Industrie des cartes de paiement (PCI)

Norme de sécurité des données (DSS) et Norme de sécurité des données d'application de paiement (PA-DSS)

Glossaire des termes, abréviations et acronymes

Version 3.2

Avril 2016

Terme	Définition
AAA	Acronyme d'« authentication, authorization, and accounting » (authentification, autorisation et traçabilité). Protocole permettant d'authentifier un utilisateur en fonction de son identité vérifiable, d'autoriser un utilisateur en fonction de ses droits d'utilisateur et de vérifier la consommation des ressources réseau d'un utilisateur.
Contrôle d'accès	Mécanisme limitant la disponibilité des informations ou des ressources de traitement des informations aux seules personnes ou applications autorisées.
Données de compte	Les données de compte sont constituées des données du titulaire de carte et/ou des données d'authentification sensibles. Voir *Données de titulaires de cartes* et *Données d'authentification sensibles.*
Numéro de compte	Voir *Numéro de compte primaire (PAN).*
Acquéreur	Également dénommé « banque du commerçant », « banque d'acquisition », ou « institution financière d'acquisition ». Entité, généralement une institution financière, qui traite les transactions par carte de paiement pour les commerçants et est définie par une marque de carte de paiement en tant qu'acquéreur. Les acquéreurs sont soumis aux procédures et règles de la marque de carte de paiement en ce qui concerne la conformité du commerçant. Voir également *Service de traitement de paiement.*
Accès administratif	Privilèges élevés ou accrus accordés à un compte afin que ce compte puisse gérer des systèmes, des réseaux et/ou des applications. L'accès administratif peut être assigné au compte d'une personne ou à un compte système intégré. Les comptes ayant un accès administratif sont souvent appelés « super-utilisateur », « racine », « administrateur », « admin », « sysadmin » ou « état-superviseur », en fonction du système d'exploitation donné et de la structure organisationnelle.
Adware	Encore appelé publiciel, ce type de logiciel malveillant, une fois installé, force un ordinateur à afficher ou télécharger des publicités de façon automatique.
Æ	Acronyme d'« Advanced Encryption Standard », norme de cryptage avancé. Chiffrement par bloc utilisé dans un système cryptographique symétrique, adopté par le NIST en novembre 2001 comme algorithme de la FIPS PUB 197 américaine (ou « FIPS 197 »). Voir *Cryptographie robuste.*
ANSI	Acronyme d'« American National Standards Institute », Institut national américain de normalisation Organisation privée à but non lucratif qui administre et coordonne le système de normalisation volontaire et d'évaluation de la conformité aux États-Unis.
Antivirus	Programme ou logiciel capable de détecter, de supprimer et d'assurer une protection contre diverses formes de codes ou de logiciels malveillants (également appelés « maliciels »), notamment les virus, vers, chevaux de Troie, spywares ou logiciels espions, adware ou publiciel et outils de dissimulation d'activité.

Terme	Définition
AOC	Acronyme d'« attestation of compliance », attestation de conformité. L'AOC est un formulaire permettant aux commerçants et aux prestataires de service d'attester les résultats d'une évaluation PCI DSS, ainsi qu'il est documenté dans le questionnaire d'auto-évaluation ou le rapport de conformité.
AOV	Acronyme d'« attestation of validation », attestation de validation. L'AOV est un formulaire permettant aux PA-QSA d'attester les résultats d'une évaluation PA-DSS, ainsi qu'il est documenté dans le rapport PA-DSS sur la validation.
Application	Ce terme regroupe tous les programmes ou groupes de programmes logiciels achetés et personnalisés, y compris les applications internes et externes (Internet, par exemple).
ASV	Acronyme d'« Approved Scanning Vendor », prestataire de services d'analyse agréé. Société agréée par le PCI SSC pour offrir des services d'analyse des vulnérabilités externes.
Journal d'audit	Également appelé « vérification à rebours ». Enregistrement chronologique des activités du système. Il fournit un suivi vérifiable et indépendant suffisant pour autoriser la reconstitution, la vérification et l'examen de l'ordre des environnements et activités impliqués dans une opération, une procédure ou un événement lors d'une transaction, du début au résultat final.
Vérification à rebours	Voir *Journal d'audit.*
Authentification	Processus de vérification de l'identité d'une personne, d'un dispositif ou d'un processus. L'authentification se fait généralement par l'utilisation d'un ou plusieurs facteurs d'authentification, tels que : ▪ 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.
Éléments d'authentification	Combinaison de l'ID utilisateur ou de l'ID compte et du ou des facteurs d'authentification utilisés pour authentifier une personne, un dispositif ou un processus,
Autorisation	Dans le contexte du contrôle d'accès, l'autorisation est la concession d'un droit d'accès ou d'autres droits à un utilisateur, programme ou processus. L'autorisation définit ce qu'une personne ou un programme peuvent effectuer après une authentification réussie. Dans le cadre d'une transaction par carte de paiement, l'autorisation est donnée lorsque le commerçant reçoit l'approbation de la transaction une fois que l'acquéreur a validé la transaction avec l'émetteur/le processeur.
Sauvegarde	Copie de données en double réalisée à des fins d'archivage ou de protection contre d'éventuels dommages ou pertes.

Terme	Définition
BAU	Un acronyme pour « business as usual », activités d'affaires courantes. Le BAU est constitué par les opérations commerciales normales d'une organisation.
Bluetooth	Protocole sans fil utilisant la technologie des communications à courte portée afin de faciliter la transmission de données sur de courtes distances.
Saturation de la mémoire tampon	Une vulnérabilité qui est créée par des méthodes de codage non sécurisées, lorsqu'un programme sature la limite de la mémoire tampon et inscrit des données dans un espace de mémoire adjacent. Les saturations de mémoire tampon sont utilisées par les pirates pour obtenir un accès non autorisé aux systèmes ou aux données.
Appareil de clonage de carte	Un appareil physique, souvent fixé à un appareil de lecture de carte légitime, conçu pour capturer illégalement et/ou stocker les informations d'une carte de paiement.

Terme	Définition
Valeur ou code de validation de carte	Également connus comme code de sécurité ou de vérification de la carte. Concerne soit : (1) les données de bande magnétique, soit (2) les fonctions de sécurité imprimées. (1) Élément de données sur la bande magnétique d'une carte qui font appel à un processus cryptographique sécurisé pour protéger l'intégrité des données figurant sur la bande et révélant une altération ou contrefaçon. Selon la marque de la carte de paiement, on s'y réfère à l'aide des acronymes CAV, CVC, CVV ou CSC. La liste suivante indique les termes utilisés par chaque marque de carte de paiement : ▪ **CAV –** valeur d'authentification de carte (Card Authentication Value) (cartes JCB) ▪ **PAN CVC –** code de validation de carte (Card Validation Code) (cartes MasterCard) ▪ **CVV –** valeur de vérification de carte (Card Verification Value) (cartes Visa et Discover) ▪ **CSC –** code de sécurité de carte (Card Security Code) (American Express) (2) Pour les cartes de paiement Discover, JCB, MasterCard et Visa, le deuxième type de valeur ou de code de vérification de carte est constitué des trois chiffres imprimés à droite de l'espace signature au dos de la carte. Pour les cartes American Express, le code est un numéro à quatre chiffres imprimé (non gravé) au-dessus du PAN, au recto de la carte. Le code est attribué de manière unique à chaque carte en plastique et relie le PAN à cette carte plastique. La liste suivante indique les termes utilisés par chaque marque de carte de paiement : ▪ **CID –** numéro d'identification de carte (Card Identification Number) (cartes American Express et Discover) ▪ **CAV2 –** valeur d'authentification de carte 2 (Card Authentication Value 2) (cartes JCB) ▪ **PAN CVC2 –** code de validation de carte 2 (Card Validation Code 2) (cartes MasterCard) ▪ **CVV2 –** valeur de vérification de carte 2 (Card Verification Value 2) (cartes Visa)
Titulaire de carte	Client consommateur ou non auquel une carte de paiement est délivrée ou toute personne autorisée à utiliser la carte de paiement.
Données du titulaire	Les données du titulaire de carte sont constituées, au minimum, de l'intégralité du PAN. Les données de titulaire de carte peuvent également apparaître sous la forme de la totalité du PAN plus l'un des éléments suivants : nom du titulaire de carte, date d'expiration et/ou code service. Voir *Données d'authentification sensibles* pour les éléments de données supplémentaires pouvant être transmis ou traités (mais non stockés) dans le cadre d'une transaction de paiement.

