LES DOSSIERS TECHNIQUES

PCI DSS v3.2 :

Vers un processus métier comme les autres

Septembre 2016

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador - 75009 Paris
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

Table des matières

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Pierre-Emmanuel	**LERICHE**	*Verizon*

Les contributeurs :

Stéphane	**BIBILONI**	*Hewlett Packard Enterprise*
Frédéric	**JESUPRET**	*Allianz Worldwide Partners*
Hervé	**SCHAUER**	*HSC by Deloitte*
Abdellaziz	**TALEB**	*Modis*

I. Introduction – Synthèse de la brève

Un an après la sortie du standard PCI DSS version 3.1, le PCI SSC a publié la version 3.2. Celui-ci n'est pas une révolution mais comporte un certain nombre d'évolutions significatives. La plupart sont considérées comme des bonnes pratiques de sécurité jusqu'au 31 janvier 2018 et seront obligatoires à partir du 1er février 2018.

Le standard dans sa version 3.2 est utilisable depuis sa sortie en avril 2016 mais il ne sera véritablement obligatoire de l'utiliser qu'à partir du 1er novembre 2016. En d'autres termes, il ne sera plus possible de réaliser des audits ou questionnaires d'auto-évaluation avec la version 3.1 à partir de cette date.

Le groupe de travail PCI DSS du CLUSIF présente ici son analyse des ajouts significatifs par rapport à la précédente version, ainsi que leurs impacts probables pour les sociétés engagées dans une démarche de mise en conformité. Cette analyse s'appuie sur les documents originaux disponibles sur le site du PCI SSC :

- Référentiel v3.2[1]
- Synthèse reprenant les modifications apportées entre les versions 3.1 et 3.2[2]

[1] https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

[2] https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss_summary_of_changes

II. Glossaire

Terme	Signification Acronyme	Explication
Acquéreur		Organisme financier ou assimilé ayant passé un accord avec un accepteur en vue de l'acquisition des données des transactions faites par carte, qui introduit ces données dans les systèmes d'échanges des émetteurs. C'est la banque domiciliataire du commerçant. Un organisme financier peut être à la fois acquéreur et émetteur
CDE	CardHolder Data Environment	L'environnement informatique utilisé pour le stockage, le traitement ou le transfert des CHD
CHD	CardHolder Data	Ce sont les données du porteur de carte. Elles comprennent en particulier le PAN, la date de fin de validité de la carte et le CVx2
Émetteur		Organisme financier ou assimilé qui émet une carte au profit d'un porteur. C'est la banque du porteur. Un organisme financier peut être à la fois émetteur et acquéreur.
HSM	Hardware Security Module	Il s'agit d'un matériel électronique offrant un service de sécurité qui consiste à générer, stocker et protéger des clefs cryptographiques. Selon son mode d'implémentation, il peut également être utilisé pour chiffrer des données.
Masquage		Masquage du PAN lorsqu'il est affiché (en d'autres termes, une partie seulement du PAN est révélée à l'écran, dans les rapports, les reçus, etc.).
Non-console		L'accès à un système par un administrateur est qualifié de "non-console" lorsqu'il s'effectue au travers du réseau, par opposition à un accès console, qui survient lorsque l'administrateur interagit directement avec un écran et un clavier physiquement connectés au système. Voici des exemples d'accès administratifs non-console : utilisation d'un outil de bureau à distance (RDP), de console à distance (SSH), ou d'une interface d'administration web, etc.
PAN	Primary Account Number	C'est ce qu'on appelle le numéro de carte bancaire composé généralement de 16 chiffres. Il est embossé sur la face avant de la carte, il fait partie des données figurant sur la piste ISO2 au dos de la carte et également dans les données de la puce.
PCI DSS	PCI Data Security Standard	Standard de sécurité qui s'applique aux systèmes d'informations qui manipulent des données sensibles au sens PCI (essentiellement les données des porteurs de carte comme le numéro de carte).
PCI PTS	PCI PIN Transaction Security	Standard de sécurité actuellement en vigueur au plan international pour les terminaux de paiement avec saisie du code PIN.
PCI SSC	PCI Security Standards Council	Organisme responsable du maintien des standards PCI DSS, de leur promotion et de leur encadrement.

