Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles

Carlisle Adams[1]

Juin 2013

Avis de non-responsabilité: Les opinions exprimées dans ce rapport sont celles de l'auteur. Elles ne reflètent pas nécessairement celles du Commissariat à la protection de la vie privée du Canada.

[1] Carlisle Adams est professeur à l'École de science informatique et de génie électrique de l'Université d'Ottawa. En congé sabbatique au Commissariat à la protection de la vie privée, il a élaboré le présent rapport dans son intégralité de janvier à juin 2013. L'auteur tient à souligner que ses discussions avec plusieurs employés du Commissariat, leurs suggestions et leurs précieux commentaires lui ont permis de grandement améliorer la qualité de son rapport. Il assume toutefois l'entière responsabilité des recommandations et des opinions qui y sont formulées (et des erreurs qui pourraient s'y trouver).

Résumé

Le monde des paiements mobiles approche à grands pas. Dans certains environnements et cas d'utilisation, il est déjà une réalité. Le présent rapport a pour ambition de faire un examen ciblé de la technologie des paiements mobiles sous l'angle de la sécurité et de la protection de la vie privée. Nous nous pencherons au premier chef sur les risques d'atteinte à la sécurité et à la vie privée et nous explorerons des moyens de les atténuer dans la mesure du possible.

Le rapport est divisé en trois parties : contexte, analyse et recommandations. La partie 1 examine les raisons d'être des paiements mobiles, décrit certains modes de paiement importants proposés, présente les principaux acteurs de l'écosystème des paiements mobiles et décrit – de façon globale – le mouvement de l'argent dans certains modes de paiement.

La partie 2 porte sur les risques d'atteinte à la sécurité et à la vie privée inhérents à certains modes de paiement. Nous y analysons certains modes de paiement en nous attardant particulièrement au paiement mobile au point de vente effectué au moyen de la communication en champ proche (NFC) et nous explorons brièvement le commerce mobile (mCommerce) actuel (en tant qu'étape de transition vers les paiements mobiles véritables) et certaines sous-catégories des paiements mobiles de personne à personne (mP2P) et d'acceptation mobile (mAccept).

Dans la partie 3, nous examinons des façons d'atténuer les risques d'atteinte à la sécurité et à la vie privée inhérents aux divers modes de paiement analysés dans la partie précédente. Nous y présentons des recommandations émanant d'autres sources qui s'appliquent aux appareils et aux paiements mobiles, et formulons nos propres recommandations découlant de l'analyse des modes de paiement de la partie précédente. Nous formulons aussi des recommandations qui s'appliquent généralement à tous les modes de paiement électronique, classées en fonction des groupes auxquels elles s'adressent : fabricants d'appareils et de systèmes d'exploitation; exploitants de réseau mobile; développeurs de portefeuille électronique ou d'applications; organismes de normalisation; commerçants; et utilisateurs finals.

Sommaire

Le présent rapport examine le paysage des paiements mobiles sous l'angle de la sécurité et de la protection de la vie privée. Dans la partie 1, qui prépare le terrain pour les deux parties suivantes, nous nous sommes efforcés de donner une vue d'ensemble. Nous avons exploré brièvement l'historique des paiements mobiles et les raisons de l'adoption de cette technologie. Nous distinguons aussi quatre types de paiements mobiles, soit le commerce mobile (mCommerce), le paiement mobile au point de vente (mPOS), le paiement mobile de personne à personne (mP2P) et l'acceptation mobile (mAccept). Nous y présentons dix groupes d'acteurs de l'écosystème des paiements mobiles : les banques ou autres institutions financières; les marques de paiement; les fournisseurs de portefeuille électronique; les utilisateurs finals; les fabricants d'appareils mobiles; les fabricants de terminaux de point de vente; les gestionnaires de services de confiance; les exploitants de réseau mobile; les commerçants; et les exploitants de réseau de paiement. Enfin, pour rendre certains concepts un peu plus concrets, nous décrivons le mouvement de l'argent dans certains modes de paiement particuliers.

Dans la partie 2 du rapport, nous présentons une analyse technique de quelques modes de paiement mobile. Nous examinons différents modes et technologies de paiement mobile : les opérations bancaires ou achats en ligne effectués au moyen d'un navigateur mobile, la facturation par l'entreprise de télécommunications mobiles, la communication en champ proche (NFC), M-Pesa (transfert de fonds utilisant la messagerie texte), Cybermonnaie et Square. Cette partie du rapport se penche aussi sur les préoccupations et les risques associés aux paiements électroniques en général (c.-à-d. les préoccupations qui s'appliquent à tous les modes de paiement mobile ou à un grand nombre d'entre eux). Nous abordons les préoccupations relatives à la sécurité et à la protection de la vie privée à la fois selon des technologies précises et les opérations électroniques en général. Par exemple, pour la technologie NFC, nous analysons la possibilité de bornes de lecture corrompues ou malveillantes (subtilisation), de fraudeurs sur le canal NFC (interception illicite ou attaque par relais) et d'appareils mobiles corrompus (attaque de matériel, de logiciels et de configuration). Certaines préoccupations communes à l'ensemble ou à un grand nombre de modes et de technologies de paiement peuvent être regroupées selon les principes relatifs à l'équité dans le traitement des renseignements :

- Mesures de sécurité
    - Mise en œuvre insuffisante des mécanismes de sécurité (possibilité que les entreprises ne mettent pas toutes en œuvre les mécanismes de sécurité offerts)
    - Employés malveillants au sein d'une entreprise d'applications de paiement (nécessité de contrôles d'audit, de journaux et d'autres mécanismes technologiques ou de procédures pour contrôler l'accès des employés aux renseignements pouvant être associés à des clients)
    - Données récupérables après une perte ou un vol (existence d'attaques permettant de contourner le chiffrement et inefficacité de certains mécanismes d'effacement à distance)
    - Catastrophes naturelles ou d'origine humaine (risque d'absence de stockage non électronique ou de remplacement pour sauvegarde si un événement désactive la mémoire électronique)
- Consentement
    - Écrans de petite taille (difficulté de présenter les politiques aux utilisateurs et d'obtenir un consentement valable)

- Exactitude
    - Protocoles de paiement exclusifs (risque que ces protocoles ne soient pas toujours conçus ou vérifiés par des spécialistes de la sécurité et de la protection de la vie privée)
    - Mise en œuvre boguée (risque d'erreurs dans les opérations ou dans les données stockées)
- Accès aux renseignements personnels
    - Catastrophes naturelles ou d'origine humaine (risque que les utilisateurs ne puissent avoir accès à leurs données, à leurs comptes, à leurs fonds et à l'historique de leurs opérations après une catastrophe)

La partie 3 du rapport renferme des recommandations découlant de l'analyse présentée dans la partie 2. Ces recommandations sont présentées en trois sections :

- Recommandations pertinentes provenant d'autres sources (notamment la Federal Trade Commission et l'industrie des cartes de paiement)
- Recommandations concernant des technologies de paiement en particulier (p. ex. NFC)
- Recommandations s'appliquant à l'ensemble ou à un grand nombre de modes de paiement électroniques. Ces recommandations sont classées en fonction des groupes auxquels elles s'adressent :
    - Fabricants d'appareils ou de systèmes d'exploitation
    - Exploitants de réseau mobile
    - Développeurs de portefeuille électronique ou d'applications de paiement
    - Organismes de normalisation
    - Commerçants
    - Utilisateurs finals

Nous espérons que le présent rapport sera utile au Commissariat à la protection de la vie privée du Canada et à tous ceux qui le liront. Notre ambition est de mieux faire connaître et comprendre un large éventail de préoccupations dans l'écosystème des paiements mobiles afin que tous ceux qui participent à la création et à l'utilisation de ces technologies puissent y répondre au fil du temps. Le but ultime consiste à faire en sorte que tous les systèmes de paiement soient aussi sécurisés que possible et qu'il respecte la vie privée. Il est à espérer que le présent rapport aidera à apporter des progrès concrets dans cette voie.

Les recommandations formulées reflètent le point de vue de l'auteur, l'objectif étant de contribuer à la recherche sur la sécurité et la protection de la vie privée menée par le Commissariat à la protection de la vie privée du Canada et d'autres parties intéressées. En ce sens, elles devraient être considérées comme une information que le Commissariat et d'autres parties peuvent prendre en compte au moment de formuler leurs propres politiques et lignes directrices dans le domaine des paiements mobiles.

Table des matières

Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles

Partie 1 – Contexte

Sommaire

La partie 1 du présent rapport examine le contexte des paiements mobiles, notamment les divers modes de paiement, les acteurs en présence et le mouvement de l'argent dans certaines opérations de paiement. Le rapport dans son ensemble s'intéresse avant tout aux paiements mobiles à un terminal de point de vente au moyen d'appareils permettant la communication en champ proche (NFC), mais il examine aussi brièvement d'autres modes et technologies de paiement.

1. Introduction

Le monde des paiements mobiles approche à grands pas. Dans certains environnements et cas d'utilisation, il est déjà une réalité. Le présent rapport a pour ambition de faire un examen ciblé de la technologie des paiements mobiles sous l'angle de la sécurité et de la vie privée. Il n'a pas pour objet explicite de décortiquer les aspects juridiques ou commerciaux, la politique, la convivialité ou la gouvernance, voire la faisabilité technologique, même si certains de ces éléments ressortiront inévitablement de l'analyse globale. Nous nous pencherons au premier chef sur les risques d'atteinte à la sécurité et à la vie privée et nous explorerons des moyens de les atténuer dans la mesure du possible.

Le rapport est divisé en trois parties : contexte, analyse et recommandations. La partie 1 examine les raisons d'être des paiements mobiles, décrit certains modes de paiement importants proposés, présente les principaux acteurs de l'écosystème des paiements mobiles et décrit – de façon globale – le mouvement de l'argent dans certains modes. Nous nous attachons au début et à la fin d'une opération et à ce qui se produit entre les deux en illustrant le mouvement de l'argent au moyen d'exemples concrets de cas d'utilisation.

D'entrée de jeu, soulignons qu'il est essentiel de limiter la portée de notre étude, car le sujet des « paiements mobiles » est vaste et complexe. Pour notre propos, un paiement mobile est une opération monétaire effectuée au moyen d'un appareil mobile (généralement un téléphone intelligent) où un utilisateur individuel est l'initiateur ou le point de terminaison (ou les deux) du transfert de fonds. Par conséquent, les opérations entre entreprises (B2B), entreprises-gouvernement (B2G) et entre gouvernements (G2G, par exemple les paiements de transfert fédéraux-provinciaux) sont exclus de la portée du présent rapport. De plus, l'appareil mobile est un élément essentiel pour amorcer, clore ou faciliter le paiement. Par conséquent, la simple utilisation d'un navigateur sur un appareil mobile pour effectuer une opération bancaire (payer des factures ou transférer des fonds d'un compte à un autre) ou faire des achats en ligne n'est pas considérée comme un paiement mobile (car on peut exécuter ces opérations de manière identique en utilisant le navigateur d'un PC). Nous excluons donc ces opérations de notre étude, même s'il s'agit d'une importante étape de transition vers les paiements mobiles et nous n'en faisons état brièvement que dans cette optique.

2. Historique et raison d'être

D'après le Groupe de travail sur l'examen du système de paiement[2], les Canadiens produisent ou utilisent plus d'un milliard de chèques par an, dont environ 60 % sont émis par les grandes sociétés, les petites et moyennes entreprises (PME) et les administrations publiques et 40 % par les particuliers. Le coût estimatif par chèque (si l'on prend en compte la facturation, les comptes clients, les comptes fournisseurs, le traitement des chèques, les frais d'affranchissement et les coûts liés à la succursale ou aux caissiers) se situe entre 1 et 30 $ selon le secteur d'activité[3].

À terme, le coût associé aux chèques papier constitue donc un facteur de motivation important en faveur des opérations de paiement numérique. En remplaçant par des paiements numériques une partie de ces chèques papier, on pourrait réaliser d'ici 2020 des économies de l'ordre de 3 à 7 milliards de dollars, soit de 0,1 à 0,3 % du produit intérieur brut du Canada[4]. Ce changement permettrait aussi d'améliorer considérablement l'aspect pratique et l'efficacité puisque les opérations pourraient être effectuées immédiatement ou presque instantanément, alors qu'il faut compter plusieurs jours avant qu'un chèque papier arrive à destination par la poste.

L'idée que le Canada est à la traîne des autres pays pour ce qui est de l'adoption des paiements numériques constitue un autre facteur de motivation invoqué. Selon certains indicateurs (p. ex. le nombre d'opérations électroniques entre entreprises), le Canada tire de l'arrière (énormément dans certains cas) par rapport à la Corée du Sud, aux États-Unis, à la Chine, au Danemark, à la Finlande, à la Norvège, à la Suède, au Royaume-Uni, à l'Australie, à l'Allemagne, à l'Espagne, à l'Italie, au Brésil et au Japon[5]. Pour diverses entités canadiennes, la situation est embarrassante et il faut y remédier le plus tôt possible. Toutefois, d'après d'autres indicateurs (p. ex. le pourcentage d'opérations électroniques effectuées au point de vente par le consommateur), le Canada figure dans le peloton de tête[6]. Il est clair que les paiements mobiles constituent une catégorie de paiements numériques et, comme nous l'avons signalé ci-dessus, notre étude porte uniquement sur les paiements mobiles auxquels participe directement l'utilisateur final (consommateur). C'est pourquoi le rang peu enviable attribué au Canada dans le « classement mondial » ne peut être considéré à nos yeux comme un argument de poids pour justifier l'adoption des paiements mobiles (en tout cas pas aussi convaincant que l'aspect pratique et l'efficacité). En fait, d'après un récent rapport de MasterCard[7], le Canada se classe au deuxième rang mondial selon l'indice de préparation aux paiements mobiles (MPRI), une fiche de pointage portant sur

[2] Groupe de travail sur l'examen du système de paiement, Le passage au numérique : Faire la transition vers les paiements numériques, rapport présenté au ministre des Finances, 2011. Voir http://paymentsystemreview.ca/wp-content/themes/psr-esp-hub/documents/r03_fra.pdf (consulté le 13 février 2013).

[3] *Ibid.*, p. 62.

