Industrie des cartes de paiement (PCI)

Norme de sécurité des données d'application de paiement

Récapitulatif des modifications entre les versions 2.0 et 3.0

Novembre 2013

Introduction

Ce document propose un récapitulatif des modifications entre la v2.0 et la v3.0 de la norme PA-DSS. Le tableau 1 donne un aperçu des types de modifications inclus dans la v3.0 de la norme PA-DSS. Le tableau 2 des pages suivantes donne un récapitulatif des modifications importantes qui se trouvent dans la v3.0 de la norme PA-DSS.

Tableau 1 : Types de modification

Type de modification	Définition
Clarification	Clarification de l'objectif de la condition. Garantit que la rédaction concise de la norme reflète l'objectif souhaité des conditions.
Directives supplémentaires	Explications, définitions et/ou instructions permettant une meilleure compréhension ou délivrant une meilleure information ou une directive à propos d'un sujet particulier.
Évolution de la condition	Modifications garantissant que les normes sont à jour et tiennent compte des nouvelles menaces et de l'évolution du marché.

Tableau 2 : Récapitulatif des modifications

Section		Modification	Type
v2.0 PA-DSS	**v3.0 PA-DSS**		
Introduction	Introduction	**Objectif de ce document** Objet et utilisation plus clairs du document et ajout d'une référence au modèle de rapport ROV de la norme PA-DSS.	Clarification
		Relation entre les normes PCI DSS et PA-DSS Meilleure clarification du fait que les applications PA-DSS se trouvent dans le champ d'application de l'évaluation PCI DSS d'une organisation.	Clarification
Informations relatives aux conditions d'application de la norme PCI DSS	Informations relatives aux conditions d'application de la norme PCI DSS	Section déplacée et mise à jour pour refléter les changements de la norme PCI DSS. Élimination de certains termes de la norme PCI DSS qui ne s'appliquent pas à PA-DSS.	Clarification
Champ d'application de la norme PA-DSS	Champ d'application de la norme PA-DSS	Information éliminée concernant les applications de paiement qui sont admissibles pour la norme PA-DSS. Les informations portant sur l'admissibilité pour la norme PA-DSS se trouvent sur le *Guide du programme de la norme PA-DSS*.	Clarification
Rôles et responsabilités		Les informations portant sur les parties prenantes pertinentes et leurs rôles et responsabilités pour PA-DSS ont été supprimées puisqu'elles sont incluses sans le *Guide du programme PA-DSS*.	Clarification
Guide de mise en œuvre de la norme PA-DSS	Guide de mise en œuvre de la norme PA-DSS	Davantage de directives sur le *Guide de mise en œuvre de la norme PA-DSS* et clarification du rôle du PA-QSA.	Directives supplémentaires
Instructions et contenu du rapport de conformité	Instructions et contenu du rapport de conformité	Contenu déplacé pour séparer le *Modèle de rapport ROV*.	Clarification
Étapes de mise en conformité avec la norme PA-DSS	Étapes de mise en conformité avec la norme PA-DSS	Section mise à jour pour se concentrer sur le processus d'évaluation plutôt que sur la documentation (détails de la documentation déplacés vers le *Modèle de rapport ROV)*.	Clarification
Guide du programme de la norme PA-DSS	Guide du programme de la norme PA-DSS	Référence supprimée pour la transition PABP, puisqu'il n'y a plus de processus de transition.	Clarification

Conditions et procédures d'évaluation de sécurité de la norme PA-DSS	Conditions et procédures d'évaluation de sécurité de la norme PA-DSS	Termes ajoutés pour définir l'en-tête de colonne de cette section et références supprimées pour les colonnes « En place », « Pas en place » et « Date/Commentaires de cible ».	Clarification

