PCI Security Standards Council

PCI (Payment Card Industry)
Norme PA-DSS

Conditions et procédures d’évaluation de sécurité

Version 3.2

Mai 2016

Modifications apportées au document

Date	Version	Description	Pages
1er octobre 2008	1.2	Harmonisation du contenu avec la nouvelle procédure PCI DSS v1.2 et implémentation des changements mineurs notés depuis la v1.1 d'origine.	
Juillet 2009	1.2.1	Sous « Champ d'application de la norme PA-DSS », harmonisez le contenu avec le Guide du programme PA-DSS, v1.2.1, pour clarifier les applications auxquelles s'applique la norme PA-DSS.	v, vi
		Dans Conditions de laboratoire 6, correction de l'orthographe de « OWASP »	30
		Dans Attestation de conformité, partie 2a, mise à jour de la « fonctionnalité des applications de paiement » pour qu'elle soit cohérente avec les types d'application indiqués dans le Guide du programme PA-DSS et clarification des procédures de revalidation annuelles dans la partie 3b	32, 33
Octobre 2010	2.0	Mise à jour et implémentation des changements mineurs depuis la version 1.2.1 et harmonisation avec la nouvelle procédure PCI DSS v2.0 Pour plus de détails, consulter *PA-DSS – Récapitulatif des changements entre les versions 1.2.1 et 2.0 de la norme PA-DSS.*	
Novembre 2013	3.0	Mise à jour de la norme PA-DSS v2. Pour plus de détails, veuillez consulter *PA-DSS – Récapitulatif des changements entre les versions 2.0 et 3.0 de la norme PA-DSS.*	
Mai 2015	3.1	Mise à jour de la norme PA-DSS v3.0. Pour plus de détails sur les changements, veuillez consulter *PA-DSS – Récapitulatif des changements entre les versions 3.0 et 3.1 de la norme PA-DSS*.	
Mai 2016	3.2	Mise à jour de la norme PA-DSS v3.1. Pour plus de détails sur les changements, veuillez consulter *PA-DSS – Récapitulatif des changements entre les versions 3.1 et 3.2 de la norme PA-DSS*.	

Table des matières

Modifications apportées au document 2
Introduction 5
Objectif de ce document 5
Relation entre les normes PCI DSS et PA-DSS 5
Revendeurs et intégrateurs 7
Informations relatives aux conditions d'application de la norme PCI DSS 7
Champ d'application de la norme PA-DSS 10
Guide de mise en œuvre de la norme PA-DSS 13
Conditions relatives aux évaluateurs de sécurité qualifiés des applications de paiement (PA-QSA) 14
Laboratoire de test 14
Instructions et contenu du rapport de conformité 14
Étapes de mise en conformité avec la norme PA-DSS 15
Guide du programme de la norme PA-DSS 15
Conditions et procédures d'évaluation de sécurité de la norme PA-DSS 16
Condition 1 : Ne pas conserver la totalité des données de bande magnétique, de code ou de valeur d'audit de carte (CAV2, CID, CVC2, CVV2), ou de données de bloc PIN 17
Condition 2 : Protéger les données de titulaires de carte stockées 23
Condition 3 : Fournir des fonctions d'authentification sécurisées 32
Condition 4 : Enregistrer l'activité de l'application de paiement 43
Condition 5 : Développer des applications de paiement sécurisées 47
Condition 6 : Protéger les transmissions sans-fil 68
Condition 7 : Tester les applications de paiement pour gérer les vulnérabilités et maintenir leurs mises à jour 72
Condition 8 : Permettre la mise en œuvre de réseaux sécurisés 76
Condition 9 : Les données de titulaires de carte ne doivent jamais être stockées sur un serveur connecté à Internet 78
Condition 10 : Faciliter l'accès à distance sécurisée à l'application de paiement 80
Condition 11 : Crypter le trafic sensible transitant par les réseaux publics 84
Condition 12 : Sécuriser tous les accès administratifs non-console 86
Condition 13 : Maintenir un Guide de mise en œuvre de la norme PA-DSS pour les clients, les revendeurs et les intégrateurs 88
Condition 14 : Affecter des responsabilités vis-à-vis de la norme PA-DSS au personnel et maintenez des programmes de formation pour le personnel, les clients, les revendeurs et les intégrateurs 90

Annexe A : Résumé du contenu du *Guide de mise en œuvre de la norme PA-DSS* 93
Annexe B : Configuration du laboratoire de test pour les évaluations de la norme PA-DSS. 110

Introduction

Objectif de ce document

Les procédures et exigences d'évaluation de sécurité de la Norme de sécurité des données de l'application de paiement PCI (PA-DSS) définissent les procédures et exigences d'évaluation de sécurité pour les fournisseurs de logiciels d'applications de paiement. Ce document est destiné à être utilisé par les évaluateurs de sécurité qualifiés des applications de paiement (PA-QSA) responsables de l'évaluation des applications de paiement, pour valider la conformité d'une application de paiement avec la norme PA-DSS. Pour de plus amples détails sur la documentation d'une évaluation PA-DSS et sur la création d'un rapport sur la validation (ROV), le PA-QSA doit se référer au *modèle de rapport PA-DSS ROV,* disponible sur le site Web du Conseil des normes de sécurité PCI (PCI SSC) —www.pcisecuritystandards.org.

Des ressources supplémentaires comprenant les attestations de conformité, la foire aux questions (FAQ) et le *glossaire des termes, abréviations, et acronymes PCI DSS et PA-DSS* sont disponibles sur le site Web du Conseil des normes de sécurité PCI (PCI SSC) – www.pcisecuritystandards.org.

Relation entre les normes PCI DSS et PA-DSS

L'utilisation d'une application, conforme à la norme PA-DSS en elle-même, n'en fait pas une entité conforme aux normes PCI DSS, car elle doit être mise en œuvre dans un environnement respectant ces normes, conformément au *Guide de mise en œuvre de la norme PA-DSS* remis par le fournisseur d'applications de paiement (d'après la condition 13 de la norme PA-DSS). Les exigences de la norme PA-DSS sont issues *des conditions et procédures d'évaluation de la Norme de sécurité de l'industrie des cartes de paiement (PCI DSS)*, qui détaillent ce qui est requis pour la conformité à la norme PCI DSS (et donc ce qu'une application de paiement doit prendre en charge pour facilité la conformité PCI DSS du client). Le PCI DSS se trouve sur www.pcisecuritystandards.org.

Toutes les applications qui stockent, traitent ou transmettent les données de titulaires de carte peuvent faire l'objet d'une évaluation PCI DSS d'entité, y compris les applications qui ont été validées pour PA-DSS. L'évaluation PCI DSS doit vérifier que l'application de paiement PA-DSS est correctement configurée et implémentée de manière sécuritaire selon les exigences PCI DSS. Si l'application de paiement a subi une personnalisation, un examen plus en profondeur sera requis pendant l'évaluation PCI DSS, dans la mesure où l'application est susceptible de ne plus être représentative de la version validée selon PA-DSS

La norme PCI DSS ne s'applique pas directement aux fournisseurs d'applications de paiement à moins que le fournisseur ne stocke, traite ou transmette les données de titulaires de carte, ou a accès aux données de titulaires de carte de leurs clients. Cependant, étant donné que ces applications de paiement sont utilisées par les clients du fournisseur d'application pour stocker, traiter et transmettre des données de titulaires de carte, et que les clients sont dans l'obligation de respecter les normes PCI DSS, les applications de paiement doivent aider, et non empêcher, le client à se conformer aux normes PCI DSS. Voici quelques exemples sur la façon dont les applications de paiement non sécurisées peuvent faire obstacle à la conformité :

1. Stockage des données de bande magnétique et/ou des données équivalentes sur la puce sur le réseau du client après autorisation.
2. Applications exigeant que les clients désactivent d'autres fonctions requises par la norme PCI DSS, comme les programmes antivirus ou les pare-feu, afin que l'application de paiement fonctionne correctement.

3. Utilisation par les fournisseurs de méthodes non sécurisées pour se connecter à l'application lors d'une intervention d'assistance au client.

Les applications de paiement sécurisées, lorsqu'elles sont mises en œuvre dans un environnement conforme aux normes PCI DSS, réduisent le potentiel de failles de sécurité compromettant le numéro de compte primaire (PAN), les données complètes de piste, les codes et valeurs d'audit de carte (CAV2, CID, CVC2, CVV2), les codes et les blocs PIN, ainsi que la fraude résultant de ces failles.

Revendeurs et intégrateurs

Les fournisseurs d'application peuvent engager des intégrateurs et des revendeurs pour vendre, installer et/ou maintenir des applications de paiement de leur part. Les intégrateurs/revendeurs ont un rôle à jouer pour assurer l'installation et le fonctionnement sécuritaires des applications de paiement, dans la mesure où, bien souvent, ils offrent des services en ligne pour les fournisseurs du client et ils aident à l'installation d'applications de paiement validées PA-DSS. Une configuration, maintenance ou support incorrect d'une application peut causer l'introduction de vulnérabilités du point de vue de la sécurité dans l'environnement des données de titulaires de carte du client qui pourraient être exploitées par des pirates. Les vendeurs d'application doivent former leurs clients, les revendeurs et les intégrateurs pour l'installation et la configuration des applications de paiement conformément aux normes PCI DSS.

Les revendeurs et les intégrateurs PCI qualifiés (QIR) sont formés par le Conseil des normes de sécurité PCI et des normes PA-DSS afin de mettre en œuvre les applications de paiement de manière sécuritaire. Pour de plus amples informations sur le programme PCI QIR, veuillez consulter www.pcisecuritystandards.org.

Informations relatives aux conditions d'application de la norme PCI DSS

La norme PCI DSS s'applique à toutes les entités impliquées dans le traitement des cartes de paiement, notamment les commerçants, les entreprises de traitement, les acquéreurs, les émetteurs et les prestataires de service. La norme PCI DSS s'applique également à ***toutes*** les autres entités qui stockent, traitent ou transmettent les données de titulaires de carte et/ou les données d'identification sensibles.

Les données de titulaires de carte et les données d'identification sensibles sont définies comme suit :

Données de compte	
Les données de titulaires de carte comprennent :	**Les données d'identification sensibles comprennent :**
▪ Numéro de compte primaire (Primary Account Number, PAN) ▪ Nom du titulaire de la carte ▪ Date d'expiration ▪ Code service	▪ Données de bande magnétique complètes (données de bande magnétique ou équivalent sur une puce) ▪ CAV2/CVC2/CVV2/CID ▪ Codes/blocs PIN

***Le numéro de compte primaire (PAN) est le facteur de définition des données de titulaires de carte*.** Si le nom du titulaire, le code de service, et/ou la date d'expiration sont stockés, traités ou transmis avec le PAN, ou existent d'une façon ou d'une autre dans l'environnement des données de titulaires de carte (cardholder data environment, CDE), ils doivent être protégés conformément à toutes les conditions applicables au PCI DSS.

Le tableau de la page suivante illustre les éléments communément utilisés des données de titulaires de carte et d'authentification sensibles, si le stockage de chaque élément de données est autorisé ou interdit, et précise si chaque élément de données doit être protégé. Ce tableau n'est pas exhaustif, mais est présenté de manière à illustrer les différentes conditions qui s'appliquent à chaque élément de données.

		Élément de données	Stockage autorisé	Rendre illisibles les données de compte stockées selon la condition 2.3 de la norme PA-DSS
Données de compte	**Données de titulaires de 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'identification sensibles[1]	Données complètes de piste magnétique [2]	Non	Stockage interdit selon la condition 1.1 de la norme PA-DSS
		CAV2/CVC2/CVV2/CID[3]	Non	Stockage interdit selon la condition 1.1 de la norme PA-DSS
		Code/bloc PIN[4]	Non	Stockage interdit selon la condition 1.1 de la norme PA-DSS

Les exigences 2.2 et 2.3 de la norme PA-DSS s'appliquent uniquement au PAN. Si le PAN est stocké avec d'autres données de titulaires de carte, seul le PAN doit être rendu illisible selon la condition 2.3 de la norme PA-DSS.

Les données d'identification sensibles ne doivent pas être stockées après autorisation, même si elles sont cryptées. Cela s'applique même lorsqu'il n'y a pas de PAN dans l'environnement.

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

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

3 *Le nombre à trois ou quatre chiffres figurant au recto ou au verso de la carte de paiement*

4 *Le numéro d'identification personnel saisi par le titulaire de la carte lors d'une transaction carte présente et/ou le bloc PIN crypté présent dans le message de la transaction*

Champ d'application de la norme PA-DSS

La norme PA-DSS s'applique aux fournisseurs de logiciels et autres qui développent des applications de paiement qui stockent, traitent ou transmettent des données de titulaires de carte et/ou des données d'identification sensibles. Pour de plus amples informations concernant les différents types d'application, veuillez consulter le *Guide du programme de la norme PA-DSS*.

Le champ d'application de l'évaluation PA-DSS doit comprendre les points suivants :

- Couverture de toutes les fonctionnalités des applications de paiement, y compris, mais non limité à :
  1) Fonctions de paiement complètes (autorisation et règlement),
  2) Entrées et sorties,
  3) Conditions d'erreur,
  4) Interfaces et connexions aux autres fichiers, systèmes et /ou application de paiement ou composants d'application,
  5) Tous les flux de données de titulaires de carte,
  6) Mécanisme de cryptage et
  7) Mécanismes d'authentification.
- Couverture de l'assistance que le fournisseur de l'application de paiement est tenu de proposer aux clients et aux revendeurs/intégrateurs (voir le *Guide de mise en œuvre de la norme PA-DSS* plus loin dans ce document) pour vous assurer que :
  1) Le client sait comment implémenter l'application de paiement conformément aux normes PCI DSS et
  2) Le client est clairement avisé que certaines configurations d'environnement et d'application de paiement peuvent nuire à sa conformité PCI DSS.

  Remarquer que le fournisseur de paiement d'application pourrait offrir de tels conseils même quand la configuration spécifique :
  1) Ne peut pas être contrôlée par le fournisseur d'application de paiement une fois que l'application est installée par le client, ou
  2) Est la responsabilité du client, pas du fournisseur d'application de paiement.
- Couverture de toutes les plates-formes sélectionnées pour la version vérifiée de l'application de paiement (les plates-formes incluses doivent être indiquées).
- Couverture des outils utilisés par ou au sein d'une application de paiement pour accéder et/ou consulter des données de titulaires de carte (outils de reporting, de journalisation, etc.).
- Couverture de tous les composants logiciels relatifs à l'application de paiement, y compris les exigences et les dépendances des logiciels tiers
- Couverture de tout autre type d'applications de paiement nécessaires pour une mise en œuvre complète
- Couverture de la méthodologie de gestion des versions du fournisseur

Conditions d'application de la norme PA-DSS aux terminaux matériels

Cette section donne des directives aux fournisseurs qui souhaitent obtenir une validation PA-DSS pour les applications de paiement résidentes sur des terminaux matériels (également terminaux autonomes ou dédiés).

Une application de paiement résidente sur un terminal matériel peut obtenir la validation PA-DSS de deux manières :

1. L'application de paiement résidente remplit directement les conditions PA-DSS et est validée selon les procédures PA-DSS standards.
2. L'application de paiement résidente ne remplit pas toutes les exigences PA-DSS, mais le matériel sur lequel l'application réside est répertorié sur la liste des dispositifs PTS (PIN Transaction Security – sécurité de transaction PIN) agréés par le PCI SSC comme un dispositif POI (Point of Interaction – point d'interaction) agréé selon les normes PCI PTS. Dans ce cas, une application peut remplir les conditions PA-DSS par le biais d'une combinaison de contrôles PA-DSS et PTS validés.

Le reste de ce chapitre concerne uniquement les applications de paiement qui résident sur un dispositif POI agréé selon les normes PCI PTS.

Si une ou plusieurs conditions PA-DSS ne sont pas remplies directement par l'application de paiement, elles peuvent l'être indirectement par des contrôles testés dans le cadre de la validation PCI PTS. Pour être intégré à une évaluation PA-DSS, le dispositif matériel DOIT être validé comme dispositif POI agréé selon les normes PCI PTS et figurer sur la liste des dispositifs PTS agréés du PCI SSC. Le dispositif POI validé PTS, qui assure un environnement informatique fiable, deviendra une « ***dépendance requise*** » de l'application de paiement, et la combinaison de l'application et du matériel figurera sur la liste PA-DSS des applications de paiement validées.

Lors de l'évaluation PA-DSS, le PA-QSA doit tester pleinement l'application de paiement ainsi que son matériel dépendant en fonction de toutes les conditions PA-DSS. Si le PA-QSA estime qu'une ou plusieurs exigences PA-DSS ne peuvent pas être remplies par l'application de paiement résidente, mais qu'elles le sont par les contrôles validés aux termes des normes PCI PTS, le PA-QSA doit :

1. Indiquer clairement les conditions remplies aux termes de la norme PA-DSS (de la manière habituelle).
2. Indiquer clairement quelle condition a été remplie aux termes des normes PCI PTS dans la case « En place » concernée par cette condition.
3. Donner l'explication détaillée des raisons pour lesquelles l'application de paiement ne remplit pas les conditions PA-DSS.
4. Documenter les procédures exécutées afin de déterminer comment cette condition a été pleinement remplie par un contrôle validé PCI PTS.
5. Répertorier le terminal matériel validé PCI PTS comme dépendance requise dans le résumé du rapport validant la conformité.

Une fois la validation de l'application de paiement terminée par le PA-QSA et acceptée par le PCI SSC, le dispositif matériel validé PTS sera répertorié comme une dépendance de l'application de paiement sur la liste PA-DSS des applications validées.

Les applications de paiement résidant sur des terminaux matériels, validées à travers une combinaison de contrôles PA-DSS et PCI PTS, doivent répondre aux critères suivants :

1. Être fournies ensemble au client (le terminal matériel et l'application), OU, si elles sont fournies séparément, le fournisseur d'applications et/ou l'intégrateur/revendeur doivent conditionner l'application en vue de sa distribution de sorte qu'elle fonctionne uniquement sur le terminal matériel sur lequel elle a été validée.
2. Être activées par défaut pour garantir la conformité PCI DSS du client.
3. Comprendre une assistance et des mises à jour permanentes pour conserver la conformité PCI DSS.
4. Si l'application est vendue, distribuée ou cédée sous licence séparément aux clients, le vendeur doit indiquer les détails du matériel dépendant requis à utiliser avec l'application, conformément à son référencement de validation PA-DSS.

Guide de mise en œuvre de la norme PA-DSS

Les applications de paiement validées doivent pouvoir être mises en œuvre en respectant les normes PCI DSS. Les fournisseurs de logiciels sont dans l'obligation de fournir un *Guide de mise en œuvre de la norme PA-DSS* pour informer leurs clients et les intégrateurs/revendeurs de la mise en œuvre sécurisée des produits, pour documenter les spécifications d'une configuration sécurisée, mentionnées tout au long de ce document, et pour indiquer clairement les responsabilités des fournisseurs, des intégrateurs/revendeurs ainsi que celles des clients afin de remplir les conditions des normes PCI DSS. Ce guide doit détailler comment le client et/ou le revendeur/intégrateur doivent activer les réglages de sécurité au sein du réseau du client. Par exemple, le *Guide de mise en œuvre de la norme PA-DSS* doit indiquer les responsabilités et les fonctionnalités fondamentales de la sécurité PCI DSS par mot de passe, même si cela n'est pas contrôlé par l'application de paiement, de façon à ce que le client ou le revendeur/intégrateur comprenne comment mettre en œuvre des mots de passe sécurisés dans le respect des normes PCI DSS.

Le *Guide de mise en œuvre de la norme PA-DSS* doit donner des détails sur la configuration de l'application de paiement pour qu'elle respecte la ou les exigences et il ne doit pas se contenter de répéter les exigences du PCI DSS ou PA-DSS. Pendant une évaluation, le PA-QSA doit vérifier que les instructions sont précises et efficaces. Le PA-QSA doit aussi vérifier que le *Guide de mise en œuvre de la norme PA-DSS* est distribué aux clients et intégrateurs/vendeurs.

Les applications de paiement, lorsqu'elles sont mises en œuvre conformément au *Guide de mise en œuvre de la norme PA-DSS* dans un environnement respectant les normes PCI DSS, doivent permettre et soutenir la conformité des clients aux normes PCI DSS.

Se reporter *à l'annexe A : Résumé du contenu du Guide de mise en œuvre de la norme PA-DSS*, pour comparer les responsabilités de la mise en œuvre des contrôles spécifiés dans le *Guide de mise en œuvre de la norme PA-DSS*.

Conditions relatives aux évaluateurs de sécurité qualifiés des applications de paiement (PA-QSA)

Seuls les évaluateurs de sécurité qualifiés des applications de paiement (PA-QSA) employés par les sociétés d'évaluation de sécurité qualifiées des applications de paiement (PA-QSA) sont autorisés à réaliser des évaluations PA-DSS. Consulter la liste de QSA d'application de paiement sur www.pcisecuritystandards.org afin d'avoir la liste des sociétés QSA qualifiées pour mener les évaluations PA-DSS.

- Le PA-QSA doit utiliser les procédures de test documentées dans ce document sur la Norme de sécurité des données d'application de paiement.
- Le PA-QSA doit avoir accès au laboratoire où le processus de validation est censé avoir lieu.

Laboratoire de test

- Les laboratoires de test peuvent exister soit sur le site du PA-QSA soit sur celui du fournisseur du logiciel.
- Ce laboratoire doit permettre de simuler une utilisation en conditions réelles de l'application de paiement.
- Le PA-QSA doit valider l'installation appropriée du laboratoire afin de garantir que celui-ci simule vraiment une situation en conditions réelles et que le fournisseur n'a pas modifié ni altéré l'environnement d'aucune façon.
- Se reporter à l'*annexe B : Confirmation de la configuration du laboratoire de test spécifique à l'évaluation de la norme PA-DSS* de ce document, pour connaître les conditions détaillées applicables au laboratoire et aux processus de laboratoire associés.
- Le PA-QSA doit compléter et renvoyer l'*annexe B*. Il doit la remplir pour le laboratoire spécifique utilisé pour l'application de paiement examinée, dans le cadre du rapport PA-DSS complet sur la validation (ROV).

Instructions et contenu du rapport de conformité

Les instructions et le contenu du rapport de conformité PA-DSS (ROV) sont désormais disponibles sur le *Modèle de rapport ROV PA-DSS.* Le *Modèle de rapport ROV PA-DSS* doit être utilisé pour créer le rapport de conformité. Seuls les ROV d'application des paiements conformes doivent être soumis au PCI SSC. Pour plus d'informations sur le processus de soumission de ROV, reportez-vous au *Guide du programme de la norme PA-DSS*.

Étapes de mise en conformité avec la norme PA-DSS

Ce document contient le tableau des conditions et procédures d'évaluation de sécurité, ainsi que *l'annexe B : Configuration du laboratoire de test pour l'évaluation de la norme PA-DSS*. Le document Conditions et procédures d'évaluation de sécurité détaille les procédures que le PA-QSA doit réaliser.

Le PA-QSA doit effectuer les étapes suivantes :

1. Confirmer le champ d'application de l'évaluation PA-DSS.
2. Effectuer l'évaluation PA-DSS.
3. Compléter le rapport de conformité (ROV) en utilisant le *Modèle de rapport ROV PA-DSS*, en incluant la confirmation de configuration de laboratoire de test utilisée pour l'évaluation PA-DSS.
4. Remplir et signer une attestation de conformité (à la fois par le PA-QSA et par le fournisseur du logiciel). L'attestation de conformité est disponible sur le site Web du PCI SSC (www.pcisecuritystandards.org).
5. Une fois remplis, soumettre tous les documents ci-dessus ainsi que le *Guide de mise en œuvre de la norme PA-DSS* au PCI SSC, selon le *Guide du programme de la norme PA-DSS.*

Remarque :

Les soumissions de PA-DSS ne doivent pas être effectuées à moins que toutes les exigences PA-DSS aient été validées comme ayant été mises en place.

Guide du programme de la norme PA-DSS

Consulter le *Guide du programme de la norme PA-DSS* pour les informations sur la gestion du programme PA-DSS, notamment sur les points suivants :

- Détails des différentes versions PA-DSS et de leurs dates d'entrée en vigueur
- Applicabilité de la norme PA-DSS aux différents types d'applications
- Processus de transmission et d'acceptation du rapport PA-DSS
- Processus de renouvellement annuel pour les applications de paiement comprises dans la liste des applications de paiement conformes
- Notification des responsabilités dans le cas où une application de paiement répertoriée serait mise en cause dans un compromis

Le PCI SSC se réserve le droit d'exiger une revalidation en cas de changements importants de la PA-DSS et/ou de vulnérabilités identifiées dans une application de paiement répertoriée.

Conditions et procédures d'évaluation de sécurité de la norme PA-DSS

Les informations suivantes définissent les en-têtes des colonnes du tableau d'exigences et procédures d'évaluation de sécurité de la norme PCI DSS :

- **Conditions de la norme PA-DSS** – Cette colonne définit les exigences de sécurité pour les applications de paiement devant être validées.
- **Procédures de test** – Cette colonne définit les processus de test à suivre par le PA-QSA pour valider que les exigences PA-DSS ont été respectées.
- **Directive** – Cette colonne décrit l'intention ou l'objectif de sécurité derrière chaque condition de la norme PA-DSS et elle est destinée à comprendre les exigences. La directive indiquée dans cette colonne ne remplace et n'étend pas les exigences et les procédures de test PA-DSS.

Remarque :

Les exigences PA-DSS ne doivent pas être considérées comme étant en place si le moindre contrôle n'a pas encore été mis en œuvre ou doit être terminé à une date future.

Condition 1 : Ne pas conserver la totalité des données de bande magnétique, de code ou de valeur d'audit de carte (CAV2, CID, CVC2, CVV2), ou de données de bloc PIN

Conditions de la norme PA-DSS	Procédures de test	Directive
1.1 Ne stocker aucune donnée d'identification sensible après autorisation (même cryptée). Si des données d'identification sensibles sont reçues, rendre toutes les données irrécupérables à la fin du processus d'autorisation. Les données concernées sont mentionnées dans les conditions suivantes 1.1.1 à 1.1.3. ***Correspond à la condition 3.2 de la norme PCI DSS***	**1.1.a** Si cette application de paiement stocke des données d'identification sensibles, vérifier que l'application est uniquement destinée aux émetteurs et/ou sociétés qui prennent en charge des services d'émission.	Les données d'identification sensibles sont constituées par les données complètes de piste, le code ou la valeur de validation de carte et les données PIN. Le stockage des données d'identification sensibles n'est pas autorisé. Ces données sont précieuses pour les individus malveillants, car elles leur permettent de créer de fausses cartes de paiement et de procéder à des transactions frauduleuses. Les entités qui émettent des cartes de paiement ou qui fournissent ou soutiennent des services d'émission créeront et contrôleront souvent des données d'identification dans le cadre de la fonction d'émission. Les émetteurs et les sociétés qui prennent en charge les services d'émissions peuvent stocker des données d'identification sensibles si ceci est justifié du point de vue professionnel et que ces données sont stockées de manière sécurisée. Pour les entités non émettrices qui conservent des données d'identification sensibles, la post-autorisation n'est pas permise et l'application doit avoir un mécanisme pour supprimer les données de manière sûre, de sorte qu'elles ne soient plus récupérables.
	1.1.b Pour toutes les autres applications de paiement, si des données d'identification sensibles (voir les conditions 1.1.1 à 1.1.3 ci-dessous) sont stockées avant autorisation, veuillez vous procurer et examiner la méthodologie de suppression des données pour s'assurer que les données sont irrécupérables.	

Conditions de la norme PA-DSS	Procédures de test	Directive
1.1.1 Après autorisation, ne jamais stocker la totalité du contenu d'une quelconque piste de la bande magnétique (au verso d'une carte, sur une puce ou ailleurs). Ces données sont également désignées piste complète, piste, piste 1, piste 2 et données de bande magnétique. ***Remarque :*** *Dans le cadre normal de l'activité, il est parfois nécessaire de conserver les éléments de données de la bande magnétique suivants :* • *Le nom du titulaire du compte* • *Le numéro de compte primaire (PAN)* • *La date d'expiration et* • *Le code de service* *Afin de réduire le risque autant que possible, stocker uniquement les éléments de données nécessaires à l'activité.* ***Correspond à la condition 3.2.1 de la norme PCI DSS***	**1.1.1** Installer l'application de paiement et effectuer plusieurs transactions de test simulant toutes les fonctions de l'application de paiement en incluant la génération de conditions d'erreur et les entrées de journaux. Utiliser des méthodes et/ou des outils légaux (outils commerciaux, scripts, etc.)[5] pour examiner toutes les sorties générées par l'application de paiement et vérifier que la totalité du contenu des pistes de la bande magnétique au verso de la carte ou les données équivalentes sur la puce, n'est pas stockée après autorisation. Inclure au moins les types de fichiers suivants (ainsi que toute autre sortie générée par l'application de paiement) : • Les données de transaction entrantes ; • Tous les journaux (par exemple, transactions ; historique, débogage, erreur) ; • Les fichiers d'historique ; • Les fichiers trace ; • Mémoire non volatile, y compris cache non volatil ; • Schémas des bases de données ; • Contenu des bases de données.	Si les données complètes de piste étaient stockées, les individus malveillants qui obtiennent ces données pourraient les utiliser pour reproduire et vendre des cartes de paiement pour effectuer des transactions frauduleuses.

[5] *Méthodes ou outils légaux : Un outil ou une méthode pour découvrir, analyser et présenter les données légales, fournissant un moyen efficace d'authentifier, de rechercher et de découvrir des preuves informatiques rapidement et précisément. Les méthodes et outils légaux utilisés par les PA-QSA doivent localiser avec précision toute donnée d'identification sensible écrite par l'application de paiement. Ces outils peuvent être distribués dans le commerce, libres ou développés en interne par les PA-QSA.*

Conditions de la norme PA-DSS	Procédures de test	Directive
1.1.2 Après autorisation, ne pas stocker le code ou la valeur de validation de carte (numéro à trois ou quatre chiffres figurant au recto ou au verso de la carte de paiement, utilisé pour vérifier les transactions de carte absente). ***Correspond à la condition 3.2.2 de la norme PCI DSS***	**1.1.2** Installer l'application de paiement et effectuer plusieurs transactions de test simulant toutes les fonctions de l'application de paiement en incluant la génération de conditions d'erreur et les entrées de journaux. Utiliser des méthodes et/ou des outils légaux (outils commerciaux, scripts, etc.) pour examiner toutes les sorties générées par l'application de paiement et vérifier que le code d'authentification de carte à trois ou quatre chiffres figurant au recto de la carte de paiement ou dans l'espace signature (données CVV2, CVC2, CID, CAV2) n'est pas stocké après autorisation. Inclure au moins les types de fichiers suivants (ainsi que toute autre sortie générée par l'application de paiement) : • Les données de transaction entrantes ; • Tous les journaux (par exemple, transactions ; historique, débogage, erreur) ; • Les fichiers d'historique ; • Les fichiers trace ; • Mémoire non volatile, y compris cache non volatil ; • Schémas des bases de données ; • Contenu des bases de données.	Le code de validation des cartes est destiné à protéger les transactions « carte absente », transactions effectuées via Internet ou ordre de paiement par e-mail/téléphone (MO/TO), en l'absence du consommateur et de la carte. Si ces données étaient volées, des individus malveillants pourraient exécuter des transactions frauduleuses par MO/TO et Internet.