Terme	Définition
CDE	Acronyme de « cardholder data environment », environnement des données de titulaire de carte. Les personnes, les processus et les technologies qui stockent, traitent ou transmettent les données de titulaires de cartes ou des données d'authentification sensibles.
Technologies cellulaires	Les communications mobiles par les réseaux téléphoniques sans fil, y compris notamment le Système Global pour communication Mobile (GSM), Code division accès multiple (CDMA) et Service radio paquet général (GPRS).
CERT	Acronyme de « Computer Emergency Response Team », équipe d'urgence de l'Internet, de l'Université Carnegie Mellon. Le programme CERT développe et promeut l'utilisation des technologies et des pratiques de gestion des systèmes appropriées pour résister aux attaques sur des systèmes en réseau, afin de limiter les dommages, et d'assurer la continuité des services essentiels.
Contrôle de changement	Les processus et procédures à examiner, tester et pour approuver les changements apportés aux systèmes et logiciels en termes d'impact avant l'implémentation.
CIS	Acronyme de « Center for Internet Security », centre de sécurité Internet. Entreprise à but non lucratif dont la mission est d'aider les organisations à réduire les risques de perturbations commerciales et du commerce électronique résultant de contrôles techniques de sécurité inappropriés.
Cryptage de base de données au niveau de colonne	Technique ou technologie (matérielle ou logicielle) de cryptage du contenu d'une colonne spécifique de la base de données au lieu de la totalité du contenu de la base de données. Voir également *Cryptage de disque* ou *Cryptage au niveau fichier.*
Contrôles compensatoires	Il est possible d'envisager des contrôles compensatoires lorsqu'une entité ne peut pas remplir une condition exactement comme elle est stipulée, en raison de contraintes techniques légitimes ou de contraintes commerciales documentées, mais qu'elle a suffisamment atténué les risques associés par la mise en œuvre d'autres contrôles. Les contrôles compensatoires doivent : (1) Respecter l'intention et la rigueur de la condition initiale de la norme PCI DSS ; (2) Fournir une protection similaire à celle de la condition initiale de la norme PCI DSS ; (3) Excéder les autres conditions de la norme PCI DSS (et non être en simple conformité aux autres conditions de la norme). (4) Correspondre aux risques supplémentaires qu'implique la non-conformité à la condition de la norme PCI DSS. Voir les annexes B et C sur les « contrôles compensatoires » dans les *Conditions et procédures d'évaluation de sécurité PCI DSS* pour plus d'informations sur leur utilisation.

Terme	Définition
Incident de sécurité	Également dénommé « compromission des données » ou « atteinte à la protection des données ». Intrusion dans un système informatique lorsque l'on soupçonne une divulgation/un vol, une modification ou la destruction non autorisés des données du titulaire de carte.
Console	Écran et clavier permettant l'accès et le contrôle d'un serveur, d'un ordinateur central ou de tout autre type de système dans un environnement de réseau.
Consommateur	Personne achetant des marchandises ou des services, ou les deux.
Systèmes stratégiques / technologies stratégiques	Un système ou une technologie considéré par l'entité comme étant d'une importance particulière. Par exemple, un système stratégique peut être essentiel pour l'exécution d'une opération commerciale ou pour maintenir une fonction de sécurité. Les exemples de systèmes stratégiques incluent souvent les systèmes de sécurité, les dispositifs et systèmes ouverts au public, les bases de données et systèmes qui stockent, traitent ou transmettent des données du titulaire. Les facteurs à prendre en compte pour déterminer quels systèmes et technologies spécifiques sont essentiels dépendront de l'environnement de l'organisation et de la stratégie d'évaluation des risques.
Attaques Cross-Site Request Forgery (CSRF)	Vulnérabilité qui est créée par des méthodes de codage non sécurisées qui permettent l'exécution d'actions indésirables au moyen d'une session d'authentification. Souvent utilisées avec une injection XSS et/ou SQL.
Attaques Cross-Site Scripting (XSS)	Vulnérabilité qui est créée par des techniques de codage non sécurisées, ce qui provoque la validation d'une entrée incorrecte. Souvent utilisées avec une injection CSRF et/ou SQL.
Clés cryptographiques	Une valeur déterminant le résultat d'un algorithme de cryptage lorsqu'il transforme un texte clair en cryptogramme. La longueur de la clé détermine généralement le degré de difficulté du décryptage du cryptogramme d'un message donné. Voir *Cryptographie robuste.*

Terme	Définition
Génération de clés cryptographiques	La génération de clés est l'une des fonctions au sein de la gestion des clés. Les documents suivants fournissent des indications reconnues sur la génération appropriée de clés : • Publication spéciale NIST 800-133 : Recommandations concernant la génération de clés cryptographiques • Services financiers ISO 11568-2 — Gestion des clés (détail) — Partie 2 : Chiffrements symétriques, leur gestion des clés et cycle de vie o 4.3 Génération de clés • Services financiers ISO 11568-4 — Gestion des clés (détail) — Partie 4 : Cryptosystèmes asymétriques — Gestion des clés et cycle de vie o 6.2 Étapes du cycle de vie des clés — Génération • Conseil européen des paiements EPC 342-08 Directives sur l'utilisation des algorithmes et la gestion des clés o 6.1.1 Génération de clés [pour les algorithmes symétriques] o 6.2.1 Génération de clés [pour les algorithmes asymétriques]
Gestion de clé cryptographique	L'ensemble des mécanismes et processus qui prennent en charge l'établissement et la maintenance des clés, notamment le remplacement d'anciennes clés par des nouvelles, le cas échéant.
Cryptographie	Discipline mathématique et informatique concernant la sécurité des informations, en particulier le cryptage et l'authentification. Dans le cadre des applications et de la sécurité du réseau, la cryptographie est un outil de contrôle d'accès, de confidentialité et d'intégrité de l'information.
Cryptopériode	Durée pendant laquelle une clé cryptographique spécifique peut être utilisée selon l'objectif défini, par exemple, par une période définie et/ou la quantité de texte chiffré produite, conformément aux directives et aux meilleures pratiques du secteur (par exemple, la *publication spéciale NIST 800-57*).
CVSS	Acronyme de « Common Vulnerability Scoring System », système de notation de vulnérabilité courante. Une norme ouverte de l'industrie indépendante des fournisseurs conçue pour retranscrire la sévérité des vulnérabilités des systèmes de sécurité informatiques et pour aider à déterminer l'urgence et la priorité de la réponse. Consultez le *Guide du programme ASV* pour de plus amples informations.
Diagramme de flux des données	Un diagramme qui présente les flux de données dans une application, un système ou un réseau.
Base de données	Format structuré pour l'organisation et la conservation d'informations facilement récupérables. Les tables et tableurs sont des exemples de bases de données simples.
Administrateur de base de données	Également dénommé « DBA ». Personne responsable de la gestion et de l'administration des bases de données.

Terme	Définition
Compte par défaut	Compte de connexion prédéfini dans un système, une application ou un dispositif, permettant l'accès au système lors de sa mise en service initiale. Des comptes par défaut supplémentaires peuvent également être générés par le système dans le cadre du processus d'installation.
Mot de passe par défaut	Mot de passe d'administration de système, d'utilisateur ou de service prédéfinis dans un système, une application ou un dispositif, ordinairement associé à un compte par défaut. Les comptes et mots de passe par défaut sont publiés et bien connus, et par conséquent, facilement devinés.
Démagnétisation	Également nommé « démagnétisation de disque ». Processus ou technique qui démagnétisent le disque, de sorte que toutes les données qui y sont stockées soient supprimées de façon permanente.
Dépendance	Dans le contexte de PA-DSS, une dépendance est un logiciel spécifique, ou un composant matériel (tel qu'un terminal matériel, une base de données, un système d'exploitation, API, librairie de codes, etc.) qui est nécessaire pour la conformité de l'application de paiement aux conditions de la norme PA-DSS.
Cryptage par disque	Technique ou technologie (logicielle ou matérielle) de cryptage de toutes les données stockées sur un dispositif (par exemple, disque dur ou clé USB). Le *cryptage au niveau fichier* ou le *cryptage de base de données au niveau colonne* sont également utilisés pour crypter le contenu de fichiers ou de colonnes spécifiques.
DMZ	Abréviation de « demilitarized zone », zone démilitarisée. Sous-réseau physique ou logique qui ajoute une couche de sécurité supplémentaire au réseau privé interne d'une organisation. La zone démilitarisée ajoute une couche supplémentaire de sécurité réseau entre Internet et le réseau interne d'une organisation, de sorte que les tiers externes puissent se connecter directement aux dispositifs de la zone démilitarisée, sans avoir accès à l'ensemble du réseau interne.
DNS	Acronyme de « Domain Name System » ou « domain name server », serveur de nom de domaine. Système stockant des informations associées à des noms de domaines dans une base de données distribuée sur des réseaux comme Internet.
DSS	Acronyme de « Data Security Standard », norme de sécurité des données. Voir *PA-DSS* et *PCI DSS.*
Double contrôle	Processus d'utilisation de deux ou plusieurs entités distinctes (habituellement des personnes) opérant de concert pour protéger des fonctions ou des informations sensibles. Les deux entités sont également responsables de la protection physique des documents impliqués dans des transactions vulnérables. Aucun individu n'est autorisé à accéder seul aux supports (par exemple, une clé cryptographique) ni à les utiliser. Pour la génération manuelle, le transfert, le chargement, le stockage et la récupération de clés, le double contrôle exige un partage des connaissances des clés entre les entités concernées. (Voir également *Connaissance partagée*).