Modifications générales mises en œuvre dans les conditions de la norme PA-DSS	Type
La nouvelle colonne « Directive » décrit le but ou l'objectif de sécurité de chaque condition. La directive indiquée dans cette colonne est destinée à aider à la compréhension de conditions et elle ne remplace pas les Conditions et procédures de test de la norme PA-DSS.	Directives supplémentaires
Les conditions mises à jour et/ou les procédures de test pour illustrer les modifications de la norme PA-DSS, lorsqu'une modification de la norme PA-DSS s'aligne avec une condition de la norme PCI DSS.	Tel que le définit la norme PCI DSS
Termes mis à jour dans les conditions et/ou procédures de test correspondantes à fin d'alignement et de cohérence.	Clarification
Conditions complexes séparées/procédures de test à fin de clarté et procédures de test redondantes/qui se chevauchent éliminées.	Clarification
Procédures de test améliorées pour clarifier le niveau de validation attendu pour chaque condition, y compris : ▪ Requis pour l'information du Guide de mise en œuvre de la norme PA-DSS ▪ Installer l'application conformément au *Guide de mise en œuvre de la norme PA-DSS* pour vérifier la précision des instructions du *Guide de mise en œuvre*.	Clarification
Les autres modifications générales d'édition comprennent : ▪ Élimination des colonnes suivants : « En place », « Pas en place » et « Date/Commentaires de cible ». ▪ Nouvelle numérotation des conditions et des procédures pour faciliter les modifications. ▪ Nouveau format des conditions et des procédures de test pour faciliter la lisibilité, par ex. format du contenu de paragraphe modifié pour inclure des puces, etc. ▪ Apport de modification mineure de terminologie pour une meilleure lisibilité. ▪ Correction des erreurs typographiques.	Clarification

Condition		Modification	Type
v2.0 PA-DSS	v3.0 PA-DSS		
Condition 1			
Condition 1 – Généralités		Titre mis à jour par souci de cohérence, pour remplacer « bande magnétique » par « données de piste ».	Clarification
1.1.c	1.1.1 – 1.1.3	Élimination des procédures de test 1.1.c et ajout des instructions portant sur les procédures de test connexes pour les conditions 1.1.1 à 1.1.3.	Clarification
Condition 2			

Condition		Modification	Type
v2.0 PA-DSS	**v3.0 PA-DSS**		
2.x	2.x	Ajout de composants du *Guide de mise en œuvre de la norme PA-DSS* aux procédures de test de cette section.	Évolution de la condition
2.1	2.1	Changement de terminologie pour faire référence à la suppression sécurisée des données plutôt que la purge.	Clarification
2.2	2.2	Procédures de test améliorées pour demander une validation des fonctions de masquage de PAN.	Clarification
2.4		Condition supprimée concernant l'utilisation de solutions de cryptage de disque. Nouvelle numérotation des conditions consécutives en fonction	Évolution de la condition
2.6.x	2.5.x	Procédures de test mises à jour pour clarifier le fait que les techniques de gestion de clés doivent être testées correctement.	Clarification
2.7	2.6	Mise à jour pour clarifier le fait que le fournisseur d'application doit fournir un mécanisme pour éliminer les matériaux cryptographiques essentiels, si la version actuelle ou précédente utilisait des matériaux ou des cryptogrammes des clés cryptographiques.	Clarification
Condition 3			
3.1	3.1	Note déplacée de l'ancienne procédure de test 3.1.b à la condition 3.1.	Clarification
3.1.b – 3.1.c	3.1.1 – 3.1.2	Nouvelles conditions créées à partir des anciennes procédures de test 3.1.b - 3.1.c pour garantir que les mots de passe par défaut sont appliqués par l'application et validés correctement.	Clarification
3.1.4	3.1.7	Condition déplacée vers 3.1.7 pour une meilleure organisation des conditions.	Clarification
3.1.6 – 3.1.7	3.1.6	Conditions de complexité combinée de mot de passe pour s'aligner avec la v3.0 de la norme PCI DSS et donner une meilleure flexibilité pour les alternatives de composition de mot de passe qui respectent les conditions de robustesse minimum.	Clarification
3.3	3.3.1 – 3.3.2	Condition 3.3 divisée en deux conditions pour se concentrer de manière séparée sur les mots de passe *transmis* (3.3.1) et les mots de passe *stockés* (3.3.2). Mise à jour 3.3.2 pour exiger l'utilisation d'un algorithme cryptographique unilatéral avec une variable d'entrée unique pour rendre les mots de passe illisibles.	Évolution de la condition

