Contact

Norme PCI MPoC

Qu'est-ce que la norme PCI MPoC ?

PCI MPoC (Mobile Payment on Commercial Off-The-Shelf) est une norme qui permet d'accepter les paiements sur les appareils mobiles commerciaux, tels que les smartphones et les tablettes. Cette norme intègre les cas d'utilisation des normes CPoC et SPoC. La nouvelle norme est conçue pour prendre en charge la saisie des données du titulaire de carte avec ou sans contact sur le même appareil et ajoute la prise en charge des transactions hors ligne.

Tout comme le **SBMP** (Software-based Mobile Payment) d'**EMVCo** est utilisé pour virtualiser les cartes à puce, le PCI MPoC fournit un cadre pour les solutions de paiement mobile sécurisées.

Composants de la norme PCI MPoC

Pour connaître le détail des composants et des exigences, il faut se référer à la documentation disponible sur le site des normes de sécurité PCI.

Ci-après, un résumé de la documentation MPoC est présenté :

Les produits déjà validés dans le cadre des programmes PCI SPoC ou PCI CPoC déjà en place peuvent être soumis à une évaluation dans le cadre du programme MPoC. S'ils sont validés par une évaluation complète, ces produits peuvent être acceptés par le PCI SSC (Security Standard Council) et figurer sur la liste des produits MPoC.

Les exigences de sécurité décrites dans la norme MPoC fournissent un cadre pour protéger la confidentialité et l'intégrité des informations de paiement sensibles capturées

et traitées dans les solutions MPoC. Ce cadre est défini avec des exigences de sécurité, des exigences d'essai et des conseils pour les entités impliquées dans le développement, le déploiement et l'exploitation de solutions d'acceptation de paiement mobile exploitées par les commerçants qui utilisent des appareils COTS.

Principales caractéristiques de la norme PCI MPoC

Les principales caractéristiques de la norme PCI MPoC sont les suivantes :

- **Approche modulaire :** Permet une approche modulaire et adaptable aux différents types de canaux d'acceptation des paiements mobiles. PCI MPoC offre des exigences ouvertes en matière de sécurité et d'essais, ce qui permet aux clients de définir et d'adapter leurs propres solutions de paiement et cas d'utilisation.
- **Approche d'intégration :** Il est possible de travailler avec des composants pré-certifiés à intégrer dans la solution finale.
- **Services AandM**: Comprend les exigences relatives aux services d'attestation et de surveillance afin de garantir une sécurité et une conformité permanentes.

Importance de la norme MPoC

La norme MPoC est exigée par plusieurs grands systèmes de paiement pour la mise en œuvre des solutions SoftPOS. Sur le marché des paiements, la confiance est primordiale, et les entreprises doivent s'assurer que leurs systèmes restent sécurisés pour maintenir cette confiance. Alors, comment peuvent-elles garantir cette fiabilité ? La norme de certification PCI MPoC est conçue à cet effet, et constitue le meilleur moyen de démontrer que votre produit est digne de confiance. Cette certification implique l'évaluation du SDK, de l'APP et des services AandM.

En outre, les produits certifiés seront répertoriés sur le site Web de PCI, où les évaluateurs, les commerçants, les acquéreurs et les autres parties intéressées peuvent examiner les solutions de paiements mobiles sur COTS (MPoC).

L'inscription sur la liste est un très bon moyen pour entrer sur ce marché qui connaît une croissance exponentielle ; en même temps, l'accréditation MPOC permet d'atténuer les risques liés à la menace croissante des cyber-attaques ciblant les terminaux commerciaux.

En résumé, toutes les parties prenantes qui ont l'intention de travailler avec les principaux systèmes de paiement pour vendre des terminaux de point de vente mobiles **sont obligées de s'assurer que leurs produits sont accrédités PCI.**

Services d'évaluation de la sécurité de la norme MPoC

Applus recommande quelques étapes pour réaliser des évaluations rapides et faciles :

- La **pré-évaluation** est une manière rapide et efficace d'identifier les informations manquantes et/ou les informations erronées dans les preuves documentaires pour faire face aux exigences de la norme PCI MPOC.

  L'objectif de cette activité est de fournir au vendeur une liste de problèmes qui réduit le risque de problèmes potentiels trouvés pendant l'évaluation, ce qui entraîne des retards dans le projet et/ou des itérations d'évaluation supplémentaires qui impliquent un coût supplémentaire.

  Les tâches incluses sont l'examen des documents et du code.

- L'**évaluation** est effectuée pour valider que le produit remplit correctement toutes les exigences de sécurité et d'essai. Cela se fait en fonction des exigences des différents domaines (en fonction des capacités du produit) :
  - Domaine 1 : Exigences de base du logiciel MPoC
  - Domaine 2 : Intégration des applications MPoC
  - Domaine 3 : Attestation et surveillance
  - Domaine 4 : Gestion du logiciel MPoC
  - Domaine 5 : Solution MPoC
    - L'évaluation se déroule en cinq opérations différentes :
      - **Examen**: Le testeur examine les données telles que les documents de conception, le code source, les fichiers de configuration, les données de suivi des beugs et les résultats des tests de sécurité.
      - **Essai**: Le testeur utilise des outils et des techniques de sécurité tels que SAST, DAST, IAST et SCA, ainsi que des méthodes manuelles telles que les revues de code, les tests de pénétration et le grattage de mémoire, pour évaluer la solution.
      - **Observation**: Le testeur observe des actions ou des essais, en notant les résultats, notamment dans des conditions variées.
      - **Entretien**: Le testeur s'entretient avec le personnel pour comprendre ses activités, sa conformité aux processus définis et sa connaissance des politiques et des procédures.
      - **Document**: Le testeur consigne les détails dans le rapport d'évaluation pour les besoins d'essais actuels ou futurs.

Les preuves documentaires nécessaires sont :

- **Les formulaires MPOC :** Comme décrit précédemment, il y a des formulaires à remplir en fonction du produit à évaluer.
- **Documentation technique :** Documentation sur l'architecture et la conception et caractéristiques/configurations de sécurité mises en œuvre, y compris les méthodes de cryptage, la gestion sécurisée des clés et le stockage sécurisé des données.

- **Évaluation des vulnérabilités :** Quelques informations sur les données de suivi des beugs sur les vulnérabilités publiques et autres, et les essais d'assurance.
- **Code source :** Le code source du produit**.**
- **Outils et techniques d'essai de sécurité :** Tous les outils de sécurité et les outils fonctionnels qui permettent au laboratoire d'opérer ou de démontrer la robustesse de la sécurité du produit. Cela inclut également les résultats des essais.
- **Documentation de tiers**: Toute sorte de conseils de sécurité, d'informations sur les produits et de certificats de tiers qui pourraient être utiles pendant l'évaluation.

Comment Applus+ Laboratories peut vous aider avec la norme PCI MPoC ?

Applus+ Laboratories offre une vaste expérience en matière de sécurité des applications de paiement mobile, allant d'une grande expertise des produits **EMVCo SBMP (Software-based Mobile Payment)** aux dernières normes **PCI MPoC**.

En outre, Common.SECC expérience d'évaluation**.** Des évaluations détaillées basées sur le profil de protection POI pour les paiements par logiciel version 1.2.

En tirant parti de notre expertise en matière de PCI PTS, d'EMVCo SBMP et de Common. SECC pour réaliser des évaluations rapides et efficaces. Nous pouvons vous aider sur la voie de la conformité PCI MPoC !