Terme	Définition
Filtrage des paquets dynamique	Voir *Contrôle avec état.*
ECC	Acronyme d'« Elliptic Curve Cryptography », cryptographie sur les courbes elliptiques. Approche de la cryptographie à clé publique basée sur des courbes elliptiques sur des champs finis. Voir *Cryptographie robuste.*
Filtrage de sortie	Méthode de filtrage du trafic sortant du réseau, de sorte que seul le trafic explicitement autorisé ait l'autorisation de quitter le réseau.
Cryptage	Processus de conversion d'informations sous une forme inintelligible, sauf pour les détenteurs de la clé cryptographique spécifique. L'utilisation du cryptage protège les informations entre les processus de cryptage et de décryptage (l'inverse du cryptage) contre toute divulgation non autorisée. Voir *Cryptographie robuste.*
Algorithme de cryptage	Également nommé « algorithme cryptographique ». Séquence d'instructions mathématiques utilisée pour transformer un texte ou des données non cryptées en texte ou données cryptées, et vice-versa. Voir *Cryptographie robuste.*
Entité	Terme utilisé pour représenter l'entreprise, l'organisation ou la société qui fait l'objet d'une vérification de sa conformité à la norme PCI DSS.
Contrôle de l'intégrité des fichiers	Technique ou technologie selon laquelle certains fichiers ou journaux sont contrôlés afin de détecter une éventuelle modification. Lorsque des fichiers ou des journaux critiques sont modifiés, des alertes doivent être envoyées au personnel de sécurité approprié.
Cryptage au niveau fichier	Technique ou technologie (logicielle ou matérielle) de cryptage de la totalité du contenu de fichiers spécifiques. Voir également *Cryptage par disque* ou *Cryptage de la base de données au niveau colonne.*
FIPS	Acronyme de « Federal Information Processing Standards », normes fédérales de traitement de l'information. Normes de traitement des informations, publiquement reconnues par le gouvernement fédéral américain ; également utilisées par les organismes non gouvernementaux et les sous-traitants.
Pare-feu	Technologie matérielle et/ou logicielle protégeant les ressources réseau contre les accès non autorisés. Un pare-feu autorise ou bloque le trafic informatique circulant entre des réseaux de différents niveaux de sécurité, selon un ensemble de règles et d'autres critères.
Informatique légale	Également dénommé « expertise judiciaire en informatique ». S'appliquant à la sécurité des informations, les outils d'investigation et de techniques d'analyse permettent de rassembler des preuves à partir des ressources informatiques afin de déterminer la cause de la compromission des données.

Terme	Définition
FTP	Acronyme de « File Transfer Protocol », protocole de transfert de fichiers. Protocole réseau utilisé pour transférer les données d'un ordinateur à un autre par l'intermédiaire d'un réseau public, comme Internet. Le FTP est très largement considéré comme un protocole non sécurisé, car les mots de passe et le contenu des fichiers sont envoyés sans protection et en texte clair. Le FTP peut être mis en œuvre de manière sécurisée par le protocole SSH ou une autre technologie. Voir *S-FTP*.
GPRS	Acronyme de « General Packet Radio Service », service général de paquets radio. Service de données mobile, à la disposition des utilisateurs de téléphones mobiles GSM. Reconnu pour l'utilisation efficace d'une largeur de bande limitée. Particulièrement adapté pour l'envoi et la réception de petits paquets de données, comme des courriers électroniques ou la navigation sur Internet.
GSM	Acronyme de « Global System for Mobile Communications », système global de communication mobile. Normes populaires pour les téléphones et les réseaux mobiles. L'omniprésence du système GSM facilite considérablement l'itinérance internationale entre opérateurs de téléphonie mobile, permettant aux abonnés d'utiliser leur téléphone dans de nombreuses régions du monde.
Hachage	Processus qui consiste à rendre des données de titulaire de carte illisibles en les convertissant en un message condensé de longueur fixe. . Le hachage est une fonction unilatérale (mathématique) dans laquelle un algorithme non secret acquiert en entrée un message de longueur aléatoire et produit une sortie de longueur fixe (généralement appelé « code de hachage » ou « empreinte cryptographique »). Une fonction de hachage doit avoir les propriétés suivantes : (1) Il doit être impossible de déterminer, à l'aide de l'informatique, une entrée initiale donnée avec uniquement le code de hachage, (2) Il doit être impossible de trouver, à l'aide de l'informatique, deux entrées donnant le même code de hachage. Dans le cadre de la norme PCI DSS, le hachage doit être appliqué à la totalité du PAN entier pour que le code de hachage soit considéré comme illisible. Il est recommandé d'inclure une entrée variable à la fonction de hachage (par exemple, un « sel ») pour les données de titulaire de carte hachées afin de réduire ou de vaincre l'efficacité des tableaux d'attaque arc-en-ciel précalculés (voir *variable d'entrée*). Pour plus de précisions, reportez-vous aux normes du secteur telles que les versions actuelles des publications spéciales NIST 800-107 et 800-106, la Federal Information Processing Standard (FIPS) (norme fédérale de traitement de l'information) norme de hachage sécurisé (SHS) 180-4, et la norme FIPS 202 SHA-3 : Hachage basé sur la permutation et fonctions de rendement extensible.
Hôte	Principal matériel informatique sur lequel le logiciel réside.

Terme	Définition
Fournisseur d'hébergement	Offre des services divers à des commerçants et autres prestataires de services. Ces services varient des plus simples aux plus complexes : du partage d'espace sur un serveur à une gamme complète d'options de « caddie », des applications de paiement aux passerelles et processeurs de paiement, ainsi que l'hébergement réservé à un seul client par serveur. Un fournisseur d'hébergement peut être un fournisseur d'hébergement partagé hébergeant plusieurs entités sur un même serveur.
HSM	Acronyme de « hardware security module », module de sécurité matérielle ou « host security module », module de sécurité hôte. Un dispositif matériel protégé physiquement et logiquement qui offre un ensemble sécurisé de services cryptographiques utilisé pour les fonctions de gestion de clé cryptographique et/ou le décryptage des données de compte.
HTTP	Acronyme de « hypertext transfer protocol », protocole de transfert hypertexte. Protocole Internet ouvert pour le transfert ou la transmission de renseignements sur le Web.
HTTPS	Acronyme de « hypertext transfer protocol over secure socket layer », protocole de transfert hypertexte sur couche de socket sécurisée. Protocole HTTP sécurisé fournissant une authentification et une communication cryptée sur le Web, conçu pour les communications de sécurité sensible, comme les connexions en ligne.
Hyperviseur	Logiciel ou firmware responsable d'héberger et gérer des ordinateurs virtuels. Dans le cadre de la conformité à la norme PCI DSS, le composant du système hyperviseur comprend également le moniteur de l'ordinateur virtuel (VMM).
ID	Identifiant d'un utilisateur ou d'une application spécifiques.
IDS	Acronyme d'« intrusion detection system », système de détection d'intrusion. Logiciel ou matériel utilisé pour identifier les tentatives d'intrusion dans un réseau ou un système et donner l'alerte. Constitué de capteurs qui génèrent des événements de sécurité, d'une console pour la surveillance des événements et des alertes et le contrôle des capteurs, ainsi que d'un moteur central qui enregistre dans une base de données les événements consignés par les capteurs. Utilise un système de règles pour déclencher des alertes en réponse aux événements de sécurité détectés. Voir *IPS*
IETF	Acronyme d'« Internet Engineering Task Force », équipe d'ingénierie Internet. Grande communauté internationale ouverte de concepteurs, opérateurs, fournisseurs de réseau et de chercheurs concernés par l'évolution de l'architecture et le bon fonctionnement d'Internet. L'IETF ne comporte aucune adhésion formelle et est ouvert à tous les individus intéressés.
IMAP	Acronyme d'« Internet Message Access Protocol », protocole d'accès aux messages Internet. Un protocole Internet de couche d'application qui permet à un client e-mail d'accéder aux e-mails sur un serveur de messagerie distant.