Condition		Modification	Type
v2.0 PA-DSS	**v3.0 PA-DSS**		
	3.4	Nouvelle condition pour que les applications limitent l'accès aux fonctions/ressources requises et appliquent le moins de privilèges pour les comptes intégrés.	Évolution de la condition
Condition 4			
4.2.5	4.2.5	Condition mise à jour pour clarifier les types de mécanismes d'identification et d'authentification qui doivent être mentionnés dans les journaux, y compris la création de nouveaux comptes.	Clarification
Condition 5			
5.1	5.1	Condition améliorée pour comprendre les analyses de sécurité dans les processus de développement.	Évolution de la condition
	5.1.5	Nouvelle condition pour que les développeurs d'applications de paiement vérifient l'intégrité du code source pendant le processus de développement.	Évolution de la condition
	5.1.6	Nouvelle condition pour que les applications de paiement soient développées selon les meilleures pratiques du secteur pour la sécurisation des techniques d'encodage, y compris : ▪ Développer avec le moins de privilèges possible pour l'environnement. ▪ Développer des paramètres de sécurité par défaut, par exemple, toute exécution est refusée par défaut sauf spécification contraire lors de la conception initiale. ▪ Développer des considérations de tous les points d'accès, y compris les entrées de variations telles que les entrées multi-canal dans l'application. ▪ Documentation de la manière dont les PAN et/ou SAD sont traités dans la mémoire.	Évolution de la condition
	5.1.7	Nouvelle condition créée à partir des anciennes procédures de test 5.2.a et 5.2.b pour que les développeurs d'applications de paiement soient formés aux pratiques de développement sécurisées.	Clarification
5.2	5.2	Condition mise à jour pour centrer la prévention des vulnérabilités d'encodage courantes.	Clarification
	5.2.10	Nouvelle condition pour traiter de la « rupture dans la gestion des authentifications et des sessions ».	Évolution de la condition
5.4	8.2	Condition déplacée vers 8.2 pour s'aligner avec les autres conditions qui facilitent la sécurisation de l'environnement PCI DSS et conserver la condition 5.x centrée sur les pratiques de développement de logiciel.	Clarification

Condition		Modification	Type
v2.0 PA-DSS	**v3.0 PA-DSS**		
	5.4	Nouvelle condition pour que le fournisseur d'applications de paiement définisse et mette en œuvre une méthodologie de gestion des versions conforme au *Guide du programme de la norme PA-DSS*.	Évolution de la condition
	5.5	Nouvelle condition pour que les fournisseurs d'applications de paiement incorporent des techniques d'évaluation des risques dans leur processus de développement logiciel.	Évolution de la condition
	5.6	Nouvelle condition pour que les fournisseurs d'applications de paiement mettent en œuvre un processus d'autorisation formelle avant le lancement final.	Évolution de la condition
Condition 6			
6.1 – 6.2	6.1 – 6.3	Conditions réorganisées pour clarifier les contrôles qui s'appliquent à toutes les applications et les contrôles qui s'appliquent uniquement quand le sans-fil est utilisé ou qu'il est prévu qu'il soit utilisé avec l'application de paiement. Nouvelle condition 6.3 créée à partir de la procédure de test formelle 6.2.b.	Clarification
Condition 7			
Condition 7 – Généralités		Le titre mis à jour reflète l'intention de la condition (répondre aux vulnérabilités *et maintenir les mises à jour de l'application)*.	Clarification
7.1	7.1.1 – 7.1.3	Divisés en conditions séparées et nécessitant l'utilisation de sources « de confiance » pour les informations sur les vulnérabilités en matière de sécurité.	Clarification
7.2	7.2.1 – 7.2.2	Divisé en deux conditions séparées.	Clarification
	7.3	Nouvelle condition pour que le fournisseur d'application donne des notes de lancement pour toutes les mises à jour de l'application.	Évolution de la condition
Condition 8			
8.1	8.1	Exemple développé pour clarifier l'objectif de la condition.	Clarification
5.4	8.2	Condition déplacée de 5.4 pour s'aligner avec les autres conditions qui facilitent la sécurisation de l'environnement PCI DSS.	Clarification

