
# *Présentation du référentiel PCI-DSS*

Hervé Hosy

*herve.hosy@oppida.fr*

*06.03.51.96.66*

# Agenda

- Référentiel PCI-DSS
  - Contexte
  - Structure du référentiel
  - Lien avec les normes ISO 270xx

# Contexte

# Contexte

## Référentiel PCI-DSS

- Acronyme anglais de « Payment Card Industry Data Security Standard », ce qui signifie « Norme de sécurité des données pour l'industrie des cartes de paiement »
- Développé par PCI Security Standards Council (PCI SSC), qui a été fondé par American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa, Inc.
  - ➔ Octobre 2008 v1.2
  - ➔ Juillet 2009 v1.2.1
  - ➔ Octobre 2010 v2.0
  - ➔ Octobre 2014 v3.0

# Contexte

- PCI-DSS
  - Norme spécifique au domaine bancaire
    - ➔ Concerne la protection des données sensibles liées aux cartes bancaires (PAN, date de validité, cryptogramme visuel, piste magnétique…)
    - ➔ But : Pallier aux faiblesses sécuritaires du e-commerce en protégeant la confidentialité de données publiques (car visibles sur le recto ou le verso des cartes bancaires !)
  - Impose des mécanismes de sécurité
    - ➔ Firewall
    - ➔ Chiffrement des réseaux
    - ➔ Journalisation
    - ➔ Intégrité des serveurs

# Contexte

## PCI-DSS

- Forces de l'approche
  - ➔ Acceptée dans le domaine bancaire : conformité imposée par VISA et Mastercard sous la menace de pénalités financières
  - ➔ Couvre l'absence d'exigences normatives
  - ➔ Autorise le non respect (partiel ou total) d'une exigence, si celle-ci est remplacée par des mesures compensatoires
- Faiblesses de l'approche
  - ➔ Les mesures compensatoires sont présentées par l'auditeur (QSA) à VISA et Mastercard, qui peuvent les refuser
  - ➔ Les QSA sont responsables financièrement avec l'audité qu'ils ont aidé à certifier PCI-DSS, en cas de fraude sur le périmètre certifié

# Contexte

## Conformité à PCI-DSS

| Niveau | Type d'activité | Action requise pour la conformité |
|---|---|---|
| 1 | Tout commerçant traitant plus de 6 millions transactions Visa ou MasterCard par an<br>Tout commerçant ayant subit une compromission | Audit de sécurité sur site<br>Scan de vulnérabilité trimestriel (si commerce en ligne) |
| 2 | Tout commerçant traitant de 1 à 6 millions de transactions Visa ou MasterCard par an | Questionnaire d'auto-évaluation annuel<br>Scan de vulnérabilité trimestriel (si commerce en ligne) |
| 3 | Tout commerçant traitant de 20,000 à 1 million de transactions Visa ou MasterCard par an | Questionnaire d'auto-évaluation annuel<br>Scan de vulnérabilité trimestriel (si commerce en ligne) |
| 4 | Tout commerçant traitant moins de 20,000 transaction de commerce en ligne Visa ou MasterCard par an<br>Tous les autres commerçants traitant jusqu'à 1 million de transactions Visa ou MasterCard par an | Questionnaire d'auto-évaluation annuel<br>Scan de vulnérabilité trimestriel recommandé (si commerce en ligne)<br><br>*(cela dépend si les données sont capturées, stockées ou transmises par l'infrastructure du commerçant ou par un fournisseur de services)* |

# Contexte

- La norme PCI DSS s'applique partout où des « données de compte » sont stockées, traitées ou transmises
  - *Qu'est-ce qu'une « données de compte »*
    - ➔ *Données du titulaires de cartes*
      - Numéro de compte primaire (PAN)
      - Nom du titulaire de la carte
      - Date d'expiration
      - Code service
    - ➔ *Données d'authentification sensibles*
      - Données de bande magnétique complètes (ou leur équivalent sur une puce)
      - CAV2/CVC2/CVV2/CID
      - Codes/blocs PIN

# Contexte

- Le numéro de compte primaire est le facteur déterminant de l'applicabilité des conditions PCI-DSS

  - Les conditions PCI-DSS sont applicables si un PAN est stocké, traité ou transmis

  - Si le PAN n'est pas stocké, traité ou transmis, les conditions PCI-DSS ne s'appliquent pas

