Industrie des cartes de paiement (PCI)

Norme de sécurité des données

Récapitulatif des modifications entre les versions 3.1 et 3.2 de la norme PCI DSS

Avril 2016

Introduction

Ce document récapitule les modifications entre les versions 3.1 et 3.2 de la norme PCI DSS. Le tableau 1 donne un aperçu des types de modifications. Le tableau 2 résume les modifications importantes qui se trouvent dans la version 3.2 de la norme PCI 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]
PCI DSS v3.1	**PCI DSS v3.2**		
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
Relation entre les normes PCI DSS et PA-DSS	Relation entre les normes PCI DSS et PA-DSS	Ajout de directives concernant les menaces de sécurité qui sont en constante évolution et les applications de paiement non prises en charge par le fournisseur sont susceptibles de ne pas offrir le même niveau de sécurité que la version supportée.	Directives supplémentaires
Portée des conditions de la norme PCI DSS	Portée des conditions de la norme PCI DSS	Clarification sur les sites de sauvegarde/rétablissement à prendre en considération pour confirmer la portée des conditions de la norme PCI DSS.	Clarification
Meilleures pratiques d'implémentation de la norme PCI DSS dans les processus d'affaires courantes	Meilleures pratiques d'implémentation de la norme PCI DSS dans les processus d'affaires courantes	Mise à jour de la section Remarque pour clarifier que certains principes d'affaires courantes peuvent être des conditions pour certaines entités, comme ceux définis dans l'Annexe A3 intitulée Validation complémentaire des entités désignées.	Clarification
	Versions de PCI DSS	Nouvelle section pour décrire l'incidence de cette version de la norme PCI DSS sur l'ancienne version en vigueur.	Directives supplémentaires
Conditions			
Généralités	Généralités	Suppression d'exemples de protocoles « robustes » ou « sécurisés » dans plusieurs conditions, car ils peuvent faire l'objet de modifications à tout moment.	Clarification
Généralités	Généralités	Suppression d'exemples dans plusieurs conditions et/ou procédures de test dans la colonne Directive, et ajout de directives, le cas échéant.	Clarification
Généralités	Généralités	Modification des « mots de passe/locutions » en « mots de passe/locutions de passage » dans plusieurs conditions dans un souci de cohérence.	Clarification
Généralités	Généralités	Clarification sur le fait que le terme approprié est « Authentification à plusieurs facteurs » plutôt que « Authentification à deux facteurs », car plus de deux facteurs peuvent être utilisés.	Clarification

Section		Modification	Type[1]
PCI DSS v3.1	**PCI DSS v3.2**		
Généralités	Généralités	Suppression des remarques dans les conditions se rapportant à la date d'entrée en vigueur du 1er juillet 2015, car celles-ci sont désormais en vigueur. Les conditions concernées sont : 6.5.10, 8.5.1, 9.9, 11.3 et 12.9.	Clarification
1.1.6	1.1.6	Clarification sur l'approbation de l'utilisation commerciale incluse dans la justification. Suppression d'exemples de protocoles « non sécurisés », car ils peuvent faire l'objet de modifications conformément aux exigences sectorielles.	Clarification
1.2.1	1.2.1	Ajout de directives pour clarifier l'objectif de la condition.	Clarification
1.3	1.3	Ajout de directives pour clarifier l'objectif de la condition.	Clarification
1.3.3		Suppression de la condition en tant qu'objectif par le biais d'autres conditions dans 1.2 et 1.3.	Clarification
1.3.4 – 1.3.8	1.3.3 – 1.3.7	Nouvelle numérotation en raison de la suppression de l'ancienne condition 1.3.3.	Clarification
1.3.6	1.3.5	Mise à jour pour clarifier l'objectif de la condition plutôt que l'utilisation d'un type particulier de technologie.	Clarification
1.4	1.4	Meilleure flexibilité en spécifiant *ou une fonctionnalité équivalente* pour offrir une autre solution au logiciel de pare-feu personnel. La condition clarifiée s'applique à tous les appareils informatiques portables qui se connectent à Internet en dehors du réseau et qui peuvent également accéder au CDE.	Clarification
2.1	2.1	La condition clarifiée s'applique aux applications de paiement.	Clarification
2.2.3	2.2.3	Suppression de la remarque et des procédures de test concernant la suppression du SSL/TLS initial et son passage dans la nouvelle Annexe A2.	Clarification

