Norme de sécurité des données (DSS) de l'industrie des cartes de paiement (PCI) et Norme de sécurité des données de l'application de paiement (PA-DSS)

Glossaire, abréviations et acronymes

Version 3.0

Janvier 2014

Terme	Définition
AAA	Acronyme d'« authentication, authorization, and accounting » (authentification, autorisation et traçabilité). Protocole permettant d'authentifier un utilisateur à partir de son identité vérifiable, d'autoriser un utilisateur à partir de ses droits d'utilisateur et d'effectuer la comptabilisation des ressources réseau d'un utilisateur.
Accès administratif non console	Fait référence à un accès administratif 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 administratif non console comprend l'accès à partir des réseaux internes/locaux, ainsi que l'accès à partir de réseaux externes ou distants.
Accès à distance	Accès à distance à des réseaux informatiques. Les connexions d'accès à distance peuvent provenir soit de l'intérieur du propre réseau de l'entreprise, soit d'un emplacement distant hors du réseau de l'entreprise. Le *VPN* est un exemple de technologie d'accès à distance.
Acquéreur	Également dénommé « banque acquéreur » ou « institution financière acquéreur ». Entité initiant et maintenant des relations avec des commerçants qui acceptent des cartes de paiement.
Administrateur de base de données	Également appelé « DBA » (Database Administrator). Personne en charge de la gestion et de l'administration des bases de données.
Administrateur de réseau	Personne responsable de la gestion du réseau au sein d'une entité. Les responsabilités comprennent généralement, mais sans s'y limiter, la sécurité du réseau, les installations, les mises à jour, la maintenance et la surveillance d'activités.
Adresse IP	Également appelée adresse numérique Internet. Code numérique identifiant de manière unique un ordinateur donné (hôte) sur Internet.
Adresse MAC	Abréviation de « media access control address » (adresse de contrôle d'accès au support). Unique valeur d'identification attribuée par les fabricants aux adaptateurs et cartes réseau.
AES	Acronyme d'« Advanced Encryption Standard ». Cryptage par bloc utilisé dans un système cryptographique à clé secrète, adopté par le NIST en novembre 2001 comme algorithme de la FIPS PUB 197 américaine (ou « FIPS 197 »). Voir *Cryptographie performante.*
Algorithme de cryptage	Également nommé algorithme cryptographique. Séquence d'instructions mathématiques utilisées pour transformer du texte ou des données non cryptées en texte ou données cryptées, et vice-versa. Voir *Cryptographie performante.*
Analyse/Évaluation des risques	Processus identifiant systématiquement les ressources système précieuses et les menaces associées. Ce processus quantifie l'exposition à des pertes (pertes éventuelles) sur la base de fréquences et de coûts d'occurrence estimés, et formule (de manière optionnelle) des recommandations quant à la manière d'affecter des ressources aux contre-mesures dans le but de minimiser l'exposition totale.

Terme	Définition
Analyse de sécurité du réseau	Processus par lequel les systèmes d'une entité sont vérifiés à distance pour déceler d'éventuelles vulnérabilités au moyen d'outils manuels ou automatisés. Les analyses de sécurité comprennent la vérification des systèmes internes et externes, ainsi que les rapports sur les services exposés au réseau. Ils identifient les vulnérabilités des systèmes d'exploitation, des services et des dispositifs susceptibles d'être utilisés par des pirates.
ANSI	Acronyme d'« American National Standard 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, y compris des virus, vers, chevaux de Troie, logiciels espions, logiciels de publicité et les programmes malveillants furtifs.
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, comme documenté dans le questionnaire d'auto-évaluation ou dans 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 PCI DSS, comme documenté dans le rapport PA-DSS sur la validation.
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.
Application	Comprend tous les programmes ou groupes de programmes logiciels achetés et personnalisés, y compris les applications internes et externes (Internet, par exemple).
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 plus de détails.
Application web	Application qui est généralement accessible par un navigateur web ou par des services web. Les applications web peuvent être disponibles par Internet ou un réseau interne privé.
ASV	Acronyme d'« Approved Scanning Vendor » (prestataire de services d'analyse agréé). Entreprise agréée par le PCI SSC pour appliquer des procédures d'analyse des vulnérabilités externes.
Attaques de grattage de mémoire	Une activité de logiciel malveillant qui examine et extrait les données demeurant dans la mémoire lorsqu'elle sont traitées ou qui n'ont pas été correctement rejetées ou écrasées.

Terme	Définition
Attaques CSRF (Cross-Site Request Forgery)	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.
Attaque de tableau arc-en-ciel	Une méthode d'attaque de données utilisant un tableau précalculé de chaînes de hachage (condensé de message de longueur fixe) pour identifier la source d'origine des données, habituellement craquer un mot de passe ou les hachages de données de titulaire de carte.
Attaques XSS (Cross-Site Scripting)	Vulnérabilité créée par des techniques de codage non sécurisées, provocant la validation d'une entrée incorrecte. Souvent utilisées avec une injection CSRF et/ou SQL.
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 comme : ▪ 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.
Authentification à deux facteurs	Méthode d'authentification d'un utilisateur par la vérification de deux facteurs ou plus. Ces facteurs sont parfois constitués d'un élément que l'utilisateur possède (comme un jeton matériel ou logiciel), d'un élément que l'utilisateur connaît (comme un mot de passe ou un code PIN), ou d'un élément que l'utilisateur effectue (comme une empreinte ou autre forme de biométrie).
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 peut 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.
Base de données	Format structuré d'organisation et de conservation de renseignements facilement récupérables. Les tableaux et tableurs sont des exemples de bases de données simples.
BAU	Acronyme de « business as usual » (activités d'affaires courantes). Le BAU est constitué par les opérations commerciales normales d'une organisation.
Bloc PIN	Bloc de données utilisé pour encapsuler 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 se compose du code PIN, de la longueur du code PIN, et peut contenir un sous-ensemble du PAN.
Bluetooth	Protocole sans fil utilisant la technologie des communications à courte portée pour faciliter la transmission de données sur une courte distance.