[4] *Ibid.*, p. 17.

[5] *Ibid.*, p. 18.

[6] *Ibid.*, p. 18.

[7] Indice de préparation aux paiements mobiles (MPRI) déterminé par MasterCard. Voir http://mobilereadiness.mastercard.com/the-index/ (consulté le 13 mars 2013).

différents facteurs, notamment la préparation des consommateurs, l'environnement, l'offre de services financiers, l'infrastructure, l'existence de pôles de commerce mobile et la réglementation[8].

Enfin, signalons que la valeur estimative des paiements mobiles se chiffre à 13 milliards de dollars à l'heure actuelle aux États-Unis (et qu'elle se situait à environ 10 milliards au Canada en 2011[9]). D'après nombre d'observateurs, l'offre croissante de tablettes et de téléphones intelligents dans tous les segments de la société devrait faire augmenter cette valeur, qui pourrait atteindre 90 milliards de dollars dès 2017[10]. Ce changement laisse entrevoir des bénéfices importants pour tous les participants à l'industrie des paiements mobiles.

3. Types de paiements mobiles

D'après un article publié en 2010 par *CNET*[11], il existe au moins quatre types de paiements mobiles distincts, soit le paiement mobile de personne à personne (mP2P), le paiement mobile à un terminal de point de vente (mPOS), le commerce mobile (mCommerce) et l'acceptation mobile (mAccept). Puisque la plupart de ces modes de paiement utilisent (ou peuvent utiliser) la communication en champ proche (NFC) comme technologie sous-jacente, nous nous intéressons de près aux paiements reposant sur cette technologie. La série de normes NFC s'applique aux téléphones intelligents et aux appareils similaires qui établissent une communication sans fil entre eux quand on les fait se toucher ou qu'on les place à proximité (à quelques centimètres de distance ou moins)[12].
Chaque type de paiement se décrit comme suit :

- **Paiement mobile de personne à personne** (mP2P) : Ce type de paiement couvre les opérations entre individus, par exemple pour payer la gardienne d'enfants ou bien prêter ou rembourser 10 $ à un ami. Ces opérations pourraient utiliser PayPal, la messagerie texte, la technologie NFC ou d'autres technologies sur l'appareil mobile de chaque personne visée. Dans ce type de paiement, aucun participant n'est un commerçant enregistré.

- **Paiement mobile à un terminal de point de vente** (mPOS) : Ce type de paiement englobe les opérations plus officielles entre une personne et un commerçant enregistré, souvent à la caisse d'un commerce ayant pignon sur rue. Les clients utilisent leur appareil mobile pour communiquer avec le terminal de point de vente afin d'acheter des produits ou des services. Ces opérations peuvent utiliser un appareil mobile équipé de la technologie NFC pour communiquer

[8] R. Fuentes, « Canadian Mobile Payments Adoption Ranks Second in the World », *TechVibes*, 10 mai 2013. Voir http://www.techvibes.com/blog/canadian-mobile-payments-adoption-ranks-second-in-the-world-2012-05-10 (consulté le 13 mars 2013).

[9] Association canadienne des paiements, *Examen des méthodes de paiement et des tendances des paiements au Canada,* rapport de l'ACP, octobre 2012. Voir http://cdnpay.ca/imis15/pdf/pdfs_publications/examining_canadian_payment_report_2012_fr.pdf (consulté le 13 mars 2013).

[10] D. Carrington, *US Mobile Payments Forecast 2013 – 2017: Mobile Payments to Reach $90B by 2017*, Forrester Research, Inc., 16 janvier 2013. Voir http://blogs.forrester.com/denee_carrington/13-01-16-us_mobile_payments_forecast_2013_2017_mobile_payments_to_reach_90b_by_2017 (consulté le 27 février 2013).

[11] J. Dolcourt, « Making Sense of Mobile Payment », *CNET*, 13 août 2010. Voir http://www.cnet.com/8301-17918_1-20013480-85.html (consulté le 14 février 2013).

[12] *Wikipedia, the Free Encyclopedia*, « Near field communication ». Voir http://en.wikipedia.org/wiki/Near_field_communication (consulté le 13 mars 2013).

avec le terminal (p. ex. l'initiative récemment lancée par Rogers, la CIBC et Blackberry[13]) ou une autre technologie (p. ex. l'initiative de lecture de codes à barres de Starbucks et MasterCard[14]). Un appareil mobile peut aussi communiquer avec un appareil non traditionnel au point de vente (p. ex. une tablette) pour effectuer des opérations sans NFC. Le Portefeuille Square, qui permet à l'utilisateur de payer un commerçant simplement en déclinant son nom si l'application est installée et ouverte sur son appareil et sur celui du commerçant est un exemple intéressant. Lorsque l'utilisateur s'approche de la caisse, les applications communiquent, puis le nom et la photo de l'utilisateur s'affichent sur l'appareil du commerçant. En confirmant son nom (et pourvu qu'il ressemble à la photo affichée), l'utilisateur effectue l'opération de paiement.

- **Acceptation mobile** (mAccept) : Cette technologie est un hybride des solutions de personne à personne et à un terminal de point de vente. Deux personnes participent à l'opération, mais l'une d'entre elles est un commerçant. Il peut s'agir d'une opération informelle, dans la mesure où le commerçant peut ne pas être un agent enregistré ou autorisé (p. ex. auprès de MasterCard ou de Visa). Le consommateur paie au moyen d'une carte de crédit ou de débit, ce qui est possible lorsque le commerçant utilise un appareil mobile et un plugiciel matériel lui permettant de lire et de traiter une carte de paiement. Au nombre des technologies facilitant ces opérations, mentionnons le Portefeuille Square[15] et le PAYware Mobile[16] (pour en savoir plus sur le Portefeuille Square, voir la section 5.2 ci-après). Il est à noter que le Conseil de normes de sécurité PCI (Payment Card Industry) a publié des lignes directrices pour l'acceptation mobile; par exemple, voir PCISSC[17].
- **Commerce mobile** (mCommerce) : Ce mode de paiement utilise une application ou le navigateur d'un appareil mobile pour faire des achats en ligne. Il a été adopté par des sites d'achat en ligne bien connus comme Amazon, eBay et iTunes. Dans cette catégorie, on utilise un appareil mobile, mais il n'est pas essentiel pour l'opération (c.-à-d. que la même opération pourrait être effectuée sur un ordinateur portatif ou de bureau), et le commerce mobile ne relève par conséquent pas de la portée de notre étude. Signalons toutefois que l'idée de faire des achats en ligne en utilisant un téléphone au lieu d'un PC contribue à préparer les gens au concept d'utilisation du téléphone comme appareil de paiement. Nous examinerons brièvement cette étape de transition.

Essentiellement, si l'on exclut la catégorie du commerce mobile, les trois modes de paiement mobile restants peuvent être considérés comme suit. Commençons par le scénario d'un achat traditionnel dans un commerce ayant pignon sur rue (le client utilise une carte de crédit ou de débit à un terminal de point

[13] *Canada Newswire*, « La Banque CIBC et Rogers présentent le futur en matière de paiements mobiles au Canada », 15 mai 2012. Voir http://www.newswire.ca/fr/story/974983/la-banque-cibc-et-rogers-presentent-le-futur-en-matiere-de-paiements-mobiles-au-canada (consulté le 22 février 2013).

[14] J. Stark, « Mobile Payments: Starbucks App », 20 juin 2011. Voir http://jonathanstark.com/blog/mobile-payments-starbucks-app (consulté le 27 février 2013). [Voir aussi http://fr.starbucks.ca/coffeehouse/mobile-apps/mystarbucks

[15] J. Dolcourt, « Start Your Own Business with Square for Android », *CNET*, 19 mai 2010. Voir http://www.cnet.com/8301-19736_1-20005441-251.html (consulté le 14 février 2013).

[16] VeriFone, *PAYware Mobile*. Voir http://www.paywaremobile.com/ (consulté le 14 février 2013).

[17] Payment Card Industry Security Standards Council, Emerging Technologies, *PCI Mobile Payment Acceptance Security Guidelines*, Version 1.0 », février 2013. Voir https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf (consulté le 1er mars 2013).

de vente) et remplaçons l'instrument utilisé par le payeur, celui utilisé par le payé ou les deux par un appareil mobile :

- pour le paiement mobile à un terminal de point de vente, l'appareil du payeur remplace une carte de crédit ou de débit (p. ex. grâce à l'utilisation d'une application de paiement);
- pour l'acceptation mobile, l'appareil du payé remplace un terminal de point de vente (p. ex. grâce à l'utilisation du Portefeuille Square);
- pour le paiement mobile de personne à personne, les appareils mobiles effectuent les fonctions du payeur et du payé.

Ces scénarios ne se limitent pas à l'utilisation d'appareils mobiles pour l'opération de paiement. Ils peuvent aussi englober des acteurs et des caractéristiques supplémentaires. Par exemple, grâce au remplacement d'un terminal de point de vente traditionnel par un appareil mobile, des personnes sont devenues de façon arbitraire des commerçants qui acceptent des paiements par carte de crédit ou de débit (il peut s'agir d'utiliser une carte MasterCard pour acheter de la limonade dans un stand au bord de la route tenu par un enfant du voisinage, un article dans une vente de garage ou des fruits et légumes dans un marché de producteurs). Autre exemple, le remplacement d'une carte de crédit ou de débit traditionnelle par un appareil mobile a permis le développement de portefeuilles électroniques (notamment celui de Google) qui renferment plusieurs instruments de paiement, y compris différentes cartes de crédit ou de débit, des coupons, des cartes de fidélité et des cartes de réduction pour les membres. Enfin, non seulement le remplacement des cartes de crédit ou de débit et des terminaux au point de vente par des appareils mobiles a ouvert la voie aux paiements informels simples au moyen d'une carte ou d'un compte bancaire entre individus (p. ex. par PayPal), mais aussi il a donné l'élan nécessaire pour lancer le mouvement en faveur de la monnaie numérique (p. ex. les pièces de monnaie et les billets de banque sous forme électronique) que diverses entités peuvent échanger tout comme s'il s'agissait d'argent liquide (p. ex., voir Cybermonnaie[18]).

Comme nous l'avons mentionné ci-dessus, nous passons en revue le paiement mobile à un terminal de point de vente (articulé autour de l'utilisation d'appareils mobiles NFC par le payeur), mais nous nous pencherons également sur certaines sous-catégories de modes de paiement mobile de personne à personne, d'acceptation mobile et de commerce mobile.

4. L'écosystème des paiements mobiles à un terminal de point de vente

La présente section donne un aperçu des différents acteurs qui participent au mode de paiement mobile à un terminal de point de vente (PDV) reposant sur la technologie NFC. L'information présentée s'inspire des sources suivantes : le livre blanc de 2009 de la Smart Card Alliance intitulé *Security of Proximity Mobile Payments*[19], le *Canadian NFC Mobile Payments Reference Model* (2012)[20];et l'article « Who Will Profit from NFC, Mobile Payments? » paru dans *CNET* en 2011[21].

[18] Monnaie royale canadienne, « Ressources pour développeurs d'applications Cybermonnaie ». Voir http://developer.deficybermonnaie.com/ (consulté le 20 juillet 2013).

19 Smart Card Alliance, Security of Proximity Mobile Payments, A Smart Card Alliance Contactless and Mobile Payments Council White Paper, publication CPMC-09001, mai 2009. Voir http://collaboration/lib-bib/Library%20Document%20Collection/Security%20of%20Proximity%20Mobile%20Payments.pdf (consulté le 14 février 2013).

[20] Institutions financières canadiennes (participants à l'initiative de l'industrie) *Canadian NFC Mobile Payments Reference Model*, version 1.03, 14 mai 2012. Voir http://collaboration/lib-

4.1 Dix catégories d'acteurs

Le paiement mobile à un terminal PDV fait intervenir dix catégories d'acteurs, soit quatre qui participent à la mise en œuvre des moyens permettant le service de paiement; deux, qui participent principalement (ou uniquement) à l'opération de paiement proprement dite; et les quatre autres, qui interviennent de ces deux façons.
Chaque catégorie d'acteurs est décrite ci-après.

Acteurs permettant les paiements et participant aux opérations de paiement

- **Banque ou institution financière** : Le rôle des banques ou des institutions financières n'est pas très différent de celui qu'elles jouent dans les opérations traditionnelles par carte de crédit ou de débit, mais l'avènement du paiement mobile leur offre la possibilité d'accroître leurs revenus. Par exemple, comme dans le cas des cartes de crédit, les banques peuvent accorder une marge de crédit à leurs clients pour l'utilisation des paiements mobiles. En outre, la capacité d'offrir de nouveaux services de paiement peut faire augmenter le volume des opérations, accroître le rayonnement de la marque et fidéliser la clientèle. Les banques peuvent aussi convaincre les commerçants qui utilisent couramment de l'argent liquide et des chèques à accepter les paiements mobiles (en invoquant l'aspect pratique et l'efficacité).

  Fait intéressant, le marché prometteur des paiements mobiles a également incité des acteurs non traditionnels à envisager de se lancer dans l'activité bancaire pour accroître leurs bénéfices. Le cas de Rogers Communications, Inc., qui a présenté une demande au gouvernement fédéral en 2011 afin d'ouvrir une banque (« Rogers Bank / Banque Rogers »)[22] est à cet égard un bon exemple.

- **Marque de paiement** : La marque de paiement (p. ex. Visa, MasterCard et American Express), qui joue aussi généralement le rôle du propriétaire ou du fournisseur de l'application de paiement, prend en charge la sécurité des authentifiants. L'acceptation et le succès grandissants des cartes de crédit ou de débit sans contact (c'est-à-dire un paiement effectué en plaçant sur la borne de lecture une carte équipé d'une puce) semblent indiquer que le passage aux appareils mobiles NFC pourrait se faire relativement en douceur et sans difficulté. C'est aussi l'occasion pour les marques de paiement de se présenter sous un jour novateur et attrayant pour les consommateurs et, à l'instar des banques, elles ont tout à gagner à persuader les commerçants d'accepter les paiements mobiles.
  De plus, il est possible d'accroître la variété et le nombre de marques de paiement à la disposition de l'utilisateur. Mentionnons notamment les émetteurs de coupons, de cartes de fidélité et de cartes de réduction pour les membres. Comme on peut utiliser ces instruments pour effectuer un

---

bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (consulté le 14 février 2013).

