Matrice de responsabilité PCI DSS de Solutions Moneris

Version 4.0.1

Date de révision : juillet 9, 2025

Table des matières

Tableaux

Vue d’ensemble du document

Objectif

Le présent document vise à fournir des directives claires aux commerçantes et commerçants sur la manière de produire des rapports précis sur leur conformité aux normes de sécurité des données de l’industrie des cartes de paiement (« PCI DSS »). Il aide les commerçantes et commerçants à faire le lien entre leurs solutions particulières et les rapports appropriés, ce qui leur permet de comprendre les exigences qui les concernent. En fournissant des directives claires et des renseignements pratiques, ce document permet aux commerçantes et commerçants de suivre le processus de production de rapport avec confiance et précision.

Portée

Le présent document traite des exigences et des processus en matière de production de rapports liés à la conformité aux normes PCI DSS propres aux commerçantes et commerçants qui utilisent les solutions de paiement de Moneris. Il traite des questions suivantes :

- Terminaux – terminaux avec chiffrement point à point (« P2PE »), terminaux sans P2PE, terminaux d’ancienne génération
- Portails et interfaces Web
- Systèmes ayant recours à l’interface de programmation d’applications (« API ») pour passerelle de paiement de Moneris
- Solution de commerce électronique

Il fournit des conseils permettant de déterminer les bons rapports à produire, de comprendre les conditions d’admissibilité au questionnaire d’autoévaluation (« SAQ »), d’avoir recours aux directives du questionnaire SAQ pour produire un rapport de conformité (« ROC ») et de gérer la conformité dans des environnements complexes.

Public cible

Le présent document est destiné aux commerçantes et commerçants qui utilisent les solutions de traitement des paiements de Moneris, ainsi qu’au personnel d’administration des technologies de l’information (« TI »), aux responsables de la conformité, aux évaluatrices certifiées et évaluateurs certifiés de sécurité PCI (« QSA »), aux évaluatrices et évaluateurs de sécurité interne PCI (« ISA ») et au personnel responsable des rapports de conformité aux normes PCI.

Vue d’ensemble des rapports sur les normes PCI DSS

Le présent document peut être utilisé par les commerçantes et commerçants de Moneris pour remplir un questionnaire SAQ ou produire un ROC.

Processus détaillé permettant de déterminer la portée et les rapports applicables

Pour chaque produit utilisé par votre entreprise, vous devez indiquer :

1. la solution particulière que vous utilisez;
2. les exigences de PCI DSS qui s’appliquent à votre entreprise, les exigences qui sont satisfaites par Moneris, les exigences qui ne s’appliquent pas et les exigences dont la responsabilité est partagée;
3. le formulaire de conformité à utiliser, y compris la possibilité (et la manière) d’utiliser un questionnaire SAQ.

Pour les solutions prises en charge par d’autres tiers, la commerçante ou le commerçant doit s’assurer que le tiers fournit tous les documents de conformité nécessaires.

Utilisation d’un questionnaire SAQ ou d’un ROC

Les questionnaires d’autoévaluation PCI sont des formulaires de déclaration abrégés destinés aux petits commerces disposant d’environnements de paiement simples. Pour les commerçantes et commerçants admissibles, ils constituent également un moyen rapide et pratique de déterminer les exigences qui s’appliquent, quel que soit le formulaire de déclaration utilisé (c.-à-d. questionnaire SAQ ou ROC).

Remarque importante : Les commerçantes et commerçants qui doivent produire un ROC peuvent utiliser les questionnaires SAQ pour déterminer les exigences qui les concernent. Pour en savoir plus, consultez l’article 1331 de la FAQ de PCI (novembre 2024).

Dans la suite du présent document, nous ferons référence aux versions abrégées des questionnaires SAQ pour les exigences applicables, même pour les commerçantes et commerçants qui produisent un ROC conformément à l’article 1331 de la FAQ.

Admissibilité au questionnaire SAQ et environnements complexes

Votre entreprise ne peut avoir recours aux questionnaires SAQ abrégés que si elle satisfait aux critères d’admissibilité particuliers énoncés à la partie 2h de chaque questionnaire SAQ. Si votre environnement n’est pas admissible, vous devez utiliser un questionnaire SAQ D pour les commerçantes et commerçants ou produire un ROC complet.

Avant d’aborder les environnements complexes, certains formulaires, comme le questionnaire SAQ P2PE, comprennent des exigences en matière de traitement des données des titulaires de carte sur papier. Si le flux de données ne comprend pas le traitement des données des titulaires de carte sur papier, la mention « S. O. – aucune donnée de titulaire de carte sur papier » et une justification appropriée peuvent être indiquées pour ces exigences.

Les commerçantes et commerçants qui disposent de plusieurs environnements distincts pourraient devoir combiner leurs rapports dans un ROC ou un questionnaire SAQ D. Voici quelques exemples :

- Les commerces de détail avec flux de données distincts pour les transactions avec carte présente et le commerce électronique sont susceptibles de produire des rapports distincts.
- Les centres d'appels ayant recours à la téléphonie (p. ex., voix sur IP et terminaux de paiement dans un seul flux) ayant recours à des flux combinés ou mixtes devraient produire un seul rapport.