Terme	Définition
Caractère de remplacement	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 de remplacement peuvent être utilisés pour représenter un changement n'ayant pas d'impact sur la sécurité. Le caractère de remplacement 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 de remplacemenet.
Carte à puce	Également appelée carte à puce ou carte à circuit intégré (integrated circuit card). Type de carte de paiement équipée de circuits intégrés. Les circuits, aussi appelés « puces » contiennent les données de la carte de paiement, comprenant notamment des données équivalentes à celles de la bande magnétique.
Cartes de paiement	Dans le cadre des normes PCI DSS, une carte/un 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.
Changement de clé	Processus de changement des clés cryptographiques. Le changement de clé périodique limite la quantité de données cryptées par une seule clé.
Cheval de Troie	Également appelé « programme de Troie ». Logiciel malveillant qui, une fois installé, permet à un utilisateur d'effectuer les fonctions normales tandis que le cheval de Troie effectue des actes malveillants sur un système informatique à l'insu de l'utilisateur.
CDE	Acronyme de « cardholder data environment » (environnement des données de titulaire de carte). Les personnes, processus et technologies qui stockent, traitent ou transmettent des données de titulaire de carte ou des données d'authentification sensibles.
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 appropriées et des pratiques de gestion des systèmes pour résister aux attaques sur des systèmes en réseau, pour limiter les dommages, et pour assurer la continuité des services essentiels.
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 relatifs au commerce électronique découlant de contrôles techniques de sécurité inappropriés.
Classification des risques	Un critère de mesure défini basé sur l'évaluation des risques et l'analyse des risques effectuée sur une entité donnée.
Codage sécurisé	Processus de création et de mise en œuvre d'applications résistant aux altérations et/ou aux compromissions.

Terme	Définition
Code service	Numéro 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 pour définir les attributs de service, distinguer les échanges internationaux et nationaux ou identifier les restrictions d'utilisation.
Commerçant	Dans le cadre des normes PCI DSS, un commerçant est défini comme une entité qui accepte les 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 biens et/ou de services. Noter qu'un commerçant qui accepte ces cartes de paiement pour acheter des biens et/ou des services peut également être un prestataire de services, si les services vendus entraînent un stockage, un traitement ou une transmission des données de titulaire de carte au nom d'autres commerçants ou prestataires de services. Par exemple, un ISP est à la fois un commerçant qui accepte les cartes de paiement comme moyen de facturation mensuelle, mais aussi un prestataire de services s'il héberge des commerçants en tant que clients.
Commutateur ou routeur virtuel	Un commutateur ou un routeur virtuel sont une entité logique présentant un routage de données au niveau de l'infrastructure du réseau et une fonctionnalité de commutation. Un commutateur virtuel fait partie intégrante d'une plateforme de serveur virtualisé comme un pilote d'hyperviseur, un module, ou un module d'extension.
Composants de système	Tout composant réseau, serveur, périphérique informatique ou application inclus ou connectés dans l'environnement des données des titulaires de cartes.
Composants réseau	Les composants réseau comprennent notamment les pare-feu, les commutateurs, les routeurs, les points d'accès sans fil, les équipements réseau et autres dispositifs de sécurité.
Compte par défaut	Compte prédéfini de connexion à un système, une application ou un dispositif, permettant d'accéder 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.
Connaissance partagée	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.
Console	Écran et clavier permettant l'accès à un serveur, un ordinateur principal ou un autre type de système ainsi que leur contrôle, dans un environnement en réseau.
Consommateur	Personne achetant des biens ou des services, ou les deux.
Contrôle	Utilisation de systèmes ou de processus supervisant en permanence des ressources informatiques ou réseau afin d'alerter le personnel en cas de rupture d'alimentation, de déclenchement d'alarmes ou d'autres événements prédéfinis.

Terme	Définition
Contrôle avec état	Également nommé filtrage dynamique à paquets. 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 différents types de connexions, uniquement les paquets contenant une connexion établie seront autorisés par le pare-feu, les autres seront rejetés.
Contrôles compensatoires	Des contrôles compensatoires peuvent être envisagés lorsqu'une entité n'est pas en mesure de se conformer à l'exigence explicitement prévue, en raison de contraintes techniques légitimes ou de contraintes commerciales consignées, mais qu'elle a suffisamment atténué les risques liés à l'exigence par la mise en œuvre d'autres contrôles. Les contrôles compensatoires doivent : (1) Respecter l'intention et la rigueur de l'exigence d'origine des normes PCI DSS. (2) Fournir une protection similaire à celle de l'exigence initiale des PCI DSS. (3) Aller au-delà des autres exigences des PCI DSS (pas seulement se trouver en conformité avec les autres exigences des normes PCI DESS). (4) Être proportionnel aux risques supplémentaires qu'implique le non-respect de l'exigence PCI DSS. Consulter les annexes B et C sur les « contrôles compensatoires » dans les *conditions et procédures d'évaluation de sécurité PCI DSS* pour plus de renseignements sur leur utilisation.
Contrôle d'accès	Mécanisme limitant la disponibilité des renseignements ou des ressources de traitement des renseignements à des personnes ou applications autorisées uniquement.
Contrôle de changement	Les processus et procédures servant à examiner, tester et approuver les changements apportés aux systèmes et logiciels en termes d'impact avant l'implémentation.
Contrôle de l'intégrité des fichiers	Technique ou technologie au moyen de laquelle certains fichiers ou journaux sont contrôlés dans le but de détecter une éventuelle modification. Lorsque des fichiers ou journaux sensibles sont modifiés, des alertes doivent être envoyées au personnel de sécurité approprié.
Correctif	Mise à jour du logiciel existant pour ajouter des fonctionnalités ou corriger un défaut.
CP/CT	Acronyme pour commande postale/commande par téléphone.
Cryptage	Processus de conversion de renseignements sous forme inintelligible, sauf pour les possesseurs d'une clé cryptographique spécifique. L'utilisation du cryptage protège les renseignements entre le processus de cryptage et le processus de décryptage (l'inverse du cryptage) contre toute divulgation non autorisée. Voir *Cryptographie performante.*
Cryptage au niveau fichier	Technique ou technologie (logicielle ou matérielle) de cryptage du contenu global de fichiers spécifiques. Voir également *Cryptage par disque* ou *Cryptage de la base de données au niveau colonne.*