Terme	Définition
Token d'index	Élément cryptographique qui remplace le PAN en fonction d'un index déterminé pour donner une valeur imprévisible.
Sécurité des informations	Protection des informations pour garantir la confidentialité, l'intégrité et la disponibilité.
Système d'information	Ensemble distinct de ressources de données structurées pour la collecte, le traitement, la maintenance, l'utilisation, le partage, la diffusion ou l'élimination des informations.
Filtrage d'entrée	Méthode de filtrage du trafic entrant du réseau, de sorte que seul le trafic explicitement autorisé ait l'autorisation d'entrer sur le réseau.
Défauts d'injection	Vulnérabilité qui est créée par des techniques de codage non sécurisées, ce qui provoque la validation d'une entrée incorrecte qui permet aux pirates de relayer des codes malveillants par une application Web au système sous-jacent. Cette classe de vulnérabilité comprend les injections SQL, les injections LDAP et les injections XPath.
Variable d'entrée	Chaîne de données aléatoires qui est concaténée avec des données de source avant qu'une fonction de hachage unilatérale ne soit appliquée. Les variables d'entrée peuvent réduire l'efficacité des attaques de tableaux arc-en-ciel. Voir aussi *hachage* et *tableaux arc-en-ciel.*
Protocole/service/port non sécurisé	Protocole, service ou port introduisant des problèmes de sécurité à cause du manque de contrôles de confidentialité et/ou d'intégrité. Ces problèmes de sécurité concernent les services, protocoles ou ports qui transmettent des données et des éléments d'authentification (par ex., mots/phrase de passe) en texte clair sur Internet ou qui autorisent facilement une exploitation par défaut ou en cas de mauvaise configuration. Les exemples de services non sécurisés comprennent notamment les protocoles FTP, Telnet, POP3, IMAP et SNMP v1 et v2.
IP	Acronyme d'« Internet protocol », protocole Internet. Protocole de couche réseau contenant des informations d'adresse et de contrôle permettant l'acheminement des paquets et leur livraison de l'hôte source à l'hôte destination. Le protocole IP est le principal protocole de couche réseau dans la suite du protocole Internet. Voir *TCP*.
Adresse IP	Également nommé « adresse de protocole Internet ». Code numérique identifiant de manière unique un ordinateur (hôte) sur Internet.
Usurpation d'adresse IP	Technique d'attaque utilisée pour obtenir un accès non autorisé à des réseaux ou des ordinateurs. L'individu malveillant envoie des messages trompeurs à un ordinateur avec une adresse IP indiquant que le message provient d'un hôte de confiance.
IPS	Acronyme d'« intrusion prevention system », système de prévention d'intrusion. Au-delà de l'IDS, un ISP prend la mesure plus poussée de bloquer la tentative d'intrusion.

Terme	Définition
IPSEC	Abréviation de « Internet Protocol Security », sécurité du protocole Internet. Norme pour sécuriser les communications IP au niveau du réseau en cryptant et/ou authentifiant l'ensemble des paquets IP dans une session de communication.
ISO	Dans le cadre des normes et des meilleures pratiques du secteur, ISO, mieux connue sous son nom complet « International Organization for Standardization » ou Organisation internationale de normalisation, est une organisation non gouvernementale constituée par un réseau des instituts nationaux de normalisation.
Émetteur	Entité qui émet des cartes de paiement ou effectue, permet ou prend en charge des services d'émission comprenant, mais sans s'y limiter, les banques et processeurs émetteurs. Également appelé « banque émettrice » ou « établissement financier émetteur ».
Services d'émission	L'autorisation et la personnalisation de la carte sont des exemples de services d'émission.
LAN	Acronyme de « local area network », réseau local. Groupe d'ordinateurs et/ou d'autres dispositifs qui partagent une ligne de communication commune, souvent dans un bâtiment ou un groupe de bâtiments.
LDAP	Acronyme de « Lightweight Directory Access Protocol », protocole d'accès au référentiel allégé. Référentiel de données d'authentification et d'autorisation, utilisé pour demander et modifier des autorisations utilisateurs et accorder l'accès à des ressources protégées.
Moindre privilège	Le fait d'avoir l'accès et/ou les privilèges minimums pour effectuer les rôles et les responsabilités de la fonction du travail.
Journal	Voir *Journal d'audit.*
LPAR	Abréviation de « logical partition », partition logique. Système de subdivision, ou cloisonnement, de toutes les ressources d'un ordinateur – processeurs, mémoire et espace de stockage – en unités plus petites capables de fonctionner avec leur propre copie distincte du système d'exploitation et des applications. La partition logique est généralement utilisée pour permettre l'utilisation de différents systèmes d'exploitation et d'applications sur un même dispositif. La partition logique peut ou non être configurée pour communiquer avec chacune des autres ressources, ou partager certaines ressources du serveur, comme des interfaces réseau.
MAC	En cryptographie, un acronyme de « message authentication code », code d'authentification de message. Un élément d'information utilisé pour authentifier un message. Voir *Cryptographie robuste.*
Adresse MAC	Abréviation de « media access control address », adresse de contrôle d'accès au support. Valeur d'identification unique, attribuée par les fabricants aux adaptateurs et cartes d'interface réseau.
Données de bande magnétique	Voir *Données de piste.*

Terme	Définition
Mainframe	Ordinateurs conçus pour traiter de très gros volumes d'entrées et de sorties de données et mettre l'accent sur le rendement informatique. Les systèmes mainframe sont capables d'exécuter plusieurs systèmes d'exploitation, fonctionnant comme un ensemble de plusieurs ordinateurs. De nombreux anciens systèmes sont équipés d'un système mainframe.
Logiciel malveillant/maliciel	Logiciel ou firmware conçu pour infiltrer ou endommager un système informatique sans l'approbation ou la connaissance de son propriétaire, avec l'intention de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications ou du système d'exploitation du propriétaire. Ce type de logiciel s'introduit généralement dans un réseau au cours d'activités approuvées par l'entreprise, et exploite les vulnérabilités du système. Les virus, les chevaux de Troie, les logiciels spyware et adware et les outils de dissimulation d'activité en sont des exemples.
Masquage	Dans le cadre de la norme PCI DSS, il s'agit d'une méthode occultant un segment de données lorsque celles-ci sont affichées ou imprimées. Le masquage est utilisé lorsqu'il n'existe aucune justification professionnelle d'afficher le PAN dans son intégralité. Le masquage concerne la protection du PAN lorsque celui-ci est affiché ou imprimé. Voir *Troncature* pour la protection du PAN lorsqu'il est stocké dans des fichiers, bases de données, etc.
Attaques de grattage de mémoire	Une activité de logiciel malveillant qui examine et extrait les données demeurant dans la mémoire lorsqu'elle son traitées ou qui n'ont pas été correctement rejetées ou écrasées.
Commerçant	Dans le cadre de la norme PCI DSS, un commerçant est défini comme une entité qui accepte des cartes de paiement portant le logo de l'un des cinq membres du PCI SSC (American Express, Discover, JCB, MasterCard ou Visa) comme moyen de paiement de marchandises et/ou de services. Noter qu'un commerçant qui accepte ces cartes de paiement pour acheter des marchandises et/ou des services peut également être un prestataire de services, si les services vendus ont pour résultat le stockage, le traitement ou la transmission des données de titulaires de cartes au nom d'autres commerçants ou prestataires de services. Par exemple, un ISP est un commerçant qui accepte les cartes de paiement pour la facturation mensuelle, mais aussi un prestataire de services s'il héberge des commerçants en tant que clients.
CP/CT	Acronyme pour « Commande postale/commande par téléphone ».
Contrôle	Utilisation de systèmes ou de processus surveillant en permanence les ressources informatiques ou réseau afin d'alerter le personnel en cas de coupure d'alimentation, d'alarmes ou d'autres événements prédéfinis.
MPLS	Acronyme de « multi protocol label switching », commutation d'étiquettes multi-protocoles. Réseau et mécanisme de télécommunications, conçus pour la connexion d'un groupe de réseaux à commutation par paquets.

Terme	Définition
Authentification à plusieurs facteurs	Méthode d'authentification d'un utilisateur par la vérification d'au moins deux facteurs. Ces facteurs sont constitués d'un élément que possède l'utilisateur (comme une carte à puce ou une clé de sécurité), d'un élément que l'utilisateur connaît (comme un mot de passe, une locution de passage ou un code PIN), ou d'un élément qui identifie ou que fait l'utilisateur effectue (comme une empreinte digitale ou autre forme de mesure biométrique, etc.).
NAC	Acronyme de « network access control », contrôle d'accès au réseau, ou « network admission control », contrôle d'admission au réseau. Une méthode d'implémentation de la sécurité au niveau du réseau en réduisant la disponibilité des ressources du réseau aux dispositifs finaux en fonction d'une politique de sécurité définie.
NAT	Acronyme de « network address translation », traduction d'adresses de réseau. Également connue sous le nom d'usurpation réseau ou usurpation d'IP. Changement d'une adresse IP utilisée dans un réseau pour une autre adresse IP connue dans un autre réseau, ce qui permet à une organisation d'avoir des adresses internes qui sont visibles à l'externe et des adresses externes qui sont visibles à l'interne.
Réseau	Deux ou plusieurs ordinateurs connectés les uns aux autres par des moyens physiques ou sans fil.
Administrateur réseau	Personne responsable de la gestion du réseau au sein d'une entité. Les responsabilités comprennent généralement, entre autres, la sécurité du réseau, les installations, les mises à jour, la maintenance et la surveillance des activités.
Composants réseau	Les composants réseau comprennent entre autres les pare-feu, commutateurs, routeurs, points d'accès sans fil, équipements réseau et autres appareils de sécurité.
Schéma du réseau	Un schéma qui montre les composants et les connexions du système dans un environnement de réseau.
Analyse de sécurité du réseau	Processus par lequel les systèmes d'une entité sont vérifiés à distance pour déceler d'éventuelles vulnérabilités à l'aide d'outils manuels ou automatisés. Les analyses de sécurité comprennent la vérification des systèmes internes et externes, ainsi que le rapport sur les services exposés au réseau. Les analyses permettent d'identifier les vulnérabilités des systèmes d'exploitation, des services et des dispositifs susceptibles d'être utilisés par des individus malveillants.
Segmentation réseau	Également nommé « segmentation » ou « isolation ». La segmentation de réseau isole les composants du système, qui stockent, traitent ou transmettent les données de titulaires de cartes, de ceux qui ne le font pas. Une segmentation réseau appropriée peut réduire le champ d'application de l'environnement des données de titulaires de cartes, et ainsi celui de l'évaluation PCI DSS. Voir le chapitre Segmentation réseau dans les *Conditions et procédures d'évaluation de sécurité de la norme PCI DSS* pour plus d'informations sur son utilisation. La segmentation réseau n'est pas une condition de la norme PCI DSS.