Les commerçantes et commerçants admissibles au questionnaire SAQ peuvent être en mesure de remplir des questionnaires SAQ spécialisés distincts si leur entité chargée de la conformité l'autorise.

Les commerçantes et commerçants ayant recours au ROC peuvent aussi produire des rapports distincts pour chaque flux de données. Toutefois, elles et ils sont plus susceptibles de regrouper toutes leurs constatations dans un seul ROC.

Les exclusions déclarées doivent être documentées séparément pour chaque formulaire. Par exemple, une commerçante ou un commerçant qui remplit un questionnaire SAQ P2PE pour les transactions avec carte présente et un questionnaire SAQ A pour le commerce électronique aura recours aux flux exclus dans la partie 2a et indiquera qu'il y a une évaluation distincte.

Produits de Moneris

Vous trouverez ci-dessous une description des processus permettant de déterminer les solutions de Moneris utilisées par votre entreprise, le formulaire de déclaration de base et les exigences qui s'appliquent à votre entreprise.

Terminaux et appareils de paiement

Déterminer la solution de terminal utilisée

Utilisez le tableau suivant pour déterminer à quel groupe appartient votre solution.

Tableau 1 : Déterminer le groupe de solutions de votre terminal

Groupe de terminaux	Nom du terminal	Description
Terminal Moneris P2PE	Terminal Moneris Go DX8000 Terminal Moneris Go EX8000 Clavier NIP P400 avec l'application POSPAD de Moneris	Les commerçantes et commerçants ayant adopté une solution P2PE qui utilisent ces produits et qui ont conservé et respecté le manuel d'instructions de la solution P2PE peuvent recevoir une certification P2PE. Remarque importante : Si vous n'avez pas adopté une solution P2PE et que vous disposez d'un de ces terminaux, veuillez trouver votre solution dans les rangées ci-dessous. Si vous ne savez pas si vous avez adopté une solution P2PE, veuillez communiquer avec Moneris.
Paiement rapide sur iPhone	iPhone	Ces solutions sont conformes à la norme PCI MPOC (« Mobile Payments on Commercial Off-The Shelf »). — Paiement rapide sur iPhone d'Apple, nº de référence 2025-01597.001

Groupe de terminaux	Nom du terminal	Description
Terminaux de Moneris	Terminal Moneris Go A35 Terminal Moneris Go A920 Terminal Moneris Go DX8000 Terminal Moneris Go EX8000 Terminal Moneris Go IM30 Clavier NIP e355 avec l'application POSPAD de Moneris Clavier NIP iCMP avec l'application POSPAD de Moneris Clavier NIP iPP320 avec l'application POSPAD de Moneris Clavier NIP P400 avec l'application POSPAD de Moneris Appareil UX300 avec Direct Connect Appareil UX301 avec Direct Connect Appareil UX410 avec Direct Connect Terminal Desk/5000 Moneris Core Terminal Move/5000 Moneris Core Terminal V400c Moneris Core Terminal V400m Moneris Core	Les commerçantes et commerçants n'ayant pas adopté une solution P2PE qui utilisent ces produits conçus et développés par Moneris avec des appareils conformes à la norme de sécurité des transactions par NIP (« PTS ») tirent parti d'un chiffrement robuste sans accès aux données des titulaires de carte et sans possibilité de désactiver ou de compromettre le chiffrement, en plus d'avoir accès à des configurations sécurisées prêtes à l'emploi et plus encore. Ces terminaux de Moneris se déclinent en quatre familles : — GO — POSPAD — Direct Connect — Core Caractéristiques de conception des terminaux de Moneris : — Les systèmes connectés, comme les points de vente (« PDV »), ne peuvent recevoir ni déchiffrer les données des titulaires de carte. — Le terminal ne peut afficher ou exporter les données des titulaires de carte. — Les contrôles de sécurité de sécurité du terminal ne peuvent pas être désactivés. Aucun accès à distance n'est possible.
Terminaux d'ancienne génération de Moneris	Terminal iCT250 de Moneris Terminal iWL220 de Moneris Terminal VX 520 de Moneris Terminal VX 820 de Moneris	Les commerçantes et commerçants qui disposent de ces terminaux conformes à la norme PTS devront satisfaire à des exigences supplémentaires des normes PCI DSS. Remarque : Ces appareils sont obsolètes et ont été abandonnés.

Groupe de terminaux	Nom du terminal	Description
Terminaux non fournis par Moneris	S. O.	Les commerçantes et commerçants qui achètent ou louent des terminaux et des produits non fournis par Moneris sont entièrement responsables de déterminer la conformité de ces appareils et de tous les systèmes et réseaux connectés. Il s'agit notamment de distributeurs de carburant automatisés et de bornes interactives, ou encore de solutions d'entreprises de services de paiement. Moneris n'assume aucune responsabilité à l'égard de ces solutions et n'a pas déterminé les exigences des normes PCI DSS qui s'appliquent aux appareils tiers.

