Livre blanc sur la sécurité des paiements

Banque de Montréal

CIBC

Banque Nationale du Canada

Banque Royale du Canada

Banque Scotia

Groupe financier TD

13 juillet 2015

.

Table des matières

Introduction

Il est essentiel de promouvoir l'innovation et la concurrence afin de stimuler le lancement de nouveaux produits et services de paiement mobile au Canada. Il est également important de maintenir l'intégrité de l'infrastructure des paiements du Canada. Le présent livre blanc a été rédigé par six des plus grandes institutions financières du Canada, soit la Banque de Montréal, la Banque CIBC, la Banque Nationale du Canada, la Banque Royale du Canada, la Banque Scotia et le Groupe financier TD. Il promeut l'ouverture du marché et l'innovation. En outre, il propose que les nouveaux produits et services de paiement mobile maintiennent le niveau élevé de sécurité des paiements sur le marché canadien afin de préserver la confiance des consommateurs et des commerçants et d'offrir une protection constante contre les fraudes par carte de paiement.

Une avancée importante pour l'écosystème des paiements est l'arrivée récente des portefeuilles mobiles ouverts qui permettent de charger les justificatifs de paiement de plusieurs émetteurs. Le but du livre blanc est de faire en sorte que l'industrie soit en bonne position pour évaluer et adopter des produits et services novateurs. Dans le cadre de l'évaluation des nouvelles technologies et des modèles commerciaux, le Livre blanc sur la sécurité des paiements vise les objectifs suivants :

- Maintenir un niveau de sécurité qui soit équivalent à celui des cartes de paiement chargées dans un portefeuille mobile ouvert ou supérieur à celles-ci.
- Prendre des mesures appropriées pour cerner les risques technologiques et opérationnels et protéger les consommateurs et les commerçants contre ces risques.
- Créer la capacité permettant aux consommateurs de charger un justificatif de paiement dans un portefeuille de leur choix et d'effectuer des opérations dans tous les réseaux (au point de vente et à distance).

L'objectif ultime est de maintenir la position du Canada comme chef de file de la sécurité des paiements.

PORTÉE

Ce livre blanc examine les nouvelles technologies de paiement mobile et les modèles commerciaux, cerne les risques de sécurité et d'interopérabilité ou les problèmes qui pourraient avoir une incidence sur l'écosystème de paiement du Canada, et explore les obstacles au développement de l'écosystème de paiements mobiles du Canada. Le livre blanc offre un aperçu des principaux événements dans le marché canadien qui sont survenus depuis la publication du *Modèle de référence des paiements mobiles NFC*[1] au début de 2012, examine les principaux aspects de la nouvelle technologie

[1] « Near Field Communication » (communication en champ proche).

HCE d'émulation de carte (Host Card Emulation) et met en lumière les possibilités et préoccupations. De plus, le livre blanc passe en revue les solutions de portefeuille mobile ouvert offertes au Canada, de même que celles proposées par les grandes sociétés mondiales, et examine les incidences que ces solutions auraient sur le marché canadien si elles devaient être mises en marché tel qu'elles sont conçues présentement.

Le présent document examine les opérations initiées au point de vente physique où l'appareil mobile communique avec le terminal du commerçant par un protocole de communication sans contact (p. ex., NFC, code QR), les paiements à distance effectués dans une application mobile ayant été téléchargée dans l'appareil mobile (in-app) et les paiements par Internet initiés par un appareil mobile, lesquels misent sur un justificatif de paiement stocké dans l'appareil. Les paiements à distance qui misent sur les renseignements de la « carte en dossier » dans le cadre des opérations, les applications bancaires mobiles, les applications de paiements mobiles qui sont strictement exclusives et les paiements entre homologues qui pourraient être initiés à partir de l'appareil mobile sortent de la portée du présent document. Le présent document ne définit pas les solutions techniques ni ne propose des modifications aux normes techniques existantes de l'industrie, aux exigences de protection des données ou aux exigences en matière de lutte contre le blanchiment d'argent.

PRINCIPES DIRECTEURS

- **Securité.** Préserver le niveau de sécurité auquel s'attendent les consommateurs de la part des fournisseurs de services de paiement au Canada, soit un niveau équivalent à la sécurité procurée par une puce EMV accompagnée de l'utilisation d'un NIP. Identifier les risques technologiques et opérationnels auxquels sont exposés les consommateurs et les commerçants, et les protéger contre ces risques.
- **Ouverture.** Créer et soutenir un environnement de paiements mobiles ouvert permettant aux consommateurs de payer pour leurs biens et services à l'aide de n'importe quel portefeuille mobile, sur n'importe quel dispositif, en utilisant les terminaux de paiement sans contact déjà installés chez plusieurs détaillants.
- **Innovation.** Soutenir l'innovation dans les paiements mobiles en créant un environnement qui favorise le choix du consommateur et qui soit propice au développement, à l'évaluation et au lancement de nouveaux produits et services.

PUBLIC VISÉ

Ce livre blanc pourrait intéresser les intervenants dans le marché canadien des paiements mobiles, notamment les consommateurs, les émetteurs de justificatifs de paiement, les fournisseurs de réseau de paiement, les commerçants, les acquéreurs, les exploitants de réseau mobile (ERM), les fabricants d'appareils mobiles, les fournisseurs de portefeuilles et les autres parties intéressées.

Aperçu du marché canadien

Au cours de la dernière décennie, le rythme de l'innovation en matière de paiements s'est accéléré. Le développement et la mise en œuvre de cartes à puce EMV et de NIP, de cartes EMV sans contact, de paiements entre homologues, de paiements mobiles par carte SIM et, plus récemment, de paiements mobiles fondés sur la technologie HCE d'émulation de carte ont transformé le marché canadien. L'arrivée de nouveaux produits de paiement offre des débouchés mais comporte aussi des enjeux quant à la sécurité de l'écosystème. L'innovation devrait maintenir ou renforcer la sécurité et l'intégrité globale de l'écosystème des paiements.

MIGRATION VERS LA TECHNOLOGIE EMV

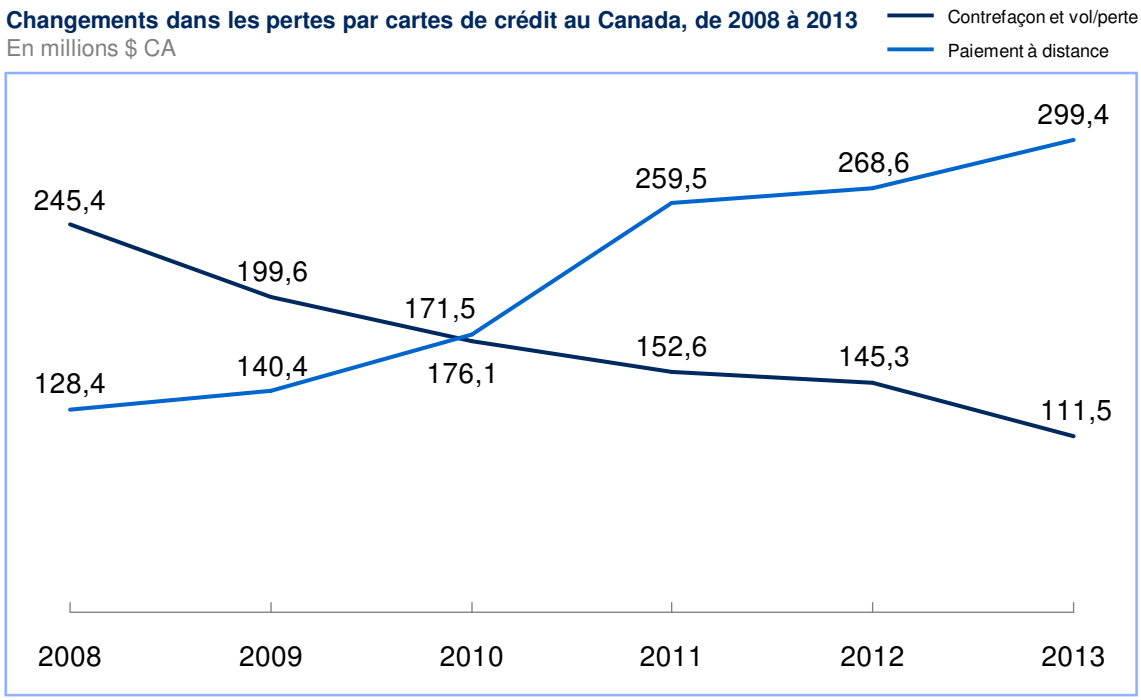
Le lancement national de la technologie reposant sur une puce EMV et l'utilisation d'un NIP a véritablement commencé en 2008, et s'est, en grande partie, terminé en 2013. L'abandon de la technologie de la bande magnétique a nécessité des investissements considérables dans l'infrastructure (p. ex., appareils des points de vente, guichets automatiques, systèmes exclusifs des détaillants et des émetteurs) et la réémission massive de cartes de paiement. Les consommateurs ont appris à changer leurs habitudes de paiement, en insérant leurs cartes de paiement plutôt que de les glisser, et en abandonnant la signature à la faveur d'un NIP à quatre chiffres sur leurs cartes de crédit.

La migration vers la technologie EMV a été considérée comme une initiative de l'industrie; un investissement nécessaire afin de maintenir l'intégrité de l'écosystème des paiements au Canada. Les intervenants dans le marché des paiements au sein de l'industrie, avec, à leur tête, les exploitants de réseaux de paiement, ont collaboré étroitement afin de gérer les incidences sur le client et le commerçant en diagnostiquant et en réglant rapidement les problèmes touchant l'interopérabilité (toutes les cartes sur tous les appareils) et l'expérience client. Les communications initiales avec les consommateurs et les commerçants ont été gérées à l'échelle de l'industrie afin d'assurer un niveau constant de formation du personnel et l'utilisation d'un langage commun dans toutes les communications avec les commerçants et les consommateurs. Le Canada a été reconnu à l'échelle internationale pour sa mise en œuvre efficace de la technologie EMV.

La technologie EMV a eu l'effet escompté sur la fraude par contrefaçon, qui a continué de diminuer. Le Canada a également observé la hausse attendue des fraudes de paiement à distance, stimulée par la croissance considérable des opérations à distance et par un intérêt accru des fraudeurs pour ce type d'opérations. Bien que des mesures aient été mises en place par les détaillants (outils exclusifs de surveillance des fraudes) et les réseaux de paiement (Vérifié par Visa, SecureCode par MasterCard), les opérations sans présentation de carte demeurent un sujet de préoccupation.

FIGURE 1 – PERTES CAUSÉES PAR LES FRAUDES AU CANADA, DE 2008 À 2013

Pertes causées par les fraudes par carte de crédit avec paiement à distance ou au point de vente au Canada



Source : Association des banquiers canadiens

INTRODUCTION DES PAIEMENTS SANS CONTACT

Les paiements sans contact ont commencé à gagner du terrain et à talonner la technologie EMV. Les paiements sans contact sont rapides et pratiques : le consommateur n'a qu'à effleurer la carte à un point de service doté de la technologie de communication en champ proche (NFC) – il n'est pas nécessaire d'insérer la carte ou d'entrer un NIP. Ce mode de paiement est particulièrement intéressant pour les commerçants où le débit est important, comme les restaurants à service rapide et les épiceries. Les paiements sans contact présentent un risque pour les émetteurs, puisqu'il n'existe aucun mode de vérification de l'identité du client et les émetteurs sont responsables des fraudes. Lorsque le paiement sans contact a fait son apparition, les réseaux de paiement (MasterCard, Visa) ont décidé que les consommateurs pourraient simplement approcher leur carte du lecteur pour les opérations de moins de 50 $. Cette limite est passée à 100 $ en 2013 dans tous les réseaux de paiement (y compris Interac) selon une analyse détaillée aux termes de laquelle les risques opérationnels associés à une valeur d'opération maximale supérieure ont été évalués.

Le dynamisme du déploiement des terminaux et des cartes dotés de la technologie NFC a hissé le Canada aux premiers rangs des pays en ce qui a trait à l'entrée de la technologie NFC[2]. À la fin de 2014, plus de 70 pour cent des cartes de crédit et 40 pour cent des cartes de débit au Canada étaient compatibles avec la technologie du paiement sans contact. Plus de 80 pour cent des appareils des points de vente des commerçants dans des catégories ciblées (p. ex., restaurants à service rapide, pharmacies et épiceries) sont dotés de la technologie NFC, et quelque 30 pour cent de tous les appareils des points de vente sont compatibles avec la technologie NFC. Lors de la rédaction du présent document, les opérations sans contact représentaient de 10 à 20 pour cent du nombre total d'opérations.[3]

ÉVOLUTION DE LA SCÈNE CANADIENNE DES PAIEMENTS MOBILES

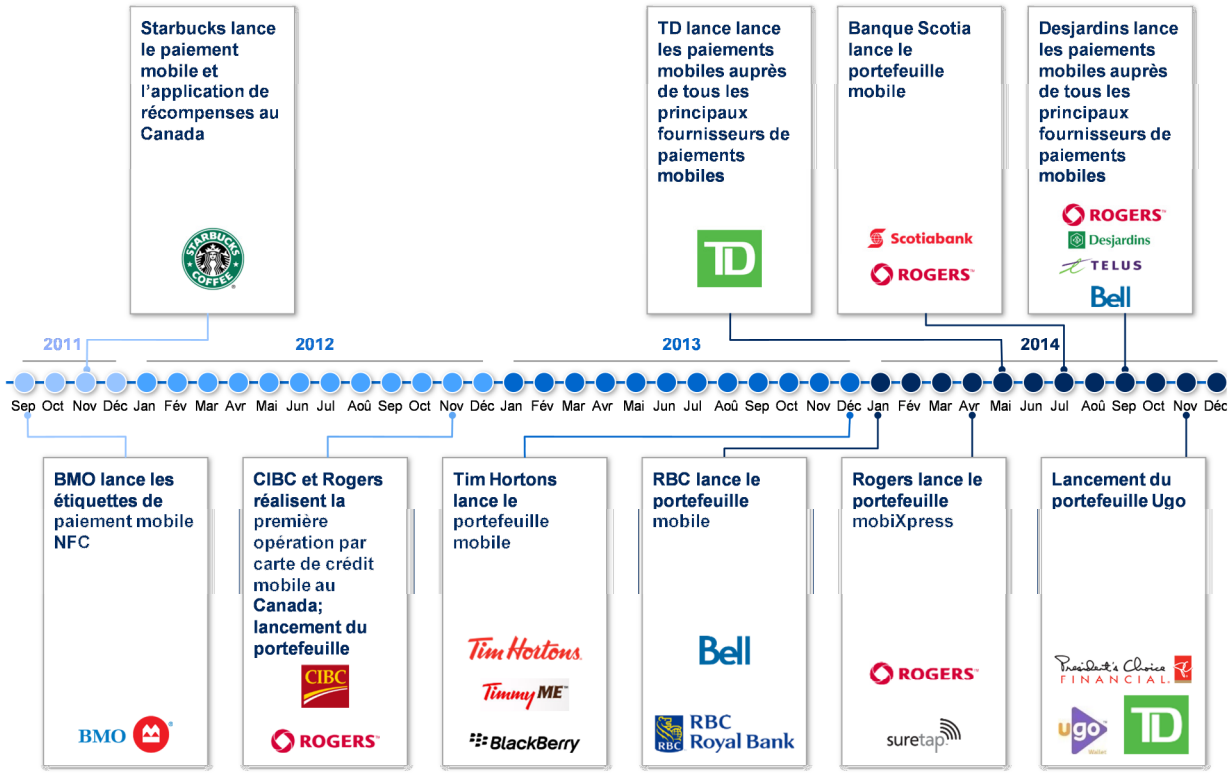
En 2012, les banques et les caisses populaires du Canada ont uni leurs forces afin d'élaborer le *Modèle de référence des paiements mobiles NFC*, qui met l'accent sur la création d'un écosystème ouvert qui soutiendrait l'innovation permanente dans le domaine des paiements mobiles. Le modèle de référence était articulé sur les solutions de paiements mobiles misant sur l'architecture EMV et la sécurité, de même que sur les processus et les politiques. Le document examine également les fonctions de portefeuille supplémentaires, notamment les reçus électroniques, les éléments de fidélisation et les coupons/bons. Le modèle de référence propose 134 normes facultatives visant à accélérer et à soutenir le lancement et l'adoption des paiements mobiles sécurisés au Canada. Nous sommes d'avis que ces normes ont été utiles dans le cadre de l'orientation du développement des paiements mobiles au Canada.