Terme	Définition
Repérage réseau	Également nommé « repérage de paquet » ou « repérage ». Une technique qui surveille de manière passive ou qui collecte les communications du réseau, décode les protocoles et examine les contenus pour obtenir des informations intéressantes.
NIST	Acronyme de « National Institute of Standards and Technology », Institut national des standards et de la technologie. Agence fédérale non réglementaire de l'Administration de la technologie du ministère du Commerce des États-Unis.
NMAP	Logiciel d'analyse de sécurité qui mappe les réseaux et identifie les ports ouverts dans les ressources réseau.
Accès non-console	Fait référence à un accès logique à un composant du système qui se produira sur une interface du réseau plutôt que par connexion physique directe au composant du système. L'accès non console comprend l'accès à partir des réseaux internes/locaux, ainsi que l'accès à partir de réseaux externes ou distants.
Utilisateurs non-clients	Toute personne, à l'exception des titulaires de cartes, accédant à des composants du système, notamment des employés, des administrateurs et des tiers.
NTP	Acronyme de « Network Time Protocol », protocole de synchronisation réseau. Protocole de synchronisation des horloges des systèmes informatiques, réseaux, dispositifs et autres composants du système.
NVD	Acronyme de « National Vulnerability Database », base de données nationale sur la vulnérabilité. Le référentiel du gouvernement américain des données de gestion des vulnérabilités sur une base normalisée. Le NVD comprend des bases de données des listes de contrôle de sécurité, les erreurs de logiciel liées à la sécurité, les mauvaises configurations, les noms de produits et les mesures d'impact.
OCTAVE®	Acronyme pour « Operationally Critical Threat, Asset, and Vulnerability Evaluation », évaluation de menace, atout et vulnérabilité critique d'un point de vue opérationnel. Une suite d'outils, de techniques et de méthodes pour l'évaluation et la planification stratégiques basée sur les risques de la sécurité de l'information.
Prêt à l'emploi	Description de produits en stock qui ne sont pas particulièrement personnalisés ni conçus pour un client ou un utilisateur spécifique, et pouvant être utilisés immédiatement.
Système d'exploitation/SE	Logiciel d'un système informatique, responsable de la gestion et de la coordination de toutes les activités et du partage des ressources informatiques. Microsoft Windows, Mac OS, Linux et Unix sont des exemples de systèmes d'exploitation.

Terme	Définition
Indépendance opérationnelle	Une structure opérationnelle qui garantit qu'il n'existe aucun conflit d'intérêts entre la personne ou le service qui effectue l'activité et la personne ou service qui évalue l'activité. Par exemple, les individus qui effectuent des évaluations sont séparés d'un point de vue opérationnel de la direction de l'environnement testé.
OWASP	Acronyme de « Open Web Application Security Project », projet de sécurité d'application Web ouverte. Une organisation à but non lucratif qui se concentre sur l'amélioration de la sécurité du logiciel d'application. L'OWASP gère une liste des vulnérabilités critiques des applications Web. (Voir http://www.owasp.org).
PA-DSS	Acronyme de « Payment Application Data Security Standard », norme de sécurité des données d'application de paiement.
PA-QSA	Acronyme de « Payment Application Qualified Security Assessor », évaluateurs de sécurité qualifiés des applications de paiement. Les PA-QSA sont qualifiés par PCI SSC pour évaluer les applications de paiement par rapport à la norme PA-DSS. Consulter le *Guide de programme PA-DSS* et les *Conditions de conformité PA-QSA* pour les détails concernant les conditions de PA-QSA pour les sociétés et les employés.
Pad	En cryptographie, le pad ponctuel est un algorithme de cryptage avec un texte combiné à une clé aléatoire ou « pad », aussi longue que le texte clair et utilisée une seule fois. En outre, si la clé est réellement aléatoire, jamais réutilisée et tenue secrète, le pad unique est inviolable.
PAN	Acronyme de « primary account number », numéro de compte primaire, également nommé « account number », numéro de compte. Numéro unique de carte de paiement (généralement pour les cartes de crédit ou de débit), identifiant l'émetteur et le compte du titulaire de carte spécifique.
Requêtes paramétrées	Un moyen de structuration des requêtes SQL pour limiter les fuites et empêcher les attaques par injection.
Mot de passe/locution de passage	Chaîne de caractères servant d'authentifiant de l'utilisateur.
PAT	Acronyme de « port address translation », traduction d'adresses de port, également appelée « traduction de port d'adresse réseau ». Type de *NAT* qui traduit également les numéros de port.
Correctif	Mise à jour du logiciel existant pour ajouter des fonctionnalités ou corriger un défaut.
Application de paiement	Dans le cadre de la norme PA-DSS, une application logicielle qui stocke, traite ou transmet des données de titulaire de carte dans le cadre d'une autorisation ou d'un règlement, lorsque cette application est vendue, distribuée ou cédée sous licence à des tiers. Consultez le *Guide du programme de la norme PA-DSS* pour de plus amples détails.

Terme	Définition
Cartes de paiement	Dans le cadre de la norme PCI DSS, toute carte ou tout moyen de paiement portant le logo des membres fondateurs du PCI SSC, c'est-à-dire American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa, Inc.
Service de traitement de paiement	Parfois appelé « passerelle de paiement » ou « prestataire de services de paiement (PSP) ». Entité engagée par un commerçant ou une autre entité pour gérer les transactions par carte de paiement en leur nom. Bien que les services de traitement de paiement fournissent généralement des services d'acquisition, les services de traitement de paiement ne sont pas considérés comme des acquéreurs, à moins qu'ils ne soient définis comme tels par la marque de carte de paiement. Voir également *Acquéreur.*
PCI	Acronyme de « Payment Card Industry », industrie des cartes de paiement.
PCI DSS	Acronyme de « Payment Card Industry Data Security Standard », norme de sécurité des données de l'industrie des cartes de paiement.
PDA	Acronyme de « personnel data assistant » ou de « personal digital assistant », assistant numérique personnel. Appareils mobiles de poche comportant des fonctionnalités comme un téléphone mobile, une messagerie électronique ou un navigateur Web.
PED	PIN entry device, dispositif de saisie du code PIN.
Test de pénétration	Les tests de pénétration essayent d'identifier les manières d'exploiter les vulnérabilités pour contourner ou vaincre les fonctions sécuritaires des composants du système. Le test d'intrusion doit inclure le test du réseau et de l'application, ainsi que des contrôles et processus relatifs aux réseaux et aux applications. Il doit être mis en œuvre aussi depuis l'extérieur de l'environnement (test externe) que de l'intérieur.
Logiciel de pare-feu personnel	Un produit logiciel de pare-feu installé sur un ordinateur unique.
Informations permettant une identification personnelle.	L'information qui peut être utilisée pour identifier ou retracer l'identité d'un individu, notamment le nom, l'adresse, le numéro de sécurité sociale, les données biométriques, la date de naissance, etc.
Personnel	Désigne les employés à temps plein et à temps partiel, les intérimaires ainsi que les sous-traitants et les consultants qui « résident » sur le site de l'entité ou ont accès d'une manière ou d'une autre à l'environnement des données des titulaires de cartes.