Aux fins de productions des rapports de conformité, vous aurez aussi besoin des détails des approbations de PCI applicables, qui se trouvent aux endroits suivants :

Tableau 2 : Emplacement des renseignements sur l'approbation de PCI

Groupe de terminaux	Description
Terminal Moneris P2PE	– Pour trouver les renseignements sur les approbations PTS et P2PE, veuillez consulter le manuel de mise en œuvre du chiffrement point à point propre à votre solution.
Paiement rapide sur iPhone	– Paiement rapide sur iPhone d'Apple – De plus, Moneris travaille actuellement à l'obtention des certifications MPOC et actualisera ce document dès leur obtention.
Terminaux de Moneris	– Pour obtenir des renseignements sur l'approbation PTS des terminaux Moneris Go, veuillez consulter le site https://soutien.moneris.com/topic/solutions-moneris-go/moneris-go. Pour les autres terminaux de Moneris, consultez le site https://soutien.moneris.com/topic/systemes-de-pdv/.
Terminaux d'ancienne génération de Moneris	– Pour obtenir des renseignements sur l'approbation PTS, veuillez consulter le site https://soutien.moneris.com/topic/systemes-de-pdv/.
Terminaux non fournis par Moneris	– Communiquez avec le fournisseur de votre terminal en ce qui a trait à l'approbation relative à la norme PTS et à toute autre approbation applicable au titre des normes PCI.

Exigences et responsabilités applicables à l'égard du terminal

Le tableau ci-dessous indique, pour chaque groupe de terminaux, les exigences de la norme PCI DSS qui s'appliquent ou ne s'appliquent pas. Cela vous permet de produire un ROC ou de remplir un questionnaire SAQ D ou l'un des questionnaires SAQ abrégés (voir la section suivante).

Afin de simplifier l'interprétation et l'actualisation de ces tableaux, les responsabilités peuvent être définies selon les questionnaires SAQ, et des exigences supplémentaires peuvent s'appliquer aux propriétaires de commerce ou à Moneris.

Lorsqu'un groupe de terminaux est assujetti à des exigences qui s'ajoutent à celles d'un questionnaire SAQ (p. ex., les terminaux Moneris qui répondent aux exigences du questionnaire SAQ P2PE) et qu'il y a un critère d'admissibilité pour l'utilisation d'une solution PCI approuvée particulière (p. ex., P2PE), le critère doit être interprété comme exigeant la solution Moneris particulière. Tous les autres critères d'admissibilité doivent être satisfaits.

Lorsque les exigences indiquent Moneris ou S. O., vous devez indiquer que l'exigence ne s'applique pas. Par exemple, si vous documentez votre conformité pour une solution de « terminaux de Moneris » dans un questionnaire SAQ D, vous devez satisfaire à toutes les exigences énumérées dans le questionnaire SAQ P2PE, ainsi qu'aux exigences supplémentaires énumérées ci-dessous. Pour toutes les autres exigences du questionnaire SAQ D, indiquez « S. O. » et la raison « S. O., satisfait par Moneris » ou « S. O. pour la solution ».

Tableau 3 : Exigences applicables par groupe de terminaux

Groupe de terminaux	Applicables au commerce	Moneris ou S. O.	Responsabilités partagées
Terminal Moneris P2PE	– Questionnaire SAQ P2PE		
Paiement rapide sur iPhone	– Toutes les exigences du questionnaire SAQ MPOC (voir la note ci-dessous)	– Toutes les autres exigences ne s'appliquent pas à la commerçante ou au commerçant.	– Aucune
Terminaux de Moneris	– Toutes les exigences du questionnaire SAQ P2PE, ainsi que 1.2.3 et 1.2.4.	– Toutes les autres exigences ne s'appliquent pas à la commerçante ou au commerçant. — Moneris est responsable des modifications mineures apportées à la solution.	– Lorsque des modifications manuelles sont nécessaires, les commerçantes et commerçants doivent assurer la coordination des changements avec Moneris.

Groupe de terminaux	Applicables au commerce	Moneris ou S. O.	Responsabilités partagées
Terminaux d'ancienne génération de Moneris	– Toutes les exigences du questionnaire SAQ B-IP, ainsi que 1.2.2, 1.2.3, 1.2.4, 1.4.1, 1.4.2, 3.2.1, 4.2.2, 6.5.1 et 6.5.2.	– Les exigences suivantes de ce questionnaire SAQ ne s'appliquent pas : 1.2.5, 1.2.6, 2.2.7, 3.3.1, 3.3.1.1, 3.3.1.3, 4.2.1, 6.3.1, 7.2.2, 8.2.2, 8.2.7 et 8.4.3. – Pour les terminaux autonomes avec connexion cellulaire, les exigences 1.3.x et 1.4.x ne sont pas applicables. – Toutes les autres exigences ne s'appliquent pas à la commerçante ou au commerçant. – Moneris est responsable des modifications mineures apportées à la solution.	– Lorsque des modifications manuelles sont nécessaires, les commerçantes et commerçants doivent assurer la coordination des changements avec Moneris.
Terminaux non fournis par Moneris	– Questionnaire SAQ D — Les systèmes connectés sont visés.	– Aucune	– Doit faire l'objet d'une approbation par Moneris et d'une certification opérationnelle.