# Contexte

- Synthèse des exigences en matière de stockage de données

| | | Élément de données | Stockage autorisé | Rendre illisibles les données de compte stockées selon la condition 3.4 |
|---|---|---|---|---|
| Données de compte | Données du titulaire de la carte | Numéro de compte primaire (PAN) | Oui | **Oui** |
| | | Nom du titulaire de la carte | Oui | Non |
| | | Code service | Oui | Non |
| | | Date d'expiration | Oui | Non |
| | Données d'authentification sensibles [1] | Données complètes de la piste magnétique [2] | **Non** | *Stockage interdit selon condition 3.2* |
| | | CAV2/CVC2/CVV2/CID | **Non** | *Stockage interdit selon condition 3.2* |
| | | Code/bloc PIN | **Non** | *Stockage interdit selon condition 3.2* |

1 *Une fois le processus d'autorisation terminé, les données d'authentification sensibles ne doivent plus être stockées (même si elles sont cryptées)*

2 *Données de piste complètes extraites de la bande magnétique, données équivalentes de la puce, ou d'un autre support*

# Contenu du référentiel PCI-DSS

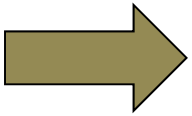
# *Référentiel PCI-DSS*

- Structure du référentiel PCI-DSS

6 thèmes (+ 1 spécifique)

- ➔ Création et gestion d'un réseau sécurisé
- ➔ Protection des données des titulaires de cartes
- ➔ Gestion d'un programme de gestion des vulnérabilités
- ➔ Mise en œuvre de mesures de contrôle d'accès strictes
- ➔ Surveillance et test réguliers des réseaux
- ➔ Gestion d'une politique de sécurité des informations

- ➔ *Autres conditions s'appliquant aux fournisseurs d'hébergement partagé*



12 conditions de sécurité (+ 1 spécifique)

204 exigences élémentaires

# *Référentiel PCI-DSS*

- Création et gestion d'un réseau sécurisé
  - Condition 1 : Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes
  - Condition 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur
- Protection des données des titulaires de cartes
  - Condition 3 : Protéger les données de titulaires de cartes stockées
  - Condition 4 : Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts

# *Référentiel PCI-DSS*

- Gestion d'un programme de gestion des vulnérabilités
  - Condition 5 : Utiliser des logiciels antivirus et les mettre à jour régulièrement
  - Condition 6 : Développer et gérer des systèmes et des applications sécurisés
- Mise en œuvre de mesures de contrôle d'accès strictes
  - Condition 7 : Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître
  - Condition 8 : Affecter un ID unique à chaque utilisateur d'ordinateur
  - Condition 9 : Restreindre l'accès physique aux données des titulaires de cartes

# *Référentiel PCI-DSS*

- Surveillance et test réguliers des réseaux
  - Condition 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes
  - Condition 11 : Tester régulièrement les processus et les systèmes de sécurité
- Gestion d'une politique de sécurité des informations
  - Condition 12 : Gérer une politique de sécurité des informations pour l'ensemble du personnel

# *Référentiel PCI-DSS*

- Autres conditions s'appliquant aux fournisseurs d'hébergement partagé
  - Condition A.1 : Les prestataires de services d'hébergement partagé doivent protéger l'environnement des données de titulaires de cartes

# *Lien avec les normes ISO 270xx*

# Lien avec la norme ISO 27002

| Contenu de la norme ISO/IEC 27002:2005 | Condition 1 | Condition 2 | Condition 3 | Condition 4 | Condition 5 | Condition 6 | Condition 7 | Condition 8 | Condition 9 | Condition 10 | Condition 11 | Condition 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ➡Politique de sécurité | | | | | | | | | | | | X |
| ➡Organisation de la sécurité de l'information | | | | | | | | | | | | X |
| ➡Gestion des biens | | | | | | | | | | | | |
| ➡Sécurité liée aux ressources humaines | | | | | | | | | | | | X |
| ➡Sécurité physique et environnementale | | | | | | | | | X | | | |
| ➡Gestion de l'exploitation et des télécommunications | X | X | | X | X | | | | | X | | |
| ➡Contrôle d'accès | | | X | | | | X | X | | | | |
| ➡Acquisition, développement et maintenance des systèmes d'information | | | | | | X | | | | | | |
| ➡Gestion des incidents liés à la sécurité de l'information | | | | | | | | | | | X | X |
| ➡Gestion du plan de continuité de l'activité | | | | | | | | | | | | |
| ➡Conformité | | | | | | | | | | | | |

# *Lien avec la norme ISO 27002*

- Politique de sécurité
  - Condition 12 : Gérer une politique de sécurité des informations pour l'ensemble du personnel
    - ➔ Processus annuel qui identifie les menaces et les vulnérabilités, et débouche sur une évaluation formelle des risques
    - ➔ Examen annuel de la Politique de sécurité des informations, avec une mise à jour chaque fois que l'environnement change