Terme	Définition
PIN	Acronyme de « personal identification number », numéro d'identification personnel. Mot de passe numérique secret, connu uniquement de l'utilisateur et du système afin d'authentifier l'utilisateur. L'utilisateur n'est autorisé à accéder au système que si le code PIN qu'il fournit correspond à celui enregistré dans le système. Les codes PIN sont utilisés pour les distributeurs automatiques pour des transactions de retrait d'espèces. Un autre type de code PIN est celui utilisé sur les cartes à puce EMV, remplaçant la signature du titulaire de carte.
Bloc PIN	Bloc de données utilisé pour condenser un code PIN en cours de traitement. Le format du bloc PIN en définit le contenu et la manière dont il est traité pour récupérer le code PIN. Le bloc PIN est constitué du code PIN, de la longueur du PIN, et peut contenir un sous-ensemble du PAN.
POI	Acronyme de « Point of Interaction », point d'interaction où les données sont lues sur une carte. Produit d'acceptation de transaction électronique, un POI est constitué d'un matériel et d'un logiciel, est hébergé dans un équipement d'acceptation pour permettre à un titulaire de carte d'effectuer une transaction avec sa carte. Le POI peut être ou non sous surveillance. Les transactions POI sont généralement des transactions de paiement par carte par circuit intégré (puce) et/ou par une bande magnétique.
Politique	Règle à l'échelle de l'organisation régissant l'utilisation acceptable des ressources informatiques, les pratiques de sécurité, et guidant l'élaboration des procédures opérationnelles.
POP3	Acronyme de « Post Office Protocol v3 », protocole de poste v3. Protocole au niveau de l'application utilisé par les clients e-mail pour récupérer les e-mails d'un serveur distant avec une connexion TCP/IP.
Port	Points de connexion logiques (virtuels) associés à un protocole de communication particulier afin de faciliter les communications sur les réseaux.
POS	Acronyme de « point of sale », point de vente. Matériel et/ou logiciel utilisé pour traiter les transactions par cartes de paiement chez les commerçants.
Réseau privé	Réseau établi par une organisation qui utilise un espace d'adresse IP privé. Les réseaux privés sont communément appelés réseaux locaux. L'accès aux réseaux privés depuis des réseaux publics doit être correctement protégé par des pare-feu et des routeurs. Voir également *Réseau public*.
Utilisateur privilégié	Tout compte d'utilisateur bénéficiant de privilèges outre l'accès de base. Généralement, ces comptes ont des privilèges élevés ou développés avec plus de droits que les comptes d'utilisateur standard. Toutefois, la portée des privilèges pour différents comptes privilégiés peut varier en fonction de l'emploi ou du rôle dans l'organisation et la technologie utilisée.
Procédure	Commentaire descriptif d'une politique. La procédure indique « comment utiliser » une politique et décrit la manière dont celle-ci est mise en œuvre.

Terme	Définition
Protocole	Méthode de communication convenue utilisée au sein des réseaux. Spécifications décrivant les règles et procédures que doivent suivre les produits informatiques pour exécuter leurs activités sur un réseau.
Serveur Proxy	Un serveur qui agit en tant qu'intermédiaire entre un réseau Internet et Internet. Par exemple, l'une des fonctions d'un serveur proxy est de terminer ou de négocier les connexions entre les connexions internes et externes de sorte que chacun communique uniquement avec le serveur proxy.
PTS	Acronyme de « PIN Transaction Security », sécurité des transactions PIN, la PTS est un ensemble de critères d'évaluation modulaire géré par le Conseil des normes de sécurité du PCI pour l'acceptation du code PIN par les terminaux des points de vente. Se reporter au site www.pcisecuritystandards.org.
Réseau public	Réseau établi et exploité par un prestataire de services en télécommunications tiers dans le but précis de fournir au public des services de transmission de données. Les données circulant sur les réseaux publics peuvent être interceptées, modifiées et/ou détournées au cours de leur transmission. Internet comme les technologies sans fil et mobiles sont des exemples de réseaux publics. Voir également *Réseau privé*.
PVV	Acronyme de « valeur de vérification de code PIN ». Valeur discrétionnaire codée sur la bande magnétique de la carte de paiement.
QIR	Acronyme pour « intégrateur ou revendeur qualifié ». Consultez le *Guide de programme QIR* sur le site Internet PCI SSC pour de plus amples informations.
QSA	Acronyume de « Qualified Security Assessor », évaluateur de sécurité qualifié Les QSA sont qualifiés par PCI SSC pour effectuer des évaluations PCI DSS sur site. Consultez les *conditions de qualification QSA* sur les détails pour les conditions applicables aux sociétés et aux employés QDA.
RADIUS	Abréviation de « Remote authentication and Dial-In User Service », service d'usager commuté à authentification distante. Système d'authentification et de comptabilité. Vérifie si des informations comme le nom d'utilisateur et le mot de passe transmis au serveur RADIUS sont exactes, et autorise ensuite l'accès au système. Cette méthode d'authentification peut être utilisée avec un token, une carte à puce, etc., pour assurer une authentification à plusieurs facteurs.
Attaque de tableau arc-en-ciel	Une méthode d'attaque de données utilisant un tableau précalculé de chaînes de hachage (digestion de message de longueur fixe) pour identifier la source d'origine des données, habituellement casser un mot de passe ou les hachages de données de titulaire de carte.
Changement de clé	Processus de changement des clés cryptographiques. Le changement de clé périodique limite la quantité de données cryptées par une seule clé.

Terme	Définition
Accès à distance	Accès à des réseaux informatiques depuis un emplacement situé en dehors de ce réseau. Les connexions d'accès à distance peuvent provenir soit de l'intérieur du propre réseau de la société soit d'un emplacement distant hors du réseau de la société. Le *VPN* est un exemple de technologie d'accès à distance.
Environnement de laboratoire à distance	Laboratoire qui n'est pas géré par le PA-QSA.
Supports électroniques amovibles	Supports qui stockent des données numériques facilement déplacées et/ou transportées d'un système informatique à un autre. Les CD-ROM, les DVD-ROM, les clés USB et les disques durs externes/portables sont des supports électroniques amovibles.
Revendeur/intégrateur	Entité qui vend et/ou intègre des applications de paiement, mais ne les développe pas.
RFC 1918	La norme identifiée par l'IETF (Internet Engineering Task Force, groupe de travail sur l'ingénierie d'Internet) qui définit l'usage et les limites d'adresses appropriées pour des réseaux privés (sans routage sur Internet).
Analyse/Évaluation des risques	Processus identifiant systématiquement les ressources système précieuses et les menaces qui leur sont associées. Ce processus quantifie l'exposition aux pertes (pertes éventuelles) en fonction de la fréquence et des coûts d'occurrence estimés, et (en option) recommande la manière d'affecter des ressources aux contre-mesures dans le but de réduire l'exposition totale.
Classification des risques	Un critère de mesure défini basé sur l'évaluation des risques et l'analyse des risques effectuée sur une entité donnée.
ROC	Acronyme de « Rapport sur la conformité ». Rapport documentant les résultats détaillés de l'évaluation PCI DSS d'une entité.
Outil de dissimulation d'activité	Type de logiciel malveillant qui, une fois installé sans autorisation, est capable de dissimuler sa présence et d'acquérir le contrôle administratif d'un système informatique.
Routeur	Matériel ou logiciel connectant deux ou plusieurs réseaux. Assure des fonctions de tri et d'interprétation en examinant les adresses et en transmettant des éléments d'information à des destinations appropriées. Les routeurs de logiciel sont parfois appelés passerelles.
ROV	Acronyme de « Rapport sur la validation ». Rapport documentant les résultats détaillés d'une évaluation PA-DSS pour un programme PA-DSS.
RSA	Algorithme pour le cryptage de clé publique décrit en 1977 par Ron Rivest, Adi Shamir et Len Adleman, du Massachusetts Institute of Technology (MIT). L'association de leurs noms de famille a produit l'acronyme RSA.
S-FTP	Acronyme de Secure-FTP, FTP sécurisé. S-FTP a la capacité de crypter les informations d'authentification et les fichiers de données en transit. Voir *FTP.*

Terme	Définition
Échantillonnage	Processus de sélection d'une section transversale d'un groupe, représentatif du groupe entier. L'échantillonnage peut être utilisé par les évaluateurs afin de réduire l'effort global de test, lorsqu'il est confirmé qu'une entité applique des processus et des contrôles opérationnels et de sécurité PCI DSS standards et centralisés. L'échantillonnage n'est pas une condition de la norme PCI DSS.
SANS	Acronyme de « SysAdmin, Audit, Networking and Security ». Institut qui propose une formation en sécurité informatique et une certification professionnelle (voir www.sans.org).
SAQ	Acronyme de « Self-Assessment Questionnaire », questionnaire d'auto-évaluation. Outil de rapport utilisé pour documenter les résultats de l'auto-évaluation de l'évaluation PCI DSS d'une entité.
Schéma	Description formelle de la manière avec laquelle une base de données est construite, y compris l'organisation des éléments de données.
Détermination du champ d'application	Processus d'identification de tous les composants du système, personnes et processus à intégrer à l'évaluation PCI DSS. La première étape d'une évaluation PCI DSS est de correctement déterminer le champ d'application de la vérification.
SDLC	Acronyme de « system development life cycle », ou « software development lifecycle », cycle de vie de développement de système. Phases du développement d'un logiciel ou d'un système informatique comprenant la planification, l'analyse, la conception, les tests et le déploiement.
Codage sécurisé	Processus de création et de mise en œuvre d'applications résistant aux altérations et/ou aux compromissions.
Périphériques cryptographiques sécurisés	Un ensemble de matériel, logiciel et firmware qui implémente les processus cryptographiques (y compris les algorithmes et la production de clés cryptographiques) et qui est contenu dans une frontière cryptographique définie. Les exemples de périphériques cryptographiques comprennent les modules de sécurité hôte/matériel (HSM) et les appareils de point d'interaction (POI) qui ont été validés selon PCI PTS.
Nettoyage sécurisé	Également nommé « suppression sécurisée », une méthode d'écrasement des données résiduelles sur un disque dur, ou un autre support numérique, afin de rendre les données irrécupérables.
Événements de sécurité	Une circonstance considérée par une organisation comme ayant des implications potentielles sur la sécurité d'un système ou de son environnement. Dans le contexte de PCI DSS, les événements de sécurité identifient les activités anormales ou suspectes.
Responsable de la sécurité	La principale personne responsable des questions liées à la sécurité d'une entité.
Politique de sécurité	Ensemble de lois, de règles et de pratiques régissant la manière dont une organisation gère, protège et distribue des informations sensibles.

