Industrie des cartes de paiement (PCI)

Norme de sécurité des données

Attestation de conformité
Évaluations sur site – Prestataires de services

Version 3.2

Avril 2016

Section 1 : Informations relatives à l'évaluation

Instructions de transmission

Cette attestation de conformité doit être complétée comme une déclaration des résultats de l'auto-évaluation du prestataire de service vis-à-vis des *Conditions et procédures d'évaluation de sécurité de la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS).* Complétez toutes les sections : Le prestataire de service est responsable de s'assurer que chaque section est remplie par les parties pertinentes, le cas échéant. Contacter la marque de paiement qui effectue la demande pour déterminer les procédures de rapport et de demande.

Partie 1. Informations sur l'évaluateur de sécurité qualifié et le prestataire de services						
Partie 1a. Informations sur le prestataire de services						
Nom de la société :			DBA (nom commercial) :			
Nom du contact :			Poste occupé :			
Téléphone :			E-mail :			
Adresse professionnelle :			Ville :			
État/province :		Pays :		Code postal :		
URL :						

Partie 1b. Informations sur la société QSA (le cas échéant)					
Nom de la société :					
Nom du principal contact QSA :		Poste occupé :			
Téléphone :		E-mail :			
Adresse professionnelle :		Ville :			
État/province :		Pays :		Code postal :	
URL :					

Partie 2. Résumé

Partie 2a. Vérification de la portée

Services qui étaient INCLUS dans la portée de l'évaluation PCI DSS (Cocher toutes les mentions applicables) :

Nom du ou des services évalués :		
Type du ou des services évalués :		
Fournisseur d'hébergement : ☐ Applications/logiciel ☐ Matériel ☐ Infrastructure/Réseau ☐ Espace physique (co-positionnement) ☐ Stockage ☐ Web ☐ Services de sécurité ☐ Prestataire de services d'hébergement sécurisé 3D ☐ Fournisseur d'hébergement partagé ☐ Autre hébergement (spécifier) :	**Services gérés (spécifier) :** ☐ Services de sécurité de systèmes ☐ Soutien IT ☐ Sécurité physique ☐ Système de gestion de terminal ☐ Autres services (spécifier) :	**Traitement des paiements :** ☐ POS/Carte absente ☐ Internet/Commerce électronique ☐ MOTO/Centre d'appel ☐ ATM ☐ Autre traitement (spécifier) :
☐ Gestion des comptes	☐ Fraudes et rejets de débit	☐ Passerelle de paiement/Commutateur
☐ Services administratifs	☐ Traitement des émetteurs	☐ Services prépayés
☐ Gestion de la facturation	☐ Programmes de fidélité	☐ Gestion des dossiers
☐ Compensation et règlement	☐ Services aux commerçants	☐ Paiements des impôts/du gouvernement
☐ Prestataire réseau		
☐ Autres (spécifier) :		

***Remarque** : Ces catégories sont uniquement fournies à titre d'aide et elles ne sont pas destinées à limiter ou à prédéterminer la description des services d'une entité. Si vous pensez que ces catégories ne s'appliquent pas à votre service, choisissez « Autres ». Si vous n'êtes pas sûr si une catégorie pourrait s'appliquer à votre service, consultez la marque de paiement pertinente.*

Partie 2a. Vérification de la portée *(suite)*		
Les services qui sont fournis par le prestataire de service, mais qui n'étaient PAS INCLUS dans la portée de l'évaluation PCI DSS (Cocher toutes les mentions applicables) :		
Nom du ou des services non évalués :		
Type du ou des services non évalués :		
Fournisseur d'hébergement : ☐ Applications/logiciel ☐ Matériel ☐ Infrastructure/Réseau ☐ Espace physique (co-positionnement) ☐ Stockage ☐ Web ☐ Services de sécurité ☐ Prestataire de services d'hébergement sécurisé 3D ☐ Fournisseur d'hébergement partagé ☐ Autre hébergement (spécifier) :	**Services gérés (spécifier) :** ☐ Services de sécurité de systèmes ☐ Soutien IT ☐ Sécurité physique ☐ Système de gestion de terminal ☐ Autres services (spécifier) :	**Traitement des paiements :** ☐ POS/Carte absente ☐ Internet/Commerce électronique ☐ MOTO/Centre d'appel ☐ ATM ☐ Autre traitement (spécifier) :
☐ Gestion des comptes	☐ Fraudes et rejets de débit	☐ Passerelle de paiement/Commutateur
☐ Services administratifs	☐ Traitement des émetteurs	☐ Services prépayés
☐ Gestion de la facturation	☐ Programmes de fidélité	☐ Gestion des dossiers
☐ Compensation et règlement	☐ Services aux commerçants	☐ Paiements des impôts/du gouvernement
☐ Prestataire réseau		
☐ Autres (spécifier) :		
Donner une brève description de la raison pour laquelle les services sélectionnés n'ont pas été inclus dans l'évaluation :		