Terme	Définition
Cryptage de base de données au niveau colonne	Technique ou technologie (logicielle ou matérielle) de cryptage du contenu d'une colonne spécifique dans une base de données, plutôt que de tout le contenu de la base de données. Voir également *Cryptage par disque* ou *Cryptage au niveau fichier.*
Cryptage par disque	Technique ou technologie (logicielle ou matérielle) de cryptage de toutes les données stockées sur un dispositif (par exemple, disque dur ou lecteur mémoire flash). Le *cryptage au niveau fichier* et *le cryptage de base de données au niveau colonne* sont également utilisés pour crypter le contenu de fichiers ou de colonnes spécifiques.
Cryptographie	Discipline mathématique et informatique se rapportant à la sécurité des renseignements, en particulier au cryptage et à l'authentification. Au niveau des applications et de la sécurité du réseau, la cryptographie est un outil de contrôle d'accès préservant la confidentialité et l'intégrité de l'information.
Cryptographie Clé	Une valeur algorithmique appliquée au texte non crypté afin de produire un cryptogramme. De manière générale, la longueur de la clé détermine le degré de difficulté du décryptage du cryptogramme d'un message donné. Voir *Cryptographie performante.*
Cryptopériode	Durée pendant laquelle une clé cryptographique spécifique peut être utilisée aux fins définies, par exemple, une période déterminée et/ou la quantité de cryptogramme 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.
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.
Démagnétisation	Aussi appelée « démagnétisation de disque ». Processus ou technique qui démagnétise le disque, de sorte que l'ensemble des données qui y sont stockées sont en permanence supprimées.
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, une API, une librairie de codes, etc.) qui est nécessaire pour la conformité de l'application de paiement aux conditions de la norme PA-DSS.
Détermination de la portée	Processus d'identification de tous les composants du système, personnes et processus à comprendre dans l'évaluation PCI DSS. La première étape d'une évaluation PCI DSS consiste à correctement déterminer le champ d'application de la vérification.

Terme	Définition
Diagramme de flux des données	Un diagramme qui présente les flux de données dans une application, un système ou un réseau.
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 manière à ce que les parties externes puissent accéder directement aux dispositifs de la zone démilitarisée, et non à l'ensemble du réseau interne.
DNS	Acronyme de « Domain Name System » (système de nom de domaine) ou de « 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.
Données de bande magnétique	Voir *Données de piste.*
Données de compte	Les données de compte se composent des données du titulaire de carte et/ou des données d'authentification sensibles. Voir *Données de titulaire de carte* et *Données d'authentification sensibles.*
Données de piste	Également appelées données de piste complète ou données de bande magnétique. Données encodées 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 titulaire de carte	Les données de titulaire de carte se composent au minimum du PAN dans son intégralité. Les données de titulaire de carte peuvent également être constituées du PAN entier plus l'un ou l'autre des éléments ci-après : nom du titulaire de carte, date d'expiration et/ou code de service. Voir *Données d'authentification sensibles* pour plus de renseignements sur les autres éléments pouvant être transmis ou traités (mais non stockés) dans le cadre d'une transaction de paiement.
Données de transaction	Données liées à une transaction électronique par carte de paiement.
Données d'identification sensibles	Renseignements liés à la sécurité (comprenant, mais sans s'y limiter, codes/valeurs de validation de carte, données de bande magnétique complète [de la bande magnétique ou équivalent sur une puce], codes et blocs PIN) utilisés pour authentifier les titulaires de carte et/ou pour autoriser les transactions par carte de paiement.

Terme	Définition
Double contrôle	Processus d'utilisation de deux ou plusieurs entités distinctes (généralement des personnes) opérant de concert pour protéger des fonctions ou renseignements sensibles. Les deux entités sont également responsables de la protection physique des documents impliqués dans des transactions vulnérables. Nul n'est autorisé à accéder aux supports (par exemple, une clé cryptographique) ou à les utiliser. Pour la génération manuelle de clés, le transfert, le chargement, le stockage et la récupération de données, le double contrôle nécessite un partage de la connaissance des clés entre les entités. (Voir également *Connaissance partagée*).
DSS	Acronyme de « data security standard » (norme de sécurité des données). Voir *PA-DSS* et *PCI DSS.*
ECC	Acronyme d'« Elliptic Curve Cryptography » (cryptographie sur les courbes elliptiques). Approche de la cryptographie à clé publique basée sur des courbes elliptiques sur champs limités. Voir *Cryptographie performante.*
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 validé qu'une entité a des processus et des contrôles opérationnels et de sécurité PCI DSS, standards et centralisés, en place. L'échantillonnage n'est pas une exigence des normes PCI DSS.
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 institution financière émettrice.
Entité	Terme utilisé pour représenter l'entreprise, l'organisation ou l'activité qui fait l'objet d'une vérification des normes PCI DSS.
Environnement de laboratoire à distance	Laboratoire qui n'est pas géré par la PA-QSA.
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 comme un équipement virtuel, tel qu'un routeur, un commutateur, ou un pare-feu.
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.
Expertise judiciaire	Également appelée « expertise judiciaire en informatique ». Relative à la sécurité de l'information, l'application d'outils d'investigation et de techniques d'analyse permet de rassembler des preuves à partir des ressources informatiques et de déterminer ainsi l'origine des incidents de données.
Filtrage d'entrée	Méthode de filtrage du trafic du réseau entrant ne permettant l'entrée au réseau qu'au seul trafic explicitement autorisé.

