Industrie des cartes de paiement (PCI)

Norme de sécurité des données d'application de paiement

Récapitulatif des modifications entre les versions 3.0 et 3.1 la norme PA-DSS

Juin 2015

Introduction

Ce document apporte un récapitulatif des modifications entre la v3.0 et la v3.1 de la norme PA-DSS. Le tableau 1 donne un aperçu des types de modifications. Le tableau 2 résume les modifications importantes qui se trouvent dans la v3.1 de la norme PA-DSS.

Tableau 1 : Types de modification

[1]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[1]
v3.0 PA-DSS	v3.1 PA-DSS		
Tous	Tous	Correction d'erreurs typographiques mineures (grammaire, ponctuation, mise en forme, etc.) et mises à jour mineures incorporées pour une meilleure lisibilité du document.	Clarification
Tous	Tous	Référence modifiée de « commerçant » à « client » lorsqu'il est question des entités qui utilisent les applications de paiement.	Clarification
Informations relatives aux conditions d'application de la norme PCI DSS	Informations relatives aux conditions d'application de la norme PCI DSS	Référence modifiée de « institutions financières » à « acquéreurs, émetteurs ». Clarification informant que la norme PCI DSS s'applique à toute entité qui stocke, traite ou transmet des données de compte.	Clarification
2.3	2.3	Clarification dans la note de l'exigence indiquant que des contrôles supplémentaires sont nécessaires si des versions tronquées et hachées du même PAN sont générées par l'application de paiement. Ajout de la procédure de test 2.3.c pour la validation de la note, et renumérotation des procédures de test subséquentes.	Clarification

2.4	2.4	Mise à jour de la directive visant à clarifier que les clés de cryptage de clés ne doivent pas être cryptées. Elles doivent toutefois être protégées conformément à l'exigence 2.4.	Directives supplémentaires
2.5	2.5	Remplacement de « cryptage » par « cryptographique » dans la procédure de test pour l'harmoniser avec l'exigence.	Clarification
3.1.a	3.1.a	Mise à jour de la procédure de test afin de clarifier que la directive du *Guide de mise en œuvre de la norme PA-DSS* comprend l'affectation d'une authentification sécurisée à tous les comptes par défaut de l'environnement, et que tout compte par défaut qui n'est pas utilisé doit être désactivé ou laissé de côté.	Clarification
3.1.7	3.1.7	Clarification que les mots de passe doivent être changés au moins *une fois* tous les 90 jours.	Clarification
5.1.d	5.1.d	Mise à jour de la procédure de test pour l'harmoniser à l'exigence.	Clarification
5.3.3.a 5.4.1.c	5.3.3.a 5.4.1.c	Termes mis à jour dans les procédures de test à fin de cohérence.	Clarification
5.4.3.a	5.4.3.a	Puces des procédures de test combinées pour éviter la redondance.	Clarification
5.4.5.b	5.4.5.b	Mise à jour de la procédure de test pour l'harmoniser à la condition.	Clarification
6.3	6.3	Suppression des termes redondants dans la procédure de test.	Clarification
8.2	8.2	Suppression de SSL comme exemple d'une technologie de sécurité. Ajout d'une note informant que le SSL et TLS initial ne sont pas considérés comme des cryptographies fortes et que les applications de paiement ne peuvent pas utiliser ou prendre en charge l'utilisation de SSL et TLS initial. Impact également les exigences 11.1 et 12.1 – 12.2.	Évolution de la condition
8.3	8.3	Mise à jour par soucis de cohérence avec PCI DSS.	Clarification
10.2.2	10.2.2	Clarification du fait qu'un justificatif d'authentification unique doit être utilisé pour chaque client.	Clarification
11.1	11.1	Suppression du SSL comme exemple de technologie sûre et note ajoutée à l'exigence. Voir l'explication ci-dessus au 8.2.	Évolution de la condition
12.1 – 12.2	12.1 – 12.2	Suppression du SSL comme exemple de technologie sûre et note ajoutée à l'exigence. Voir l'explication ci-dessus au 8.2.	Évolution de la condition

Annexe A : Résumé du contenu du Guide de mise en œuvre de la norme PA-DSS	Annexe A : Résumé du contenu du Guide de mise en œuvre de la norme PA-DSS	Mise à jour afin de refléter les modifications apportées aux exigences, le cas échéant.	Clarification