PCI DSS

Français

PCI DSS est la norme de sécurité des données de l'industrie des cartes de paiement et contient un ensemble de règles pour le traitement sécurisé des transactions par carte de crédit. En principe, toutes les parties impliquées dans un paiement par carte de crédit (par exemple, les commerçants et les PSP sont soumis à ces règles dès qu'ils traitent, transfèrent ou enregistrent des données de carte de crédit.

Il existe 12 exigences de base définies par la norme PCI DSS:

1. Installer et maintenir une configuration de pare-feu pour protéger les données des porteurs de cartes
2. N'utilisez pas les paramètres par défaut fournis par le fournisseur pour les mots de passe du système et autres paramètres de sécurité
3. Protéger les données de détenteur de carte stockées
4. Chiffrer la transmission des données des titulaires de cartes à travers les réseaux publics ouverts
5. Utilisez et mettez régulièrement à jour les logiciels ou programmes antivirus
6. Développer et maintenir des systèmes et applications sécurisés
7. Restreindre l'accès aux données des porteurs de cartes selon les besoins de l'activité
8. Attribuer un identifiant unique à chaque personne ayant accès à l'ordinateur
9. Restreindre l'accès physique aux données des porteurs de cartes
10. Suivre et surveiller tout accès aux ressources réseau et aux données des titulaires de cartes
11. Testez régulièrement les systèmes et processus de sécurité
12. Maintenir une politique qui traite de la sécurité des informations pour les employés et les sous-traitants

L'ensemble complet des règles PCI DSS est publié ici: https://www.pcisecuritystandards.org/document_library

La conformité à ces règles est vérifiée dans le cadre d'une certification PCI DSS.

Des preuves sont fournies:

- soit par le biais de questionnaires que vous devez remplir (SAQ - questionnaire d'auto-évaluation).
    - Les questionnaires sont divisés en différentes classes selon la manière dont vous traitez les données des cartes de crédit (SAQ A, SAQ A-EP, ... jusqu'à SAQ D).
- soit via un audit PCI DSS

La plateforme technique d'Axepta BNP Paribas est auditée et certifiée annuellement selon le niveau 1 PCI DSS - le niveau PCI DSS le plus strict.

La plateforme Axepta BNP Paribas vous aide à réduire votre exposition PCI DSS lorsque vous utilisez la Page de paiement hébergée ou le formulaire de carte sécurisé (paySSL).

Dans ces configurations, vous ne manipulez pas directement les données de carte, ce qui permet généralement de s'orienter vers une évaluation de type SAQ A, sous réserve que toutes les exigences applicables soient respectées.

Par ailleurs, le PCNr (pseudo-numéro de carte) n'est pas considéré comme une donnée de carte au sens de PCI DSS : il s'agit d'un jeton qui référence une carte réelle sans permettre d'en déduire le numéro d'origine. En conséquence, il n'est pas soumis aux contrôles PCI DSS, tant qu'il ne peut pas être reconverti en PAN.