

Directives pour la certification de sécurité PCI DSS des partenaires affiliés

Au niveau mondial, tous les partenaires affiliés qui transmettent, traitent ou stockent des données de carte sont tenus de respecter les directives de sécurité spécifiées dans la norme Payment Card Industry Data Security Standard (PCI DSS). En cas de non-respect de ces directives, SIX Payment Services est en droit de terminer avec effet immédiat la relation contractuelle en vigueur et de faire valoir d'éventuelles prétentions en dommages-intérêts.

Les présentes directives, qui ont une portée à la fois technique et liée à l'organisation des entreprises, sont contractuellement contraignantes pour tous les partenaires affiliés de SIX Payment Services.

Que recouvre PCI DSS?

La norme PCI DSS comprend 12 exigences contraignantes visant à protéger les données de carte durant leur traitement, leur stockage et leur transmission. La mise en œuvre de PCI DSS est gérée au travers des programmes de sécurisation des organisations de cartes: en l'occurrence les programmes AIS de Visa, SDP de Mastercard, ainsi que les programmes correspondants d'American Express, Discover (Diners Club) et JCB.

Pour quelle raison la norme PCI DSS a-t-elle été éditée?

Les vols de données de carte ont augmenté de manière continue au cours de ces dernières années. L'usage frauduleux des données volées cause des préjudices considérables à toutes les parties concernées.

Quel est le but précis de PCI DSS?

Avec la norme PCI DSS, les organisations de cartes souhaitent encore renforcer la sécurité des paiements par carte et, par conséquent, protéger encore plus efficacement les commerçants et les titulaires de cartes, ainsi que l'ensemble de la branche contre le vol et l'utilisation abusive de données.

Qui est tenu de respecter la norme PCI DSS?

La norme PCI DSS contraint tous les partenaires affiliés dans le monde qui transmettent, traitent ou stockent des données de carte à prendre et à appliquer des mesures efficaces en matière de sécurité.

La responsabilité des partenaires affiliés implique par ailleurs de veiller à ce que les sociétés tierces mandatées par elles pour transmettre, traiter ou stocker en leur nom des données de carte respectent également les directives

de sécurité. Ces sociétés peuvent être, par exemple, des «Payment Service Providers» (PSP – fournisseurs de service de paiement) ou des «Data Storage Entities» (DSE – entreprises mandatées par un commerçant pour stocker des données de cartes).

Veillez vous référer également aux points relatifs à la «protection des données» et à la «responsabilité» contenus dans les conditions générales applicables à l'acceptation des cartes.

Qui est responsable du respect de la norme PCI DSS?

Il incombe à chaque partenaire affilié de respecter les directives de sécurité. Par ailleurs, les organisations de cartes lui demandent de fournir une déclaration (certification) relative aux mesures qu'il a prises en matière de sécurité. La portée de cette déclaration (certification) dépend du nombre de transactions, ainsi que du contact ou non du partenaire affilié avec des données de carte transmises, traitées ou stockées.

Quels sont les types de mesures de certification?

La norme PCI DSS distingue ces trois types de mesures de certification (voir également le tableau au dos):

– Self-Assessment Questionnaire (SAQ)

Il s'agit d'un questionnaire d'auto-évaluation à remplir.

– Network Scan

D'entente avec le partenaire affilié, une entreprise de certification accréditée (Approved Scanning Vendor) effectue chaque trimestre une attaque informatique «amicale», afin de déceler d'éventuelles failles de sécurité.

– On-Site Audit

Les partenaires contractuels avec de gros volumes de transactions ou les partenaires contractuels qui ont été victimes d'un vol de données de cartes ont l'obligation de compléter un ROC (Report on Compliance). Les résultats doivent être vérifiés et confirmés par un QSA (Qualified Security Assessor) ou par un auditeur dûment formé (ISA – Internal Security Assessor).

Si le partenaire affilié ne remplit pas tous les critères de certification, il est tenu de remédier immédiatement à la situation dans les secteurs concernés.

Qui doit prendre à sa charge les frais de certification?

Tous les frais de certification incombent au partenaire affilié ou à l'éventuel tiers mandaté; de même en ce qui

concerne les dépenses visant à remédier aux lacunes constatées lors de l'examen.

Que se passe-t-il si un partenaire affilié omet de se faire certifier?

Si, malgré ses obligations, un partenaire affilié omet de se faire certifier, SIX Payment Services est en droit de terminer avec effet immédiat la relation contractuelle et d'exiger des dommages-intérêts pour d'éventuels préjudices subis par les organisations de cartes, ainsi que pour toutes revendications émanant des sociétés émettrices de cartes.