[21] J. Dolcourt, « Who Will Profit from NFC, Mobile Payments? », *CNET*, 7 avril 2011. Voir http://www.cnet.com/8301-17918_1-20049894-85.html (consulté le 14 février 2013).

[22] P. Evans, « Rogers Wants to Start a Bank », *CBC News*, 6 septembre 2011. Voir http://www.cbc.ca/news/business/story/2011/09/06/rogers-bank.html (consulté le 22 février 2013); *Les affaires.com,* « Rogers veut lancer une banque » Voir http://www.lesaffaires.com/imprimer/strategie-d-entreprise/developpement-des-affaires/rogers-veut-lancer-une-banque/534512 .

paiement ou réduire le prix d'un article au moment de l'achat, le nombre d'acteurs dans l'espace des marques de paiement est pratiquement illimité : n'importe quel commerçant peut facilement envoyer un coupon à tous ses clients, n'importe quel groupe peut envoyer une carte de réduction à tous ses membres, et ainsi de suite. Cette situation présente l'inconvénient de compliquer grandement la sécurisation du processus de paiement (car il est difficile pour le commerçant de s'assurer de la validité d'un coupon qu'il n'a pas émis).

- **Fournisseur de portefeuille électronique** : La possibilité que l'utilisateur ait accès à plusieurs marques de paiement a naturellement donné naissance au concept du portefeuille électronique (sous forme d'applications sur l'appareil ou de service sur un serveur distant). Si les utilisateurs ont des cartes de crédit ou de débit, plusieurs cartes de membres et des coupons de différents émetteurs sur leur appareil mobile, il faut une application pour gérer et sécuriser ces instruments. Le fournisseur de portefeuille électronique propose une application ou un service (en l'occurrence le portefeuille), qui gère ces instruments et assure l'interface avec le payeur. Google, Isis[23], Visa, MasterCard, les institutions financières et d'autres tiers sont des fournisseurs de ce type de portefeuilles. Les clients peuvent généralement s'en procurer un gratuitement, mais les fournisseurs peuvent imposer aux commerçants des frais fixes ou un pourcentage du montant de tout achat effectué par ce moyen[24].

- **Utilisateur final** : L'utilisateur final est le consommateur des services de paiement mobile et de connectivité mobile. Il s'agit manifestement d'un acteur essentiel de l'opération de paiement, mais l'utilisateur final joue aussi un rôle en permettant le service de paiement de différentes façons : il demande des marques de paiement particulières (bien que certaines puissent avoir été installées au préalable sur l'appareil) et l'émission d'authentifiants (pour permettre le fonctionnement des applications de paiement). De façon générale, l'utilisateur fait des choix concernant l'exploitant de réseau mobile, l'appareil mobile, le fournisseur de portefeuille électronique, l'institution financière et le commerçant.

Acteurs permettant la prestation des services de paiement

- **Fabricant d'appareils mobiles** : Le fabricant d'appareils mobiles (p. ex. Apple, BlackBerry et Nexus) peut obtenir un avantage concurrentiel en construisant des appareils qui permettent les paiements mobiles. En particulier, il s'agit de construire des appareils NFC comportant un élément de sécurité (c'est-à-dire une carte à puce intégrée assurant un stockage sécurisé) qui stocke l'application de paiement et l'information sur le compte. Le nombre de téléphones intelligents NFC, qui est déjà élevé, continue d'augmenter rapidement (voir *NFCWorld*[25] pour consulter une liste à jour).

[23] Isis Mobile Wallet (AT&T Mobility, T-Mobile USA et Verizon Wireless ont fondé Isis pour concrétiser leur vision commune du commerce mobile). Voir http://www.paywithisis.com/ (consulté le 28 février 2013).

[24] *Wikipedia, the Free Encyclopedia*, « Digital Wallet ». Voir http://en.wikipedia.org/wiki/Digital_wallet (consulté le 15 février 2013). Voir aussi *A Global Overview of Digital Wallet Technologies*, publié par le ID Lab, Université de Toronto, le 28 mai 2011 : http://propid.ischool.utoronto.ca/digiportefeuille électronique_overview/ (consulté le 15 février 2013).

[25] *NFC World*, « A Definitive List of NFC Phones », version à jour le 19 février 2013. Voir http://www.nfcworld.com/nfc-phones-list/ (consulté le 19 février 2013).

Grâce aux applications mobiles novatrices (y compris le paiement mobile), les fabricants d'appareils attireront de nouveaux clients et forgeront de nouvelles relations d'affaires. Il s'agit donc pour eux d'une possibilité attrayante sur le plan financier.

- **Fabricant de terminaux PDV** : Le fabricant de terminaux de point de vente (PDV) produit les appareils qui se trouvent près des caisses, à bord des autobus, dans les stations de métro, etc. Les terminaux PDV équipés de la technologie NFC permettent d'effectuer les paiements au moyen d'une génération d'appareils mobiles NFC. La rapidité et l'aspect pratique de cette opération attirent les commerçants partout dans le monde. VeriFone a été l'un des pionniers de l'écosystème, mais de nombreux autres acteurs profitent maintenant des ventes de terminaux PDV NFC.

- **Gestionnaire de services de confiance** : Le gestionnaire de services de confiance (p. ex. Vodafone, Oberthur, Gemalto, Giesecke & Devrient et Telefonica) joue un rôle central et déterminant pour ce qui est de permettre (c.-à-d. provisionner) les paiements mobiles, même s'il ne participe pas à l'opération de paiement proprement dite. En particulier, comme il est expliqué de façon assez détaillée à la section 10 du *Canadian NFC Mobile Payments Reference Model*[26], les institutions financières, les marques de paiement, les sociétés de transport en commun, les détaillants et les autres intervenants qui souhaitent offrir une application de paiement, de billetterie ou de fidélité aux utilisateurs d'appareils NFC doivent le faire par l'intermédiaire d'un gestionnaire de services de confiance. Faisant office de guichet unique et de poste de sécurité qui contrôle les intervenants autorisés à installer des instruments de paiement sur l'appareil, le gestionnaire recueille les données de l'application de paiement NFC et les renseignements personnels de l'utilisateur (p. ex. son nom, son numéro de carte de crédit et la date d'expiration), qu'il transmet ensuite par ondes hertziennes (par l'intermédiaire de l'exploitant de réseau mobile) jusqu'à l'élément de sécurité sur l'appareil mobile. Le gestionnaire de services de confiance assure des services de téléchargement et de gestion du cycle de vie pour les données des applications de paiement NFC et des consommateurs.

  De façon générale, les marques de paiement imposent des exigences rigoureuses aux entités qui souhaitent faire office de gestionnaire de services de confiance. Par exemple, elles effectuent un audit de sécurité avant de les autoriser à traiter la transmission des données des cartes de paiement. Les gestionnaires de services de confiance doivent gérer adéquatement les clés de chiffrement pour sécuriser la communication entre l'institution financière et l'appareil mobile de l'utilisateur.

  Le rôle de gestionnaire de services de confiance représente une nouvelle possibilité d'affaires dans l'écosystème des paiements mobiles[27]. Les tiers (p. ex. les fournisseurs de services de personnalisation utilisés avec les cartes de crédit et de débit traditionnelles) peuvent demander à être agréés comme gestionnaires de services de confiance et offrir leurs services aux institutions financières et aux exploitants de réseau mobile. Ces institutions ou ces exploitants peuvent aussi

[26] Institutions financières canadiennes (participants à l'initiative de l'industrie) *Canadian NFC Mobile Payments Reference Model*, version 1.03, 14 mai 2012. Voir http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (consulté le 14 février 2013).

[27] *NFC Times*, « Topic: "Trusted Service Manager" », 2013 (recueil des contrats de gestionnaires de services de confiance récemment signés). Voir http://nfctimes.com/tags/trusted-service-manager (consulté le 28 février 2013).

choisir de devenir eux-mêmes des gestionnaires de services de confiance accrédités et de remplir cette fonction pour élargir leur offre de services et accroître leurs revenus.

- **Exploitant de réseau mobile** : Le principal rôle de l'exploitant de réseau mobile (p. ex. Rogers) concernant les paiements mobiles consiste à fournir le canal par lequel les données des applications de paiement et les renseignements des consommateurs peuvent être transmis des institutions financières, des marques de paiement, etc., à l'élément de sécurité sur l'appareil. Il incombe donc à l'exploitant de réseau mobile d'assurer l'intégrité des clés et des certificats qui seront utilisés pour protéger la communication sur le réseau (p. ex. au moyen du protocole TLS). Lorsque l'élément de sécurité appartient à l'exploitant (en particulier lorsqu'il est intégré à la carte de circuit intégré universelle [carte UICC], communément appelée « carte d'identification d'abonné » [carte SIM]) et fournie à l'utilisateur par l'exploitant de réseau mobile, l'exploitant doit aussi assurer l'intégrité des clés qui donnent accès (lecture et écriture) à l'élément de sécurité. Il est à noter que l'exploitant n'a pas pour autant accès aux renseignements du consommateur : il utilise une clé pour déverrouiller l'élément de sécurité afin d'y inscrire les données et une autre clé pour protéger la communication TSL de ces données de la marque de paiement à l'élément de sécurité. Les données proprement dites sont chiffrées par la marque de paiement avant d'être transmises au moyen d'une autre clé connue uniquement des responsables de la marque de paiement (ainsi, seule l'application de paiement de la marque de paiement peut les lire ou les modifier). L'exploitant de réseau mobile peut aussi jouer un autre rôle dans le processus de paiement en offrant des appareils NFC à ses clients.

  Comme il y a habituellement un certain roulement dans leur base d'abonnés, les exploitants de réseau mobile sont à la recherche d'applications et de services leur permettant non seulement d'attirer de nouveaux clients, mais aussi de conserver leur clientèle actuelle. Les paiements mobiles peuvent leur procurer des avantages financiers de cette façon et leur permettre d'accroître leurs revenus grâce aux nouveaux services connexes, par exemple les messages texte publicitaires et les coupons.

Acteurs participant principalement (ou uniquement) aux opérations de paiement proprement dites

- **Commerçant ou détaillant** : Les paiements mobiles NFC sont attrayants pour les commerçants qui utilisent telle quelle l'infrastructure de paiement par carte sans contact. C'est pourquoi les commerçants qui acceptent actuellement ces paiements disposent de tous les éléments voulus pour accepter immédiatement les paiements mobiles NFC. Les paiements par carte sans contact sont utilisés dans le monde entier depuis un certain temps à la fois pour accélérer les opérations de paiement (parce que les opérations se font plus rapidement et que la manipulation d'argent est moins nécessaire) et en raison de l'aspect pratique pour les clients. En plus d'hériter de ces avantages, les paiements mobiles NFC permettent aux commerçants d'établir des relations plus étroites avec les clients et de les fidéliser.

  Les paiements mobiles NFC permettent aussi de générer des revenus qui font défaut dans le cas des cartes sans contact. Par exemple, à l'instar des institutions financières, les commerçants peuvent offrir à leurs clients des services liés à leurs achats et des services fidélisateurs et améliorer l'efficacité des programmes de cartes-cadeaux et de fidélité (puisque les « cartes de paiement » d'un client seront toujours disponibles dans son appareil mobile). En outre, les reçus sans papier (reçus électroniques transmis au client par NFC, courriel ou message texte) seront

toujours accessibles sur l'appareil, ce qui simplifiera les retours ou les échanges. Enfin, les programmes de marketing et de promotion mobiles avancés peuvent transmettre des messages aux clients en fonction du contexte ou de leur emplacement et ainsi influencer leur comportement en matière d'achat à l'intérieur et à l'extérieur du commerce dans l'espoir de générer des ventes supplémentaires et de fidéliser la clientèle.

- **Exploitant de réseau de paiement** : L'autorisation et le règlement des opérations de paiement mobile se font par les réseaux financiers existants. Les exploitants de réseau mobile (p. ex. Interac) jouent le même rôle qu'à l'heure actuelle dans les opérations traditionnelles par carte de crédit ou de débit. L'adoption des paiements mobiles ne modifie en rien la fonction ou le fonctionnement de ces réseaux de traitement des paiements en aval.

Il est à noter que **l'on peut aussi mentionner une onzième catégorie d'acteurs**, même s'ils ne participent pas au processus de paiement proprement dit : **les réseaux de publicité.** Ces acteurs envoient des publicités aux appareils mobiles des utilisateurs pour les inciter à faire des achats (« il y a un café Starbucks à deux coins de rue d'ici », « il y a une réduction cette semaine sur la crème glacée Häagen-Dazs » ou « les clients qui ont acheté ce livre achètent souvent tel autre livre »). En déclenchant l'impulsion de se procurer un article et en rappelant au client une décision d'achat antérieure, cette publicité axée sur le contexte ou l'emplacement l'incite parfois à faire un achat.
Dans le contexte du présent rapport, cette catégorie englobera les tiers annonceurs (qui tirent une grande partie de leurs revenus de la publicité qu'ils font auprès d'une clientèle fort variée), par opposition aux commerçants ou aux détaillants qui envoient des publicités ou des recommandations directement, voire exclusivement, à leurs propres clients. La pertinence de cette catégorie pour notre étude tient au fait que l'utilisateur final peut utiliser « gratuitement » certains modes de paiement et que le fournisseur de portefeuille électronique ou d'authentifiants peut profiter de la vente de l'information à des tiers annonceurs, ce qui suscite des préoccupations concernant la protection de la vie privée.

La figure ci-après montre certains acteurs de l'écosystème du paiement mobile à un terminal de point de vente (tirée de la figure 1 du livre blanc de la Smart Card Alliance[28]) :

[28] Smart Card Alliance, *Security of Proximity Mobile Payments : A Smart Card Alliance Contactless and Mobile Payments Council White Paper*, publication CPMC-09001, mai 2009. Voir http://collaboration/lib-bib/Library%20Document%20Collection/Security%20of%20Proximity%20Mobile%20Payments.pdf (consulté le 14 février 2013).