Condition		Modification	Type
v2.0 PA-DSS	**v3.0 PA-DSS**		
10.1	8.3	Condition déplacée de 10.1 pour s'aligner avec les autres conditions qui facilitent la sécurisation de l'environnement PCI DSS.	Clarification
Condition 9			
9.1	9.1	Terminologie ajoutée pour clarifier l'objectif de la condition selon lequel il n'est pas demandé aux serveurs Web et aux composants de stockage de données du titulaire d'être dans le même réseau, avec les bases de données comme exemple d'un composant de stockage de données du titulaire et la DMZ comme exemple de zone réseau.	Clarification
Condition 10			
10.1	8.3	Condition déplacée de 8.3 pour s'aligner avec les autres conditions qui facilitent la sécurisation de l'environnement PCI DSS. Nouvelle numérotation des conditions ultérieures.	Clarification
10.2	10.1	La condition clarifiée s'applique aux accès à distance provenant de l'extérieur du réseau du client.	Clarification
	10.2.2	Nouvelle condition pour que les fournisseurs qui assurent des services d'assistance/maintenance aux clients maintiennent des justificatifs d'authentification uniques pour chaque client.	Évolution de la condition
10.3.2	10.2.3	Mise à jour pour clarifier le fait que cette condition s'applique à tous les types d'accès à distance.	Clarification
Condition 11			
11.1	11.1	Les mises à jour mineures offrent une plus grande clarté et s'alignent avec la norme PCI DSS.	Clarification
Condition 12			
12.1	12.1 12.2	Conditions réorganisées pour clarifier les contrôles qui s'appliquent à toutes les applications et les contrôles qui s'appliquent uniquement quand l'application de paiement facilite l'accès administratif non console.	Clarification
Condition 13			
Condition 13 – Généralités		Changement de titre pour se concentrer sur les conditions du *Guide de mise en œuvre de la norme PA-DSS*. Conditions relatives à la documentation d'instruction et aux programmes de formation déplacées vers la nouvelle condition 14.	Clarification

Condition		Modification	Type
v2.0 PA-DSS	**v3.0 PA-DSS**		
	13.1.1	Nouvelle condition pour valider que le *Guide de mise en œuvre de la norme PA-DSS* est spécifique à l'application et à la version ou aux versions à évaluer.	Clarification
13.1.3	13.1.3	L'objectif clarifié est que le *Guide de mise en œuvre de la norme PA-DSS* soit révisé et mis à jour lorsque l'application ou les conditions de la norme PA-DSS changent.	Clarification
Condition 14			
Condition 14 – Généralités		Voir « Généralités – 13 » ci-dessus. Nouvelle condition pour se concentrer la documentation d'instruction et les programmes de formation, y compris la formation interne pour le personnel du fournisseur aux responsabilités de la norme PA-DSS.	Clarification
	14.1	Nouvelle condition pour apporter les informations en matière de sécurité et la formation à la norme PA-DSS pour le personnel du fournisseur ayant des responsabilités au regard de la norme PA-DSS.	Évolution de la condition
	14.2	Nouvelle condition pour l'affectation des responsabilités pour la norme PA-DSS du personnel du fournisseur.	Évolution de la condition
13.2	14.3	Conditions améliorées précédemment incluses en 13 pour les programmes de formation d'intégrateur/revendeur. L'objectif clarifié est que la documentation de formation soit révisée et mise à jour lorsque l'application ou les conditions de la norme PA-DSS changent.	Clarification
Annexe B			
Confirmation de la configuration du laboratoire de test spécifique à l'évaluation de la norme PA-DSS	Configuration du laboratoire de test pour les évaluations de la norme PA-DSS	Annexe réorientée pour donner des informations concernant les attentes et les capacités du laboratoire utilisé pour conduire les évaluations de la norme PA-DSS. Détails et modèle pour documenter la configuration de laboratoire de test déplacée vers un *modèle de rapport ROV PA-DSS* séparé.	Clarification