Conditions de la norme PA-DSS	Procédures de test	Directive
1.1.3 Après autorisation, ne pas stocker de code d'identification personnelle (PIN) ou de bloc PIN crypté. ***Correspond à la condition 3.2.3 de la norme PCI DSS***	**1.1.3** Installer l'application de paiement et effectuer plusieurs transactions de test simulant toutes les fonctions de l'application de paiement en incluant la génération de conditions d'erreur et les entrées de journaux. Utiliser des méthodes et/ou des outils légaux (outils commerciaux, scripts, etc.) pour examiner toutes les sorties générées par l'application de paiement et vérifier que les codes PIN et les blocs PIN cryptés ne sont pas stockés après autorisation. Inclure au moins les types de fichiers suivants (ainsi que toute autre sortie générée par l'application de paiement). • Les données de transaction entrantes ; • Tous les journaux (par exemple, transactions ; historique, débogage, erreur) ; • Les fichiers d'historique ; • Les fichiers trace ; • Mémoire non volatile, y compris cache non volatil ; • Schémas des bases de données ; • Contenu des bases de données.	Ces valeurs ne doivent être connues que du titulaire de la carte ou de la banque émettrice de la carte. Si ces données étaient volées, des individus malveillants pourraient exécuter des transactions de débit frauduleuses à l'aide du code PIN (par exemple, retraits à un GAB).

Conditions de la norme PA-DSS	Procédures de test	Directive
1.1.4 Supprimer de façon sécurisée toute donnée de bande magnétique (de la bande magnétique, ou données équivalentes contenues sur une puce), valeur ou code de validation de carte, et données de codes ou blocs PIN, stockées par les versions précédentes de l'application de paiement, conformément aux normes du secteur relatives à la suppression sécurisée, comme défini, par exemple, par la liste des produits agréés gérée de la National Security Agency ou par tout autre organisme de normalisation ou de réglementation étatique ou national. ***Remarque :*** *Cette condition s'applique uniquement si les versions précédentes de l'application de paiement stockaient des données d'identification sensibles.* ***Correspond à la condition 3.2 de la norme PCI DSS***	**1.1.4.a** Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que la documentation comprend les instructions suivantes pour les clients et les intégrateurs/revendeurs : • Les données d'historique (données de bande magnétique, codes de validation de carte, codes ou blocs PIN, stockés par les versions précédentes de l'application de paiement) doivent être supprimées. • Comment supprimer les données d'historique. • Indication que cette suppression est nécessaire pour la conformité aux normes PCI DSS. **1.1.4.b** Examiner les fichiers du logiciel d'application de paiement et les documents de configuration pour vérifier que le fournisseur fournit un outil ou une procédure d'effacement sécurisés pour supprimer les données. **1.1.4.c** Vérifier, à l'aide d'outils et/ou de méthodes légaux, que l'outil ou la procédure d'effacement sécurisés proposés par le fournisseur suppriment les données de façon sécurisée, conformément aux normes du secteur en la matière.	Tous ces éléments de données d'identification sensibles ne peuvent pas être stockés post-autorisation. Si des versions antérieures des applications de paiement ont stocké cette information, le vendeur d'application de paiement doit donner des instructions dans le *Guide de mise en œuvre de la norme PA-DSS*, ainsi qu'un outil ou une procédure de nettoyage sécurisé. Si ces données ne sont pas supprimées de manière sûre, elles pourraient demeurer cachées sur les systèmes des clients, et des individus malveillants qui obtiennent accès à cette information pourraient l'utiliser pour produire des cartes de paiement contrefaites et/ou effectuer des transactions frauduleuses.

Conditions de la norme PA-DSS	Procédures de test	Directive
1.1.5 Ne stocker aucune donnée d'identification sensible sur les systèmes de fournisseurs. Si des données d'identification sensibles (données de pré-autorisation) doivent être utilisées pour le débogage ou le dépannage, s'assurer de respecter ce qui suit : • Les données d'identification sensibles sont uniquement collectées lorsque cela est nécessaire pour résoudre un problème particulier. • Ces données sont stockées à un emplacement spécifique connu dont l'accès est restreint. • Une quantité minimale de données est collectée, selon la quantité nécessaire pour résoudre un problème spécifique. • Les données d'identification sensibles sont cryptées avec une cryptographie robuste pour leur stockage. • Ces données sont supprimées de façon sécurisée immédiatement après leur utilisation, y compris à partir des : - Fichiers journaux ; - Fichiers de débogage ; - Autres sources de données reçues des clients. ***Correspond à la condition 3.2 de la norme PCI DSS.***	**1.1.5.a** Examiner les procédures du *fournisseur de logiciel* en ce qui concerne le dépannage des clients et vérifier que les procédures comprennent : • Collecte des données d'identification sensibles uniquement lorsque cela est nécessaire pour résoudre un problème particulier. • Stockage de ces données à un emplacement spécifique connu dont l'accès est restreint. • Collecte d'une quantité de données limitée requise pour résoudre un problème particulier. • Cryptage des données d'identification sensibles lors du stockage. • Suppression sécurisée des données immédiatement après leur utilisation. **1.1.5.b** Sélectionner un échantillon de demandes de dépannage récentes émanant des clients et vérifier que chaque événement a respecté la procédure 1.1.5.a. **1.1.5.c** Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que la documentation comprend les instructions suivantes pour les clients et les intégrateurs/revendeurs : • Collecter des données d'identification sensibles uniquement lorsque cela est nécessaire pour résoudre un problème spécifique ; • Stocker de telles données uniquement dans des emplacements spécifiques et connus, d'accès restreint ; • Collecter les données en se cantonnant à la quantité nécessaire pour résoudre un problème spécifique ; • Le cryptage des données d'authentification sensibles lors de leur stockage ; • Supprimer ces données immédiatement après leur utilisation, en appliquant un processus sécurisé.	Si le vendeur offre des services à ses clients qui sont susceptibles de provoquer la collecte de données d'identification sensibles (par exemple pour le dépannage ou le débogage), le vendeur doit minimiser la collecte de données et s'assurer que les données sont sécurisées et supprimées de manière sécurisée dès qu'elles ne sont plus nécessaires. Si le dépannage d'un problème nécessite que l'application soit temporairement configurée pour capturer des données d'identification sensibles (SAD), l'application doit être retournée à sa configuration sécurisée d'origine (c'est-à-dire, désactiver la collecte de SAD), immédiatement après que les données nécessaires aient été capturées. Une fois qu'elles ne sont plus nécessaires, les SAD doivent être supprimées conformément aux normes du secteur (par exemple, à l'aide d'un programme de nettoyage sécurisé qui assure que les données ne puissent jamais être récupérées).

Condition 2 : Protéger les données de titulaires de carte stockées

Conditions de la norme PA-DSS	Procédures de test	Directive
2.1 Les fournisseurs de logiciel doivent conseiller les clients quant à la suppression des données de titulaires de carte après expiration de la période de rétention définie par le client. ***Correspond à la condition 3.1 de la norme PCI DSS***	**2.1.**Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que la documentation comprend les directives suivantes pour les clients et les revendeurs/intégrateurs : • Les données de titulaires de carte dépassant la période de rétention définie par le client doivent être supprimées. • La liste de tous les emplacements où l'application de paiement stocke les données de titulaires de carte (de manière à ce que le client connaisse l'emplacement des données à supprimer). • Les instructions dont le client a besoin pour supprimer en toute sécurité les données de titulaires de carte lorsqu'elles ne sont plus requises pour les besoins légaux, réglementaires ou commerciaux. • Les instructions sur la manière sécurisée de supprimer les données de titulaires de carte stockées par l'application de paiement, y compris les données stockées par des logiciels ou systèmes sous-jacents (tels que SE, bases de données, etc.) • Les instructions de configuration du logiciel ou des systèmes sous-jacents (SE, bases de données, etc.) pour prévenir la capture ou la rétention accidentelle des données de titulaires de carte - par exemple, avec des points de sauvegarde ou des restaurations du système.	Pour prendre en charge la condition 3.1 de la norme PCI DSS, le vendeur doit donner les détails de tous les emplacements où l'application de paiement est susceptible de stocker des données de titulaires de carte, y compris tout logiciel ou système sous-jacent (tels que SE, base de données, etc.), ainsi que les instructions relatives à la suppression sécuritaire des données de ces emplacements une fois que les données ont dépassé la période de rétention fixée par le client. Les clients et les intégrateurs/vendeurs doivent aussi fournir les détails de configuration des systèmes et logiciels sous-jacents que l'application utilise, afin d'assurer que ces systèmes sous-jacents ne capturent pas des données de titulaires de carte sans que le client le sache. Le client a besoin de savoir comment les systèmes sous-jacents pourraient capturer des données de l'application pour qu'ils puissent les empêcher d'être capturées ou s'assurer que les données sont correctement protégées.

Conditions de la norme PA-DSS	Procédures de test	Directive
2.2 Masquer le PAN lorsqu'il s'affiche (les six premiers chiffres et les quatre derniers sont le maximum de chiffres affichés), de manière à ce que seul le personnel, dont le besoin commercial est légitime, puisse voir plus que les six premiers/les quatre derniers chiffres du PAN. ***Remarque :*** *Cette condition ne se substitue pas aux conditions plus strictes qui sont en place et qui régissent l'affichage des données de titulaires de carte, par exemple, pour les reçus des points de vente (POS).* ***Correspond à la condition 3.3 de la norme PCI DSS***	**2.2.a** Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que la documentation comprend les directives suivantes pour les clients et les revendeurs/intégrateurs : • Détails de toutes les instances pour lesquelles le PAN est affiché, comprenant, entre autres, les dispositifs de POS, les écrans, les journaux et les reçus. • Confirmation que l'application de paiement masque le PAN par défaut sur tous les écrans. • Instructions concernant la configuration de l'application de paiement de sorte que seul le personnel qui a un besoin professionnel légitime puisse voir les six premiers/les quatre derniers chiffres du PAN (ce qui inclut le PAN entier).	Grâce à l'affichage du PAN intégral sur un écran d'ordinateur, un reçu de carte de paiement, un fax ou un rapport sur papier, des individus non autorisés pourraient y avoir accès et l'utiliser de manière frauduleuse. Le masquage doit toujours s'assurer que seul le nombre minimal nécessaire de chiffres s'affiche pour exécuter une fonction professionnelle spécifique. Par exemple, si seuls les quatre derniers chiffres sont requis pour exécuter une fonction professionnelle, masquez le PAN afin que les individus chargés de cette fonction puissent afficher uniquement les quatre derniers chiffres. *(suite à la page suivante)*
	2.2.b Installer l'application de paiement et examiner toutes les instances pour lesquelles le PAN est affiché, comprenant entre autres, les dispositifs de POS, les écrans, les journaux et les reçus. Pour chaque instance où le PAN est affiché, vérifier qu'il est masqué lors de son affichage.	En outre, si une fonction doit accéder au numéro d'identification bancaire (BIN) dans un souci d'acheminement, démasquer les chiffres BIN uniquement (habituellement les six premiers chiffres) pendant l'exécution de cette fonction. Cette condition porte sur la protection du PAN visible sur les écrans, reçus papier, impressions, etc., et elle ne doit pas être confondue avec la condition 2.3 de la norme PA-DSS pour la protection du PAN lorsqu'il est stocké dans des fichiers, des bases de données, etc.
	2.2.c Configurer l'application de paiement selon le *Guide de mise en œuvre de la norme PA-DSS* de sorte que seul le personnel qui a un besoin professionnel légitime puisse voir plus que les six premiers/les quatre derniers chiffres du PAN. Pour chaque instance où le PAN est affiché, examiner les configurations de l'application et les affichages du PAN pour s'assurer que les instructions relatives au masquage du PAN sont correctes, et que seul le personnel qui a un besoin professionnel légitime puisse voir les six premiers/les quatre derniers chiffres du PAN.	
2.3 Rendre le PAN illisible où qu'il soit stocké (y compris les données sur support numérique portable, support de sauvegarde et journaux), en utilisant l'une des approches suivantes : • Hachage unilatéral s'appuyant sur une méthode	**2.3.a** Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que la documentation comprend les directives suivantes pour les clients et les revendeurs/intégrateurs : • Détail des options configurables pour chaque	L'absence de protection des PAN peut permettre à des individus malveillants de voir ou de télécharger ces données. Les fonctions de hachage unilatéral reposant

Conditions de la norme PA-DSS	Procédures de test	Directive
cryptographique robuste (la totalité du PAN doit être hachée) ; • Troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du PAN) ; • Jetons et pads d'index (les pads doivent être stockés de manière sécurisée) ; • Cryptographie robuste associée aux processus et procédures de gestion des clés. *(suite à la page suivante)*	méthode utilisée par l'application pour rendre les données de titulaires de carte illisibles et instructions relatives à la configuration de chaque méthode pour les emplacements ou les données de titulaires de carte sont stockées par l'application de paiement (selon la condition 2.1 de la norme PA-DSS). • Une liste des instances où les données de titulaires de carte pourraient être produites pour que le client les stocke hors de l'application de paiement, ainsi que les instructions relatives à la responsabilité du client de rendre le PAN illisible dans toutes ces instances. • Si les journaux de débogage sont activés (à des fins de dépannage, par exemple) et s'ils comprennent le PAN, ils doivent être protégés conformément à la norme PCI DSS, désactivés dès que le dépannage est terminé et supprimés en toute sécurité lorsqu'ils ne sont plus requis.	sur une cryptographie robuste peuvent être utilisées pour rendre les données de titulaires de carte illisibles. Ces fonctions de hachage sont appropriées lorsqu'il n'est pas nécessaire de récupérer le numéro d'origine (le hachage unilatéral est irréversible). La troncature vise à ne stocker qu'une partie seulement du PAN (sans dépasser les six premiers et les quatre derniers chiffres). Un « jeton d'index » est un élément cryptographique qui remplace le PAN en fonction d'un indice donné, par une valeur imprévisible. Un pad ponctuel est un système dans lequel une clé privée, générée de façon aléatoire, est utilisée une seule fois pour crypter un message, qui est ensuite décrypté à l'aide de la clé et du pad ponctuel correspondant. *(suite à la page suivante)*
Remarques : • Il s'agit d'un effort relativement peu important pour un individu malveillant de reconstruire les données du PAN d'origine, s'il a à la fois accès à la version tronquée et hachée d'un PAN. Lorsque les versions hachées et tronquées du même PAN sont générées par une application de paiement, des contrôles supplémentaires doivent être en place pour garantir que les versions hachées et tronquées ne peuvent pas être corrélées pour reconstituer le PAN d'origine. • Le PAN doit être rendu illisible où qu'il soit stocké, même en dehors de l'application de paiement (par exemple, les fichiers de journaux produits par l'application pour le stockage dans l'environnement du commerçant). ***Correspond à la condition 3.4 de la norme PCI***	**2.3.b** Examiner la méthode utilisée pour protéger le PAN, y compris les algorithmes de cryptage (s'il y a lieu). Vérifier que le PAN est rendu illisible en utilisant l'une des méthodes suivantes : • Hachage unilatéral s'appuyant sur une méthode cryptographique robuste ; • Troncature ; • Jetons et pads d'index, les pads devant être stockés de manière sécurisée ; • Cryptographie robuste associée aux processus et procédures de gestion des clés. **2.3.c** Si l'application crée des versions hachées et tronquées du même PAN, examiner des méthodes de création de versions hachées et tronquées pour s'assurer que les versions hachées et tronquées ne peuvent pas être corrélées pour reconstituer le PAN d'origine.	L'objectif de la cryptographie robuste (selon la définition du *Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS*) est de fonder le cryptage sur un algorithme testé et accepté par le secteur (non pas un algorithme exclusif ou « développé en interne »), avec de robustes clés cryptographiques.

Conditions de la norme PA-DSS	Procédures de test	Directive
DSS	**2.3.d** Examiner plusieurs tableaux ou fichiers des référentiels de données, créés ou générés par l'application, pour vérifier que le PAN a bien été rendu illisible.	
	2.3.e Si l'application crée ou génère des fichiers à utiliser en dehors de l'application (par exemple, des fichiers générés pour l'export ou la sauvegarde), y compris pour le stockage sur des supports amovibles, examiner un échantillon des fichiers générés, y compris ceux générés sur des supports amovibles (par exemple, des bandes de sauvegarde), pour confirmer que le PAN est bien illisible.	
	2.3.f Examiner un échantillon des journaux de vérification créés ou générés par l'application pour confirmer que le PAN est bien illisible ou supprimé des journaux.	
	2.3.g Si le fournisseur de logiciel stocke le PAN, quelle qu'en soit la raison (par exemple, parce que les fichiers journaux, les fichiers de débogage et d'autres sources de données sont reçus des clients pour débogage ou dépannage), vérifier que le PAN est rendu illisible conformément aux conditions 2.3.b à 2.3.f mentionnées ci-dessus.	
2.4 L'application de paiement doit protéger les clés utilisées pour sécuriser les données de titulaires de carte contre la divulgation et l'utilisation illicites. ***Remarque :*** *Cette condition s'applique aux clés utilisées pour crypter les données de titulaires de carte stockées ainsi qu'aux clés de cryptage de clés associées utilisées pour protéger les clés de cryptage de données. Ces clés de cryptage de clés doivent être au moins aussi robustes que la clé de cryptage de données.* ***Correspond à la condition 3.5 de la norme PCI DSS***	**2.4.a** Examiner la documentation du produit et interroger le personnel responsable pour vérifier que des contrôles sont en place pour restreindre l'accès aux clés cryptographiques utilisées par l'application.	Les clés cryptographiques doivent être parfaitement protégées, car tout individu qui parviendrait à y accéder pourrait décrypter les données. L'obligation pour les applications de paiement de protéger les clés d'une divulgation et d'une utilisation illicites s'applique aux clés de cryptage des données comme aux clés assurant le cryptage des clés. Il n'est pas prévu de crypter les clés assurant le cryptage des clés, mais celles-ci doivent cependant être protégées de la divulgation et de l'utilisation illicites comme le définit la condition 2.4.
	2.4.b Examiner les fichiers de configuration du système pour vérifier que : • Les clés sont stockées sous un format crypté. • Les clés de cryptage de clés sont stockées à un emplacement différent des clés de cryptage de données. • Ces clés de cryptage de clés doivent être au moins aussi robustes que les clés des cryptages de données qu'elles protègent.	

Conditions de la norme PA-DSS	Procédures de test	Directive
	2.4.c Examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que les clients et revendeurs/intégrateurs ont été formés pour : • Restreindre l'accès aux clés cryptographiques au plus petit nombre d'opérateurs possible. • Stocker les clés de manière sécurisée dans aussi peu d'emplacements et sous aussi peu de formes que possible.	Un petit nombre de personnes seulement doit avoir accès aux clés cryptographiques, en général ceux qui sont chargés de la gestion de ces clés.
2.5 L'application de paiement doit au moins mettre en œuvre des processus et procédures pour la gestion des clés cryptographiques utilisés pour le cryptage des données de titulaires de carte : ***Correspond à la condition 3.6 de la norme PCI DSS***	**2.5** Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que la documentation comprend les instructions suivantes pour les clients et les intégrateurs/revendeurs : • Comment générer, distribuer, protéger, changer, stocker et retirer/replacer de manière sécurisée les clés cryptographiques, lorsque les clients ou les intégrateurs/revendeurs sont impliqués dans ces activités de gestion de clés. • Un formulaire aux opérateurs chargés des clés cryptographiques reconnaissant qu'ils comprennent et acceptent leurs responsabilités en tant que telles.	La manière avec laquelle les clés cryptographiques sont gérées est un aspect essentiel de la continuité de la sécurité de l'application de paiement. Un bon processus de gestion des clés, qu'il soit manuel ou automatique dans le cadre du produit de cryptage, se base sur les normes du secteur et prend en charge tous les éléments essentiels décrits aux points 2.5.1 à 2.5.7. Donner des directives aux clients sur la manière de transmettre, stocker et mettre à jour les clés cryptographiques de manière sécurisée peut aider à empêcher que les clés soient mal gérées ou communiquées à des entités non autorisées. Cette condition s'applique aux clés utilisées pour crypter les données de titulaires de carte stockées ainsi qu'à toute clé de cryptage de clé associée.
2.5.1 Génération de clés cryptographiques robustes	**2.5.1.a** Examiner le *Guide de mise en œuvre de la norme PA-DSS* et vérifier qu'il comprend des instructions pour les clients et les intégrateurs/revendeurs sur la production sécuritaire de clés cryptographiques.	L'application de paiement doit générer des clés robustes, aux termes du *Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS*, à « cryptographie robuste ».
	2.5.1.b Tester l'application, y compris les méthodes utilisées pour générer des clés cryptographiques, pour vérifier que les instructions du *Guide de mise en œuvre de la norme PA-DSS* donne lieu à la génération de clés cryptographiques robustes.	

Conditions de la norme PA-DSS	Procédures de test	Directive
2.5.2 Sécuriser la distribution des clés cryptographiques	**2.5.2.a** Examiner le *Guide de mise en œuvre de la norme PA-DSS* et vérifier qu'il comprend des instructions pour les clients et les intégrateurs/revendeurs sur la production sécuritaire de clés cryptographiques.	L'application de paiement doit distribuer les clés de manière sécurisée, c'est-à-dire que les clés ne sont pas distribuées en texte clair et uniquement au moyen de processus autorisés.
	2.5.2.b Tester l'application, y compris les méthodes utilisées pour générer des clés cryptographiques, pour vérifier que les instructions du *Guide de mise en œuvre de la norme PA-DSS* donne lieu à la distribution sécurisée des clés cryptographiques.	
2.5.3 Sécuriser le stockage des clés cryptographiques	**2.5.3.a** Examiner le *Guide de mise en œuvre de la norme PA-DSS* et vérifier qu'il comprend des instructions pour les clients et les intégrateurs/revendeurs sur le stockage sécuritaire des clés cryptographiques.	L'application de paiement doit stocker les clés de manière sécurisée (par exemple, en les cryptant à l'aide d'une clé de cryptage de clé).
	2.5.3.b Tester l'application, y compris les méthodes utilisées pour générer des clés cryptographiques, pour vérifier que les instructions du *Guide de mise en œuvre de la norme PA-DSS* donnent lieu au stockage sécurisé des clés cryptographiques.	
2.5.4 Changements de clé cryptographique pour les clés ayant atteint la fin de leur cryptopériode (par exemple, après la fin d'une période définie et/ou après la production d'une certaine quantité de cryptogrammes par une clé donnée), comme l'a défini le fournisseur de l'application associée ou le propriétaire de la clé, et selon les meilleures pratiques et directives du secteur (par exemple, *la publication spéciale NIST 800-57*).	**2.5.4.a** Consulter le *Guide de mise en œuvre de la norme PA-DSS* et vérifier qu'elle comprend les instructions suivantes pour les clients et les intégrateurs/revendeurs : • Cryptopériode définie pour chaque type de clé utilisée par l'application. • Procédures d'application des changements de clé à la fin de la cryptopériode définie.	La cryptopériode est la période durant laquelle une clé cryptographique donnée peut être utilisée dans le but pour lequel elle est prévue. Les facteurs à prendre en compte pour définir la cryptopériode sont, sans s'y limiter, la complexité de l'algorithme sous-jacent, la taille ou la longueur de la clé, le risque de compromission de la clé, et la sensibilité des données cryptées. Il est impératif de changer les clés de cryptage une fois leur cryptopériode écoulée, afin de réduire le risque qu'un tiers se les procure et les utilise pour décrypter des données.
	2.5.4.b Tester l'application, y compris les méthodes de changement de clé cryptographique, pour vérifier que les instructions du *Guide de mise en œuvre de la norme PA-DSS* donnent lieu aux changements essentiels nécessaires à la fin de la cryptopériode définie.	

Conditions de la norme PA-DSS	Procédures de test	Directive
2.5.5 Retrait ou remplacement des clés (par exemple, en les archivant, détruisant, et/ou révoquant selon le cas), si nécessaire lorsque le degré d'intégrité d'une clé est affaibli (par exemple, suite au départ d'un employé ayant connaissance du texte clair d'une clé, etc.) ou lorsque des clés sont susceptibles d'avoir été compromises. ***Remarque :*** *Si les clés cryptographiques retirées ou remplacées doivent être conservées, ces clés doivent être archivées de manière sécurisée (par exemple, en utilisant une clé de cryptage de clé). Les clés cryptographiques archivées doivent être utilisées uniquement pour un décryptage ou une vérification.*	**2.5.5.a** Consulter le *Guide de mise en œuvre de la norme PA-DSS* et vérifier qu'il comprend les instructions suivantes pour les clients et les intégrateurs/revendeurs : • Des instructions expliquant que les clés doivent être retirées ou remplacées lorsque l'intégrité de la clé a été affaiblie, ou lorsque l'on sait ou que l'on soupçonne qu'une clé a été compromise. • Les procédures de retrait ou de remplacement des clés (par exemple, pour l'archivage, la destruction et/ou la révocation selon les cas). • Les procédures pour assurer que les clés cryptographiques retirées ou remplacées ne sont pas utilisées pour les opérations de cryptages.	Les clés qui ne sont plus utilisées ni nécessaires, ou les clés dont on sait ou on soupçonne qu'elles sont compromises, doivent être révoquées et/ou détruites pour assurer qu'elles ne puissent plus être utilisées. Ces clés doivent être conservées (par exemple, pour prendre en charge des données cryptées archivées), elles doivent être parfaitement protégées. L'application de paiement doit également permettre et faciliter un processus de remplacement des clés qui doivent être remplacées ou dont on sait, ou dont on soupçonne qu'elles sont compromises.
	2.5.5.b Tester l'application, y compris les méthodes utilisées pour retirer ou remplacer les clés cryptographiques, pour vérifier que les instructions du *Guide de mise en œuvre de la norme PA-DSS* donne lieu au retrait ou au remplacement des clés (par exemple, par l'archivage, la destruction et/ou la révocation selon le cas).	
	2.5.5.c Tester l'application avec les clés retirées/remplacées pour vérifier que les instructions du *Guide de mise en œuvre de la norme PA-DSS* garantissent que l'application n'utilise pas de clés retirées ou remplacées pour les opérations de cryptage.	

Conditions de la norme PA-DSS	Procédures de test	Directive
2.5.6 Si l'application de paiement prend en charge les opérations de gestion manuelle de clés cryptographiques en texte clair, ces opérations doivent appliquer le fractionnement des connaissances et un double contrôle. ***Remarque :*** *La génération, la transmission, le chargement, le stockage et la destruction de clés sont quelques-uns des exemples d'interventions de gestion manuelle des clés.*	**2.5.6.a** Consulter le *Guide de mise en œuvre de la norme PA-DSS* et vérifier qu'il comprend les instructions suivantes pour les clients et les intégrateurs/revendeurs : • Détails de toutes les opérations de gestion manuelle de clés cryptographiques en texte clair prises en charge par l'application. • Instructions pour la mise en œuvre du fractionnement des connaissances et du double contrôle de ces opérations.	Le fractionnement des connaissances et le double contrôle sont utilisés pour éliminer la possibilité qu'une seule personne puisse accéder à l'intégralité d'une clé. Ce contrôle est applicable pour toutes les opérations de gestion manuelle de clé. Le fractionnement des connaissances est une méthode par laquelle deux personnes ou plus détiennent séparément des composants clés qui, individuellement, ne contiennent aucune connaissance des clés cryptographiques ; chaque personne connaît uniquement son propre composant de clé et les composants de clé individuels ne contiennent aucune connaissance de la clé cryptographique d'origine. Le double contrôle demande que deux personnes ou plus effectuent une fonction et qu'une seule personne ne puisse pas accéder ou utiliser le matériel d'authentification d'une autre.
	2.5.6.b Tester l'application, y compris toutes les opérations de gestion manuelle de clés cryptographiques en texte clair, pour vérifier que les instructions du *Guide de mise en œuvre de la norme PA-DSS* donnent lieu au fractionnement des connaissances et au double contrôle des clés requis pour les procédures de gestion manuelle des clés cryptographiques.	
2.5.7 Prévenir la substitution non autorisée des clés cryptographiques	**2.5.7.a** Examiner le *Guide de mise en œuvre de la norme PA-DSS* et vérifier qu'il comprend des instructions pour les clients et les intégrateurs/revendeurs expliquant comment empêcher la substitution non autorisée des clés cryptographiques.	L'application de paiement doit définir des méthodes pour que les utilisateurs de l'application s'assurent que seules les substitutions de clés autorisées aient lieu. La configuration de l'application ne doit pas autoriser ni accepter la substitution de clés de la part de sources non autorisées ou de processus inattendus.
	2.5.7.b Tester l'application, y compris les méthodes utilisées pour générer des clés cryptographiques, pour vérifier que les instructions du *Guide de mise en œuvre de la norme PA-DSS* empêche la substitution non autorisée des clés cryptographiques.	

Conditions de la norme PA-DSS	Procédures de test	Directive
2.6 Fournir un mécanisme pour rendre irrécupérable tout élément de clé cryptographique ou de cryptogramme, stocké par l'application de paiement, conformément aux normes acceptées par le secteur. Il s'agit de clés cryptographiques utilisées pour crypter ou vérifier les données de titulaires de carte. ***Remarque :*** *Cette condition s'applique uniquement si l'application de paiement ou ses versions précédentes utilise(nt) des éléments de clés cryptographiques ou des cryptogrammes pour crypter les données de titulaires de carte.* ***Correspond à la condition 3.6 de la norme PCI DSS***	**2.6.a** Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que la documentation comprend les instructions suivantes pour les clients et les intégrateurs/revendeurs : • Procédures détaillées sur l'utilisation de l'outil ou de la procédure fournie avec l'application pour rendre les éléments cryptographiques irrécupérables. • Ces éléments de clé cryptographique doivent être rendus irrécupérables lorsque les clés ne sont plus utilisées et selon les conditions de gestion des clés de la norme PCI DSS. • Procédures pour crypter une nouvelle fois les données historiques avec de nouvelles clés, y compris les procédures pour maintenir la sécurité des données en texte clair pendant le processus de décryptage/re-cryptage.	Les fournisseurs doivent apporter un mécanisme pour que leurs clients puissent supprimer leurs anciens éléments cryptographiques de manière sécurisée lorsqu'ils n'en ont plus besoin. Noter que l'élimination des anciens éléments cryptographiques est à la discrétion du client. Les éléments de clés cryptographiques et/ou les cryptogrammes peuvent être rendus inaccessibles par l'utilisation d'outils ou de processus comprenant, mais sans s'y limiter : • La suppression sécurisée, définie, par exemple, dans la liste des produits agréés, établie par la National Security Agency, ou par d'autres normes ou réglementations étatiques ou nationales ; • La suppression de clé de cryptage de clé (KEK) à condition que les clés de cryptage de données résiduelles n'existent que sous une forme cryptée dans la KEK supprimée.
	2.6.b Examiner le produit de l'application finale pour vérifier que le vendeur apporte un outil et/ou des procédures avec l'application pour rendre les éléments cryptographiques irrécupérables.	
	2.6.c Tester l'application, y compris les méthodes offertes pour rendre les éléments de clé cryptographique irrécupérables. Vérifier, à l'aide d'outils et/ou de méthodes légaux, que l'outil ou la procédure d'effacement offerte par le vendeur rend les éléments cryptographiques irrécupérables, conformément aux normes du secteur en la matière.	
	2.6.d Tester l'application pour le nouveau cryptage des données historiques avec la nouvelle clé pour vérifier que les instructions du *Guide de mise en œuvre de la norme PA-DSS* donnent lieu au nouveau cryptage des données historiques avec les nouvelles clés.	