---

2 *MasterCard Mobile Payment Readiness Index*, mai 2012; Entrevues au sein de l'industrie

3 Entrevues au sein de l'industrie

PIÈCE 2 – ÉVOLUTION DE LA SCÈNE CANADIENNE DES PAIEMENTS MOBILES



Source : *Sites Web des sociétés*

Depuis la publication du *Modèle de référence des paiements mobiles NFC* en mai 2012, plusieurs émetteurs canadiens de justificatifs de paiement ont élaboré et lancé des solutions de paiements mobiles par carte SIM. Le premier portefeuille mobile ouvert soutenant les paiements a été lancé au Canada en novembre 2014[4]. Idéalement, les consommateurs devraient être en mesure de télécharger l'un ou l'autre de leurs justificatifs de paiement (crédit, débit) à partir de tout réseau (American Express, Interac, MasterCard, Visa), dans tout appareil mobile (Android, Apple, Blackberry, Windows, etc.) sur tout réseau mobile (Bell, Rogers, TELUS, etc.). Or, c'est impossible pour le moment. Bien que plusieurs produits aient été lancés sur le marché, le taux d'adoption des consommateurs demeure faible en raison des problèmes de déploiement associés aux solutions par carte SIM, notamment :

[4] Communiqué de presse Ugo, cnw.ca

- **Appareils compatibles avec la technologie NFC.** Pour accepter les paiements effectués à l'aide de la technologie NFC, l'appareil mobile doit être compatible avec la technologie NFC. Lorsque la CIBC a lancé son application de paiements mobiles, un seul téléphone mobile (BlackBerry Bold 9900) était alors compatible avec la technologie NFC. Tous les appareils mobiles doivent être certifiés par l'ERM avant le téléchargement d'un justificatif de paiement, un processus qui exige beaucoup de temps. Le nombre d'appareils compatibles avec la technologie NFC a monté en flèche au cours des trois dernières années, et la technologie NFC est presque devenue une caractéristique standard sur les nouveaux appareils. Lors de la rédaction du présent document, les appareils compatibles avec la technologie NFC n'étaient pas tous certifiés aux fins de paiement par tous les ERM. Ainsi, un consommateur pourrait avoir un appareil doté de la technologie NFC qui n'acceptera pas les paiements mobiles.
- **ERM appuyant les paiements mobiles**. Afin d'appuyer les paiements mobiles, les applications de paiement appartenant aux émetteurs doivent être téléchargées sur des cartes SIM appartenant aux ERM. Pour ce faire, chaque émetteur de justificatifs et chaque ERM doit négocier une entente commerciale. Pour cette raison, les émetteurs ne peuvent soutenir le déploiement que lorsqu'une telle entente est conclue. Lors de la rédaction du présent document, certaines solutions exclusives d'émetteurs n'étaient offertes qu'aux clients d'un seul ERM.
- **Cartes SIM prêtes aux paiements.** Jusqu'à tout dernièrement, les cartes SIM livrées avec un appareil mobile n'acceptaient pas les applications de paiement, et les consommateurs devaient acheter une carte SIM de remplacement prête aux paiements. D'emblée, les émetteurs ont été confrontés à des taux d'échec d'inscription aux portefeuilles de 80 à 90 pour cent en raison de l'incompatibilité des cartes SIM.[5] Il s'agissait là d'un obstacle considérable. Pour remédier à la situation, les ERM les plus importants au Canada vendent maintenant des téléphones mobiles Android et BlackBerry dotés de la technologie NFC et de cartes SIM prêtes aux paiements.
- **Justificatifs numérisés.** Les premiers justificatifs numérisés offerts aux fins de paiements mobiles étaient des produits de crédit. Les émetteurs ont accru le nombre de produits offerts aux consommateurs, mais la plupart des consommateurs ne peuvent toujours pas payer à l'aide d'un appareil mobile toutes les cartes de leur portefeuille. L'application de débit mobile Interac n'est offerte que depuis 2012 et, lors de la rédaction du présent document, un seul émetteur acceptait le paiement par carte de débit mobile.
- **Approvisionnement des justificatifs.** L'approvisionnement des justificatifs, c.-à-d., l'installation de l'application de paiement mobile sur la carte SIM de l'appareil mobile, s'est révélé problématique dès le départ. Le justificatif numérique est approvisionné en direct dans l'appareil mobile du consommateur. Ce processus peut prendre plusieurs heures et, si la connexion Internet est

[5] Entrevues auprès des émetteurs

perdue, il peut échouer. En 2012, EnStream – une coentreprise fondée par Bell, Rogers et TELUS – a lancé les services de gestionnaire de services de confiance (GSC) et une interface mobile commune aux émetteurs canadiens et aux ERM en vue d'améliorer l'expérience d'approvisionnement. Bien que l'approvisionnement ait été amélioré, il demeure problématique.

On estime que, malgré le nombre de relations établies entre les émetteurs et les ERM, moins de 25 pour cent des consommateurs ont tous les éléments requis pour effectuer des paiements mobiles.[6] Puisque la capacité de paiements mobiles n'est offerte qu'à un nombre restreint de consommateurs, il est difficile pour les émetteurs de communiquer et de promouvoir les paiements mobiles à grande échelle et la sensibilisation au paiement mobile demeure faible.

CODE DE CONDUITE

Le Code de conduite destiné à l'industrie canadienne des cartes de crédit et de débit (le « Code ») est entré en vigueur en août 2010. Il a été élaboré afin de résoudre les problèmes soulevés par les commerçants relativement aux pratiques commerciales des réseaux, des émetteurs et des acquéreurs de cartes de crédit et de débit, et il s'applique aux cartes de débit et de crédit utilisées afin d'effectuer des opérations auprès des commerçants au Canada. Le Code avait pour objectifs de s'assurer que les commerçants au Canada bénéficient d'une transparence quant aux coûts, d'une souplesse des prix et d'un choix quant aux options de paiement acceptées. La conformité au Code est assurée par l'Agence de la consommation en matière financière du Canada (ACFC).

Le Code a été révisé en avril 2015 pour inclure les paiements mobiles. Les révisions prévoient de nouvelles protections pour les utilisateurs de paiements mobiles afin de s'assurer que le consommateur a le contrôle total des paramètres par défaut des portefeuilles mobiles et des appareils mobiles. Le Code assure également aux commerçants la possibilité de choisir de ne pas accepter les paiements mobiles si les frais de paiements mobiles augmentent par rapport à ceux des paiements sans contact avec carte.[7] Le Code révisé offre également de nouvelles protections aux commerçants. Aux termes du Code, les cartes de débit dites « mixtes »[8] doivent être représentées comme deux applications de paiement distinctes dans les portefeuilles mobiles ou sur les appareils mobiles. Il s'agit là d'un changement pour les consommateurs, puisque de nombreuses cartes de débit en circulation acceptent deux réseaux de paiement.

---

[6] Analyse exclusive

[7] « Code de conduite destiné à l'industrie canadienne des cartes de crédit et de débit », Agence de la consommation en matière financière du Canada, 24 avril 2015

[8] Les cartes mixtes sont des cartes de débit qui acceptent au moins deux réseaux de cartes de paiement.

Le gouvernement a procédé à de vastes consultations auprès de l'industrie avant de présenter le Code en 2010, et il continue de rencontrer périodiquement les principales parties prenantes. L'élaboration du Code et les révisions continues qui y sont apportées démontrent l'engagement du gouvernement et l'intérêt dans l'ensemble de l'industrie des paiements, de même qu'un désir d'assurer des pratiques commerciales justes et transparentes qui protègent aussi bien les commerçants que les consommateurs.
Le Code devrait continuer d'évoluer.

Technologies de paiement mobile

Le paiement mobile est un terme général qui comprend les paiements effectués à l'aide de codes à barres, de codes QR, par Internet et au moyen de la technologie NFC. Fondamentalement, le succès des paiements mobiles est stimulé par la perception du consommateur sur le plan de l'utilité, de la sécurité et de la valeur supérieure à celles offertes par la carte de paiement. La croissance des appareils « intelligents » permet aux intervenants dans le marché des paiements classiques et non classiques de se concentrer sur l'élaboration de solutions mobiles pour stimuler l'engagement et offrir une valeur accrue aux commerçants et aux consommateurs.

Des solutions de codes à barres et de codes QR ont été déployées au Canada, habituellement dans le cadre de solutions exclusives de paiements mobiles à circuit fermé (p. ex., Starbucks, Tim Hortons). Ces solutions nécessitent des logiciels et souvent des mises à niveau du matériel dans le cadre du déploiement. La réticence des commerçants à investir dans du matériel supplémentaire susceptible d'occuper une précieuse place sur le comptoir pourrait être un défi dans le cadre du déploiement général de ces solutions.

La capacité d'accepter la technologie NFC est devenue une caractéristique standard sur les appareils des points de vente, et la plupart des détaillants au Canada peuvent maintenant accepter les paiements NFC s'ils le désirent. La technologie NFC a la cote : lors de la rédaction du présent document, quelque 30 pour cent[9] des appareils des points de vente au Canada pouvaient accepter les paiements NFC, avec un taux d'acceptation considérablement plus élevé dans les marchés verticaux ciblés, comme les restaurants à service rapide). Les consommateurs sont de plus en plus conscients de l'existence de la capacité de paiement sans contact pour la majorité des cartes de paiement au Canada. La proposition de valeur d'une expérience au point de vente rapide sans mode de vérification de l'identité du client (p. ex., un NIP) est bien reçue, malgré le nombre limité de campagnes sur le marché visant à promouvoir l'utilisation du paiement sans contact.

TECHNOLOGIES DE PAIEMENT MOBILE OFFERTES

Les premières solutions de paiement mobile NFC ont mis à profit l'élément matériel sécurisé situé physiquement dans l'appareil mobile. Les solutions de matériel offrent un niveau de sécurité élevé en raison du stockage sécurisé inviolable des justificatifs de paiement. Les deux principaux éléments de matériel sécurisés sont l'ES intégré (ESI), qui est intégré dans l'appareil par le fabricant, et l'ES fondé sur un module d'identité d'abonné (SIM) appartenant à l'ERM qui le fournit également.

---

[9] Entrevues au sein de l'industrie

Un élément de matériel sécurisé est en quelque sorte une « carte à puce dans le téléphone ». Des processus d'essai et de certification sont en place pour assurer que les solutions répondent aux exigences définies par les réseaux de paiement et d'autres instances sectorielles. L'ES est protégé par une interface dont l'accès est restreint et par un cryptage très robuste destiné à le rendre inviolable. L'élément du matériel sécurisé est directement connecté au contrôleur NFC dans l'appareil mobile; le système d'exploitation de l'appareil mobile n'a pas accès aux données échangées entre la carte SIM et le contrôleur NFC. L'ES présent dans un appareil mobile contient l'information relative aux justificatifs de paiement et les autres renseignements nécessaires pour créer des cryptogrammes de paiement pour *cet appareil seulement*, ce qui limite son attrait pour les fraudeurs. Des solutions fondées sur la carte SIM sont offertes sur le marché depuis plusieurs années et sont soutenues efficacement par les spécifications de la marque et des processus d'essai et de certification.

Les solutions mobiles plus récentes mettent à profit la technologie HCE d'émulation de carte, capacité qui a été lancée par Android en 2013. Dans une solution HCE, l'élément sécurisé n'est pas situé dans l'appareil : les justificatifs de paiement sont stockés dans l'infonuage. *La technologie HCE d'émulation de carte représente une réorientation fondamentale pour la sécurité.* L'hypothèse est que l'appareil mobile n'est pas sécurisé : pour atténuer les risques liés à la sécurité des paiements, il faut stratifier de multiples mécanismes de sécurité de rechange, y compris les justificatifs de paiement dont l'utilisation est limitée, qui sont générés dynamiquement. HCE est une technologie en évolution qui a été déployée à une étape précoce dans plusieurs pays. Les documents à l'appui, y compris les processus d'essai et de certification, continueront d'évoluer au cours des prochaines années.

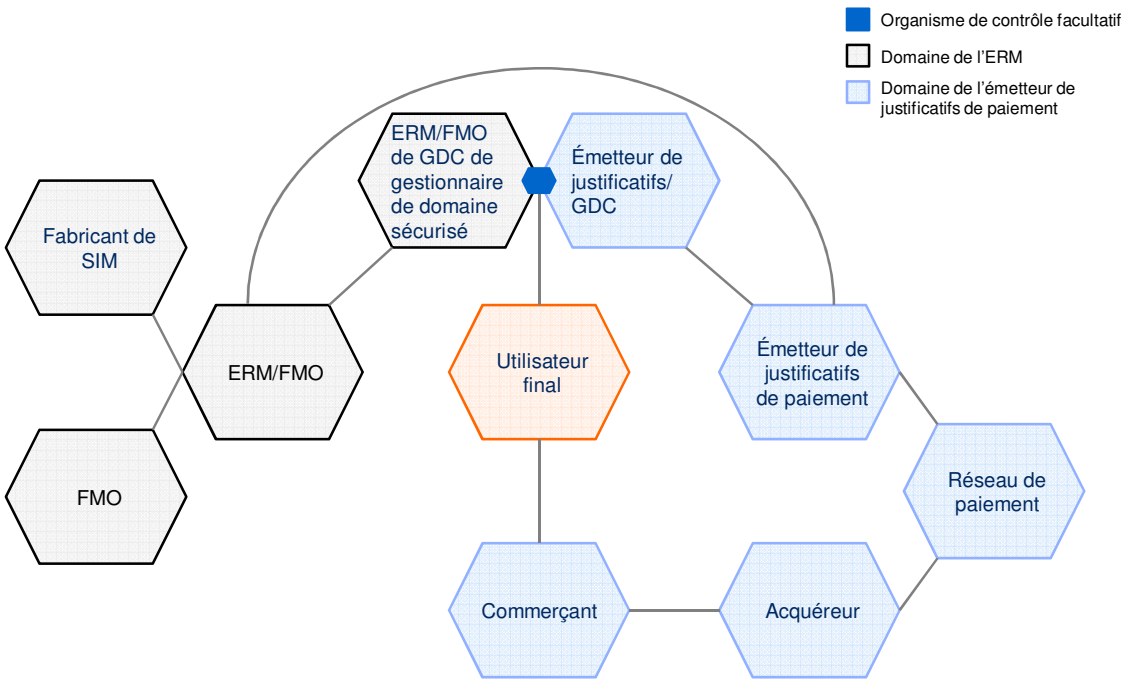
Un aperçu conceptuel de la sécurité et de la maturité des technologies de paiement est présenté à l'Annexe A.

SOLUTIONS FONDÉES SUR LA CARTE SIM

Les paiements par cartes classiques comportent quatre parties : l'émetteur de carte, le client, le commerçant et l'acquéreur. Les réseaux de paiement relient l'acquéreur et l'émetteur pour permettre l'autorisation de l'opération. Les solutions de paiement mobile qui mettent à profit l'ES ou l'ESI nécessitent l'entrée en scène de nouveaux intervenants dans l'écosystème pour créer et gérer des cartes numérisées et déployer la carte numérisée dans l'appareil mobile du consommateur. Les nouveaux rôles et responsabilités qui ont été mis en place pour soutenir les paiements mobiles NFC sont indiqués à l'Annexe B.

Le positionnement de ces nouveaux participants dans l'écosystème pour soutenir les paiements mobiles fondés sur la carte SIM est illustré ci-après.

FIGURE 3 – ÉCOSYSTÈME DES PAIEMENTS MOBILES FONDÉS SUR LA CARTE SIM



Source : *Modèle de référence des paiements mobiles NFC au Canada*

Le tableau 1 fait ressortir quelques-uns des risques possibles associés aux solutions de paiement mobile fondées sur la carte SIM.

TABLEAU 1 – RISQUES POSSIBLES ASSOCIÉS AUX SOLUTIONS FONDÉES SUR LA CARTE SIM

Risque	**Description**	**Impact sur le consommateur/commerçant**
Technologie ***Évaluation : faible risque***	■ L'information relative aux paiements est stockée dans un élément de matériel sécurisé qui est inviolable ■ Les spécifications sont rédigées clairement, en fonction de celles d'EMV	■ Expérience positive des utilisateurs (il n'est pas nécessaire que l'appareil soit mis en marche/il n'est pas nécessaire que l'appareil soit connecté/les opérations hors ligne sont acceptées)

Risque	Description	Impact sur le consommateur/commerçant
	■ Les critères de certification sont clairs et cohérents ■ Quelques problèmes d'interopérabilité – collisions entre les justificatifs stockés dans différents portefeuilles	■ Il n'est pas nécessaire de mettre à niveau les TPV qui ne sont pas équipés de la technologie NFC ■ Les problèmes d'interopérabilité entre les applications du même appareil peuvent limiter leur adoption par les consommateurs
Exploitation ***Évaluation : risque moyen***	■ Écosystèmes complexes nécessitant de multiples participants, des partenariats et une gouvernance connexe ■ L'approvisionnement est long et parfois peu fiable. ■ La gestion du cycle de vie peut être difficile si le nouvel appareil ou produit de paiement n'est pas accepté	■ Le paiement mobile n'est pas constamment disponible (il faut avoir la bonne carte de paiement, le bon téléphone et le bon réseau). Des frictions peuvent inciter les consommateurs à décrocher du processus d'enregistrement et d'approvisionnement ■ Les consommateurs peuvent ne pas être en mesure de transférer la capacité de paiement à un autre produit ou appareil mobile de paiement
Réputation ***Évaluation : Risque faible à moyen***	■ Les appareils et les produits de paiement ne sont pas tous acceptés	■ Leur adoption par les consommateurs sera limitée à moins que l'ubiquité ne soit réalisée

Les solutions de paiement mobile dotées d'éléments de matériel sécurisés reposent sur des spécifications EMV solides et éprouvées, et le niveau de sécurité offert au PDV est équivalent à celui de la carte de paiement. Le risque de fraude associé au fait de ne pas exiger un mode de vérification des titulaires a été atténué par la mise en place d'un montant limite pour les opérations sans contact. Si ce montant est dépassé, le consommateur doit insérer la carte de paiement dans le terminal au point de vente. Les difficultés de déploiement concernent l'expérience utilisateur et les interactions

imprévues de multiples applications de portefeuille chargées dans le même appareil. Des essais détaillés devront être effectués pour assurer qu'il n'y a pas d'interaction entre de multiples applications de paiement, ce qui pourrait se traduire par une expérience client négative.