POI	Point of Interaction	Point d'interaction (Lecteur de carte, terminal de paiement…).
POS	Point of Sale	Point de vente
QSA	Qualified Security Assessor	Prestataire habilité par le PCI SSC pour réaliser des audits PCI DSS.
Segmentation		La segmentation réseau est une technique ayant pour objectif de diviser un réseau informatique en plusieurs sous-réseaux. La segmentation est principalement utilisée afin d'augmenter les performances globales du réseau et améliorer sa sécurité.
SSL	Secure Sockets Layer	Protocoles de sécurisation des échanges sur Internet. Le protocole SSL a été développé à l'origine par Netscape. L'IETF, en a poursuivi le développement en le rebaptisant Transport Layer Security (TLS).
TLS	Transport Layer Security	Protocoles de sécurisation des échanges sur Internet. Cf. SSL
Troncature		La troncature vise à ce qu'une partie seulement du PAN soit stockée. La FAQ du PCI SSC précise les différents formats de troncature autorisés en fonction des cartes traitées : https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/What-are-acceptable-formats-for-truncation-of-primary-account-numbers

III. Protection des données stockées

Exigence	Type	Domaine	Applicabilité	Entité impactée
3.3	Évolution mineure	Organisationnel et technique	1er novembre 2016	Marchands et fournisseurs de services

Libellé de l'exigence

3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.

Traduction française (traduction officielle du PCI SSC)

3.3 Masquer le PAN lorsqu'il s'affiche (les six premiers chiffres et les quatre derniers sont le maximum de chiffres affichés), de manière à ce que seul le personnel, dont le besoin commercial est légitime, puisse voir plus que les six premiers/les quatre derniers chiffres du PAN.

Contrôle de couverture de l'exigence

Le QSA vérifiera la politique et la procédure de gestion et de maintien d'une liste de fonctions, justifiées par un besoin métier, permettant d'accéder à plus que les premiers 6 chiffres et les quatre derniers chiffres du PAN. L'approche du masquage devrait toujours s'assurer qu'est affiché uniquement le nombre minimum de chiffres nécessaires pour réaliser une fonction.

Le QSA vérifiera le paramétrage des systèmes, les différents écrans accessibles aux opérateurs, et prendra des captures d'écran pour s'assurer du respect de cette exigence.

Point(s) d'attention ou impact(s) à envisager

Il est donc nécessaire pour satisfaire cette exigence de maintenir à jour une documentation et des procédures qui montrent l'adéquation entre le nombre de chiffres affichés et l'utilisation métier de ces affichages.

IV. Gestion du matériel cryptographique

Exigence	Type	Domaine	Applicabilité	Entité impactée
3.5.1	Nouvelle exigence	Organisationnel et technique	1er février 2018	Fournisseurs de services

Libellé de l'exigence

3.5.1 Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes:

- ***Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date***
- ***Description of the key usage for each key***
- ***Inventory of any HSMs and other SCDs used for key management***

Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.

Traduction française (traduction officielle du PCI SSC)

3.5.1 Conditions supplémentaires pour les prestataires de services uniquement : Conserver une description documentée de l'architecture cryptographique qui comprend ce qui suit :

- ***Détails de tous les algorithmes, protocoles et clés utilisés pour protéger les données de titulaires de carte, y compris la robustesse des clés et la date d'expiration***
- ***Description de l'utilisation de chaque clé***
- ***Inventaire des HSM et autres SCD dans le cadre de la gestion des clés***

Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.

Contrôle de couverture de l'exigence

Le QSA contrôlera qu'il existe un document à jour décrivant l'architecture cryptographique comprenant les trois points mentionnés ci-dessus et mènera des entretiens avec le personnel pour vérifier sa bonne application.