Condition 3 : Fournir des fonctions d'authentification sécurisées

Conditions de la norme PA-DSS	Procédures de test	Directive
3.1 L'application de paiement doit prendre en charge et exiger l'utilisation d'ID utilisateur uniques et d'une authentification sécurisée pour tous les accès administratifs et pour tous les accès aux données de titulaires de carte. L'authentification sécurisée doit être exigée pour tous les comptes générés ou gérés par l'application, dès la fin de l'installation et lors des changements ultérieurs à l'installation. L'application doit répondre aux conditions 3.1.1 à 3.1.11 ci-dessous : ***Remarque :*** *Le terme « changements consécutifs » utilisé dans le cadre de la Condition 3 fait référence à tous les changements de l'application qui entraînent le retour des comptes utilisateurs aux paramètres par défaut, tous les changements aux paramètres de comptes existants et tous les changements qui génèrent de nouveaux comptes ou recréent des comptes existants.* ***Remarque :*** *Ces contrôles de mot de passe ne sont pas destinés à être appliqués aux employés qui n'ont accès qu'à un numéro de carte à la fois dans le cadre d'une transaction unique. Ces contrôles sont applicables pour l'accès du personnel ayant les capacités administratives pour accéder aux systèmes avec des données de titulaires de carte, et pour l'accès contrôlé par l'application de paiement.* *Cette condition s'applique à l'application de paiement et à tous les outils associés, utilisés pour afficher ou accéder aux données de titulaires de carte.* ***Correspond aux conditions 8.1 et 8.2 de la norme PCI DSS***	**3.1.a** Examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur pour vérifier que les clients et revendeurs/intégrateurs : • Reçoivent de manière claire et sans ambiguïté des instructions sur la manière avec laquelle l'application de paiement utilise une authentification robuste pour tous les justificatifs que l'application génère ou gère, en : - Exigeant l'application de changements sécurisés aux justificatifs d'authentification dès la fin de l'installation selon les conditions 3.1.1 à 3.1.11. - Exigeant l'application de changements sécurisés pour tous changements ultérieurs (après l'installation) des justificatifs d'authentification selon les conditions 3.1.1 à 3.1.11. • Sont informés que, pour maintenir la conformité à la norme PCI DSS, tout changement effectué aux configurations d'authentification devrait être vérifié comme apportant des méthodes d'authentification qui sont au moins aussi rigoureuses que les conditions de la norme PCI DSS. • Sont informés qu'ils doivent affecter une authentification sécurisée aux comptes par défaut dans l'environnement. • Ils sont informés qu'ils doivent affecter une authentification sécurisée pour tous les comptes par défaut qui ne seront pas utilisés, puis désactiver ou ne pas utiliser les comptes. • Reçoivent de manière claire et sans ambiguïté des instructions sur tous les justificatifs d'authentification utilisés par l'application de paiement (mais qui ne sont pas générés ou gérés par l'application), sur la manière avec laquelle, en complétant l'installation et par tout changement après l'installation, les justificatifs d'authentification sont changés et une authentification robuste est crée selon les conditions 3.1.1 à 3.1.11 ci-dessous, pour tous les niveaux de l'application et tous les comptes ayant un accès administratif, et pour tous les comptes ayant accès aux données de titulaires de carte. • Identification de tous les rôles et comptes par défaut dans l'application dotée d'un accès administratif.	En s'assurant que chaque utilisateur est identifié de manière unique, au lieu d'utiliser un ID unique pour plusieurs employés, une application prend en charge les conditions de la norme PCI DSS selon laquelle la responsabilité individuelle des actions doit être maintenue ainsi que la piste d'audit pour les employés. Cela accélérera la résolution des problèmes et en limitera les conséquences en cas d'erreur ou d'intentions malveillantes. L'authentification sécurisée, lorsqu'elle est utilisée en plus des ID uniques, assiste la protection des ID uniques des utilisateurs et évite qu'ils ne soient compromis, puisque quiconque compromet un compte aurait besoin de connaître à la fois l'ID unique et le mot de passe (ou autre authentification utilisée).

Conditions de la norme PA-DSS	Procédures de test	Directive
3.1.1 L'application de paiement n'utilise pas (ou ne requiert pas l'utilisation) de comptes administratifs par défaut pour les autres logiciels nécessaires (par exemple, l'application de paiement ne doit pas utiliser le compte administratif par défaut de la base de données). ***Correspond à la condition 2.1 de la norme PCI DSS***	**3.1.1** Installer et configurer l'application de paiement selon le *Guide de mise en œuvre de la norme PA-DSS,* y compris en configurant tous les comptes administratifs pour tous les logiciels nécessaires. Tester l'application de paiement pour vérifier que l'application de paiement n'utilise pas (et ne nécessite pas) de comptes administratifs par défaut pour les logiciels nécessaires.	Les comptes administratifs par défaut (et les mots de passe) sont de notoriété publique et connus de quiconque connaît l'application de paiement ou les composants sous-jacents du système. Si des comptes administratifs et des mots de passe par défaut sont utilisés, une personne non autorisée pourrait accéder à l'application et aux données simplement en ouvrant une session avec des justificatifs connus du public.
3.1.2 L'application doit assurer le changement de tous les mots de passe par défaut de l'application pour tous les comptes qui sont générés ou gérés par l'application, lors de l'accomplissement de l'installation et pour les changements ultérieurs à l'installation. Cette notion s'applique à tous les comptes, y compris les comptes d'utilisateurs, les comptes d'application et de service et les comptes utilisés par le fournisseur dans le cadre du support. ***Remarque :*** *Cette condition ne peut être respectée en spécifiant un processus d'utilisateur ou avec des instructions dans le Guide de mise en œuvre de la norme PA-DSS. Une fois l'installation terminée et suite aux changements ultérieurs, l'application doit techniquement empêcher que tout compte par défaut ou compte intégré soit utilisé jusqu'à ce que le mot de passe par défaut ait été changé.* ***Correspond à la condition 2.1 de la norme PCI DSS***	**3.1.2** Pour tous les comptes générés ou gérés par l'application, tester l'application comme suit : **3.1.2.a** Installer l'application selon le *Guide de mise en œuvre de la norme PA-DSS*, examiner les paramètres de compte et de mot de passe et essayer d'utiliser tous les mots de passe par défaut pour vérifier que l'application vous impose de changer les mots de passe par défaut de l'application de paiement à la fin du processus d'installation. **3.1.2.b** Tester toutes les fonctionnalités de l'application qui font qu'un utilisateur revient aux paramètres par défaut, les changements aux configurations de comptes existants, la génération de nouveaux comptes et la recréation de comptes existants. Pour tous les types de changements effectués, examinez les paramètres de compte et de mot de passe et essayer d'utiliser tous les mots de passe par défaut pour vérifier que l'application applique les changements à tous les mots de passe par défaut une fois le changement terminé.	Si l'application ne supporte pas le changement des mots de passe par défaut, l'application pourrait être laissée exposée aux accès non autorisés par quiconque a connaissance des paramètres par défaut.

Conditions de la norme PA-DSS	Procédures de test	Directive
3.1.3 L'application de paiement assigne des ID uniques pour les comptes utilisateurs. ***Correspond à la condition 8.1.1 de la norme PCI DSS***	**3.1.3** Pour tous les comptes générés ou gérés par l'application, tester l'application comme suit : **3.1.3.a** Installer l'application de paiement selon le *Guide de mise en œuvre de la norme PA-DSS* et essayer de créer différents comptes d'application avec le même ID d'utilisateur pour vérifier que l'application de paiement affecte des ID d'utilisateur uniques une fois le processus d'installation terminé. **3.1.3.b** Tester toutes les fonctionnalités de l'application qui font qu'un utilisateur revient aux paramètres par défaut, les changements aux configurations de comptes existants, la génération de nouveaux comptes et la recréation de comptes existants. Pour tous les types de changement effectués, examiner les paramètres de compte et tester la fonctionnalité de l'application pour vérifier que les ID de clients uniques sont assignés pour tous les comptes une fois que le changement est terminé.	Lorsqu'un ID unique d'utilisateur est attribué à chaque utilisateur, les accès et les activités de cet utilisateur dans l'application de paiement peuvent être retracés jusqu'à l'individu qui les a effectués.
3.1.4 L'application de paiement emploie au moins l'une des méthodes suivantes pour authentifier tous les utilisateurs : ▪ Quelque chose de connu du seul utilisateur, comme un mot de passe ou une locution de passage ; ▪ Quelque chose de détenu par l'utilisateur, comme un dispositif de jeton ou une carte à puce ; ▪ Quelque chose que vous détenez, comme une mesure biométrique. ***Correspond à la condition 8.2 de la norme PCI DSS***	**3.1.4** Pour tous les comptes générés ou gérés par l'application, tester l'application comme suit : **3.1.4.a** Installer l'application de paiement selon le *Guide de mise en œuvre de la norme PA-DSS* et tester les méthodes d'authentification pour vérifier que l'application requiert au moins une des méthodes d'authentification définies pour tous les comptes une fois le processus d'installation terminé. **3.1.4.b** Tester toutes les fonctionnalités de l'application qui font qu'un utilisateur revient aux paramètres par défaut, les changements aux configurations de comptes existants, la génération de nouveaux comptes et la recréation de comptes existants. Pour tous les types de changement effectués, tester les méthodes d'authentification pour vérifier que l'application requiert au moins une des méthodes d'authentification définies pour tous les comptes une fois le changement terminé.	Ces méthodes d'authentification, lorsqu'elles sont utilisées en plus des ID uniques, protègent les ID uniques des utilisateurs et évitent qu'ils ne soient compromis, puisque la personne qui est responsable de cette tentative doit connaître l'ID unique et le mot de passe (ou tout autre élément d'authentification utilisé).

Conditions de la norme PA-DSS	Procédures de test	Directive
3.1.5 L'application de paiement n'exige **pas** ou n'utilise aucun mot de passe et compte collectif, partagé ou générique. ***Correspond à la condition 8.5 de la norme PCI DSS.***	**3.1.5** Pour tous les comptes générés ou gérés par l'application, tester l'application comme suit :	Si plusieurs utilisateurs partagent les mêmes justificatifs d'authentification (par exemple, même compte utilisateur et mot de passe), il devient impossible de déterminer leurs responsabilités ni de consigner efficacement leurs actes individuels, puisque ceux-ci peuvent avoir été exécutés par quiconque connaît les justificatifs d'authentification.
	3.1.5.a Installer l'application de paiement selon le *Guide de mise en œuvre de la norme PA-DSS*, examiner les configurations de compte et tester les fonctions de l'application pour vérifier que, une fois le processus d'installation terminé, l'application ne requiert pas et n'utilise pas de comptes et des mots de passe collectifs, partagés ou génériques.	
	3.1.5.b Tester toutes les fonctionnalités de l'application qui font qu'un utilisateur revient aux paramètres par défaut, les changements aux configurations de comptes existants, la génération de nouveaux comptes et la recréation de comptes existants. Pour tous les types de changement effectués, examiner les paramètres de compte et tester la fonctionnalité de l'application pour vérifier qu'elle n'invoque pas, et n'utilise pas, de comptes et de mots de passe collectifs, partagés ou génériques une fois le changement terminé.	
3.1.6 L'application de paiement exige que les mots de passe respectent les critères suivants : • Exiger une longueur minimale d'au moins sept caractères ; • Comporter à la fois des caractères numériques et des caractères alphabétiques. Autrement, les mots de passe/locutions de passage doivent avoir une complexité et une puissance au moins équivalentes aux paramètres spécifiés ci-dessus.	**3.1.6** Pour tous les comptes générés ou gérés par l'application, tester l'application comme suit :	Les individus malveillants essayeront souvent de trouver des comptes ayant des mots de passe qui sont faibles ou inexistants afin d'accéder à une application ou à un système. Si les mots de passe sont courts ou faciles à deviner, il est relativement facile pour un individu malveillant de découvrir ces faibles comptes et de compromettre une application ou un système sous couvert d'un ID utilisateur valide. *(suite à la page suivante)*
	3.1.6.a Installer l'application de paiement selon le *Guide de mise en œuvre de la norme PA-DSS* et examiner les paramètres du compte pour vérifier que, une fois le processus d'installation terminé, l'application nécessite que les mots de passe aient au moins la complexité et la force décrites ci-après : • Avoir au moins sept caractères de longueur. • Comporter à la fois des caractères numériques et des caractères alphabétiques.	

Conditions de la norme PA-DSS	Procédures de test	Directive
	3.1.6.b Tester toutes les fonctionnalités de l'application qui font qu'un utilisateur revient aux paramètres par défaut, les changements aux configurations de comptes existants, la génération de nouveaux comptes et la recréation de comptes existants. Pour tous les types de changements effectués, examiner les configurations de compte et tester la fonctionnalité de l'application pour vérifier que, une fois le changement terminé, l'application nécessite que les mots de passe aient au moins la complexité et la force décrites ci-après : • Avoir au moins sept caractères de longueur ; • Comporter à la fois des caractères numériques et des caractères alphabétiques.	Cette condition spécifie que les mots de passe doivent être d'une longueur minimum de sept caractères et utiliser à la fois des caractères numériques et des caractères alphabétiques. Pour les cas où ce minimum ne peut pas être respecté en raison de limitations techniques, les entités peuvent utiliser une « force équivalente » pour évaluer leur alternative. NIST SP 800-63-1 définit « l'entropie » comme « une mesure de la difficulté de deviner ou de déterminer un mot de passe ou une clé ». Ce document et les autres documents qui traitent de « l'entropie de mot de passe » peuvent être consultés pour obtenir de plus amples informations sur la valeur d'entropie et les forces équivalentes de mot de passe pour les mots de passe de formats différents.
	3.1.6.c Si l'application utilise un ensemble différent de caractères et de longueur de mot de passe, calculer l'entropie des mots de passe requis par l'application et vérifier qu'elle est au moins équivalente aux paramètres spécifiés ci-dessus (c'est à dire, une longueur d'au moins 7 caractères, avec des caractères numériques et alphabétiques).	
3.1.7 L'application de paiement exige des utilisateurs de changer leurs mots de passe au moins une fois tous les 90 jours. ***Correspond à la condition 8.2.4 de la norme PCI DSS***	**3.1.7** Pour tous les comptes générés ou gérés par l'application, tester l'application comme suit :	Les mots/phrases de passe qui sont valides pour longtemps sans être changés donnent aux individus malveillants plus de temps pour les découvrir.
	3.1.7.a Installer l'application de paiement selon le *Guide de mise en œuvre de la norme PA-DSS* et examiner les paramètres du compte pour vérifier que l'application demande que les mots de passe d'utilisateur soient changés au moins une fois tous les 90 jours en effectuant le processus d'installation.	

Conditions de la norme PA-DSS	Procédures de test	Directive
	3.1.7.b Tester toutes les fonctionnalités de l'application qui font qu'un utilisateur revient aux paramètres par défaut, les changements aux configurations de comptes existants, la génération de nouveaux comptes et la recréation de comptes existants. Pour tous les types de changements effectués, examiner les configurations de compte et tester la fonctionnalité de l'application pour vérifier que l'application exige que les mots de passe soient changés au moins une fois tous les 90 jours une fois le changement terminé.	

Conditions de la norme PA-DSS	Procédures de test	Directive
3.1.8 L'application de paiement conserve l'historique des mots de passe et exige d'un nouveau mot de passe qu'il soit différent des quatre derniers mots de passe utilisés. ***Correspond à la condition 8.2.5 de la norme PCI DSS***	**3.1.8** Pour tous les comptes générés ou gérés par l'application, tester l'application comme suit :	Si l'historique de mot de passe n'est pas maintenu, l'efficacité du changement de mot de passe est réduite, dans la mesure où il est possible de réutiliser indéfiniment les mots de passe précédents. Demander à ce que les mots de passe ne puissent pas être réutilisés pendant une certaine période de temps réduit la possibilité que des mots de passe qui ont été devinés ou forcés soient utilisés à l'avenir.
	3.1.8.a Installer l'application de paiement selon le *Guide de mise en œuvre de la norme PA-DSS* et examiner les paramètres du compte pour vérifier que, une fois le processus d'installation terminé, l'application conserve l'historique des mots de passe et nécessite qu'un mot de passe différent des quatre derniers mots de passe soit utilisé.	
	3.1.8.b Tester toutes les fonctionnalités de l'application qui font qu'un utilisateur revient aux paramètres par défaut, les changements aux configurations de comptes existants, la génération de nouveaux comptes et la recréation de comptes existants. Pour tous les types de changements effectués, examiner les configurations de compte et tester la fonctionnalité de l'application pour vérifier que l'application conserve l'historique des mots de passe et nécessite qu'un nouveau mot de passe soit différent des quatre derniers mots de passe utilisés, une fois le changement terminé.	
3.1.9 L'application de paiement limite les tentatives d'accès répétées en verrouillant le compte de l'utilisateur après six tentatives au maximum. ***Correspond à la condition 8.1.6 de la norme PCI DSS***	**3.1.9** Pour tous les comptes générés ou gérés par l'application, tester l'application comme suit :	Sans des mécanismes de blocage de compte, un pirate peut en permanence tenter de deviner un mot de passe à l'aide d'outils manuels ou automatiques (par exemple, craquage de mots de passe), jusqu'à ce qu'il réussisse et l'utilise pour accéder au compte d'un utilisateur.
	3.1.9.a Installer l'application de paiement selon le *Guide de mise en œuvre de la norme PA-DSS* et examiner les paramètres du compte pour vérifier que, une fois le processus d'installation terminé, l'application bloque les comptes d'utilisateur après plus de six tentatives de connexion infructueuses.	

Conditions de la norme PA-DSS	Procédures de test	Directive
	3.1.9.b Tester toutes les fonctionnalités de l'application qui font qu'un utilisateur revient aux paramètres par défaut, les changements aux configurations de comptes existants, la génération de nouveaux comptes et la recréation de comptes existants. Pour tous les types de changements effectués, examiner les configurations de compte et tester la fonctionnalité de l'application pour vérifier que l'application bloque les comptes utilisateur après pas plus de six tentatives de connexion infructueuses, une fois le changement terminé.	
3.1.10 L'application de paiement règle la durée de verrouillage sur 30 minutes au moins ou jusqu'à ce que l'administrateur active l'ID de l'utilisateur. ***Correspond à la condition 8.1.7 de la norme PCI DSS***	**3.1.10** Pour tous les comptes générés ou gérés par l'application, tester l'application comme suit :	Si un compte est bloqué parce que quelqu'un a essayé à plusieurs reprises d'en deviner le mot de passe, des contrôles retardant la réactivation de ce compte empêchent l'individu malveillant de poursuivre (il devra s'arrêter pendant au moins 30 minutes jusqu'à la réactivation du compte). De plus, si la réactivation devait être demandée, l'administrateur peut valider que c'est effectivement le propriétaire du compte qui demande sa réactivation.
	3.1.10.a Installer l'application de paiement selon le *Guide de mise en œuvre de la norme PA-DSS* et examiner les paramètres du compte pour vérifier que, une fois le processus d'installation terminé, l'application configure le blocage à un minimum de 30 minutes ou jusqu'à ce que l'administrateur réactive l'ID utilisateur.	
	3.1.10.b Tester toutes les fonctionnalités de l'application qui font qu'un utilisateur revient aux paramètres par défaut, les changements aux configurations de comptes existants, la génération de nouveaux comptes et la recréation de comptes existants. Pour tous les types de changements effectués, examiner les configurations de compte et tester la fonctionnalité de l'application pour vérifier que l'application configure la durée de blocage à un minimum de 30 minutes, ou jusqu'à ce que l'administrateur réactive l'ID utilisateur, une fois les changements terminés.	
3.1.11 Si une session d'application de paiement reste inactive pendant plus de 15 minutes, l'application exige de l'utilisateur d'entrer de nouveau ses éléments d'authentification pour réactiver la session. ***Correspond à la condition 8.1.8 de la norme***	**3.1.11** Pour tous les comptes générés ou gérés par l'application, tester l'application comme suit :	Lorsque les utilisateurs s'éloignent de leur ordinateur allumé ayant accès à l'application de paiement, cette connexion peut être utilisée par d'autres en l'absence de l'utilisateur, ce qui donne lieu à un accès non autorisé au compte et/ou à une
	3.1.11.a Installer l'application de paiement selon le *Guide de mise en œuvre de la norme PA-DSS* et examiner les paramètres du compte pour vérifier que, une fois le processus d'installation terminé, l'application configure le	

Conditions de la norme PA-DSS	Procédures de test	Directive
PCI DSS	temps de blocage à un minimum de 15 minutes ou moins.	utilisation malveillante du compte.
	3.1.11.b Tester toutes les fonctionnalités de l'application qui font qu'un utilisateur revient aux paramètres par défaut, les changements aux configurations de comptes existants, la génération de nouveaux comptes et la recréation de comptes existants. Pour tous les types de changements effectués, examiner les configurations de compte et tester la fonctionnalité de l'application pour vérifier que l'application configure la durée de blocage à un minimum de 15 minutes ou moins, une fois le changement terminé.	
3.2 Le fournisseur de logiciel doit indiquer à ses clients que tous les accès aux PC, serveurs et bases de données hébergeant les applications de paiement doivent exiger un ID d'utilisateur unique et une authentification sécurisée. ***Correspond aux conditions 8.1 et 8.2 de la norme PCI DSS***	**3.2** Examiner le *Guide de mise en œuvre de la norme PA-DSS* créé par le fournisseur pour vérifier qu'il est vivement recommandé aux clients et revendeurs/intégrateurs de contrôler l'accès, à l'aide d'un ID d'utilisateur unique et de l'authentification sécurisée conformes aux normes PCI DSS, à tout PC, serveur et base de données hébergeant des applications de paiement et des données de titulaires de carte.	Si l'application est installée sur des systèmes qui n'appliquent pas de contrôles d'authentification stricts, ou s'ils y ont accès, l'authentification stricte offerte par l'application pourrait être contournée et causer des accès non sécurisés.
3.3 Sécuriser tous les mots de passe de l'application de paiement (y compris les mots de passe pour utilisateur et comptes d'application) pendant la transmission et le stockage. ***Correspond à la condition 8.2.1 de la norme PCI DSS***	**3.3** Effectuez les tâches suivantes :	Si les mots de passe de l'application de paiement sont stockés ou transmis sur le réseau sans cryptage, un individu malveillant pourrait facilement intercepter le mot de passe à l'aide d'un « renifleur », ou accéder directement aux mots de passe dans les fichiers où ils sont stockés et utiliser ces données volées pour obtenir un accès non autorisé. La concaténation d'une entrée variable unique à chaque mot de passe avant que le hachage de l'algorithme ne soit
3.3.1 Utiliser une cryptographie robuste pour rendre tous les mots de passe de l'application illisibles pendant la transmission.	**3.3.1.a** Examiner la documentation du vendeur et les configurations de l'application pour vérifier qu'une cryptographie robuste est utilisée pour rendre tous les mots de passe illisibles en permanence pendant la transmission.	

Conditions de la norme PA-DSS	Procédures de test	Directive
	3.3.1.b Pour tous les types de mots de passe d'application, examiner la transmission des mots de passe (par exemple, en ouvrant une session à partir d'un autre système et en authentifiant l'application à d'autres systèmes) pour vérifier qu'une cryptographie robuste est utilisée pour rendre tous les mots de passe illisibles en permanence pendant la transmission.	
3.3.2 Utilisez un algorithme cryptographique unilatéral, basé sur les normes approuvées pour rendre les mots de passe d'application de paiement illisibles pendant le stockage. Chaque mot de passe doit avoir une variable d'entrée unique qui est concaténée avec le mot de passe avant que l'algorithme cryptographique ne soit appliqué.	**3.3.2.a** Examiner la documentation du fournisseur et les configurations de l'application pour vérifier que **:** • Les mots de passe stockés sont rendus illisibles à l'aide d'un algorithme cryptographique unilatéral robuste, basé sur les normes approuvées. • Une variable d'entrée unique est concaténée avec chaque mot de passe avant que l'algorithme cryptographique ne soit appliqué.	
Remarque : *La variable d'entrée n'a pas besoin d'être imprévisible ou secrète*	**3.3.2.b** Pour tous les types de mot de passe d'application, identifier tous les emplacements où l'application peut stocker les mots de passe, y compris au sein de l'application elle-même, sur les systèmes sous-jacents, les fichiers de journaux, les configurations de registre, etc. Pour tous les emplacements et types de mots de passe, examiner les fichiers stockés pour vérifier que les mots de passe sont rendus illisibles en permanence lors du stockage à l'aide d'un algorithme cryptographique unilatéral fiable, avec une variable d'entrée unique.	

Conditions de la norme PA-DSS	Procédures de test	Directive
3.4 L'application de paiement doit limiter l'accès aux fonctions/ressources requises et appliquer le moins de privilèges pour les comptes intégrés. • Par défaut, tous les comptes d'application/service ont accès uniquement aux fonctions/ressources dont ils ont spécifiquement besoin pour leur compte d'application/service. • Par défaut, tous les comptes d'application/service ont un niveau de privilège minimum affecté à chaque fonction/ressource selon les besoins du compte d'application/service. ***Correspond à la condition 7 de la norme PCI DSS***	**3.4.a** Installer l'application de paiement selon le *Guide de mise en œuvre de la norme PA-DSS* et examiner les paramètres des comptes intégrés pour vérifier que, lorsque le processus d'installation est terminé : • Tous les comptes d'application/service ont accès uniquement aux fonctions/ressources dont ils ont spécifiquement besoin pour leur compte d'application/service. • Tous les comptes d'application/service ont un niveau de privilège minimum affecté à chaque fonction/ressource selon les besoins du compte d'application/service.	Afin de limiter l'accès aux données de titulaires de carte et aux fonctions sensibles uniquement aux comptes qui ont besoin d'un tel accès, les besoins d'accès et le niveau de privilège requis doivent être définis pour chaque compte intégré, de sorte que ses fonctions assignées puissent être accomplies, mais qu'aucun accès supplémentaire ou inutile ne soit accordé. L'emploi du principe du moindre privilège aide à empêcher les utilisateurs qui ne connaissent pas suffisamment l'application de modifier sa configuration accidentellement ou de manière incorrecte, ou de modifier ses réglages de sécurité. Appliquer le moins de privilèges aide à minimiser la portée des dommages si une personne non autorisée obtient l'accès à un ID utilisateur.
	3.4.b Tester toutes les fonctions de l'application qui provoquent des changements aux comptes intégrés, y compris ceux qui ramènent les comptes utilisateurs aux paramètres par défaut, les changements aux configurations de compte existants, la production de nouveaux comptes et la recréation de comptes existants. Pour tous les types de changements effectués, examiner les configurations des comptes intégrés et tester la fonctionnalité de l'application pour vérifier que, une fois le changement accompli : • Tous les comptes d'application/service ont accès uniquement aux fonctions/ressources dont ils ont spécifiquement besoin pour leur compte d'application/service. • Tous les comptes d'application/service ont un niveau de privilège minimum affecté à chaque fonction/ressource selon les besoins du compte d'application/service.	

Condition 4 : Enregistrer l'activité de l'application de paiement

Conditions de la norme PA-DSS	Procédures de test	Directive
4.1 À l'issue du processus d'installation, l'installation par défaut « prête à l'emploi » de l'application de paiement doit enregistrer tous les accès utilisateur et permettre d'associer toutes les activités à leurs utilisateurs individuels. ***Correspond à la condition 10.1 de la norme PCI DSS***	**4.1.a** Installer l'application de paiement. Tester l'application pour vérifier que les pistes d'audit de l'application sont automatiquement activées à l'installation.	Il est essentiel que l'application de paiement dispose d'un processus ou d'un mécanisme qui relie les utilisateurs aux ressources accédées de l'application, génère des journaux d'audit et donne la possibilité de retracer les activités suspectes à un utilisateur spécifique. Les équipes d'enquête après incident dépendent de ces journaux pour lancer leur investigation.
	4.1.b Examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur pour vérifier que les informations suivantes sont incluses : • Comment installer l'application pour que les journaux soient configurés et activés par défaut lorsque le processus d'installation est terminé. • Comment configurer les paramètres de journaux conformément à la norme PCI-DSS, selon les conditions 4.2, 4.3 et 4.4 de la norme PA-DSS ci-dessous, pour toutes les options de journalisation qui sont configurables par le client après installation. • Les journaux ne doivent pas être désactivés, car cela entraînerait la non-conformité aux normes PCI DSS. • Comment configurer les paramètres de journaux conformément à la norme PCI-DSS pour tous les composants de logiciel tiers en paquetage avec l'application de paiement ou requise par celle-ci, pour toute option de journalisation pouvant être configurée par le client après installation.	
4.2 L'application de paiement doit fournir des pistes d'audit automatiques pour reconstituer les événements suivants : ***Correspond à la condition 10.2 de la norme PCI DSS***	**4.2** Tester l'application de paiement en examinant les paramètres et sorties de ses journaux d'audit et en exécutant les opérations suivantes :	Consigner les événements décrits en 4.2.1 - 4.2.7 permet à l'organisation d'identifier et de retracer des activités potentiellement malveillantes.