# *Lien avec la norme ISO 27002*

- Organisation de la sécurité de l'information
  - Condition 12 : Gérer une politique de sécurité des informations pour l'ensemble du personnel
    - ➔ S'assurer que la politique et les procédures de sécurité définissent clairement les responsabilités de tout le personnel en la matière

# *Lien avec la norme ISO 27002*

- Sécurité liée aux ressources humaines
  - Condition 12 : Gérer une politique de sécurité des informations pour l'ensemble du personnel
    - ➔ Effectuer une sélection préalable à l'embauche du personnel pour minimiser les risques d'attaques par des sources internes
    - ➔ Mettre en œuvre un programme annuel de sensibilisation à la sécurité pour sensibiliser les employés à l'importance de la sécurité des données de titulaires de cartes

# *Lien avec la norme ISO 27002*

- Sécurité physique et environnementale
  - Condition 9 : Restreindre l'accès physique aux données des titulaires de cartes
    - ➔ Installer des caméras vidéo et/ou d'autres mécanismes de contrôle d'accès pour surveiller l'accès physique des individus aux zones sensibles
    - ➔ Examiner les données enregistrées et les mettre en corrélation avec d'autres informations. Les conserver pendant trois mois au minimum, sauf stipulation contraire de la loi
      - – *En France, maximum 30 jours (loi Informatique et Liberté)*
    - ➔ Restreindre l'accès physique aux prises réseau accessibles au public
    - ➔ Restreindre l'accès physique aux points d'accès, passerelles, dispositifs portables, matériel réseau/communications et lignes de télécommunication sans fil

# Lien avec la norme ISO 27002

- Sécurité physique et environnementale (suite)
  - ➔ Utiliser un registre des visites pour tenir un contrôle physique de la circulation des visiteurs
    Conserver ce registre pendant trois mois au minimum, sauf stipulation contraire de la loi
  - ➔ Ranger les sauvegardes sur support en lieu sûr, de préférence hors de l'installation, par exemple sur un autre site ou un site de secours, ou encore un site de stockage commercial
    Inspecter la sécurité du site au moins une fois par an
  - ➔ Assurer un contrôle strict de la distribution interne ou externe de tout type de support
  - ➔ S'assurer que les responsables approuvent tous les supports déplacés d'une zone sécurisée (en particulier s'ils sont distribués à des individus)

# Lien avec la norme ISO 27002

- Gestion de l'exploitation et des télécommunications
  - Condition 1 : Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes
    - ➔ Placer les composants du système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone de réseau interne, isolée de la DMZ et des autres réseaux non approuvés
    - ➔ Sécuriser et synchroniser les fichiers de configuration des routeurs
    - ➔ Installer un logiciel pare-feu personnel (non modifiable par les utilisateurs) sur tout ordinateur portable et/ou ordinateur appartenant à un employé équipé d'une connexion directe à Internet, qui est utilisé pour accéder au réseau de l'entreprise
    - ➔ Processus formel d'approbation et de test de toutes les connexions réseau et des modifications apportées aux configurations des pare-feu et des routeurs
    - ➔ Nécessité d'examiner les règles des pare-feu et des routeurs au moins tous les six mois

# *Lien avec la norme ISO 27002*

- Gestion de l'exploitation et des télécommunications (suite)
  - Condition 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur
    - ➔ N'appliquer qu'une fonction principale par serveur (physique ou virtuel) afin d'éviter la coexistence, sur le même serveur, de fonctions exigeant des niveaux de sécurité différents
    - ➔ N'activer que les services, protocoles, démons, etc., nécessaires et sécurisés pour le fonctionnement du système
    - ➔ Changer systématiquement les paramètres par défaut définis par le fournisseur avant d'installer un système sur le réseau
    - ➔ Modifier les clés de chiffrement par défaut des équipements réseau sans fil à l'installation et à chaque fois qu'un employé qui les connaît quitte l'entreprise ou change de poste

# *Lien avec la norme ISO 27002*

- Gestion de l'exploitation et des télécommunications (suite)
  - Condition 4 : Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts
    - ➔ Utiliser des protocoles de sécurité et de cryptographie robustes (par exemple, SSL/TLS, IPSEC, SSH, etc.) afin de protéger les données sensibles des titulaires de cartes durant la transmission sur des réseaux publics ouverts
  - Condition 5 : Utiliser des logiciels antivirus et les mettre à jour régulièrement
    - ➔ Déployer des logiciels antivirus sur tous les systèmes régulièrement affectés par des logiciels malveillants (en particulier PC et serveurs)
    - ➔ S'assurer que tous les mécanismes antivirus sont à jour, en cours d'exécution et génèrent des journaux d'audit