Terme	Définition
Filtrage de sortie	Méthode de filtrage du trafic sortant du réseau ne permettant la sortie du réseau qu'au trafic explicitement autorisé.
Filtrage dynamique à paquets	Voir *Contrôle avec état.*
FIPS	Acronyme de « Federal Information Processing Standards » (normes fédérales de traitement de l'information). Normes publiquement reconnues par le gouvernement fédéral américain. Également utilisées par les organismes non gouvernementaux et les sous-traitants.
Fournisseur d'hébergement	Offre des services divers à des commerçants et autres prestataires de services. Ces services vont des plus simples aux plus complexes : du partage d'espace sur un serveur à une gamme complète d'options de « chariot virtuel » , d'applications de paiement à des portails de paiement et entités de traitement jusqu'à l'hébergement réservé à un seul client par serveur. Un fournisseur d'hébergement peut être un fournisseur partagé qui héberge plusieurs entités sur un même serveur.
FTP	Acronyme de « File Transfer Protocol » (protocole de transfert de fichiers). Protocole réseau utilisé pour transférer des données d'un ordinateur à un autre via un réseau public, tel qu'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. FTP peut être mis en œuvre de manière sécurisée via SSH ou une autre technologie. Voir *S-FTP*.
Gestion de clé cryptographique	L'ensemble des mécanismes et processus qui prennent en charge l'établissement et l'entretien des clés, y compris le remplacement des anciennes clés par de nouvelles clés, le cas échéant.
GPRS	Acronyme de « General Packet Radio Service » (service général de paquets radio). Service mobile de données à la disposition des utilisateurs de téléphones mobiles GSM. Réputé pour une utilisation efficace d'une largeur de bande limitée. Particulièrement adapté à l'envoi et à la réception de petits paquets de données, tels que des messages électroniques, ainsi qu'à la navigation sur Internet.
GSM	Acronyme de « Global System for Mobile Communications » (système global de communication mobile). Norme populaire pour les téléphones et réseaux mobiles. La présence très étendue de la norme GSM facilite considérablement le roaming international entre opérateurs de téléphonie mobile, permettant aux abonnés d'utiliser leur téléphone dans de nombreuses régions du monde.

Terme	Définition
Hachage	Processus qui consiste à rendre des données de titulaire de carte illisibles en les convertissant en une empreinte numérique à longueur fixe par une *cryptographie performante.* Le hachage est une fonction unilatérale (mathématique) dans laquelle un algorithme non-secret prend un message de longueur aléatoire comme entrée et produit une sortie de longueur fixe (généralement appelé « code de hachage » ou « condensé de message »). Une fonction de hachage doit avoir les propriétés suivantes : (1) Il est impossible de déterminer informatiquement l'entrée originale donnée uniquement avec le code de hachage. (2) Il est impossible de trouver informatiquement les deux entrées qui donnent le même code de hachage. Dans le cadre des normes PCI DSS, le hachage doit être appliqué au 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*).
Hôte	Principal matériel informatique sur lequel le logiciel informatique réside.
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 d'informations 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 permettre une communication sensible à la sécurité, comme les connexions en ligne.
Hyperviseur	Logiciel ou micrologiciel responsable de l'hébergement et de la gestion de postes de travail virtuels. À des fins de conformité aux normes PCI DSS, le composant du système hyperviseur comprend également un moniteur de poste de travail virtuel (VMM).
Hyperviseur virtuel	Voir *Hyperviseur*.
ID	Identifiant d'un utilisateur ou d'une application spécifiques.

Terme	Définition
IDS	Acronyme d'« intrusion detection system » (système de détection d'intrusion). Logiciel ou matériel utilisé pour identifier et prévenir 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 de surveillance des événements et alertes et de contrôle des capteurs, ainsi que d'un moteur central qui enregistre dans une base de données les événements détectés 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 de réseau, opérateurs, fournisseurs et chercheurs concernés par l'évolution de l'architecture du Web et le bon fonctionnement de l'Internet. L'IETF ne dispose pas de système d'adhésion et est ouvert à toute personne intéressée.
IMAP	Acronyme d'« Internet Message Access Protocol » (protocole d'accès aux messages Internet). Un protocole Internet de couche d'application qui permet à un logiciel de courrier électronique client d'accéder aux courriels sur un serveur de messagerie distant.
Incident de sécurité	Également appelé « incident de sécurité des données » ou « faille de sécurité des données ». Intrusion dans un système informatique lorsqu'une divulgation/un vol, une modification ou la destruction non autorisés de données de titulaire de carte sont soupçonnés.
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 le 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.
Injection de commandes SQL	Type d'attaque sur un site Web régi par 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 informations provenant d'une base de données dont les données ne seraient normalement pas disponibles et/ou pour accéder aux ordinateurs hôtes par le biais de l'ordinateur hébergeant la base de données.
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 Internet est le principal protocole de couche de réseau dans la suite du protocole Internet. Voir *TCP*.
IPS	Acronyme d'« intrusion prevention system » (système de prévention d'intrusion). L'IPS ne se contente pas de détecter les tentatives d'intrusion comme l'IDS, mais les bloque.

Terme	Définition
IPSEC	Abréviation de « Internet Protocol Security » (sécurité du protocole Internet). Norme de sécurisation des communications IP au niveau du réseau en cryptant et/ou authentifiant l'ensemble des paquets IP dans une session de communication.
ISO	Mieux connu sous le nom de « International Organization for Standardization » (Organisation internationale de normalisation). Organisation non gouvernementale constituée par un réseau des instituts nationaux de normalisation.
Jeton	Dans le contexte de l'authentification et du contrôle d'accès, un jeton 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 deux facteurs. Voir *RADIUS, TACACS* et *VPN.*
Jeton d'index	Jeton cryptographique qui remplace le PAN à partir d'un index donné et pour une valeur imprévisible.
Journal	Voir *Journal de vérification.*
Journal de vérification	Également appelé « piste de vérification ». Enregistrement chronologique des activités du système. Fournit un suivi de vérification indépendant suffisant pour autoriser la reconstruction, la vérification et l'examen de séquences d'environnements et d'activités entourant ou menant à une opération, une procédure ou un événement lors d'une transaction, de l'origine aux résultats finaux.
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 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 utilisateur et accorder l'accès à des ressources protégées.
Logiciel de pare-feu personnel	Un produit logiciel de pare-feu installé sur un seul ordinateur.
Logiciel espion	Type de logiciel malveillant qui, une fois installé, intercepte ou prend partiellement le contrôle d'un ordinateur à l'insu de son utilisateur.
Logiciel malveillant/maliciel	Logiciel ou micrologiciel 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 dans un réseau dans le cadre d'activités professionnelles approuvées, et exploite les vulnérabilités du système. Les virus, les chevaux de Troie, les logiciels espions et publicitaires et les dissimulateurs d'activités représentent différents types de logiciels malveillants.