Conditions de la norme PA-DSS	Procédures de test	Directive
4.2.1 Tous les accès des utilisateurs aux données de titulaires de carte à partir de l'application	**4.2.1** Vérifier que tous les accès individuels aux données de titulaires de carte effectués par l'application de paiement sont consignés.	Les individus malveillants peuvent avoir connaissance d'un compte utilisateur qui a accès aux données de titulaires de carte à l'aide de l'application, ou ils pourraient créer un nouveau compte non autorisé afin d'accéder à ces données. Enregistrer tous les accès individuels aux données de titulaires de carte permet d'identifier les comptes compromis ou utilisés de manière illicite.
4.2.2 Toutes les actions de tout individu ayant des privilèges administratifs assignés dans l'application	**4.2.2** Vérifier que toutes les actions prises par tout individu ayant des privilèges administratifs dans l'application de paiement sont consignées.	Les comptes possédant des privilèges accrus, comme les comptes « administrateur », ont le potentiel d'avoir le plus grand impact sur la sécurité ou la fonctionnalité opérationnelle de l'application. Sans un journal des activités exécutées, une organisation est incapable de retracer tout problème provoqué par une erreur administrative ou d'une utilisation illicite d'un privilège à l'action et à l'individu spécifiques.
4.2.3 Accès aux journaux d'audit de l'application gérée par ou contenue dans l'application	**4.2.3** Vérifier que l'accès aux journaux d'audit de l'application gérée par ou contenue dans l'application est consigné dans le journal.	Des utilisateurs malveillants tentent souvent de modifier les journaux d'audit afin de dissimuler leurs activités et un enregistrement des accès permet à une organisation de retracer toutes les incohérences ou altérations potentielles des journaux pour un compte individuel.
4.2.4 Tentatives d'accès logique non valides	**4.2.4** Vérifier que les tentatives d'accès logique non valides sont consignées.	Les individus malveillants font souvent plusieurs tentatives pour accéder aux systèmes ciblés. De multiples tentatives infructueuses de connexion peuvent indiquer qu'un utilisateur non autorisé tente d'utiliser la « force brute » ou de deviner un mot de passe.

Conditions de la norme PA-DSS	Procédures de test	Directive
4.2.5 L'utilisation et la modification des mécanismes d'identification et d'authentification de l'application (comprenant, entre autres, la création de nouveaux comptes, l'élévation de privilèges, etc.) et toutes les modifications, additions, suppressions aux comptes de l'application avec privilèges racines ou administratifs	**4.2.5** Vérifier que l'utilisation et les modifications des mécanismes d'identification et d'authentification de l'application (comprenant, entre autres, la création de nouveaux comptes, l'élévation de privilèges, etc.) et toutes les modifications, additions, suppressions aux comptes de l'application avec privilèges racines ou administratifs sont consignés dans le journal.	Si l'on ne dispose pas du moyen de savoir qui était connecté au moment de l'incident, il est impossible d'identifier les comptes qui ont été utilisés. En outre, les utilisateurs malveillants peuvent tenter de manipuler les contrôles d'authentification avec l'intention de les contourner ou d'usurper un compte valide. Les activités comprenant, sans y être limitées, la création de nouveaux comptes, l'élévation de privilèges ou des modifications des autorisations d'accès peuvent indiquer une utilisation non autorisée des mécanismes d'authentification du système.
4.2.6 Initialisation, interruption ou pause des journaux d'audit de l'application	**4.2.6** Vérifier que ce qui suit est consigné dans le journal : • Initialisation des journaux d'audit de l'application ; • Interruption ou pause des journaux d'audit de l'application.	La désactivation (ou pause) des journaux d'audit avant de se livrer à des activités illicites est une pratique courante des individus mal intentionnés souhaitant éviter d'être détectés. L'initialisation des journaux d'audit peut indiquer que la fonction de journalisation a été désactivée par un utilisateur pour dissimuler son activité.
4.2.7 Création et suppression d'objets de niveau système au sein de, ou par, l'application	**4.2.7** Vérifier que la création et la suppression d'objets de niveau système au sein de l'application ou par l'application sont consignées.	Souvent, les utilisateurs malveillants créent ou remplacent des objets au niveau système, sur le système visé, afin de prendre le contrôle d'une fonction particulière ou de l'activité de ce système. En effectuant les enregistrements dans le journal lorsque les objets au niveau du système, tels que les tableaux de base de données ou les procédures enregistrées, sont créés ou supprimés, il sera plus facile de déterminer si ces modifications ont été autorisées.
4.3 L'application de paiement doit enregistrer au moins les entrées du journal d'audit suivantes pour chaque événement : ***Correspond à la condition 10.3 de la norme PCI DSS***	**4.3** Tester l'application de paiement en examinant les paramètres du journal d'audit et les sorties du journal d'audit et, pour chaque événement à vérifier (à partie de 4.2), exécuter les opérations suivantes :	En enregistrant les détails décrits en 4.3.1 - 4.3.6 pour les événements vérifiables au point 4.2, un compromis potentiel peut être rapidement identifié et, avec suffisamment de détails pour connaître l'auteur, l'objet, l'emplacement, le moment et la méthode

Conditions de la norme PA-DSS	Procédures de test	Directive
4.3.1 Identification de l'utilisateur	**4.3.1** Vérifier que l'identification d'utilisateur est incluse dans les entrées des journaux.	employée.
4.3.2 Type d'événement	**4.3.2** Vérifier que le type d'événement est inclus dans les entrées des journaux.	
4.3.3 Date et heure	**4.3.3** Vérifier que l'horodatage est inclus dans les entrées de journaux.	
4.3.4 Indication de succès ou d'échec	**4.3.4** Vérifier que l'indication de succès ou d'échec est incluse dans les entrées de journaux.	
4.3.5 Origine de l'événement	**4.3.5** Vérifier que l'origine de l'événement est incluse dans les entrées de journaux.	
4.3.6 Identité ou nom des données, du composant du système ou de la ressource affectés	**4.3.6** Vérifier que l'identité ou le nom des données, du composant du système ou de la ressource affectés est inclus dans les entrées de journaux.	
4.4. L'application de paiement doit permettre une journalisation centralisée. ***Remarque :*** *Les exemples de cette fonctionnalité peuvent comprendre, entre autres :* • Journalisation par des mécanismes de fichier journal standards du secteur comme le CLFS (Common Log File System, système commun de fichier journal), le protocole Syslog, un texte délimité, etc. ; • Fourniture de la fonctionnalité et de la documentation pour convertir le format journal exclusif de l'application aux formats journal standards du secteur permettant une journalisation centralisée immédiate. ***Correspond à la condition 10.5.3 de la norme PCI DSS***	**4.4.**a Examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur pour vérifier que les clients et revendeurs/intégrateurs reçoivent : • Une description des mécanismes de journalisation centralisés qui sont pris en charge ; • Des instructions et des procédures pour intégrer les journaux de l'application de paiement dans un environnement de journalisation centralisé. **4.4.b** Installer et configurer l'application de paiement selon le *Guide de mise en œuvre de la norme PA-DSS* pour vérifier que les instructions sont précises et que la fonctionnalité qui facilite la capacité d'un client à intégrer les journaux à leur serveur de journaux centralisé est incluse.	Sans une protection adéquate des journaux d'audit, il ne sera pas possible d'en garantir l'intégralité, l'exactitude et l'intégrité, et ils seront inutiles en tant qu'outil d'investigation une fois le système compromis. Inclure les journaux de l'application de paiement dans un système de journalisation centralisé permet au client d'intégrer et de mettre en corrélation leurs journaux, et de sécuriser les journaux de manière cohérente dans leur environnement.

Condition 5 : Développer des applications de paiement sécurisées

Conditions de la norme PA-DSS	Procédures de test	Directive
5.1 Le fournisseur du logiciel a défini et mis en œuvre un processus formel pour sécuriser le développement des applications de paiement, qui comprend : • Les applications de paiement sont développées conformément à la norme PCI DSS et la norme PA-DSS (par exemple, authentification et connexion sécurisées) ; • Les processus de conception de logiciel sont basés sur les normes/meilleures pratiques du secteur ; • La sécurité des informations est intégrée à l'ensemble du cycle de vie du développement du logiciel ; • Les vérifications de sécurité sont effectuées avant le lancement d'une application ou de la mise à jour d'une application. ***Correspond à la condition 6.3 de la norme PCI DSS***	**5.1.a** Examiner le processus de développement de logiciel écrit et vérifier que les processus respectent les normes du secteur et/ou les meilleures pratiques.	Faute d'intégrer la sécurité pendant les phases de définition des conditions, de conception, d'analyse et de test du développement du logiciel, des vulnérabilités de sécurité peuvent être introduites, accidentellement ou par malveillance, dans le code de l'application.
	5.1.b Vérifier que les processus documentés du développement du logiciel comprennent des procédures pour les éléments suivants : • Incorporer la sécurité des informations au cours du cycle de vie de la conception d'un logiciel. • Développer des applications de paiement selon les conditions des normes PCI DSS et PA-DSS.	
	5.1.c Vérifier que les processus documentés du développement du logiciel comprennent : • Les vérifications de sécurité définies avant le lancement d'une application ou la mise à jour d'une application. • Les procédures de vérification de sécurité à suivre pour garantir que les objectifs de sécurité des normes PCI DSS et PA-DSS sont respectés.	
	5.1.d Entretien avec les développeurs de logiciel pour confirmer que les processus documentés sont respectés tels que : • La sécurité des informations est intégrée à l'ensemble du cycle de vie du développement du logiciel. • Les applications de paiement sont développées conformément aux exigences des normes PCI DSS et PA-DSS. • Les vérifications de sécurité sont effectuées avant le lancement, pour garantir que les objectifs de sécurité, y compris les conditions des normes PCI DSS et PA-DSS, sont respectés.	
5.1.1 Les PAN actifs ne sont pas utilisés à des fins de test ou de développement. ***Correspond à la condition 6.4.3 de la norme PCI DSS***	**5.1.1.a** Vérifier les processus de développement de logiciel pour vérifier qu'ils comprennent des procédures garantissant que les PAN actifs ne sont pas utilisés à fin de test ou de développement.	Les marques de cartes de paiement et de nombreux émetteurs sont à même de fournir des numéros de compte convenant au test dans le cas où un PAN réaliste est nécessaire pour tester la fonctionnalité
	5.1.1.b Examiner les processus de test et interroger le	

Conditions de la norme PA-DSS	Procédures de test	Directive
	personnel pour vérifier que les PAN actifs ne sont pas utilisés à fin de test ou de développement.	d'un système avant lancement.
	5.1.1.c Examiner les échantillons de données de test pour vérifier que les PAN actifs ne sont pas utilisés à fin de test ou de développement.	
5.1.2 Les données de test et les comptes sont éliminés avant la mise à la disposition du client. ***Correspond à la condition 6.4.4 de la norme PCI DSS***	**5.1.2.a** Examiner les processus de développement de logiciel pour vérifier qu'ils comprennent des procédures garantissant que les données et les comptes de test sont éliminés avant que l'application ne soit mise à disposition pour les clients.	Les données et les comptes de test doivent être éliminés de l'application avant qu'elle ne soit fournie au client, dans la mesure où l'inclusion de ces éléments pourrait communiquer des informations à propos des constructions clés dans l'application.
	5.1.2.b Examiner les processus de test et interroger le personnel pour vérifier que les données et les comptes de test sont éliminés avant la mise à disposition pour le client.	
	5.1.2.c Examiner le produit final de l'application de paiement pour vérifier que les données et les comptes de test ont été éliminés avant la mise à disposition pour le client.	
5.1.3 Les comptes personnalisés d'application de paiement, les ID utilisateurs et les mots de passe sont supprimés avant que l'application de paiement ne soit mise à la disposition des clients ***Correspond à la condition 6.3.1 de la norme PCI DSS***	**5.1.3.a** Examiner les processus de développement de logiciel pour vérifier qu'ils comprennent des procédures garantissant que les données et les comptes de test sont éliminés avant que l'application ne soit mise à disposition pour les clients.	Les comptes client, ID utilisateurs et mots de passe créés avant le lancement pourraient être utilisés comme porte d'entrée pour que les développeurs et les autres individus ayant connaissance de ces comptes puissent accéder à l'application, ce qui pourrait compromettre l'application et les données de titulaires de carte en rapport.
	5.1.3.b Examiner les procédures de test et interroger le personnel pour vérifier que leurs comptes personnalisés dans l'application de paiement, les ID utilisateur et les mots de passe sont supprimés avant que l'application de paiement ne soit mise à la disposition des clients.	
	5.1.3.c Examiner le produit final de l'application de paiement afin de vérifier que les comptes personnalisés dans l'application de paiement, les ID utilisateur et les mots de passe sont supprimés avant que l'application de paiement ne soit mise à la disposition des clients.	

Conditions de la norme PA-DSS	Procédures de test	Directive
5.1.4 Le code de l'application de paiement est renouvelé avant la mise à la disposition des clients après tout changement d'importance, afin d'identifier toute vulnérabilité de codage éventuelle (en utilisant un processus manuel ou automatique) pour inclure au moins l'un des éléments suivants : • Les modifications de code sont examinées par des individus autres que l'auteur initial du code, qui doivent être compétents en la matière et maîtriser les pratiques de codage sécurisées. • Les examens du code garantissent que le code est développé conformément aux bonnes pratiques de codage sécurisé. (Voir la condition 5.2 de la norme PA-DSS.) • Les corrections appropriées sont implémentées avant la publication. • Les résultats de l'examen du code sont passés en revue et approuvés par les responsables avant le lancement. • Les résultats documentés de l'examen du code comprennent l'approbation des responsables, de l'auteur du code et du réviseur de code, ainsi que les corrections qui ont été mises en œuvre avant le lancement. ***Remarque :*** *Cette condition s'applique à tous les composants d'application de paiement (aussi bien les applications Web internes qu'orientées public), dans le cadre du cycle de développement du système. Les examens du code peuvent être réalisés par le personnel interne compétent ou par des prestataires tiers.* ***Correspond à la condition 6.3.2 de la norme PCI DSS***	**5.1.4.a** Examiner les procédures écrites de développement de logiciel et interroger le personnel responsable pour vérifier que le fournisseur effectue les examens de code pour tous les changements significatifs du code de l'application (en utilisant des processus manuels ou automatisés) comme suit : • Les modifications de code sont examinées par des individus autres que l'auteur initial du code, qui doivent être compétents en la matière et maîtriser les pratiques de codage sécurisées. • Les examens du code garantissent que le code est développé conformément aux bonnes pratiques de codage sécurisé. (Voir la condition 5.2 de la norme PA-DSS.) • Les corrections appropriées sont implémentées avant la publication. • Les résultats de l'examen du code sont passés en revue et approuvés par les responsables avant le lancement. • Les résultats documentés de l'examen du code, y compris l'approbation des responsables, de l'auteur du code et du réviseur de code, ainsi que les corrections ont été mises en œuvre avant le lancement. **5.1.4.b** Examiner les résultats de l'examen de code pour observer un échantillon des changements de code afin de vérifier que : • Les examens de code ont été effectués par une personne éclairée autre que l'auteur du code. • Les examens du code ont été développés en fonction des directives relatives au codage sécurisé. • Les corrections appropriées ont été implémentées avant la publication. • Les résultats de l'examen du code sont passés en revue et approuvés par les responsables avant le lancement.	Les vulnérabilités de sécurité du code d'application sont généralement exploitées par les individus malveillants pour accéder à un réseau et compromettre les données de titulaires de carte. Afin de protéger l'application contre ce type d'attaques, des techniques d'examen de code correctes doivent être utilisées. Les techniques d'examen de code doivent vérifier que les meilleures pratiques de codage sécurisé ont été utilisées au cours du processus de développement. Le fournisseur d'application doit intégrer les pratiques de codage sécurisé pertinentes, dans la mesure où elles sont applicables à la technologie particulière utilisée. Les examens doivent être effectués par une personne compétente pour la technologie et expérimentée en matière de techniques d'examen de code afin d'identifier tout problème de codage potentiel. Affecter des examens de code à une personne autre que le développeur du code permet d'exécuter un contrôle indépendant et objectif. La correction des erreurs de codage avant que le code ne soit lancé empêche que des codes défectueux ne soient exposés aux exploits potentiels dans les environnements de client. Un code défectueux est bien plus difficile et cher à réparer après qu'il ait été déployé. Inclure un examen formel et une signature des responsables avant le lancement aide à garantir que ce code est approuvé et a été développé selon les politiques et procédures.

Conditions de la norme PA-DSS	Procédures de test	Directive
5.1.5 Les pratiques sécuritaires de contrôle de source sont implémentées pour vérifier l'intégrité du code source pendant le processus de développement.	**5.1.5.a** Examiner les procédures écrites de développement de logiciel et interroger le personnel responsable pour vérifier que le vendeur maintient des pratiques de contrôle de source sécurisées pour vérifier l'intégrité du code source pendant le processus de développement.	De bonnes pratiques de contrôle de code source aident à garantir que les changements apportés au code sont prévus et autorisés, et accomplis uniquement par ceux qui ont une raison de changer le code. Les exemples de ces pratiques comprennent les procédures d'entrée et de sortie pour les codes avec des contrôles d'accès stricts et une comparaison immédiatement avant le téléchargement du code pour confirmer que la dernière version approuvée n'a pas été changée (par exemple, une somme de contrôle).
	5.1.5.b Examiner les mécanismes et observez les procédures de sécurisation du code source pour vérifier que l'intégrité du code source est maintenue pendant le processus de développement.	
5.1.6 Les applications de paiement sont développées selon les meilleures pratiques du secteur pour la sécurisation des techniques de codage sécurisées, y compris : • Développer en utilisant le principe du moindre privilège pour l'environnement de l'application. • Développer des paramètres de sécurité par défaut (toute exécution est refusée par défaut sauf spécification dans la conception initiale). • Développer des considérations de tous les points d'accès, y compris les entrées de variations telles que les entrées multi-canaux dans l'application.	**5.1.6.a** Examiner le processus de développement de logiciel écrit pour vérifier que des techniques de codage sécurisées sont définies et comprennent : • Développer en utilisant le principe du moindre privilège pour l'environnement de l'application. • Développer des paramètres de sécurité par défaut (toute exécution est refusée par défaut sauf spécification dans la conception initiale) • Développer des considérations de tous les points d'accès, y compris les entrées de variations telles que les entrées multi-canaux dans l'application.	Développer des applications avec moins de privilèges est la meilleure manière de garantir que des éléments peu sécurisés ne sont pas introduits dans l'application. Inclure des paramètres de sécurité par défaut pourrait empêcher un pirate d'obtenir des informations sensibles à propos d'un échec de l'application qui pourrait ensuite être utilisé pour créer des attaques ultérieures. Garantir que la sécurité est appliquée à tous les accès et à toutes les entrées à l'application évite les possibilités qu'un canal d'entrée puisse être laissé ouvert et compromis. Oublier de prendre ces concepts en compte lors du développement du code pourrait causer le lancement d'une application non sécurisée et des mesures de réparation potentiellement excessive dans l'avenir.
	5.1.6.b Interroger les développeurs pour vérifier que les applications sont développées selon les meilleures pratiques du secteur pour la sécurisation des techniques de codage sécurisées, y compris : • Développer en utilisant le principe du moindre privilège pour l'environnement de l'application. • Développer des paramètres de sécurité par défaut (toute exécution est refusée par défaut sauf spécification dans la conception initiale). • Développer des considérations de tous les points d'accès, y compris les entrées de variations telles que les entrées multi-canaux dans l'application.	

Conditions de la norme PA-DSS	Procédures de test	Directive
5.1.6.1 Les techniques de codage comprennent la documentation sur comment le PAN et/ou SAD sont traités dans la mémoire.	**5.1.6.1.a** Examiner les techniques de codage pour vérifier qu'elles comprennent la documentation sur comment le PAN et/ou SAD sont traités dans la mémoire.	Les pirates utilisent des outils de logiciels malveillants pour récupérer les données sensibles de la mémoire. Minimiser l'exposition des PAN/SAD lorsqu'ils sont en mémoire aidera à réduire la possibilité qu'ils soient capturés par un utilisateur malveillant ou involontairement sauvegardés sur un fichier mémoire sur un disque et laissés sans protection. Cette condition est destinée à assurer que la manière avec laquelle les PAN et SAD sont traités dans la mémoire est prise en compte. Comprendre quand et pour combien de temps les données sensibles sont présentes dans la mémoire, ainsi que sous quel format, aidera les fournisseurs de l'application à identifier les faiblesses potentielles à la sécurité de leur application et à déterminer si des protections supplémentaires sont nécessaires. Que des techniques de codage découlent ou non de cette activité dépendra du logiciel particulier en cours de développement et des technologies utilisées.
	5.1.6.1.b Interroger les développeurs pour vérifier qu'ils tiennent compte de la manière avec laquelle les PAN/SAD sont traités dans la mémoire pendant le processus de développement.	

Conditions de la norme PA-DSS	Procédures de test	Directive
5.1.7 Assurer la formation à jour aux pratiques de développement sécurisées pour les développeurs d'application au moins une fois par an, comme le requièrent leurs fonctions professionnelles et la technologie utilisée, par exemple : • Conception sécurisée de l'application. • Sécuriser les techniques de codage pour éviter les vulnérabilités de codage les plus fréquentes (par exemple, directives du fournisseur, 10 principales directives de la norme OWASP, 25 principales directives de la norme SANS CWE, codage sécurisé CERT, etc.). • Gérer les données sensibles dans la mémoire. • Examens de code. • Test de sécurité (par exemple, techniques de test de pénétration). • Techniques d'évaluation des risques. ***Remarque :*** *La formation des développeurs de l'application peut être effectuée en interne ou par des tiers. Les exemples de la technique de formation à utiliser peuvent comprendre la formation sur le terrain, par un instructeur ou par ordinateur.*	**5.1.7a** Vérifier que les processus de ce développement de logiciel documentés comprennent la formation à jour aux pratiques de développement sécurisées pour les développeurs d'application au moins une fois par an, comme le requièrent leurs fonctions professionnelles et la technologie utilisée.	Assurer que les développeurs sont informés des pratiques de développement sécurisées aidera à minimiser le nombre de vulnérabilités de la sécurité introduites par de mauvaises pratiques de codage. Le personnel formé doit également être plus à même d'identifier les problèmes de sécurité potentiels dans la conception et le code de l'application. Les plateformes et les méthodologies de développement de logiciel changent fréquemment, ainsi que les menaces et les risques pour les applications logicielles. La formation aux pratiques de développement sécurisées doit rester à jour du point de vue des changements de pratiques de développement.
	5.1.7.b Interroger un échantillon des développeurs afin de vérifier qu'ils connaissent les pratiques de développement et de codage sécurisées pertinentes à la technologie utilisée.	
	5.1.7.c Examiner la documentation des formations afin de vérifier que tous les développeurs d'application reçoivent une formation adéquate au moins une fois par an, comme le requièrent leurs fonctions professionnelles et la technologie utilisée.	
5.1.7.1 Mettre à jour la formation au besoin pour répondre aux derniers développements technologiques et aux méthodes utilisées.	**5.1.7.1** Examiner la documentation de formation et interroger un échantillon des développeurs pour vérifier que la formation est actualisée pour répondre aux nouvelles technologies de développement et aux méthodes utilisées.	

Conditions de la norme PA-DSS	Procédures de test	Directive
5.2 Développer toutes les applications de paiement pour prévenir des vulnérabilités de logiciel les plus courantes lors du processus de développement de logiciel. ***Remarque :*** *Les vulnérabilités décrites aux conditions 5.2.1 à 5.2.10 de la norme PA-DSS et aux points 6.5.1 à 6.5.10 de la norme PCI DSS faisaient partie des meilleures pratiques du secteur au moment de la publication de cette version de la norme PA DSS. Cependant, comme les meilleures pratiques de gestion de la vulnérabilité du secteur sont actualisées (par exemple, le Top 10 OWASP, le Top 25 SANS CWE, le codage sécurisé CERT, etc.), se reporter aux meilleures pratiques actuelles pour ces conditions.* ***Correspond à la condition 6.5 de la norme PCI DSS***	**5.2** Vérifier que les applications de paiement ne sont pas vulnérables aux vulnérabilités de codage courantes en effectuant un test manuel ou automatique de pénétration permettant spécifiquement d'exploiter chacun des éléments suivants :	La couche application comporte un risque élevé et peut être la cible de menaces internes et externes. Sans une sécurité appropriée, les données de titulaires de carte et autres informations confidentielles de la société peuvent être exposées. Les conditions 5.2.1 à 5.2.10 représentent les contrôles minimums à mettre en place. Cette liste est composée des vulnérabilités les plus courantes au moment de la publication de cette version de la norme PA-DSS. Lorsque les pratiques de codage sécurisé, acceptées par le secteur, changent, les pratiques de codage des fournisseurs doivent elles aussi être mises à jour.
Remarque : *Les conditions 5.2.1 à 5.2.6, ci-dessous, s'appliquent à toutes les applications (internes ou externes) :*		

Conditions de la norme PA-DSS	Procédures de test	Directive
5.2.1 Attaques par injections, notamment les injections de commandes SQL. Envisager également les attaques par injection OS, LDAP et Xpath ainsi que les autres attaques par injection.	**5.2.1** Les attaques par injection, en particulier injection de commandes SQL, sont effectuées au moyen de techniques de codage qui comprennent : • La validation d'entrée pour vérifier que les données utilisateurs ne peuvent pas modifier le sens des commandes et des requêtes. • Utiliser des requêtes paramétrées.	Les attaques par injection, en particulier injection de commandes SQL, sont une méthode couramment utilisée pour compromettre des applications. Une attaque par injection se produit lorsque les données saisies par un utilisateur sont transmises à un programme d'interprétation dans le cadre d'une commande ou d'une requête. Les données hostiles du pirate trompent le programme d'interprétation pour lui faire exécuter des commandes non prévues ou pour modifier les données, ce qui expose les composants à l'intérieur de l'application à des attaques telles que la saturation de la mémoire tampon. Les informations saisies doivent être validées par l'application avant d'être traitées, par exemple en vérifiant tous les caractères alphabétiques, le mélange de caractères alphanumériques, etc.
5.2.2 Saturation de la mémoire tampon	**5.2.2** Les saturations de la mémoire tampon sont résolues par des techniques de codage qui comprennent : • Validation de limites de la mémoire tampon ; • Troncage des chaînes d'entrées.	La saturation de la mémoire tampon se produit lorsqu'une application ne dispose pas de contrôles de limites sur l'espace de sa mémoire tampon. Ceci a pour résultat de pousser les informations de la mémoire tampon en dehors de son espace et dans l'espace exécutable de la mémoire. Lorsque cela se produit, le pirate a la possibilité d'insérer un code malveillant à une extrémité de la mémoire puis de le pousser dans l'espace exécutable de la mémoire en saturant la mémoire tampon. Le code malveillant est ensuite exécuté et permet souvent l'accès à distance du pirate, à l'application et/ou au système infecté.

Conditions de la norme PA-DSS	Procédures de test	Directive
5.2.3 Stockage cryptographique non sécurisé	**5.2.3** Le stockage cryptographique non sécurisé peut être résolu par des techniques de codage qui comprennent : • Prévenir les défauts cryptographiques. • Utiliser des algorithmes et des clés cryptographiques robustes.	Les applications qui n'utilisent pas de robustes fonctions cryptographiques correctement pour stocker des données présentent un risque accru d'être compromises et d'exposer les justificatifs d'authentification et/ou les données de titulaires de carte.
5.2.4 Communications non sécurisées	**5.2.4** Les communications non sécurisées sont résolues à l'aide de techniques de codage qui authentifient et cryptent correctement toutes les communications sensibles.	Les applications qui ne réussissent pas à correctement crypter le trafic réseau sensible à l'aide d'une cryptographie robuste présentent un risque accru d'être compromises et d'exposer les données de titulaires de carte.
5.2.5 Traitement inapproprié des erreurs	**5.2.5** Le traitement inapproprié des erreurs est résolu à l'aide de techniques de codage qui ne laissent fuir aucune information par le biais de messages d'erreur (par exemple, en retournant des détails d'erreur génériques plutôt que spécifiques).	Les applications qui laissent filtrer accidentellement des informations sur leur configuration, leurs mécanismes internes, ou qui exposent des informations privilégiées en raison de méthodes de traitement incorrectes risquent d'être compromises. Les pirates exploitent ces faiblesses pour subtiliser des données sensibles ou pour compromettre le système dans sa globalité. Si un individu malveillant peut créer des erreurs que l'application ne gère pas correctement, il peut alors obtenir des informations détaillées sur le système, créer des interruptions par déni de service, mettre la sécurité en échec ou entraîner une panne de l'application ou du système. Par exemple, le message selon lequel le « mot de passe saisi est incorrect » indique à un pirate que l'ID utilisateur fourni est correct et qu'il doit concentrer ses efforts sur le décryptage du mot de passe. Utiliser des messages d'erreur plus génériques, comme « Impossible de vérifier les données ».

Conditions de la norme PA-DSS	Procédures de test	Directive
5.2.6 Toutes les vulnérabilités à « risque élevé », identifiées dans le processus d'identification de vulnérabilité selon la condition 7.1 de la norme PA-DSS.	**5.2.6** Les techniques de codage répondent aux vulnérabilités à « risque élevé » qui pourraient affecter l'application, comme identifié par la condition 7.1. de la norme PA-DSS.	Toutes les vulnérabilités déterminées par le processus de classement des risques de vulnérabilité du fournisseur (défini dans la condition 7.1 de la norme PA-DSS) comme étant un « risque élevé » et qui pourraient affecter l'application doivent être identifiées et résolues pendant le développement de l'application.
Remarque : *les conditions 5.2.7 à 5.2.10, ci-dessous, s'appliquent aux applications Web et aux interfaces d'application (internes ou externes) :*		Les applications Web comportent des risques de sécurité uniques dus à leur architecture, à leur manque de difficulté relatif et aux possibilités de les compromettre.
5.2.7 Attaques par script inter-site (XSS).	**5.2.7** Les attaques par script inter-site sont résolues par des techniques de codage qui comprennent : • La validation de tous les paramètres avant l'inclusion. • L'utilisation d'un mécanisme d'échappement sensible au contexte.	Les attaques XSS se produisent chaque fois qu'une application extrait les données fournies par un utilisateur et les transmet à un navigateur Web sans d'abord les valider ou coder le contenu. Une attaque XSS permet aux pirates d'exécuter, dans le navigateur de la victime, un script qui peut détourner les sessions d'utilisateur, rendre des sites Web illisibles, introduire des vers, etc.

Conditions de la norme PA-DSS	Procédures de test	Directive
5.2.8 Contrôle d'accès inapproprié comme des références d'objet directes non sécurisées, impossibilité de limiter l'accès URL, et survol de répertoire	**5.2.8** Le contrôle d'accès inapproprié, comme des références d'objet directes non sécurisées, l'impossibilité de limiter l'accès URL et le survol de répertoire, est résolu à l'aide de techniques de codage qui comprennent : • L'authentification correcte des utilisateurs ; • L'assainissement des entrées ; • Ne pas exposer les références d'objets internes aux utilisateurs ; • Les interfaces utilisateurs qui ne permettent pas d'accéder aux fonctions non autorisées.	Une référence d'objet directe existe lorsqu'un développeur expose la référence à un objet d'implémentation interne, par exemple un fichier, un répertoire, un enregistrement de base de données ou une clé, comme une adresse URL ou un paramètre de formulaire. Les pirates peuvent manipuler ces références pour accéder à d'autres objets sans autorisation. Un pirate peut être en mesure de détailler la structure du répertoire d'un site Web (répertoire transversal) et de le parcourir, obtenant ainsi accès à des informations non autorisées ainsi que la compréhension du fonctionnement du site qu'il exploitera plus tard. Des interfaces utilisateurs, qui donnent accès à des fonctions non autorisées, pourraient permettre à des individus non autorisés d'accéder à des justificatifs privilégiés ou à des données de titulaires de carte. Limiter l'accès aux ressources de données aidera à empêcher que les données de titulaires de carte ne soient présentées à des ressources non autorisées.
5.2.9 Attaques CSRF (falsification de requête inter-site)	**5.2.9** Les attaques de falsification de requête inter-site (CSRF) sont résolues en utilisant des techniques de codage qui assurent que les applications ne comptent pas sur des justificatifs d'autorisation et sur des jetons soumis automatiquement par les navigateurs.	Une attaque CSRF force le navigateur d'une victime connectée à envoyer une requête pré-authentifiée à une application Web vulnérable, qui permet ensuite au pirate d'effectuer les opérations de changement d'état que la victime est autorisée à effectuer (comme de mettre à jour les détails de compte, effectuer des achats ou même s'authentifier envers l'application).