Remarques :

- Paiement rapide sur iPhone : les solutions nécessitant une approbation PCI MPOC peuvent être déclarées dans le questionnaire SAQ MPOC. Toute solution approuvée par Moneris qui n'est pas encore répertoriée dans la liste des solutions PCI MPOC doit être déclarée dans le questionnaire SAQ D en indiquant les exigences qui ne s'appliquent pas conformément aux directives ci-dessus.
- Les livres blancs de Moneris recommandent fortement l'utilisation de pare-feu pour protéger les appareils du groupe « terminaux de Moneris », mais ne les exigent pas pour la norme PCI DSS.

Déterminer votre modèle de rapport de base (SAQ)

Utilisez le tableau ci-dessous pour comprendre les modes de communication pris en charge par les terminaux de Moneris et les terminaux d'ancienne génération de Moneris. Ceux-ci seront utilisés de concert avec le tableau suivant pour déterminer le questionnaire SAQ de PCI adéquat.

Vous n'avez pas besoin de ce tableau si vous disposez d'un terminal de Moneris avec P2PE validé ou d'une solution de paiement rapide sur iPhone.

Tableau 4 : Déterminer le modèle de rapport : partie 1 – modes de communication

Mode	Groupe ou famille de terminaux	Description du mode
Connexion commutée	Terminaux d'ancienne génération de Moneris	Terminaux autonomes qui se connectent à Moneris uniquement au moyen d'une connexion commutée (non VoIP).
Solution autonome	Terminaux de Moneris (Go), terminaux d'ancienne génération de Moneris	Terminaux autonomes qui se connectent à Moneris au moyen du protocole TCP/IP (« Transmission Control Protocol/Internet Protocol ») ou d'un réseau Wi-Fi ou cellulaire.
Infonuagique	Terminaux de Moneris (Go, POSPAD)	Terminaux autonomes qui se connectent à Moneris au moyen du protocole TCP ou d'un réseau Wi-Fi ou cellulaire et qui interagissent indirectement avec le PDV de la commerçante ou du commerçant par l'intermédiaire du système de PDV infonuagique de Moneris et de jetons de jumelage.
Communication directe avec le serveur de traitement et solution semi-intégrée d'ancienne génération	Terminaux de Moneris (Go, POSPAD, Direct Connect, autres produits Moneris Core), terminaux d'ancienne génération de Moneris	Terminaux semi-intégrés avec connexion réseau directe à Moneris pour l'autorisation et autres connexions (p. ex., port série, bus série universel [« USB »], protocole TCP/IP, Wi-Fi ou Bluetooth) aux systèmes des commerçantes et commerçants afin de prendre en charge l'intégration des PDV.
Transfert direct sécurisé	Terminaux de Moneris (POSPAD)	Terminaux entièrement intégrés qui chiffrent toutes les données des titulaires de carte. Le terminal ne se connecte pas directement à Moneris. Le PDV connecté facilite plutôt la transmission des données chiffrées des titulaires de carte à Moneris, mais ne reçoit pas et ne peut pas déchiffrer les données des titulaires de carte.

Mode	Groupe ou famille de terminaux	Description du mode
Application à application	Terminaux de Moneris (Go)	Les terminaux Moneris Go qui prennent en charge l'intégration d'application à application permettent l'inclusion d'applications tierces sans fonction de traitement des paiements (c.-à-d. sans accès aux données des titulaires de carte) qui s'exécutent dans le terminal parallèlement à l'application de paiement de Moneris. Ce mode de communication ressemble au mode de communication directe avec le serveur de traitement et les rapports de conformité sont produits de la même manière. Les applications tierces doivent faire l'objet d'une signature et d'une attribution par Moneris et peuvent nécessiter un examen de sécurité supplémentaire avant d'être acceptées.

Utilisez ce tableau pour déterminer le questionnaire SAQ de base à utiliser pour déclarer la conformité en fonction du mode de communication de la solution.

Vous n'avez pas besoin de ce tableau si vous disposez d'un terminal de Moneris avec P2PE validé.

Tableau 5 : Déterminer le modèle de rapport : partie 2 – questionnaire SAQ

Mode de communication	Questionnaire SAQ
Autonome (connexion commutée)	B
Autonome (cellulaire)	B-IP
Autonome (réseau ou Wi-Fi)	B-IP
Communication directe avec le serveur de traitement (port série ou USB)	B-IP
Communication directe avec le serveur de traitement (réseau ou Wi-Fi) et solution semi-intégrée d'ancienne génération	D
Infonuagique	B-IP
Transfert direct sécurisé	D
Application à application	D

Veuillez noter qu'il n'y a pas de questionnaire SAQ abrégé applicable aux terminaux de paiement semi-intégrés (p. ex., communication directe avec le serveur de traitement [réseau ou Wi-Fi]). Ni le questionnaire SAQ B-IP ni le questionnaire SAQ C ne peuvent être utilisés, car ils ne satisfont pas aux critères d'admissibilité « non connecté à d'autres systèmes au sein de l'environnement de la commerçante ou du commerçant ». Le questionnaire SAQ D est requis pour les commerçantes et les commerçants qui ne stockent pas de données de compte électroniquement et qui ne répondent pas aux critères des autres questionnaires SAQ.