Partie 2b. Description de l'entreprise de carte de paiement	
Décrire comment et dans quelle mesure votre entreprise stocke, traite et/ou transmet des données de titulaires de carte.	
Décrire comment et dans quelle mesure votre entreprise est impliquée ou à la capacité d'avoir une influence sur la sécurité des données de titulaires de carte.	

Partie 2c. Emplacements

Énumérer les types de locaux (par exemple : commerces de détail, siège social, centre de données, centre d'appel, etc.) et un résumé des emplacements inclus dans l'examen PCI DSS.

Type de local :	Nombre de locaux de ce type	Emplacement(s) du local (ville, pays) :
Exemple : Commerces de détail	*3*	*Boston, Massachusetts, États-Unis*

Partie 2d. Applications de paiement

Est-ce que l'organisation utilise une ou plusieurs applications de paiement ? ☐ Oui ☐ Non

Fournir les informations suivantes concernant les applications de paiement utilisées par votre organisation :

Nom de l'application de paiement	Numéro de version	Vendeur de l'application	L'application est-elle listée PA-DSS ?	Date d'expiration du listing PA-DSS (le cas échéant)
			☐ Oui ☐ Non	
			☐ Oui ☐ Non	
			☐ Oui ☐ Non	
			☐ Oui ☐ Non	
			☐ Oui ☐ Non	
			☐ Oui ☐ Non	
			☐ Oui ☐ Non	
			☐ Oui ☐ Non	

Partie 2e. Description de l'environnement

Donner une description ***détaillée*** de l'environnement couvert par cette évaluation. *Par exemple :* • *Connexions entrantes et sortantes à l'environnement de données de titulaires de carte (CDE).* • *Composants critiques du système dans le CDE, comme les appareils de POS, les bases de données, les serveurs Web, etc., ainsi que les autres composants de paiement nécessaires, le cas échéant.*	
Est-ce que votre entreprise utilise la segmentation de réseau pour affecter la portée de votre environnement PCI DSS ? *(Consulter la section « Segmentation de réseau » de PCI DSS pour les recommandations concernant la segmentation de réseau)*	☐ Oui ☐ Non

Partie 2f. Prestataires de services tiers	
Votre société entretient-elle une relation avec un intégrateur et revendeur qualifié (QIR) dans le cadre des services en cours de validation ? Si oui : Nom de la société QIR : Nom individuel QIR : Description des services fournis par QIR :	☐ Oui ☐ Non
Est-ce que votre société entretient une relation avec un ou plusieurs prestataires de services tiers (par exemple, intégrateurs et revendeurs qualifiés (QIR), passerelles, services de traitement de paiement, services de prestataires de paiement (PSP), prestataires de services d'hébergement sur le Web, organisateurs de voyages, agents de programmes de fidélisation, etc.) dans le cadre des services en cours de validation ?	☐ Oui ☐ Non

Si oui :

Nom du prestataire de services :	**Description du service fourni :**

Remarque : *La condition 12.8 s'applique à toutes les entités de cette liste.*

Partie 2g. Résumé des conditions testées

Pour chaque condition PCI DSS, sélectionner une des options suivantes :

- **Pleine** - La conditions et toutes les sous-conditions ont été évaluées pour cette condition et aucune sous-condition n'a été marquée comme « Non testée » ou « Non applicable » dans le ROC.
- **Partielle** - Une ou plusieurs des sous-conditions de cette condition ont été marquées comme « Non testée » ou « Non applicable » dans le ROC.
- **Aucune** - Toutes sous-conditions de cette condition ont été marquées comme « Non testée » et/ou « Non applicable » dans le ROC.