Conditions de la norme PA-DSS	Procédures de test	Directive
5.2.10 Rupture dans la gestion des authentifications et des sessions	**5.2.10** La rupture dans la gestion des authentifications et des sessions est résolue à l'aide de techniques de codage qui comprennent fréquemment : • Étiqueter les jetons de session (par exemple les cookies) comme étant « sécurisés ». • Ne pas exposer les ID de session dans l'URL. • Incorporer des durées limites de session et des rotations d'ID de session avec une connexion réussie.	Sécuriser l'authentification et la gestion de session empêche les individus non autorisés de compromettre les justificatifs de compte légitimes, les clés ou les jetons de session qui, autrement, permettrait à l'intrus d'assurer l'identité d'un utilisateur autorisé.
5.3 Le fournisseur de logiciel doit suivre les procédures de contrôle des changements pour toute modification apportée à l'application. Les procédures de changement du contrôle doivent suivre les mêmes processus de développement de logiciel que les logiciels nouvellement lancés (comme défini dans la condition 5.1 de la norme PA-DSS) et inclure les points suivants : ***Correspond à la condition 6.4.5 de la norme PCI DSS***	**5.3.a** Examiner les procédures de contrôle des changements du fournisseur pour les modifications logicielles et • Vérifier que les procédures respectent les processus documentés de développement de logiciel, tel que le définit la condition 5.1. • Vérifier que les procédures nécessitent les éléments 5.3.1 à 5.3.4 ci-dessous.	En cas de gestion inadéquate, l'impact des mises à jour du logiciel et des correctifs de sécurité ne sera pas pleinement effectif et risquerait d'avoir des conséquences non intentionnelles.
	5.3.b Interroger les développeurs pour déterminer les changements récents de l'application de paiement. Examiner les changements récemment apportés à l'application de paiement et remonter à la documentation de contrôle des changements associée. Pour chaque changement examiner, vérifier que les points suivants ont été documentés selon les procédures de contrôle des changements :	
5.3.1 Documentation de l'impact	**5.3.1** Vérifier que la documentation de l'impact sur les clients est comprise dans la documentation de contrôle des changements, et ce pour chaque changement.	L'impact de la modification doit être documenté de sorte que toutes les parties concernées soient en mesure de planifier en conséquence pour tout changement du traitement.
5.3.2 Documentation du changement approuvée par les parties autorisées appropriées	**5.3.2** Vérifier que la documentation du changement, approuvée par les parties autorisées appropriées, existe pour chaque modification.	L'approbation par les parties autorisées indique que la modification est légitime et que le changement approuvé est ratifié par la direction.
5.3.3 Test de fonctionnalité pour vérifier que le changement ne compromet pas la sécurité du système	**5.3.3.a** Vérifier que le test de fonctionnalité a été exécuté pour vérifier que le changement ne compromet pas la sécurité du système.	Un test approfondi doit être effectué afin de vérifier que la sécurité de l'application de paiement n'est pas diminuée par la

Conditions de la norme PA-DSS	Procédures de test	Directive
	5.3.3.b Vérifier que la conformité de tous les changements (y compris les correctifs) à la condition 5.2 a été testée, avant publication.	mise en œuvre d'une modification. Le test doit valider que tous les contrôles de sécurité existants restent en place, sont remplacés par des contrôles de force équivalente, ou sont renforcés après toute modification de l'application.
5.3.4 Procédures de suppression et de désinstallation des produits	**5.3.4** Vérifier que des procédures de suppression ou de désinstallation des produits sont prévues pour chaque changement.	Pour chaque modification, il doit exister des procédures de retrait au cas où la modification échouerait ou aurait des effets néfastes sur la sécurité de l'application, afin de permettre de restaurer le système à son état antérieur.

Conditions de la norme PA-DSS	Procédures de test	Directive
5.4 Le fournisseur de l'application de paiement doit documenter et suivre une méthodologie de contrôle des versions de logiciel dans le cadre du cycle de vie du développement de système. Cette méthodologie doit suivre les procédures du *Guide du programme de la norme PA-DSS* pour les changements de l'application de paiement et inclure au moins les éléments suivants :	**5.4** Examiner les processus documentés de développement de logiciel pour vérifier qu'ils comprennent la méthodologie de contrôle de version du logiciel du vendeur et que la méthodologie de contrôle de version doit respecter le Guide du programme de la norme PA-DSS. Vérifier que la méthodologie de contrôle de version documentée doit être suivie pour l'application de paiement, y compris pour tous les changements de l'application de paiement.	Sans une méthodologie de contrôle de version définie minutieusement, les changements apportés à l'application sont susceptibles de ne pas être identifiés correctement ; les clients et intégrateurs/revendeurs pourraient ne pas comprendre l'impact d'un changement de version de l'application.
5.4.1 La méthodologie de contrôle de version doit définir les éléments de version spécifiques qui sont utilisés, tels que : • Les détails sur la manière avec laquelle les éléments du système de version s'accordent avec les conditions spécifiées dans le *Guide du programme de la norme PA-DSS*. • Le format du système de version, y compris le nombre d'éléments, les séparations, les ensembles de caractères, etc. (constitué par des caractères alphabétiques, numériques et/ou alphanumériques). • Une définition de ce que chaque élément représente dans le système de gestion de version (par ex. type de changement, majeur, mineur ou changement d'entretien, caractère générique, etc.) • Définition des éléments qui indique l'utilisation de caractères génériques. ***Remarque :*** *Les caractères génériques peuvent*	**5.4.1.a** Examiner la méthodologie de contrôle de version documentée pour vérifier qu'elle comprend les éléments suivants : • Les détails sur la manière avec laquelle les éléments du système de numérotation de version s'accordent avec les conditions spécifiées dans le *Guide du programme de la norme PA-DSS.* • Le format du système de numérotation des versions est spécifié et comprend les détails du nombre d'éléments, les séparations, les ensembles de caractères, etc. (par exemple, 1.1.1.N, constitué par des caractères alphabétiques, numériques et/ou alphanumériques). • Une définition de ce que chaque élément représente dans le système de numérotation de version (par ex. type de changement, majeur, mineur ou changement d'entretien, caractère générique, etc.) • Définition des éléments qui indique l'utilisation de caractères génériques. **5.4.1.b** Vérifier que les éléments du système de version s'accordent avec les types de changement spécifiés dans le Guide du programme de la norme PA-DSS.	La méthodologie de gestion des versions du fournisseur d'application de paiement doit inclure une méthode définie de gestion des versions qui identifie de manière spécifique les éléments utilisés, le format de la version, la hiérarchie des différents éléments de version et ainsi de suite, pour l'application de paiement spécifique. La méthode de gestion des versions doit spécifier clairement comment chacun des différents éléments est utilisé dans le numéro de version. Le système de version peut être indiqué de différentes manières - par exemple, N.NN.NNA, où « N » indique un élément numérique et « A » est un élément alphabétique. Le système de version doit inclure l'identification de l'ensemble de caractères (par exemple : 0-9, A-Z, etc.) qui peut être utilisé pour chaque élément

Conditions de la norme PA-DSS	Procédures de test	Directive
uniquement être substitués par des éléments du numéro de version qui représente les changements n'ayant pas d'impact sur la sécurité. Consulter la condition 5.4.3 pour découvrir les conditions supplémentaires de l'utilisation des caractères génériques.	**5.4.1.c** Sélectionner un échantillon des changements récents de l'application de paiement, les numéros de version assignés et la documentation de contrôle de changement qui spécifie le type de changement d'application, et vérifier que les éléments du numéro de version correspondent au changement applicable et aux paramètres définis dans la méthodologie documentée de contrôle des versions.	de la version. Sans système de version correctement défini, les changements apportés à l'application ne seront pas représentés de manière fiable par le format du numéro de version.
	5.4.1.d Interroger un échantillon des développeurs afin de vérifier qu'ils connaissent le système de version, y compris l'utilisation acceptable des caractères génériques dans le numéro de version.	
5.4.2 La méthodologie de gestion des versions utilisée doit indiquer le type et l'impact de tous les changements de l'application selon le *Guide du programme de la norme PA-DSS*, y compris : • La description de tous les types et impacts des changements de l'application. • Une définition et une identification spécifique des changements qui : - N'ont pas d'impact sur la fonctionnalité de l'application ou de ses dépendances. - Ont un impact sur la fonctionnalité de l'application, mais pas d'impact sur la sécurité ou sur les conditions de la norme PA-DSS. - Ont un impact sur n'importe quelle fonctionnalité de sécurité ou condition de la norme PA-DSS. • Comment chaque type de changement est lié à un numéro de version spécifique.	**5.4.2.a** Examiner la méthodologie de gestion des versions du fournisseur de logiciel pour vérifier que la méthodologie de gestion des versions comprend : • Une description des types et des impacts de changements d'application (par exemple, les changements qui n'ont pas d'impact, qui ont un impact faible ou un impact élevé sur l'application) • Une définition et une identification spécifique des changements qui : - N'ont pas d'impact sur la fonctionnalité de l'application ou de ses dépendances. - Ont un impact sur la fonctionnalité de l'application, mais pas d'impact sur la sécurité ou sur les conditions de la norme PA-DSS. - Ont un impact sur n'importe quelle fonctionnalité de sécurité ou condition de la norme PA-DSS. • Comment chaque type de changement est lié à un numéro de version spécifique.	
	5.4.2.b Vérifier que la méthodologie de gestion des versions correspond aux exigences du *Guide du programme de la norme PA-DSS*.	

Conditions de la norme PA-DSS	Procédures de test	Directive
	5.4.2.c Interroger le personnel et observer les processus pour chaque type de changement afin de vérifier que la méthodologie documentée est suivie pour chaque type de changement.	
	5.4.2.d Sélectionner un échantillon des changements récents de l'application de paiement et examiner la documentation de contrôle du changement qui spécifie le type de changement d'application pour lequel vérifier que la version assignée au changement correspond au type de changement selon la méthodologie documentée.	
5.4.3 La méthodologie de gestion des versions doit identifier de manière spécifique si des caractères génériques sont utilisés et, si c'est le cas, comment ils sont utilisés. Les éléments suivants doivent être indiqués : • Détails sur la méthode d'utilisation des caractères génériques dans la méthodologie de gestion des versions. • Les caractères génériques ne sont jamais utilisés pour les changements qui ont un impact sur la sécurité ou pour la moindre condition de la norme PA-DSS. • Aucun élément du numéro de version utilisé pour représenter un changement n'ayant pas d'impact sur la sécurité (y compris un élément de caractère générique) ne doit être utilisé pour représenter un changement ayant un impact sur la sécurité. • Les éléments de caractère générique ne doivent pas précéder les éléments de la version qui pourraient représenter des changements ayant un impact sur la sécurité. Aucun élément de version apparaissant après un élément de caractère générique ne doit être utilisé pour représenter les changements ayant un impact sur la sécurité.	**5.4.3.a** Examiner la méthodologie de gestion des versions documentée du fournisseur de logiciel pour vérifier qu'elle inclut une identification spécifique sur l'utilisation des caractères génériques, y compris : • Détails sur la méthode d'utilisation des caractères génériques dans la méthodologie de gestion des versions. • Les caractères génériques ne sont jamais utilisés pour les changements qui ont un impact sur la sécurité ou pour la moindre condition de la norme PA-DSS. • Aucun élément du numéro de version utilisé pour représenter un changement n'ayant pas d'impact sur la sécurité (y compris un élément de caractère générique) ne doit être utilisé pour représenter un changement ayant un impact sur la sécurité. • Aucun élément à la droite d'un caractère générique ne peut être utilisé pour un changement ayant un impact sur la sécurité. Les éléments de version illustrant un changement ayant un impact sur la sécurité doivent s'afficher à gauche du premier élément du caractère générique.	Un élément de « caractère générique » PA-DSS pourrait aussi être utilisé dans le système de version pour représenter des changements multiples n'ayant pas d'impact sur la sécurité. Un caractère générique est le seul élément variable du système de version du fournisseur et il est utilisé pour indiquer qu'il existe des changements mineurs n'ayant pas d'impact sur la sécurité entre chaque version représentée par l'élément de caractère générique. Par exemple, un numéro de version 1.1.x recouvrirait les versions spécifiques 1.1.2 et 1.1.3, etc. pour faire savoir au client que le code de base entre eux est effectivement inchangé à l'exception de changements cosmétiques ou d'autres changements de types mineurs. Toute utilisation de caractères génériques doit être prédéfinie dans la méthodologie de gestion des versions du fournisseur et être uniquement utilisée selon le *Guide du programme de la norme PA-DSS*. ***Remarque :*** *L'utilisation de caractère générique est facultative et elle n'est pas nécessaire.*
	5.4.3.b Vérifier que toute utilisation de caractère générique respecte les conditions du *Guide du programme de la norme PA-DSS*. Par exemple, les éléments qui apparaissent après un élément de caractère générique ne doivent pas être utilisés pour les changements ayant un impact sur la sécurité.	

Conditions de la norme PA-DSS	Procédures de test	Directive
Remarque : *Les caractères génériques peuvent uniquement être utilisés selon le Guide du programme de la norme PA-DSS.*	**5.4.3.c** Interroger le personnel et observer les processus pour chaque type de changement afin de vérifier que : • Les caractères génériques ne sont jamais utilisés pour les changements qui ont un impact sur la sécurité ou pour la moindre condition de la norme PA-DSS. • Les éléments du numéro de version utilisé pour représenter des changements n'ayant pas d'impact sur la sécurité (y compris un élément de caractère générique) ne doivent jamais être utilisés pour représenter un changement ayant un impact sur la sécurité.	
	5.4.3.d Sélectionner un échantillon des changements récents de l'application de paiement et examiner la documentation de contrôle du changement qui spécifie le type de changement d'application. Vérifier que : • Les caractères génériques ne sont pas utilisés pour les changements qui ont un impact sur la sécurité ou pour la moindre condition de la norme PA-DSS. • Les éléments du numéro de version utilisé pour représenter des changements n'ayant pas d'impact sur la sécurité (y compris un élément de caractère générique) ne sont pas utilisés pour représenter un changement ayant un impact sur la sécurité.	

Conditions de la norme PA-DSS	Procédures de test	Directive
5.4.4 La méthodologie de gestion des versions publiée par le fournisseur doit être communiquée aux clients et aux intégrateurs/revendeurs.	**5.4.4** Vérifier que le *Guide de mise en œuvre de la norme PA-DSS* comprend une description de la méthodologie de gestion des versions publiées par le fournisseur pour les clients et les intégrateurs/revendeurs, et que cette description comprend ce qui suit : • Les détails du système de version, y compris son format (nombre d'éléments, séparations, ensembles de caractères, etc.). • Les détails de la manière avec laquelle les changements qui ont un impact sur la sécurité seront indiqués par le système de version. • Les détails de la manière avec laquelle les types de changement affecteront la version. • Les détails de tout élément de caractère générique utilisé, y compris la confirmation qu'il ne sera jamais utilisé pour représenter un changement ayant un impact sur la sécurité.	Assurer que la méthodologie de gestion des versions du fournisseur qui est incluse dans le *Guide de mise en œuvre de la norme PA-DSS* apportera aux clients et/ou aux intégrateurs/revendeurs les informations nécessaires pour comprendre quelle version de l'application de paiement ils utilisent, ainsi que les types de changement qui ont été apportés à chaque version de l'application de paiement.
5.4.5 Si un mappage interne de version est utilisé vers la gestion de la version publiée, la méthodologie de gestion des versions doit inclure le mappage des versions internes vers les versions externes.	**5.4.5.a** Examiner la méthodologie de gestion des versions documentée pour vérifier qu'elle comprend un mappage des versions internes vers les versions externes. **5.4.5.b** Examiner tous les changements récents pour confirmer que le mappage de version interne vers le système de version est mis à jour conformément au type de changement, comme défini dans la méthodologie documentée.	Certains fournisseurs d'application de paiement ont des méthodologies de gestion des versions pour utilisation interne ou pour référence, qui diffèrent de la méthodologie de gestion des versions utilisée pour les lancements externes (ou publics). Dans ces situations, il est important que les deux méthodologies de gestion des versions soient bien définies et documentées, de même que la relation entre elles.

Conditions de la norme PA-DSS	Procédures de test	Directive
5.4.6 Le fournisseur de logiciel doit avoir mis en place un processus pour vérifier la conformité des mises à jour de l'application avec la méthodologie de gestion des versions avant le lancement.	**5.4.6.a** Examiner les processus de développement de logiciel et la méthodologie de gestion des versions pour vérifier qu'un processus est mis en place pour examiner les mises à jour de l'application et vérifier leur conformité aux méthodologies de gestion des versions avant le lancement.	Il est essentiel que les fournisseurs d'application de paiement aient un processus en place pour garantir que les mises à jour de produit correspondent à l'objectif et à la portée du lancement prévu et que ces changements sont communiqués aux clients avec précision. Au cas contraire, des changements pourraient être apportés à une application qui a un impact négatif sur la sécurité de l'application du client sans qu'il le sache.
	5.4.6.b Interroger les développeurs de logiciel et observer les processus pour vérifier que les mises à jour de l'application sont conformes à la méthodologie de gestion des versions avant le lancement.	

Conditions de la norme PA-DSS	Procédures de test	Directive
5.5 Les techniques d'évaluation des risques (par exemple, la modélisation des risques à l'application) sont utilisés pour identifier les déficiences et les vulnérabilités potentielles de la conception de la sécurité de l'application pendant le processus de développement du logiciel. Les processus d'évaluation des risques doivent inclure ce qui suit : • La couverture de toutes les fonctions de l'application de paiement, comprenant, entre autres, les fonctionnalités ayant un impact sur la sécurité et les fonctionnalités qui dépassent les limites de confiance. • L'évaluation des points de décision de l'application, les flux de processus, le stockage des données et les limites de confiance. • L'identification de toutes les zones dans l'application de paiement qui interagissent avec le PAN et/ou le SAD, ou « l'environnement de données de titulaires de carte (CDE) », ainsi que de tout résultat orienté vers le processus susceptible de provoquer une exposition des données de titulaires de carte. • Une liste des menaces et des vulnérabilités potentielles résultant des analyses de flux de données de titulaires de carte et attribuer des notations de risque (par exemple : priorité élevée, moyenne ou faible) à chacun. • La mise en œuvre de mesures de correction et de contre-mesures appropriées pendant le processus de développement. • La documentation des résultats de l'évaluation de risque pour l'examen et l'approbation de la gestion.	**5.5** Examiner les procédures écrites de développement de logiciel et interroger le personnel responsable pour vérifier que le vendeur utilise des techniques d'évaluation des risques dans le cadre du processus de développement du logiciel et que les processus comprennent : • La couverture de toutes les fonctions de l'application de paiement, comprenant, entre autres, les fonctionnalités ayant un impact sur la sécurité et les fonctionnalités qui dépassent les limites de confiance. • L'évaluation des points de décision de l'application, les flux de processus, le stockage des données et les limites de confiance. • L'identification de toutes les zones dans l'application de paiement qui interagissent avec le PAN/SAD, ou l'environnement de données de titulaires de carte (CDE), ainsi que de tout résultat orienté vers le processus susceptible de provoquer une exposition des données de titulaires de carte. • Une liste des menaces et des vulnérabilités potentielles résultant des analyses de flux de données de titulaires de carte et affecter des notations de risque (par ex. : priorité élevée, moyenne ou faible) à chacun. • La mise en œuvre de mesures de correction et de contre-mesures appropriées pendant le processus de développement. • La documentation des résultats de l'évaluation de risque pour l'examen et l'approbation de la gestion.	Pour maintenir la qualité et la sécurité des applications de paiement, les techniques d'évaluation de risque doivent être utilisées par les fournisseurs d'application pendant le processus de développement de logiciel. La modélisation des risques est une forme d'évaluation des risques qui peut être utilisée pour analyser les constructions d'une application et les flux de données pour découvrir les possibilités que des informations confidentielles puissent être exposées aux applications d'utilisateurs non autorisées. Ces processus permettent aux développeurs et aux architectes de logiciel d'identifier et de résoudre les problèmes de sécurité potentiels dans le processus de développement, tout en améliorant la sécurité de l'application et en minimisant les coûts de développement.

Conditions de la norme PA-DSS	Procédures de test	Directive
5.6 Le fournisseur de logiciel doit mettre en œuvre un processus pour documenter et autoriser le lancement final de l'application ainsi que toute mise à jour de l'application. La documentation comprend : • La signature d'une partie autorisée à approuver formellement le lancement de l'application ou la mise à jour de l'application • La confirmation que des processus de développement sécurisés ont été développés par le fournisseur.	**5.6.a** Examiner les processus documentés pour vérifier que la version finale de l'application, ainsi que toute mise à jour de l'application, doit être formellement approuvée et documentée, comprendre une signature par une partie autorisée à approuver de manière formelle le lancement et la confirmation que tous les processus SDLC ont été respectés.	Quelqu'un de l'organisation du fournisseur de l'application de paiement doit être responsable des examens et s'assurer que tous les aspects du processus de développement (comme défini dans les conditions 5.1 à 5.5) ont été respectés. Sans examen formel et reconnaissance d'une partie responsable, les processus de sécurité critiques pourraient être manqués ou exclus, ayant pour résultat une application défectueuse ou moins sécurisée.
	5.6.b Pour consulter un échantillon des versions récentes d'application et des mises à jour d'application, consultez la documentation d'application pour vérifier qu'elle comprend : • L'approbation formelle et la signature d'une partie autorisée. • La confirmation que tous les processus de développement sécurisés ont été suivis.	

Condition 6 : Protéger les transmissions sans-fil

Conditions de la norme PA-DSS	Procédures de test	Directive
6.1 Pour les applications de paiement utilisant une technologie sans-fil, changer la configuration par défaut du fournisseur du dispositif sans-fil, y compris, sans s'y limiter, leurs clés de cryptage, mots de passe, et chaînes de communauté SNMP par défaut. La technologie sans-fil doit être mise en œuvre de manière sécurisée. ***Correspond aux conditions 1.2.3 et 2.1.1 de la norme PCI DSS***	**6.1** Pour les applications de paiement développées pour une utilisation avec la technologie sans-fil, ainsi que pour toutes les applications sans-fil groupées avec l'application de paiement, vérifier que les applications sans-fil n'utilisent pas les paramètres par défaut du vendeur comme suit : **6.1.a** Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier qu'il comprend les instructions suivantes pour les clients et les intégrateurs/revendeurs : • Les applications de paiement appliquent des changements de clés de cryptage par défaut, de mots de passe et de chaînes de communauté SNMP, lors de l'installation de tous les composants sans-fil contrôlés par l'application. • Les procédures de changement de clés de cryptage et de mot de passe de réseau sans-fil, y compris les chaînes SNMP, dès lors que quelqu'un qui connaît les clés/mots de passe quitte la société ou change de poste. • Les instructions relatives au changement de clés de cryptage par défaut, de mots de passe et de chaînes de communauté SNMP de n'importe quel composant sont fournies par l'application de paiement, mais elles ne sont pas sous son contrôle. • Les instructions relatives à l'installation d'un pare-feu entre tous les réseaux sans-fil et les systèmes qui stockent les données de titulaires de carte. • Les détails de tout trafic sur le réseau sans-fil (y compris les informations portant sur le port spécifique) que la fonction sans-fil de l'application de paiement pourrait utiliser. • Les instructions relatives à la configuration des pare-feu pour qu'ils refusent ce trafic si nécessaire pour des raisons commerciales - pour permettre uniquement au trafic autorisé de circuler entre l'environnement du réseau sans-fil et l'environnement des données de titulaires de carte.	L'exploitation de la technologie sans-fil est une méthode fréquemment utilisée par les individus malveillants pour accéder au réseau et aux données de titulaires de carte. Si les réseaux sans-fil ne sont pas déployés avec une sécurité suffisante (y compris par la modification des paramètres par défaut), des renifleurs sans-fil peuvent intercepter le trafic, capturer facilement des données et des mots de passe et pénétrer sans difficulté le réseau pour l'attaquer. Pour ces raisons, les applications de paiement ne doivent pas nécessiter l'utilisation de paramètres de réseau sans-fil par défaut ou non sécurisés. Si les pare-feu ne restreignent pas l'accès des réseaux sans-fil dans le CDE, les individus malveillants qui accèdent au réseau sans-fil sans autorisation peuvent facilement se connecter au CDE et compromettre les informations de comptes.

Conditions de la norme PA-DSS	Procédures de test	Directive
	6.1.b Installer l'application selon le *Guide de mise en œuvre de la norme PA-DSS* et tester l'application et les paramètres du réseau sans-fil pour vérifier les points suivants, pour toutes les fonctionnalités sans-fil gérées par l'application de paiement : • Les clés de cryptage ont été modifiées depuis le réglage par défaut de l'installation. • Les chaînes de communauté SNMP par défaut sur les périphériques sans-fil ont été modifiées à l'installation. • Les mots/phrases de passe par défaut des points d'accès ont été modifiés à l'installation. • Le firmware des périphériques sans-fil est mis à jour de manière à prendre en charge un cryptage robuste pour l'authentification et la transmission sur les réseaux sans-fil. • Les autres paramètres par défaut liés à la sécurité, définis par le fournisseur des équipements sans-fil, ont été changés, le cas échéant.	
	6.1.c Pour toutes les fonctionnalités sans-fil gérées par l'application de paiement, suivre les instructions du *Guide de mise en œuvre de la norme PA-DSS* pour changer les clés de cryptage du réseau sans-fil, les mots/phrases de passe et les chaînes SNMP. Vérifier que les instructions du *Guide de mise en œuvre de la norme PA-DSS* sont précises et donnent lieu au changement des clés de cryptage sans-fil, mots de passe et chaînes SNMP.	
	6.1.d Pour tous les composants sans-fil fournis avec l'application, mais non gérés par l'application de paiement, suivre les instructions du *Guide de mise en œuvre de la norme PA-DSS* pour changer les clés de cryptage par défaut du réseau sans-fil, les mots/phrases de passe et les chaînes de communauté SNMP. Vérifier que les instructions du *Guide de mise en œuvre de la norme PA-DSS* sont précises et donnent lieu au changement des clés de cryptage sans-fil, mots de passe et chaînes SNMP.	

Conditions de la norme PA-DSS	Procédures de test	Directive
	6.1.e Installer l'application et tester les fonctions sans-fil pour vérifier que le trafic sur le réseau sans-fil et les ports utilisés par l'application respectent les critères documentés dans le *Guide de mise en œuvre de la norme PA-DSS*.	
6.2 Pour les applications de paiement utilisant la technologie sans-fil, l'application de paiement doit permettre de mettre en œuvre les meilleures pratiques du secteur (par exemple, IEEE 802.11i) afin d'appliquer un cryptage robuste pour l'authentification et la transmission. ***Remarque :*** *L'utilisation du protocole WEP comme contrôle de sécurité est interdite.* ***Correspond à la condition 4.1.1 de la norme PCI DSS***	**6.2.a** Pour les applications de paiement développées pour une utilisation avec la technologie sans-fil, tester toutes les fonctionnalités sans-fil pour vérifier que l'application utilise les meilleures pratiques du secteur (par exemple, IEEE 802.11.i) pour donner un cryptage robuste pour l'authentification et la transmission.	Les utilisateurs malveillants emploient des outils gratuits et largement répandus pour écouter les communications sans-fil. L'utilisation d'une cryptographie robuste peut aider à limiter la divulgation d'informations sensibles sur les réseaux sans-fil. Une cryptographie robuste pour l'authentification et la transmission des données de titulaires de carte est obligatoire pour empêcher les utilisateurs malveillants d'accéder aux données sur un réseau sans-fil, ou d'utiliser les réseaux sans-fil pour accéder à d'autres données ou systèmes.
	6.2.b Pour les applications sans-fil groupées avec l'application de paiement, tester la fonctionnalité sans-fil pour vérifier que les meilleures pratiques du secteur (par exemple IEEE 802.11.i) sont utilisées pour donner un cryptage robuste à l'authentification et à la transmission.	
	6.2.c Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier qu'il comprend les instructions suivantes pour les clients et les intégrateurs/revendeurs : • Comment configurer l'application pour utiliser les meilleures pratiques du secteur (par exemple, IEEE 802.11i) pour appliquer un cryptage robuste à l'authentification et la transmission et/ou • Comment configurer toutes les applications sans-fil groupées avec l'application de paiement pour utiliser les meilleures pratiques du secteur pour l'authentification et la transmission.	

Conditions de la norme PA-DSS	Procédures de test	Directive
6.3 Donner des instructions au client concernant l'utilisation sécurisée de la technologie sans-fil, ***Remarque :*** *Cette condition s'applique à toutes les applications de paiement, que l'application soit ou non développée pour être utilisée avec les technologies sans-fil.* **Correspond aux conditions *1.2.3, 2.1.1 et 4.1.1 de la norme PCI DSS***	**6.3** Examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur pour vérifier que les clients et les revendeurs/intégrateurs ont été informés des paramètres sans fil compatibles avec PCI DSS : • Instructions relatives au changement des clés de cryptage, mots de passe et les chaînes de communauté SNMP par défaut à l'installation. • Instructions relatives au changement de clés de cryptage, mots de passe et chaînes SNMP, dès lors que quelqu'un qui connaît les clés/mots de passe quitte la société ou change de poste. • Les instructions relatives à l'installation d'un pare-feu entre les réseaux sans-fil et les systèmes qui conservent les données de titulaires de carte ; et à la configuration des pare-feu pour qu'ils refusent ce trafic si nécessaire pour des raisons commerciales ou pour permettre uniquement au trafic autorisé de circuler entre l'environnement du réseau sans-fil et l'environnement des données de titulaires de carte. • Les instructions relatives à l'utilisation des meilleures pratiques du secteur (par exemple, IEEE 802.11i) pour appliquer un cryptage robuste à l'authentification et la transmission.	Les fournisseurs d'application de paiement devront fournir des instructions aux clients pour la configuration de l'application pour qu'elle prenne en charge l'utilisation des technologies sans-fil, même si l'application n'est pas explicitement conçue pour une utilisation dans un environnement sans-fil. Les réseaux sans-fil sont fréquents et les clients doivent être informés des paramètres de sécurité des réseaux sans-fil qui doivent être mis en œuvre pour assurer la sécurité de l'application de paiement.