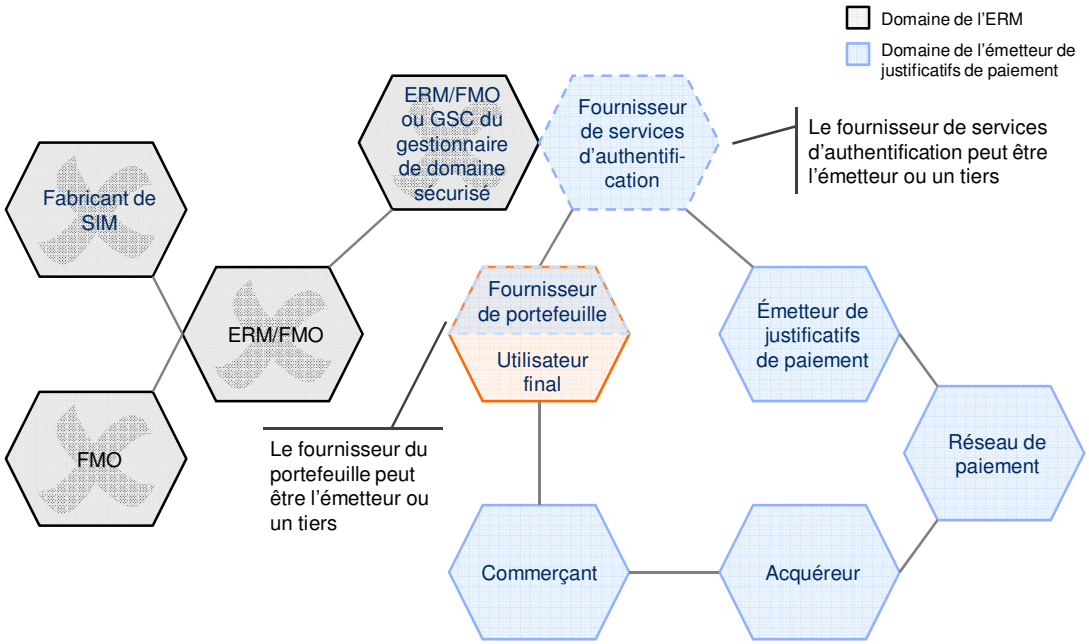
Au moment de la publication, il y avait sur le marché cinq émetteurs canadiens dotés de solutions fondées sur des ES (la CIBC, Desjardins, RBC, la Banque Scotia et la TD). De plus en plus d'appareils sont acceptés par les émetteurs, car les nouveaux appareils qui font appel à la technologie NFC sont en train de devenir la norme.

SOLUTIONS HCE D'ÉMULATION DE CARTE

L'émulation de carte (HCE) désigne une technologie intégrée dans l'appareil, grâce à laquelle les appareils mobiles qui utilisent la technologie NFC peuvent émuler une carte de paiement sans être tributaires de l'accès à un élément sécurisé. Les solutions HCE font uniquement appel à des logiciels.

HCE simplifie considérablement l'écosystème des applications de paiement mobile. Les consommateurs peuvent télécharger l'application de paiement ou de portefeuille à partir d'Internet (du site Web de leur banque, d'un magasin d'applications, etc.). Les solutions HCE dispensent les émetteurs de justificatifs de paiement d'obtenir de l'espace sur un élément sécurisé tiers, ce qui élimine le recours à l'ERM et au FMO dans l'écosystème. Cela élimine aussi le recours au GSC de l'ERM et du GSC de l'émetteur. Tout comme les solutions fondées sur la carte SIM, les solutions HCE nécessitent un système d'exploitation ouvert qui accorde l'accès de l'antenne NFC aux applications tierces.

FIGURE 4 – ÉCOSYSTÈME DES PAIEMENTS MOBILES HCE



Éléments rendus nécessaires par une solution HCE

De nombreux aspects des solutions HCE s'apparentent à ceux des solutions fondées sur la carte SIM, moyennant quelques améliorations pour accepter la communication entre l'appareil et le nuage.

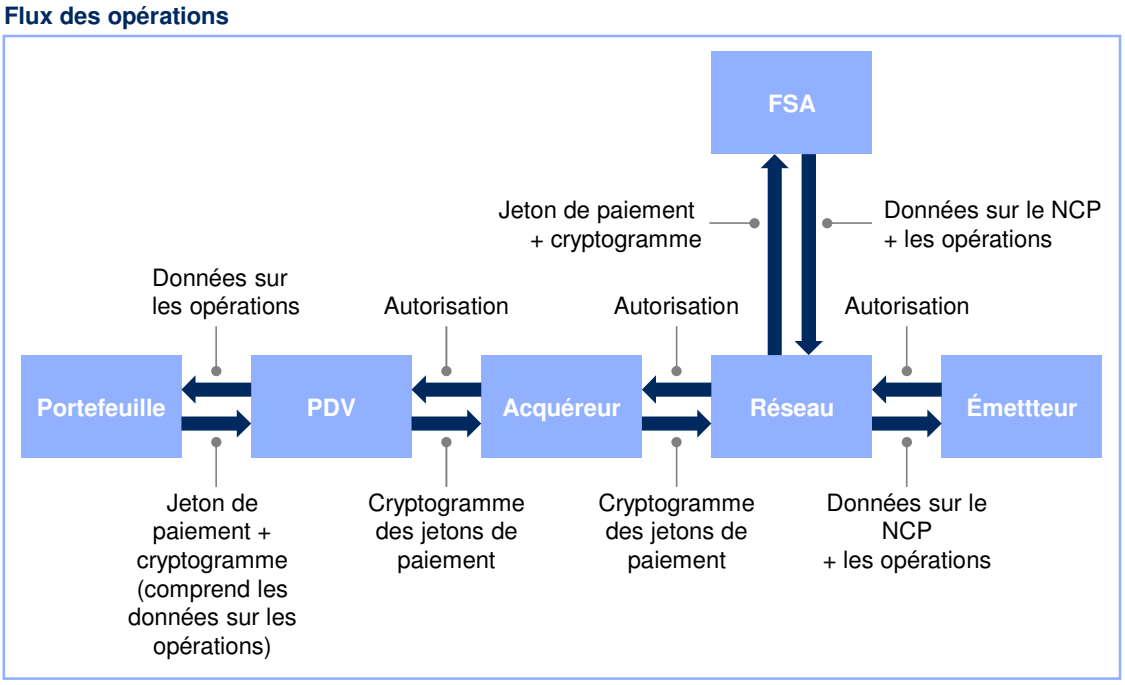
- **Plateforme de paiements dans l'infonuage.** Les solutions HCE nécessitent le recours à un logiciel pour gérer le compte de paiements dans le nuage. Les fonctions comprennent la gestion de numéros de comptes primaires (NCP) et de clés dont l'utilisation est limitée, la validation des demandes de reconstitution dynamique des données, l'apport en données dynamiques dans l'appareil, la vérification du mode de vérification des titulaires et la gestion du cycle de vie et des fonctions de paiement du compte d'applications mobiles des consommateurs. La construction et la gestion des plateformes de paiement dans le nuage peuvent être assurées par les émetteurs de justificatifs ou être imparties à des tiers.
- **Application mobile (portefeuille).** L'application mobile comprend une interface client qui soutient l'inscription au service de paiement dans le nuage et intervient

dans l'approvisionnement des justificatifs au moment de l'activation et en permanence. L'application mobile doit communiquer en toute sécurité avec la plateforme de paiement. La mise au point et la gestion des applications mobiles peuvent être assurées par les émetteurs (portefeuilles mobiles exclusifs) ou être imparties à des tiers (portefeuilles mobiles ouverts).

– **Fournisseur de services d'authentification (FSA).** La nécessité d'obtenir des données dynamiques crée un nouveau rôle dans l'écosystème HCE pour les fournisseurs de services d'authentification. La segmentation en unités consiste à remplacer le numéro de compte primaire (NCP)[10] réel par un NCP de rechange, soit un jeton. Les caractéristiques du jeton sont décrites pour que les NCP à jeton soient transmis dans le système de paiement exactement comme les NCP réels. Ces jetons ont la capacité d'avoir un impact sur chaque participant de l'écosystème, car ils passent par l'opération de bout en bout, de sorte qu'il est important que leur fonctionnement soit conforme à ce qui est prévu. La figure 5 montre où la spécification de segmentation en unités propose que les fournisseurs de services d'authentification se situent dans l'écosystème.

[10] Le NCP est le numéro composé de 16 à 19 chiffres qui figure au recto de la carte de crédit.

FIGURE 5 – APERÇU DE L'APPORT DES JETONS DE PAIEMENT



Note : Le rôle du FSA pourrait être rempli par l'émetteur, le réseau ou un tiers.

Source : *EMV Payment Tokenization Specification*

RISQUES LIÉS À LA TECHNOLOGIE HCE

Comme les solutions HCE ne nécessitent pas le stockage sécurisé des justificatifs de paiement dans l'appareil, la sécurité des paiements est assurée par la stratification de multiples solutions en matière de sécurité pour apporter la sécurité que procure une solution de matériel. Et comme l'appareil mobile est jugé moins sécuritaire qu'un élément de matériel sécurisé, tous les aspects de la solution HCE font l'objet d'un contrôle continu. La sécurité stratifiée est conçue pour qu'il soit difficile pour les fraudeurs de voler des jetons à l'appareil et d'utiliser les jetons une fois qu'ils ont été volés. La sécurité de l'application, la sécurité de l'appareil et la sécurité des communications sont essentielles pour protéger le stockage des jetons dans l'appareil et empêcher leur vol. Si un jeton est volé, les données dynamiques sont essentielles pour empêcher l'utilisation des jetons ou limiter leur utilisation possible. Les données dynamiques offrent aux émetteurs et aux FSA une source abondante d'information sur

laquelle fonder les décisions relatives aux autorisations et limitent le risque associé à la relecture des jetons.[11]

FIGURE 6 – ÉLÉMENTS DE LA SÉCURITÉ DE LA SOLUTION HCE

Couche de sécurité HCE	Description	Instance responsable
Sécurité de la communication	Les communications entre l'application de paiement mobile et le FSA doivent être confidentielles et sécurisées.	Fournisseur de portefeuille, FSA
Sécurité de l'appareil	Assure que l'appareil n'a pas été corrompu. Les mécanismes de détection portent sur le *rootage*, le débogage et l'émulation.	FMO, FSA
Sécurité de l'application	Assure que l'application mobile n'avait pas été corrompue. Comprend l'obscurcissement, la cryptographie en boîte blanche et l'utilisation de l'environnement d'exécution fiable.	Fournisseur de portefeuille, FSA
NCP segmenté en jetons	Assure que le NCP n'est pas stocké dans l'appareil. Le NCP segmenté en jetons peut être propre au domaine de sorte qu'il ne peut être utilisé que pour les opérations sans contact ou à distance.	FSA
Données dynamiques (clés de session)	Les clés peuvent avoir un usage unique ou limité pour réduire l'impact d'une fuite de données. Les données dynamiques (propres à l'opération et à l'appareil) limitent la mystification et la relecture.	FSA (ou gestionnaire des justificatifs de paiement)

Sources : *Consult Hyperion, HCE and Tokenisation for Payment Services; Sequent, Beyond Tokenization White Paper*

[11] La relecture des jetons désigne une tentative par un fraudeur d'utiliser plusieurs fois un jeton à usage unique. Si le jeton intègre des données dynamiques solides (p. ex., s'il intègre l'information propre à une opération ou s'il est utilisé une seule fois), le fraudeur ne pourra pas utiliser ou relire le jeton. Le FSA ou l'émetteur sera en mesure de relever les discordances dans les données dynamiques et de refuser l'opération.

Les données dynamiques

Comme les justificatifs de paiement ne peuvent être stockés en toute sécurité dans l'appareil, la technologie HCE nécessite l'utilisation de données de paiement qui changent constamment. Le paiement est activé par le chargement dans l'appareil de justificatifs de paiement propres au domaine et dont l'utilisation est limitée, et leur stockage dans l'appareil jusqu'à ce qu'ils soient nécessaires pour une opération. Ces justificatifs dynamiques peuvent être limités par le nombre d'utilisations, un laps de temps, ou les deux, avant d'expirer. La courte durée de vie et la nature dynamique de ces justificatifs limitent les risques de vol et d'interception. Si des justificatifs de paiement sont volés, les FSA et les émetteurs devraient pouvoir déceler les discordances dans les données dynamiques et refuser l'opération. Si les paramètres des données dynamiques sont absents ou ne sont pas robustes, des fraudeurs peuvent les modifier et effectuer de nouvelles opérations avec les jetons volés (les « relire ».) Il se peut que les émetteurs et les FSA soient incapables de distinguer un jeton « relu » d'un jeton légitime.

Les émetteurs ont des options dans la création de données dynamiques. L'une consiste à utiliser un NCP dynamique qui modifie chaque opération. Si la segmentation dynamique est l'approche retenue, le jeton dynamique est fourni par le FSA avant l'opération et est stocké dans l'appareil mobile. Lorsque le consommateur effectue une opération au moyen du jeton, l'opération doit passer par le FSA, où le NCP est désegmenté et l'information relative à l'opération, dont le NCP initial, est transmise à l'émetteur pour soutenir l'autorisation. Une autre option consiste à utiliser des clés de session, qui sont des clés cryptographiques valides pour une seule opération. Le processus d'autorisation des opérations évaluera les données dynamiques pour déceler les éventuelles erreurs et refusera les opérations en cas de non-correspondance.

Les émetteurs qui mettent en place des solutions HCE devront peut-être déterminer comment gérer l'apport en données dynamiques de l'application de paiement de l'appareil mobile. On ne peut télécharger les données dynamiques selon les besoins en raison de l'impact négatif que cela pourrait avoir sur l'expérience de l'opération (les justificatifs de paiement doivent être présents avant que le paiement puisse être amorcé, à défaut de quoi des problèmes de latence peuvent survenir, ce qui empêcherait le traitement des opérations hors ligne). Les émetteurs doivent déterminer comment authentifier la demande de justificatifs de paiement dynamiques provenant de l'application de paiement mobile et le nombre d'opérations qui seront acceptées en un seul téléchargement de données dynamiques (plus le nombre d'opérations est faible, plus le risque qu'elles présentent est faible). Des paramètres doivent être définis par les émetteurs pour assurer que le client a toujours un nombre suffisant de données dynamiques (des jetons ou des clés de session) pour être en mesure d'effectuer des opérations sans interruption. Il est important que les données dynamiques puissent être relayées à l'aide de canaux de communication sécurisés.

Les solutions HCE doivent continuellement évaluer les composantes de la solution pour confirmer que le risque lié à l'opération est géré et que la sécurité du paiement est maintenue. Cela comporte la validation initiale (et potentiellement permanente) du client et la validation permanente de l'application de paiement, de l'appareil mobile et des communications entre l'application et l'ES dans le nuage associé à la demande et à l'apport en données dynamiques.

Sécurité de l'application

La sécurité de l'application assure que l'application de paiement stockée dans l'appareil n'a pas été corrompue de quelque façon que ce soit. De plus, les clés de paiement et les autres données délicates stockées dans l'appareil devraient être protégées. La cryptographie en boîte blanche offre une option à cet égard. Elle empêche l'exposition des clés dans une mémoire ou un code. Une autre option consiste à utiliser un environnement d'exécution fiable, qui assure également le stockage sécuritaire des clés.

Ces mesures empêchent les fraudeurs d'utiliser des logiciels malveillants ou d'autres méthodes pour voler des justificatifs de paiement et des clés cryptographiques provenant de l'appareil. Advenant le vol de ces documents, il se peut que les fraudeurs puissent effectuer des opérations à l'aide des justificatifs stockés dans l'appareil.

Sécurité de l'appareil

Les solutions HCE reposent sur l'hypothèse que l'appareil mobile est un environnement de stockage moins sécuritaire que les éléments de matériel sécurisés, et les mises en œuvre devraient comporter des mécanismes de détection logiciels liés au système d'exploitation de l'appareil mobile, qui peuvent déterminer si l'appareil a été corrompu. Ces mécanismes devraient pouvoir détecter si un appareil a été *rooté*, fonctionne en mode développeur ou débogage ou fonctionne à l'aide d'un émulateur (entre autres). Ces scénarios compromettent la sécurité des solutions HCE en exposant des zones de l'appareil qui sont habituellement protégées. Les fraudeurs peuvent être en mesure de voler et d'utiliser les justificatifs d'une application de paiement mobile qui fonctionne dans un appareil corrompu.

Sécurité des communications

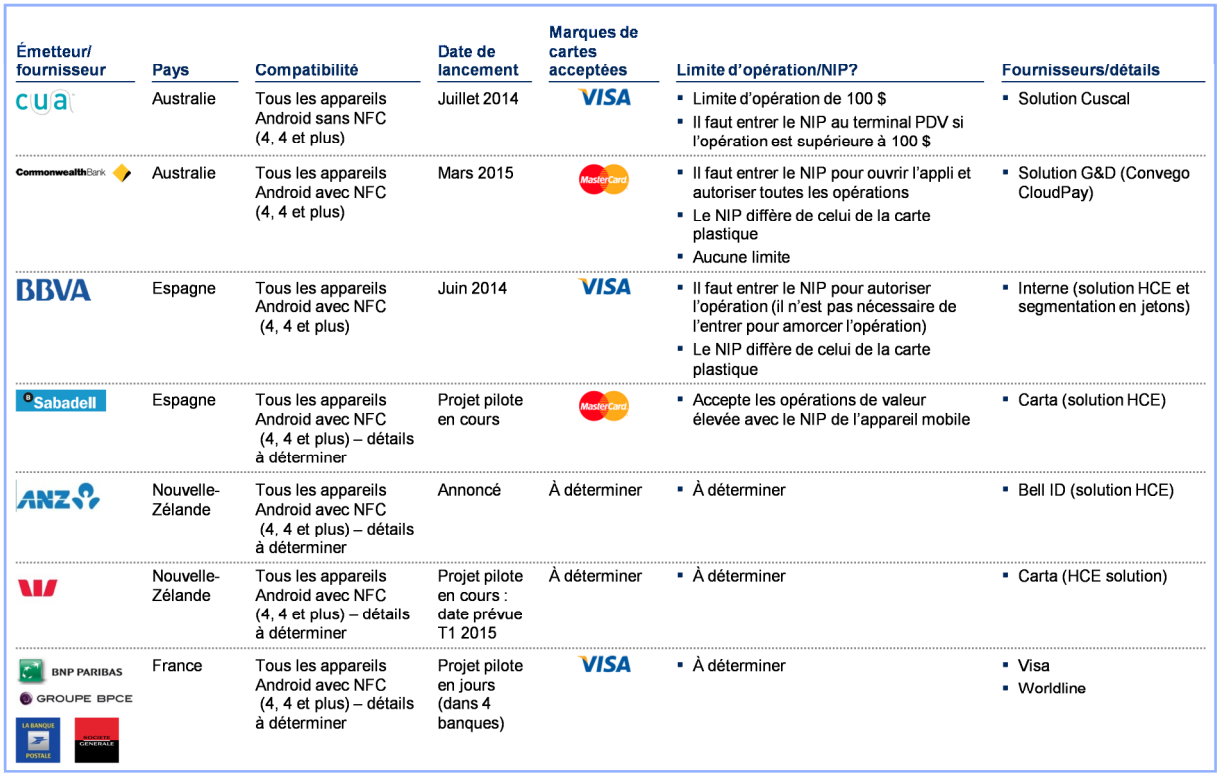
La nécessité continuelle de fournir des données dynamiques pour soutenir la solution HCE sous-tend qu'il y a une communication fréquente entre le nuage et l'appareil pour soutenir l'apport de données dynamiques. Les communications entre l'application de téléphone portable et le nuage de l'émetteur sont confidentielles et doivent être protégées (p. ex., à l'aide d'un cryptage robuste). Si les communications sont interceptées et décryptées, les fraudeurs peuvent voler les données dynamiques

transmises à l'appareil et effectuer des opérations. Les fraudeurs peuvent aussi usurper des demandes provenant de l'appareil et les acheminer vers l'infonuage pour obtenir davantage de données dynamiques et effectuer encore plus d'opérations frauduleuses.