Terme	Définition
Logiciel publicitaire	Type de logiciel malveillant qui, une fois installé, force un ordinateur à afficher ou télécharger des publicités de façon automatique.
LPAR	Abréviation de « logical partition » (partition logique). Système de sous-division ou de partitionnement de toutes les ressources d'un ordinateur - processeurs, mémoire et stockage – en unités plus petites capables de fonctionner avec leur propre copie distincte du système d'exploitation et des applications. Le partitionnement logique est généralement utilisé pour permettre l'utilisation de différents systèmes d'exploitation et d'applications sur un même dispositif. Les partitions peuvent être configurées ou non pour communiquer entre elles ou partager certaines ressources du serveur, comme les interfaces réseau par exemple.
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 performante.*
Masquage	Dans le cadre des normes PCI DSS, il s'agit d'une méthode de dissimulation d'un segment de données lorsqu'elles sont affichées ou imprimées. Le masquage est utilisé si aucune exigence professionnelle ne justifie d'afficher le PAN dans son intégralité. Le masquage a trait à la protection du PAN lorsqu'il est affiché ou imprimé. Voir *Troncature* pour la protection du PAN lorsqu'il est stocké dans des fichiers, bases de données, etc.
Menace	Situation ou activité susceptible d'entraîner la perte, la modification, l'exposition ou l'indisponibilité intentionnelle ou accidentelle de renseignements ou de ressources de traitement des renseignements, ou encore de les affecter de toute autre manière au préjudice de l'organisation.
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 défini par le fournisseur du logiciel. Les numéros de version sont habituellement attribués en ordre croissant et ils correspondent à un changement spécifique dans le logiciel.
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.
Moniteur d'ordinateur virtuel (VMM)	Le VMM, un logiciel qui met en œuvre une abstraction de matériel informatique virtuel, est compris dans l'hyperviseur. Il gère le processeur du système, la mémoire et d'autres ressources pour attribuer ce que chaque système d'exploitation invité exige.
Mot de passe par défaut	Mot de passe de comptes 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 là même, facilement prévisibles.
Mot de passe/Phrase passe	Chaîne de caractères faisant office d'authentifiant de l'utilisateur.

Terme	Définition
MPLS	Acronyme de « multi protocol label switching » (commutation d'étiquettes multi-protocoles). Réseau ou mécanisme de télécommunication conçu pour connecter un groupe de réseaux à commutation de paquets.
NAC	Acronyme de « network access control » (contrôle d'accès au réseau) ou « network admission control » (contrôle d'admission au réseau). Une méthode de mise en oeuvre 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'interne et des adresses externes qui sont visibles à l'externe.
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.
NIST	Acronyme de « National Institute of Standards and Technology » (Institut national des normes et des technologies). Agence fédérale non réglementaire de l'Administration de la technologie du ministère du commerce des États-Unis.
NMAP	Logiciel d'analyse de la sécurité qui mappe les réseaux et identifie les ports ouverts dans les ressources réseau.
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.
Numéro de compte	Voir *Numéro de compte primaire (PAN).*
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.
Objet au niveau système	Tout objet sur un composant du système 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.

Terme	Définition
OCTAVE[MD]	Acronyme de « 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.
Ordinateur virtuel	Environnement d'exploitation autonome qui se comporte comme un ordinateur séparé. Il est également connu comme « Invité », et fonctionne au-dessus d'un hyperviseur.
OWASP	Acronyme de « Open Web Application Security Project » (projet de sécurité d'application Web ouverte). Un organisme sans but lucratif fondé en 2004 et dédié à l'amélioration de la sécurité des logiciels d'application. L'OWASP gère une liste de vulnérabilités critiques pour les applications Web. (Voir http://www.owasp.org).
PA-DSS (Application de paiement - Normes en matière de sécurité des données)	Acronyme de « Payment Application Data Security Standard » (norme de sécurité des données des applications 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	Dans le domaine de la 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 de carte de paiement unique (typiquement pour les cartes de crédit ou de débit) qui identifie l'émetteur et le compte du titulaire de carte spécifique).
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 ports.
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 équipés de différents niveaux de sécurité, selon un ensemble de règles et d'autres critères.
PCI	Acronyme de « Payment Card Industry » (industrie des cartes de paiement).
PCI DSS (Norme en matière de sécurité des données de PCI)	Acronyme de « Payment Card Industry Data Security Standard » (norme de sécurité des données de l'industrie des cartes de paiement).