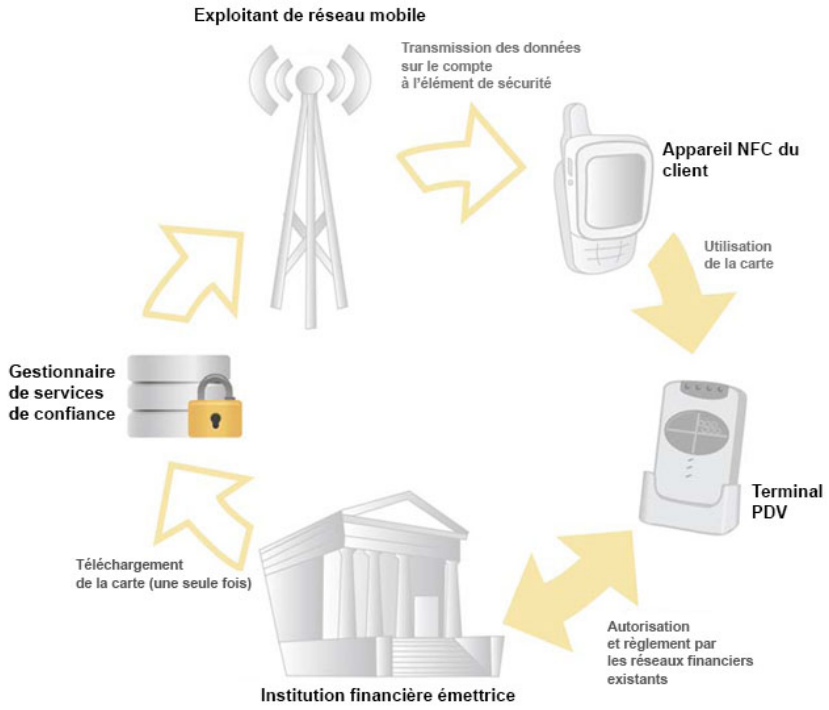

Figure 1. Certains acteurs de l'écosystème de paiement mobile à un terminal PDV

Comme on pouvait s'y attendre, l'écosystème de paiement mobile à un terminal PDV est similaire à n'importe quel autre écosystème financier : tout le monde veut sa part du gâteau; tout le monde veut faire de l'argent (ou en économiser dans le cas de l'utilisateur) dans l'opération de paiement. On trouve à une extrémité les utilisateurs, qui ont fixé le prix maximum qu'ils sont prêts à payer pour un article (p. ex. 3 $), et à l'autre les commerçants, qui ont défini le montant minimum qu'ils doivent recevoir pour couvrir leurs coûts et réaliser un bénéfice (p. ex. 2,50 $). L'écart entre les deux représente l'argent qui sera réparti entre tous les acteurs de l'écosystème (p. ex., si la différence est de 50 cents, peut-être que cinq cents iront à l'utilisateur [l'article sera vendu à 2,95 $], cinq cents au commerçant [il conservera 2,55 $] et 40 cents seront répartis entre les autres acteurs).

4.2 Provisionnement ou initialisation de l'application et des données de paiement mobile

Pour effectuer des paiements à un terminal PDV NFC, l'utilisateur doit avoir un appareil mobile NFC, une application de paiement et un authentifiant. D'après le *Canadian NFC Mobile Payments Reference Model*[29], p. 27, l'application de paiement est similaire à celle installée sur une carte sans contact (p. ex. PayWave de Visa et PayPass de MasterCard), et l'authentifiant représente l'information personnalisée dans cette application qui est unique au type de paiement visé (y compris le mot de passe). En règle générale, le logiciel de l'utilisateur comprendrait aussi un portefeuille électronique pour gérer plusieurs

[29] Institutions financières canadiennes (participants à l'initiative de l'industrie), *Canadian NFC Mobile Payments Reference Model*, version 1.03, 14 mai 2012. Voir http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (consulté le 14 février 2013).

applications de paiement et assurer une interface avec elles. Le portefeuille électronique ou une autre application permet d'afficher différents renseignements associés à l'authentifiant, soit le nom du réseau de paiement, l'illustration de la carte (p. ex. le logo), l'instrument de paiement (p. ex. une carte de crédit ou de débit) et un petit segment (p. ex. les trois ou quatre derniers chiffres) du numéro de compte de la carte de crédit ou de débit, ce qui permet au client de s'identifier et de choisir un authentifiant au moment de l'opération de paiement.

C'est l'institution financière qui lance l'application de paiement et le processus d'authentification, mais uniquement une fois que le consommateur est prêt à amorcer l'opération sur l'appareil mobile (ce qui peut nécessiter la saisie d'un code d'activation fourni par la banque). Comme il est expliqué à la section 10 du *Canadian NFC Mobile Payments Reference Model,* l'institution financière fournit l'application et les données au gestionnaire de services de confiance, qui installe l'application et les données sur l'élément de sécurité de l'appareil (s'il y a lieu, par l'intermédiaire du portefeuille électronique, qui a uniquement accès à l'information visible, tandis que tous les autres renseignements ne sont stockés que dans l'élément de sécurité). Après ce processus d'authentification, le consommateur peut effectuer des opérations de paiement mobile.

5. Autres modes de paiement

Outre le mode de paiement mobile présenté ci-dessus, nous en présenterons brièvement deux autres, soit le paiement de personne à personne et l'acceptation mobile, dans les deux prochaines sections (et dans la partie 2 du présent rapport). Ces modes de paiement ne semblent pas aussi importants ou fréquents que le paiement à terminal PDV NFC au Canada, mais nous les examinons ici parce qu'ils reçoivent l'aval de solides promoteurs ou qu'ils sont répandus dans d'autres régions du monde.

5.1 Paiement mobile de personne à personne (opérations entre personnes)

Pour les opérations de paiement mobile de personne à personne (aussi appelées « de poste à poste », quoique certains auteurs établissent une distinction entre les deux; par exemple, voir Charrat[30]) effectuées au moyen d'appareils mobiles, on peut utiliser de nombreuses technologies sous-jacentes différentes. Les plus répandues sont PayPal (qui utilise Bump ou NFC) et M-Pesa (qui utilise la messagerie texte), mais la technologie Cybermonnaie (qui utilise de l'argent numérique) pointe à l'horizon.

[30] B. Charrat, « Debunking NFC Peer-to-Peer Myths », *Inside Secure*, février 2012. Voir http://insidesecure.com/eng/Media/White-papers (consulté le 20 février 2013).

5.1.1 PayPal

PayPal est en activité depuis mars 2000 comme service de paiement pour le commerce électronique et de transfert de fonds[31]. En 2004, l'entreprise a commencé à explorer l'utilisation d'appareils mobiles pour le transfert de fonds (PayPal Mobile) au moyen de messages texte sur les téléphones cellulaires[32].
En 2010, PayPal a associé sa technologie à Bump (qu'elle a par la suite abandonnée, mais qui est encore utilisée par ING et d'autres). À la fin de 2011, une application Android utilisant NFC pour le transfert de fonds a été lancée.

Les opérations Bump ressemblent beaucoup aux opérations NFC, mais Bump n'utilise pas la technologie NFC. L'application Bump Pay reconnaît les « chocs » et elle les localise. Lorsqu'elle reconnaît un « choc », elle envoie un signal aux serveurs en nuage qui l'associent à un autre « choc » qui a été donné exactement au même endroit et au même moment. Elle décide alors que les deux « chocs » coïncident et échange l'information entre eux[33]. Pour utiliser l'application, Alice se connecte à son compte PayPal, saisit le montant qu'elle souhaite transférer, entrechoque son téléphone et celui de Robert et confirme le paiement. L'application Bump Pay doit être installée sur le téléphone de Robert pour qu'il puisse recevoir le paiement. Si les deux comptes PayPal sont associés à des comptes-chèques, le transfert est gratuit. Toutefois, si le compte est uniquement associé à une carte de crédit, un pourcentage quelconque sera prélevé[34].

Pour NFC, PayPal a une application qui permet de transférer des fonds au moyen d'une interface très simple. Alice et Robert doivent avoir chacun un téléphone Android NFC et l'application PayPal. La fonction « Request Money » doit être installée. Pour demander des fonds, Alice saisit le montant et entrechoque son téléphone et celui de Robert. Lorsqu'il reçoit la demande, Robert saisit son mot de passe pour envoyer les fonds[35]. Fait intéressant, PayPal a récemment délaissé NFC, affirmant qu'il s'agissait d'une « technologie pour la technologie » et qu'elle ne « réglait pas les irritants pour les clients »[36], même si les paiements mobiles effectués au moyen d'appareils NFC (qui utilisent des canaux de paiement autres que PayPal, par exemple Osaifu-Keitai = [portefeuille électronique mobile] de DoCoMo) ont gagné du terrain depuis nombre d'années dans certains pays, notamment au Japon et en Chine.

---

[31] *Wikipedia, the Free Encyclopedia*, « PayPal ». Voir http://en.wikipedia.org/wiki/PayPal (consulté le 20 février 2013).

[32] PayPal, « Texting with PayPal – easy as lifting a finger ». Voir https://personal.paypal.com/ca/cgi-bin/?cmd=_render-content&content_ID=marketing_ca/mobile_text (consulté le 20 février 2013).

[33] S. Kessler, *Bank Lets Customers Pay Friends By Bumping iPhones*, 29 avril 2011. Voir http://mashable.com/2011/04/29/ing-direct-customers-bump/ (consulté le 20 février 2013).

[34] J. Constine, « Bump Pay Lets You PayPal Someone With A Tap, But Only In-Person », *TechCrunch Hot Topics*, 29 mars 2012. Voir http://techcrunch.com/2012/03/29/bump-pay/ (consulté le 20 février 2013).

[35] S. Samuel, « New in the Android Market: Updated PayPal Mobile App Featuring P2P NFC Capabilities », *The PayPal Blog*, 8 novembre 2011. Voir https://www.thepaypalblog.com/2011/11/new-in-the-android-market-updated-paypal-mobile-app-featuring-p2p-nfc-capabilities-2/ (consulté le 20 février 2013).

[36] C. Gabriel, « PayPal extends mobile wallet, but no NFC », *Rethink Wireless*, 15 janvier 2013. Voir http://www.rethink-wireless.com/2013/01/15/paypal-extends-mobile-wallet-nfc.htm (consulté le 23 février 2013).

5.1.2 M-Pesa

Lancé au Kenya en 2007, M-Pesa (argent mobile) est maintenant utilisé par beaucoup plus de la moitié de la population kenyane pour payer les factures, les salaires et les taxis, faire les achats et envoyer de l'argent directement au téléphone mobile d'une autre personne. Une forte proportion de la population kenyane n'a pas accès aux institutions bancaires et M-Pesa permet de transférer des fonds rapidement et facilement dans cet environnement. On compte à la grandeur du pays environ 50 000 agents M-Pesa, généralement établis dans de petites épiceries ou stations-service. Les clients vont rencontrer l'un de ces agents et s'inscrivent auprès de Safaricom, l'exploitant du réseau de téléphonie mobile. Une fois inscrits, ils peuvent déposer des fonds dans leur téléphone en remettant à l'agent le montant correspondant. L'agent encaisse l'argent et provisionne le téléphone par voie électronique. Le client peut alors, par exemple, envoyer de l'argent à une autre personne par message texte. Le bénéficiaire apporte le message à l'agent le plus proche, qui lui remet le montant correspondant en argent comptant[37].

M-Pesa (ou un service très similaire) est également utilisé dans d'autres pays d'Afrique, notamment en Côte d'Ivoire, au Sénégal et au Mali, ainsi qu'ailleurs dans le monde, par exemple en Afghanistan[38]. Le paiement mobile par message texte est très populaire dans plusieurs pays d'Europe et de nombreux pays d'Amérique latine ainsi qu'au Royaume-Uni, en Inde et en Australie.

5.1.3 Cybermonnaie

[Il est à noter que la Monnaie royale canadienne n'a pas encore lancé Cybermonnaie. Pour rédiger la présente sous-section, nous avons consulté la section de son site Web consacrée à Cybermonnaie[39].]

Après s'être penchée sur l'évolution de la monnaie et des technologies de paiement (en particulier dans l'écosystème des paiements au point de vente de volume élevé et de faible valeur), la Monnaie royale canadienne a mis au point Cybermonnaie[40]. Elle considère Cybermonnaie comme l'équivalent numérique des pièces de monnaie et des billets de banque et s'attend à ce qu'elle soit très largement utilisée pour les micropaiements (moins de 10 $) et les nanopaiements (moins de 1 $).

La « puce » Cybermonnaie est le cœur du système. Il s'agit d'un circuit intégré sur carte sécurisée, qui sert à stocker l'argent numérique. Cette puce, qui peut être déployée de différentes façons, offre aux utilisateurs au moins quatre options.

Premièrement, la puce peut être mise en place dans une clé USB Cybermonnaie à usage unique. Il suffit de brancher la clé USB dans n'importe quel PC ou ordinateur portatif pour effectuer des opérations de paiement en ligne ou hors ligne. Deuxièmement, la puce peut être placée dans un module de sécurité matériel à usage unique. Ce module s'adresse aux grands commerçants en ligne et aux environnements comportant un taux élevé d'opérations. Troisièmement – aspect le plus pertinent pour les besoins de notre étude –, la puce peut être mise en place dans une carte MicroSD (c'est-à-dire une petite carte

[37] Mobile Transaction, *Growing Use of SMS Payments Around the World*. Voir http://www.mobiletransaction.org/growing-sms-payments-world/ (consulté le 20 février 2013).

[38] *Ibid.*

[39] Monnaie royale canadienne, « Ressources pour développeurs d'applications – Cybermonnaie ». Voir http://developer.Cybermonnaiechallenge.com/devguide/index.php (consulté le 14 février 2013).

[40] *Ibid.*

mémoire couramment utilisée dans les appareils photo et d'autres appareils, mais aussi offerte sur certains téléphones intelligents), facilement insérable dans un appareil mobile pour permettre d'utiliser Cybermonnaie. On peut facilement enlever la puce lorsque cette fonction n'est plus nécessaire. Enfin, un tiers fournisseur de services peut héberger une série de puces Cybermonnaie dans le nuage pour ses utilisateurs, qui doivent s'identifier auprès du fournisseur de services pour avoir accès à leur argent numérique. Avec cette option, les utilisateurs peuvent effectuer des opérations au moyen d'un dispositif Cybermonnaie qui n'accueille pas la carte MicroSD ni une clé USB, par exemple un iPhone d'Apple.

