Payment Services

Aide-mémoire relatif à la norme de sécurité PA-DSS

La norme de sécurité Payment Application Data Security Standard (PA-DSS), en vigueur à l'échelle internationale, comporte diverses directives de sécurité pour le développement d'applications de paiement qui stockent, traitent ou transmettent des données de cartes lors de la procédure de paiement.

Grâce à la mise en place d'applications de paiements certifiées selon la norme PA-DSS, le risque de vol de données de cartes peut être considérablement réduit. PA-DSS permet en outre aux entreprises d'obtenir et de respecter plus facilement la norme de sécurité PCI DSS (Payment Card Industry Data Security Standard).

Nous avons rassemblé pour vous les informations les plus importantes concernant ce programme PA-DSS.

Pourquoi la norme PA-DSS a-t-elle été instaurée?

L'examen de divers cas de vols de données de cartes a montré qu'ils provenaient sans cesse d'applications de paiement pas suffisamment protégées. C'est la raison pour laquelle PA-DSS, norme de sécurité uniforme en vigueur à l'échelle internationale, a été instaurée en 2008.

À quoi sert la norme PA-DSS?

Le recours à des applications de paiement certifiées contribue à minimiser le risque de vol de données de cartes. PA-DSS aide les fournisseurs de solutions à concevoir de nouvelles applications de paiement et les commerçants à être conformes à PCI DSS (Payment Card Industry Data Security Standard).

Que contient la norme PA-DSS?

La norme englobe 14 exigences principales et environ 90 exigences de détail permettant aux fournisseurs de solutions de s'orienter lors de la conception d'applications de paiement sécurisées. Les exigences se concentrent principalement sur les secteurs suivants: conception, processus, implémentation, cryptage et accès.

Qui est tenu de respecter la norme PA-DSS?

Sont tenus au respect les fabricants d'applications de paiement qui stockent, traitent ou transmettent des données de cartes. Pour cela, il faut que ces applications fassent partie du processus d'autorisation et/ou de la procédure de paiement et soient vendues à des tiers.

Qui est responsable du respect de la norme PA-DSS?

Les fournisseurs de solutions doivent en premier lieu garantir que leurs applications de paiement soient conformes à PA-DSS. Les associés commerciaux, intégrateurs et partenaires affiliés qui achètent, vendent ou installent des applications de paiement, doivent s'assurer que les applications de paiement qu'ils utilisent soient certifiées selon la norme PA-DSS.

Quels types d'applications sont soumis à la norme PA-DSS?

- Les applications de paiement en série qui sont vendues et installées à des tiers.
- Les applications de paiement modulaires (uniquement les modules avec fonctions de paiement).
- Les terminaux de paiement autonomes qui
  1. sont reliés au système ou au réseau du commerçant.
  2. ne sont pas uniquement reliés à l'opérateur qui traite le paiement (acquirer).
  3. ne permettent pas une télémaintenance sécurisée de l'application de paiement.
  4. stockent des données de cartes sensibles (données de la piste magnétique, CVV2, CVC2, CAV2, CID ou NIP) suite à la procédure d'autorisation.

Quels types d'applications ne sont pas tenus de respecter la norme PA-DSS?

1. Les solutions clients sur mesure (pas de distribution).
2. Les applications conçues spécialement par le commerçant, uniquement à usage interne.
3. Les systèmes d'exploitation (Windows, Unix, etc.), les bases de données, les systèmes de gestion (back office) et autres systèmes similaires.

Ces applications sont contrôlées dans le cadre de la certification PCI DSS du commerçant.

Qui a le droit d'effectuer une certification PA-DSS?

Les applications de paiement doivent obligatoirement être inspectées et certifiées par des évaluateurs de sécurité qualifiés (PA-QSA – Payment Application Qualified Security Assessor). Ces évaluateurs de sécurité sont accrédités par le Conseil PCI. Vous trouverez une liste de tous les PA-QSA reconnus en vous rendant sur:
https://www.pcisecuritystandards.org/security_standards/vpa/

Quelle est la durée de validité du certificat PA-DSS?

La norme est révisée tous les trois ans et publiée dans une nouvelle version. La certification devient caduque trois ans après la publication de la nouvelle version de la norme. La conformité est ainsi garantie pendant au moins 3 ans.

Les applications de paiement doivent cependant être accréditées tous les ans. En cas de modification apportée à l'application de paiement, une revalidation par un PA-QSA peut éventuellement s'avérer obligatoire, tout dépend du type de modification.

À combien revient une certification et qui paie la facture?

Le montant des frais pour la certification d'une application de paiement varie selon les cas. Outre la taille et la complexité d'une application de paiement, le choix de l'évaluateur de sécurité (PA-QSA) entre également toujours en ligne de compte.

Une fois l'application de paiement certifiée, son enregistrement dans le répertoire du Conseil PCI coûte 1,250 USD par application de paiement. Par la suite, des frais de gestion à concurrence de 500 USD sont prélevés chaque année par application de paiement.

Où puis-je trouver de plus amples informations sur PA-DSS?

D'autres informations sur la norme PA-DSS sont disponibles sur le site Internet du Conseil PCI:
https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

Nous vous recommandons également leur webinaire consacré à la norme PA-DSS:
http://www.webcastgroup.com/client/start.asp?wid=0800522084108

Vous trouverez ici la liste actualisée de toutes les applications de paiement certifiées:
https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html

110.0115.03 CHE_FR/04.2012

Votre contact personnel: www.six-payment-services.com/contact

SIX Payment Services SA
Hardturmstrasse 201
8005 Zurich
Suisse

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