Le QSA pourra également demander à l'opérateur accrédité d'accéder aux HSM (récupération des identifiants de clés, usages et algorithmes) et aux numéros de séries des HSM, SCD pour en vérifier la présence dans l'inventaire.

Point(s) d'attention ou impact(s) à envisager

Cette exigence s'applique uniquement pour les données qui sont stockées. Le transport n'est pas pris en compte. Mais elle impose la mise en place d'un plan de contrôle pour s'assurer de sa bonne application. En maintenant ce document à jour, le fournisseur de service sera plus à même à faire évoluer son infrastructure pour répondre à l'évolution des exigences cryptographiques (algorithmes, longueur des clefs, expiration des certificats…).

V. La gestion du changement

Exigence	Type	Domaine	Applicabilité	Entité impactée
6.4.6	Nouvelle exigence	Organisationnel	1er février 2018	Marchands et fournisseurs de services

Libellé de l'exigence

6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.

Traduction française (traduction officielle du PCI SSC)

6.4.6 Suite à un changement important, toutes les conditions pertinentes PCI DSS doivent être mises en œuvre sur tous les systèmes et réseaux, qu'ils soient nouveaux ou modifiés, et la documentation est mise à jour, le cas échéant.

Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.

Contrôle de couverture de l'exigence

Le processus de gestion du changement doit être en mesure de produire les preuves nécessaires. Lors de l'audit annuel, le QSA vérifiera tout d'abord les changements significatifs qui ont eu lieu pendant les 12 derniers mois, puis demandera à l'audité de fournir les preuves associées (ex : checklist PCI DSS associée à chaque changement).

Lors de l'audit, le QSA vérifiera :

- l'existence et la pertinence de la procédure de gestion du changement ;
- que les changements significatifs ont été correctement référencés ;
- que l'ensemble des exigences applicables ont été couvertes ;
- un échantillon de tickets de changement.

Point(s) d'attention ou impact(s) à envisager

Il est important de faire évoluer le processus de gestion du changement afin de permettre le respect de cette nouvelle exigence. L'objectif est de s'assurer du maintien de la conformité et d'éviter d'oublier la mise en conformité de certains composants qui auraient pu être installés pendant l'année.

Il n'est pas obligatoire de faire appel à un QSA pour réaliser un audit du périmètre après chaque changement significatif. Cependant, il est recommandé d'inclure le QSA dans le cadre d'un changement significatif, et éventuellement de lui demander de prendre position sur la validité des mesures de sécurité mises en place.

VI. La formation des développeurs

Exigence	Type	Domaine	Applicabilité	Entité impactée
6.5	Clarification	Organisationnel	1er novembre 2016	Marchands et fournisseurs de services

Libellé de l'exigence

6.5 Address common coding vulnerabilities in software-development processes as follows :

- ***Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities.***
- ***Develop applications based on secure coding guidelines.***

Traduction française (traduction officielle du PCI SSC)

6.5 Adresser les vulnérabilités de code les plus fréquentes dans les processus de développement de logiciel, afin d'inclure les éléments suivants :

- ***Former les développeurs au moins une fois par an pour perfectionner leurs techniques de codage sécurisé, afin qu'ils sachent notamment comment éviter les vulnérabilités de codage courantes.***
- ***Développer des applications basées sur les directives de codage sécurisé.***
-

Contrôle de couverture de l'exigence

Lors de l'audit annuel, le QSA vérifiera à la fois que la formation aux techniques de développement sécurisés est requise de manière annuelle pour les développeurs (examen des politiques et programmes de formation notamment), que cette formation leur a réellement été apportée de manière annuelle (attestation de formations, feuilles d'émargement, …), et que son contenu est basé sur les meilleures pratiques et les directives de l'industrie (plan des formations suivies). Il vérifiera également si la teneur de la formation est adaptée aux technologies utilisées par l'audité, et si les politiques et procédures en matière de développement permettent de protéger les applications d'une liste de vulnérabilités explicitement décrites dans le standard (CRSS, XSS, SQL injection, Gestion des exceptions, etc)