L'écosystème de Cybermonnaie vise à reproduire le mode de distribution actuel des pièces de monnaie. La puce Cybermonnaie est fabriquée par la Monnaie royale canadienne, distribuée sur le marché par un courtier de confiance (voir ci-après) et utilisée par les consommateurs et les commerçants. Les consommateurs achètent un montant de Cybermonnaie auprès d'un courtier de confiance, puis ils effectuent des opérations avec des commerçants ou d'autres consommateurs qui utilisent l'outil pour acheter des produits ou des services ou simplement pour transférer des fonds. L'utilisateur qui reçoit un montant de Cybermonnaie se fait rembourser la valeur par le courtier de confiance, qui fait aussi généralement affaire avec une institution financière pour acquérir et déposer de l'argent liquide au besoin.

Dans le paiement mobile de personne à personne, les deux personnes qui participent à l'opération ont chacune dans leur téléphone une puce Cybermonnaie sur une carte MicroSD (la clé USB et le module de sécurité matériel ne font pas appel à un appareil mobile et, bien que l'on puisse utiliser un appareil mobile pour avoir accès à une puce Cybermonnaie dans le nuage, ce n'est pas essentiel; ces trois supports ne relèvent pas de la portée du présent rapport). Les appareils échangent par message texte, courriel ou communication NFC des messages faisant état de la demande et du montant d'argent. D'après le site Web de Cybermonnaie, lorsque l'expéditeur crée un message demandant le paiement d'un montant en utilisant la puce de sa propre application Cybermonnaie, ce montant est déduit du solde de la puce. Lorsque le message a été créé, l'expéditeur ne peut interrompre ou annuler l'opération. Une fois en possession du message affichant le montant, l'application de la personne appelée à recevoir les fonds s'assure de sa validité (en vérifiant une signature numérique et une valeur de sécurité). Si le message est valide, le montant précisé dans le message est ajouté au solde du receveur.

On ignore encore qui fera office de courtier de confiance dans l'écosystème Cybermonnaie. Les banques et Postes Canada sont au nombre de candidats possibles, mais d'autres entités pourraient militer pour assumer cette tâche. On ne sait pas non plus comment quiconque gagnera de l'argent grâce à ce mode de paiement. Tout porte à croire que la Monnaie royale canadienne pourrait en théorie réaliser un bénéfice en vendant à prime un montant de Cybermonnaie au courtier de confiance (p. ex. une valeur de 1,00 $ au prix de 1,02 $). En outre, le courtier de confiance pourrait probablement réaliser un bénéfice en traitant Cybermonnaie comme une devise et en prélevant un taux de change (« cours actuel : nous vendons un montant de Cybermonnaie de 1,00 $ au prix de 1,05 $; nous l'achetons au prix de 97 cents »). Mais il reste encore à savoir ce que sera la future monétisation éventuelle des opérations une fois le système déployé et quelle sera l'éventail complet d'entités qui gagneront de l'argent.

5.2 Acceptation mobile

Avec le mode d'acceptation mobile, un appareil mobile remplace le terminal PDV du commerçant (tandis que le payeur utilise une carte de crédit traditionnelle). Une petite pièce qui se fixe à l'appareil mobile permet de faire glisser une carte de crédit afin que les commerçants indépendants puissent traiter les paiements par carte de crédit n'importe quand et n'importe où. Square[41] est au nombre des quelques technologies qui permettent ce mode de paiement. Un cube en plastique se branche dans la prise casque d'un téléphone Android ou Apple. Ce cube est muni d'une fente mince, où l'on fait glisser la carte de crédit. L'application Square est exécutée sur le téléphone pour traiter les paiements. Le commerçant peut faire glisser la carte, prendre une photo de la marchandise afin d'aider les deux parties à se rappeler ce qui a été vendu et joindre sa photo, son logo, etc., afin de rappeler au payeur l'identité du payé. L'application Square cache les détails de la carte, de sorte que le payé ne puisse jamais voir le numéro ou le code de sécurité de la carte de crédit, et elle envoie au payeur par courriel ou message texte un reçu numérique.

D'après le site Web de Square[42], le commerçant doit verser 2,75 % du montant total de chaque opération (glissement d'une carte) et 3,5 % plus 15 cents par opération pour les cartes dont le numéro est saisi manuellement. Cette stratégie de tarification est similaire à celle de PayPal (1,9 et 2,9 % pour chaque vente plus 30 cents) et inférieure aux frais d'exploitation prélevés par certaines banques. PayPal a connu beaucoup de succès avec cette stratégie. En outre, avec Square, l'opération de paiement peut vraiment se faire n'importe quand et n'importe où.

6. Illustration du mouvement de l'argent

Il peut être utile d'envisager le mouvement de l'argent dans les opérations de paiement mobile. Nous l'illustrerons en présentant trois exemples concrets (les deux premiers portent sur le paiement à un terminal PDV et le troisième sur le paiement de personne à personne).

Scénario n^{o} 1 : achat au terminal PDV d'un commerçant

Dans ce scénario, Alice souhaite acheter un café et un muffin dans une brûlerie locale au moyen de son appareil mobile NFC. Après avoir donné sa commande, elle ouvre l'application de portefeuille électronique de son téléphone, vérifie que l'instrument de paiement par défaut (en l'occurrence une carte de débit MasterCard) est sélectionné et informe le commis qu'elle utilisera une carte de débit MasterCard. À la demande du commis, elle place son téléphone près du terminal PDV sans contact. Comme il s'agit d'une opération considérée comme courante (c'est-à-dire fréquente et rapide), Alice n'a qu'à passer son appareil devant la borne de lecture. En particulier, aucune vérification de la carte n'est nécessaire (il n'y a aucun mot de passe à entrer). Une fois l'opération approuvée au terminal PDV, un reçu électronique est créé et envoyé à Alice par courriel, message texte ou NFC. Pour cette dernière option, il faudrait présenter le téléphone mobile devant le terminal une deuxième fois, mais elle comporte un avantage du fait que le reçu est directement acheminé au portefeuille électronique mobile, où il est stocké, ce qui serait utile pour l'achat d'un article que l'on pourrait retourner par la suite).

[41] J. Dolcourt, « Start Your Own Business with Square for Android », *CNET*, 19 mai 2010. Voir http://www.cnet.com/8301-19736_1-20005441-251.html (consulté le 14 février 2013).

[42] Tarification de Square. Voir https://squareup.com/ca/fr/pricing (consulté le 27 février 2013).

La règle s'appliquant aux opérations courantes (p. ex. aucun NIP ni aucun mot de passe) et l'émission du reçu électronique sont exclusifs à la technologie NFC (voir le *Canadian NFC Mobile Payments Reference Model*[43], p. 35). Par ailleurs, l'opération est similaire à un paiement effectué au moyen d'une carte de crédit sans contact. Plus précisément, le mouvement de l'argent sous-jacent se fait de la même manière qu'aujourd'hui.

Scénario n^{o} 2 : primes accumulées sur les cartes de fidélité (un muffin gratuit après l'achat de 10 muffins)

Ce scénario s'inspire du scénario n^{o} 1, mais on ajoute la carte de fidélité de la brûlerie. Dans ce cas, la carte de fidélité est stockée dans le portefeuille électronique mobile d'Alice et transmise au terminal PDV en même temps que les détails de sa carte de débit lorsqu'elle passe son téléphone devant la borne de lecture. Le système du commerçant vérifie et met à jour le solde des points de fidélité d'Alice et détermine si elle a droit à une réduction (c'est-à-dire si le prix du muffin doit être soustrait du total). L'opération de paiement se déroule comme indiqué ci-dessus et la carte de fidélité mise à jour est transmise au portefeuille électronique d'Alice en même temps que son reçu électronique la deuxième fois qu'elle passe son téléphone devant la borne de lecture.

Il est à noter que le volet coupon, carte de fidélité ou carte de membre du paiement mobile est encore relativement nouveau et peut par conséquent encore évoluer. Pour l'heure, aucune norme ne permet de déterminer comment ces opérations se déroulent exactement. En particulier, on ne sait pas encore si Alice aura besoin de faire une recherche manuelle dans son portefeuille électronique pour trouver la carte de fidélité de la brûlerie ou si cette carte s'affichera automatiquement dès que les renseignements du commerçant (nom et emplacement) auront été transmis au téléphone. On ne sait pas non plus si l'information de la carte de fidélité sera transmise en même temps que les détails de la carte de débit dans un seul échange NFC ou s'il faudra faire passer le téléphone une deuxième fois devant la borne de lecture. De même, l'information de la carte de fidélité mise à jour sera peut-être transmise en même temps que le reçu électronique à la fin de l'opération ou il pourrait être nécessaire de faire passer le téléphone une autre fois devant la borne de lecture. À court terme, il est possible que les divers portefeuilles électroniques et les commerçants eux-mêmes adoptent des pratiques différentes jusqu'à ce qu'un déroulement normalisé s'impose.

Scénario n^{o} 3 : transfert de fonds entre deux amis (« Puis-je t'emprunter 10 $?)

Dans ce scénario, Alice veut remettre 10 $ à Robert afin qu'il achète une carte d'anniversaire pour son frère. Un certain nombre de technologies ont été déployées (ou proposées) pour ce type d'opération, notamment Bump Pay (p. ex. avec PayPal ou ING Direct), la messagerie texte (p. ex. avec M-Pesa), la technologie NFC (p. ex. avec PagSeguro[44] au Brésil) et l'argent électronique (p. ex. Cybermonnaie). Nous avons déjà présenté certaines de ces opérations (voir la section 5.1). Toutefois, à tout le moins en

[43] Institutions financières canadiennes (participants à l'initiative de l'industrie), *Canadian NFC Mobile Payments Reference Model*, version 1.03, 14 mai 2012. Voir http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (consulté le 14 février 2013).

[44] *The Paypers: Insights in Payments*, « Brazil: PagSeguro, Nokia to introduce NFC P2P payments », 3 mai 2012. Voir http://www.thepaypers.com/news/mobile-payments/brazil-pagseguro-nokia-to-introduce-nfc-p2p-payments/747502-16 (consulté le 22 février 2013).

Amérique du Nord, aucune de ces technologies n'a connu beaucoup de succès jusqu'à présent et on ignore laquelle dominera (le cas échéant) le mode de paiement de personne à personne au cours des prochaines années.

7. Conclusion

Dans la partie 1 du rapport, nous avons étudié le contexte des paiements mobiles, y compris les divers modes existants, les principaux acteurs de l'écosystème et la façon dont les fonds circulent de l'expéditeur au récepteur dans certaines opérations de paiement. Nous avons mis l'accent sur les opérations mobiles au point de vente utilisant la technologie de communication en champ proche (NFC), mais nous avons également mentionné d'autres technologies et modes de paiement.

Dans la partie 2, nous examinerons les répercussions de quelques modes de paiement mobile sur la sécurité et la protection de la vie privée.

Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles

Partie 2 – Analyse de certains modes de paiement

Résumé

Dans la présente partie, nous analysons certains modes de paiement en nous attachant particulièrement aux paiements mobiles au point de vente effectués au moyen de la communication en champ proche (NFC) et nous explorons brièvement d'autres technologies et modes de paiement.

1. Introduction

Le présent rapport sur les paiements mobiles est divisé en trois parties : contexte, analyse et recommandations. La partie 2, « Analyse de certains modes de paiement », porte sur les risques d'atteinte à la sécurité et à la vie privée inhérents à certains modes de paiement. Nous nous attardons au paiement mobile à un terminal PDV NFC, mais nous explorons brièvement le commerce mobile (mCommerce) actuel (en tant qu'étape de transition vers les paiements mobiles véritables) et certaines sous-catégories des paiements mobiles de personne à personne (mP2P) et d'acceptation mobile (mAccept).

Le reste de la partie 2 est structuré comme suit. Nous examinons dans la section 2 deux modes paiement axés sur le commerce mobile (achats ou opérations bancaires en ligne et facturation par les entreprises de télécommunications mobiles), tandis que nous amorçons dans la section 3 l'analyse des véritables modes de paiement mobile. Nous y examinons de manière assez détaillée le paiement à un terminal PDV NFC en mettant l'accent sur les trois aspects qui comportent des risques d'atteinte à la sécurité et à la vie privée. Dans la section 4, nous examinons brièvement le paiement mobile de personne à personne utilisé pour les transferts de fonds, en particulier M-Pesa et Cybermonnaie. La section 5 passe brièvement en revue le mode d'acceptation mobile et présente une étude de cas portant sur la technologie Square. La section 6 traite dans une optique globale des risques des opérations financières effectuées exclusivement sous forme électronique (cette analyse s'applique à tous les modes de paiement mobile). Enfin, la section 7 renferme certaines observations finales.

2. Étape de transition : deux modes de paiement de commerce mobile

Comme nous l'avons mentionné à la partie 1 du présent rapport (voir la section 3 de la partie 1), les opérations bancaires et les achats en ligne ne relèvent pas de la portée de notre étude parce que l'appareil mobile constitue dans ces cas l'intermédiaire utilisé pour effectuer l'opération sans y être essentiel. Il s'agit toutefois d'une étape de transition importante dans la société, puisqu'elle aide les gens à se familiariser avec l'idée d'effectuer des opérations financières (p. ex. payer une facture ou acheter un article) en utilisant un téléphone au lieu d'un ordinateur.

Un deuxième mode de paiement, qui s'inscrit également dans la catégorie du commerce mobile, mérite que nous nous l'analysions brièvement en raison de sa popularité croissante : la facturation par l'entreprise de télécommunications mobiles. Selon ce mode de paiement, l'appareil mobile est plus essentiel (l'utilisateur doit avoir un appareil mobile pour conclure un contrat avec l'entreprise), mais le règlement se fait de façon non classique (l'utilisateur « achète » un article en demandant que son prix soit ajouté à sa prochaine facture de téléphonie). Ce mode de paiement requiert la conclusion d'une entente commerciale au préalable entre l'entreprise de télécommunications mobiles et le commerçant.