Pour toutes les conditions identifiées comme étant « Partielles » ou « Aucune », donner des détails dans la colonne « Justification de l'approche », y compris :

- Les détails des sous-conditions spécifiques qui ont été marquées comme étant « Non testées » et/ou « Non applicables » dans le ROC.
- La Raison pour laquelle la ou les sous-conditions n'ont pas été testées ou ne sont pas applicables

Remarque : *Un tableau doit être rempli pour chaque service couvert par cet AOC. D'autres exemplaires de cette section sont disponibles sur le site Web du PCI SSC*

Nom du service évalué :	

Condition PCI DSS	**Détails des conditions testées**			
	Pleine	**Partielle**	**Aucune**	**Justification de l'approche** (Requis pour toutes les réponses « Partielle » et « Aucune ». Identifier les sous-conditions qui n'ont pas été testées et la raison.)
Condition 1 :	☐	☐	☐	
Condition 2 :	☐	☐	☐	
Condition 3 :	☐	☐	☐	
Condition 4 :	☐	☐	☐	
Condition 5 :	☐	☐	☐	
Condition 6 :	☐	☐	☐	
Condition 7 :	☐	☐	☐	
Condition 8 :	☐	☐	☐	
Condition 9 :	☐	☐	☐	
Condition 10 :	☐	☐	☐	
Condition 11 :	☐	☐	☐	
Condition 12 :	☐	☐	☐	
Annexe A1 :	☐	☐	☐	
Annexe A2 :	☐	☐	☐	

Section 2 : Rapport de conformité

Cette attestation de conformité reflète les résultats d'une évaluation sur site, qui est un document dans un ROC s'y rattachant.

L'évaluation documentée dans cette attestation et dans le ROC a été réalisée le :		
Des contrôles compensatoires ont-ils été utilisés pour répondre à une éventuelle condition du ROC ?	☐ *Oui*	☐ Non
Avez-vous identifié des conditions du ROC qui n'étaient pas applicables ?	☐ *Oui*	☐ Non
Des conditions n'ont-elles pas été testées ?	☐ *Oui*	☐ Non
Des conditions du ROC n'ont-elles pas pu être satisfaites en raison d'une contrainte juridique ?	☐ *Oui*	☐ Non

Section 3 : Détails d'attestation et de validation

Partie 3. Validation de la norme PCI DSS

Cet AOC dépend des résultats figurant dans ROC en date du *(date d'achèvement du ROC).*

En se basant sur les résultats documentés dans le ROC noté ci-dessus, les signataires identifiés dans les parties 3b-3d, le cas échéant, confirment le statut de conformité suivant pour l'entité identifiée dans la partie 2 de ce document (***cocher la mention applicable) :***

☐	**Conforme :** Toutes les sections du ROC PCI DSS sont complétées, toutes les questions ayant eu une réponse affirmative, ce qui justifie une classification globale comme **CONFORME**, ainsi, *(nom de la société de prestataire de service)* a apporté la preuve de sa pleine conformité à la norme PCI DSS.
☐	**Non conforme :** Toutes les sections du ROC PCI DSS ne sont pas complétées, toutes les questions n'ont pas eu une réponse affirmative, ce qui justifie une classification globale comme **NON CONFORME**, ainsi, *(nom de la société de prestataire de service)* n'a pas apporté la preuve de sa pleine conformité à la norme PCI DSS. **Date cible** de mise en conformité : Une entité qui soumet ce formulaire avec l'état Non conforme peut être invitée à compléter le plan d'action décrit dans la Partie 4 de ce document. *Vérifier auprès de la ou des marques de carte de paiement avant de compléter la Partie 4.*
☐	**Conforme, mais avec exception légale :** Une ou plusieurs conditions donnent lieu à une mention « Pas en place » en raison d'une restriction légale qui ne permet pas de respecter la condition. Cette option nécessite un examen supplémentaire de la part de l'acquéreur ou de la marque de paiement. *Si elle est cochée, procéder comme suit :*

Condition affectée	Détails de la manière avec laquelle les contraintes locales empêchent que la condition soit respectée.