Point(s) d'attention ou impact(s) à envisager

Dans les versions précédentes du standard, l'obligation de formation des développeurs, bien que déjà présente, ne revêtait pas de caractère de fréquence minimale obligatoire. L'audité était tenu de s'assurer que le niveau de formation de ses développeurs était approprié, c'est-à-dire en accord avec les pratiques de codage sécurisé en vigueur dans son secteur. Avec la version 3.2, l'obligation d'une fréquence annuelle des formations est introduite, ce qui va engendrer la nécessité pour les organisations de s'assurer que les plans de formation de ses développeurs sont bien en accord avec cette fréquence, et que les formations suivies datent bien de moins d'un an au moment de l'audit annuel.

VII. Authentification

Exigence	Type	Domaine	Applicabilité	Entité impactée
8.3	Nouvelle exigence	Organisationnel et technique	1er février 2018	Marchands et fournisseurs de services

Libellé de l'exigence

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.

8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.

Traduction française (traduction officielle du PCI SSC)

8.3 Sécuriser tous les accès administratifs non-console et tous les accès distants au CDE par authentification à plusieurs facteurs.
8.3.1 Incorporer l'authentification à plusieurs facteurs pour tous les accès non-console dans CDE pour les membres du personnel dotés d'un accès administratif.
8.3.2 Incorporer une authentification à plusieurs facteurs pour tous les accès réseau à distance (utilisateur et administrateur, y compris l'accès des parties tierces dans un souci d'assistance ou de maintenance) provenant de l'extérieur du réseau de l'entité.

Contrôle de couverture de l'exigence

Cette exigence était auparavant applicable uniquement aux accès distants, mais de nombreuses attaques étant basées sur le vol d'identifiants de connexion, elle est aujourd'hui étendue à l'ensemble des accès administratifs non-console, même ceux émanant de l'intérieur de l'entité. Tandis que dans les versions précédentes du standard, il était fait mention d'authentification double facteur, la notion employée est dorénavant l'authentification à multiple facteurs. Ceci offre la possibilité aux organisations qui le souhaitent d'utiliser plus que deux facteurs d'authentification, leur permettant de complexifier encore davantage une éventuelle compromission, tout en garantissant le respect de l'exigence telle qu'elle est maintenant formulée.

Durant l'audit, le QSA :

- vérifiera les configurations systèmes ;
- interviewera les administrateurs et leur demandera de se connecter aux équipements afin de vérifier que leur authentification est conditionnée à la fourniture de plusieurs facteurs.

VIII. Journalisation

Exigence	Type	Domaine	Applicabilité	Entité impactée
10.8.x	Nouvelle exigence	Organisationnel et technique	1er février 2018	Fournisseurs de services

Libellé de l'exigence

10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:

- ***Firewalls***
- ***IDS/IPS***
- ***FIM***
- ***Anti-virus***
- ***Physical access controls***
- ***Logical access controls***
- ***Audit logging mechanisms***
- ***Segmentation controls (if used)***

10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:

- ***Restoring security functions***
- ***Identifying and documenting the duration (date and time start to end) of the security failure***
- ***Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause***
- ***Identifying and addressing any security issues that arose during the failure***
- ***Performing a risk assessment to determine whether further actions are required as a result of the security failure***
- ***Implementing controls to prevent cause of failure from reoccurring***
- ***Resuming monitoring of security controls***

Traduction française (traduction officielle du PCI SSC)

10.8 Condition supplémentaire pour les prestataires de services uniquement : Implémenter un processus pour détecter et signaler à temps les pannes des systèmes de contrôle de sécurité critiques, y compris, mais sans s'y limiter, les pannes relatives aux :

- **Pare-feu**
- **IDS/IPS**
- **FIM**
- **Antivirus**
- **Contrôles d'accès physiques**
- **Contrôles d'accès logiques**
- **Mécanismes de journalisation d'audit**
- **Contrôles de segmentation (le cas échéant)**

10.8.1 Condition supplémentaire pour les prestataires de services uniquement : Intervenir face aux pannes de contrôles de sécurité critiques en temps opportun. Les processus de résolution des pannes de contrôles de sécurité doivent comprendre :