Condition 7 : Tester les applications de paiement pour gérer les vulnérabilités et maintenir leurs mises à jour

Conditions de la norme PA-DSS	Procédures de test	Directive
7.1 Les fournisseurs de logiciel doivent établir un processus afin d'identifier et de gérer les vulnérabilités comme suit : ***Remarque :*** *Tout logiciel ou système sous-jacent fourni avec, ou requis par, l'application de paiement (par exemple, des serveurs Web, bibliothèques de tiers et programmes) doit être inclus dans ce processus.* ***Correspond à la condition 6.1 de la norme PCI DSS***	**7.1.a** Examiner la documentation du processus de gestion de la vulnérabilité pour vérifier que les procédures sont définies pour : • Identifier les nouvelles vulnérabilités de sécurité en utilisant des sources de bonne réputation pour obtenir les informations concernant la vulnérabilité de la sécurité. • Attribuer un classement du risque de toutes les vulnérabilités identifiées. • Tester les applications de paiement et les mises à jour pour la présence de vulnérabilité avant le lancement.	Les fournisseurs doivent demeurer informés des nouvelles vulnérabilités susceptibles d'avoir un impact sur leurs applications, y compris les vulnérabilités des composants sous-jacents ou des logiciels groupés à l'application ou requis par l'application. Les vendeurs d'application de paiement informés des vulnérabilités dans leurs propres applications ou dans les composants sous-jacents doivent ensuite être à même de résoudre ces vulnérabilités avant le lancement, ou de mettre en œuvre d'autres mécanismes pour réduire la possibilité que la vulnérabilité ne soit exploitée au cas où un correctif de sécurité tiers ne soit pas immédiatement disponible.
	7.1.b Vérifier que les processus d'identification des nouvelles vulnérabilités et de mise en œuvre des corrections dans l'application de paiement sont appliqués à tous les logiciels fournis avec ou requis par l'application de paiement (par exemple, des serveurs Web, des bibliothèques tierces et des programmes).	
7.1.1 Identifier les nouvelles vulnérabilités de sécurité en utilisant des sources de bonne réputation pour obtenir les informations concernant la vulnérabilité de la sécurité.	**7.1.1** Interroger le personnel responsable et examiner les processus afin de vérifier que les nouvelles vulnérabilités de la sécurité sont identifiées : • Dans l'application de paiement comme dans tous logiciel ou système sous-jacent fourni avec l'application de paiement ou requis par celle-ci. • L'utilisation de sources de bonne réputation (telles que des sites Web de fournisseur de systèmes/logiciels, les sites Web de NVD de NIST, CVE de MITRE, et US-CERT de DHS).	Des sources de bonne réputation doivent être utilisées pour obtenir des informations concernant la vulnérabilité et/ou des correctifs des composants de logiciels tiers. Les sources d'informations concernant la vulnérabilité doivent être fiables et elles comprennent souvent les sites Web des fournisseurs, les groupes d'information du secteur, les listes de diffusion ou les flux RSS. Les exemples de sources du secteur comprennent la base de données des vulnérabilités nationales de NIST, la liste des vulnérabilités et expositions courantes de MITRE et les sites Web US-CERT du département de la sûreté nationale américaine.

Conditions de la norme PA-DSS	Procédures de test	Directive
7.1.2 Attribuer un classement de risque à toutes les vulnérabilités identifiées, y compris les vulnérabilités qui impliquent un logiciel ou des systèmes sous-jacents fournis avec l'application de paiement ou requise par celle-ci. ***Remarque :*** *Le classement des risques doit se baser sur les meilleures pratiques du secteur, ainsi que sur la prise en compte de l'impact potentiel. Par exemple, les critères de classement des vulnérabilités peuvent inclure la prise en compte du score de base CVSS et/ou la classification par le fournisseur, et/ou l'impact sur la fonctionnalité de l'application.* *Le classement de risque doit, au minimum, identifier toutes les vulnérabilités considérées comme un « risque élevé » pour l'application. En plus du classement de risque, les vulnérabilités peuvent être considérées comme « critiques » si elles posent une menace imminente, ont un impact critique sur les composants de l'application ou si elles sont susceptibles de compromettre l'application si elles ne sont pas résolues.*	**7.1.2** Interroger le personnel responsable et observer les processus pour vérifier que les nouvelles vulnérabilités se voient attribuer un classement de risque, y compris les vulnérabilités impliquant un logiciel ou système sous-jacent fourni par l'application de paiement ou requis par celle-ci.	Une fois que le fournisseur identifie une vulnérabilité qui pourrait affecter son application, il lui faut évaluer et classer le risque que pose cette vulnérabilité. Cette opération requiert un processus de surveillance active des sources de l'industrie afin de découvrir des informations concernant la vulnérabilité. Établir un classement des risques (par exemple, « élevé », « moyen » et « faible ») permet aux fournisseurs d'identifier et de répondre plus rapidement aux éléments de risque de priorité élevée (par exemple, en lançant des correctifs de haute priorité plus rapidement) et de réduire la probabilité que les vulnérabilités impliquant les risques les plus élevés soient exploitées.
7.1.3 Tester les applications de paiement et les mises à jour pour la présence de vulnérabilité avant le lancement	**7.1.3** Interroger le personnel responsable et observer les processus pour vérifier que les applications de paiement sont testées pour la présence de vulnérabilités avant leur lancement.	Des tests adéquats doivent être inclus dans tous processus de gestion des vulnérabilités de l'application de paiement du fournisseur afin d'assurer que les vulnérabilités identifiées ont été correctement traitées avant le lancement. *Les exemples de méthodes de test pourraient inclure les tests de pénétration et/ou des techniques de test flou pour identifier les vulnérabilités potentielles - par exemple en injectant des données mal formées ou inattendues, ou en modifiant la taille en octet des données.*

Conditions de la norme PA-DSS	Procédures de test	Directive
7.2 Les fournisseurs de logiciel doivent établir un processus de développement et de déploiement rapide des correctifs de sécurité et des mises à jour des logiciels.	**7.2** Examiner la documentation des processus pour connaître le développement et la distribution des correctifs et des mises à jour pour vérifier que le processus comprend les procédures 7.2.1 à 7.2.2 :	Les mises jour de logiciel pour répondre aux vulnérabilités de sécurité doivent être développées et communiquées aux clients dès que possible une fois qu'une vulnérabilité critique a été identifiée, afin de minimiser le calendrier et la possibilité d'exploitation de la vulnérabilité.
7.2.1 Les correctifs et les mises à jour sont délivrés aux clients de manière sécurisée, avec une chaîne de confiance connue.	**7.2.1** Interroger le personnel responsable et observer les processus pour vérifier que les correctifs et les mises à jour sont délivrés aux clients de manière sécurisée, avec une chaîne de confiance connue.	Les correctifs de sécurité doivent être distribués d'une manière qui empêche les individus malveillants d'intercepter les mises à jour en transit, de les modifier et de les redistribuer aux clients sans méfiance.
7.2.2 Les correctifs et les mises à jour sont délivrés au client d'une manière qui garantit l'intégrité du correctif et du code de mise à jour.	**7.2.2.a** Interroger le personnel responsable et observer les processus pour vérifier que les correctifs et les mises à jour sont délivrés au client d'une manière qui garantit l'intégrité du correctif et du code de mise à jour.	Les correctifs de sécurité doivent inclure un mécanisme dans le processus de mise à jour pour vérifier que le code de mise à jour n'a pas été remplacé ou altéré. Les exemples de vérifications comprennent, mais ne sont pas limités aux sommes de contrôles, aux certificats à signature numérique, etc.
	7.2.2.d Interroger le personnel responsable et observer les processus de mise à jour de l'application pour vérifier que les correctifs et mises à jour sont testés du point de vue de l'intégrité sur le système cible, avant l'installation.	
	7.2.2.c Vérifier que l'intégrité du correctif et du code de mise à jour est préservée, en appliquant le processus de mise à jour avec un code arbitraire et en s'assurant que le système ne permettra pas à la mise à jour de s'exécuter.	
7.2.3 Donner des instructions aux clients concernant l'installation sécurisée des correctifs et des mises à jour.	**7.2.3** Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier qu'il comprend les instructions suivantes pour les clients et les intégrateurs/revendeurs : • la communication des nouveaux correctifs et mises à jour au fournisseur ; • la mise à disposition sécurisée des correctifs et des mises à jour avec une chaîne de confiance connue ; • le mode d'accès aux correctifs et aux mises à jour, ainsi que leur mode d'installation de manière à assurer l'intégrité des codes correspondants.	Informer les clients et les intégrateurs/revendeurs du mode de réception et d'installation des correctifs de manière sécurisée permet de protéger l'intégrité du processus de mise à jour et l'application.

Conditions de la norme PA-DSS	Procédures de test	Directive
7.3 Inclure des notes de lancement pour les mises à jour de l'application, y compris les détails et l'impact de la mise à jour et comment le numéro de version a été changé pour illustrer la mise à jour de l'application.	**7.3.a** Examiner les processus de lancement pour les mises à jour et interroger le personnel pour vérifier que les notes de lancement sont préparées pour toutes les mises à jour, y compris les détails et l'impact de la mise à jour et comment le numéro de version a été changé pour illustrer la mise à jour de l'application.	Les notes de lancement donnent aux clients des détails sur les mises à jour du logiciel, y compris les fichiers qui ont été changés, les fonctionnalités de l'application qui ont été modifiées, ainsi que les fonctions de sécurité qui sont susceptibles d'être affectées. Les notes de lancement doivent aussi indiquer comment un correctif particulier ou une mise à jour affecte le numéro de version global associé au lancement de correctif.
	7.3.b Examiner les notes de lancement pour un échantillon de mises à jour d'application et vérifier qu'elles en tiennent compte.	

Condition 8 : Permettre la mise en œuvre de réseaux sécurisés

Conditions de la norme PA-DSS	Procédures de test	Directive
8.1 L'application de paiement doit pouvoir être mise en œuvre dans un environnement réseau sécurisé. Les applications ne doivent pas interférer avec l'utilisation des périphériques, des applications ou des configurations requises pour la conformité à la norme PCI DSS. *Par exemple, l'application ne peut pas interférer avec l'utilisation de correctifs, de protection contre les logiciels malveillants, les configurations de pare-feu ou tout autre périphérique, ou configuration requise pour la conformité à la norme PCI DSS.* ***Correspond aux conditions 1, 3, 4, 5 et 6 de la norme PCI DSS***	**8.1.a** Installer l'application dans un environnement de laboratoire conforme à la norme PCI DSS selon le *Guide de mise en œuvre de la norme PA-DSS.* Tester l'application de paiement pour obtenir des preuves qu'elle peut fonctionner dans un réseau pleinement conforme à la norme PCI DSS. **8.1.b** Tester l'application et les systèmes sous-jacents pour vérifier que l'application de paiement sans exclure ou perturber les fonctions PCI DSS sur les systèmes sous-jacents — par exemple, l'application ne gène pas l'installation de correctifs ou de mises à jour de protection contre les logiciels malveillants, ou ne perturbe pas le fonctionnement des autres fonctions PCI DSS.	Les applications de paiement doivent être conçues et développées de telle sorte que l'installation et le fonctionnement de l'application n'empêchent pas une organisation d'implémenter les autres contrôles requis pour la conformité à la norme PCI DSS. Par exemple, l'application de paiement doit pouvoir fonctionner dans un environnement qui utilise des solutions anti-virus (par exemple, elle n'a pas besoin que ces anti-virus soient désactivés ou désinstallés).
8.2 L'application de paiement doit uniquement utiliser ou exiger l'utilisation de services, protocoles, démons, composants, et matériel et logiciel dépendants, nécessaires et sécurisés, y compris ceux fournis par des tiers, pour toute fonctionnalité de l'application de paiement. *Remarque : Le SSL ou le TLS initial ne sont pas considérés comme étant une cryptographie robuste. Les applications de paiement ne doivent ni utiliser ni prendre en charge le SSL ou le TLS initial. Les applications qui utilisent ou prennent en charge le TLS ne doivent pas autoriser un repli sur le SSL.* ***Correspond à la condition 2.2.3 de la norme PCI DSS***	**8.2.a** Examiner les services de système, les protocoles, les démons, les composants, et le matériel et logiciel dépendants, activés ou exigés par l'application de paiement. Vérifier que seuls les services, protocoles, démons, composants, matériel et logiciel dépendants, nécessaires et sécurisés, sont activés « prêts à l'emploi » par défaut. **8.2.b** Installer l'application et tester les fonctions de l'application pour vérifier que, si l'application prend en charge tous services, démons, protocoles ou composants non sécurisés, ils sont configurés de manière sécurisée « prêts à l'emploi » par défaut. **8.2.c** Vérifier que le *Guide de mise en œuvre de la norme PA-DSS* documente tous les protocoles, services, composants, et matériel et logiciel dépendants nécessaires pour une fonctionnalité de l'application de paiement, y compris ceux fournis par des tiers.	Une entreprise peut avoir besoin de nombreux protocoles (ou les avoir activés par défaut) qui sont fréquemment utilisés par les individus malveillants pour endommager un réseau ou un système. L'application de paiement ne doit pas requérir l'utilisation d'un protocole, service, démon, etc. non sécurisé. Si l'application ne prend pas en charge l'utilisation de services, démons, protocoles ou composants non sécurisés, ils doivent être sécurisés par défaut.

Conditions de la norme PA-DSS	Procédures de test	Directive
8.3 L'application de paiement ne doit pas exiger l'utilisation de services ou de protocoles qui entravent ou interfèrent avec le fonctionnement normal des technologies d'authentification à plusieurs facteurs. ***Remarque :*** *L'authentification à plusieurs facteurs exige d'utiliser au moins deux des trois méthodes d'authentification (voir ci-dessous). L'utilisation à deux reprises d'un facteur (par exemple, l'utilisation de deux mots de passe distincts) ne constitue pas une authentification à plusieurs facteurs. Les méthodes d'authentification, également connues comme facteurs, sont :* • Quelque chose de connu du seul utilisateur, comme un mot de passe ou une locution de passage ; • Quelque chose de détenu par l'utilisateur, comme un dispositif de jeton ou une carte à puce ; • Quelque chose concernant l'utilisateur, comme une mesure biométrique. ***Correspond à la condition 8.3 de la norme PCI DSS***	**8.3.a** Examiner la fonctionnalité de l'application de paiement pour vérifier qu'elle ne requiert pas l'utilisation d'un service ou protocole qui entrave ou interfère avec le fonctionnement normal de la technologie d'authentification à plusieurs facteurs. **8.3.b** Identifier les mécanismes d'accès à distance pris en charge par l'application et vérifier que les mécanismes n'empêchent pas l'authentification à plusieurs facteurs.	Les applications de paiement doivent être conçues et développées de telle sorte que l'installation et le fonctionnement de l'application ne requièrent pas d'une organisation qu'elle utilise des services ou protocoles qui l'empêcheraient de mettre en œuvre des solutions d'authentification à plusieurs facteurs pour un accès sécurisé. Par exemple, l'application ne doit pas, par défaut, utiliser le port 1812 (qui est globalement connu pour son affectation à RADIUS par RFC 2865) si RADIUS doit être une technologie d'authentification et d'autorisation prise en charge. *Les exemples de technologies à plusieurs facteurs comprennent, mais sans s'y limiter, les technologies RADIUS avec jetons et les technologies TACAS avec jetons, ou autres technologies facilitant l'authentification à plusieurs facteurs.*

Condition 9 : Les données de titulaires de carte ne doivent jamais être stockées sur un serveur connecté à Internet

Conditions de la norme PA-DSS	Procédures de test	Directive
9.1 L'application de paiement doit être développée de façon à ce que tout serveur Internet et tout composant de stockage de données de titulaires de carte (par exemple, un serveur de base de données) ne doivent pas se situer sur le même serveur et que le composant de stockage de données ne doive pas se situer dans la même zone du réseau (comme un DMZ) dans le serveur Web. ***Correspond à la condition 1.3.7 de la norme PCI DSS***	**9.1.a** Identifier tous les composants de stockage de données de l'application (par exemple, les bases de données) et tous les serveurs internet. Installer les composants de stockage de données et les serveurs Web sur des serveurs différents et tester la fonctionnalité de l'application sur les différents serveurs. Vérifier que l'application de paiement ne requiert pas que les composants de stockage (tels que la base de données) soient installés sur le même serveur qu'un serveur Web pour fonctionner.	Tout composant de serveur Web d'une application de paiement se trouve à un risque substantiellement plus élevé d'être compromis, étant donnée la nature ouverte des réseaux publics (Internet, réseau sans-fil public, etc.), la nature et le volume des attaques pouvant provenir de ces réseaux. Les composants de stockage de données de titulaires de carte doivent bénéficier d'un niveau de protection plus élevé que les composants d'application destinés au public. Si les données de titulaires de carte se trouvent dans la DMZ, il est plus facile pour les pirates externes d'accéder à ces informations, puisqu'il y a moins de couches à pénétrer. Pour la même raison, les serveurs Web ne
	9.1.b Installer les composants de stockage des données et les serveurs Web dans des zones différentes du réseau. Tester toutes les fonctions de l'application sur les zones du réseau pour vérifier que l'application de paiement ne requiert pas que les composants de stockage des données (tels que la base de données) soient installés sur la même zone du réseau qu'un serveur Web pour fonctionner.	

	9.1.c Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier qu'il comprend les instructions suivantes pour les clients et les intégrateurs/revendeurs : • Des instructions stipulant de ne pas stocker de données de titulaires de carte sur les systèmes destinés au public (par exemple, un serveur Web et un serveur de base de données ne doivent pas se trouver sur le même serveur). • Des instructions expliquant comment configurer l'application de paiement pour utiliser une DMZ pour séparer Internet des systèmes qui stockent les données de titulaires de carte (par exemple, installer un composant de serveur Web dans une DMZ et installer un composant de stockage de données sur une zone interne différente du réseau). • Une liste des services/ports que l'application a besoin d'utiliser afin de communiquer sur les deux zones du réseau (afin que le client puisse configurer son pare-feu pour ouvrir uniquement les ports requis).	doivent jamais être stocké sur le même serveur que les composants de stockage des données. Si un individu malveillant pouvait compromettre un compte sur le serveur Web, il pourrait également compromettre la base de données des données de titulaires de carte sans aucun effort supplémentaire.

Condition 10 : Faciliter l'accès à distance sécurisée à l'application de paiement

Conditions de la norme PA-DSS	Procédures de test	Directive
10.1 L'authentification à plusieurs facteurs doit être utilisée pour tous les accès à distance à l'application de paiement, provenant de l'extérieur de l'environnement client. ***Remarque :*** *L'authentification à plusieurs facteurs requiert d'utiliser au moins deux des trois méthodes d'authentification (voir la condition 3.1.4 de la norme PA-DSS pour la description des méthodes d'authentification).* **Correspond à la *condition 8.3 de la norme PCI DSS*** **10.1.a** Consulter le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier qu'il comprend les instructions suivantes pour les clients et les intégrateurs/revendeurs : • Des instructions stipulant que tous les accès à distance issus de l'extérieur du réseau du client vers l'application de paiement doivent utiliser l'authentification à plusieurs facteurs pour respecter les conditions de la norme PCI DSS. • Une description des mécanismes d'authentification à plusieurs facteurs pris en charge par l'application. • Des instructions expliquant la configuration de l'application pour prendre en charge l'authentification à plusieurs facteurs (au moins deux des trois méthodes d'authentification décrites à la condition 3.1.4 de la norme PA DSS).	L'authentification à plusieurs facteurs requiert au moins deux méthodes d'authentification pour les accès provenant de l'extérieur du réseau. Les fournisseurs d'application de paiement devront fournir des instructions aux clients pour la configuration de l'application pour qu'elle prenne en charge les mécanismes spécifiés d'authentification à plusieurs facteurs, afin d'assurer que ces mécanismes puissent être implémentés correctement et respecter les conditions applicables de la norme PCI DSS. La condition d'authentification à plusieurs facteurs doit s'appliquer à tout le personnel doté d'un accès à distance qui provient de l'extérieur de l'environnement client.
	10.1.b Si le fournisseur de l'application a un accès à distance à une application de paiement qui provient de l'extérieur de l'environnement du client, examiner les politiques du fournisseur pour vérifier que le fournisseur prend en charge les conditions des clients pour l'authentification à plusieurs facteurs pour cet accès.	
10.2 Tout accès à distance à l'application de paiement doit se faire de manière sécurisée, comme suit :	**10.2** Vérifier que tout accès à distance est exécuté comme suit :	Tout mécanisme d'accès à distance employé par le fournisseur de l'application de paiement et/ou les intégrateurs/revendeurs -

Conditions de la norme PA-DSS	Procédures de test	Directive
10.2.1 Si les mises à jour de l'application de paiement sont délivrées par un accès distant aux systèmes des clients, les fournisseurs de logiciels doivent indiquer aux clients d'activer les technologies d'accès à distance uniquement lorsque c'est indispensable pour effectuer les téléchargements provenant du fournisseur et de les désactiver immédiatement après le téléchargement. Sinon, en cas de livraison par réseau privé virtuel (VPN) ou autre connexion haut débit, les fournisseurs de logiciels doivent recommander aux clients de configurer correctement un pare-feu ou un produit pare-feu personnel pour sécuriser les connexions « permanentes ». ***Correspond aux conditions 1 et 12.3.9 de la norme PCI DSS***	**10.2.1.a** Si les mises à jour de l'application de paiement sont livrées par un accès distant aux systèmes du client, examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur pour vérifier qu'il contient : • Les instructions pour les clients et revendeurs/intégrateurs concernant l'utilisation sécurisée des technologies d'accès à distance, précisant que ces technologies utilisées par les fournisseurs et partenaires commerciaux ne doivent être activées que lorsqu'ils en ont besoin et être désactivées immédiatement après utilisation. • La recommandation pour les clients et revendeurs/intégrateurs d'utiliser un pare-feu ou un produit pare-feu personnel si l'ordinateur est connecté par VPN ou autre connexion haut débit, afin de sécuriser les connexions permanentes conformément à la condition 1 de la norme PCI DSS.	par exemple pour prendre en charge les services fournis par ces prestataires - doit prendre en charge toutes les conditions applicables de la norme PCI DSS.
	10.2.1.b Si le fournisseur livre l'application de paiement et/ou les mises à jour par un accès distant sur les réseaux du client, observer les méthodes du fournisseur pour la livraison de l'application de paiement et/ou des mises à jour par accès distant aux réseaux de clients et vérifier que la méthode du vendeur comprend : • L'activation des technologies d'accès à distance pour les réseaux de client strictement lorsque cela est nécessaire et la désactivation immédiate après usage. • Si un accès à distance est effectué par VPN ou autre connexion haut débit, la connexion sera sécurisée selon la condition 1 de la norme PCI DSS.	

Conditions de la norme PA-DSS	Procédures de test	Directive
10.2.2 Si les fournisseurs ou les intégrateurs/revendeurs peuvent accéder à distance aux applications de paiement des clients, un justificatif d'authentification unique (comme un mot de passe/une locution de passage) doit être utilisé pour chaque client. ***Correspond à la condition 8.5.1 de la norme PCI DSS***	**10.2.2** Si les fournisseurs ou les intégrateurs/revendeurs peuvent accéder à distance aux applications de paiement des clients, examiner les processus du fournisseur et interroger le personnel pour vérifier qu'un élément d'authentification unique (comme un mot de passe/une locution de passage) est utilisé pour chaque client auquel ils ont accès.	Pour empêcher que de multiples environnements de client soient compromis en utilisant un seul ensemble de justificatifs, les fournisseurs ayant des comptes d'accès à distance aux environnements de client doivent utiliser un justificatif d'authentification différent pour chaque client. Éviter d'utiliser des formules pouvant se répéter pour générer des mots de passe faciles à deviner. Ces mots de passe sont facilement découverts avec le temps et ils peuvent être utilisés par des individus non autorisés pour compromettre les clients du fournisseur.

Conditions de la norme PA-DSS	Procédures de test	Directive
10.2.3 L'accès à distance des fournisseurs, intégrateurs/revendeurs ou clients aux applications de paiement des clients doit être mis en œuvre de manière sécurisée, par exemple : • Modifier les paramètres par défaut dans le logiciel d'accès distant (par exemple, modifier les mots de passe par défaut et utiliser des mots de passe uniques pour chaque client). • Autoriser les connexions uniquement depuis des adresses IP/MAC connues. • Utiliser une authentification robuste et des mots de passe complexes pour les connexions (voir les conditions 3.1.1 à 3.1.11 de la norme PA-DSS). • Activer la transmission de données cryptées conformément à la condition 12.1 de la norme PA-DSS. • Activer le verrouillage de compte après un certain nombre de tentatives de connexion infructueuses. (Voir les conditions 3.1.9 à 3.1.10 de la norme PA-DSS.) • Établir une connexion VPN par pare-feu avant que l'accès ne soit autorisé. • Activer la fonction de journalisation. • Limiter l'accès aux environnements de client au personnel autorisé des revendeurs/intégrateurs. ***Correspond aux conditions 2, 8 et 10 de la norme PCI DSS***	**10.2.3.a** Examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que les clients et revendeurs/intégrateurs sont informés que tous les accès à distance à l'application de paiement doivent être implémentés de manière sécuritaire, par exemple : • Modifier les paramètres par défaut dans le logiciel d'accès distant (par exemple, modifier les mots de passe par défaut et utiliser des mots de passe uniques pour chaque client). • Autoriser les connexions uniquement depuis des adresses IP/MAC connues. • Utiliser une authentification robuste et des mots de passe complexes pour les connexions (voir les conditions 3.1.1 à 3.1.11 de la norme PA-DSS). • Activer la transmission de données cryptées conformément à la condition 12.1 de la norme PA-DSS. • Activer le verrouillage de compte après un certain nombre de tentatives de connexion infructueuses. (Voir les conditions 3.1.9 à 3.1.10 de la norme PA-DSS.) • Établir une connexion VPN par pare-feu avant que l'accès ne soit autorisé. • Activer la fonction de journalisation. • Limiter l'accès aux environnements de client au personnel autorisé. **10.2.3.b** Si le fournisseur de logiciel peut accéder à distance aux applications de paiement du client, observer les méthodes d'accès à distance du fournisseur et interroger le personnel pour vérifier que l'accès à distance est mis en œuvre de manière sécurisée	Les fournisseurs d'application de paiement devront fournir des instructions aux clients et aux intégrateurs/revendeurs pour la configuration de l'application afin de prendre en compte l'accès à distance sécurisé afin de garantir que ces mécanismes peuvent être mis en œuvre correctement et respecter les conditions de la norme PCI DSS. Cette condition s'applique à tous les types d'accès à distance utilisés pour accéder à l'environnement du client.

Condition 11 : Crypter le trafic sensible transitant par les réseaux publics

Conditions de la norme PA-DSS	Procédures de test	Directive
11.1 Si l'application de paiement envoie ou permet d'envoyer des données de titulaire de carte via des réseaux publics, l'application de paiement doit prendre en charge l'utilisation d'une cryptographie et de protocoles de sécurité forts pour protéger les données de titulaire de carte pendant la transmission sur les réseaux publics ouverts, y compris ce qui suit au minimum : • Seuls des clés et certificats approuvés sont acceptés. • Le protocole utilisé prend uniquement en charge les versions ou configurations sécurisées. • La force du cryptage est appropriée pour la méthodologie de cryptage employée. ***Remarque :*** *Le SSL ou le TLS initial ne sont pas considérés comme étant une cryptographie robuste. Les applications de paiement ne doivent ni utiliser ni prendre en charge le SSL ou le TLS initial. Les applications qui utilisent ou prennent en charge le TLS ne doivent pas autoriser un repli sur le SSL* *Voici quelques exemples, parmi d'autres, de réseaux publics ouverts :* • Internet • Les technologies sans-fil, comprenant, entre	**11.1.a** Si l'application de paiement envoie, ou permet l'envoi, de données de titulaires de carte par des réseaux publics, vérifier qu'une cryptographie et des protocoles de sécurité robustes sont fournis, ou que l'utilisation de ceux-ci est spécifiée. **11.1.b** Examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que le fournisseur inclut des instructions pour les clients et revendeurs/intégrateurs afin qu'ils utilisent une cryptographie et des protocoles de sécurité robustes, fournis ou spécifiés pour l'utilisation avec l'application, y compris : • Des instructions selon lesquelles une cryptographie et des protocoles de sécurité robustes doivent être utilisés si les données de titulaires de carte sont transmises sur des réseaux publics. • Des instructions pour vérifier que seuls des clés/certificats approuvés sont acceptés. • Comment configurer l'application de paiement pour utiliser uniquement des versions sécurisées et des mises en œuvre sécurisées des protocoles de sécurité. • Comment configurer l'application de paiement pour empêcher le repli sur une version ou une configuration non sécurisée (par exemple, si le TLS est utilisé, l'application ne doit pas autoriser le repli sur SSL). • Comment configurer l'application de paiement pour utiliser un cryptage de force adéquate pour la méthodologie de cryptage utilisée.	Dans la mesure où il est facile et courant qu'un individu malveillant intercepte et/ou détourne des données au cours du transit, les informations sensibles doivent être cryptées pendant la transmission sur les réseaux publics. La transmission sécurisée des données de titulaires de carte nécessite des clés/certificats fiables, un protocole sécurisé pour le transport et un cryptage d'une force suffisante pour le codage des données de titulaires de carte. Noter que l'implémentation de certains protocoles (comme SSL, SSH version 1.0 et TLS initial) a des vulnérabilités connues, comme la saturation de la mémoire tampon, qu'un pirate peut utiliser pour obtenir le contrôle du système affecté. Quel que soit le protocole de sécurité utilisé par l'application de paiement, s'assurer qu'il est configuré de manière à n'utiliser que des configurations et versions sécurisées par défaut pour empêcher l'utilisation de toute connexion non sécurisée.