DÉPLOIEMENT DE LA SOLUTION HCE

Depuis que la solution HCE est devenue accessible à la fin de novembre 2013, des portefeuilles exclusifs HCE ont été lancés en Australie, en Espagne, en Nouvelle-Zélande et en France. Des projets pilotes sont menés dans d'autres pays, dont le Canada.

FIGURE 7 – MISE EN ŒUVRE DE SOLUTIONS HCE DANS LE MARCHÉ



Émetteur/ fournisseur	Pays	Compatibilité	Date de lancement	Marques de cartes acceptées	Limite d'opération/NIP?	Fournisseurs/détails
cua	Australie	Tous les appareils Android sans NFC (4, 4 et plus)	Juillet 2014	VISA	▪ Limite d'opération de 100 $ ▪ Il faut entrer le NIP au terminal PDV si l'opération est supérieure à 100 $	▪ Solution Cuscal
CommonwealthBank	Australie	Tous les appareils Android avec NFC (4, 4 et plus)	Mars 2015	MasterCard	▪ Il faut entrer le NIP pour ouvrir l'appli et autoriser toutes les opérations ▪ Le NIP diffère de celui de la carte plastique ▪ Aucune limite	▪ Solution G&D (Convego CloudPay)
BBVA	Espagne	Tous les appareils Android avec NFC (4, 4 et plus)	Juin 2014	VISA	▪ Il faut entrer le NIP pour autoriser l'opération (il n'est pas nécessaire de l'entrer pour amorcer l'opération) ▪ Le NIP diffère de celui de la carte plastique	▪ Interne (solution HCE et segmentation en jetons)
Sabadell	Espagne	Tous les appareils Android avec NFC (4, 4 et plus) – détails à déterminer	Projet pilote en cours	MasterCard	▪ Accepte les opérations de valeur élevée avec le NIP de l'appareil mobile	▪ Carta (solution HCE)
ANZ	Nouvelle-Zélande	Tous les appareils Android avec NFC (4, 4 et plus) – détails à déterminer	Annoncé	À déterminer	▪ À déterminer	▪ Bell ID (solution HCE)
W	Nouvelle-Zélande	Tous les appareils Android avec NFC (4, 4 et plus) – détails à déterminer	Projet pilote en cours : date prévue T1 2015	À déterminer	▪ À déterminer	▪ Carta (HCE solution)
BNP PARIBAS GROUPE BPCE LA BANQUE POSTALE SOCIÉTÉ GÉNÉRALE	France	Tous les appareils Android avec NFC (4, 4 et plus) – détails à déterminer	Projet pilote en jours (dans 4 banques)	VISA	▪ À déterminer	▪ Visa ▪ Worldline

Sources : Sites Web des entreprises

Vu sa nouveauté, la solution HCE suscite des préoccupations quant à l'insuffisance des détails pour soutenir des mises en œuvre sécuritaires et au manque de clarté des rôles et des responsabilités des participants dans l'écosystème HCE. Le déploiement plus vaste des justificatifs de paiement dans des portefeuilles mobiles ouverts peut renforcer considérablement l'impact des discordances entre les spécifications ou les lacunes sur le plan de la sécurité qui sont décelées.

Le tableau 2 indique quelques-uns des risques possibles associés aux solutions de paiement mobile HCE.

TABLEAU 2 – RISQUES POSSIBLES ASSOCIÉS AUX SOLUTIONS DE PAIEMENT MOBILE HCE

Risque	Description	Impact sur le consommateur/le commerçant
Risque technologique ***Évaluation : risque moyen à élevé***	Les jetons de paiement sont stockés dans l'appareil. Si celui-ci n'est pas sécuritaire, il est dangereux que le jeton soit volé et relu Les spécifications en sont à leur début et devront être mises à jour au fur et à mesure que la technologie devient plus compréhensible et plus stable. Cela s'applique en particulier à la sécurité de l'application, à la sécurité de l'appareil et à la segmentation en unités L'approche de la mise en œuvre peut avoir un impact considérable sur la sécurité offerte par une solution HCE Les critères de certification ne sont pas clairs Il y a vraisemblablement des problèmes d'interopérabilité, car les solutions HCE sont déployées à l'échelle mondiale et les consommateurs téléchargent plusieurs portefeuilles HCE dans un seul appareil	L'expérience utilisateur n'est peut-être pas aussi convaincante qu'avec la carte SIM (l'appareil doit être mis en marche, il doit être connecté pour que les jetons soient transmis, les opérations hors ligne ne sont peut-être pas acceptées) bien que le processus d'approvisionnement soit plus rapide Les problèmes d'interopérabilité peuvent avoir un impact sur l'expérience du consommateur et celle du commerçant
Risque d'exploitation ***Évaluation : risque moyen à élevé***	Une gouvernance plus rigoureuse sera nécessaire pour assurer la fiabilité des nouveaux fournisseurs Le risque de fraude lié aux opérations est possible en raison du vol ou de la relecture des jetons; la gestion des risques assurée par les paramètres des jetons est insuffisante La gestion du cycle de vie est simplifiée avec la solution HCE parce que les portefeuilles HCE sont plus facilement transférés d'un appareil mobile à un autre	Le paiement mobile peut être virtuellement constant, ce qui accélère son adoption (peut fonctionner dans tous les appareils activés par NFC, quel que soit l'ERM)
Risque pour la réputation ***Évaluation : risque moyen***	L'absence de normes sectorielles pourrait mener à des mises en œuvre qui ne sont pas équivalentes à celles de la technologie EMV	Les manquements à la sécurité peuvent nuire à l'intégrité du système de paiements canadien et miner la confiance des

Risque	Description	Impact sur le consommateur/le commerçant
		consommateurs et des commerçants

HCE est une nouvelle technologie qui évolue rapidement. Bien qu'un ensemble explicite d'exigences encadre le paiement par nuage informatique, il n'y a que des spécifications préliminaires en ce qui concerne la technologie HCE (Visa a été le premier réseau à publier des spécifications en février 2014). Certains problèmes se posent lorsqu'il est question de cette nouvelle technologie, notamment les suivants :

- **Une mise en œuvre trop rapide de la technologie HCE pourrait ne pas respecter un niveau de sécurité EMV.** L'interprétation des spécifications existantes pourrait entraîner la mise en œuvre de systèmes HCE non optimaux qui ne seraient pas conformes à des normes de sécurité équivalentes aux normes EMV (p. ex., les applications de portefeuille ou la segmentation en unités). Si les paramètres de sécurité sont insuffisants ou manquants (notamment la sécurité de l'appareil et de l'application), il est possible que des fraudeurs arrivent à intercepter les données ou les jetons d'authentification d'un paiement et à effectuer d'autres opérations à l'aide de ces données.
  Une sécurité accrue des appareils et des applications, l'utilisation de techniques, comme la cryptographie en boîte blanche et le brouillage, rendent plus complexe le vol de jetons d'authentification.
- **Les stratégies visant à gérer les données dynamiques doivent être exhaustives.** Les paramètres de protection applicables aux jetons d'authentification doivent être établis avec rigueur. Ces paramètres, comme les restrictions de domaine, visent à atténuer les risques en cas de vol de jetons d'authentification. À l'heure actuelle, il n'existe aucune ligne directrice claire et contraignante susceptible de favoriser un établissement de paramètres de protection optimaux applicables aux données dynamiques. Il est important que la technologie HCE assure la gestion continue des paramètres de protection de données de manière à minimiser les risques.
- **Des problèmes liés à l'interopérabilité pourraient se présenter.** L'interopérabilité est une préoccupation constante, puisque les portefeuilles dotés de la technologie HCE sont de plus en plus utilisés. Les différences quant à la configuration de ces portefeuilles pourraient entraîner des problèmes d'acceptation ou des conséquences involontaires pour les clients et les commerçants. Les consommateurs ont le droit d'installer plus d'un portefeuille doté de la technologie HCE et peuvent utiliser les mêmes données d'identification pour plusieurs d'entre eux. Par exemple, un consommateur pourrait avoir un portefeuille doté d'un élément sécurisé et un portefeuille doté

de la technologie HCE sur le même appareil. Gérer l'accès au contrôleur NFC pourra être complexe. À l'heure actuelle, il n'y a aucune mesure de coordination au sein de l'industrie pour veiller à ce que les multiples portefeuilles sur un même appareil fonctionnent conjointement.

Du point de vue du consommateur et du commerçant, il y a peu, voire aucune, différence au moment de réaliser un achat dans un point de vente entre la technologie de l'élément sécurisé et la technologie HCE. Ces deux solutions optimisent la communication en champ proche et répondent aux messages reçus du point de vente lorsqu'une MVC est utilisée.

Le tableau ci-après présente les principales différences entre la technologie de l'élément sécurisé et la technologie HCE qui devraient être prises en considération par les émetteurs.

TABLEAU 3 – COMPARAISON DES TECHNOLOGIES HCE ET SIM

Caractéristique	**SIM (élément sécurisé)**	**HCE**
Exigences liées à l'appareil	Appareil mobile muni d'un contrôleur NFC Carte SIM munie d'un contrôleur NFC L'appareil doit être approuvé par l'ERM et l'émetteur	Appareil mobile muni d'un contrôleur NFC
Approvisionnement	Exige du GSC qui est l'émetteur et du GSC qui est la société de télécommunications de mettre au point une application devant être installée dans l'appareil en vue de procéder au paiement et d'obtenir les justificatifs. Le client doit alors installer l'interface utilisateur du portefeuille ou il peut être installé au préalable par l'ERM En cas de changement d'appareil mobile par le client, ce dernier devra de	Le client doit installer les applications du portefeuille dans son appareil; les justificatifs de paiement sont transmis initialement et sont reconstitués dans le monde virtuel Les portefeuilles dotés de la technologie HCE peuvent être plus facilement transférés dans un nouvel appareil mobile

Caractéristique	SIM (élément sécurisé)	HCE
	nouveau installer le portefeuille et tous les justificatifs; le nouvel appareil mobile pourrait ne pas l'accepter	
Convivialité	Fonctionne en ligne et hors connexion Fonctionne que l'appareil soit en marche ou éteint (selon la configuration) Un mot de passe peut être enregistré directement dans l'appareil Liaison de données requise pour l'approvisionnement initial; mais pas pour la réalisation de l'opération	Opérations hors connexion difficiles à réaliser en raison de la pertinence des données dynamiques Le mot de passe ne peut être pris en charge hors connexion L'appareil doit être en marche et l'application servant au paiement doit être activée pour réaliser l'opération Liaison de données non requise pour l'approvisionnement initial et la reconstitution continue du jeton d'authentification; ni pour la réalisation de la transaction
Sécurité	Justificatifs mémorisés dans l'élément sécurisé sur une base matérielle ou dans l'élément sécurisé inviolable de la carte SIM Le PAN peut servir de jeton d'authentification ou non	Justificatifs mémorisés dans l'élément sécurisé du nuage informatique Les jetons d'authentification servant au paiement stockés dans l'appareil sont à usage unique ou limité de façon à contrôler le risque qu'ils soient mémorisés dans le logiciel La sécurité par couches est nécessaire pour contrôler le risque lié au fait de ne pas avoir un élément sécurisé sur une base matérielle
Gestion	Communication avec l'ERM individuel pour faciliter l'installation des justificatifs sur la carte SIM Le gestionnaire de services de confiance gère	Communication avec le FSA pour la gestion des justificatifs de paiement

Caractéristique	SIM (élément sécurisé)	HCE
	l'application de paiement	
Maturité	S'appuie sur des normes rigoureuses et de longue date Processus de certification bien défini par les marques de service de paiement	Les spécifications continuent d'évoluer et pourraient devoir être harmonisées pour l'ensemble des FMO et des réseaux de paiement Processus de certification pas encore bien défini pour l'ensemble des marques de service de paiement
Interopérabilité	Des normes existent pour encadrer l'interopérabilité à la plupart des points de contact clés	L'interopérabilité devra être surveillée au fur et à mesure que de nouveaux systèmes sont lancés

Portefeuilles mobiles ouverts

Au début, les paiements mobiles ont entraîné la création de solutions exclusives en circuit fermé, comme celle offerte par Starbucks, lesquelles permettent à l'émetteur de justificatifs de contrôler tous les volets de l'écosystème. Ces premières solutions reposent sur des justificatifs statiques (comme les codes à barres) et sur des systèmes existants optimisés dans les points de vente (les lecteurs numériques, par exemple).

La création de systèmes de paiement mobile en circuit ouvert nécessite que l'opération soit approuvée au point de vente, ce qui a été facilité par la mise au point de terminaux NFC. Les portefeuilles appartenant à des établissements financiers optimisent la technologie NFC et les éléments sécurisés sur une base matérielle (une carte SIM) et ont permis la réalisation d'opérations mobiles sécurisées sans contact. Les émetteurs ont créé l'application mobile, ont retenu les services d'un gestionnaire de services de confiance (GSC) afin qu'il lance et gère l'application, puis ont loué de l'espace auprès d'un ERM sur l'élément sécurisé de manière à installer l'application sur l'appareil mobile.

L'évolution des modèles de gestion en matière de paiement mobile est accélérée par l'évolution de la technologie. Au cours des six derniers mois, diverses annonces majeures ont été faites et témoignent de l'évolution constante du marché du paiement mobile. Le lancement d'Apple Pay en octobre 2014 a notamment amené au premier plan le modèle de gestion appelé « portefeuille mobile ouvert ».

Un survol détaillé des solutions de portefeuilles mobiles ouverts offerts au Canada et aux États-Unis est présenté à l'annexe C.

PORTEFEUILLES MOBILES OUVERTS – RÉPERCUSSIONS ÉVENTUELLES SUR LES ÉMETTEURS

Les différentes annonces qui ont été faites concernant les paiements mobiles au cours des six derniers mois permettent de tirer certaines déductions. Les grandes sociétés de technologie s'intéressent sérieusement aux paiements mobiles et lancent différentes solutions qui misent sur une meilleure expérience client. Nous estimons qu'il est essentiel que les portefeuilles mobiles ouverts offerts au Canada respectent des normes de sécurité équivalentes aux normes EMV.

Si Apple Pay demeure la seule plateforme viable pour le iPhone, la lutte en faveur de la pertinence sera vraisemblablement engagée sur la plateforme Android. L'introduction de la technologie HCE a éliminé de nombreux obstacles qui freinaient l'élaboration rapide de solutions de paiement mobile. La création de réseaux de paiement dans de nouveaux secteurs d'activités (p. ex., les jetons d'authentification) devrait permettre d'accélérer le développement et le déploiement de nouveaux portefeuilles ouverts au moyen de solutions qui simplifient considérablement le téléchargement des justificatifs de paiement. Les plus importants joueurs dans l'industrie du paiement consolident leur position par l'introduction de nouveaux produits et services (p. ex., Android Pay et

Samsung Pay) et par le biais d'acquisitions (p. ex., l'achat par Google de Softcard ou l'achat par PayPal de Paydiant).

Ce marché en rapide évolution comporte certains problèmes et certains risques importants susceptibles d'avoir des répercussions sur le marché des paiements mobiles au Canada. On suppose qu'il y aura une prolifération de portefeuilles mobiles ouverts dotés de la technologie HCE et d'autres produits et services similaires à Android Pay. On s'attend également à ce que les consommateurs souhaitent éventuellement installer leurs justificatifs de paiement dans plus d'un portefeuille.

RISQUES ÉVENTUELS ASSOCIÉS AUX PORTEFEUILLES MOBILES OUVERTS

En ce qui concerne les applications de portefeuilles exclusifs, les émetteurs sont en mesure de contrôler étroitement la sécurité de la solution et l'expérience du consommateur. Ils gèrent la disponibilité de l'application de paiement mobile et s'assurent de reconnaître l'utilisateur qui demande un justificatif numérique. Les émetteurs choisissent par ailleurs la MVC souhaitée (NIP ou mot de passe), définissent les paramètres de protection des données dynamiques, gèrent la production des jetons d'authentification et supervisent le processus d'approvisionnement. En revanche, pour les portefeuilles mobiles ouverts, les émetteurs délèguent certaines de ces fonctions au fournisseur du portefeuille et au FSA.

Participer à des portefeuilles mobiles ouverts peut exiger de l'émetteur qu'il externalise des composantes importantes du processus d'enregistrement et d'approvisionnement, ainsi que de la sécurité globale de l'opération, au fournisseur du portefeuille et au FSA. Bien que les émetteurs puissent ne pas gérer tous les volets des failles éventuelles à la sécurité en ce qui a trait au portefeuille mobile ouvert, ils demeurent responsables de l'opération de bout en bout. Cet engagement comporte de nombreux risques.