Terme	Définition
PDA	Acronyme de « personnel data assistant » ou de « personal digital assistant » (assistant numérique personnel). Appareils mobiles de poche équipés de fonctionnalités comme le téléphone mobile, la messagerie électronique ou le navigateur Internet.
PED	Dispositif de saisie du code PIN.
Périphériques cryptographiques sécurisés	Un ensemble de matériel, de logiciels et de micrologiciels qui met en oeuvre 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.
Personnel	Employés à temps plein et à temps partiel, intérimaires ainsi que sous-traitants et consultants qui « résident » sur le site de l'entité ou qui ont accès à l'environnement des donnés de titulaire de carte.
PIN	Acronyme de « personal identification number » (numéro d'identification personnel). Mot de passe numérique secret, connu uniquement de l'utilisateur et du système sur lequel l'utilisateur s'authentifie. L'utilisateur n'accède au système que si le code PIN qu'il saisit correspond à celui enregistré dans le système. Les codes PIN peuvent être utilisés pour les distributeurs automatiques lors de retraits d'espèces. Un autre type de code PIN se trouve sur les cartes à puce EMV et remplace la signature du titulaire de carte.
Piste de vérification	Voir *Journal de vérification.*
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 de matériel et logiciel et est hébergé dans un équipement d'acceptation pour permettre à un titulaire de carte d'effectuer une transaction par carte. Le POI peut être surveillé ou non. Les transactions POI sont généralement des transactions de paiement par carte par circuit intégré (puce) et/ou par une bande magnétique.
Point d'accès sans fil	Également rencontré sous la forme « AP » (Access Point). Équipement 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 périphériques sans fil et des périphériques câblés sur le réseau.
Politique	Règle à l'échelle de l'organisation régissant l'utilisation acceptable des ressources informatiques, les pratiques en matière de sécurité, et guidant l'élaboration des procédures opérationnelles.
Politique de sécurité	Ensemble de lois, règles et pratiques régissant la manière dont une organisation gère, protège et distribue des renseignements sensibles.
POP3	Acronyme de « Post Office Protocol v3 » (protocole de poste v3). Protocole au niveau de l'application utilisé par les logiciel de courrier électronique client pour récupérer les courriels d'un serveur distant avec une connexion TCP/IP.

Terme	Définition
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.
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. Comprend également les sociétés qui fournissent des services contrôlant ou susceptibles d'affecter la sécurité des données de titulaire de carte. 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 sont des prestataires de services. 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 (même si elle puisse être considérée comme un prestataire de service pour d'autres services).
Prêt à l'emploi	Description de produits en stock non spécifiquement personnalisés ou conçus pour un client ou un utilisateur particulier et prêts à l'emploi.
Procédure	Narration descriptive d'une politique. La procédure est le « comment faire » d'une politique et décrit la manière dont celle-ci est mise en œuvre.
Programme malveillant furtif	Type de logiciel malveillant qui, une fois installé sans autorisation, est capable de dissimuler sa présence et d'obtenir le contrôle administratif d'un système informatique.
Protocole	Méthode de communication convenue dans le cadre des réseaux. Spécifications décrivant les règles et procédures auxquelles les produits informatique doivent se conformer pour exécuter leurs activités sur un réseau.
Protocoles de sécurité	Protocoles de communication réseaux conçus pour sécuriser la transmission de données. Les exemples de protocoles de sécurité comprennent, mais sans s'y limiter, SSL/TLS, IPSEC, SSH, HTTPS, etc.
Protocole/service/port non sécurisés	Protocole, service ou port entraînant 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.
PTS	Acronyme de « PIN Transaction Security » (sécurité des transactions PIN), la PTS est un ensemble d'exigences d'évaluation modulaire géré par le Conseil de normes de sécurité PCI pour l'acceptation du code PIN par les terminaux POI. Se référer à www.pcisecuritystandards.org.
PVV	Acronyme de valeur de vérification de code PIN. Valeur secondaire codée sur la bande magnétique de la carte de paiement.

Terme	Définition
QAÉ	Acronyme de questionnaire d'auto-évaluation. Outil de rapport utilisé pour documenter les résultats de l'auto-évaluation de l'évaluation PCI DSS d'une entité.
QIR	Acronyme d'intégrateur ou revendeur qualifié. Consultez le *Guide de programme QIR* sur le site Internet PCI SSC pour de plus amples informations.
QSA	Acronyme de « Qualified Security Assessor » (évaluateur de sécurité qualifié). Les QSA sont qualifiés par PCI SSC pour réaliser des évaluations PCI DSS sur site. Consultez les *conditions de qualification QSA* pour plus de détails sur les conditions s'appliquant aux sociétés et aux employés QSA.
RADIUS	Abréviation de « Remote authentication and Dial-In User Service » (service d'usager commuté à authentification distante). Système d'authentification et système comptable Vérifie si des renseignements tels que le nom d'utilisateur et le mot de passe communiqués au serveur RADIUS sont exacts, et autorise ensuite l'accès au système. Cette méthode d'authentification peut être utilisée avec un jeton, une carte à puce, etc., pour fournir une authentification à deux facteurs.
RFC 1918	Norme identifiée par l'IETF (Internet Engineering Task Force) qui définit l'usage et les plages d'adresses appropriées pour des réseaux privés (non routable sur Internet).
Renseignements 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.
Renseignements personnels permettant l'identification.	Renseignements qui peuvent être utilisés pour identifier un individu, y compris, mais sans s'y limiter, ses nom, adresse, numéro de sécurité sociale, données biométriques, date de naissance, etc.
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.
Requêtes paramétrées	Un moyen de structuration des requêtes SQL pour limiter les fuites et empêcher les attaques par injection.
Réseau	Deux ou plusieurs ordinateurs connectés ensemble par des moyens physiques ou sans fil.
Réseau approuvé	Réseau de contrôle et de gestion d'une organisation.
Réseau non approuvé	Réseau externe aux réseaux appartenant à une organisation et qui n'est pas sous le contrôle ou la gestion de l'organisation.
Réseau privé	Réseau mis en place par une organisation qui utilise un espace privé d'adresse IP. Les réseaux privés sont communément désignés comme les réseaux locaux. L'accès aux réseaux privés à partir de réseaux publics doit être correctement protégé par des pare-feu et des routeurs.