2.1 Opérations bancaires ou achats en ligne au moyen d'un navigateur mobile donnant accès à un site Web

Les opérations bancaires ou les achats effectués en ligne au moyen d'un navigateur mobile sur un téléphone intelligent ou une tablette se font essentiellement de la même façon qu'au moyen d'un ordinateur portatif ou de bureau (entre autres changements mineurs, mentionnons l'adaptation à un écran plus petit ou les pages Web spéciales conçues expressément pour les appareils mobiles). La seule différence notable tient au fait que l'opération peut se faire n'importe où et n'importe quand (par le simple fait que l'utilisateur a plus de chances d'avoir sur lui son appareil mobile qu'un ordinateur de bureau ou même un ordinateur portatif). Toutefois, comme nous l'avons mentionné précédemment, cette façon de faire aide les consommateurs à se familiariser avec l'idée de payer une facture ou de faire un achat « en utilisant un appareil mobile » au lieu d'un ordinateur (même si la marche à suivre est la même, par exemple la saisie d'un numéro de carte de crédit et de la date d'expiration sur un formulaire en ligne).

Comme le processus est identique, il est assez logique que les considérations en matière de sécurité et de protection de la vie privée soient similaires : les failles du navigateur peuvent entraîner la perte ou une utilisation abusive des renseignements et permettre le téléchargement d'un logiciel malveillant dans l'appareil. Un facteur atténuant, par rapport aux ordinateurs de bureau ou portatifs, tient au fait que les applications sont compartimentées sur certaines plateformes d'appareils mobiles, par exemple Android, afin d'éviter qu'une application puisse voir (ou corrompre) le traitement ou les données d'autres applications. Cette précaution permettrait de limiter les dommages susceptibles de découler des failles d'un navigateur. En revanche, si le logiciel malveillant téléchargé permet au fraudeur d'accroître ses privilèges (p. ex. en tirant parti du fait que l'utilisateur a « rooté » ou débridé son téléphone pour éliminer certaines restrictions touchant le téléchargement et la configurabilité des logiciels), n'importe quel élément se trouvant sur le téléphone pourra par la suite être volé, modifié ou détruit.

2.2 Facturation par l'entreprise de télécommunications mobiles

Dans les systèmes de paiement à l'entreprise de télécommunications mobiles, le prix d'un article acheté figure sur la facture de téléphonie suivante. L'entreprise fait alors office d'établissement de crédit (c'est-à-dire qu'elle paie le commerçant au moment de l'achat et reçoit l'argent du client au cours du cycle de facturation suivant). En pareil cas, le client n'utilise aucun instrument de paiement classique (p. ex. une carte de crédit ou de débit) pour faire l'achat. Un nombre croissant de tiers concluent des ententes avec des entreprises de télécommunications pour mettre en place cette méthode de paiement (p. ex. Google permet de porter sur la facture de téléphonie mobile d'un client les achats effectués au moyen d'un

appareil Android pour les réseaux pris en charge[45] et BlackBerry World a récemment conclu une entente similaire[46] avec Wind Mobile).

Les données volumineuses et l'utilisation de traitements analytiques pourraient susciter des préoccupations en matière de protection de la vie privée dans le cas des paiements faits à une entreprise de télécommunications mobiles, car celle-ci en saura beaucoup plus sur ses clients que si elle ne s'occupait pas de la facturation (p. ex. historique détaillé des achats et identité des commerçants visés) et pourrait par le fait même, à dessein ou par accident, utiliser les renseignements de façon abusive (p. ex. en les communiquant à d'autres à des fins de marketing).

Les problèmes touchant les consommateurs ne se limitent toutefois pas à la protection de la vie privée. Les paiements à une entreprise de télécommunications mobiles suscitent une autre préoccupation du fait qu'aucune loi fédérale (à tout le moins aux États-Unis[47] et au Canada[48]) n'offre à l'heure actuelle aux clients une protection en cas de différend concernant les frais imposés de façon frauduleuse ou sans autorisation sur les factures de ce type d'entreprise. En pareil cas, les clients doivent s'en remettre aux modalités de l'entente conclue avec leur entreprise ou à sa bonne volonté (voir le compte rendu de l'atelier de la Federal Trade Commission (FTC) des États-Unis[49], p. 8. Cet état de choses a entraîné une augmentation du « bourrage de factures » (en anglais *cramming),* pratique mise en évidence pour la première fois il y a quelques années sur la plateforme de facturation pour la téléphonie filaire[50]. Selon cette pratique, des tiers inscrivent frauduleusement des frais sur les factures qu'une entreprise de télécommunications mobiles envoie à ses clients dans l'espoir qu'ils acquitteront leur facture mensuelle sans les remarquer. D'après les recommandations formulées dans le compte rendu de l'atelier de la FTC sur la question, il y aurait notamment lieu en pareil cas d'autoriser les consommateurs à bloquer tous les frais de tiers sur leur compte de téléphonie mobile et mettre en place une procédure uniforme et clairement définie à l'intention des consommateurs désireux de contester des frais douteux et d'obtenir un remboursement (p. 8). Selon les auteurs du rapport, on pourrait obliger les entreprises de télécommunications mobiles [traduction] « à normaliser et à mettre en évidence les frais de tiers sur les factures en indiquant clairement leur raison d'être, le nom du fournisseur ou du commerçant à l'origine de ces frais et le bien ou le service fourni » (p. 9).

---

[45] *Google Play*, « Purchase with carrier billing ». Voir http://support.google.com/googleplay/bin/answer.py?hl=en&answer=167794&topic%20=1046%20718&ctx=topic (consulté le 8 avril 2013).

[46] I. Hardy, « WIND Mobile goes live with BlackBerry World carrier billing », *MobileSyrup*, 1er avril 2013. Voir http://mobilesyrup.com/2013/04/01/wind-mobile-goes-live-with-blackberry-world-carrier-billing/ (consulté le 30 avril 2013).

[47] U.S. Federal Trade Commission (FTC), Division of Financial Practices (D. Pozza, P. Poss, J. Chen et coll.), *Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments*, rapport à l'intention du personnel de la FTC, mars 2013. Voir http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (consulté le 5 avril 2013).

[48] Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), *Vous avez des droits. Renseignements sur vos services téléphoniques locaux de résidence*, section « Contestation des frais de téléphone ». Voir http://www.bell.ca/web/common/fr/all_regions/pdfs/wireline/SCR_Final.pdf (consulté le 10 mai 2013).

[49] U.S. Federal Trade Commission (FTC), Division of Financial Practices (D. Pozza, P. Poss, J. Chen et coll.), *Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments*, rapport à l'intention du personnel de la FTC, mars 2013. Voir http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (consulté le 5 avril 2013).

[50] U.S. Federal Communications Commission (FCC), document infographique sur le bourrage de factures. Voir http://www.ftc.gov/os/2011/12/111227crammingcomment.pdf (consulté le 8 avril 2013).

Le bourrage de factures suscite de vives inquiétudes, car de nombreux consommateurs ignorent que des tiers peuvent inscrire des frais sur leur facture de téléphonie mobile, alors qu'ils ne leur ont pas communiqué les données d'une carte de crédit ni d'autre information de paiement (p. 10). De plus, ces frais peuvent être indiqués sur la facture en tant que « frais de service », « autres frais », « messagerie vocale », « serveur de messagerie », « forfait » ou « adhésion » (il peut s'agir d'un bourrage de factures si ces frais n'ont pas été autorisés ou que le coût a été falsifié) et qu'ils peuvent donc passer inaperçus indéfiniment[51].

3. Paiement mobile à un terminal de point de vente NFC

Dans le paiement mobile à un terminal de point de vente NFC, l'utilisateur a un appareil mobile équipé d'une puce de communication en champ proche et d'un ou de plusieurs instruments de paiement (p. ex. des applications de carte de crédit ou de débit, des cartes de fidélité, de rabais ou de membre, des cartes prépayées et des coupons). Le commerçant a un terminal au point de vente sans contact devant lequel les utilisateurs peuvent placer leur appareil NFC pour effectuer des opérations de paiement.

Trois points vulnérables des opérations de paiement NFC

Le paiement mobile NFC comporte au moins trois points vulnérables, dont deux sont communs aux cartes de crédit ou de débit sans contact : il est possible que le terminal PDV (généralement la borne de lecture) soit corrompu pour une raison quelconque et qu'il y ait une brèche dans le canal entre l'appareil mobile et une borne de lecture légitime (p. ex. dans les ondes). Troisièmement, la différence entre les paiements mobiles NFC (comparativement aux paiements NFC effectués au moyen d'une carte sans contact) tient au fait que l'appareil proprement dit peut subir des attaques de plusieurs façons.

Dans les sous-sections suivantes, nous examinons l'incidence de chacun de ces points vulnérables sur la sécurité et la protection de la vie privée.

3.1 Terminal PDV corrompu

On peut utiliser un appareil mobile NFC de trois façons différentes. Premièrement, il peut servir d'appareil actif (borne de lecture) qui envoie un signal de radiofréquence pour alimenter en énergie électrique un appareil passif (c.-à-d. sans source d'alimentation telle qu'une pile) pour lui permettre de répondre aux messages. C'est le mode employé lorsque l'on place un téléphone près d'une étiquette NFC sur une affiche ou un babillard pour obtenir davantage de renseignements que ceux fournis dans le texte de l'affiche (p. ex. une description supplémentaire, de l'information sur le prix ou un lien conduisant à un site Web).

Deuxièmement, l'appareil mobile peut être un appareil passif, qui reçoit un signal d'une borne de lecture active externe. On emploie l'expression « mode émulation de cartes » parce que l'appareil ressemble exactement à une carte sans contact ordinaire pour la borne de lecture (p. ex. un terminal PDV). C'est le mode utilisé pour les paiements mobiles.

[51] Ibid.

Enfin, l'appareil mobile et l'appareil externe sont des appareils actifs qui s'envoient mutuellement des signaux. Par exemple, c'est le mode utilisé lorsque l'on entrechoque deux téléphones pour échanger des cartes professionnelles.

En mode émulation de cartes, l'appareil est passif et attend un message d'une borne de lecture externe. Cette situation rend parfois l'appareil vulnérable parce que cette borne peut être corrompue ou même entièrement factice (p. ex., il pourrait s'agir d'une borne de lecture construite par un fraudeur à des fins malveillantes et maquillée en terminal PDV). Ces fausses bornes de lecture peuvent transmettre à l'appareil mobile des messages qui semblent valides, si bien que l'appareil détecte une opération de paiement apparemment légitime et transfère les fonds du compte de l'utilisateur à la borne de lecture. Pour les paiements de valeur élevée (50 $ ou plus), l'utilisateur doit parfois donner une confirmation supplémentaire (peut-être simplement appuyer sur un bouton « OK »), si bien que ce type de fraude peut difficilement réussir. Mais, pour les montants peu élevés (quelques dollars), on peut contourner l'étape de la vérification (en particulier si l'authentifiant a été activé dans le portefeuille électronique).

Tout indique qu'il serait possible de commettre des fraudes de faible valeur au moyen d'une fausse borne de lecture (on utilise parfois le terme « subtilisation » [en anglais *skimming attack*] lorsque le fraudeur se tient près de différentes personnes, par exemple dans un autobus ou un wagon de métro bondé, et « subtilise » quelques dollars à chacun d'un) en utilisant un appareil mobile NFC. La preuve d'attaques similaires (subtilisation du numéro de la carte et de la date d'expiration) a été faite à plusieurs reprises dans le cas de cartes de crédit NFC (c.-à-d. sans contact)[52,53]. Il est également possible de subtiliser l'information de la carte de crédit stockée sur un appareil mobile (c.-à-d. en n'effectuant aucune opération de paiement) lorsque l'appareil est en mode émulation de cartes et que la puce NFC est activée. (Signalons que la subtilisation des données de la carte de crédit ne révèle pas le numéro de trois ou quatre chiffres [valeur de vérification de carte] indiqué au dos, ce qui limite le nombre d'endroits où les données subtilisées peuvent être utilisées pour faire des achats frauduleux.) Il est beaucoup plus difficile pour un fraudeur de corrompre le terminal PDV d'un commerçant véritable (même si le fraudeur peut être le commerçant lui-même!), par exemple en prélevant un montant légèrement supérieur à celui qui est affiché, mais ce type de fraude est certainement possible à tout le moins en théorie.

Les pochettes ou les étuis de sécurité comportant une doublure métallique peuvent protéger les cartes de crédit ou de débit contre les échanges forcés avec des bornes de lecture malveillantes, mais il serait fort probablement impossible d'utiliser ce type de protection avec les appareils mobiles, car on nuirait ainsi au fonctionnement normal du téléphone. En revanche, de nombreux téléphones NFC désactivent automatiquement la fonction NFC lorsque l'écran est éteint pour assurer une protection contre la subtilisation (mécanisme de protection que n'offrent pas les cartes sans contact). Signalons toutefois que cette pratique semble incompatible avec l'énoncé figurant dans le *Canadian NFC Mobile Payments Reference Model*[54] (p. 26) selon lequel un authentifiant par défaut permet d'effectuer des paiements même si l'appareil est en mode veille.

---

[52] *Snopes.com*, « Electronic Pickpocketing », 4 octobre 2012. Voir http://www.snopes.com/fraud/identity/pickpocket.asp (consulté le 22 mars 2013). Voir aussi http://www.youtube.com/watch?v=EKks3vfiy6Q

[53] D. Pauli, « Android app steals contactless credit card data », *SC Magazine*, 21 juin 2012. Voir http://www.scmagazine.com.au/News/305881,android-app-steals-contactless-credit-card-data.aspx (consulté le 22 mars 2013).

[54] Institutions financières canadiennes (participants à l'initiative de l'industrie), *Canadian NFC Mobile Payments Reference Model*, version 1.03, 14 mai 2012. Voir http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (consulté le 14 février 2013).