L'identification et la vérification inadéquates des clients peuvent accroître le piratage des comptes

La capacité de confirmer avec certitude l'identité d'un client est particulièrement importante en ce qui concerne les portefeuilles mobiles ouverts. Un portefeuille mobile ouvert qui assure le plus haut niveau de sécurité peut tout de même comporter un risque de fraude si l'identité du client faisant une demande de justificatifs n'est pas validée.

Par exemple, un fraudeur qui vole une carte de paiement ou un numéro de carte pourrait tenter d'enregistrer la carte dans un portefeuille mobile ouvert. Si le processus d'identification et de vérification est inadéquat, le fraudeur pourrait bien réussir à enregistrer la carte et activer le portefeuille. S'il y parvient, il pourra utiliser impunément la carte dans des points de vente ou à distance jusqu'à ce que le véritable détenteur de la carte ou l'émetteur détecte la fraude. Même la solution de paiement mobile la plus sécuritaire ne sera pas en mesure de contrebalancer un processus d'identification et de vérification inadéquat. Un processus d'identification et de vérification rigoureux est essentiel pour soutenir l'intégrité du système de paiement.

Dans le cas d'une solution de portefeuille mobile ouvert, l'émetteur des justificatifs de paiement continue de gérer la communication avec le client ainsi que toutes les obligations qui en découlent. Pour cette raison, chaque demande de justificatifs de paiement devrait être transmise à l'émetteur des justificatifs aux fins d'examen et d'une prise de décision. En tant que propriétaire des responsabilités associées au compte, l'émetteur (et non le fournisseur du portefeuille ou le FSA) sera en meilleure position pour décider d'approuver ou non une demande de justificatifs. De cette façon, l'émetteur demeure responsable et imputable en ce qui concerne la validation de l'identité du client qui demande des justificatifs. Si l'émetteur souhaite impartir le processus d'authentification, il peut le faire au vendeur de son choix qui satisfait aux exigences en matière d'identification et de vérification.

Jusqu'à aujourd'hui, les émetteurs n'ont, en règle générale, pas été contraints de répondre aux demandes de justificatifs de paiement reçues de tiers et ils devront mettre au point des processus visant à valider l'identité du client. Des renseignements supplémentaires sont donnés dans le cadre du processus d'enregistrement de portefeuille mobile ouvert et les émetteurs devraient demander que les données appartenant à l'appareil mobile (p. ex., un lecteur d'empreinte digitale) et à l'application de paiement mobile (p. ex., numéro d'identification individuel) soient saisies et transmises par le fournisseur du portefeuille, de même que les renseignements sur le client et les justificatifs de paiement. L'information portant sur la méthode de vérification (p. ex., les empreintes digitales et le mot de passe) devrait également être demandée par les émetteurs et donnée par le fournisseur du portefeuille. L'ensemble de ces données aidera l'émetteur à valider efficacement l'identité du client, les justificatifs, l'application de paiement et l'appareil. Les données saisies au moment de l'enregistrement peuvent également être utilisées pour étayer la prise de décision concernant l'autorisation ou non d'une opération.

Le processus d'identification et de vérification sera au centre des mesures de sécurité relatives au portefeuille mobile ouvert. Il sera primordial de déceler toute tentative de piratage de compte au moment de l'enregistrement. Le processus d'identification et de vérification défaillant d'un seul émetteur pourrait bien miner la confiance des consommateurs et des commerçants envers tout le système de paiement canadien. Il est essentiel de valider avec certitude l'identité du client.

S'il existe des disparités entre les stratégies en matière d'identification et de vérification adoptées par les émetteurs, les fraudeurs seront capables de repérer rapidement les émetteurs munis de systèmes inadéquats. Les émetteurs aux États-Unis ont eu à résoudre ce problème et les autres territoires pourraient tirer de précieuses leçons de cette expérience. Il est dans l'intérêt de l'industrie canadienne du paiement que les processus d'identification et de vérification soient fiables à l'échelle de l'industrie. Le défi consistera à mettre en œuvre des pratiques rigoureuses en matière d'identification et de vérification sans trop entraver le processus d'approvisionnement.

De nouvelles méthodes de vérification de cartes (MVC) sont mises au point

Au sein de l'écosystème des paiements mobiles, il existe de méthodes de vérification de cartes solides visant à assurer que seuls des clients autorisés peuvent effectuer des opérations. L'identité d'une personne peut être validée de trois manières :

Facteur connaissances. Une chose que l'utilisateur **sait**

– Exemples : mot de passe, phrase passe, NIP, configuration ou question/réponse

Facteur propriété. Une chose que l'utilisateur **possède**

– Exemples : carte d'identité, carte de paiement ou jeton d'authentification sur base matérielle ou logicielle

Facteur inhérence. Une chose que l'utilisateur **est** ou **fait**

– Exemples : signature, paramètres biométriques (empreinte digitale, reconnaissance faciale, reconnaissance vocale, lecture d'empreinte rétinienne ou reconnaissance du rythme cardiaque)

Les émetteurs se fient surtout à deux de ces facteurs d'authentification, une chose que l'utilisateur possède (p. ex., une carte de paiement ou un appareil mobile) et une chose que l'utilisation sait (p. ex., un NIP). Par le passé, le facteur inhérence, une chose que l'utilisateur est, s'est avérée être la méthode de vérification la plus faible. Les signatures faites à la main sont difficiles à valider avec certitude en personne, et c'est pire à distance.

Les progrès technologiques récents, notamment la création de matériel informatique doté d'un processus d'authentification biométrique, ont ramené le facteur inhérence à l'avant-plan. Les téléphones intelligents, comme le iPhone 6 et le Galaxy S6, comportent des lecteurs d'empreintes digitales. Les consommateurs peuvent utiliser le lecteur d'empreintes digitales pour déverrouiller l'appareil ainsi que pour accéder aux applications installées dans l'appareil mobile. Apple Pay optimise la capacité du iPhone Touch ID de valider chaque opération de paiement; on s'attend à ce que le Samsung Pay offre lui aussi un lecteur d'empreintes digitales similaire.

La lecture d'empreintes digitales pose certains problèmes et pourrait éventuellement servir involontairement à de la fraude par un membre de la famille (fraude effectuée par un membre de la famille au moyen d'une carte de crédit). L'utilisateur peut souvent entrer de cinq à 10 empreintes digitales dans l'appareil pouvant être utilisées pour servir à différentes fins, en plus d'autoriser une opération de paiement. Par exemple, l'enfant du propriétaire de l'appareil peut enregistrer ses empreintes digitales afin d'être en mesure de déverrouiller l'appareil; permettant ainsi à l'enfant du détenteur de la carte d'effectuer des achats non autorisés à l'insu du détenteur de la carte.

Par ailleurs, ces appareils sont généralement couverts d'empreintes digitales et, dans l'éventualité où l'appareil serait volé ou perdu, les fraudeurs pourraient être en mesure de créer une empreinte digitale et d'avoir accès au contenu de l'appareil, notamment y effectuer des achats. Cette éventualité n'est pas que théorique, des directives expliquant comment forcer divers lecteurs d'empreintes digitales offerts sur le marché circulent déjà sur le Web.

D'autres solutions biométriques (p. ex., la reconnaissance de la voix, du visage et du rythme cardiaque) devraient être accessibles dans le monde entier à court terme. Les avantages anticipés pour les clients sont évidents : une expérience de paiement plus rapide et plus conviviale.

La MVC utilisée pour les paiements par portefeuille mobile ouvert ne sera sans doute pas celle de l'émetteur

Pour la carte à puce EMV avec utilisation d'un NIP, il est conseillé au client de choisir un NIP de quatre chiffres qui sera réservé à cette carte. Pour les portefeuilles mobiles ouverts, la méthode de vérification des paiements pourrait être la même pour tous les justificatifs de paiement dans le portefeuille et sera fort probablement celle qui est utilisée pour déverrouiller l'appareil.

Lorsqu'une opération est effectuée au PDV au moyen d'une carte à puce EMV nécessitant l'entrée d'un NIP, l'émetteur reçoit une confirmation que le NIP entré dans le terminal PDV correspond au NIP enregistré sur la carte (la correspondance est confirmée par le PDV) ou au NIP indiqué au dossier (le NIP est confirmé par l'ordinateur hôte de l'émetteur). Pour les portefeuilles mobiles ouverts, la méthode de vérification pourrait ne pas être un NIP et la correspondance entre la méthode fournie par le consommateur et celle enregistrée dans l'appareil mobile sera confirmée par l'appareil. Les émetteurs n'ont aucune visibilité directe de la méthode de vérification utilisée et doivent donc « faire confiance » à l'appareil pour confirmer la correspondance. Les méthodes d'authentification biométrique risquent de ne pas être aussi sécuritaires qu'un NIP. Alors que les méthodes basées sur les connaissances, comme les mots de passe et les NIP, exigent une correspondance exacte, les méthodes biométriques donnent lieu à des données « bruitées ». La position et la pression du doigt influent sur la reconnaissance de l'empreinte et l'éclairage peut fausser la reconnaissance faciale. Pour composer avec ces « bruits », les niveaux de tolérance sont établis de manière à permettre de légères variations.

La méthode de vérification revêt de l'importance pour les émetteurs lorsque les opérations au PDV sont supérieures au plafond de 100 $ fixé pour les paiements de valeur élevée sans contact. Jusqu'à ce que les méthodes d'authentification biométrique aient fait leur preuve, nous préférerions une méthode de vérification de données que les clients connaissent à une méthode d'authentification de caractéristiques personnelles.

Les méthodes de vérification des paiements mobiles pourraient avoir des répercussions sur les clients. Ainsi, des mesures de sécurité additionnelles seront intégrées aux options de vérification des paiements mobiles. Il sera important d'informer les clients de ces répercussions afin qu'ils soient au courant des risques et apprennent à différencier et à protéger leurs méthodes de vérification de paiements mobiles, tout comme ils protègent leur NIP.

Les MVC évoluent en raison des nouveaux systèmes de reconnaissance biométrique. À mesure que les consommateurs feront plus d'opérations mobiles, les émetteurs devront sans doute moins compter sur les méthodes de vérification des appareils

mobiles et faire davantage confiance à d'autres données (informations sur l'appareil et l'application) pour vérifier et valider l'identité des clients.

Les normes minimales et les processus de certification et d'examen s'appliquant aux portefeuilles mobiles ouverts ne sont pas clairs

Même si les spécifications relatives aux paiements dans l'infonuage peuvent être obtenues auprès des réseaux de paiement, leur mise en application par les fournisseurs de portefeuilles mobiles ouverts n'est pas claire. De plus, il n'existe aucun processus clair de certification, d'examen ou d'approbation permettant d'assurer que les portefeuilles mobiles ouverts satisfont aux normes minimales ou aux exigences des réseaux de paiement. La vérification des demandeurs de jetons d'authentification, y compris des portefeuilles, incombe au FSA. Au moment de mettre sous presse, il n'y avait aucune ligne directrice concernant l'évaluation des demandeurs. Essentiellement, les émetteurs doivent se fier aux mesures de sécurité mises en place par des tiers pour protéger les renseignements sur les clients et les paiements.

Les émetteurs devront probablement compter sur les mesures de sécurité mises en place par des tiers

Les portefeuilles mobiles ouverts basés sur la technologie HCE pourraient présenter plus de risques, puisque les émetteurs n'auront sans doute qu'un contrôle limité sur la façon dont la solution de portefeuille protège l'appareil mobile (p. ex., sécurité de l'application, de l'appareil et des communications), sur les paramètres qui définissent la nature des données dynamiques et sur la saisie de ces données dans l'appareil mobile. Le fournisseur de portefeuilles ou ses partenaires/contractants pourraient ne pas offrir le même niveau de sécurité que les solutions mises au point par les émetteurs.
Ces derniers devront parfaitement comprendre tous les aspects de la sécurité liés à un portefeuille mobile ouvert doté de la technologie HCE pour être en mesure d'évaluer le risque technologique de la solution de portefeuille.

Les rôles et responsabilités du FSA devraient évoluer

Les portefeuilles mobiles ouverts ont introduit la notion de segmentation en unités des numéros de compte primaire *(PAN tokenization)* dans les flux de paiements. Au lieu du numéro de la carte elle-même, un autre numéro (un PAN segmenté en unités) est fourni. Les commerçants ne voient jamais le véritable numéro de la carte, seulement le PAN segmenté en unités. La segmentation en unités n'est pas nouvelle, mais elle n'a jamais été utilisée dans le processus de paiement.

Au moment de publier, d'importants fournisseurs de portefeuilles mobiles ouverts (Apple, Samsung, Android) avaient annoncé l'établissement de relations avec les réseaux de paiement. La segmentation en unités pour ces solutions de portefeuille mobile ouvert devrait être effectuée par American Express Token Service, MasterCard Data Enablement Services, Visa Tokenization Services, et par Interac au Canada. L'établissement d'un partenariat avec ces réseaux permet aux fournisseurs de portefeuilles mobiles ouverts d'avoir un seul point de contact par réseau avec tous les émetteurs de carte associés (l'inverse est aussi vrai). Ce modèle assure une mise en marché beaucoup plus rapide pour les fournisseurs de portefeuilles, mais limite le choix de fournisseurs pour les émetteurs.

En mars 2014, EMVCo a publié ses spécifications relatives à la segmentation en unités des paiements. Ce document est une première version et sera mis à jour au fil du temps. Dans sa version actuelle, il fournit peu d'informations sur l'établissement et la maintenance des interfaces API des demandeurs de jetons d'authentification et sur la garde, le stockage, la sécurité, les plateformes d'approvisionnement et les registres des jetons. Pour en savoir plus sur les préoccupations concernant les spécifications publiées par EMVCo, veuillez consulter l'Annexe D.

Même si cette fonction n'est pas définie dans les spécifications d'EMVCo relatives à la segmentation en unités, les FSA des réseaux de paiement ont aussi pris en charge l'installation de justificatifs numériques dans un élément sécurisé. Comme les portefeuilles mobiles ouverts sont basés sur la technologie HCE, les rôles et responsabilités du FSA devraient être élargis pour inclure l'installation de données dynamiques. Il est important que ces rôles et responsabilités soient clairement définis.

Idéalement, les émetteurs n'auront pas à s'en remettre à un tiers pour définir les paramètres des données dynamiques et pourront déterminer et surveiller l'efficacité de la stratégie relative aux données dynamiques. Toutefois, les modèles d'affaires évoluent rapidement et les émetteurs pourraient décider de fournir des justificatifs à des entités qui en font la demande et qu'ils connaissent peu et sur lesquelles ils ont peu de contrôle. Lorsque le FSA agit comme intermédiaire, il devrait, en principe, s'assurer que tous les aspects de la segmentation en unités et de l'installation de données dynamiques sont sécuritaires et que toutes les parties concernées sont protégées contre les risques.

Les opérations dans les portefeuilles mobiles ouverts généreront plus de données pour un plus grand nombre d'entités

Les paiements mobiles pourraient générer plus de données que les opérations traditionnelles par carte à puce avec NIP au PDV. Chose certaine, il y aura plus de données, accessibles à plus d'entités et stockées dans un plus grand nombre d'endroits. Cette situation présentera à la fois des possibilités et des défis pour les émetteurs et pour l'écosystème des paiements.

Les opérations effectuées à partir d'un portefeuille pourraient fournir à l'émetteur des renseignements supplémentaires sur l'appareil (IMEI [identité internationale d'équipement mobile], MEID [identifiant d'équipement mobile], adresse IP), sur le matériel (spécifications, ID Android, UDID [numéro d'identifiant unique] iPhone), sur le portefeuille (ID App) et sur l'emplacement (GPS). Les émetteurs pourraient intégrer ces données dans leurs systèmes afin de soutenir l'autorisation des opérations et la surveillance de la fraude.

Par ailleurs, ces données, y compris celles sur les opérations, seront sans doute accessibles à d'autres parties (fournisseurs de portefeuilles mobiles ouverts), qui pourraient les trouver utiles. L'accès aux données et leur propriété n'ont pas été clairement définis. Les fournisseurs de portefeuilles pourraient les consulter pour mieux comprendre leurs clients et les commerçants, pour fidéliser leurs clients et pour mettre au point des offres personnalisées.

Un accès accru aux données présente des possibilités et des risques. Les données sur les opérations seront sans doute stockées par des tiers fournisseurs de portefeuilles et par les FSA. Les émetteurs n'ont aucun contrôle sur la façon dont les tiers protègent les données. Aucune mesure claire visant à empêcher l'accès aux données par des tiers n'a été adoptée et l'émetteur n'a aucun contrôle sur la sécurité des systèmes de stockage. Il importe que les émetteurs sachent où les données des opérations sont saisies et stockées afin qu'ils puissent respecter leur engagement de protéger les renseignements des titulaires de carte et partager leurs obligations avec les tiers, au besoin.

Aspects à considérer pour accélérer l'adoption des portefeuilles mobiles ouverts au Canada

Pour accroître l'utilisation des paiements mobiles, l'expérience client devra être aussi, sinon plus, satisfaisante que les opérations par carte. Les consommateurs devront être en mesure de télécharger leurs justificatifs de paiement dans le portefeuille de leur choix et de régler leurs opérations, peu importe le montant, par l'entremise de tout canal sur leur appareil mobile. L'adoption des paiements mobiles pourrait continuer de progresser lentement jusqu'à ce que les appareils mobiles offrent les mêmes fonctions, voire un plus grand nombre de fonctions, que les cartes de paiement.

Selon les estimations, environ 30 pour cent des terminaux PDV au Canada acceptent des paiements[12] mobiles NFC sans contact. Pour que les consommateurs effectuent exclusivement des opérations mobiles, il faudra que ce taux continue d'augmenter et que, finalement, tous les terminaux PDV acceptent les paiements NFC. Des paiements sans contact peuvent actuellement être effectués pour des montants inférieurs à 100 $. Les consommateurs adopteront plus facilement les paiements mobiles s'ils peuvent effectuer des opérations de n'importe quel montant aux terminaux PDV. Les terminaux seront mis à niveau pour accepter des opérations de valeur élevée. Ces mises à niveau devraient être terminées en 2018.