Exemple concret

Voyons un exemple concret d'un commerce de Moneris qui produit un rapport de conformité à l'aide de la méthode ci-dessus. Bien qu'une personne ayant suivi une formation sur les normes PCI DSS devrait être en mesure de suivre le processus, cela peut s'avérer difficile pour quelqu'un qui n'a pas autant d'expérience.

Un commerce fictif, Cadeaux ACME, gère une petite chaîne de magasins physiques. Ces magasins ont récemment mis en œuvre des terminaux Moneris Go DX8000 autonomes connectés à leur réseau local (« RL »). Cet exemple illustre un flux de données de titulaire de carte simple, sans acceptation de carte par envoi postal, par téléphone ou par commerce électronique, et sans utilisation d'une solution de terminal virtuel pour saisir les données des titulaires de carte (pour en savoir plus sur les flux plus complexes, voir la section Admissibilité au questionnaire SAQ et environnements complexes ci-dessus).

1. Le terminal DX8000 fait partie du groupe « terminaux de Moneris », au titre duquel la commerçante ou le commerçant est responsable de toutes les exigences du questionnaire SAQ P2PE, ainsi que des exigences 1.2.3 et 1.2.4.
2. Le mode de communication « Autonome (réseau ou Wi-Fi) » doit être déclaré dans un questionnaire SAQ B-IP.
3. La commerçante ou le commerçant doit récupérer les questionnaires SAQ B-IP et SAQ P2PE actuels dans la bibliothèque de documents de PCI.
4. Consultez les critères d'admissibilité du questionnaire SAQ B-IP (partie 2h). En outre, il doit s'agir d'un terminal appartenant au groupe « terminaux de Moneris ». Si l'un des critères d'admissibilité n'est pas satisfait, vous devrez produire un rapport à l'aide du questionnaire SAQ D – Commerçant.
5. À l'aide du questionnaire SAQ approprié (B-IP ou D – Commerçant), suivez ces étapes :
    a) Remplissez le sommaire, y compris les références PCI PTS de vos terminaux.
    b) À la section 2, vous répondrez à toutes les questions figurant dans le questionnaire SAQ P2PE, ainsi qu'aux exigences supplémentaires relevées.
    c) Toutes les autres exigences (p. ex., 1.2.5) peuvent être désignées « S. O. » et énumérées à l'annexe C, « Explication des exigences indiquées comme non applicables », avec la raison « S. O., satisfait par Moneris » ou « S. O. pour la solution ». Modifiez ensuite la partie 2g du sommaire.

Portails et interfaces Web

Utilisez le tableau suivant pour déterminer à quel groupe appartient votre solution.

Tableau 6 : Déterminer les fonctionnalités de votre portail visées par les normes PCI DSS

Solution de portail	Groupe de portails
Centre de ressources pour commerçants	Portails avec terminaux virtuels permettant la saisie des données des titulaires de cartes à partir des systèmes des propriétaires de commerce.
Portail Moneris Go	Comprend l'enregistrement des cartes et des jetons dans la chambre forte.
Marchand Direct	Portails qui ne permettent pas la saisie des données des titulaires de carte ni l'accès à celle-ci.

Tableau 7 : Exigences applicables pour les solutions de portail

Groupe de portails	Applicables au commerce	Moneris ou S. O.	Responsabilités partagées
Portails avec terminaux virtuels	Utilisez le questionnaire SAQ C-VT pour les postes de travail et les systèmes des commerçantes et commerçants	Moneris est entièrement responsable de l'infrastructure du portail.	Aucune
Portails sans accès aux données des titulaires de carte	Les postes de travail et les systèmes des commerçantes et commerçants ne sont pas visés par les normes PCI DSS.	Moneris est entièrement responsable de l'infrastructure du portail.	Aucune

Remarques :

- La commerçante ou le commerçant peut être assujetti à des exigences de sécurité non liées aux normes PCI DSS en ce qui concerne les fonctionnalités du portail.
- Les responsabilités ci-dessus ne prévalent pas sur les obligations légales et ententes juridiques antérieures relatives aux interfaces personnalisées qui pourraient exister.