Terme	Définition
Réseau public	Réseau mis en place et exploité par un prestataire de services de télécommunication dans le but spécifique de fournir au public des services de transmission de données. Les données circulant sur les réseaux publics peuvent être interceptées, modifiées et/ou détournées lors de leur transmission. Internet, ainsi que les technologies sans fil et mobiles font partie des réseaux publics pris en considération par les PCI DSS.
Réseau sans fil	Réseau qui connecte les ordinateurs sans connexion physique par des câbles.
Responsable de la sécurité	Personne principalement responsable des affaires liées à la sécurité d'une entité.
Revendeur/Intégrateur	Entité qui vend et/ou intègre des applications de paiement mais ne les développe pas.
ROC	Acronyme de « Report on Compliance » (rapport sur la conformité). Rapport documentant les résultats détaillés de l'évaluation PCI DSS d'une entité.
Routeur	Matériel ou logiciel connectant deux réseaux ou plus. Fonctions de tri et d'interprétation par l'examen d'adresses et la transmission d'éléments d'information vers des destinations appropriées. Les routeurs de logiciel sont parfois désignés sous le nom de « passerelles ».
ROV	Acronyme de « Report on Validation » (rapport sur la validation). Rapport qui documente 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'acronyme RSA est constitué des initiales de leurs noms de famille.
SANS	Acronyme de « SysAdmin, Audit, Networking and Security », un institut qui propose une formation sur la sécurité informatique et une certification professionnelle. (Voir www.sans.org).
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.
Sauvegarde	Copie de données dupliquées réalisée à des fins d'archivage ou de protection contre d'éventuels dommages ou pertes.
Schéma	Description formelle de la manière dont une base de données est construite, y compris l'organisation des éléments de données.
Schéma du réseau	Un schéma qui montre les composants et les connexions du système dans un environnement de réseau.
SDLC	Acronyme de « system development life cycle » ou « software development lifecycle » (cycle de vie de développement de système). Phases de conception d'un logiciel ou d'un système informatique incluant la planification, l'analyse, la conception, les tests et la mise en œuvre.

Terme	Définition
Sécurité des renseignements	Protection des renseignements garantissant la confidentialité, l'intégrité et la disponibilité.
Segmentation réseau	Également nommé segmentation ou isolation. La segmentation de réseau isole les composants du système qui stockent, traitent ou transmettent les données de titulaire de carte, des systèmes qui ne le font pas. Une segmentation adéquate du réseau peut réduire la portée de l'environnement de données de titulaire de carte, et ainsi la portée de l'évaluation PCI DSS. Voir la section Segmentation de réseau dans les *Conditions et procédures d'évaluation de sécurité PCI DSS* pour plus de renseignements sur son utilisation. La segmentation de réseau n'est pas une exigence des normes PCI DSS.
Séparation des obligations	Pratique consistant à répartir les diverses étapes d'une fonction entre diverses personnes, afin d'éviter qu'une personne seule ne puisse subvertir l'ensemble du processus.
Serveur	Ordinateur fournissant un service à d'autres ordinateurs, tel que le traitement de communications, le stockage de fichiers ou l'accès à une imprimante. Les serveurs incluent notamment Internet, les bases de données, les applications, les systèmes d'authentification, les DNS, les serveurs de messagerie, les proxies et NTP.
Serveur proxy	Un serveur qui agit comme un intermédiaire entre un réseau interne 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.
Serveur web	Ordinateur contenant un programme qui accepte les requêtes HTTP des clients web et fournit les réponses HTTP (en général des pages web).
Services d'émission	Les exemples de services d'émission comprennent, mais sans s'y limiter, l'autorisation et la personnalisation de la carte.
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.*
SHA-1/SHA-2	Acronyme de « Secure Hash Algorithm » (algorithme de hachage sécurisé). Famille ou ensemble de fonctions de chiffrement cryptographique incluant SHA-1 et SHA-2. Voir *Cryptographie performante.*
SNMP	Acronyme de « Simple Network Management Protocol » (protocole de gestion de réseau simple). Prend en charge le contrôle des dispositifs liés au réseau lorsqu'une attention administrative est requise.
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.
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.

Terme	Définition
SSL	Acronyme de « Secure Sockets Layer » (protocole SSL). Norme sectorielle établie qui crypte le canal entre un navigateur ou un serveur Internet, afin de garantir le caractère privé et la fiabilité des données transmises sur ce canal. Voir *TLS.*
Supports électroniques amovibles	Supports qui stockent des données numériques facilement déplaçables et/ou transportables d'un système informatique à un autre. Les CD-ROM, les DVD-ROM, les clés USB et les disques durs amovibles sont des supports électroniques amovibles.
SysAdmin	Abréviation de « system administrator » (administrateur de système). Personne bénéficiant de hauts privilèges, responsable de la gestion d'un système informatique ou d'un réseau.
Système d'exploitation (ES)	Logiciel d'un système informatique chargé de la gestion et de la coordination de l'ensemble des activités et du partage des ressources informatiques. Microsoft Windows, Mac OS, Linux et Unix sont des exemples de systèmes d'exploitation.
Système de renseignements	Ensemble distinct de ressources en données structurées pour la collecte, le traitement, la maintenance, l'utilisation, le partage, la diffusion ou l'élimination des renseignements.
Système mainframe	Ordinateurs conçus pour traiter de grands volumes d'entrée et de sortie de données et mettre l'accent sur le rendement. Les systèmes mainframe sont capables d'exécuter plusieurs systèmes d'exploitation, comme avec plusieurs ordinateurs. De nombreux systèmes patrimoniaux sont équipés d'un système mainframe.
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 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 jeton, une carte à puce, etc., pour fournir une authentification à deux facteurs.
TCP	Acronyme de « Transmission Control Protocol » (protocole de contrôle de transmission). L'un des principaux protocoles de couche transport de la suite de protocole Internet (IP) et la langue de communication, ou protocole de base d'Internet. Voir *IP*.
TDES	Acronyme de « Triple Data Encryption Standard », également appelé 3DES ou triple DES. Cryptage par bloc créé à partir du cryptage DES utilisé trois fois. Voir *Cryptographie performante.*
Technologies cellulaires	Les communications mobiles par les réseaux téléphoniques sans fil, y compris notamment le Système Global pour communication Mobile (GSM), le Code division accès multiple (CDMA) et le Service radio paquet général (GPRS).