Un obstacle important à l'adoption des paiements mobiles par les consommateurs canadiens est le manque d'uniformité des solutions relatives à l'élément sécurisé. Les institutions financières canadiennes n'arrivent pas à commercialiser les paiements mobiles auprès de l'ensemble de leurs clients. Les consommateurs ont de la difficulté à confirmer leur admissibilité aux paiements mobiles (*Puis-je effectuer des paiements mobiles avec ma carte? Mon fournisseur est-il admissible? Mon appareil mobile est-il accepté?*). Bien que cinq banques canadiennes émettent actuellement des justificatifs de paiement mobile et que tous les ERM acceptent les paiements mobiles au moyen de nombreux appareils pour un ou plusieurs émetteurs, il est estimé que moins de 25 pour cent[13] des consommateurs canadiens ont le chevauchement nécessaire entre les justificatifs de paiement, les fournisseurs de services et l'appareil mobile pour effectuer des paiements mobiles.

Les émetteurs canadiens évaluent des solutions HCE qui pourraient résoudre un grand nombre de problèmes liés aux paiements mobiles. La technologie HCE est nouvelle et, au cours des prochaines années, le secteur s'efforcera de préciser les spécifications ainsi que de déterminer et de gérer les risques liés à la technologie et à l'interopérabilité.

Les sociétés technologiques, comme Apple, Samsung et Google, changeront sans doute la perception des consommateurs et des intervenants à l'égard des paiements mobiles. Ces sociétés tireront parti des nouvelles technologies, se doteront de nouveaux modèles d'affaires et fourniront une expérience client exceptionnelle.

---

[12] Entrevues au sein de l'industrie

[13] Analyse exclusive

Leurs solutions offriront des choix aux consommateurs canadiens. L'adoption de ces solutions dépendra de la proposition de valeur du portefeuille, de la pénétration du marché des appareils mobiles pouvant utiliser un portefeuille (système d'exploitation et technologie NFC) et de l'acceptation des services de paiement mobile NFC.

L'adoption restera limitée jusqu'à ce que les consommateurs puissent effectuer tous leurs paiements à l'aide de leur appareil mobile. Les opérations de valeur élevée au point de vente devraient être offertes au cours des prochaines années, lorsque les terminaux auront été mis à niveau. Pour rivaliser avec les gros portefeuilles mondiaux, les portefeuilles canadiens exclusifs devront sans doute accepter les systèmes de paiement à distance. Les paiements effectués à l'aide d'une application devraient augmenter considérablement. Les émetteurs canadiens devront déterminer s'ils acceptent les paiements de cette nature et de quelle façon.

Jusqu'à maintenant, deux portefeuilles mobiles ouverts canadiens ont été lancés. L'un des principaux défis pour les fournisseurs de portefeuilles mobiles ouverts et les émetteurs de justificatifs est de savoir comment donner suite à une demande de téléchargement d'un justificatif de paiement mobile exclusif dans le portefeuille mobile ouvert d'une autre partie. Cette opération peut être assez complexe dans un environnement d'élément sécurisé où chaque émetteur pourrait ne pas avoir de lien avec chaque ERM et ne pas accepter tous les appareils. Pour les solutions HCE, les défis pourraient avoir trait aux paramètres des données dynamiques et aux exigences minimales des émetteurs en matière de sécurité.

Pour accélérer l'adoption des solutions de portefeuille mobile ouvert, il pourrait être utile de cerner pour les émetteurs et pour les fournisseurs de portefeuilles des occasions de partager facilement les données et les justificatifs de paiement.

Pistes à privilégier pour la mise en œuvre des principes directeurs

Les paiements mobiles évoluent rapidement et pourraient bouleverser la façon dont les biens sont achetés et vendus au Canada. Tous les participants de l'industrie sont susceptibles de tirer profit des portefeuilles mobiles ouverts, en particulier les consommateurs et les commerçants, car ils réduisent les frictions et procurent des services à valeur ajoutée. Pour que les paiements mobiles soient adoptés dans l'ensemble de l'écosystème, la proposition de valeur devra attirer les consommateurs et les commerçants. De plus, le niveau de sécurité devra être équivalent ou supérieur à celui offert par les cartes de paiement. Ce n'est qu'à ces conditions que les consommateurs laisseront leur portefeuille chez eux.

Offrir un niveau de sécurité équivalent à celui des cartes de paiement EMV

L'évolution des solutions de paiement s'accélère au Canada et c'est à la fois une source d'occasions et de risques. À la suite du lancement des portefeuilles mobiles ouverts aux États-Unis, les émetteurs canadiens ont mesuré les effets de cette nouvelle technologie sur la sécurité des paiements, en plus de tirer les leçons de l'expérience américaine. Le Canada a réalisé des investissements considérables dans l'infrastructure EMV et les consommateurs, comme les commerçants, comptent sur une certaine sécurité. Les fournisseurs de portefeuilles mobiles ouverts qui exercent des activités au Canada devront proposer des solutions dont le niveau de sécurité est semblable à celui qui existe sur le marché canadien.

La technologie HCE est la dernière technologie de paiement lancée au Canada. Il est probable qu'elle sera largement utilisée dans les portefeuilles exclusifs d'émetteurs et les portefeuilles mobiles ouverts. L'intégrité des solutions HCE dépend de l'implantation judicieuse d'une sécurité multiniveaux, notamment d'une approche rigoureuse à l'égard des données dynamiques, afin de fournir la sécurité des paiements requise.
Les émetteurs canadiens devront définir un modèle de collaboration efficace avec les réseaux de paiement, les fournisseurs de portefeuilles et les fournisseurs de services d'authentification afin de s'assurer que les solutions commercialisées offrent une sécurité équivalente à celle des paiements EMV.

Pour appuyer le déploiement de la technologie HCE, l'adoption de normes sectorielles strictes et de spécifications relatives aux réseaux de paiement sera nécessaire, mais elle prendra du temps. Dans l'intervalle, les rôles et les responsabilités continueront d'évoluer et, par conséquent, des problèmes de sécurité et d'interopérabilité pourraient survenir. Dans un tel contexte, les émetteurs devront naviguer avec prudence.

L'innovation en termes de solutions de paiement mobile devrait renforcer la sécurité et l'intégrité de l'écosystème de paiement canadien et offrir une sécurité des paiements équivalente à celle des justificatifs de paiement EMV actuellement présents sur le marché.

Établir un processus rigoureux d'identification et de vérification afin de protéger adéquatement les consommateurs contre la fraude par carte de paiement

Les émetteurs de portefeuilles mobiles ouverts exclusifs gèrent leur solution de A à Z, ainsi que les risques connexes. En revanche, pour participer aux portefeuilles ouverts, les émetteurs pourraient être obligés d'externaliser certains aspects clés de leur solution aux fournisseurs de portefeuilles. Ils continueront de gérer les relations avec les clients et devraient envisager d'examiner toutes les demandes de justificatifs numériques envoyées par les fournisseurs de portefeuilles mobiles ouverts. Un processus d'identification et de vérification rigoureux sera indispensable pour protéger les consommateurs contre la fraude par prise de contrôle d'un compte. Même si la sécurité des opérations est excellente, le chargement frauduleux de justificatifs de paiement peut compromettre un portefeuille mobile ouvert.

Dans le cadre du processus d'inscription, les émetteurs devraient songer à demander un minimum de données sur l'appareil, l'application de portefeuille et la méthode de vérification (p. ex., empreinte digitale ou mot de passe). Ces données permettront d'établir une liaison fiable entre le consommateur, les justificatifs de paiement, l'appareil et l'application de portefeuille afin d'étayer les décisions d'autorisation des opérations.

Actuellement, les émetteurs canadiens se fient au NIP pour autoriser les opérations aux points de vente. Les intervenants du secteur des paiements canadien communiquent d'une même voix pour souligner l'importance de protéger son NIP et d'avoir un NIP différent pour chaque carte de paiement. En ce qui concerne les solutions de portefeuilles mobiles, les consommateurs utiliseront probablement la même méthode de vérification pour toutes les cartes de paiement de leur portefeuille, mais aussi, éventuellement, pour toutes les applications de leur appareil. De l'autre côté, l'information de vérification fournie aux émetteurs pourrait se limiter à confirmer que la méthode de vérification conservée sur l'appareil mobile correspond à celle présentée par le consommateur. Dans le cas des portefeuilles qui recourent à une préautorisation des opérations (méthode de vérification « tapez »), la méthode de vérification permettra d'effectuer tous les paiements, peu importe le montant ou le canal choisi.

Selon les pratiques exemplaires relatives aux paiements EMV, il est recommandé d'attribuer un NIP de quatre chiffres unique à chaque carte de paiement. Le fait d'utiliser une méthode de vérification biométrique qui n'est pas spécifique à une carte, ni même à un portefeuille, et qui n'est pas un renseignement que seul le consommateur connaît (comme un mot de passe) peut exposer les émetteurs et les consommateurs à certains risques. Idéalement, le secteur suivra un processus de paiement pour les opérations supérieures à 100 $ dans tous les canaux (paiements aux points de vente, paiements à distance, paiements à l'aide d'une application) qui sera le même pour tous les produits de paiement et les portefeuilles.

Les émetteurs pourraient être obligés de recourir à d'autres données, en plus de la méthode de vérification, pour approuver les opérations en toute confiance. Des processus efficaces d'identification et de vérification devraient donner lieu à une liaison fiable entre le consommateur, les justificatifs, l'application de paiement et l'appareil. Les émetteurs pourront demander aux fournisseurs de portefeuilles des données complémentaires qui ont été fournies au moment de l'inscription en vue de confirmer l'identité des titulaires de cartes. Les émetteurs pourront utiliser ces renseignements complémentaires pour étayer leurs décisions d'autorisation des opérations, de façon à réduire leur dépendance aux méthodes de vérification, tout en maintenant la sécurité globale des opérations.

Présenter une proposition de valeur attrayante aux consommateurs

Afin de généraliser l'adoption des paiements mobiles, l'expérience client offerte par les appareils mobiles doit être aussi bonne ou meilleure que celle offerte par les cartes de paiement. Idéalement, les consommateurs devraient avoir la possibilité de charger n'importe lequel de leurs justificatifs de paiement dans le portefeuille de leur choix. Ils devraient être capables de payer toutes leurs opérations, peu importe le montant et le canal, à l'aide de leur appareil mobile.

Au Canada, la technologie NFC affiche un taux d'acceptation raisonnable, celui-ci étant particulièrement élevé dans les marchés verticaux clés. En fin de compte, tous les appareils aux points de vente devront accepter les paiements mobiles utilisant la technologie NFC, afin que la plupart des consommateurs optent pour ce mode de paiement.

Bien que des solutions de paiement mobile existent actuellement sur le marché, les consommateurs attendent une harmonisation entre les émetteurs, les ERM et leur appareil avant de participer. Non seulement les couvertures de chaque émetteur et ERM sont-elles limitées, mais en plus elles ne se chevauchent pas. Les solutions HCE qui seront lancées à court terme devraient s'attaquer aux défis liés aux fournisseurs de services et, dans une certaine mesure, aux appareils. Grâce à la solution Apple Pay dont le lancement est prévu au Canada, les consommateurs qui possèdent un appareil mobile iPhone pourront utiliser la fonction de paiement mobile.

Les émetteurs canadiens devront évaluer les caractéristiques de leurs solutions de paiements mobiles exclusives à la lumière des fonctions que les fournisseurs mondiaux de portefeuille, comme Samsung, Android et Apple, intégreront à leurs appareils. À l'heure actuelle, les solutions canadiennes n'acceptent pas les opérations aux points de vente supérieures à 100 $ et ne permettent pas d'effectuer des paiements à distance ni des paiements à l'aide d'une application. Les émetteurs devraient chercher et étudier des options d'acceptation à distance.

On s’attend à ce que les portefeuilles mobiles ouverts facilitent l’adoption des paiements mobiles. L’utilisation d’interfaces « un à plusieurs » pourrait considérablement accélérer la disponibilité des portefeuilles mobiles ouverts au Canada. Une capacité de service sectorielle connectant fournisseurs de portefeuilles et émetteurs de justificatifs de paiement pourrait servir à étayer les demandes de justificatifs, à surveiller la fraude dans l’ensemble du secteur et à tester l’interopérabilité, ainsi qu’à fournir et à gérer les données dynamiques.

Les intervenants du secteur canadien des paiements mobiles ont des intérêts communs. Le contexte mondial des paiements évolue. Les progrès technologiques appuieront le déploiement rapide des capacités de paiements mobiles. Les acteurs les plus importants entendent jouer un rôle déterminant dans le domaine des paiements mobiles. Les émetteurs canadiens continueront de gérer les relations avec la clientèle et d’assumer les responsabilités connexes. Lorsqu’ils évaluent les occasions de fournir de nouvelles options de paiements mobiles aux consommateurs, les émetteurs doivent absolument maintenir la priorité sur la sécurité, s’assurer que les consommateurs et les détaillants sont protégés contre la fraude et veiller à gérer les risques adéquatement. Ainsi, les investissements canadiens dans la sécurité des paiements seront préservés.

Proposition de marche à suivre

Authentification rigoureuse du client à l'adhésion

Étant donné que l'adhésion aux portefeuilles mobiles ouverts peut être effectuée de multiples manières, l'authentification des clients sera essentielle pour maintenir l'intégrité des portefeuilles mobiles ouverts et des justificatifs de paiement. Il sera primordial pour les émetteurs de repérer les tentatives de prise de contrôle d'un compte au moment de l'enregistrement d'un portefeuille mobile, avant de fournir un justificatif de paiement. Comme les émetteurs demeurent responsables en cas de fraude, chaque demande de justificatif de paiement devra être adressée à l'émetteur du justificatif, aux fins de notation et de prise de décision.

Les émetteurs canadiens sont encouragés à s'assurer que les consommateurs restent protégés contre la fraude par prise de contrôle d'un compte, en mettant en place des procédures adéquates d'identification et de vérification des clients. Idéalement, la totalité des demandes de justificatifs de paiement des portefeuilles mobiles ouverts devrait être envoyée aux émetteurs et notée en fonction de leurs protocoles de gestion du risque exclusifs. Il serait utile de définir les exigences minimales en matière de données visant à étayer l'émission de justificatifs. En outre, il conviendrait de déterminer la façon dont les portefeuilles mobiles ouverts transmettraient ces données aux émetteurs, dans le cadre du processus d'émission des justificatifs. Ces données pourraient faire partie des éléments requis dans une demande de justificatifs de paiement. Si cette approche était retenue, chaque FSA exerçant au Canada serait obligé d'être en mesure d'enregistrer ces données et de les transférer des fournisseurs de portefeuilles aux émetteurs. Idéalement, les données d'identification et de vérification exigées seront les mêmes dans tous les réseaux de paiement (American Express, Interac, MasterCard et Visa).

Authentification du client au moment de l'opération

En plus de favoriser l'émergence de nouveaux modèles d'affaires dans le secteur des paiements canadien, les portefeuilles mobiles ouverts créeront de nouvelles méthodes de vérification (p. ex., empreinte digitale) et permettront d'effectuer de nouveaux types d'opérations (p. ex., opération par l'entremise d'une application). Traditionnellement, les émetteurs ont utilisé le NIP, une méthode éprouvée de vérification de l'identité du client, pour confirmer la présence du titulaire de carte au moment de l'achat. Les portefeuilles mobiles ouverts peuvent être conçus de façon à utiliser des renseignements de vérification qui sont enregistrés sur l'appareil mobile, mais que l'émetteur ne détient pas ou ne connaît pas. Dans ce cas, lorsqu'un client effectue des opérations, l'émetteur dépendra du fournisseur de portefeuille pour déterminer si les renseignements de vérification présentés correspondent bien à ceux enregistrés sur l'appareil mobile. Le fait d'être incapable de vérifier l'identité du client sera problématique pour les émetteurs, puisqu'ils doivent respecter les codes de pratiques du secteur et les politiques de responsabilité zéro des réseaux de paiement.

Les émetteurs canadiens préfèrent un processus de paiement qui exige la saisie d'une information de vérification pour les opérations à valeur élevée (présentement, tout montant supérieur à 100 $), afin de pouvoir valider ces opérations et ainsi exercer un contrôle sur leur responsabilité en cas de fraude. Lorsque les opérations dépasseront le seuil de 100 $, les consommateurs devront fournir l'information de vérification afin de confirmer qu'ils sont l'auteur de la transaction. Idéalement, le processus de paiement des opérations à valeur élevée sera le même pour tous les justificatifs de paiement détenus dans un portefeuille, ainsi que pour tous les portefeuilles que le consommateur choisira d'utiliser, afin de favoriser l'adoption de ces modes de paiement par les consommateurs et d'en faciliter l'utilisation.