Terme	Définition
Protocoles de sécurité	Protocoles de communication réseau conçus pour sécuriser la transmission de données. Les exemples de protocoles de sécurité comprennent, notamment, TLS, IPSEC, SSH, HTTPS, etc.
Zone sensible	Tout centre de données, salle de serveur ou zone abritant des systèmes qui stockent, traitent ou transmettent des données de titulaires de cartes. Ceci exclut les zones où ne sont installés que des terminaux de point de vente, comme les zones de caisse dans un magasin.
Données d'identification sensibles	Informations relatives à la sécurité (comprenant notamment les codes/valeurs de validation de carte, les données de bande magnétique complètes [de la piste magnétique ou équivalent sur une puce], les codes et blocs PIN), utilisées pour authentifier les titulaires de carte et/ou pour autoriser les transactions par carte de paiement.
Séparation des obligations	Pratique consistant à répartir les divers aspects d'une fonction entre divers individus, afin d'éviter qu'une personne seule ne puisse corrompre l'ensemble du processus.
Serveur	Ordinateur fournissant un service à d'autres ordinateurs, comme le traitement des communications, le stockage de fichiers ou l'accès à une imprimante. Les serveurs comprennent, notamment, le Web, les bases de données, les applications, l'authentification, des DNS, la messagerie, les serveurs proxy et le NTP.
Code service	Nombre à trois ou quatre chiffres dans la bande magnétique, qui suit la date d'expiration de la carte de paiement sur les données de piste. Il peut être utilisé à des fins diverses comme définir les attributs de service, distinguer les échanges internationaux et nationaux ou identifier les restrictions d'utilisation.
Prestataire de services	Entité commerciale qui n'est pas une marque de paiement, directement impliquée dans le traitement, le stockage et la transmission des données de titulaires de cartes de la part d'une autre entité. Ceci comprend également les sociétés qui assurent des services de contrôle ou susceptibles d'affecter la sécurité des données de titulaires de cartes. Les prestataires de services gérés qui mettent à disposition des pare-feu, des IDS et autres services, ainsi que les fournisseurs et autres entités d'hébergement en sont des exemples. Si une entité fournit un service qui comprend *uniquement* l'accès aux réseaux publics, comme une société de télécommunication qui fournit simplement le lien de communication, l'entité n'est pas considérée comme un prestataire de service pour ce service (bien qu'elle puisse être considérée comme un prestataire de service pour d'autres services.
Jeton de session	Dans le cadre de la gestion de sessions Web, un jeton de session (également appelé « identifiant de session » ou « ID de session »), est un identifiant unique (comme un « cookie ») utilisé pour suivre une session spécifique entre un navigateur Web et un serveur Web.
SHA-1/SHA-2	Acronyme de « Secure Hash Algorithm », algorithme de hachage sécurisé. Famille ou ensemble de fonctions de hachage cryptographique, notamment SHA-1 et SHA-2. Voir *Cryptographie robuste.*

Terme	Définition
Carte à puce	Également nommé « carte à microprocesseur» ou « carte IC (carte à circuit intégré) ». Un type de carte de paiement qui est pourvue d'un circuit intégré. Les circuits ou « puces » contiennent les données de la carte de paiement, comprenant notamment, des données équivalentes à celles de la bande magnétique.
SNMP	Acronyme de « Simple Network Management Protocol », protocole de gestion de réseau simple. Prend en charge la surveillance de dispositifs connectés au réseau lorsqu'ils exigent une attention administrative.
Fractionnement des connaissances	Une méthode par laquelle deux ou plusieurs entités détiennent séparément des composants de la clé qui, à eux seuls, ne leur permettent pas d'avoir connaissance de la clé cryptographique qui en résulte.
Spyware	Le logiciel espion est un type de logiciel malveillant qui, une fois installé, intercepte ou prend partiellement le contrôle d'un ordinateur à l'insu de son utilisateur.
SQL	Acronyme de « Structured Query Language », langage structuré de requêtes. Langage informatique utilisé pour créer, modifier ou récupérer des données provenant de systèmes de gestion de bases de données relationnelles.
Injection de commandes SQL	Type d'attaque sur un site Web depuis une base de données. Un pirate exécute des commandes SQL non autorisées en profitant d'un code non sécurisé sur un système connecté à Internet. Les attaques par injection de commandes SQL sont utilisées pour dérober des renseignements provenant d'une base de données dont les données ne seraient normalement pas disponibles, et/ou pour accéder aux ordinateurs hôtes par l'intermédiaire de l'ordinateur hébergeant la base de données.
SSH	Abréviation de « Secure Shell », enveloppe sécurisée. Suite de protocole fournissant un cryptage pour des services de réseau tels que la connexion à distance ou le transfert de fichiers à distance.
SSL	Acronyme de « Secure Sockets Layer », protocole SSL. Norme du secteur cryptant le canal entre un navigateur et un serveur Web. Désormais remplacé par TLS. Voir *TLS.*
Contrôle avec état	Également nommé « filtrage des paquets dynamique ». Capacité de pare-feu qui fournit une sécurité renforcée en gardant la trace du statut des connexions de réseau. Programmé pour distinguer les paquets légitimes pour diverses connexions, uniquement les paquets contenant une connexion établie seront autorisés par le pare-feu, les autres seront rejetés.

Terme	Définition
Cryptographie robuste	Cryptographie basée sur des algorithmes éprouvés et acceptés par le secteur, ainsi que sur des longueurs de clés qui fournissent un minimum de 112 bits de robustesse effective de clé et des pratiques appropriées de gestion des clés. La cryptographie est une méthode de protection des données, comprenant à la fois un cryptage (réversible) et un hachage (« unilatéral » ou non réversible). Voir *Hachage.* Au moment de la publication, les exemples de normes et d'algorithmes éprouvés et acceptés par le secteur comprennent AES (128 bits et plus), TDES/TDEA (clés à triple longueur), RSA (2048 bits et plus), ECC (224 bits et plus) et DSA/D-H (2048/224 bits et plus). Voir la version actuelle de la publication spéciale NIST 800-57 Partie 1 (http://csrc.nist.gov/publications/) pour des recommandations plus approfondies sur la robustesse des clés cryptographiques et les algorithmes. ***Remarque :*** *Les exemples ci-dessus sont appropriés pour un stockage permanent des données de titulaire de carte. Les exigences minimales de cryptographie pour les opérations basées sur les transactions, comme définies dans PCI PIN et PTS, sont plus souples car il existe des contrôles supplémentaires mis en place pour réduire le niveau d'exposition.* *Il est recommandé que toutes les nouvelles implémentations utilisent un minimum de 128 bits de robustesse effective de clé.*
SysAdmin	Abréviation de « system administrator », administrateur de système. Individu bénéficiant de droits d'accès élevés, responsable de la gestion d'un système informatique ou d'un réseau.
Composants de système	Tout composant réseau, serveur, périphérique informatique ou application inclus ou connectés dans l'environnement des données des titulaires de cartes.
Objet au niveau système	Tout objet sur un composant du système qui est requis pour son fonctionnement, y compris les tableaux de bases de données, les procédures stockées, les fichiers d'application exécutables et les fichiers de configuration, les fichiers de configuration de système, les librairies statiques et partagées et les DLL, les fichiers exécutables du système, les pilotes de périphériques et les fichiers de configuration de périphériques, ainsi que les composants tiers.
TACACS	Acronyme de « Terminal Access Controller Access Control System », système de contrôle d'accès au contrôleur d'accès au terminal. Protocole d'authentification à distance, communément utilisé dans les réseaux communiquant entre un serveur d'accès à distance et un serveur d'authentification, afin de déterminer les droits d'accès au réseau de l'utilisateur. Cette méthode d'authentification peut être utilisée avec un token, une carte à puce, etc., pour assurer une authentification à plusieurs facteurs.
TCP	Acronyme de « Transmission Control Protocol », protocole de contrôle de transmission. L'un des principaux protocoles de transport de niveau de la suite de protocole Internet (IP) et la langue de communication, ou protocole de base d'Internet. Voir *IP*.