Section		Modification	Type[1]
PCI DSS v3.1	PCI DSS v3.2		
2.3	2.3	Suppression de la remarque et des procédures de test concernant la suppression du SSL/TLS initial et son passage dans la nouvelle Annexe A2. Suppression de la référence à la « gestion Web », car la condition spécifie déjà « tous les accès administratifs non-console », condition qui par définition comprend tout accès au Web.	Clarification
3.3	3.3	Mise à jour de la condition pour clarifier que tout affichage du PAN supérieur aux six premiers/quatre derniers chiffres du PAN requiert un besoin professionnel légitime. Ajout de directives sur les scénarios courants de masquage.	Évolution de la condition
3.4.d	3.4.d	Mise à jour de la procédure de test pour clarifier que l'examen des journaux d'audit comprend les journaux d'applications de paiement.	Clarification
3.4.1	3.4.1	Ajout de la remarque pour clarifier que cette condition s'applique aussi à toutes les autres conditions de gestion des clés et de cryptage PCI DSS.	Clarification
	3.5.1	Nouvelle condition pour les prestataires de services en vue de conserver une description documentée de l'architecture cryptographique. *Date d'entrée en vigueur 1er février 2018*	Évolution de la condition
3.5.1 – 3.5.3	3.5.2 – 3.5.4	Nouvelle numérotation suite à l'ajout de la nouvelle condition 3.5.1.	Clarification
3.6.1.b	3.6.1.b	Mise à jour de la procédure de test pour clarifier que le test suppose l'observation des procédures plutôt que la méthode de génération de clé, car cela ne doit pas faire l'objet d'une observation. Ajout de directives se rapportant à la définition dans le glossaire de la « Génération de clés cryptographiques »	Clarification
4.1	4.1	Suppression de la remarque et des procédures de test concernant la suppression du SSL/TLS initial et son passage dans la nouvelle Annexe A2.	Clarification
6.2	6.2	Ajout de clarification dans la colonne Directive pour indiquer que la condition du correctif de tous les logiciels comprend les applications de paiement.	Clarification
6.4.4	6.4.4	Mise à jour de la condition afin de s'harmoniser avec la procédure de test.	Clarification

Section		Modification	Type[1]
PCI DSS v3.1	PCI DSS v3.2		
6.4.5	6.4.5	Clarification portant sur les processus de contrôle de changement, qui ne sont pas limités aux correctifs et aux modifications logicielles.	Clarification
	6.4.6	Nouvelle condition pour les processus de contrôle de changement, qui consiste à inclure la vérification des conditions de la norme PCI DSS affectées par une modification. *Date d'entrée en vigueur 1er février 2018*	Évolution de la condition
6.5	6.5	Clarification pour indiquer que les développeurs doivent suivre une formation actualisée et au moins une fois par an.	Clarification
6.5.a – 6.5.d	6.5.a – 6.5.c	Suppression de la procédure de test 6.5.b et nouvelle numérotation des autres procédures de test.	Clarification
7.2	7.2	Mise à jour de la condition, des procédures de test et de la colonne Directive pour indiquer qu'au moins un système de contrôle d'accès est utilisable.	Clarification
Condition 8	Condition 8	Ajout de la remarque à l'introduction de la condition 8 pour indiquer que les conditions d'authentification ne s'appliquent pas aux comptes utilisés par les consommateurs (par ex. les titulaires de carte).	Clarification
8.1.5	8.1.5	Clarification de la condition destinée à toutes les parties tierces, et non seulement aux fournisseurs, munies d'un accès à distance.	Clarification
8.2.3	8.2.3	Mise à jour de la colonne Directive pour illustrer les modifications des normes sectorielles.	Clarification
8.3	8.3	Clarification sur le fait que le terme approprié est « Authentification à plusieurs facteurs » plutôt que « Authentification à deux facteurs », car plus de deux facteurs peuvent être utilisés.	Clarification

