerçants stockant électroniquement les données de titulaire de carte ;
- Les commerçants qui ne stockent pas électroniquement les données de titulaire de carte mais qui ne remplissent pas les critères d'un autre type de SAQ ;
- Les commerçants dont les environnements pourraient correspondre à un autre SAQ mais pour lesquels d'autres exigences PCI DSS s'appliquent.

SAQ D pour les prestataires de services – Prestataires de services éligibles à un SAQ

SAQ D pour les prestataires de services s'applique à tous les prestataires de services définis par une marque de paiement comme éligibles au SAQ.

Remarque pour les commerçants et prestataires de services correspondant au SAQ D : Même si de nombreuses entreprises remplissant un SAQ D devront valider leur conformité pour chaque exigence PCI DSS, certaines sociétés dont les modèles économiques sont très spécifiques peuvent estimer que des exigences ne s'appliquent pas. Par exemple, on n'attend pas d'une entreprise n'utilisant jamais la technologie sans fil de valider la conformité aux paragraphes de la norme PCI DSS qui abordent cette question. Consulter les conseils spécifiques dans le SAQ D concerné pour en savoir plus sur l'exclusion d'autres exigences spécifiques.

Pour choisir un type de SAQ à l'aide d'un graphique, allez à la page 20 « Quel SAQ correspond le plus à mon environnement ? ».

Quel SAQ est le plus adapté à mon environnement ?