Partie 3a. Reconnaissance du statut

Le ou les signataires confirment :

(Cocher toutes les mentions applicables)

☐	Le Rapport sur la conformité a été complété conformément aux *Conditions et procédures d'évaluation de sécurité de la norme PCI DSS*, version *(numéro de version)*, et aux instructions du présent document.
☐	Toutes les informations présentes dans le ROC susmentionné ainsi que dans cette attestation illustrent honnêtement les résultats de mon évaluation à tous points de vue.
☐	J'ai vérifié auprès de mon fournisseur d'application de paiement que mon système de paiement ne stocke pas de données d'authentification sensibles après autorisation.
☐	J'ai lu la norme PCI DSS et je reconnais être tenu de maintenir la pleine conformité à cette norme, ainsi qu'elle s'applique à mon environnement, à tout moment.
☐	Si mon environnement change, je reconnais que je dois procéder à une nouvelle évaluation de mon environnement et implémenter toute condition PCI DSS applicable.

Partie 3a. Reconnaissance du statut (suite)	
☐	Aucune preuve de stockage de données de bande magnétique[1], de données CAV2, CVC2, CID ou CVV2[2], ou de données de code PIN [3]après transaction n'a été trouvée sur AUCUN système examiné pendant cette évaluation.
☐	Les analyses ASV sont effectuées par le fournisseur d'analyse approuvé par le PCI SSC *(nom de l'ASV)*

Partie 3b. Attestation de prestataire de services	
Signature du représentant du prestataire de services ↗	*Date :*
Nom du représentant du prestataire de services :	*Poste occupé :*

Partie 3c. Reconnaissance de l'évaluateur de sécurité qualifié (QSA) (le cas échéant)	
Si un QSA a pris part ou a contribué à cette évaluation, décrire la fonction remplie :	

Signature du cadre supérieur dûment autorisé de la société QSA ↗	*Date :*
Nom du cadre supérieur dûment autorisé :	*Société QSA :*

Partie 3d. Implication de l'évaluateur de sécurité interne (ISA) (le cas échéant)	
Si un ou des ISA ont pris part ou ont contribué à cette évaluation, identifier le personnel ISA et décrire la fonction remplie :	

[1] Données encodées sur la bande magnétique ou données équivalentes sur une puce utilisées pour une autorisation lors d'une transaction carte présente. Les entités ne peuvent pas conserver l'ensemble des données de piste après autorisation des transactions. Les seuls éléments de données de piste pouvant être conservés sont le numéro de compte primaire (PAN), la date d'expiration et le nom du titulaire de carte.

[2] La valeur à trois ou quatre chiffres imprimée sur l'espace dédié à la signature ou au verso d'une carte de paiement, utilisée pour vérifier les transactions carte absente.

[3] Les données PIN (Personal Identification Number, numéro d'identification personnel) saisies par le titulaire de la carte lors d'une transaction carte présente et/ou le bloc PIN crypté présent dans le message de la transaction.

Partie 4. Plan d'action pour les conditions non conformes

Sélectionner la réponse appropriée pour « conforme aux conditions PCI DSS » pour chaque condition. Si votre réponse est « Non » à la moindre condition, vous êtes susceptible de devoir indiquer la date à laquelle votre société s'attend à être conforme à la condition et une brève description des actions prises pour respecter la condition.

Vérifier auprès de la ou des marques de paiement applicables avant de compléter la Partie 4.

Condition PCI DSS	Description de la condition	Conforme aux conditions de la norme PCI DSS *(Sélectionner un point)*		Date et actions de mise en conformité (si « NON » a été sélectionné pour la moindre des conditions)
		OUI	NON	
1	Installer et gérer une configuration de pare-feu pour protéger les données de titulaires de carte	☐	☐	
2	Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur	☐	☐	
3	Protéger les données de titulaires de carte stockées	☐	☐	
4	Crypter la transmission des données de titulaires de carte sur les réseaux publics ouverts	☐	☐	
5	Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels ou programmes anti-virus	☐	☐	
6	Développer et maintenir des systèmes et des applications sécurisés	☐	☐	
7	Restreindre l'accès aux données de titulaires de carte aux seuls individus qui doivent les connaître	☐	☐	
8	Identifier et authentifier l'accès aux composants du système	☐	☐	
9	Restreindre l'accès physique aux données de titulaires de carte	☐	☐	
10	Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaires de carte	☐	☐	
11	Tester régulièrement les processus et les systèmes de sécurité	☐	☐	
12	Gérer une politique de sécurité des informations pour l'ensemble du personnel	☐	☐	

Annexe A1	Autres conditions de la norme PCI DSS s'appliquant aux fournisseurs d'hébergement partagé	☐	☐	
Annexe A2	Autres conditions de la norme PCI DSS s'appliquant aux entités qui utilisent le SSL/TLS initial	☐	☐