Sécurité équivalente à celle des paiements EMV et gestion des données dynamiques par les émetteurs

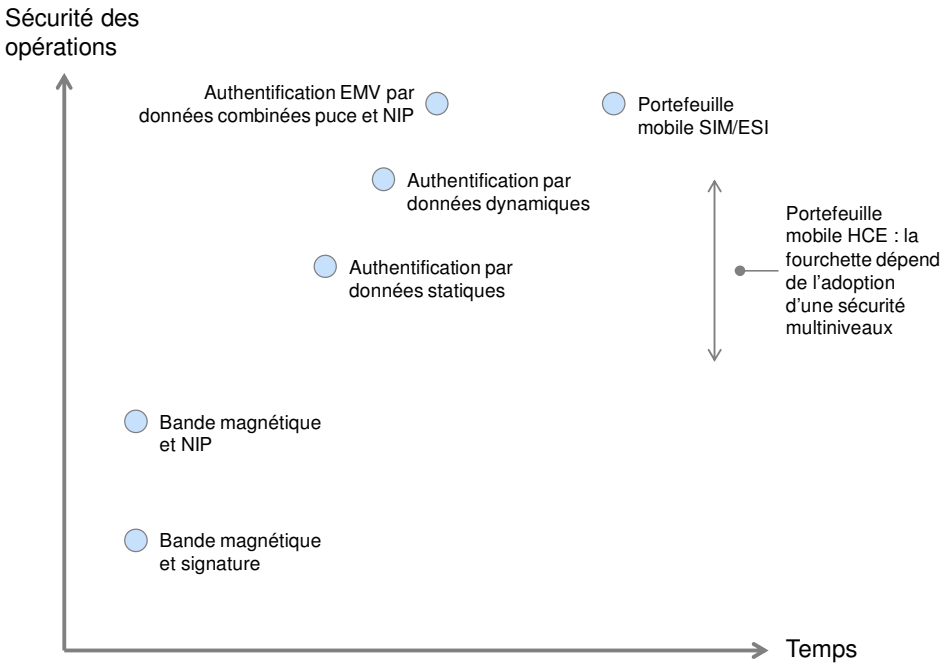
Les solutions et les services proposés par les fournisseurs de portefeuilles mobiles ouverts et les FSA devraient offrir une sécurité des paiements d'un niveau égal à celui en vigueur au Canada. En vue de préserver les investissements considérables consacrés à l'infrastructure canadienne des paiements et de maintenir le niveau de sécurité auquel les consommateurs et les commerçants se sont habitués et dont ils dépendent, les fournisseurs de portefeuilles mobiles ouverts qui veulent se lancer sur le marché canadien devront garantir une sécurité équivalente à celle offerte par la technologie reposant sur la puce EMV et l'utilisation d'un NIP.

Les solutions fondées sur l'infonuage nécessitent une gestion vigilante des données liées aux paiements stockées sur le téléphone. Afin de protéger les consommateurs et les commerçants, il est important que ces données ne soient pas utiles aux fraudeurs. On y parvient en déguisant le numéro de carte (par segmentation en unités) et en rafraîchissant régulièrement d'autres éléments de données importants (données dynamiques). Plus les données sont rafraîchies fréquemment, plus la solution sera sûre. Les données dynamiques et leur protection sont cruciales pour la sécurité des paiements. Les émetteurs aimeraient être en mesure de gérer les principales caractéristiques de leurs stratégies relatives à la segmentation en unités et aux données dynamiques, afin d'appuyer la gestion de leur responsabilité à l'égard des opérations. Il est de l'intérêt de tous les participants du secteur canadien des paiements mobiles que des normes minimales en matière de données dynamiques soient développées afin d'offrir une sécurité équivalente à celle des paiements EMV. Idéalement, les émetteurs seront en mesure de contrôler les paramètres des données dynamiques pour garantir une sécurité d'un niveau équivalant aux paiements EMV.

Annexe A – Sécurité et maturité de quelques technologies de paiement

Sécurité et maturité de quelques technologies de paiement

CONCEPTUEL



Annexe B – Nouveaux rôles destinés à soutenir les paiements mobiles NFC

Rôle	Description
Autorité de contrôle (AC)	L'AC peut gérer les principaux échanges effectués relativement à un portefeuille mobile ouvert. Il s'agit d'un modèle reconnu dans le *Modèle de référence des paiements mobiles NFC au Canada*, mais il n'est pas obligatoire. Ce modèle est considéré comme une solution de rechange aux relations « plusieurs à plusieurs » entre le gestionnaire de services de confiance (GSC) d'un émetteur de justificatifs de paiement et le GSC d'un gestionnaire de domaine sécurisé.
Exploitation de réseau mobile (ERM)	L'ERM fournit des services de connectivité associés à des appareils mobiles. Exemples : Bell Mobilité, Rogers, TELUS
Fabricant de matériel d'origine (FMO)	Le FMO fabrique les appareils mobiles utilisés par les utilisateurs finaux. Exemples : Apple, Blackberry, HTC, Samsung
Gestionnaire de domaine sécurisé (GDS)	Le GDS gère l'accès à l'élément sécurisé. Ce rôle est souvent combiné avec celui de l'ERM.
Gestionnaire de services de confiance (GSC)	Le GSC installe les justificatifs de paiement dans l'élément sécurisé. Il fournit un lien sécurisé entre plusieurs intervenants (p. ex., émetteur de justificatifs et ERM) afin de faciliter l'installation des justificatifs de paiement.
Fournisseur de portefeuille	Le fournisseur de portefeuille est chargé de l'interface destinée à l'utilisateur final.

Source : *Modèle de référence des paiements mobiles NFC au Canada*

Annexe C – Aperçu des fournisseurs de portefeuille mobile ouvert

Apple

Apple Pay

En octobre 2014, Apple a lancé Apple Pay, une solution de paiement mobile qui prend en charge les opérations au PDV et à distance. Soutenu à l'origine par une poignée de banques, Apple Pay est maintenant pris en charge par plus de 200 banques partenaires aux États-Unis (avril 2015). Avec sa part du marché des téléphones intelligents avoisinant les 40 pour cent aux États-Unis[14], Apple est en voie de transformer les modes de paiement dans ce pays.

Apple s'est associée à Visa, MasterCard, Discover et American Express pour fournir une solution de paiement clé en main. Pour pouvoir l'utiliser, les émetteurs doivent établir un processus d'identification et de vérification pour valider l'identité des titulaires de carte, et fournir une clé maîtresse d'émetteur au réseau de paiement afin de générer un NCP de jeton pour Apple Pay.

Apple a tiré profit d'un grand nombre d'apprentissages de l'industrie pour le lancement d'Apple Pay. Le téléchargement du portefeuille est simple, tout comme le chargement des justificatifs. L'expérience de paiement au PDV est rapide et fluide. Apple Pay ne nécessite aucun investissement particulier de la part des commerçants, mais ils doivent se procurer des terminaux dotés de la technologie NFC. Dans les pays comme le Canada et l'Australie où le taux d'acceptation des paiements sans contact est élevé, les détaillants peuvent déjà accepter les paiements Apple Pay sans autre démarche. Apple a introduit un processus de paiement mobile qui consiste simplement à approcher sa carte du terminal PDV. Bien que la loyauté ne soit pas encore gagnée pour Apple Pay, on peut facilement penser que ce sera chose faite dans un proche avenir.

Apple est aussi en voie de transformer les paiements en ligne et les paiements à distance. Elle a créé sa propre « marque d'acceptation », qui permet aux clients de payer leurs achats sur le site Web d'un détaillant ou à partir d'une appli en choisissant simplement « Apple Pay » et en autorisant le paiement au moyen d'une empreinte digitale. L'expérience de paiement Apple Pay convient bien aux paiements à distance, et un certain nombre de détaillants (Uber, Panera Bread, Target, Airbnb) ont déjà déployé l'acceptation des paiements Apple Pay dans leurs applis.

Au moment d'écrire ces lignes, Apple Pay n'était offert qu'aux États-Unis. Aucun lancement dans d'autres pays n'a encore été annoncé officiellement.

[14] MobiLens de comScore, mars 2015.

Google

Google Wallet

Google a lancé son portefeuille sur carte SIM en septembre 2011. En collaboration étroite avec MasterCard, la solution fonctionne à l'aide d'un justificatif de carte de crédit MasterCard virtuel chargé sur la carte SIM, qui permet à l'utilisateur d'effectuer des paiements aux PDV dotés de la technologie NFC. Le commerçant est payé par Google, puis Google porte le montant à la carte de crédit inscrite au dossier du client. Le modèle d'affaires du portefeuille Google Wallet a été malmené, car ses frais d'échange avec carte lors des opérations au PDV sont moins élevés que les frais d'échange sans carte payés à l'émetteur de carte de crédit. Tel qu'il a été créé, le modèle d'affaires posait des difficultés opérationnelles aux émetteurs et aux consommateurs relativement aux cartes de fidélité, et permettait à Google de collecter toutes les données transactionnelles. Le problème quant aux programmes de fidélisation, c'est que les émetteurs ne pouvaient déterminer où les titulaires de cartes avaient fait leurs opérations, et qu'ils ne pouvaient donc pas offrir des multiplicateurs de points (par exemple le double des points dans les épiceries). Le déploiement a été difficile pour Google, car Sprint est le seul ERM ayant accepté de prendre le portefeuille en charge (les ERM associés à Softcard, un service de portefeuille mobile sur carte SIM soutenu par AT&T, Verizon et T-Mobile, n'ont pas donné leur appui au produit).

En novembre 2013, Google a annoncé que le système d'exploitation Android 4.4 KitKat utiliserait la technologie HCE et, en mars 2014, elle a annoncé qu'elle ne prendrait plus en charge les paiements sans contact au moyen de la technologie NFC pour les systèmes d'exploitation Android antérieurs à Android 4.4 KitKat. En février 2015, Google a annoncé l'acquisition de la technologie et des brevets de Softcard pour améliorer son service de paiement. Dans le cadre de cet achat, Google a négocié des conditions qui feront en sorte que le portefeuille Google Wallet sera chargé par défaut sur les appareils Android dotés de la technologie NFC vendus par AT&T, Verizon et T-Mobile. Au début de mars 2015, Softcard a annoncé qu'elle fermerait tous les comptes au 31 mars 2015, précisant que Google ne prendrait pas en charge les solutions fondées sur les cartes SIM. Google semble privilégier la technologie HCE pour les paiements mobiles.

Au moment d'écrire ces lignes, le portefeuille Google Wallet n'était offert qu'aux États-Unis.

Android Pay

Au début de mars 2015, Google a annoncé l'arrivée d'Android Pay, une plateforme qui permettra aux développeurs d'intégrer les paiements mobiles dans leurs applications, au moyen d'une couche d'API. Les émetteurs et commerçants pourront aussi utiliser l'API pour concevoir leurs propres applications de paiement sur Android. La plateforme Android Pay prendra en charge la technologie HCE, les numéros de carte faisant l'objet de jetons et la technologie NFC. Les prochaines améliorations permettront à Android Pay d'utiliser des appareils biométriques, comme les lecteurs d'empreintes digitales.

On ne sait pas quand Android Pay sera offert au public; des renseignements sur un lancement possible en 2015 sont attendus prochainement.

Google a indiqué que Visa, MasterCard et American Express soutiendront Android Pay lorsque cette plateforme sera lancée. Des services d'authentification par jeton pourraient être fournis par les réseaux de paiement, comme c'est le cas pour Apple Pay. Le cas échéant, Android Pay sera en mesure de fournir une solution de bout en bout à l'intention des créateurs de portefeuille, qui n'exigera que la création de l'interface utilisateur. Les émetteurs devront travailler avec les FSA des réseaux de paiement pour assurer la prise en charge d'Android Pay.

PayPal

PayPal est un joueur important du commerce en ligne, et il est toujours au cœur de la majorité des opérations[15]. PayPal a fait l'essai des paiements physiques aux PDV pendant quelques années, et a annoncé le lancement de son portefeuille numérique en septembre 2013. L'appli de portefeuille PayPal permet aux consommateurs d'enregistrer leurs cartes de crédit, de payer leurs achats dans les commerces physiques qui acceptent PayPal, de passer leur commande à l'avance dans certains restaurants, d'envoyer ou de recevoir des fonds, et de trouver les promotions en vigueur à proximité. En 2014, tout près de 20 pour cent des ventes totales de 226 milliards de dollars de PayPal avaient été réalisées au moyen d'appareils mobiles – un petit pourcentage était des opérations physiques aux PDV.

En mars 2015, PayPal a annoncé l'achat de Paydiant, une société qui produit une technologie de portefeuille mobile qu'exploitent les commerçants et les émetteurs dans leurs applis de paiement. Paydiant est une solution logicielle qui génère un code QR soit sur un terminal PDV, soit sur un reçu. Le client prend une photo du code QR et peut sélectionner le mode de paiement qu'il préfère pour payer son achat, à partir des justificatifs enregistrés dans son portefeuille. Les justificatifs sont stockés en toute sécurité dans le nuage et ne sont jamais transmis au commerçant. Les justificatifs sont envoyés de façon sécurisée à l'acquéreur, qui traite l'opération de la manière habituelle. Paydiant est le fournisseur de portefeuille qu'a choisi MCX, un regroupement de commerçants américains qui ont uni leurs forces pour mettre au point un portefeuille mobile ouvert qui offre un choix supplémentaire aux commerçants, en plus des paiements par cartes de crédit et de débit.

[15] www.paypal-media.com; données sur le quatrième trimestre de 2014

Samsung

Samsung Pay

Au début de mars 2015, Samsung a annoncé qu'il prévoyait le lancement de Samsung Pay au cours de l'été, aux États-Unis et en Corée. Samsung Pay propose deux solutions : selon le modèle d'appareil et le pays, les justificatifs seront stockés de façon matérielle dans un élément sécurisé intégré, ou de façon virtuelle dans le nuage. En Amérique du Nord, les appareils Samsung ont toujours été livrés sans élément sécurisé intégré – et il est possible que cela continue. Dans un cas comme dans l'autre, des données dynamiques seront générées dans le nuage.

Comme Apple Pay, Samsung Pay met à profit la segmentation en unités, c'est-à-dire que les numéros de carte de crédit seront marqués et remplacés par un jeton propre à l'appareil. Cette solution s'appuiera sur la technologie HCE. Les services d'authentification par jeton seront vraisemblablement fournis par les réseaux de paiement, comme dans le cas d'Apple Pay.

En plus de la technologie NFC, Samsung Pay prendra en charge, aux États-Unis seulement, les opérations effectuées par lecture d'une bande magnétique, au moyen d'une technologie exclusive appelée Magnetic Secure Transmission (MST), que Samsung a obtenue lors de l'acquisition de LoopPay en février 2015. Cette technologie permet au client d'effectuer des paiements sans contact au moyen des terminaux PDV à bande magnétique traditionnels qui ne sont pas dotés de la technologie NFC. En théorie, environ 90 pour cent des commerçants aux États-Unis auront la possibilité d'accepter immédiatement les paiements sans contact par Samsung Pay, grâce à la technologie MST[16].

Rogers

Portefeuille mobiXpress

Rogers a lancé son portefeuille mobiXpress en avril 2014 – une solution sur carte SIM offerte uniquement aux clients de Rogers. Le portefeuille mobiXpress prend en charge la carte MasterCard prépayée de Rogers, que les clients peuvent charger quand ils le désirent. La carte doit être chargée avant l'utilisation, car les opérations ne sont pas « redirigées » vers une autre carte inscrite. Rogers applique les frais suivants pour l'utilisation de cette carte : des frais d'approvisionnement de 2 $ pour l'ajout d'un montant à la carte, et des frais de maintenance mensuels de 2,50 $. Les utilisateurs du portefeuille mobiXpress peuvent acheter et charger des cartes-cadeaux de certains commerçants, dont Swiss Chalet, Indigo et Harvey's.

Au moment d'écrire ces lignes, le portefeuille mobiXpress n'était offert qu'au Canada.

---

[16] Communiqué de presse sur Samsung et LoopPay, businesswire.com, le 18 février 2015.

TD Canada Trust/Services financiers le Choix du Président

UGO

Le portefeuille UGO a été annoncé en novembre 2013 et lancé en novembre 2014, à titre de premier portefeuille mobile ouvert au Canada combinant de multiples modes de paiement et programmes de fidélisation. Coentreprise réunissant TD Canada Trust et les Services financiers le Choix du Président, UGO permet aux clients de ces deux banques de charger des cartes de crédit afin d'effectuer des paiements mobiles. Le portefeuille UGO prend en charge de multiples programmes de fidélisation, dont le programme PC Plus. Les membres du programme PC Plus gagnent des points PC automatiquement lorsqu'ils font des achats admissibles dans les épiceries participantes au moyen de leurs justificatifs de paiement TD Visa ou MasterCard Services financiers le Choix du Président.

UGO est une solution sur carte SIM qui est prise en charge par les trois principaux ERM canadiens, soit Bell, Rogers et TELUS. Les appareils dotés de la technologie NFC qui utilisent Android KitKat 4.4 ou une version ultérieure de même que les appareils Blackberry 10 sont pris en charge. Une version du portefeuille UGO est également offerte pour les iPhone, mais ne prend en charge que les cartes de fidélité (et non les cartes de paiement).

Comme pour les autres portefeuilles canadiens, seules les opérations de moins de 100 $ sont actuellement permises aux PDV. On ne sait pas quand UGO permettra les opérations de valeur élevée et quelles méthodes de vérification des clients seront utilisées. Les opérations à distance ne sont pas encore prises en charge, ce qui limite l'adoption par les consommateurs.

Au moment d'écrire ces lignes, le portefeuille UGO n'était offert qu'au Canada.

Annexe D – Norme EMVCo sur la segmentation en unités

La norme EMVCo a été publiée en mars 2014. Dans sa version actuelle, elle fournit des indications minimales concernant l'établissement et la maintenance des API des demandeurs de jetons d'authentification, des chambres fortes pour les jetons, des plateformes d'approvisionnement de jetons, des registres de jetons, etc. Le FSA est une entité centrale. Les chambres fortes pour les jetons servent à conserver à la fois les NCP et les NCP de jetons, et seront une cible de choix pour les fraudeurs. Les restrictions de domaine pour les jetons devraient contribuer grandement à éviter la fraude entre les canaux, et des exigences claires devront être établies pour déterminer comment les attributs des jetons seront utilisés dans les décisions d'autorisation.

Le tableau suivant décrit les éléments préoccupants de la norme EMVCo sur la segmentation en unités.