Systèmes utilisant les API de la passerelle de paiement de Moneris

Moneris fournit plusieurs solutions d'API qui peuvent être utilisées avec les passerelles de paiement suivantes :

Tableau 8 : Exigences et responsabilités partagées applicables aux API de paiement

API de passerelle	Applicables au commerce	Moneris ou S. O.	Responsabilités partagées
IPGate, Passerelle Moneris, passerelle de terminal, passerelle pour le transport en commun	– Les commerçantes et commerçants et les tiers sont entièrement responsables de tout code d'application qui consulte les données des titulaires de carte ou les données d'authentification confidentielles et qui utilise les API des passerelles de Moneris ou s'intègre aux passerelles de Moneris. – Les logiciels de paiement tiers peuvent nécessiter une approbation au moyen d'une évaluation de la sécurité logicielle de PCI.	– Moneris est responsable des documents de spécification et du développement sécurisé du code d'API qu'elle fournit aux commerçantes et commerçants afin que ces API puissent être intégrées à leurs applications ou à celles de tiers. – Moneris est entièrement responsable de l'infrastructure des passerelles de paiement.	– Les commerçantes et commerçants doivent coordonner les modifications et les mises à jour de leurs applications avec Moneris, y compris pour toute modification de sécurité apportée aux API.

Commerce électronique Moneris Checkout

Responsabilités

Les tableaux suivants présentent les différentes solutions de commerce électronique utilisées par les commerçantes et commerçants de Moneris et le cadre relatif aux rapports de conformité applicable à chacune d'entre elles.

Tableau 9 : Déterminer le type de mise en œuvre du commerce électronique

Solution		Questionnaire SAQ
Moneris Checkout	Le panier d'achat de la commerçante ou du commerçant appelle le script Moneris Checkout, ce qui crée un « iframe » contenant le formulaire qui envoie directement à Moneris toutes les données confidentielles relatives à la titulaire ou au titulaire de carte et à l'authentification (p. ex., le numéro de carte, la date d'expiration, les codes de sécurité).	A
Moneris Checkout avec panier d'achat hébergé	La commerçante ou le commerçant utilise une intégration tierce à Moneris Checkout pour son panier d'achat. Le panier d'achat comprend un lien ou une redirection vers une page hébergée par Moneris qui génère l'« iframe » de Moneris Checkout.	A
Panier d'achat de Moneris avec une entreprise de services de paiement tierce	La solution de commerce électronique de la commerçante ou du commerçant utilise l'« iframe », le lien, la redirection, le formulaire direct POST ou la passerelle d'une entreprise de services de paiement tierce. Le formulaire de déclaration applicable à la commerçante ou au commerçant sera déterminé en fonction du mécanisme qui transmet les données des titulaires de carte au tiers.	A, A-EP D
Page de paiement de la commerçante ou du commerçant	La solution de commerce électronique de la commerçante ou du commerçant reçoit toutes les données des titulaires de carte et les transmet directement ou indirectement à Moneris à l'aide d'une des API de passerelle (voir ci-dessus) ou d'une entreprise de services de paiement tierce.	D

Tableau 10 : Responsabilités relatives à Moneris Checkout

Solution	Applicables au commerce	Moneris ou S. O.	Responsabilités partagées
Moneris Checkout	– La commerçante ou le commerçant est responsable de son panier d'achat et doit protéger le script Moneris Checkout.	– Moneris est responsable du développement et du contenu du script Moneris Checkout et des passerelles de Moneris qui reçoivent les données des titulaires de carte.	– Voir la remarque ci-dessous.
Moneris Checkout avec panier d'achat hébergé	– La commerçante ou le commerçant est responsable de son panier d'achat et doit protéger le lien vers Moneris Checkout.	– Moneris est responsable du développement et du contenu du script Moneris Checkout et des passerelles de Moneris qui reçoivent les données des titulaires de carte. Moneris est aussi responsable de la protection du script de Moneris Checkout.	– Voir la remarque ci-dessous.
Panier d'achat de Moneris avec une entreprise de services de paiement tierce, page de paiement de la commerçante ou du commerçant	– La commerçante ou le commerçant est responsable de la conformité de sa solution de commerce électronique et de tout prestataire de services tiers.	– Aucune	– Aucune

Remarques :

— Moneris Checkout n'utilise pas de formulaires direct POST pour transmettre les données des titulaires de carte.

- Pour consulter la documentation du produit Moneris Checkout, consultez le site https://developer.moneris.com/ (en anglais seulement).
- Pour les exigences 6.4.3 et 11.6.1, les responsabilités sont essentiellement partagées. Moneris est responsable de la mise en œuvre de ces contrôles dans l'« iframe » de Moneris Checkout, et l'entreprise cliente est responsable de ces exigences en ce qui a trait à son panier d'achat (c.-à-d. qu'elle doit protéger le script qu'elle invoque pour faire appel à Moneris Checkout).

Évolution des lignes directrices de PCI DSS relatives au commerce électronique

La norme PCI DSS v4.0 a introduit deux nouvelles exigences, 6.4.3 et 11.6.1, qui sont entrées en vigueur en avril 2025 et qui visent à protéger l'intégrité de JavaScript et à lutter contre les menaces d'attaques par clonage électronique de cartes (également appelées « Magecart »). Les directives précises relatives à ces exigences sont techniques et évoluent constamment. Il n'est pas rare que les nouvelles exigences de PCI DSS fassent l'objet d'ajustements après leur mise en place.