# *Lien avec la norme ISO 27002*

- Gestion de l'exploitation et des télécommunications (suite)
  - Condition 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes
    - ➔ Passer en revue les journaux d'audit relatifs à tous les composants du système au moins une fois par jour, notamment les serveurs exécutant des fonctions des sécurité (IDS, RADIUS…)
    - ➔ Conserver l'historique des journaux d'audit pendant une année au moins, en gardant immédiatement à disposition les journaux des trois derniers mois au moins, pour analyse (par exemple, disponibles en ligne, dans des archives ou restaurables à partir d'une sauvegarde)

# Lien avec la norme ISO 27002

- Contrôle d'accès
  - Condition 3 : Protéger les données de titulaires de cartes stockées
    - ➔ Ne stocker aucune donnée d'authentification sensible après autorisation (même chiffrée), ni la totalité du contenu d'une quelconque piste (sur la bande magnétique au verso d'une carte, sur une puce ou ailleurs)
    - ➔ Ne pas stocker le CVx2, le code PIN, ni le PIN-bloc chiffré
    - ➔ Masquer le PAN lorsqu'il s'affiche (les six premiers chiffres et les quatre derniers sont le maximum de chiffres affichés)
    - ➔ Rendre le PAN illisible où qu'il soit stocké, en utilisant l'une des approches suivantes : hachage unilatéral, troncature, tokens et pads d'index, cryptographie robuste
    - ➔ Protéger les clés utilisées pour protéger les données de titulaires de cartes de la divulgation et de l'utilisation illicites

# *Lien avec la norme ISO 27002*

- Contrôle d'accès (suite)
  - Condition 7 : Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître
    - ➔ Restreindre l'accès aux composants du système et aux données des titulaires de cartes aux seuls individus qui doivent y accéder pour mener à bien leur travail
  - Condition 8 : Affecter un ID unique à chaque utilisateur d'ordinateur
    - ➔ S'assurer qu'une gestion appropriée des mots de passe et de l'authentification des utilisateurs est mise en œuvre
    - ➔ Intégrer l'authentification à deux facteurs pour l'accès à distance (accès au niveau du réseau depuis l'extérieur du réseau) des employés, des administrateurs et de tiers au réseau

# *Lien avec la norme ISO 27002*

- Acquisition, développement et maintenance des systèmes d'information
  - Condition 6 : Développer et gérer des systèmes et des applications sécurisés
    - ➔ S'assurer que tous les logiciels et les composants du système sont dotés des derniers correctifs de sécurité développés par le fournisseur, afin de les protéger des vulnérabilités connues
    - ➔ Développer des applications logicielles (internes et externes, y compris l'accès administratif aux applications par le Web) conformément à la norme PCI DSS, basées sur les meilleures pratiques du secteur
    - ➔ Pour les applications Web orientées public, traiter les nouvelles menaces et vulnérabilités de manière régulière et veiller à ce que ces applications soient protégées contre les attaques connues

# Lien avec la norme ISO 27002

- Gestion des incidents liés à la sécurité de l'information
  - Condition 11 : Tester régulièrement les processus et les systèmes de sécurité
    - ➔ Utiliser des systèmes de détection d'intrusions (IDS) et/ou des systèmes de prévention d'intrusions (IPS)
    - ➔ Déployer des logiciels de contrôle de l'intégrité des fichiers pour alerter le personnel de toute modification non autorisée des fichiers de configuration, des fichiers de contenu ou des fichiers système stratégiques
    - ➔ Tester la présence de points d'accès sans fil et détecter les points d'accès sans fil non autorisés tous les trimestres
    - ➔ Analyser les vulnérabilités potentielles des réseaux internes et externes au moins une fois par trimestre et après tout changement significatif des réseaux
    - ➔ Effectuer des tests de pénétration externe et interne au moins une fois par an et après tout changement ou mise à niveau significatif de l'infrastructure ou des applications

# *Lien avec la norme ISO 27002*

- Gestion des incidents liés à la sécurité de l'information (suite)
  - Condition 12 : Gérer une politique de sécurité des informations pour l'ensemble du personnel
    - ➔ Mettre en œuvre un plan de réponse aux incidents
      Être prêt à réagir immédiatement à toute intrusion dans le système

# Conclusion

# Conclusion

- PCI-DSS
  - Très proche du référentiel ISO 27002
  - Impacte profondément les applications bancaires, surtout pour le back-office (plus de manipulation de PAN en clair, par défaut)
  - Nécessite de créer un sous-ensemble informatique conforme, pour pouvoir migrer progressivement les applications bancaires