



delivering comprehensive
payment security experience

Résumé des exigences en matière de sécurité liées au chiffrement bout-en-bout

Le 27 mai 2010

La *Secure POS Vendor Alliance*¹ définit le chiffrement bout en bout de la manière suivante, « La transmission des données du titulaire de carte dans un format de chiffrement, à partir de sa présentation, de façon à ce qu'on empêche les données en clair d'être déchiffrées et ce, jusqu'au décryptage. » En d'autres mots, le chiffrement bout-en-bout se réfère à un système où les informations confidentielles du titulaire sont chiffrées à partir de l'accès au système POS et transmis au système du traitement de paiement crypté.

Les *exigences en matière de sécurité liées au chiffrement bout en bout* représentent une gamme de normes d'industrie pour la mise en œuvre du chiffrement bout en bout des dispositifs de paiement. Les exigences définies dans le présent document sont basées sur les normes existantes, telles que celles utilisées pour les transactions par carte de débit. En utilisant les normes existantes, on pourra bénéficier de deux avantages importants : premièrement, les exigences sont basées sur les meilleures pratiques qui ont été éprouvées au sein des environnements dans le domaine de la production ; deuxièmement, le temps et le coût nécessaires pour la mise en œuvre de ces exigences sont minimisés, puisque les parties prenantes sont déjà familiarisées avec les normes en question.

Les *exigences en matière de sécurité liées au chiffrement bout en bout* sont vérifiables, afin qu'une mise en œuvre adéquate puisse être contrôlée et ce, de mise en œuvre en mise en œuvre.

Le document définit les exigences suivantes :

- Informations nécessaire à chiffrer – Ceci définit les informations confidentielles du titulaire qui doivent être chiffrées, y compris les numéros des cartes, détection des informations et les codes de sécurité, tout en tenant compte tout formulaire lié aux informations du titulaire, y compris la Bande magnétique, Smartcard, Contactless et l'entrée manuelle des données.
- Exigences – gestion des clés – Ceci fournit des normes générales tout en se référant aux normes existantes liées aux exigences en question.
- Exigences chiffrement bout en bout – Définit les algorithmes de chiffrement autorisés.

¹ La *Secure POS Vendor Alliance* (SPVA) – Alliance des fournisseurs de solutions sécurisées de paiement pour points de vente)

- Exigences – mesures de sécurité physique – Définit les exigences de sécurité physique des clés et dispositifs cryptographiques
- Exigences – mesure de sécurité logique – Définit les mesures en matière de sécurité logique en ce qui a trait aux opérateurs au sein du processus de la gestion des clés et les applications qui accèdent aux informations confidentielles sur des dispositifs sécurisés.
- Surveillance et des exigences en matière de suivi du chiffrement et système de gestion – Définit les exigences d'enregistrement des systèmes en fin d'opération dans le cadre d'un environnement de chiffrement bout en bout. Cela permet la détection des mécanismes et la vérification des informations, ce qui améliore la sécurité globale et la conformité de la solution.

Les systèmes de chiffrement bout en bout sauront améliorer la sécurité de toutes les parties prenantes dans le cadre des paiements électroniques. Le lancement du système facilitera la mise en œuvre à SPVA de ces systèmes hautement sécurisés à travers l'industrie.

Les recommandations en matière de sécurité du chiffrement de bout-en-bout (« Recommandations E³ ») présentées par la SPVA (Secure POS Vendor Alliance - Alliance des fournisseurs de solutions sécurisées de paiement pour points de vente) résultent d'un travail collectif de l'ensemble de ses membres, et ne saurait représenter le travail ou la réflexion d'une personne ou d'une entreprise membre de SPVA. Bien que tous les efforts aient été portés pour que les Recommandations E₃ s'inscrivent dans les « bonnes pratiques » telles que définies par la SPVA, ni la SPVA ni aucun de ses membres ne peut les garantir d'aucune façon. En conséquence le fait qu'un tiers utilise, fasse référence à ou se prévale de la caution des Recommandations E₃ ne saurait engager la responsabilité de la SPVA ou de ses membres.