Terme	Définition
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 renseignements d'identification des utilisateurs sont transmis en texte clair.
Terminal de paiement virtuel	Un terminal de paiement virtuel est un accès basé sur un navigateur web à un acquéreur, un processeur ou un site web d'un prestataire de services tiers pour autoriser des transactions par carte de paiement, pour lequel le commerçant saisit manuellement les données de carte de paiement par le biais d'un navigateur web connecté sécurisé. Contrairement aux terminaux physiques, les terminaux virtuels ne lisent pas les données directement sur une carte de paiement. Parce que les transactions par carte de paiement sont saisies manuellement, les terminaux virtuels sont généralement utilisés au lieu des terminaux physiques dans des environnements de commerçants ayant de faibles volumes de transactions.
Test de pénétration	Les tests de pénétration tentent d'identifier les manières d'exploiter les vulnérabilités pour contourner ou vaincre les fonctions sécuritaires des composants du système. Le test de pénétration 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 bien sur le plan externe (test externe) qu'au sein du réseau.
Titulaire de carte	Client, consommateur ou non, auquel une carte de paiement est délivrée ou toute personne autorisée à utiliser une carte de paiement.
TLS	Acronyme de « Transport Layer Security » (sécurité de couche transport). Conçue 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.
Troncature;	Méthode permettant de rendre le PAN entièrement illisible en supprimant en permanence un segment de ses données. La troncature a trait à la protection du PAN lorsqu'il est *stocké* dans des fichiers, bases de données, etc. Voir *Masquage* pour la protection du PAN lorsqu'il est *affiché* sur des écrans, des reçus papier, etc.
URL	Acronyme de « Uniform Resource Locator » (localisateur de ressources uniformes).Une chaîne de texte formatée utilisée par les navigateurs Web, les logiciels de courrier électronique client et les autres logiciels pour identifier une ressource du réseau sur Internet.
Usurpation d'adresse IP	Technique d'attaque utilisée pour obtenir un accès non autorisé à des réseaux ou des ordinateurs. Le pirate envoie des messages trompeurs à un ordinateur avec une adresse IP indiquant que le message provient d'un hôte de confiance.
Utilisateurs non-clients	Toute personne, à l'exception des clients consommateurs, accédant à des systèmes, notamment des employés, des administrateurs et des parties tierces.

Terme	Définition
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.
Valeur ou code de validation de carte	Également connu(e) sous le nom de code de sécurité de la carte. Réfère soit : (1) aux données de bande magnétique, soit (2) aux fonctions de sécurité imprimées. (1) Éléments 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 qui révèlent une altération ou une contrefaçon. Désigné(e) par les acronymes CAV, CVC, CVV ou CSC, en fonction de la marque de la carte de paiement. La liste ci-après inclut les termes pour chaque marque : ▪ **CAV –** Card Authentication Value, valeur d'authentification de carte (cartes de paiement JCB) ▪ **CVC –** Card Validation Code, code de validation de carte (cartes de paiement MasterCard) ▪ **CVV –** Card Verification Value, valeur de vérification de carte (cartes de paiement Visa et Discover) ▪ **CSC –** Card Security Code, code de sécurité de carte (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 une valeur à trois chiffres imprimée à droite de l'espace signature au dos de la carte. Pour les cartes de paiement American Express, le code est un numéro à quatre chiffres imprimé (et non gravé) au-dessus du PAN, au recto de la carte. Le code est associé à chaque carte de plastique et lie le PAN à cette carte. La liste ci-après inclut les termes pour chaque marque : ▪ **CID –** Card Identification Number, numéro d'identification de carte (cartes de paiement American Express et Discover) ▪ **CAV2 –** Card Authentication Value 2, valeur d'authentification de carte 2 (cartes de paiement JCB) ▪ **CVC2 –** Card Validation Code 2, code de validation de carte 2 (cartes de paiement MasterCard) ▪ **CVV2 –** Card Verification Value 2, valeur de vérification de carte 2 (cartes de paiement Visa)
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.*

Terme	Définition
Virtualisation	La virtualisation se réfère à l'abstraction logique des ressources informatiques des contraintes physiques. Une abstraction commune est l'ordinateur virtuel ou VM, recevant le contenu d'un ordinateur physique et lui permettant de fonctionner sur un matériel physique différent et/ou avec d'autres ordinateurs virtuels sur le même matériel physique. En plus des VM, une virtualisation peut être effectuée sur beaucoup d'autres ressources informatiques, notamment des applications, des ordinateurs de bureaux, des réseaux et un espace 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 réseau local physique traditionnel unique.
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 grand, comme Internet, remplaçant les connexions directes par des câbles physiques. Les extrémités du réseau virtuel sont liées à travers le réseau plus grand, le cas échéant. Alors qu'une application commune consiste en plusieurs communications sécurisées par le réseau Internet public, un VPN peut avoir ou non des fonctionnalités de sécurité, comme l'authentification ou le cryptage du contenu. Un VPN peut être utilisé avec un jeton, une carte à puce, etc., pour fournir une authentification à deux facteurs.
Vulnérabilité	Défaut ou faiblesse qui, s'il est exploité, peut compromettre, intentionnellement ou non, un système.
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 entreprise.
WEP	Acronyme de « Wired Equivalent Privacy » (protocole WEP). Algorithme faible utilisé pour crypter les réseaux sans fil. De nombreuses faiblesses différentes 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.*
WLAN	Acronyme de « wireless local area network » (réseau local sans fil). Réseau qui relie au moins deux ordinateurs ou périphériques sans câbles.
WPA/WPA2	Acronyme de « WiFi Protected Access » (accès WiFi protégé). Protocole de sécurité créé pour sécuriser les réseaux sans fil. Le WPA a remplacé le WEP. Il existe désormais un WPA de nouvelle génération, le WPA2.
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. Cette définition exclut les zones où ne sont installés que des terminaux de point de vente, tels que les zones de caisse dans un magasin.