Le rapport de conformité PCI DSS à utiliser et les nouvelles exigences applicables dépendent des mécanismes utilisés dans le cadre du commerce électronique.

- Les paniers d'achat ayant recours à des mécanismes comme les « iframe », les liens ou les redirections créent un nouveau modèle DOM (« Document Object Model ») dans le navigateur des titulaires de carte, empêchant ainsi les scripts de leurs pages d'intercepter les renseignements saisis dans les champs de paiement.
- Différents mécanismes peuvent être altérés de manière dynamique dans le navigateur des titulaires de carte par des scripts JavaScript. Les mécanismes reliant le panier d'achat de la commerçante ou du commerçant et la page de paiement de l'entreprise de services de paiement nécessitent des contrôles anti-altération.

Vous trouverez ci-dessous une liste des directives de PCI disponibles au moment de la rédaction du présent document. Nous recommandons fortement aux commerçantes et commerçants de vérifier qu'elles et ils suivent les dernières directives en vigueur.

Remarques :

- Les entreprises qui remplissent le questionnaire SAQ A n'ont pas besoin de répondre directement aux exigences 6.4.3 et 11.6.1, mais doivent répondre à la question d'admissibilité « Le commerçant a confirmé que son site n'est pas vulnérable aux attaques de scripts pouvant affecter son(ses) système(s) de commerce électronique » (voir le questionnaire SAQ A r1).
- Les entreprises qui remplissent une ROC en fonction de l'applicabilité du questionnaire SAQ A doivent répondre directement aux exigences 6.4.3 et 11.6.1 (voir les directives de PCI DSS relatives aux exigences 6.4.3 et 11.6.1 v1.0).
- Tous les mécanismes de liaison ne nécessitent pas nécessairement des contrôles d'intégrité (p. ex., certains types de redirections). Toutefois, cela peut changer. Nous recommandons aux commerçantes et commerçants de revoir les directives actuelles, leur niveau de risque et d'examiner attentivement les contrôles d'intégrité pour tous les mécanismes de liaison.

Vous trouverez ci-dessous une liste des directives et des FAQ de PCI relatives au commerce électronique disponibles au moment de la rédaction du présent document. Nous recommandons fortement aux commerçantes et commerçants de vérifier qu'elles et ils suivent les dernières directives en vigueur.

- Directives de PCI DSS relatives aux exigences 6.4.3 et 11.6.1 v1.0 (avril 2025) (« Guidance for PCI DSS Requirements 6.4.3 and 11.6.1 v1.0R1 (April 2025) », en anglais seulement)

- FAQ 1592 (mars 2025) Les fournisseurs de scripts tiers pour les environnements de commerce électronique sont-ils considérés comme des fournisseurs de services tiers au sens des exigences 12.8 et 12.9 des normes PCI DSS? (« FAQ 1592 (Mar 2025) Are providers of third-party scripts for e-commerce environments considered third-party service providers for PCI DSS Requirements 12.8 and 12.9? », en anglais seulement)
- FAQ 1588 (mars 2025) Comment un commerce en ligne peut-il satisfaire aux critères d'admissibilité du questionnaire SAQ A en ce qui a trait aux scripts? (« FAQ 1588 (Mar 2025) How does an e-commerce merchant meet the SAQ A eligibility criteria for scripts? », en anglais seulement)
- FAQ 1581 (août 2024) Comment l'exigence 6.4.3 des normes PCI DSS s'applique-t-elle aux scripts 3DS appelés depuis la page de paiement d'un commerce dans le cadre du traitement 3DS? (« FAQ 1581 (Aug 2024) How does PCI DSS Requirement 6.4.3 apply to 3DS scripts called from a merchant check-out page as part of 3DS processing? », en anglais seulement)
- Meilleures pratiques en matière de sécurité pour le commerce électronique (avril 2017) (« Best Practices for Securing E-commerce (Apr 2017) », en anglais seulement)
- FAQ 1438 (novembre 2016) Comment la page de paiement est-elle déterminée pour les commerces admissibles au questionnaire SAQ A qui utilisent les « iframe »? (« FAQ 1438 (Nov 2016) How is the payment page determined for SAQ A merchants using iframe? », en anglais seulement)
- FAQ 1291 (août 2015) Pourquoi le questionnaire SAQ A-EP est-il utilisé pour la méthode direct POST, tandis que le questionnaire SAQ A est utilisé pour les « iframe » et les adresses URL de redirection? (« FAQ 1291 (Aug 2015) Why is SAQ A-EP used for Direct Post while SAQ A is used for iFrame or URL redirect? », en anglais seulement)
- FAQ 1293 (juin 2014) Si la mise en œuvre du commerce électronique d'un commerce répond aux critères selon lesquels tous les éléments des pages de paiement proviennent d'un fournisseur de services conforme à la norme PCI DSS, le commerce est-il admissible au questionnaire SAQ A ou au questionnaire SAQ A-EP? (« FAQ 1293 (Jun 2014) If a merchant's e-commerce implementation meets the criteria that all elements of payment pages originate from a PCI DSS compliant service provider, is the merchant eligible to complete SAQ A or SAQ A-EP? », en anglais seulement)

Aide relative aux normes PCI DSS

Si votre entreprise a besoin d'aide pour interpréter les exigences des normes PCI DSS, mener des activités de validation, produire la documentation de conformité ou si elle souhaite obtenir d'autres conseils, veuillez communiquer avec une évaluatrice qualifiée ou un évaluateur qualifié de sécurité (« QSA ») ou une évaluatrice ou un évaluateur de sécurité interne (« ISA ») agréé de votre entreprise, le cas échéant.