Les étiquettes NFC corrompues sont un sujet lié dans une certaine mesure au concept de borne de lecture corrompue. Une étiquette NFC est un appareil passif alimenté et lu par un appareil mobile fonctionnant en mode actif. Comme nous l'avons mentionné ci-dessus, on peut insérer ces étiquettes sur des affiches ou dans des lieux publics pour que l'utilisateur place son téléphone à proximité afin d'obtenir des renseignements supplémentaires (p. ex. la bande-annonce d'un film dont l'affiche fait la promotion). Toutefois, une technologie permettant aux utilisateurs de rédiger eux-mêmes des étiquettes pour automatiser des fonctions ou des tâches particulières suscite l'intérêt depuis quelque temps – l'étiquette renferme essentiellement une liste d'instructions (un script) que le téléphone exécute une à une[55,56]. Par exemple, lorsqu'un utilisateur quitte le travail et prend sa voiture pour rentrer chez lui, il peut modifier quelques réglages de son téléphone, notamment désactiver la connectivité Wi-Fi, activer Bluetooth, choisir le mode de sonnerie silencieux, modifier la luminosité de l'écran et lancer une application particulière. Il est possible de créer une étiquette NFC (ce qui nécessite uniquement une étiquette inscriptible et une application comme NFC Task Launcher) pour conserver toutes ces instructions; ensuite, l'utilisateur n'aura qu'à placer son téléphone près de l'étiquette pour déclencher automatiquement toutes ces actions[57].

Manifestement, s'il peut y avoir des bornes de lecture malveillantes, nous ne sommes pas à l'abri des étiquettes falsifiées. Ainsi, un fraudeur pourrait créer une étiquette NFC renfermant une série d'instructions qu'un utilisateur n'aurait pas données autrement, par exemple désactiver certains mécanismes de protection et visiter une page Web qui tire parti d'un bogue dans le navigateur permettant au fraudeur d'avoir accès aux données sur le téléphone[58]. Dans le contexte des paiements mobiles, un fraudeur pourrait donc être en mesure de créer une étiquette qui lance le portefeuille électronique et désactive la vérification pour les paiements de valeur élevée. Ce stratagème pourrait être utilisé en même temps qu'une fausse borne de lecture pour subtiliser des montants élevés à des gens se trouvant dans un autobus ou un wagon de métro bondé.

3.2 Canal corrompu entre un appareil mobile et un terminal PDV

Avec la communication en champ proche, les messages sont transmis par ondes hertziennes entre un appareil mobile et un terminal PDV. Le canal de transmission est très court (généralement moins de 10 cm, peut-être même de 0 cm si on passe le téléphone sur la borne de lecture), certains chercheurs ont examiné s'il est possible de commettre une fraude sur ce canal. Au nombre des types de fraudes étudiées, mentionnons l'interception, la corruption de données, la modification de données, l'insertion

[55] R. Whitwam, « How To Have Fun with Near Field Communication on Android », *Tested*, 27 avril 2011. Voir http://www.tested.com/tech/android/2234-how-to-have-fun-with-near-field-communication-on-android/ (consulté le 25 mars 2013).

[56] O. Kharif, « NFC Stickers Make Smartphones Smarter », *Bloomberg Businessweek: Technology*, 12 juillet 2012. Voir http://www.businessweek.com/articles/2012-07-12/nfc-stickers-make-smartphones-smarter (consulté le 25 mars 2013).

[57] R. Holly, « How to use NFC to automate your mobile routine », *geek.com*, 8 février 2012. Voir http://www.geek.com/articles/mobile/how-to-use-nfc-to-automate-your-mobile-routine-2012028/ (consulté le 25 mars 2013).

[58] S. Cowley, « NFC exploit: Be very, very careful what your smartphone gets near », *CNN Money*, 26 juillet 2012. Voir http://money.cnn.com/2012/07/26/technology/nfc-hack/index.htm (consulté le 25 mars 2013).

de données et une attaque par intermédiaire. Dans une étude[59], Kremer a présenté les conclusions suivantes (voir aussi les sections 2.1.2 et 2.2.1 de Kerschberger[60]).

- Un fraudeur possédant un niveau de compétences techniques faible ou moyen pourrait faire de l'interception sur le canal NFC au moyen d'un appareil offert dans le commerce, mais la qualité du signal en pareil cas varie en fonction d'un grand nombre de paramètres, notamment la géométrie de l'antenne de l'émetteur et du fraudeur, la qualité du récepteur et du décodeur de signal du fraudeur, le lieu où la fraude est commise (murs, métal, bruit ambiant, etc.) et la puissance du signal de l'appareil NFC du transmetteur. Il a été démontré dans certains cas que l'interception peut se faire à une distance pouvant atteindre 10 m par rapport à un dispositif d'émission actif (1 m s'il s'agit d'un dispositif d'émission passif).
- Il est relativement facile de corrompre des données (pour une personne possédant un niveau de compétences techniques faible ou moyen et utilisant un appareil offert sur le marché). Il s'agit dans les faits d'une attaque entraînant un refus de service où le fraudeur transmet un signal de brouillage afin que le récepteur légitime ne puisse comprendre le signal réel. Toutefois, dans une opération de paiement, on ne sait pas vraiment quel avantage un fraudeur pourrait en retirer.
- Il est possible que des données soient modifiées, selon le stratagème de modulation utilisé entre l'émetteur et le récepteur (p. ex. modulation par déplacement d'amplitude de 100 % ou de 10 %), mais on a alors besoin d'équipement perfectionné et d'un bon niveau de compétences techniques. Avec une modulation par déplacement d'amplitude de 100 %, le fraudeur ne peut modifier que quelques bits (un bit d'une valeur de 1 peut être remplacé par un bit d'une valeur de 0, mais uniquement s'il est précédé par un bit d'une valeur de 1; dans tous les autres cas, il est pratiquement impossible de modifier les bits). Avec une modulation de 10 %, le fraudeur peut en théorie modifier les bits de son choix (remplacer les 0 par des 1 et inversement). Signalons que l'utilisation des deux mécanismes de modulation (appelés type A et type B selon la norme ISO 14443[61]) est très répandue pour les opérations de paiement NFC.
- Il est relativement difficile d'insérer des données, car on doit avoir beaucoup de chance, utiliser un appareil perfectionné et posséder un bon niveau de compétences techniques. Comme il y a un protocole défini (un nombre fixe de messages déterminés) entre les appareils émetteur et récepteur, le fraudeur ne pourra insérer un message que si l'une des parties légitimes transmet très lentement son message légitime (p. ex. s'il y a un intervalle hors norme où le fraudeur peut glisser son message). Signalons que si la partie légitime commence à envoyer son propre message avant que le fraudeur ait terminé de transmettre le sien, les deux messages se chevaucheront et seront corrompus.

- Dans une attaque par intermédiaire, le fraudeur se place entre l'émetteur et le récepteur de manière à ce qu'ils aient l'impression de parler ensemble, alors qu'en réalité tous leurs messages

[59] J. Kremer, *NFC: Near Field Communication White Paper*, Jan Kremer Consulting Services. Voir http://jkremer.com/White%20Papers/Near%20Field%20Communication%20White%20Paper%20JKCS.pdf (consulté le 26 mars 2013).

[60] M. Kerschberger, « Near Field Communication: A survey of safety and security measures », Bachelorarbeit, Université technique de Vienne, 17 juillet 2011. Voir https://www.auto.tuwien.ac.at/bib/pdf_TR/TR0156.pdf (consulté le 26 mars 2013).

[61] Comité technique conjoint ISO/IEC n° 1, sous-comité n° 17, groupe de travail n° 8, *Cartes d'identification ISO/IEC 14443 – Cartes à circuit(s) imprimé(s) sans contact – Cartes de proximité*.

passent par le fraudeur (qui peut donc ajouter, supprimer ou modifier des messages à sa guise). Avec la technologie NFC, compte tenu de la très grande proximité de l'émetteur et du récepteur et du fait que l'appareil actif envoie constamment un signal pour alimenter l'appareil passif, il est pratiquement impossible pour un fraudeur de supprimer les messages transmis, d'en insérer de nouveaux ou de modifier des messages légitimes en passant inaperçu.

En ce qui a trait à l'interception, Berkes[62] a examiné dans son mémoire présenté à l'Université de Waterloo la possibilité d'obtenir des renseignements sensibles grâce à une analyse chronologique des messages envoyés par un émetteur à un récepteur sur un canal NFC. Il en a conclu que ce type d'attaque est possible (dans le cas d'un fraudeur utilisant un appareil offert sur le marché et possédant un bon niveau de compétences techniques). En observant seulement les messages envoyés et reçus dans la communication sans contact (pourvu que l'on possède une connaissance raisonnable du jeu d'instructions et de la vitesse du microprocesseur de la carte à puce, information qui figure dans les spécifications accessibles au public), il est parfois possible de déduire quel calcul est effectué dans la puce, voire d'obtenir certaines données confidentielles cachées (p. ex. des segments d'une clé privée). Certaines données se trouvant dans l'élément de sécurité (Voir « élément de sécurité, section 3.3.1.1 ci-après) d'un téléphone mobile pourraient donc être vulnérables à l'interception par ondes hertziennes au moyen d'un simple appareil passif.

L'attaque par relais (parfois appelée « attaque par trou de ver ») constitue une dernière attaque par canal qui mérite d'être abordée. Elle est assez similaire à l'interception et à l'attaque par intermédiaire, mais vise un objectif différent : le fraudeur n'essaie pas de prendre connaissance du contenu des messages (c'est le cas pour ces deux autres types d'attaque) ni d'insérer, de supprimer ou de modifier des messages entre les parties légitimes (comme pour les attaques par intermédiaire). En fait, il essaie d'intercepter des messages valides d'un émetteur et de les acheminer (relayer) à une certaine distance afin que le récepteur à distance pense que l'émetteur se trouve physiquement à proximité. L'attaque se déroule selon le scénario suivant. Un complice du fraudeur se tient près d'une personne choisie au hasard qui a un appareil de paiement mobile doté de la technologie NFC (Alex) et relaie les signaux entre Alex et Robert, qui se trouve à une certaine distance d'un terminal PDV NFC. Ignorant ce qui se passe, Alex paie l'achat de Robert. (Ce type d'attaque peut être particulièrement efficace pour les opérations de faible valeur qui ne nécessitent pas la confirmation de l'utilisateur.)

Le chercheur suisse Tomas Rosa a montré que les attaques par relais sont possibles lorsque le fraudeur utilise un appareil, des logiciels et d'un appareil informatique généralement accessibles[63].

La conclusion concernant les attaques par canal NFC est la suivante : bien qu'il soit très difficile de lancer certaines attaques (voire impossible dans un contexte pratique), par exemple la modification de messages par un intermédiaire, une personne possédant un niveau de compétence technique faible ou moyen et utilisant des outils offerts sur le marché peut mener à bien assez facilement d'autres types d'attaques, par exemple l'interception, la corruption des données et le relais de messages. Même dans les cas faciles, le fraudeur (ou un complice) doit cependant se trouver physiquement très près de la victime (généralement à 50 cm ou moins), ce qui peut souvent dans le monde réel limiter le risque

[62] J. Berkes, *Side-Channel Monitoring of Contactless Java Cards*, mémoire de maîtrise, Département de génie électrique et informatique, Université de Waterloo, 2008. Voir http://www.berkes.ca/archive/jb-thesis-final-electronic.pdf (consulté le 26 mars 2013).

[63] T. Rosa, *RFID Wormholes: The Case of Contactless Smartcards »,* SmartCard Forum, Prague, en République tchèque, 2011. Voir http://crypto.hyperlink.cz/files/rosa_wormhole_v1a.pdf (consulté le 26 mars 2013).

inhérent aux opérations de paiement pour l'utilisateur. Signalons que les mécanismes cryptographiques, par exemple le chiffrement des messages, peuvent aider à assurer une protection contre l'interception, mais non prévenir la corruption de données ou les attaques par relais.

3.3 Appareil mobile corrompu

Pour comprendre certains risques d'atteinte à la sécurité et à la vie privée liés aux appareils mobiles NFC, il est utile de se pencher sur l'architecture du segment paiement de l'appareil – sur la nature des différents composants et leurs interactions. Nous décrirons ensuite différents types d'attaques possibles.

3.3.1 Architecture de l'appareil mobile NFC

Un appareil mobile NFC, par exemple un téléphone intelligent, est composé de matériel et de logiciels qui permettent d'effectuer des opérations de paiement. Le matériel comprend la puce de l'élément de sécurité et une puce NFC, tandis que les logiciels incluent un portefeuille électronique et au moins une application de paiement (et les données connexes).

3.3.1.1 Élément de sécurité

L'élément de sécurité constitue un composant essentiel pour les paiements mobiles. Il s'agit d'une puce de stockage sur une carte intelligente qui résiste à la falsification (comportant parfois des certifications reliées aux critères communs et aux FIPS) permettant de stocker les applications de paiement et l'information sur le compte. D'après Elenkov[64] :

> [traduction] Une carte intelligente est essentiellement un environnement informatique minimaliste complet sur une seule puce, comprenant une unité centrale de traitement, une mémoire ROM, une mémoire EEPROM, une mémoire RAM et un port d'entrée-sortie. Les cartes récentes sont aussi équipées de coprocesseurs cryptographiques mettant en œuvre des algorithmes courants comme DES, AES et RSA. Les cartes intelligentes utilisent différentes techniques pour résister à la falsification afin qu'il soit très difficile d'extraire des données en désassemblant ou en analysant la puce. Ces cartes préprogrammées utilisent un système d'exploitation multi-applications qui tire parti des caractéristiques de protection de la mémoire du matériel pour que chaque application soit la seule à avoir accès à ses propres données. Afin de contrôler l'installation des applications et leur accès (facultatif), une clé de chiffrement doit être utilisée pour chaque opération.

L'élément de sécurité peut donc renfermer plusieurs applications de paiement et il est conçu de sorte que les applications soient compartimentées et qu'un tiers ne puisse extraire facilement les données des applications installées.

L'élément de sécurité se compose de domaines de sécurité et de domaines de sécurité supplémentaires distincts. Un domaine de sécurité est un contexte de confiance au sein de l'élément de sécurité : il comprend une série d'opérations de chiffrement, de communication et de gestion des données auxquelles on peut accéder uniquement au moyen de matériel à clé unique et qui sont contrôlées par une série d'autorisations particulières[65]. Une application de paiement sur l'élément de sécurité demande

---

[64] N. Elenkov, *Accessing the embedded secure element in Android 4.x*, 22 août 2012. Voir http://nelenkov.blogspot.ca/2012/08/accessing-embedded-secure-element-in.html#!/2012/08/accessing-embedded-secure-element-in.html (consulté le 12 mars 2013).