Conditions de la norme PA-DSS	Procédures de test	Directive
autres, 802.11 et Bluetooth • Les technologies cellulaires, par exemple, Système global pour les communications mobiles (GSM), Accès multiple de division de code (CDMA) • GPRS (service général de radiocommunication en mode paquet) • Communications par satellite ***Correspond à la condition 4.1 de la norme PCI DSS***	**11.1.c** Si une cryptographie et des protocoles de sécurité forts sont fournis avec l'application de paiement, installer et tester l'application selon les instructions du *Guide de mise en œuvre de la norme PA-DSS* et vérifier : • Le protocole est implémenté par défaut pour utiliser uniquement des clés et/ou des certificats approuvés. • Le protocole est déployé par défaut de manière à n'utiliser que des configurations sécurisées et il ne prend en charge aucune version ni configuration non sécurisées. • Le protocole est déployé par défaut de manière à empêcher le repli sur une version ou une configuration non sécurisée (par exemple, si le TLS est utilisé, l'application ne doit pas autoriser le repli sur SSL). • Le niveau de cryptage approprié est mis en œuvre pour la méthodologie de cryptage employée.	
11.2 Si l'application de paiement autorise l'envoi de PAN par des technologies de messagerie de l'utilisateur final (par exemple, courrier électronique, messagerie instantanée, discussions en ligne), l'application de paiement doit fournir une solution rendant le PAN illisible ou mettre en œuvre une cryptographie robuste, ou spécifier l'utilisation d'une cryptographie robuste pour crypter les PAN. ***Correspond à la condition 4.2 de la norme PCI DSS***	**11.2.a** Si l'application autorise et/ou facilite l'envoi de PAN par des technologies de messagerie pour les utilisateurs finaux, vérifier qu'une solution qui rend le PAN illisible ou met en place une cryptographie robuste est fournie, ou que son utilisation est spécifiée.	La messagerie électronique, la messagerie instantanée et le chat peuvent être facilement interceptés par reniflage de paquets durant le survol des échanges sur les réseaux internes et publics. Ne jamais envoyer de PAN à l'aide de ces outils de messagerie à moins que l'application de paiement ne prenne en charge l'utilisation de cryptographie robuste avec ces technologies ou ne rende le PAN illisible.
	11.2.b Examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier que le fournisseur inclut des instructions pour les clients et revendeurs/intégrateurs afin qu'ils utilisent une solution fournie ou spécifiée pour l'utilisation avec l'application, y compris : • Des procédures pour utiliser la solution définie pour rendre le PAN illisible ou pour sécuriser le PAN avec une cryptographie robuste. • Des instructions selon lesquelles le PAN doit toujours être rendu illisible ou protégé par une cryptographie robuste chaque fois qu'il est envoyé à l'aide de technologies de messagerie aux utilisateurs finaux.	
	11.2.c Si une solution est fournie avec l'application de paiement, installer et tester l'application pour vérifier que la solution rend le PAN illisible ou implémente une cryptographie robuste.	

Condition 12 : Sécuriser tous les accès administratifs non-console

Conditions de la norme PA-DSS	Procédures de test	Directive
12.1 Si l'application de paiement facilite l'accès administratif non-console, crypter tous ces accès avec une cryptographie robuste. ***Remarques :*** • *Les protocoles à texte clair tels que Telnet ou rlogin ne doivent jamais être utilisés pour l'accès administratif.* • *Le SSL ou le TLS initial ne sont pas considérés comme étant une cryptographie robuste. Les applications de paiement ne doivent ni utiliser ni prendre en charge le SSL ou le TLS initial. Les applications qui utilisent ou prennent en charge le TLS ne doivent pas autoriser un repli sur le SSL.* ***Correspond à la condition 2.3 de la norme PCI DSS***	**12.1.a** Installer l'application de paiement dans un laboratoire et tester les connexions d'administration non console pour vérifier qu'une méthode de cryptage robuste est invoquée avant que l'administrateur ne soit invité à taper son mot de passe. **12.1.b** Examiner les paramètres de configuration de l'application de paiement pour vérifier que les protocoles à texte clair, tels que Telnet et rlogin, ne sont pas utilisés par l'application de paiement pour les accès administratifs non console. **12.1.c** Examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur, puis vérifier qu'il comprend des instructions pour les clients et les intégrateurs/revendeurs expliquant comment configurer l'application pour utiliser une cryptographie robuste pour le cryptage des accès administratifs non console.	Si l'administration à distance ne s'effectue pas par le biais d'une authentification sécurisée et de communications cryptées, les informations administratives ou de niveau opérationnel sensibles (comme les mots de passe de l'administrateur) peuvent être interceptées. Un individu malveillant pourrait utiliser cette information pour accéder à l'application et/ou au réseau, modifier les permissions et voler des données.
12.1.1 Indiquer aux clients de crypter tous les accès administratifs non-console à l'aide d'une cryptographie robuste pour la gestion par Internet et les autres accès administratifs non-console. ***Remarque :*** *Les protocoles à texte clair tels que Telnet ou rlogin ne doivent jamais être utilisés pour l'accès administratif.* ***Correspond à la condition 2.3 de la norme PCI DSS***	**12.1.1** Examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur et vérifier qu'il comprend des instructions pour les clients et les intégrateurs/revendeurs pour qu'ils implémentent une cryptographie robuste pour le cryptage de tous les accès administratifs non console.	Les fournisseurs d'application de paiement devront fournir des instructions aux clients et aux intégrateurs/revendeurs pour la configuration de l'application afin qu'elle utilise une cryptographie robuste pour le cryptage des accès administratifs non console. Cette opération aide à garantir que les contrôles de sécurité sont correctement mis en œuvre et respectent les directives des normes PCI DSS et PA-DSS.

Conditions de la norme PA-DSS	Procédures de test	Directive
12.2 Utiliser l'authentification à plusieurs facteurs pour tous les membres du personnel dotés d'un accès administratif non-console. ***Remarque :*** *L'authentification à plusieurs facteurs requiert d'utiliser au moins deux des trois méthodes d'authentification (voir la condition 3.1.4 de la norme PA-DSS pour la description des méthodes d'authentification).* ***Correspond à la condition 8.3 de la norme PCI DSS***	**12.2.a** Vérifier que l'authentification à plusieurs facteurs est fournie avec l'application, ou que son utilisation est spécifiée.	L'accès administratif exige un niveau supérieur d'assurance dans la mesure où l'individu tentant un accès doit correspondre à la personne qu'il prétend être. Dans la mesure où l'authentification à plusieurs facteurs peut être implémentée au niveau de l'application, du système ou du réseau, il n'est pas obligatoire que toutes les applications comprennent une solution d'authentification à plusieurs facteurs. Les fournisseurs d'application peuvent octroyer une authentification à plusieurs facteurs avec leur application ou inclure des instructions pour les utilisateurs et revendeurs/intégrateurs en vue d'installer une authentification à plusieurs facteurs pour un accès administratif à l'application.
	12.2.b Examiner le *Guide de mise en œuvre de la norme PA-DSS* préparé par le fournisseur, puis vérifier s'il comprend des instructions pour les clients et les intégrateurs/revendeurs sur l'utilisation de l'authentification à plusieurs facteurs, y compris ce qui suit : • Instructions spécifiant que l'authentification à plusieurs facteurs est obligatoire pour tous les membres du personnel dotés d'un accès administratif non-console au CDE. • Procédures d'utilisation de l'authentification à plusieurs facteurs fournies avec l'application (le cas échéant).	
	12.2.c Si l'authentification à plusieurs facteurs est fournie avec l'application de paiement, installer et tester l'application pour vérifier que l'authentification à plusieurs facteurs est appliquée avant l'octroi de l'accès.	

Condition 13 : Maintenir un Guide de mise en œuvre de la norme PA-DSS pour les clients, les revendeurs et les intégrateurs

Conditions de la norme PA-DSS	Procédures de test	Directive
13.1 Développer, gérer et diffuser le ou les *Guide(s) de mise en œuvre de la norme PA-DSS* pour les clients, les revendeurs et les intégrateurs. Ce guide doit :	**13.1** Examiner le *Guide de mise en œuvre de la norme PA-DSS* et les processus connexes du vendeur, et interroger le personnel pour vérifier : • Le *Guide de mise en œuvre de la norme PA-DSS* est communiqué à tous les clients, revendeurs et intégrateurs avec l'application. • Le vendeur a mis en place un mécanisme pour fournir le *Guide de mise en œuvre de la norme PA-DSS* aux clients, revendeurs et intégrateurs sur demande.	Un *Guide de mise en œuvre de la norme PA-DSS* bien conçu et détaillé aide à guider les clients et les intégrateurs/revendeurs dans la mise en œuvre des mesures de sécurité et des configurations appropriées dans l'application de paiement et ses composants sous-jacents afin de respecter les directives pertinentes des normes PCI DSS et PA-DSS pour la protection de données de titulaires de carte.
13.1.1 Fournit des informations pertinentes, spécifiques à l'application destinées à l'utilisation des clients, revendeurs et intégrateurs.	**13.1.1** Examiner le *Guide de mise en œuvre de la norme PA-DSS* et vérifier qu'il : • Identifie clairement le nom et la version de l'application de paiement à laquelle il s'applique. • Donne des détails des dépendances d'application qui sont requises pour que l'application soit configurée pour être conforme à la norme PCI DSS.	
13.1.2 Traiter toutes les exigences du présent document chaque fois que le *Guide de mise en œuvre de la norme PA-DSS* est mentionné.	**13.1.2** Examiner le *Guide de mise en œuvre de la norme PA-DSS* et utiliser l'annexe A comme référence, vérifier que le *Guide de mise en œuvre de la norme PA-DSS* recouvre toutes les conditions liées à ce document.	
13.1.3 Comprend un examen au moins annuel et suite aux changements de l'application ou des conditions de la norme PA-DSS, et est mis à jour au besoin pour que le document demeure d'actualité avec tous les changements affectant l'application, ainsi que selon les conditions de ce document.	**13.1.3.a** Examiner le *Guide de mise en œuvre de la norme PA-DSS* et interroger le personnel pour vérifier que le *Guide de mise en œuvre de la norme PA-DSS* est examiné : • Au moins une fois par an ; • Suite à des changements apportés à l'application ; • Suite à des changements apportés à ces directives de la norme PA-DSS.	Avec chaque mise à jour de l'application, la fonctionnalité du système et, dans certains cas, les mécanismes critiques pour la sécurité de l'application, sont modifiés ou introduits. Si le *Guide de mise en œuvre de la norme PA-DSS* ne reste pas à jour par rapport aux dernières versions de l'application de paiement, les

Conditions de la norme PA-DSS	Procédures de test	Directive
	13.1.3.b Vérifié que le *Guide de mise en œuvre de la norme PA-DSS* reste à jour par rapport : • Aux changements apportés aux directives de la norme PA-DSS • Aux changements apportés à l'application ou à ses dépendances	clients et les intégrateurs/revendeurs pourraient ignorer ou mal configurer des contrôles de sécurité critiques pour l'application, ce qui pourrait permettre à un pirate de contourner ces mécanismes de sécurité et de compromettre des données sensibles.
	13.1.3.c Examiner le *Guide de mise en œuvre de la norme PA-DSS* et les processus de fournisseur connexes, et interroger le personnel pour vérifier que le fournisseur a mis en place un mécanisme pour communiquer les mises à jour aux clients, revendeurs et intégrateurs, et pour fournir les versions mises à jour si besoin.	

Condition 14 : Affecter des responsabilités vis-à-vis de la norme PA-DSS au personnel et maintenez des programmes de formation pour le personnel, les clients, les revendeurs et les intégrateurs

Conditions de la norme PA-DSS	Procédures de test	Directive
14.1 Assurer la formation en matière de sécurité et concernant la norme PA-DSS au moins une fois par an pour le personnel du fournisseur ayant des responsabilités au regard de la norme PA-DSS.	**14.1** Examiner les documents de formation et interroger le personnel responsable pour vérifier que tout le personnel du vendeur ayant des responsabilités aux regards de la norme PA-DSS sera formé et informé au moins une fois par an à propos de la norme PA-DSS.	Afin qu'une application de paiement soit conçue de manière efficace pour respecter les directives de la norme PA-DSS, le personnel du fournisseur de l'application de paiement doit connaître la norme PA-DSS ainsi que leurs responsabilités au regard des évaluations de la norme PA-DSS. Le fournisseur de l'application de paiement est responsable de s'assurer que son personnel soit correctement formé dans ce domaine.
14.2 Affecter les rôles et responsabilités au personnel du fournisseur, y compris ce qui suit : • La responsabilité globale pour respecter les conditions de la norme PA-DSS ; • Rester à jour par rapport à tout changement du Guide de programme PCI SSC PA-DSS ; • S'assurer que les pratiques de codage sécurisées sont utilisées ; • S'assurer que les intégrateurs/revendeurs reçoivent une formation adéquate ainsi que les documents associés ; • S'assurer que le personnel du fournisseur ayant des responsabilités au regard de la norme PA-DSS, y compris les développeurs,	**14.2.a** Examiner les responsabilités documentées pour vérifier que les responsabilités pour les rôles suivants sont formellement assignées : • La responsabilité globale pour respecter les conditions de la norme PA-DSS ; • Rester à jour par rapport à tout changement du Guide de programme PCI SSC PA-DSS ; • S'assurer que les pratiques de codage sécurisées sont utilisées ; • S'assurer que les intégrateurs/revendeurs reçoivent une formation adéquate ainsi que les documents associés ; • S'assurer que le personnel du fournisseur ayant des responsabilités au regard de la norme PA-DSS, y compris les développeurs, sont formés.	Dans chaque organisation du fournisseur d'application de paiement, une partie responsable (soit un individu soit une équipe) doit recevoir une responsabilité formelle pour la norme PA-DSS pour garantir que les conditions de la norme PA-DSS sont respectées en conséquence.

Conditions de la norme PA-DSS	Procédures de test	Directive
sont formés.	**14.2.b** Interroger le personnel auquel des responsabilités ont été attribuées dans les rôles suivant pour confirmer que les rôles et responsabilités sont définis et compris : • La responsabilité globale pour respecter les conditions de la norme PA-DSS ; • Rester à jour par rapport à tout changement du Guide de programme PCI SSC PA-DSS ; • S'assurer que les pratiques de codage sécurisées sont utilisées ; • S'assurer que les intégrateurs/revendeurs reçoivent une formation adéquate ainsi que les documents associés ; • S'assurer que le personnel du fournisseur ayant des responsabilités au regard de la norme PA-DSS, y compris les développeurs, sont formés.	
14.3 Développer et implémenter des programmes de communication pour les intégrateurs et les revendeurs de l'application de paiement. La formation doit inclure au moins les points suivants : • Comment implémenter l'application de paiement et les systèmes et réseaux associés d'une manière conforme à la norme PCI DSS. • Couvrir tous les éléments notés pour le *Guide de mise en œuvre de la norme PA-DSS* dans ce document (et dans l'annexe A).	**14.3.a** Examiner les documents de formation pour les intégrateurs et les revendeurs, et confirmer que les documents comprennent ce qui suit : • Une formation expliquant comment implémenter l'application de paiement et les systèmes et réseaux associés d'une manière conforme à la norme PCI DSS. • Couvrir tous les éléments notés pour le *Guide de mise en œuvre de la norme PA-DSS* dans ce document (et dans l'annexe A).	Une configuration, maintenance ou support incorrects d'une application peuvent causer l'introduction de vulnérabilités du point de vue de la sécurité dans l'environnement des données de titulaires de carte du client qui pourraient être exploitées par des pirates. Les fournisseurs d'application doivent assurer la formation des intégrateurs/revendeurs à l'installation et la configuration sécurisée de l'application pour assurer que, lorsque l'application est installée dans l'environnement du client, l'application facilite la conformité à la norme PCI DSS Le fournisseur de l'application de paiement est responsable de la formation des intégrateurs et des revendeurs dans ces domaines.
	14.3.b Examiner le programme de communication du fournisseur et les processus connexes du fournisseur, et interroger le personnel pour vérifier que : • Les documents de formation sont fournis aux intégrateurs et aux revendeurs. • Le fournisseur a mis en place un mécanisme pour fournir les matériaux de formation aux revendeurs et aux intégrateurs sur demande.	
	14.3.c Interroger un échantillon de revendeurs et d'intégrateurs et les contacter pour vérifier qu'ils ont bien reçu la formation et les documents de formation de la part du fournisseur de l'application.	

Conditions de la norme PA-DSS	Procédures de test	Directive
	14.3.d Examiner les preuves que les intégrateurs et les revendeurs ont reçu les documents de formation de la part du fournisseur de logiciel.	
14.3.1 Contrôler les documents de formation au moins une fois par an, à la suite des changements apportés à l'application ou selon les exigences de la norme PA-DSS. Mettre à jour les documents de formation au besoin afin qu'ils restent d'actualité en cas de nouvelles versions de l'application de paiement et de changements aux conditions de la norme PA-DSS.	**14.3.1.a** Examiner les documents de formation pour les intégrateurs et les revendeurs, et vérifier qu'ils sont : • Examinés au moins une fois par an et suite aux changements de l'application ou des conditions de la norme PA-DSS. • Mis à jour au besoin afin qu'ils restent d'actualité en cas de nouvelles versions de l'application de paiement et de changements aux conditions de la norme PA-DSS.	Les documents de formation pour le personnel du fournisseur de paiement d'application, les intégrateurs et les revendeurs doivent être mis à jour au moins une fois pas an pour garantir qu'ils demeurent pertinents avec les dernières versions de l'application et les conditions de la norme PA-DSS. L'utilisation de documents de formation obsolètes pourrait rendre les programmes de formation inefficaces, provoquer des fonctions de sécurité de conception médiocre dans l'application ou des configurations incorrectes de l'application par les intégrateurs et les revendeurs.
	14.3.1.b Examiner le processus de distribution des nouvelles versions de l'application de paiement et vérifier que la documentation mise à jour est bien distribuée aux intégrateurs et aux revendeurs avec l'application de paiement mise à jour.	
	14.3.1.c Interroger un échantillon de revendeurs et d'intégrateurs et vérifier qu'ils ont bien reçu les documents de formation mis à jour de la part du fournisseur de l'application.	