Références de PCI

Normes PCI DSS et questionnaires SAQ : https://www.pcisecuritystandards.org/lang/fr-fr/. En particulier, consultez les documents SAQ Instructions et Directives, SAQ A, SAQ A-EP, SAQ P2PE, SAQ MPOC, SAQ B, SAQ B-IP, SAQ C, SAQ C-VT et SAQ D, publiés ou actualisés entre octobre 2024 et avril 2025.

Foire aux questions PCI : https://www.pcisecuritystandards.org/faqs/ (en anglais seulement)

Répertoires PCI

Solutions P2PE : https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions (en anglais seulement)

Paiements mobiles et solutions commerciales sur étagère : https://listings.pcisecuritystandards.org/assessors_and_solutions/mpoc_solutions (en anglais seulement)

Logiciels sécurisés : https://listings.pcisecuritystandards.org/assessors_and_solutions/payment_software (en anglais seulement)

Solutions conformes à la norme PA DSS : https://listings.pcisecuritystandards.org/assessors_and_solutions/payment_applications (en anglais seulement)

Appareils conformes à la norme PTS (à jour) : https://listings.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices (en anglais seulement)

Appareils conformes à la norme PTS (expirés ou ancienne génération) : https://listings.pcisecuritystandards.org/assessors_and_solutions/approved_pin_transaction_security_expired (en anglais seulement)

Remarque :

- Les produits dont la conformité à la norme PCI est expirée pourraient toujours être acceptables pour les mises en œuvre préexistantes.

Communiquer avec Moneris

Si vous avez des questions concernant les solutions présentées dans ce document ou les solutions de Moneris, veuillez consulter les ressources suivantes.

Pour en savoir plus sur les solutions, consultez les ressources suivantes de Moneris mentionnées dans ce document :

- Terminaux Moneris Go : https://soutien.moneris.com/topic/solutions-moneris-go/moneris-go
- Terminaux de Moneries : https://soutien.moneris.com/topic/systemes-de-pdv/
- Ressources de Moneris à l'intention des développeuses et développeurs, y compris le centre de ressources pour commerçants, le terminal virtuel, les API de passerelles et Moneris Checkout : https://developer.moneris.com/ (en anglais seulement)

Si vous avez des questions sur le présent document de conformité, veuillez communiquer avec votre gestionnaire de compte de Moneris ou envoyer un courriel à l'adresse PCIDSS@moneris.com.

Pour toute autre demande, consultez notre page « Nous joindre » https://www.moneris.com/fr-ca/soutien/contact.

Définitions et acronymes

Pour obtenir la liste complète des termes et acronymes du glossaire de PCI, veuillez consulter le glossaire officiel (en anglais seulement) du PCI Security Standards Council.

- PCI DSS : normes de sécurité des données de l'industrie des cartes de paiement (« Payment Card Industry Data Security Standard »)
- P2PE : norme de chiffrement point à point (« Point-to-Point Encryption ») et produits P2PE approuvés
- MPOC : norme relative aux solutions de paiements mobiles commerciales sur étagère (Mobile Payments on Commercial Off-the-Shelf)
- ROC : rapport de conformité (« Report on Compliance »)
- SAQ : questionnaire d'autoévaluation (« Self-Assessment Questionnaire ») pour la production de rapports de conformité des petits commerces
- Admissibilité au questionnaire SAQ : critères d'admissibilité qui doivent être remplis pour utiliser chaque questionnaire SAQ particulier aux fins de production de rapport
- PDV : point de vente, généralement un système de caisse enregistreuse électronique
- PTS : norme de sécurité des transactions par NIP (« PIN Transaction Security »), une norme relative aux terminaux et appareils de paiement
- API : interface de programmation d'applications (« Application Programming Interface »)
- QSA : évaluatrice ou évaluateur qualifié de sécurité (« Qualified Security Assessor »)
- ISA : évaluatrice ou évaluateur de sécurité interne (« Internal Security Assessor »)

Commented [PD1]: Note from translator:
We have removed acronyms that weren't used in the document and those for which we haven't used acronyms in French for clarity.

Historique des examens et des révisions.

Version	Date	Description
1.0	24-04-25	Version initiale pour la norme PCI DSS 4.0.1
1.0.1	05-05-25	Clarifications mineures et précisions. Ajout de la fonction Paiement rapide sur iPhone.