Domaine de préoccupation	Explication
Sécurité et contrôles	La norme indique que les chambres fortes pour les jetons (*token vaults*) doivent être protégées au moyen de mesures de sécurité physiques et logiques robustes conformes aux normes de l'industrie, mais ne fournit aucune exigence en ce qui a trait au stockage des données elles-mêmes (stockage du NCP et du jeton dans des emplacements différents, etc.) ou à d'autres parties du service d'authentification où des données sont stockées. Compte tenu de l'importance des jetons d'authentification dans les paiements basés sur la technologie HCE, on pourrait s'attendre à des normes minimales concernant la sécurité et le stockage des données. Cela est particulièrement important dans les modèles de portefeuille mobile ouvert où les émetteurs sont responsables, mais dépendent du FSA pour la protection des données sensibles.
Inscription des demandeurs et niveau d'assurance des jetons	La norme indique que chaque FSA détermine quels sont les renseignements qu'il doit recueillir auprès d'un demandeur de jeton, y compris les contrôles KYC (*Know Your Customer)* et les contrôles des opérations (c'est-à-dire les restrictions de domaine). Aucun champ obligatoire n'est défini. Le FSA doit établir le niveau d'assurance des jetons pour chaque demandeur, mais il n'y a aucune ligne directrice quant à la façon d'évaluer le demandeur et d'attribuer la valeur d'assurance (aucune assurance – 0 à assurance élevée – 99). Les demandeurs de jetons peuvent être des commerçants détenant des numéros de carte en dossier, des acquéreurs, des commerçants, des FMO, des fournisseurs de portefeuille

Domaine de préoccupation	Explication
	numérique et des émetteurs de carte.
Identification et vérification	La norme n'indique pas clairement qui doit effectuer l'identification et la vérification, ni les éléments qui doivent être saisis à cette fin pour établir le niveau d'assurance des jetons. Des exemples d'activités d'identification et de vérification sont fournis, mais sont peu utiles. La norme n'indique pas clairement ce qui est validé afin d'établir le niveau d'assurance : le demandeur de jeton, le justificatif ou le détenteur du justificatif. La norme indique que l'identification et la vérification de l'émetteur doivent se faire en fonction des valeurs d'assurance des jetons contenues dans le jeton de paiement pour la combinaison NCP-détenteur, mais ne fournit pas d'exigence concernant l'établissement de la valeur d'assurance du jeton. Elle n'indique pas non plus quelle entité devrait être responsable de déterminer le niveau d'identification et de vérification à effectuer. En tant que détenteur de la relation client et de la responsabilité associée au compte, il est proposé que le détenteur du justificatif détermine le degré de rigueur à appliquer aux processus d'identification et de vérification pour les différents types de demandeurs de jetons.
Génération d'un jeton de paiement	La norme ne fournit aucune indication quant à la façon de générer un jeton, hormis une exigence visant la date d'expiration du jeton. On ne sait pas quelle partie établit les paramètres d'émission des jetons. On ne sait pas non plus comment la génération des jetons intégrera les restrictions de domaine relatives au canal, au commerçant, au portefeuille, etc., ainsi que toute exigence relative à un cryptogramme. La norme indique que les fonctions opérationnelles doivent être intégrées au réseau de paiement pertinent, mais ne dirige pas le fournisseur de jetons vers des spécifications d'un réseau de paiement relativement à l'authentification par jeton.
Émission et approvisionnement des jetons de paiement	La norme indique que l'approvisionnement des jetons s'effectue au moyen d'une interface entre le demandeur de jeton et le FSA. Selon la norme EMVCo, « les méthodologies associées à l'approvisionnement peuvent être propres à chaque fournisseur de service d'authentification par jeton, et ne font pas partie du champ d'application de la présente norme ». Des exigences devraient être fournies afin de préciser les protocoles de sécurité entourant la transmission des jetons de paiement entre le FSA et le demandeur de jeton.

Bibliographie

Rapports et livres blancs

Association des banquiers canadiens[17], *Paiements mobiles NFC au Canada – modèle de référence*, mai 2012.

Banque centrale européenne, *Recommendations for the security of mobile payments* (en anglais seulement), novembre 2013.

Consult Hyperion, *HCE And SIM Secure Element: It's Not Black And White* (en anglais seulement), juin 2014.

Consult Hyperion et GSMA, *HCE and Tokenization for Payment Services* (en anglais seulement), octobre 2014.

European Payments Council, *Mobile Payments Initiatives* (en anglais seulement), décembre 2014.

European Payments Council, *Mobile Wallet Payments* (en anglais seulement), janvier 2014.

First Data, *EMV and Encryption + Tokenization: A Layered Approach to Security* (en anglais seulement), 2012.

Sequent, *Beyond Tokenization: Ensuring secure mobile payments using dynamic issuance with on-device security and management* (en anglais seulement), consulté en avril 2015.

Smart Card Alliance, *Card-Not-Present Fraud: A Primer on Trends and Authentication Processes* (en anglais seulement), février 2014.

Smart Card Alliance, *Host Card Emulation (HCE) 101* (en anglais seulement), août 2014.

Smart Card Alliance, *Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization* (en anglais seulement), octobre 2014.

TSYS, *Tokenization: FAQS & General Information* (en anglais seulement), 2014.

Norme

EMVCo, *EMV Payment Tokenisation Specification Technical Framework* (en anglais seulement), mars 2014.

---

[17] L'Association a publié le Modèle de référence au nom des institutions financières canadiennes

Glossaire

Terme	Définition
Acquéreur	Institution qui traite les paiements par carte de débit ou de crédit au nom d'un commerçant.
Appareil mobile	Appareil informatique portable qui est doté d'un système d'exploitation, qui peut exécuter des applications et qui peut se connecter à des réseaux de communication (données cellulaires, Wi-Fi, Bluetooth, NFC, etc.).
Application de paiement mobile	Voir *Portefeuille.*
Authentification combinée des données	Technique d'authentification utilisée dans les opérations par carte à puce hors ligne, qui calcule pour chaque opération un cryptogramme propre à la carte et à l'opération. La carte à puce doit pouvoir effectuer un traitement cryptographique basé sur le système RSA. Au cours de l'opération de paiement, la carte à puce génère une deuxième signature dynamique, que le terminal doit vérifier au moyen de la cryptographie RSA. Cela confirme que la carte à puce qui a été authentifiée par DDA est la même carte qui a été utilisée pour autoriser l'opération.
Authentification dynamique des données (DDA)	Technique d'authentification utilisée dans les opérations par carte à puce hors ligne, qui calcule pour chaque opération un cryptogramme propre à la carte et à l'opération. L'authentification DDA offre une protection contre le clonage et la contrefaçon des cartes.
Authentification statique des données (SDA)	Technique d'authentification utilisée dans les opérations par carte à puce hors ligne, qui calcule un cryptogramme à partir d'un certificat de clé publique statique et d'éléments de données statiques. Les données utilisées dans l'authentification SDA sont statiques – les mêmes données sont utilisées au début de chaque opération.
Bluetooth Low Energy (BLE)	Technologie de réseau personnel sans fil conçue pour réduire la consommation d'énergie et les coûts. Le système Beacon de PayPal s'appuie sur cette technologie.
Boutique d'applis	Fournisseur d'applications pour les appareils mobiles. Les boutiques d'applis sont généralement rattachées à un système d'exploitation (par exemple Apple Store et Google Play Store).
Carte SIM (module d'identité d'abonné)	Matériel appartenant à l'ERM et qui est installé dans un téléphone. Les justificatifs de l'émetteur peuvent y être stockés de façon sécurisée. Aussi appelée carte universelle à circuits intégrés (UICC, ou *Universal Integrated Circuit Card*).
Carte universelle à	Matériel appartenant à l'ERM et qui est installé dans l'appareil

Terme	Définition
circuits intégrés (UICC)	mobile. Les justificatifs de l'émetteur peuvent y être stockés de façon sécurisée. Aussi appelé carte SIM.
Chambre forte pour les jetons	Dépôt, mis en place par un système d'authentification par jeton, qui maintient la mise en correspondance établie entre le jeton de paiement et le NCP. Ce dépôt est appelé chambre forte pour les jetons. Il peut aussi conserver d'autres attributs du demandeur de jeton déterminés au moment de l'inscription et que le FSA peut utiliser pour appliquer des restrictions de domaine ou d'autres contrôles durant le traitement des opérations.
Code QR (*Quick Response*)	Type de code à barres matriciel (étiquette à lecture optique) qui contient des données concernant l'article sur lequel il est apposé. Le système de code QR est devenu populaire du fait qu'il se lit rapidement et que sa capacité de stockage est supérieure à celle des codes à barres CUP.
Communication en champ proche (NFC)	Technologie de communication sans fil à courte portée pour les téléphones intelligents et appareils similaires, qui permet le transfert de données entre les appareils. La technologie NFC fonctionne à 13,56 MHz dans un rayon de 10 cm et est conforme aux normes ISO/IEC 14443 et ISO/IEC 18092.
Contrôleur NFC	Matériel frontal sans contact conçu pour capter les données échangées entre le lecteur NFC et l'application cible, de la couche radio à la couche applicative.
Cryptogramme	Valeur alphanumérique issue des éléments de données saisis dans un algorithme et chiffrés, qui est largement utilisée pour valider l'intégrité des données. Les cryptogrammes courants sont les cryptogrammes de requête d'autorisation (ARQC, pour *Authorization Request Cryptogram*), les cryptogrammes de réponse d'autorisation (ARPC, pour *Authorization Response Cryptogram*), les certificats d'opération (TC, pour *Transaction Certificate*) et les cryptogrammes d'application de l'authentification (AAC, pour *Application Authentication Cryptogram*).
Cryptographie en boîte blanche	Méthode d'obscurcissement du code qui permet de cacher des clés et des processus cryptographiques. L'objectif est de protéger les clés secrètes dans une implémentation logicielle.
Données dynamiques (jeton)	Justificatifs de paiement à utilisation limitée qui sont fournis à une application pour la prise en charge d'une opération.
Élément sécurisé	Plateforme inviolable (généralement un microcontrôleur sécurisé contenu dans une puce) pouvant accueillir de façon sécurisée des applications et leurs données confidentielles et cryptographiques (par exemple les données sur les clés) conformément aux règles et exigences de sécurité établies par

Terme	Définition
	un ensemble d'autorités fiables bien identifiées (Global Platform).
Élément sécurisé intégré (ESI)	Microcontrôleur sécurisé inviolable qui est intégré dans une seule puce d'un appareil mobile. Plusieurs téléphones intelligents, comme le iPhone 6 et certains modèles du S6 de Samsung sont livrés avec des éléments sécurisés intégrés.
Émetteur de justificatif	Organisation qui émet un justificatif.
Émulation de carte (HCE)	Architecture logicielle qui fournit une représentation virtuelle exacte des cartes d'identité électroniques (y compris les cartes de crédit et de débit) en n'utilisant que des fonctions logicielles. La technologie HCE permet aux applications mobiles d'offrir des solutions de paiement NFC en l'absence d'un élément sécurisé dans le téléphone (ESI ou carte SIM).
EMVco	Société qui établit des normes d'interopérabilité des cartes à circuit intégré, des terminaux PDV et des guichets automatiques pour l'authentification des opérations par cartes de crédit et de débit. Les membres actuels d'EMVCo sont MasterCard, Visa, JCB, American Express, China UnionPay et Discover, qui détiennent tous une participation de valeur égale dans la société.
Environnement d'exécution fiable (TEE)	Zone sécurisée du processeur principal d'un téléphone intelligent (ou de tout appareil connecté, y compris les tablettes, les décodeurs et les téléviseurs). Elle garantit la protection du code et des données chargés dans l'appareil afin de préserver leur confidentialité et leur intégrité.
Exploitant de réseau mobile (ERM)	Fournisseur de services de communications sans fil qui détient ou contrôle tous les éléments nécessaires pour vendre et fournir des services à un utilisateur, y compris un spectre de fréquences, une infrastructure de réseau sans fil, une infrastructure de liaison descendante, un système de facturation, un soutien à la clientèle, des systèmes informatiques d'approvisionnement et des structures de marketing et de réparation. Aussi appelé fournisseur de service sans fil, fournisseur de réseau sans fil, société de téléphonie cellulaire ou opérateur de réseau mobile.
Fabricant de matériel d'origine (FMO)	Entité qui acquiert et assemble des composants pour en faire un nouveau produit, vendu sous une nouvelle marque.
Fournisseur de chambre forte pour les jetons	Entité qui établit et assure le maintien d'une chambre forte pour les jetons.
Fournisseur de portefeuille	Entité qui conçoit, crée et gère l'application de portefeuille mobile, c'est-à-dire l'interface utilisateur.

Terme	Définition
Fournisseur de service d'authentification (FSA)	Entité qui fournit un service d'authentification comprenant la chambre forte pour les jetons et le traitement correspondant. Le fournisseur de service d'authentification aura la possibilité de mettre de côté des numéros d'identification bancaire (NIB) certifiés ISO en tant que NIB de jeton, afin d'émettre des jetons de paiement pour les NCP soumis conformément à cette norme.
Gestionnaire de service de confiance (GSC)	Rôle au sein d'un écosystème de paiement mobile fondé sur le matériel. Le GSC agit comme un courtier neutre qui établit des ententes commerciales et des connexions techniques avec les exploitants de réseaux mobiles et les autres entités qui contrôlent l'élément sécurisé à l'intérieur des téléphones mobiles. Le GSC permet aux fournisseurs de service de distribuer et de gérer à distance les applications sans contact et les justificatifs en assurant l'accès à l'élément sécurisé des appareils dotés de la technologie NFC.
Identifiant d'équipement mobile (MEID)	Numéro unique à l'échelle mondiale qui identifie un élément d'équipement de station mobile CDMA. Il s'agit d'un IMEI en chiffres hexadécimaux.
Identificateur unique (UDID)	Code alphanumérique unique associé à un appareil iOS. Tous les iPhone, iPad et iPod Touch en ont un.
Identification et vérification	Méthode valide qui permet à une entité de valider le titulaire de carte et son compte afin de fournir des justificatifs de paiement.
Identité internationale d'équipement mobile (IMEI)	Code à 15 ou 17 chiffres qui identifie chaque téléphone mobile de manière unique. Le code IMEI peut permettre à un réseau GSM (système global de télécommunications mobiles) ou UMTS (système universel de télécommunications mobiles) de bloquer un téléphone perdu ou volé afin qu'on ne puisse l'utiliser pour faire des appels.
Jeton (dynamique)	Justificatifs de paiement à utilisation limitée qui sont fournis à une application pour la prise en charge d'une opération. Le jeton est *dynamique* si la valeur de remplacement est différente à chaque utilisation, et peut comprendre des données propres à l'opération, comme le montant et l'heure.
Jeton (statique)	Justificatifs de paiement à utilisation limitée qui sont fournis à une application pour la prise en charge d'une opération. Le jeton est *statique* si la valeur de remplacement demeure la même à chaque utilisation.
Justificatif	Information sécurisée et chiffrée associée à une seule carte de

Terme	Définition
	paiement, carte de fidélité, carte émise par le gouvernement, etc.
Justificatif de paiement	Voir *Justificatif.*
Liaison en direct	Mode de transmission de données à l'aide d'un réseau sans fil.
Méthode de vérification de carte (MVC)	Méthode de vérification du titulaire d'une carte utilisée pour assurer que la personne utilisant le justificatif est bel et bien celle qui détient ce justificatif.
Mot de passe	Numéro à quatre chiffres entré dans un appareil mobile et qui sert de méthode de vérification de carte (MVC).
Numéro d'identification de l'émetteur	Six premiers chiffres du numéro de compte primaire (NCP).
Numéro d'identification personnel (NIP)	Code numérique secret comptant de 4 à 6 caractères, utilisé pour l'identification des titulaires de carte, qui l'entrent eux-mêmes au moyen d'un clavier. Les NIP peuvent être vérifiés en ligne par l'émetteur, ou envoyés à la carte à puce pour être vérifiés hors ligne.
Numéro de compte primaire (NCP)	Numéro à 16 chiffres qui désigne un justificatif de paiement. Les six premiers chiffres sont le numéro d'identification de l'émetteur.
Obscurcissement du code	Technique utilisée pour empêcher la rétroconception d'un algorithme cryptographique. Une technique de ce type est la *cryptographie en boîte blanche* (voir ci-dessous).
Opération de valeur élevée (OVE)	Opération de paiement qui excède le plafond recommandé du réseau pour les opérations sans MVC. Au moment d'écrire ces lignes, ce plafond est fixé à 100 $ au Canada.
PDV	Point de vente
Portefeuille	Le portefeuille mobile désigne l'application destinée à l'utilisateur final, c'est-à-dire celle qui doit être installée sur l'appareil mobile. L'application permet à l'utilisateur de saisir et de gérer des renseignements précis liés à son compte, qui seront utilisés dans le cadre d'une transaction mobile NFC. Un appareil mobile peut contenir un ou plusieurs portefeuilles mobiles à la fois, en tout temps.
Portefeuille exclusif	Application de paiement mobile qui accepte les justificatifs d'un seul émetteur. Le fournisseur du portefeuille est l'émetteur lui-même.
Portefeuille mobile	Voir *Portefeuille.*
Portefeuille mobile ouvert	Application de paiement mobile qui accepte les justificatifs de plus d'un émetteur.

Terme	Définition
Réseau de paiement	Système qui fournit des spécifications pour la prise en charge des paiements mobiles et qui gère le réseau utilisé pour traiter les opérations de paiement (American Express, Interac, MasterCard, Visa, etc.).
Segmentation en unités	Remplacement du numéro de compte primaire (NCP) par une valeur appelée jeton de paiement. La segmentation en unités peut être appliquée pour accroître l'efficience des opérations, améliorer la sécurité des opérations, accroître la transparence du service ou pour fournir une méthode de mise en œuvre pour les tiers.
Service d'authentification par jeton	Système réunissant les fonctions clés qui facilitent la génération et l'émission de jetons de paiement à partir des numéros d'identification bancaires (NIB) des jetons, et qui maintient la correspondance établie entre les jetons de paiement et les NCP lorsque le demandeur de jeton fait une demande. Le service permet aussi le traitement des jetons d'opérations de paiement afin de retirer le jeton d'authentification pour dégager le NCP.
SIM	*Subscriber Identity Module* (Module d'identité de l'abonné)
Terminal point de vente (PDV)	Matériel mis en place par un commerçant et qui sert à saisir les justificatifs de traitement d'une opération.