- **Rétablissement des fonctions de sécurité**

Exigence	Type	Domaine	Applicabilité	Entité impactée
10.8.x	Nouvelle exigence	Organisationnel et technique	1er février 2018	Fournisseurs de services

- **Identification et documentation de la durée (date et heure de début et de fin) de la panne de sécurité**
- **Identification et documentation des causes de la panne, y compris la cause fondamentale, et documentation des rectificatifs requis pour résoudre la cause fondamentale**
- **Identification et résolution des problèmes de sécurité survenus pendant la panne**
- **Évaluation des risques pour déterminer si d'autres actions sont indispensables suite à une panne de sécurité**
- **Implémentation des contrôles pour prévenir la répétition d'une telle panne**
- **Reprise de la surveillance des contrôles de sécurité**

Contrôle de couverture de l'exigence

Lors de l'audit, le QSA :

- vérifiera le mécanisme technique de surveillance des défaillances du système de contrôle ;
- vérifiera également la politique de sécurité et les procédures en place pour répondre aux défaillances des contrôles de sécurité ;
- interviewera le personnel pour s'assurer que l'ensemble des processus de surveillance sont en place.

Point(s) d'attention ou impact(s) à envisager

La mise en œuvre d'un contrôle automatique des défaillances de contrôle de sécurité peut s'avérer difficile à mesurer, et ce d'autant plus qu'elle n'a éventuellement pas d'impact visible sur le fonctionnement de la plateforme. Il peut être nécessaire de mettre en place une vérification manuelle. Le coût de mise en place pour les fournisseurs de service est donc important.

IX. Tests d'intrusion

Exigence	Type	Domaine	Applicabilité	Entité impactée
11.3.4.1	Nouvelle exigence	Organisationnel et technique	1er février 2018	Fournisseurs de services
Libellé de l'exigence				
11.3.4.1 Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods				
Traduction française (traduction officielle du PCI SSC)				
11.3.4.1 Condition supplémentaire pour les prestataires de services uniquement : En cas de segmentation, confirmer le champ d'application de la norme PCI DSS en effectuant des tests de pénétration sur les contrôles de segmentation au moins une fois par semestre et après des modifications apportées aux contrôles/méthodes de segmentation.				
Contrôle de couverture de l'exigence				
Le QSA vérifiera que des tests d'intrusion ont été menés semestriellement pour vérifier l'efficacité de la segmentation. Il vérifiera également que les tests ont été menés par une ressource interne qualifiée ou par un prestataire qualifié et qu'un rapport a été rédigé.				
Point(s) d'attention ou impact(s) à envisager				
Il conviendra de prendre en compte cette nouvelle exigence dans la définition budgétaire annuelle. Les tests d'intrusion devront donner lieu à un rapport qui sera fourni au QSA durant la phase d'audit.				

X. Gouvernance PCI DSS

Exigence	Type	Domaine	Applicabilité	Entité impactée
12.4.1	Nouvelle exigence	Organisationnel et technique	1er février 2018	Fournisseurs de services

Libellé de l'exigence

12.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:

- ***Overall accountability for maintaining PCI DSS compliance***
- ***Defining a charter for a PCI DSS compliance program and communication to executive management***

Traduction française (traduction officielle du PCI SSC)

12.4.1 Condition supplémentaire pour les prestataires de services uniquement : L'équipe de direction a défini la responsabilité relative à la protection des données de titulaires de carte et un programme de conformité à la norme PCI DSS, comme suit :

- **Responsabilité globale pour respecter la conformité à la norme PCI DSS**
  Définition d'une charte pour un programme de conformité à la norme PCI DSS et des canaux de communication avec la direction

Contrôle de couverture de l'exigence

Le QSA examinera la charte définissant le programme de conformité PCI DSS. Il s'assura également que la direction est sensibilisée à la question de la conformité PCI DSS et apporte son support au programme.

