Conformité d'un commerçant

- **PCI-DSS s'applique aux accepteurs que sont les commerçants, comme à toute autre entité manipulant ces données,**
  - soit directement (paiement ou retrait), sur quelque média que ce soit (terminal de paiement, paiement à distance),
  - soit indirectement pour tout autre processus utilisant ces données.
- **PCI-DSS est un standard ouvert.**
  - Chaque réseau de cartes définit les modalités de mise en conformité chaque acteur
  - Ces modalités sont mises en œuvre de façon appropriée à la nature de l'entité concernée en fonction d'une analyse des risques..
  - Les accepteurs sont classés en 4 niveaux en fonction du niveau de risque qu'ils représentent, en prenant en compte :
    - le volume des opérations traitées,
    - le canal utilisé (e-commerce, autre canal),
    - le niveau de sécurité mis en œuvre dans le traitement de l'opération (EMV ou non),
    - l'utilisation ou non des données pistes.

La conformité au regard des règles PCI-DSS s'apprécie suivant le référentiel de contrôle PCI-DSS

Niveau	Activité de l'accepteur toutes cartes « CB » et agrées « CB » combinées	Normes ou recommandations PCI-DSS
1	▪Plus de 6 millions* d'opérations par an ou, ▪Informatique non conforme au bulletin 10 ou, ▪Compromission l'année précédente. *Reclassement en niveau 2 si au moins 85% des opérations sont EMV et si l'informatique est conforme au bulletin 10 (non stockage des données discrétionnaires de la piste ISO2).*	• **audit annuel** sur site par auditeur certifié • **scans** périodiques du réseau par auditeur certifié (ASV) ou, par dispositif interne accrédité 1.interne et 2.Externe (depuis l'Internet)
2	1 à 6 millions d'opérations / an **ou** plus de 6 millions d'opérations par an si : au moins 85% d'opérations EMV et informatique conforme au bulletin 10 et pas compromission l'année précédente	1. auto-évaluation annuelle (questionnaire* disponible sur le site PCI, à la rubrique SAQ) 2. scan réseau de vulnérabilité trimestriel depuis l'Internet
3	Tout accepteur réalisant de 20.000 à 1 million de transactions e-commerce / an	1. auto-évaluation annuelle (questionnaire* PCI-DSS) 2. scan réseau de vulnérabilité trimestriel depuis l'Internet
4	Tout autre accepteur	1. auto-évaluation annuelle (questionnaire* disponible sur le site PCI, à la rubrique SAQ 2. scan réseau de vulnérabilité trimestriel

[1] Auditeur certifié PCI-DSS : la certification QSA est une garantie suffisante. Auditeur interne : références de formation certifiantes pour garantir une bonne maîtrise du contexte monétique.

[2 4 questionnaires (A,B,C,D) sont disponibles, en fonction du contexte du commerçant.

Les normes de protection des données monétiques sont de plus en plus contraignantes pour faire face à des menaces de plus en plus lourdes.

- **PCI-DSS évolue**
  - Version 1.3 : prévue au 2ème trimestre 2011, consultable sur le site du PIC Council
- **Le commerçant peut se décharger de la gestion des contraintes sécuritaires PCI DSS s'il ne manipule aucune donnée carte.**
  - Souscription à l'offre Merc@net, offre conforme aux exigences de sécurité PCI-DSS*,
  - Délégation de la fonction paiement carte à un prestataire certifié conforme PCI-DSS, sans échange de données cartes avec ce prestataire.
    - Le prestataire certifié s'est doté des moyens et des compétences pour mettre en œuvre toutes les exigences de sécurités monétiques et suivre les évolutions interbancaires.
    - Le Système d'Information du commerçant est ainsi isolé de la fonction monétique, et échappe de facto aux contraintes liées à la mise en œuvre de PCI-DSS.
- **Pour les commerces doté d'un Système d'Information utilisant des données cartes, approche rationnelle des risques**
  - cartographie du SI pour identifier les risques monétiques : où peuvent être traitées, stockées et échangées des données sensibles monétiques ?
  - réduction du périmètre soumis aux normes de sécurité PCI en limitant traitement, échange et stockage de donnés sensibles au strict nécessaire, y compris dans les journaux et les dispositifs de sauvegarde. « *Si vous n' avez pas un besoin indispensable d'une donnée monétique, ne la stockez pas !*».
  - La mise en œuvre des normes de sécurité PCI-DSS, ou l'application des mesures compensatoires, pour abaisser le niveau de risque résiduel sont ainsi limitées au strict nécessaire.

* Sauf en cas de création de paiements via les offres Merc@net Gestion Plus, Merca VPC via l'outil de gestion de Merc@net.