Section		Modification	Type[1]
PCI DSS v3.1	**PCI DSS v3.2**		
8.3	8.3, 8.3.1, 8.3.2	Développement de la condition 8.3 en sous-conditions pour exiger une authentification à plusieurs facteurs de tous les membres du personnel dotés d'un accès administratif non-console et d'un accès à distance au CDE. La nouvelle condition 8.3.2 porte sur l'authentification à plusieurs facteurs de tous les membres du personnel dotés d'un accès à distance au CDE (incorpore l'ancienne condition 8.3). La nouvelle condition 8.3.1 gère l'authentification à plusieurs facteurs de tous les membres du personnel dotés d'un accès administratif non-console au CDE. *Date d'entrée en vigueur 1er février 2018 pour la condition 8.3.1*	Évolution de la condition
9.1.1	9.1.1	Clarification du mode d'utilisation des caméras vidéo ou des mécanismes de contrôle d'accès (ou les deux).	Clarification
9.5.1.a – 9.5.1.b	9.5.1	Association des procédures de test pour indiquer que l'évaluateur vérifie que l'emplacement de stockage est examiné au moins une fois par an.	Clarification
	10.8, 10.8.1	Nouvelle condition pour les prestataires de services afin qu'ils détectent et signalent les pannes des systèmes de contrôle de sécurité critiques. *Date d'entrée en vigueur 1er février 2018*	Évolution de la condition
10.8	10.9	Nouvelle numérotation suite à l'ajout de la nouvelle condition 10.8.	Clarification
11.2.1	11.2.1	Clarification portant sur toutes les vulnérabilités à « risque élevé », qui doivent être traitées conformément à la classe de vulnérabilité de l'entité (comme défini dans la condition 6.1) et vérifiées par de nouvelles analyses.	Clarification
11.3.4	11.3.4	Ajout de la procédure de test 11.3.4.c pour confirmer que le test de pénétration est effectué par une ressource interne qualifiée ou un tiers externe qualifié.	Clarification
	11.3.4.1	Nouvelle condition pour les prestataires de services en vue d'effectuer le test de pénétration sur les contrôles de segmentation au moins une fois par semestre. *Date d'entrée en vigueur 1er février 2018*	Évolution de la condition

Section		Modification	Type[1]
PCI DSS v3.1	**PCI DSS v3.2**		
11.5.a	11.5.a	Suppression de la mention « au sein de l'environnement des données de titulaires de carte » dans la procédure de test, dans un souci de cohérence avec la condition. En effet, cette condition peut s'appliquer aux systèmes critiques situés en dehors du CDE désigné.	Clarification
12.3.3	12.3.3	Reformatage de la procédure de test à des fins de simplification.	Clarification
	12.4	Nouvelle condition pour l'équipe de direction des prestataires de services devant définir des responsabilités relatives à la protection des données de titulaires de carte et un programme de conformité à la norme PCI DSS. *Date d'entrée en vigueur 1er février 2018*	Évolution de la condition
12.4	12.4.1	Nouvelle numérotation suite à l'ajout de la nouvelle condition 12.4.	Clarification
12.6	12.6	Clarification de l'objectif du programme de sensibilisation à la sécurité, qui doit sensibiliser le personnel à l'importance de la politique et des procédures de sécurité des données de titulaires de carte.	Clarification
12.8.1	12.8.1	Clarification sur le fait que la liste des prestataires de services doit inclure une description des services fournis.	Clarification
12.8.2	12.8.2	Ajout de directives stipulant que la responsabilité des prestataires de services dépendra du service fourni et de l'accord entre les deux parties.	Directives supplémentaires
12.10.2	12.10.2	Clarification pour préciser que l'examen du plan de réponse aux incidents englobe tous les éléments répertoriés dans la condition 12.10.1.	Clarification
	12.11, 12.11.1	Nouvelle condition destinée aux prestataires de services qui doivent effectuer des examens au moins une fois par trimestre pour confirmer que le personnel respecte les politiques de sécurité et les procédures opérationnelles. *Date d'entrée en vigueur 1er février 2018*	Évolution de la condition
Annexe A	Annexe A1	Nouvelle numérotation dans l'Annexe « *Autres conditions de la norme PCI DSS s'appliquant aux fournisseurs d'hébergement partagé* » compte tenu de l'insertion de nouvelles annexes.	Clarification

Section		Modification	Type[1]
PCI DSS v3.1	**PCI DSS v3.2**		
	Annexe A2	Nouvelle annexe avec des conditions supplémentaires pour les entités utilisant le SSL/TLS initial en insérant de nouvelles dates butoir de migration pour supprimer le SSL/TLS initial.	Clarification
	Annexe A3	Nouvelle annexe pour insérer la section « Validation complémentaire des entités désignées (DESV) », qui faisait précédemment partie d'un document distinct.	Clarification