Point(s) d'attention ou impact(s) à envisager

Une méthodologie de reporting auprès de la direction (ex : pourcentage de conformité, obtenu ou échec d'une attestation de conformité…) devra être établie.

Il conviendra de sensibiliser la direction aux problématiques de conformité PCI DSS.

XI. Maintien de la conformité PCI DSS

Exigence	Type	Domaine	Applicabilité	Entité impactée
12.11	Nouvelle exigence	Organisationnelle	1er février 2018	Fournisseurs de services

Libellé de l'exigence

12.11 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:

- ***Daily log reviews***
- ***Firewall rule-set reviews***
- ***Applying configuration standards to new systems***
- ***Responding to security alerts***
- ***Change management processes***

Traduction française (traduction officielle du PCI SSC)

12.11 Condition supplémentaire pour les prestataires de services uniquement : Effectuer des vérifications au moins une fois par trimestre pour confirmer que le personnel respecte les politiques de sécurité et les procédures opérationnelles. Les examens doivent couvrir les processus suivants :

- **Examens quotidiens des journaux**
- **Examens des règles liées aux pare-feu**
- **Application des normes de configuration aux nouveaux systèmes**
- **Intervention suite aux alertes de sécurité**
- **Modifier les processus de gestion**

Contrôle de couverture de l'exigence

Le QSA demandera :

- les rapports résultant du contrôle de cette exigence.

Point(s) d'attention ou impact(s) à envisager

Comme pour l'ensemble des exigences récurrentes, il conviendra de s'assurer que cette revue est réalisée assidument sans quoi elle pourrait être considérée comme non conforme par l'auditeur.

XII. Annexes A-1 – Exigences complémentaires pour les prestataires d'hébergement mutualisé

Annexe renumérotée en raison de l'inclusion de nouvelles annexes.

Exigence	Type	Domaine	Applicabilité	Entité impactée
Annexe A1	Changement de numérotation	Organisationnelle	N/A	Prestataire d'hébergement mutualisé
Libellé de l'exigence				
As referenced in Requirement 12.8 and 12.9, all service providers with access to cardholder data (including shared hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.6 states that shared hosting providers must protect each entity's hosted environment and data. **Therefore, shared hosting providers must additionally comply with the requirements in this Appendix.**				
Traduction française (traduction officielle du PCI SSC)				
Comme il est indiqué dans les conditions 12.8 et 12.9, tous les prestataires de services qui ont accès aux données de titulaires de carte (notamment les prestataires de services d'hébergement partagé) doivent respecter la norme PCI DSS. En outre, la condition 2.6 stipule que les prestataires de services d'hébergement partagé doivent protéger les données et l'environnement hébergés de chaque entité. En conséquence, les prestataires de services d'hébergement partagé doivent par ailleurs se conformer aux exigences définies dans cette annexe.				

XIII. Annexes A-2 – Exigences complémentaires pour les entités utilisant SSL ou d'anciennes versions de TLS

Nouvelle annexe avec des exigences supplémentaires pour les entités utilisant SSL ou d'anciennes versions de TLS, incorporant de nouveaux délais de migration pour le retrait de SSL ou d'anciennes versions de TLS.

Exigence	Type	Domaine	Applicabilité	Entité impactée
Annexes A-2	Clarification	Technique	30 Juin 2018 30 Juin 2016 pour les fournisseurs de services	Marchands et fournisseurs de services

Libellé de l'exigence

Entities using SSL and early TLS must work toward upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where those protocols don't already exist.

At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment environments.

However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up to date with vulnerability trends and determine whether or not they are susceptible to any known exploits.

The PCI DSS requirements directly affected are:

Requirement 2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.

Requirement 2.3 Encrypt all non-console administrative access using strong cryptography.