Terme	Définition
TDES	Acronyme de « Triple Data Encryption Standard », également appelé « 3DES » ou « Triple DES ». Cryptage de bloc formé à partir de trois utilisations d'un cryptage DES. Voir *Cryptographie robuste.*
TELNET	Abréviation de « telephone network protocol », protocole de réseau téléphonique. Généralement utilisé pour mettre à disposition des sessions de connexion par ligne de commande orientées utilisateur sur un réseau. Les éléments d'authentification sont transmis en texte clair.
Menace	Situation ou activité susceptible d'entraîner la perte, la modification, l'exposition ou l'indisponibilité intentionnelle ou accidentelle d'informations ou de ressources de traitement des informations, ou de les affecter au détriment de l'organisation.
TLS	Acronyme de « Transport Layer Security », protocole TLS. Conçu dans le but d'assurer la confidentialité et l'intégrité des données entre deux applications de communication. Le protocole TLS a remplacé le protocole SSL.
Token	Dans le contexte de l'authentification et du contrôle d'accès, un token est une valeur fournie par un matériel ou un logiciel qui fonctionne avec un serveur d'authentification ou un VPN pour effectuer une authentification dynamique ou à plusieurs facteurs. Voir *RADIUS, TACACS* et *VPN.* Voir également *Jeton de session*.
Données de piste.	Également nommées « données de piste » ou « données de bande magnétique ». Données codées sur la bande magnétique ou sur la puce, utilisées pour l'authentification et/ou l'autorisation lors des transactions de paiement. Il peut s'agir de l'image de bande magnétique sur une puce ou de données figurant sur la portion de piste 1 et/ou de piste 2 de la bande magnétique.
Données de transaction	Données relatives à une transaction électronique par carte de paiement.
Trojan	Également appelé « cheval de Troie ». Logiciel malveillant qui, une fois installé, permet à un utilisateur d'effectuer les fonctions normales tandis que le Trojan effectue des actes malveillants sur un système informatique à l'insu de l'utilisateur.
Troncature ;	Méthode permettant de rendre la totalité du PAN illisible en supprimant en permanence un segment de ses données. La troncature porte sur la protection du PAN lorsqu'il est *stocké* dans des fichiers, des bases de données, etc. Voir *Masquage* pour la protection du PAN lorsqu'il est *affiché* sur des écrans, des reçus papier, etc.
Réseau approuvé	Réseau d'une organisation qu'elle peut gérer ou sur lequel elle dispose d'un contrôle.
Réseau non approuvé	Réseau externe aux réseaux appartenant à une organisation que celle-ci ne gère pas ou sur lequel elle ne peut exercer aucun contrôle.

Terme	Définition
URL	Acronyme de « Uniform Resource Locator », localisateur de ressources uniformesUne chaîne de texte formatée utilisée par les navigateurs Web, les clients d'e-mail et les autres logiciels pour identifier une ressource du réseau sur Internet.
Méthodologie de contrôle de version	Un processus d'affectation de systèmes de version pour identifier de manière unique le statut particulier d'une application ou un logiciel. Ces systèmes suivent un format de numéro de version, une utilisation de numéro de version et n'importe quel élément de caractère générique définit par le fournisseur du logiciel. Les numéros de version sont généralement affectés en ordre croissant et ils correspondent à un changement spécifique du logiciel.
Équipement virtuel (VA)	Un équipement virtuel reprend le concept d'un dispositif préconfiguré pour effectuer un ensemble spécifique de fonctions et exécuter ce dispositif comme une charge de travail. Souvent, un dispositif réseau existant est virtualisé pour fonctionner en tant qu'équipement virtuel, comme un routeur, un commutateur, ou un pare-feu.
Hyperviseur virtuel	Voir *Hyperviseur*.
Ordinateur virtuel	Environnement d'exploitation autonome qui se comporte comme un ordinateur distinct. Il est également appelé « invité », et fonctionne au-dessus d'un hyperviseur.
Moniteur d'ordinateur virtuel (VMM)	Le moniteur d'ordinateur virtuel, compris dans l'hyperviseur, est un logiciel qui déploie l'abstraction de matériel informatique virtuel. Il gère le processeur du système, la mémoire et d'autres ressources pour attribuer ce que chaque système d'exploitation invité exige.
Terminal de paiement virtuel	Un terminal de paiement virtuel est un accès par navigateur Web au site Web d'un acquéreur, un processeur ou un prestataire de services tiers pour autoriser les transactions par carte de paiement, lorsque le commerçant saisit manuellement les données de carte de paiement par le biais d'une connexion sécurisée à un navigateur Web. Contrairement aux terminaux physiques, les terminaux de paiement virtuels ne lisent pas les données directement sur la carte de paiement. Les transactions par carte de paiement étant saisies manuellement, les terminaux virtuels sont généralement utilisés plutôt que des terminaux physiques dans l'environnement des commerçants dont le volume de transactions est faible.
Commutateur ou routeur virtuels	Un commutateur ou un routeur virtuel sont des entités logiques présentant un routage de données au niveau de l'infrastructure du réseau et une fonctionnalité de commutation. Un commutateur virtuel fait partie intégrante de la plateforme de serveur virtualisé comme un pilote d'hyperviseur, un module, ou un module d'extension.

Terme	Définition
Virtualisation	La virtualisation concerne l'abstraction logique des ressources informatiques des contraintes physiques. Les ordinateurs virtuels (VM) sont une abstraction commune, qui reçoit le contenu d'un ordinateur physique et lui permet de fonctionner sur un matériel différent et/ou avec d'autres ordinateurs virtuels sur le même équipement. En plus des ordinateurs virtuels, la virtualisation peut être effectuée sur beaucoup d'autres ressources informatiques, notamment des applications, des ordinateurs de bureaux, des réseaux et des espaces de stockage.
VLAN	Abréviation de « virtual LAN » ou de « virtual local area network », réseau local virtuel. Réseau local logique qui s'étend au-delà du simple réseau local physique traditionnel.
VPN	Acronyme de « virtual private network », réseau privé virtuel. Réseau informatique dans lequel certaines connexions sont des circuits virtuels au sein d'un réseau plus important, comme Internet, remplaçant les connexions directes par des câbles physiques. Les points terminaux du réseau virtuel sont alors tunnelisés à travers le réseau de plus grande dimension. Alors qu'une application commune consiste en plusieurs communications sécurisées par le réseau Internet public, un VPN peut comporter ou non des fonctionnalités de sécurité, comme l'authentification ou le cryptage de contenu. Un VPN peut être utilisé avec un token, une carte à puce, etc., pour assurer une authentification à deux facteurs.
Vulnérabilité	Défaut ou faiblesse qui, s'il est exploité, peuvent compromettre un système, intentionnellement ou non.
WAN	Acronyme de « wide area network », réseau étendu. Réseau informatique couvrant une large zone, souvent un système informatique régional ou à l'échelle d'une société.
Application Web	Application qui est généralement accessible par un navigateur ou des services Web. Les applications Web peuvent être disponibles par Internet ou par le biais d'un réseau interne privé.
Serveur Web	Ordinateur contenant un programme qui accepte les requêtes HTTP des clients Web et fournit des réponses HTTP (généralement des pages Web).
WEP	Acronyme de « Wired Equivalent Privacy », protocole WEP. Algorithme peu complexe, utilisé pour crypter des réseaux sans fil. De nombreuses faiblesses ont été identifiées par les experts du secteur ; en effet, une connexion WEP peut être piratée en quelques minutes avec un logiciel prêt à l'emploi. Voir *WPA.*

Terme	Définition
Caractère générique	Un caractère qui peut être substitué pour un sous-ensemble défini de caractères possibles dans un système de version d'application. Dans le contexte du PA-DSS, les caractères génériques peuvent être utilisés pour représenter un changement 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.
Point d'accès sans fil	Également dénommé « PA ». Dispositif permettant aux périphériques sans fil de se connecter à un réseau sans fil. Généralement connecté à un réseau câblé, le point d'accès sans fil peut transmettre des données entre des dispositifs sans fil et des dispositifs câblés sur le réseau.
Réseau sans fil	Réseau qui connecte les ordinateurs sans une connexion physique par des câbles.
WLAN	Acronyme de « wireless local area network », réseau local sans fil. Réseau qui relie deux ou plusieurs ordinateurs ou dispositifs sans câbles.
WPA/WPA2	Acronyme de « WiFi Protected Access », accès WiFi protégé. Protocole de sécurité créé pour sécuriser les réseaux sans fil. Le protocole WPA a remplacé le protocole WEP. Le WPA2 est la dernière génération de WPA.