Qui a le droit de consulter les données de certification?

Seuls le partenaire affilié et l'entreprise de certification ont un droit de regard sur les données recueillies lors de la certification. Le partenaire affilié est cependant tenu d'envoyer à SIX Payment Services le résumé des résultats de la certification. SIX Payment Services a également le droit de consulter les Self-Assessment Questionnaires. Les organisations de cartes ne reçoivent, par contre, que des analyses statistiques.

A quels intervalles convient-il de renouveler la certification?

Les dispositions relatives à la certification sont à répéter périodiquement, conformément au tableau ci-dessous: les

modifications réalisées chez un partenaire affilié, par exemple l'installation d'un nouveau matériel informatique/ordinateur ou logiciel, un nouveau site web ou le remplacement d'un fournisseur de services (Service Provider) qui ont un rapport avec l'acceptation des paiements par carte, doivent être immédiatement signalées à SIX Payment Services. Selon les circonstances, il peut s'avérer nécessaire d'effectuer une nouvelle certification.

Par quelles entreprises les mesures de certification doivent-elles être réalisées?

Vous trouverez sur Internet un répertoire des entreprises de certification accréditées:

- pour l'exécution des On-Site Audits:
www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- pour l'exécution des Network Scans:
www.pcisecuritystandards.org/pdfs/asv_report.html

Où trouver davantage d'informations sur PCI DSS?

Vous trouverez de plus amples informations concernant la norme PCI DSS sur les sites web suivants:

- SIX Payment Services:
www.six-payment-services.com/pci
- PCI Security Standards Council:
www.pcisecuritystandards.org

Quelles sont les mesures de certification à prendre et par qui?

Level (niveau)	Désignation	Visa, Mastercard/Maestro, Diners/Discover	JCB	American Express
1	Commerçant réalisant plus de 6 millions de transactions par an	- On-Site Audit annuel ¹ - Network Scan trimestriel		
	Commerçant victime après une attaque informatique avec une utilisation abusive de données des cartes			
	Commerçant réalisant plus de 2,5 millions de transactions par an		- On-Site Audit annuel - Network Scan trimestriel	
	Commerçant réalisant plus de 1 million de transactions par an		- On-Site Audit annuel - Network Scan trimestriel	
2	Commerçant réalisant de 1 à 6 millions de transactions par an	- Self-Assessment Questionnaire annuel ² - Network Scan trimestriel		
	Commerçant réalisant de 50 000 à 2,5 millions de transactions par an			- Network Scan trimestriel
3	Commerçant «e-commerce» réalisant de 20 000 à 1 million de transactions par an	- Self-Assessment Questionnaire annuel - Network Scan trimestriel		
	Commerçant réalisant moins de 50 000 transactions par an			- Network Scan trimestriel
4	Commerçant «e-commerce» réalisant moins de 20 000 transactions par an	- Self-Assessment Questionnaire annuel - Network Scan trimestriel	- Self-Assessment Questionnaire annuel - Network Scan trimestriel	
	Commerçant (sauf «e-commerce») réalisant moins de 1 million de transactions par an			

¹ Le commerçant peut décider s'il souhaite exécuter un On-Site Audit avec le soutien d'un QSA (Qualified Security Assessor) ou le faire exécuter par un ISA (Internal Security Assessor).

² Les personnes chargées de compléter le SAQ doivent être certifiées en tant que ISA (Internal Security Assessor).

L'exécution des tests On-Site Audit et/ou Network Scan n'est contraignante que pour les partenaires affiliés qui traitent, transmettent ou enregistrent des données de cartes sous une forme électronique. Indépendamment de cela, nous recommandons cependant à tous les partenaires affiliés, notamment à ceux qui disposent d'infrastructures complexes, d'effectuer ces mesures de validation. Les partenaires affiliés doivent respecter en permanence les directives PCI DSS. Néanmoins, ils ne sont tenus d'en apporter la preuve que si SIX Payment Services leur en fait la demande par écrit.

Les coordonnées de votre interlocuteur local sont disponibles sous: www.six-payment-services.com/contacts

SIX Payment Services SA
Hardturmstrasse 201
Case postale
CH-8021 Zurich

SIX Payment Services (Europe) S.A.
10, rue Gabriel Lippmann
5365 Munsbach
Luxembourg

SIX Payment Services (Austria) GmbH
Marxergasse 1B
1030 Vienne
Autriche

SIX Payment Services (Germany) GmbH
Langenhorn Chaussee 92-94
22415 Hambourg
Allemagne