Requirement 4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

SSL and early TLS should not be used as a security control to meet these requirements. To support entities working to migrate away from SSL/early TLS, the following provisions are included:

- **New implementations must not use SSL or early TLS as a security control.**
- **All service providers must provide a secure service offering by June 30, 2016.**
- **After June 30, 2018, all entities must have stopped use of SSL/early TLS as a security control, and use only secure versions of the protocol (an allowance for certain POS POI terminals is described in the last bullet below).**
- **Prior to June 30, 2018, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.**
- **POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS, may continue using these as a security control after June 30, 2018.**

Exigence	Type	Domaine	Applicabilité	Entité impactée
Annexes A-2	Clarification	Technique	30 Juin 2018 30 Juin 2016 pour les fournisseurs de services	Marchands et fournisseurs de services

This Appendix applies to entities using SSL/early TLS as a security control to protect the CDE and/or CHD (for example, SSL/early TLS used to meet PCI DSS Requirement 2.2.3, 2.3, or 4.1), Refer to the current PCI SSC Information Supplement Migrating from SSL and Early TLS for further guidance on the use of SSL/early TLS.

Traduction française (traduction officielle du PCI SSC)

Les entités, qui utilisent le SSL et le TLS initial, doivent s'employer à adopter un protocole cryptographique fiable dès que possible. Qui plus est, le SSL et/ou le TLS initial ne doivent pas être introduits dans des environnements contenant déjà ces protocoles. Au moment de la publication, les vulnérabilités connues sont difficiles à exploiter dans les environnements de paiement POS POI. Cependant, de nouvelles vulnérabilités pourraient survenir à tout moment. C'est à l'organisation de s'informer des dernières tendances en matière de vulnérabilité et de déterminer si celles-ci sont susceptibles de créer des failles connues.

Les conditions de la norme PCI DSS directement concernées sont les suivantes :

- **Condition 2.2.3 : Implémentation des fonctions de sécurité supplémentaires pour tout service, protocole ou démon nécessaire et jugé comme non sécurisé.**
- **Condition 2.3 : Crypter tous les accès administratifs non console, à l'aide d'une cryptographie robuste.**
- **Condition 4.1 : Utiliser des protocoles de cryptographie et de sécurité robustes pour sauvegarder les données des titulaires de cartes sensibles lors de leur transmission sur des réseaux publics et ouverts.**

Ne pas utiliser le SSL et le TLS initial en tant que contrôles de sécurité pour remplir ces conditions. Les mesures suivantes sont disponibles pour aider les entités à abandonner le SSL et le TSL initial :

- **Les nouvelles implémentations ne doivent pas utiliser le SSL ou le TLS initial comme contrôles de sécurité.**
- **D'ici le 30 juin 2016, tous les prestataires de services doivent proposer un service sécurisé.**
- **Après le 30 juin 2018, toutes les entités doivent avoir interrompu leurs recours au SSL/TLS initial en tant que contrôles de sécurité et utiliser exclusivement les versions sécurisées du protocole (le recours à certains terminaux POS POI est autorisé et décrit dans le dernier point ci-dessous).**
- **D'ici le 30 juin 2018, les implémentations existantes, qui utilisent le SSL et/ou le TLS initial, doivent comporter un plan formel d'atténuation des risques et de migration.**
- **Vous pouvez continuer d'utiliser les terminaux POS POI (et les points de terminaisons SSL/TLS auxquels ils sont connectés) en tant que contrôles de sécurité après le 30 juin 2018 après vous être assuré qu'ils ne sont pas susceptibles d'occasionner des failles connues pour le SSL ou le TLS initial.**

Exigence	Type	Domaine	Applicabilité	Entité impactée
Annexes A-2	Clarification	Technique	30 Juin 2018 30 Juin 2016 pour les fournisseurs de services	Marchands et fournisseurs de services

Cette annexe s'applique à toutes les entités ayant recours au SSL/TLS initial en tant que contrôles de sécurité pour protéger le CDE et/ou le CHD (par exemple, utilisation du SSL/TLS initial pour remplir la condition 2.2.3, 2.3 ou 4.1 de la PCI DSS). Se reporter aux récentes informations complémentaires PCI SSC sur la migration depuis le SSL et le TLS initial pour obtenir des directives complémentaires sur l'utilisation du SSL/TLS initial.