Annexe A : Résumé du contenu du *Guide de mise en œuvre de la norme PA-DSS*

Cette annexe a pour but de résumer les conditions de la norme PA-DSS dont les sujets se rapportent au *Guide de mise en œuvre de la norme PA-DSS*thème, pour expliquer le contenu du *Guide de mise en œuvre de la norme PA-DSS* fourni aux clients et aux intégrateurs/revendeurs (voir « Guide de mise en œuvre de la norme PA-DSS » en page 11) et pour décrire les responsabilités de la mise en œuvre des contrôles connexes.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
1.1.4	Supprimer les données d'identification sensibles stockées par les versions précédentes des applications de paiement.	Les instructions suivantes doivent être fournies aux clients et aux intégrateurs/revendeurs : ▪ Les données d'historique (données de bande magnétique, codes de validation de carte, codes ou blocs PIN, stockés par les versions précédentes de l'application de paiement) doivent être supprimées. ▪ Comment supprimer les données d'historique. ▪ Cette suppression est absolument nécessaire pour la conformité à la norme PCI DSS.	**Fournisseur de logiciels** : Fournir l'outil ou la procédure aux clients pour supprimer les données d'identification sensibles stockées par les versions précédentes en toute sécurité, conformément à la condition 1.1.4 de la norme PA-DSS. **Clients et intégrateurs/revendeurs** : Supprimer toutes les données d'historique conformément au *Guide de mise en œuvre de la norme PA-DSS* et à la condition 1.1.4 de la norme PA-DSS.
1.1.5	Supprimer toute donnée d'identification sensible (pré-autorisation) recueillie à l'issue du dépannage de l'application de paiement.	Les instructions suivantes doivent être fournies aux clients et aux intégrateurs/revendeurs : ▪ Les données d'identification sensibles (pré-autorisation) doivent uniquement être collectées lorsque cela est nécessaire pour résoudre un problème particulier. ▪ Ces données doivent être stockées à un emplacement spécifique connu dont l'accès est restreint. ▪ Collecter uniquement une quantité limitée de données, nécessaires pour résoudre un problème particulier. ▪ Les données d'identification sensibles doivent être cryptées lors du stockage. ▪ Ces données doivent être supprimées de façon sécurisée immédiatement après leur utilisation.	**Fournisseur de logiciels** : Ne pas stocker de données d'identification sensibles et effectuer le dépannage des problèmes de clients conformément à la condition 1.1.5.a de la norme PA-DSS. **Clients et intégrateurs/revendeurs :** Ne pas stocker de données d'identification sensibles et effectuer le dépannage des problèmes conformément au *Guide de mise en œuvre de la norme PA-DSS* et à la condition 1.1.5.a de la norme PA-DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
2.1	Supprimer les données de titulaires de carte de manière sécuritaire une fois la période de rétention définie écoulée par le client.	Les informations suivantes doivent être fournies aux clients et aux intégrateurs/revendeurs : ▪ Des instructions selon lesquelles les données de titulaires de carte dépassant la période de rétention définie par le client doivent être supprimées. ▪ Une liste de tous les emplacements où l'application de paiement stocke les données de titulaires de carte, de manière à ce que le client connaisse l'emplacement des données à supprimer. ▪ Des instructions selon lesquelles le client a besoin de supprimer les données de titulaires de carte lorsqu'elles ne sont plus requises pour les besoins légaux, réglementaires ou commerciaux. ▪ Comment supprimer les données de titulaires de carte stockées par l'application de paiement de manière sécurisée, y compris les données stockées par des logiciels ou systèmes sous-jacents (tels que SE, bases de données, etc.). ▪ Comment configurer les logiciels ou systèmes sous-jacents (tels que SE, bases de données, etc.) pour prévenir la capture ou la rétention accidentelle des données de titulaires de carte.	**Fournisseur de logiciels** : Signaler aux clients que les données de titulaires de carte dépassant la période de rétention définie par le client doivent être supprimées de manière sécuritaire lorsque ces données sont stockées par l'application de paiement et les logiciels ou systèmes sous-jacents ; et expliquer comment supprimer les données de titulaires de carte stockées par l'application de paiement de manière sécuritaire. **Clients et intégrateurs/revendeurs** : Supprimer de manière sécuritaire les données de titulaires de carte dépassant la période de rétention définie par le client, conformément au *Guide de mise en œuvre de la norme PA-DSS* et à la condition 2.1 de la norme PA-DSS.
2.2	Masquer le PAN affiché de sorte que seul le personnel qui a un besoin professionnel légitime puisse voir plus que les six premiers/les quatre derniers chiffres du PAN.	Les informations suivantes doivent être fournies aux clients et aux intégrateurs/revendeurs : ▪ Détails de toutes les instances pour lesquelles le PAN est affiché, comprenant, entre autres, les dispositifs de POS, les écrans, les journaux et les reçus. ▪ Confirmation que l'application de paiement masque le PAN par défaut sur tous les écrans. ▪ Instructions concernant le mode de configuration de l'application de paiement de sorte que seul le personnel ayant un besoin professionnel légitime puisse voir les six premiers/les quatre derniers chiffres du PAN (PAN entier).	**Fournisseur de logiciels** : Donner des instructions aux clients expliquant comment masquer le PAN de sorte que seul le personnel ayant un besoin professionnel légitime puisse voir les six premiers/les quatre derniers chiffres du PAN. **Clients et intégrateurs/revendeurs** : Masquer le PAN lorsqu'il est affiché de sorte que seul le personnel ayant un besoin professionnel légitime puisse voir les six premiers/les quatre derniers chiffres du PAN, conformément au *Guide de mise en œuvre de la norme PA-DSS* et à la condition 2.2 de la norme PA-DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
2.3	Rendre le PAN illisible où qu'il soit stocké (y compris les données sur support numérique portable, support de sauvegarde et journaux).	Les informations suivantes doivent être fournies aux clients et aux intégrateurs/revendeurs : ▪ Détail des options configurables pour chaque méthode utilisée par l'application pour rendre les données de titulaires de carte illisibles et instructions relatives à la configuration de chaque méthode pour les emplacements ou les données de titulaires de carte sont stockées par l'application de paiement (selon la condition 2.1 de la norme PA-DSS). ▪ Une liste des instances où les données de titulaires de carte pourraient être produites pour que le client les stocke hors de l'application de paiement, ainsi que les instructions relatives à la responsabilité du client de rendre le PAN illisible dans toutes ces instances. ▪ Si les journaux de débogage sont activés (à des fins de dépannage, par exemple) et s'ils comprennent le PAN, ils doivent être protégés conformément à la norme PCI DSS, désactivés dès que le dépannage est terminé et supprimés en toute sécurité lorsqu'ils ne sont plus requis.	**Fournisseur de logiciels** : Donner des instructions aux clients pour rendre le PAN illisible lorsqu'il est stocké ou produit par l'application. **Clients et intégrateurs/revendeurs** : Rendre le PAN illisible à chaque fois qu'il est stocké, conformément au *Guide de mise en œuvre de la norme PA-DSS* et à la condition 2.3 de la norme PA-DSS.
2.4	Protéger les clés utilisées pour le cryptage des données de titulaires de carte contre la divulgation et l'utilisation illicite.	Les instructions suivantes doivent être fournies aux clients et aux intégrateurs/revendeurs : ▪ Restreindre l'accès aux clés cryptographiques au plus petit nombre d'opérateurs possible. ▪ Stocker les clés de manière sécurisée dans aussi peu d'emplacements et sous aussi peu de formes que possible.	**Fournisseur de logiciels** : Fournir des directives aux clients indiquant que les clés utilisées pour sécuriser les données de titulaires de carte doivent être stockées de manière sécurisée dans le minimum d'endroits possibles et que l'accès à ces clés doit être restreint au minimum d'opérateurs possible. **Clients et intégrateurs/revendeurs** : Stocker les clés de manière sécuritaire dans le minimum d'endroits possibles et restreindre l'accès aux clés au minimum d'opérateurs possibles, conformément au *Guide de mise en œuvre de la norme PA-DSS* et la condition 2.4 de la norme PA-DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
2.5	Mettre en œuvre des processus et procédures de gestion pour les clés cryptographiques utilisées pour le cryptage des données de titulaires de carte.	Les informations suivantes doivent être fournies aux clients et aux intégrateurs/revendeurs : ▪ Instructions pour savoir comment générer, distribuer, protéger, changer, stocker et retirer/replacer de manière sécurisée les clés cryptographiques, lorsque les clients ou les intégrateurs/revendeurs sont impliqués dans ces activités de gestion de clés. ▪ Un formulaire aux opérateurs chargés des clés cryptographiques reconnaissant qu'ils comprennent et acceptent leurs responsabilités en tant que telles.	**Fournisseur de logiciels** : Donner des instructions aux clients qui accèdent aux clés cryptographiques utilisées pour le cryptage des données de titulaires de carte pour qu'ils implémentent les processus et procédures de gestion des clés. **Clients et intégrateurs/revendeurs** : Implémenter des processus et procédures pour les clés cryptographiques utilisés pour le cryptage des données de titulaires de carte conformément au *Guide de mise en œuvre de la norme PA-DSS* et la condition 2.5 de la norme PA-DSS.
2.5.1 – 2.5.7	Implémenter les fonctions de gestion sécurisée de clé.	Donner des instructions aux clients et aux intégrateurs/revendeurs sur l'accomplissement des fonctions de gestion de clé, y compris : ▪ La génération de clés cryptographiques robustes ; ▪ Sécuriser la distribution des clés cryptographiques ; ▪ Sécuriser le stockage des clés cryptographiques ; ▪ Les changements de clés cryptographiques pour les clés qui ont atteint la fin de leur cryptopériode ; ▪ Retrait ou remplacement des clés si nécessaire lorsque le degré d'intégrité d'une clé a été ou lorsqu'on soupçonne que les clés sont compromises ; ▪ Le fractionnement des connaissances et le double contrôle des opérations manuelles de gestion des clés cryptographiques en texte clair prises en charge par l'application de paiement ; ▪ Prévention de la substitution non autorisée des clés cryptographiques.	**Fournisseur de logiciels** : Donner des instructions aux clients pour implémenter les fonctions de gestion sécurisée de clé. **Clients et intégrateurs/revendeurs** : Implémenter des fonctions de gestion de clé cryptographique sécurisées conformément au *Guide de mise en œuvre de la norme PA-DSS* et aux conditions 2.5.1 - 2.5.7 de la norme PA-DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
2.6	Fournir un mécanisme pour rendre irrécupérable tout élément de clé cryptographique ou de cryptogramme, stocké par l'application de paiement.	Les informations suivantes doivent être fournies aux clients et aux intégrateurs/revendeurs : ▪ Procédures détaillées sur l'utilisation de l'outil ou de la procédure fournie avec l'application pour rendre les éléments cryptographiques irrécupérables. ▪ Des instructions selon lesquelles les éléments de clé cryptographique doivent être rendus irrécupérables lorsque les clés ne sont plus utilisées, conformément aux conditions de gestion des clés de la norme PCI DSS. ▪ Instructions expliquant comment crypter une nouvelle fois les données d'historique avec de nouvelles clés, y compris les procédures pour maintenir la sécurité des données en texte clair pendant le processus de décryptage/re-cryptage.	**Fournisseur de logiciels** : Fournir un outil ou une procédure de suppression sécurisée des éléments de clé cryptographiques ou des cryptogrammes stockés par l'application et fournir un outil ou une procédure pour crypter de nouveau les données d'historique avec de nouvelles clés. **Clients et intégrateurs/revendeurs** : Supprimer tout élément cryptographique d'historique conformément aux conditions de gestion des clés du *Guide de mise en œuvre de la norme PA-DSS* et à la condition 2.6 de la norme PA-DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
3.1	Utiliser des ID d'utilisateur uniques et sécuriser l'authentification pour l'accès administratif et l'accès aux données de titulaires de carte	Les informations suivantes doivent être fournies aux clients et aux intégrateurs/revendeurs : ▪ Des instructions sur la manière avec laquelle l'application de paiement utilise une authentification robuste pour tous les justificatifs d'authentification (par exemple, utilisateurs, mots de passe) que l'application génère ou gère, en : – Appliquant des changements sécurisés aux justificatifs d'authentification dès la fin de l'installation selon les conditions 3.1.1 à 3.1.11 de la norme PA-DSS. – Appliquant des changements sécurisés aux justificatifs d'authentification pour tout changement consécutif (dès la fin de l'installation) selon les conditions 3.1.1 à 3.1.11 de la norme PA-DSS. ▪ Ils sont informés que, pour maintenir la conformité à la norme PCI DSS, tout changement effectué aux configurations d'authentification devrait être vérifié comme, apportant des méthodes d'authentification qui sont au moins aussi rigoureuses que les conditions de la norme PCI DSS. ▪ Ils sont informés qu'ils doivent affecter une authentification sécurisée à tous les comptes par défaut dans l'environnement. ▪ Ils sont informés qu'ils doivent affecter une authentification sécurisée pour tous les comptes par défaut qui ne seront pas utilisés, puis désactiver ou ne pas utiliser les comptes. ▪ Comment changer et créer des justificatifs d'authentification lorsque ceux-ci ne sont pas générés ou gérés par l'application de paiement, conformément aux conditions 3.1.1 à 3.1.11 de la norme PCI DSS, dès la fin de l'installation et pour tout changement ultérieur après l'installation, pour tous les comptes de niveau application avec un accès administratif ou un accès aux données de titulaires de carte. ▪ Identification de tous les rôles et comptes par défaut dans l'application dotée d'un accès administratif.	**Fournisseur de logiciels** : Pour tous les justificatifs d'authentification générés ou gérés par l'application, s'assurer que l'application de paiement exige que le client utilise un ID utilisateur unique et une authentification sécurisée pour les comptes/mots de passe, conformément aux conditions 3.1.1 à 3.1.11 de la norme PA-DSS. Pour les justificatifs d'authentification qui ne sont pas générés ou gérés par l'application de paiement, s'assurer que le *Guide de mise en œuvre de la norme PA-DSS* fournit des directives claires et sans ambiguïté aux clients et aux revendeurs/intégrateurs sur la manière de changer ou de créer des justificatifs d'authentification conformément aux conditions 3.1.1 à 3.1.11 de la norme PA-DSS. **Clients et intégrateurs/revendeurs** : Établir et maintenir des ID d'utilisateur uniques et une authentification sécurisée, conformément au *Guide de mise en œuvre de la norme PA-DSS* et aux conditions 3.1.1 à 3.1.11 de la norme PA-DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
3.2	Utiliser des ID d'utilisateur et sécuriser l'authentification pour l'accès aux PC, serveurs et bases de données.	Indiquer aux clients et aux intégrateurs/revendeurs d'utiliser des noms uniques et une authentification sécurisée pour accéder aux PC, serveurs et bases de données avec des applications de paiement et/ou des données de titulaires de carte, conformément aux conditions 3.1.1 à 3.1.11 de la norme PA-DSS.	**Fournisseur de logiciels** : S'assurer que l'application de paiement prend en charge l'utilisation par le client d'ID d'utilisateur unique et d'une authentification sécurisée pour les comptes/mots de passe si de telles méthodes ont été définies par le fournisseur pour accéder aux PC, serveurs et bases de données, conformément aux conditions 3.1.2 à 3.1.9 de la norme PA-DSS. **Clients et intégrateurs/revendeurs** : Établir et maintenir des ID d'utilisateur uniques et une authentification sécurisée, conformément au *Guide de mise en œuvre de la norme PA-DSS* et aux conditions 3.1.1 à 3.1.11 de la norme PA-DSS.
4.1	Mettre en œuvre une vérification à rebours automatisée.	Donner des instructions que l'implémentation des pistes d'audit automatique comprenne : ▪ Comment installer l'application pour que les journaux soient configurés et activés par défaut lorsque le processus d'installation est terminé. ▪ Comment configurer les paramètres de journaux conformément à la norme PCI-DSS, selon les conditions 4.2, 4.3 et 4.4 de la norme PA-DSS, pour toutes les options de journalisation qui sont configurables par le client après installation. ▪ Les journaux doivent être activés ; leur désactivation entraînera la non-conformité aux normes PCI DSS. ▪ Comment configurer les paramètres de journaux conformément à la norme PCI pour tous les composants de logiciel tiers en paquetage avec l'application de paiement ou requise par celle-ci, pour toute option de journalisation pouvant être configurée par le client après installation.	**Fournisseur de logiciels** : S'assurer que l'application de paiement prend en charge l'utilisation par le client de journaux conformes aux conditions 4.2, 4.3 et 4.4 de la norme PA-DSS. **Clients et intégrateurs/revendeurs :** Établir et maintenir des journaux conformes à la norme PCI DSS selon le *Guide de mise en œuvre de la norme PA-DSS* et selon les conditions 4.2, 4.3 et 4.4 de la norme PA-DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
4.4	Permettre une journalisation centralisée.	Fournir une description des mécanismes de journalisation centralisée pris en compte, ainsi que des instructions et procédures pour intégrer les journaux d'application de paiement dans un serveur de journalisation centralisé.	**Fournisseur de logiciels** : S'assurer que l'application de paiement prend en charge la journalisation centralisée dans les environnements de client conformément à la condition 4.4 de la norme PA-DSS. **Clients et intégrateurs/revendeurs :** Établir et maintenir une journalisation centralisée selon le *Guide de mise en œuvre de la norme PA-DSS* et la condition 4.4 de la norme PA-DSS.
5.4.4	Implémenter et communiquer une méthodologie de gestion des versions d'application.	Donner une description de la méthodologie de gestion des versions du fournisseur et inclure des directives pour ce qui suit : ▪ Les détails du système de version, y compris son format (nombre d'éléments, séparations, ensembles de caractères, etc.). ▪ Les détails de la manière avec laquelle les changements qui ont un impact sur la sécurité seront indiqués par le système de version. ▪ Les détails de la manière avec laquelle les types de changement affecteront la version. ▪ Les détails de tout élément de caractère générique qui est utilisé, y compris la confirmation qu'il ne sera jamais utilisé pour représenter un changement ayant un impact sur la sécurité.	**Fournisseur de logiciels** : Documenter et implémenter une méthodologie de gestion des versions de logiciel dans le cadre du cycle de vie du développement de système. Cette méthodologie doit suivre les procédures du *Guide du programme de la norme PA-DSS* pour les changements des applications de paiement, selon la condition 5.5 de la norme PA-DSS. **Clients et intégrateurs/revendeurs :** Comprendre quelle version de l'application de paiement ils utilisent et garantir que des versions validées sont utilisées.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
6.1	Mettre en œuvre la technologie sans-fil de façon sécurisée.	Pour les applications de paiement développées pour une utilisation avec la technologie sans-fil, les éléments suivants doivent être fournis aux clients et aux intégrateurs/revendeurs : ▪ Des instructions selon lesquelles l'application de paiement impose des changements de clés de cryptage par défaut, de mots de passe et de chaînes de communauté SNMP, lors de l'installation de tous les composants sans-fil contrôlés par l'application. ▪ Les procédures de changement de clés de cryptage et de mot de passe de réseau sans-fil, y compris les chaînes SNMP, dès lors que quelqu'un qui connaît les clés/mots de passe quitte la société ou change de poste. ▪ Les instructions relatives au changement de clés de cryptage par défaut, de mots de passe et de chaînes de communauté SNMP de n'importe quel composant sont fournies par l'application de paiement, mais elles ne sont pas sous son contrôle. ▪ Les instructions relatives à l'installation d'un pare-feu entre tous les réseaux sans-fil et les systèmes qui stockent les données de titulaires de carte. ▪ Les détails de tout trafic sur le réseau sans-fil (y compris les informations portant sur le port spécifique) que la fonction sans-fil de l'application de paiement pourrait utiliser. ▪ Les instructions relatives à la configuration des pare-feu pour qu'ils refusent ce trafic ou (si ce trafic est nécessaire à des fins commerciales) permettre uniquement au trafic autorisé de circuler entre l'environnement du réseau sans-fil et l'environnement des données de titulaires de carte.	**Fournisseur de logiciels** : Indiquer aux clients et aux revendeurs/intégrateurs que, si une technologie sans-fil est utilisée avec l'application de paiement, les paramètres par défaut du fournisseur de la technologie sans-fil doivent être modifiés conformément à la condition 6.1 de la norme PA-DSS. **Clients et intégrateurs/revendeurs** : Pour la technologie sans-fil mise en œuvre dans l'environnement de paiement par les clients ou les revendeurs/intégrateurs, changer les paramètres par défaut du fournisseur, conformément à la condition 6.1 de la norme PA-DSS et installer un pare-feu conformément au *Guide de mise en œuvre de la norme PA-DSS* et à la condition 2.1.1 de la norme PCI DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
6.2	Sécuriser les transmissions de données de titulaires de carte sur les réseaux sans-fil.	Pour les applications de paiement développées pour une utilisation avec la technologie sans-fil, inclure les instructions pour l'utilisation de meilleures pratiques du secteur (par exemple IEEE 802.11i) pour appliquer un cryptage robuste à l'authentification et à la transmission des données de titulaires de carte. Ce qui comprend : ▪ Comment configurer l'application pour utiliser les meilleures pratiques du secteur (par exemple, IEEE 802.11i) pour appliquer un cryptage robuste à l'authentification et la transmission et/ou ▪ Comment configurer toutes les applications sans-fil groupées avec l'application de paiement pour utiliser les meilleures pratiques du secteur pour l'authentification et la transmission.	**Fournisseur de logiciels** : Indiquer aux clients et aux revendeurs/intégrateurs que, si une technologie sans-fil est utilisée avec l'application de paiement, les transmissions cryptées sécurisées doivent être effectuées conformément à la condition 6.2 de la norme PA-DSS. **Clients et intégrateurs/revendeurs** : Pour la technologie sans-fil utilisée dans l'environnement de paiement par les clients ou les revendeurs/intégrateurs, utiliser des transmissions cryptées conformément au *Guide de mise en œuvre de la norme PA-DSS* et à la condition 6.2 de la norme PA-DSS.
6.3	Donner des instructions concernant l'utilisation sécurisée de la technologie sans-fil.	Donner des instructions pour les paramètres de réseau sans-fil conforme à la norme PCI DSS, y compris : ▪ Instructions relatives au changement des clés de cryptage, mots de passe et les chaînes de communauté SNMP par défaut à l'installation. ▪ Instructions relatives au changement de clés de cryptage, mots de passe et chaînes SNMP, dès lors que quelqu'un qui connaît les clés/mots de passe quitte la société ou change de poste. ▪ Instructions relatives à l'installation d'un pare-feu entre les réseaux sans-fil et les systèmes qui conservent les données de titulaires de carte ; et à la configuration des pare-feu pour qu'ils refusent ou contrôlent tout trafic (si ce trafic est nécessaire à des fins commerciales) entre l'environnement du réseau sans-fil et l'environnement des données de titulaires de carte. ▪ Les instructions relatives à l'utilisation des meilleures pratiques du secteur (par exemple, IEEE 802.11i) pour appliquer un cryptage robuste à l'authentification et la transmission.	**Fournisseur de logiciels** : Indiquer aux clients et aux intégrateurs/revendeurs de sécuriser les technologies sans-fil selon la condition 6.3 de la norme PA-DSS. **Clients et intégrateurs/revendeurs** : Sécuriser les technologies sans-fil selon le *Guide de mise en œuvre de la norme PA-DSS* et la condition 6.2 de la norme PA-DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
7.2.3	Donner des instructions aux clients concernant l'installation sécurisée des correctifs et des mises à jour.	Les informations suivantes doivent être fournies aux clients et aux intégrateurs/revendeurs : • la communication des nouveaux correctifs et mises à jour au fournisseur ; • la mise à disposition sécurisée des correctifs et des mises à jour avec une chaîne de confiance connue ; • le mode d'accès aux correctifs et aux mises à jour, ainsi que leur mode d'installation de manière à assurer l'intégrité des codes correspondants.	**Fournisseur de logiciels :** Documenter et implémenter les processus pour communiquer, livrer et sécuriser l'installation des correctifs et des mises à jour. **Clients et intégrateurs/revendeurs :** Accéder aux correctifs et aux mises à jour, et les installer, de manière sécurisée conformément au *Guide de mise en œuvre de la norme PA-DSS*.
8.2	N'utiliser que les services, protocoles, composants, et matériel et logiciel dépendants nécessaires et sécurisés, y compris ceux fournis par des tiers.	Documenter tous les protocoles, services, composants, et matériel et logiciel dépendants nécessaires aux fonctionnalités de l'application de paiement.	**Fournisseur de logiciels :** S'assurer que l'application de paiement prend en charge l'utilisation par le client des seuls protocoles, services, etc. nécessaires et sécurisés, 1) en ayant uniquement les protocoles, services, etc. nécessaires, établis « prêts à l'emploi » par défaut, 2) en ayant ces protocoles, services, etc. nécessaires, configurés de manière sécurisée par défaut, et 3) en documentant les protocoles, services, etc. nécessaires, à titre de référence pour les clients et revendeurs/intégrateurs. **Clients et intégrateurs/revendeurs :** Utiliser la liste documentée du *Guide de mise en œuvre de la norme PA-DSS* pour garantir que seuls les protocoles, services, etc. nécessaires et sécurisés sont utilisés sur le système, conformément à la condition 5.4 de la norme PA-DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
9.1	Stocker des données de titulaires de carte uniquement sur les serveurs non connectés à Internet	Les informations suivantes doivent être fournies aux clients et aux intégrateurs/revendeurs : ▪ Des instructions stipulant de ne pas stocker de données de titulaires de carte sur les systèmes destinés au public (par exemple, un serveur Web et un serveur de base de données ne doivent pas se trouver sur le même serveur). ▪ Des instructions expliquant comment configurer l'application de paiement pour qu'elle utilise une DMZ pour séparer Internet des systèmes qui trient les données de titulaires de carte. ▪ Une liste des services/ports que l'application a besoin d'utiliser afin de communiquer sur les deux zones du réseau (afin que le client puisse configurer son pare-feu pour ouvrir uniquement les ports requis).	**Fournisseur de logiciel** : S'assurer que l'application de paiement ne requiert pas de stocker des données de titulaires de carte dans la DMZ ou sur des systèmes accessibles via Internet et permettra d'utiliser une DMZ conformément à la condition 9 de la norme PA-DSS. **Clients et intégrateurs/revendeurs** : Établir et maintenir des applications de paiement de façon à ce que les données de titulaires de carte ne soient pas stockées sur des systèmes accessibles par Internet, conformément au *Guide de mise en œuvre de la norme PA-DSS* et à la condition 9 de la norme PA-DSS.
10.1	Implémenter l'authentification à plusieurs facteurs pour tous les accès à distance à l'application de paiement provenant de l'extérieur de l'environnement client.	Apporter les informations suivantes aux clients et aux intégrateurs/revendeurs : ▪ Des instructions stipulant que tous les accès à distance issus de l'extérieur du réseau du client vers l'application de paiement doivent utiliser l'authentification à plusieurs facteurs afin de respecter les conditions de la norme PCI DSS. ▪ Une description des mécanismes d'authentification à plusieurs facteurs pris en charge par l'application. ▪ Des instructions expliquant la configuration de l'application pour prendre en charge l'authentification à plusieurs facteurs (au moins deux des trois méthodes d'authentification décrites à la condition 3.1.4 de la norme PA DSS).	**Fournisseur de logiciel** : Assurer que l'application de paiement prend en charge l'utilisation par le client de l'authentification à plusieurs facteurs pour tous les accès à distance à l'application de paiement qui sont originaires de l'extérieur de l'environnement client, selon la condition 10.2 de la norme PA-DSS. **Clients et intégrateurs/revendeurs** : Établir et maintenir l'authentification à plusieurs facteurs pour tous les accès à distance à l'application de paiement provenant de l'extérieur de l'environnement client, conformément au *Guide de mise en œuvre de la norme PA-DSS* et la condition 10.2 de la norme PA-DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
10.2.1	Livrer les mises à jour des applications de paiement à distance de façon sécurisée.	Si les mises à jour de l'application de paiement sont livrées par un accès distant aux systèmes du client, fournir ce qui suit : ▪ Des instructions pour l'activation des technologies d'accès à distance pour les mises à jour d'application de paiement, uniquement lorsque des téléchargements sont nécessaires, et les désactiver dès que le téléchargement est terminé, conformément à la condition 12.3.9 de la norme PCI DSS. ▪ Des instructions stipulant que, si un ordinateur est connecté par VPN ou autre connexion haut débit, les mises à jour des applications de paiement à distance doivent être reçues à travers un pare-feu ou un produit pare-feu personnel, conformément à la condition 1 de la norme PCI DSS.	**Fournisseur de logiciel** : Livrer les mises à jour des applications de paiement à distance de façon sécurisée, conformément à la condition 10.3 de la norme PA-DSS. **Clients et intégrateurs/revendeurs** : Recevoir des mises à jour des applications de paiement à distance du fournisseur, de façon sécurisée, conformément au *Guide de mise en œuvre de la norme PA-DSS* et aux conditions 10.3 de la norme PA-DSS et 1 de la norme PCI DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
10.2.3	Mettre en œuvre le logiciel d'accès distant de façon sécurisée.	Inclure des instructions selon lesquelles l'accès à l'application de paiement doit être implémenté de manière sécuritaire, par exemple : ▪ Modifier les paramètres par défaut dans le logiciel d'accès distant (par exemple, modifier les mots de passe par défaut et utiliser des mots de passe uniques pour chaque client). ▪ Autoriser les connexions uniquement depuis des adresses IP/MAC connues. ▪ Utiliser une authentification robuste et des mots de passe complexes pour les connexions (voir les conditions 3.1.1 à 3.1.11 de la norme PA-DSS). ▪ Activer la transmission de données cryptées conformément à la condition 12.1 de la norme PA-DSS. ▪ Activer le verrouillage des comptes après un certain nombre de tentatives de connexion infructueuses (voir les conditions 3.1.9 à 3.1.10 de la norme PA-DSS). ▪ Établir une connexion de VPN (réseau virtuel privé) par pare-feu avant que l'accès ne soit autorisé. ▪ Activer la fonction de journalisation. ▪ Limiter l'accès aux environnements de client au personnel autorisé du revendeur/intégrateur.	**Fournisseur de logiciel** : (1) Si le fournisseur peut accéder à distance aux applications de paiement du client, observer les méthodes d'accès à distance sécurisé, telles que celles qui sont spécifiées dans la condition 10.3.2 de la norme PA-DSS. (2) S'assurer que l'application de paiement prend en charge l'utilisation par le client des fonctions de sécurité d'accès distant. **Clients et intégrateurs/revendeurs** : Utiliser les fonctions de sécurité d'accès à distance pour tous les accès distants à l'application de paiement, conformément au *Guide de mise en œuvre de la norme PA-DSS* et à la condition 10.3.2 de la norme PA-DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
11.1	Sécuriser les transmissions de données de titulaires de carte sur les réseaux publics.	Si l'application de paiement envoie ou permet d'envoyer des données de titulaires de carte par des réseaux publics, inclure des instructions sur l'implémentation et l'utilisation d'une cryptographie robuste et de protocoles de sécurité pour une transmission sécurisée des données de titulaires de carte sur les réseaux publics, y compris : ▪ Requérir l'utilisation d'une cryptographie et des protocoles de sécurité robustes si les données de titulaires de carte sont transmises sur des réseaux publics. ▪ Des instructions pour vérifier que seuls des clés/certificats approuvés sont acceptés. ▪ Comment configurer l'application de paiement pour utiliser uniquement des versions sécurisées et des mises en œuvre sécurisées des protocoles de sécurité. ▪ Comment configurer l'application de paiement pour empêcher le repli sur une version ou une configuration non sécurisée (par exemple, si le TLS est utilisé, l'application ne doit pas autoriser le repli sur SSL). ▪ Comment configurer l'application de paiement pour utiliser un cryptage de force adéquate pour la méthodologie de cryptage utilisée.	**Fournisseur de logiciel** : S'assurer que l'application de paiement prend en charge l'utilisation par le client d'une cryptographie et de protocoles de sécurité robustes pour la transmission des données de titulaires de carte sur les réseaux publics, selon la condition 11.1 de la norme PA-DSS. **Clients et intégrateurs/revendeurs** : Établir et maintenir une cryptographie et des protocoles de sécurité robustes pour la transmission des données de titulaires de carte, selon le *Guide de mise en œuvre de la norme PA-DSS* et la condition 11.1 de la norme PA-DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
11.2	Crypter les données de titulaires de carte envoyées via des technologies de messagerie pour les utilisateurs finaux	Si l'application autorise et/ou facilite l'envoi de PAN par des technologies de messagerie pour les utilisateurs finaux, inclure des instructions pour l'implémentation et l'utilisation d'une solution qui rend le PAN illisible ou met en place une cryptographie robuste, y compris : ▪ Des procédures pour utiliser la solution définie pour rendre le PAN illisible ou pour sécuriser le PAN avec une cryptographie robuste. ▪ Des instructions selon lesquelles le PAN doit toujours être rendu illisible ou protégé par une cryptographie robuste chaque fois qu'il est envoyé à l'aide de technologies de messagerie aux utilisateurs finaux.	**Fournisseur de logiciel** : Apporter ou spécifier l'utilisation d'une solution qui rend le PAN illisible ou met en place une cryptographie robuste et garantir que l'application de paiement prend en charge le cryptage, ou rend illisible, les PAN s'ils sont envoyés avec les technologies de messagerie d'utilisateurs finaux, conformément à la condition 11.2 de la norme PA-DSS. **Clients et intégrateurs/revendeurs** : Rendre le PAN illisible ou crypter avec une cryptographie robuste tous les PAN envoyés avec les technologies de messagerie d'utilisateurs finaux, conformément au *Guide de mise en œuvre de la norme PA-DSS* et à la condition 11.2 de la norme PA-DSS.
12.1	Crypter les accès administratifs non-console.	Si l'application de paiement facilite l'accès administratif non console, inclure des instructions stipulant comment configurer l'application pour utiliser une cryptographie robuste pour le cryptage de tous les accès administratifs non console à l'application de paiement ou aux serveurs de l'environnement de données de titulaires de carte.	**Fournisseur de logiciel** : Si l'application de paiement facilite l'accès administratif non console, s'assurer que l'application de paiement utilise une cryptographie robuste pour tous les accès administratifs non console, selon la condition 12.1 de la norme PA-DSS. **Clients et intégrateurs/revendeurs** : Crypter tous les accès administratifs non-console, conformément au *Guide de mise en œuvre de la norme PA-DSS* et à la condition 12.1 de la norme PA-DSS.
12.1.1	Crypter les accès administratifs non-console.	Inclure des instructions pour les clients et les intégrateurs/revendeurs pour qu'ils implémentent une cryptographie robuste pour le cryptage de tous les accès administratifs non console.	**Fournisseur de logiciel** : S'assurer que l'application de paiement prend en charge le cryptage par le client des accès administratifs non console, conformément à la condition 12.1.1 de la norme PA-DSS. **Clients et intégrateurs/revendeurs** : Crypter tous les accès administratifs non console, conformément au *Guide de mise en œuvre de la norme PA-DSS* et à la condition 12.1.1 de la norme PA-DSS.

Conditions de la norme PA-DSS	Section de la norme PA-DSS	Contenu du guide de mise en œuvre	Responsabilité de la mise en œuvre du contrôle
12.2	Utiliser l'authentification à plusieurs facteurs pour tous les membres du personnel dotés d'un accès administratif non-console.	Inclure les instructions pour les clients et les intégrateurs/revendeurs concernant l'utilisation de l'authentification à plusieurs facteurs, y compris ce qui suit : • Instructions spécifiant que l'authentification à plusieurs facteurs est obligatoire pour tous les membres du personnel dotés d'un accès administratif non-console au CDE. • Procédures d'utilisation de l'authentification à plusieurs facteurs fournies avec l'application (le cas échéant).	**Fournisseur de logiciel** : Vérifier que l'application de paiement fournit ou spécifie l'utilisation de l'authentification à plusieurs facteurs pour tous les membres du personnel dotés d'un accès administratif non-console, conformément à la condition 12.2 de la norme PA-DSS. **Clients et intégrateurs/revendeurs** : Utiliser l'authentification à plusieurs facteurs pour tous les membres du personnel dotés d'un accès administratif non console, conformément au *Guide de mise en œuvre de la norme PA-DSS* et à la condition 12.2 de la norme PA-DSS.

Annexe B : Configuration du laboratoire de test pour les évaluations de la norme PA-DSS.

À chaque évaluation PA-DSS réalisée, le PA-QSA doit confirmer le statut et les capacités du laboratoire utilisé pour les tests effectués lors de l'évaluation PA-DSS. Cette confirmation doit être soumise avec le *rapport de validation (ROV)* complété.

Pour chaque procédure de validation de laboratoire, le PA-QSA doit indiquer si le laboratoire utilisé pour l'évaluation et le laboratoire qui entreprend ces procédures de validation était le laboratoire du PA-QSA ou le laboratoire du fournisseur de logiciel. Les PA-QSA doivent maintenir un laboratoire de test qui respecte toutes les exigences mentionnées ci-dessous et utiliser leur propre laboratoire pour conduire les expériences à chaque fois que c'est possible. Le laboratoire du fournisseur de logiciel peut uniquement être utilisé lorsque c'est nécessaire (par exemple, lorsque le PA-QSA ne dispose pas de l'unité centrale, de l'AS400 ou de Tandem avec lesquels fonctionne l'application) et après avoir vérifier que toutes les conditions portant sur les laboratoires sont satisfaites.

Le PA-QSA doit confirmer tous les éléments du tableau ci-dessous, ainsi que :

- **L'identification de l'emplacement et des propriétaires du ou des laboratoires utilisés pour l'examen de la norme PA-DSS**
- **La description du laboratoire d'architecture de test et l'environnement en place pour l'examen de la norme PA-DSS**
- **La description de la manière avec laquelle un usage de l'application en conditions réelles a été simulé dans le laboratoire pour cet examen de la norme PA-DSS**

Le *modèle de rapport PA-DSS ROV* donne les détails sur la validation du laboratoire, qui doivent être mentionnés à chaque examen.

Condition pour le laboratoire	Procédure de conformité du laboratoire
1. Installer l'application de paiement en respectant les instructions d'installation du fournisseur ou la formation assurée au client	**1.** Vérifier que le manuel d'installation du fournisseur ou la formation assurée au client a été appliqué pour procéder à l'installation par défaut de l'application de paiement sur toutes les plates-formes listées dans le rapport PA-DSS pour simuler des expériences client en conditions réelles.
2. Installer et tester toutes les versions de l'application de paiement listées dans le rapport PA-DSS	**2.a** Vérifier que toutes les implémentations courantes (y compris les versions spécifiques à la région/pays) de l'application de paiement à tester ont été installées.
	2.b Vérifier que toutes les plateformes et versions de l'application de paiement ont été testées, y compris tous les composants et toutes les dépendances nécessaires du système.
	2.c Vérifier que toutes les fonctionnalités critiques de l'application de paiement ont été testées pour chaque version.

Condition pour le laboratoire	Procédure de conformité du laboratoire
3. Installer et mettre en œuvre tous les périphériques de sécurité requis par les normes PCI DSS	**3.** Vérifier que tous les systèmes de sécurité requis par les normes PCI DSS (par exemple, un pare-feu et des logiciels antivirus) ont été mis en œuvre sur les systèmes de test.
4. Installer et/ou configurer tous les paramètres de sécurité requis par les normes PCI DSS	**4.** Vérifier que tous les paramètres système, correctifs, etc., ont été implémentés sur des systèmes test pour les systèmes d'exploitation, logiciel de système et applications utilisées par l'application de paiement.
5. Simuler un usage en conditions réelles de l'application de paiement	**5.a** Le laboratoire simule un usage en conditions réelles de l'application de paiement, dont tous les systèmes et applications sur lesquels l'application de paiement est mise en œuvre. Ainsi, la mise en œuvre standard d'une application de paiement peut inclure un environnement client/serveur avec dispositif de point de vente dans la partie accueil de la boutique et un système de back-office ou un réseau d'entreprise. Le laboratoire simule la mise en œuvre globale.
	5.b Le laboratoire utilise uniquement des numéros de cartes de test pour la simulation/les tests, sans avoir recours à de vrais PAN. ***Remarque :*** *Les cartes de test peuvent généralement être obtenues auprès du fournisseur, ou bien d'un processeur ou d'un acquéreur.*
	5.c Le laboratoire exécute les fonctions d'autorisation et/ou de règlement de l'application de paiement et toutes les sorties sont examinées selon le point 6 ci-dessous.
	5.d Le laboratoire et/ou les processus appliquent toutes les sorties générées par l'application de paiement à tous les scénarios possibles, qu'il s'agisse de sorties temporaires, permanentes, de traitement d'erreurs, de mode débogage, de fichiers journaux, etc.
	5.e Le laboratoire et/ou les processus simulent et valident toutes les fonctions de l'application de paiement, afin d'inclure la génération de toutes les conditions d'erreur et de toutes les entrées de journaux en utilisant à la fois des données « réelles » simulées et des données non valides.
6. Fournir les fonctionnalités nécessaires et les tester à l'aide des méthodologies suivantes de test d'intrusion :	**6.a** Utilisation de méthodes/d'outils légaux : Des méthodes/outils légaux ont été utilisés pour analyser toutes les sorties identifiées, afin d'y rechercher la présence de données d'identification sensibles (outils commerciaux, scripts, etc.), conformément aux conditions 1.1.1 à 1.1.3 de la norme PA-DSS.[6]

[6] Méthodes ou outils légaux : Un outil ou une méthode pour découvrir, analyser et présenter les données légales, fournissant un moyen efficace d'authentifier, de rechercher et de découvrir des preuves informatiques rapidement et précisément. Les méthodes et outils légaux utilisés par les PA-QSA doivent localiser

Condition pour le laboratoire	Procédure de conformité du laboratoire
	6.b Tentative d'exploitation des vulnérabilités de l'application : Les vulnérabilités actuelles (par exemple, le Top 10 OWASP, le Top 25 SANS CWE, le codage sécurisé CERT, etc.), ont été utilisées pour tenter d'exploiter la ou les applications de paiement, conformément à la condition 5.2 de la norme PA-DSS.
	6.c Le laboratoire et/ou les processus ont tenté d'exécuter un code arbitraire lors du processus de mise à jour de l'application de paiement : Exécuter le processus de mise à jour avec un code arbitraire, conformément à la condition 7.2.2 de la norme PA-DSS.
7. N'utiliser le laboratoire du fournisseur QU'APRÈS avoir vérifié que toutes les conditions sont satisfaites.	Si l'utilisation du laboratoire du fournisseur de logiciel est nécessaire (par exemple, lorsque le PA-QSA ne dispose pas de l'unité centrale, de l'AS400 ou de Tandem avec lesquels fonctionne l'application), le PA-QSA peut (1) utiliser l'équipement du fournisseur en prêt, ou (2) utiliser l'installation de laboratoire du fournisseur, tant que cet arrangement est mentionné dans le rapport, ainsi que l'emplacement des tests. Dans un cas comme dans l'autre, le PA-QSA vérifie que les équipements et le laboratoire du fournisseur répondent aux exigences suivantes :
	7.a Le PA-QSA vérifie que le laboratoire du fournisseur répond à toutes les exigences spécifiées dans ce document et consigne les détails dans le rapport.
	7.b Le PA-QSA doit valider l'installation appropriée du laboratoire afin de garantir que celui-ci simule vraiment une situation en conditions réelles et que le fournisseur ne l'a pas modifié ni altéré cet environnement d'aucune façon.
	7.c Tous les tests sont réalisés par le PA-QSA (le fournisseur ne peut pas faire de tests de sa propre application).
	7.d Tous les tests sont soit (1) réalisés sur site dans les locaux du fournisseur, soit (2) réalisés à distance via une connexion réseau utilisant une liaison sécurisée (par exemple, un VPN).
	7.e Seuls des numéros de cartes de test sont utilisés pour la simulation/les tests, sans avoir recours à de vrais PAN. Ces cartes de test peuvent généralement être obtenues auprès du fournisseur, ou bien d'un processeur ou d'un acquéreur.
8. Maintenir un processus efficace d'assurance qualité (QA).	**8.a** Le personnel QA du PA-QSA vérifie que toutes les plateformes identifiées dans le rapport PA-DSS ont été incluses dans les tests.

avec précision toute donnée d'identification sensible écrite par l'application de paiement. Ces outils peuvent être distribués dans le commerce, libres ou développés en interne par les PA-QSA.

Condition pour le laboratoire	Procédure de conformité du laboratoire
	8.b Le personnel QA du PA-QSA vérifie que toutes les conditions de la norme PA-DSS ont été testées.
	8.c Le personnel QA du PA-QSA vérifie que les conditions et processus du laboratoire de PA-QSA respectent les exigences et ont été documentés avec précision dans le rapport.
	8.d Le personnel QA du PA-QSA vérifie que le rapport rend compte précisément des résultats des tests.