Contrôle de couverture de l'exigence

Dans l'esprit de la présente annexe, les entités utilisant SSL ou d'anciennes versions de TLS se doivent de mettre en place un processus de migration vers des protocoles de chiffrement plus robustes. En outre, SSL ou les versions anciennes de TLS ne doivent pas être installées dans des environnements ou ces protocoles sont absents par défaut.

Lors de l'audit, le QSA vérifiera :

- la présence d'un planning de migration,
- que les processus/procédures d'acquisition/développement de nouveaux produits incluent la présente exigence,
- la présence de la liste des équipements à migrer,
- la présence de la liste des équipements dispensés de la conformité.

Point(s) d'attention ou impact(s) à envisager

Si les terminaux de paiement sont vulnérables à des exploits connus, alors la planification de la migration vers une alternative sécurisée devrait commencer immédiatement. L'exemption pour les terminaux de paiement qui ne sont actuellement pas vulnérable aux exploits est basée sur les risques actuels et connus. Si de nouveaux exploits sont découverts, il conviendra de mettre à jour les terminaux de paiement.

XIV. Annexes A-3 – Designated Entities Supplemental Validation

Il est à noter que cette annexe incorpore le contenu du document « PCI DSS Designated Entities Supplemental Validation » publié en juin 2015 et qui est maintenant complètement intégré à la version définitive du standard.

Exigence	Type	Domaine	Applicabilité	Entité impactée
Annexe A3	Clarification	Technique, documentaire et organisationnel	Immédiat	A la discrétion des banques acquéreurs et des réseaux de cartes

Libellé de l'exigence

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Examples of entities that this Appendix could apply to include:

- **Those storing, processing, and/or transmitting large volumes of cardholder data,**
- **Those providing aggregation points for cardholder data, or**
- **Those that have suffered significant or repeated breaches of cardholder data.**

These supplemental validation steps are intended to provide greater assurance that PCI DSS controls are maintained effectively and on a continuous basis through validation of business-as-usual (BAU) processes, and increased validation and scoping consideration.

The additional validation steps in this document are organized into the following control areas:

A3.1 Implement a PCI DSS compliance program.
A3.2 Document and validate PCI DSS scope.
A3.3 Validate PCI DSS is incorporated into business-as-usual (BAU) activities.
A3.4 Control and manage logical access to the cardholder data environment.
A3.5 Identify and respond to suspicious events.

Traduction française (traduction officielle du PCI SSC)

Exigence	Type	Domaine	Applicabilité	Entité impactée
Annexe A3	Clarification	Technique, documentaire et organisationnel	Immédiat	A la discrétion des banques acquéreurs et des réseaux de cartes

Cette annexe s'applique uniquement aux entités désignées par des marques de paiement ou un acquéreur dans la mesure où une validation supplémentaire des conditions PCI DSS existantes est exigée. Exemples d'entités auxquelles cette annexe peut s'appliquer :

- **Entités avec de grands volumes de stockage, traitement et/ou transmission des données de titulaires de carte**
- **Entités avec des points d'agrégation pour les données de titulaires de carte, ou**
- **Entités ayant subi des fuites importantes ou répétées des données de titulaires de cartes.**

Ces étapes de validation complémentaire permettent d'améliorer la gestion efficace et continue des contrôles PCI DSS grâce à la validation des processus d'affaires courantes (business-as-usual, BAU), une validation accrue et une réflexion sur la détermination du champ d'application.

Les étapes de validation supplémentaires figurant dans ce document sont classées en fonction des domaines de contrôle suivants :

- **A3.1 Implémenter un programme de conformité à la norme PCI DSS.**
- **A3.2 Documenter et valider le champ d'application de la norme PCI DSS.**
- **A3.3 Confirmer que la norme PCI DSS est incorporée dans les activités courantes (BAU).**
- **A3.4 Contrôler et gérer l'accès logique à l'environnement des données de titulaires de carte.**
- **A3.5 Identifier et résoudre les événements suspects.**

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 rue de Mogador
75009 Paris
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

Téléchargez toutes les productions du CLUSIF sur
www.clusif.fr