[65] Définition affichée dans le site Web de la société Sequent; voir http://www.sequent.com/glossary/s (consulté le 12 mars 2013).

des services cryptographiques (p. ex. le chiffrement ou le déchiffrement, la signature numérique ou l'authentification des données) en sollicitant le domaine de sécurité associé. Le propriétaire d'un élément de sécurité (p. ex. l'exploitant de réseau mobile) gère une série d'applications et les domaines de sécurité correspondants sur l'élément de sécurité. En outre, le propriétaire peut créer une portion de l'élément de sécurité et en céder le contrôle à un autre fournisseur de services NFC; cette portion renfermera l'application du fournisseur de services et un contexte de sécurité pour cette application. L'expression « domaine de sécurité supplémentaire » est employée pour désigner ce contexte de sécurité contrôlé par un tiers. On trouvera dans le document de Global Platform[66] une analyse approfondie des domaines de sécurité.

Signalons que le terme « propriétaire » utilisé dans le contexte de l'élément de sécurité n'est pas nécessairement synonyme de « partie responsable ». Le propriétaire de l'élément de sécurité est l'entité qui a en sa possession cet élément avant la livraison au consommateur et qui a l'autorité voulue pour déterminer les applications et les données qu'il renfermera. Bien entendu, cette autorité lui confère une certaine responsabilité (p. ex. il devrait lui incomber de rétablir le niveau de fonctionnalité attendu de l'utilisateur si l'élément de sécurité cesse de fonctionner, fonctionne mal ou corrompt des données stockées). Toutefois, si le contrôle d'une portion de l'élément de sécurité est cédé à une autre partie (c.-à-d. un domaine de sécurité supplémentaire), une certaine responsabilité doit également lui être cédée. Ce qui complique encore plus les choses, même si le propriétaire de l'élément de sécurité détermine les applications et les données que renfermera cet élément, il ne voit pas ces données (qui sont chiffrées au moyen d'une clé qui n'est connue que de l'émetteur de l'application). Par conséquent, la responsabilité de contenu réel des données de l'élément de sécurité, qui peut renfermer des renseignements personnels des consommateurs (entièrement à la discrétion de l'émetteur de l'application), doit reposer sur l'émetteur de l'application. C'est pourquoi le propriétaire de l'élément de sécurité n'est qu'une des parties qui peuvent avoir des obligations relativement à la responsabilité.

Fait intéressant, l'élément de sécurité peut occuper trois emplacements différents dans un appareil mobile[67]. Il peut être intégré dans le téléphone mobile proprement dit, mis en œuvre sur une carte de circuit intégré universelle (UICC – *Universal Integrated Circuit Card*), souvent appelée « carte SIM » (*Subscriber Identity Module*), ou bien mis en œuvre sur une carte mémoire MicroSD. La première méthode est simple du point de vue conceptuel (l'utilisateur achète un téléphone NFC qui comporte déjà un élément de sécurité), mais elle présente au moins deux inconvénients : comme l'élément de sécurité doit être personnel, il faudra l'enregistrer et le personnaliser après l'achat de l'appareil; par la suite, si l'utilisateur souhaite changer d'appareil, il faudra transférer dans le nouvel appareil toutes les applications et les données de l'élément de sécurité, désactiver l'élément de sécurité de l'ancien appareil et peut-être supprimer toutes ses données de façon sécuritaire.

Les deuxième et troisième méthodes (carte UICC ou MicroSD) comportent un avantage du fait qu'elles permettent la transférabilité entre deux appareils mobiles : si l'utilisateur change d'appareil, il lui suffit d'enlever la carte UICC ou MicroSD de l'ancien appareil et de l'insérer dans le nouveau. Toutefois, dans le cas de la troisième méthode, les appareils mobiles ne comportent pas tous de fente pour carte MicroSD, ce qui limite manifestement les possibilités de déploiement.

---

[66] Global Platform, *Card Specification,* Version 2.2, mars 2006. Voir http://www.win.tue.nl/pinpasjc/docs/GPCardSpec_v2.2.pdf (consulté le 15 mars 2013).

[67] D. Ericsson, *The role of SIM OTA and the Mobile Operator in the NFC environment*, livre blanc de SmartTrust, avril 2009. Voir http://www.paymentscardsandmobile.com/research/reports/SIM-OTA-Mobile-Operator-role-NFC.pdf (consulté le 12 mars 2013).

La question de l'emplacement de l'élément de sécurité revêt une grande importance, car elle définit généralement à qui il appartient. Si cet élément est intégré dans l'appareil mobile, il appartient au fabricant. S'il est mis en œuvre sur une carte UICC, il appartient à l'exploitant du réseau mobile (qui fournit généralement la carte à ses clients). Enfin, si l'élément de sécurité est mis en œuvre sur une carte MicroSD, il appartient à celui qui donne ou vend la carte mémoire à l'utilisateur (p. ex. un émetteur de cartes de crédit ou une banque pourrait décider de fournir directement à ses clients des cartes MicroSD renfermant sa propre application de paiement). Comme le propriétaire de l'élément de sécurité choisit les applications de paiement qui peuvent y être installées, la question de la propriété revêt une importance stratégique pour divers acteurs de l'industrie des paiements, car elle détermine en fin de compte les instruments auxquels aura accès un utilisateur donné. Toutefois, comme nous l'avons déjà signalé, les acteurs de cette industrie qui souhaitent être propriétaires de l'élément de sécurité doivent savoir que ce rôle comporte inévitablement une certaine part de responsabilité.

On ne sait pas avec certitude si l'emplacement de l'élément de sécurité a des répercussions particulières sur la protection de la vie privée, puisque le propriétaire de l'élément de sécurité n'a pas accès aux données de l'application de paiement peu importe son emplacement (il a droit de regard sur les applications à installer, mais les données ne peuvent être vues que par l'émetteur de l'application). Il pourrait toutefois y avoir de légères répercussions sur le plan de la sécurité. Plus précisément, le risque de perte ou de défaillance pourrait être accru dans le cas d'une carte UICC ou MicroSD que pour l'appareil mobile (simplement en raison de leur petite taille); en revanche, il serait de toute évidence plus facile pour un voleur de s'emparer d'un téléphone que d'emprunter un téléphone, d'enlever la carte UICC ou MicroSD et de rendre le téléphone sans se faire prendre.

3.3.1.2 Puce NFC

La puce NFC (« contrôleur NFC ») est un composant matériel et logiciel (circuit intégré et micrologiciel) qui contrôle les signaux radio NFC transmis et reçus par l'antenne[68]. Elle est reliée à l'élément de sécurité ainsi qu'à d'autres applications NFC d'origine (ne servant pas au paiement) placées ailleurs sur l'appareil mobile[69]. Plus précisément, le contrôleur NFC et l'élément de sécurité sont des puces séparées qui communiquent sur un canal (un ou deux fils) au moyen d'un protocole normalisé. Si l'élément de sécurité est mis en œuvre sur une carte UICC, le protocole entre le contrôleur NFC et cet élément est appelé « SWP » (*Single Wire Protocol*[70]). En revanche, si l'élément de sécurité se trouve dans l'appareil ou sur une carte MicroSD, le protocole entre le contrôleur NFC et l'élément est appelé « NFC-WI » (*NFC Wired Interface*[71] ou « S2C[72] »).

[68] Définition affichée dans le site Web de la société Sequent; voir http://www.sequent.com/glossary/n (consulté le 15 mars 2013).

[69] Inside Secure, *Opening the NFC stack to Java and native applications*, document d'information de l'entreprise, novembre 2010. Voir http://www.insidesecure.com/content/download/1095/12802/version/6/file/WHITE%20PAPER_NEW%20CHARTE-3.pdf (consulté le 15 mars 2013).

[70] *Wikipedia, the Free Encyclopedia*, « Single Wire Protocol ». Voir http://en.wikipedia.org/wiki/Single_Wire_Protocol (consulté le 15 mars 2013).

[71] *Wikipedia, the Free Encyclopedia*, « NFC-WI ». Voir http://en.wikipedia.org/wiki/NFC-WI (consulté le 15 mars 2013).

[72] CommTech Knowledge, *NFC-Near Field Communication: General Architecture of NFC Enabled Mobile Phones*. Voir http://mp-nfc.org/nfc_near_field_communication_architecture.html (consulté le 15 mars 2013).

Signalons que le contrôleur NFC peut être relié à plusieurs éléments de sécurité (p. ex. des éléments présents en même temps sur la carte UICC, la carte MicroSD et le téléphone)[73]. Sur l'appareil mobile, un module logiciel appelé « contrôleur hôte » est relié au contrôleur NFC (par l'interface HCI [*Host Controller Interface*]) et les éléments de sécurité (par l'interface ISO 7816[74]). Entre autres choses, le contrôleur hôte définit les modes opératoires du contrôleur NFC et établit une connexion entre le contrôleur NFC et l'élément de sécurité[75], si bien qu'il est responsable de la gestion de tout conflit éventuel si l'appareil comporte plus d'un élément de sécurité (p. ex. il doit s'assurer qu'un seul élément de sécurité est actif à tout moment).

La figure 2 ci-après montre les divers composants associés au contrôleur (illustration tirée du site Web de CommTech[76]).

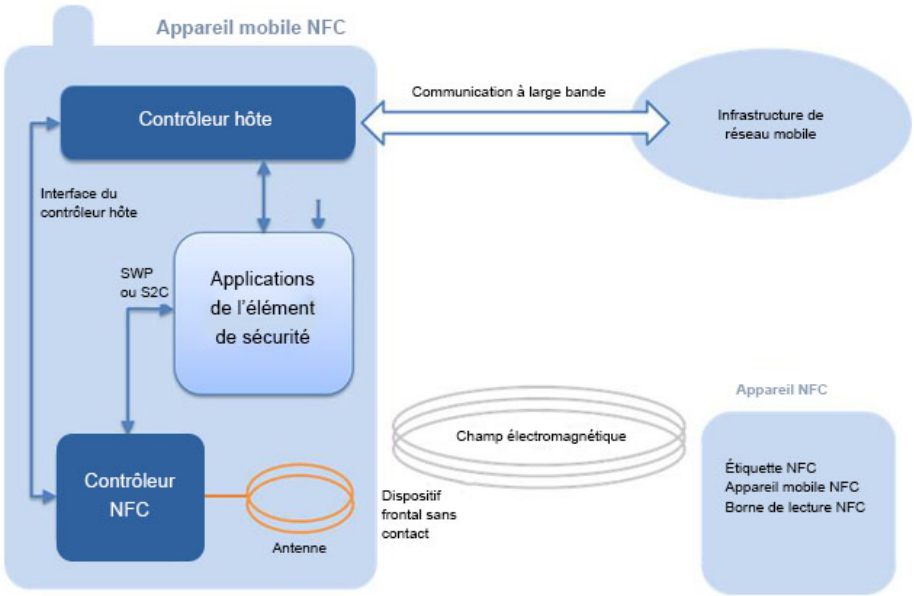

Figure 2. Architecture générale des téléphones mobiles NFC

Dans les paragraphes qui suivent, nous décrivons brièvement le déroulement d'une opération de paiement NFC.

- Étape du provisionnement : Le canal NFC n'est pas utilisé à l'étape du provisionnement (téléchargement de l'application et des données de la marque de paiement ou de la banque dans le portefeuille électronique et l'élément de sécurité par l'intermédiaire de l'exploitant du réseau

[73] *Ibid.*

[74] Comité technique conjoint ISO/IEC n° 1, Sous-comité n° 17, *ISO/IEC 7816 : Cartes d'identification – cartes à circuit(s) imprimé(s) sans contact.*

[75] CommTech Knowledge, *NFC-Near Field Communication: General Architecture of NFC Enabled Mobile Phones*. Voir http://mp-nfc.org/nfc_near_field_communication_architecture.html (consulté le 15 mars 2013).

[76] *Ibid.*

mobile). Ce téléchargement ne passe pas par le contrôleur NFC. Il utilise plutôt le réseau mobile sans fil jusqu'au contrôleur hôte en passant par l'interface ISO 7816 pour atteindre l'élément de sécurité. À cette étape, les applications et les données sont placées physiquement sur les différents éléments de sécurité et toutes les mesures requises pour leur permettre d'effectuer les paiements mobiles sont mises en place.

- Étape de la configuration des paiements : L'application du portefeuille électronique interroge l'élément de sécurité (en passant par le contrôleur hôte et l'interface ISO 7816) pour déterminer les applications de paiement qui sont présentes afin de pouvoir afficher ces choix à l'intention de l'utilisateur. Lorsque l'utilisateur choisit un instrument de paiement en particulier (p. ex. une carte de débit MasterCard), l'application du portefeuille électronique ordonne au contrôleur NFC (en passant par le contrôleur hôte et l'interface HCI) d'établir le contact avec la carte de débit MasterCard sur un élément de sécurité particulier (en utilisant des identifiants particuliers pour cet instrument de paiement et cet élément de sécurité). Le contrôleur NFC met ensuite en mode arrêt tous les autres éléments de sécurité qui pourraient se trouver sur l'appareil (en envoyant un signal au moyen du protocole SWP ou S2C), met en mode communication en cours l'élément de sécurité qui renferme l'application de la carte de débit MasterCard (en envoyant un signal au moyen du protocole SWP ou S2C) et établit le contact avec cet instrument de paiement en envoyant à l'élément de sécurité un message qui renferme l'identifiant de l'application et lui indique de se préparer (ce qui, en fait, dit à l'application de se mettre à l'écoute et à toutes les autres applications de cet élément de sécurité de ne pas tenir compte des messages suivants). Enfin, le contrôleur NFC indique à cet élément de sécurité qu'il est en communication avec le monde extérieur (en envoyant un signal au moyen du protocole SWP ou S2C).
- Étape du paiement : Les messages du terminal PDV sans contact (plus précisément d'une application MasterCard sur un PC relié à ce terminal) parcourent cette très courte distance par ondes hertziennes en utilisant le protocole ISO 14443 jusqu'au dispositif frontal sans contact sur le téléphone et sont captés par l'antenne, convertis du format analogique au format numérique, puis acheminés par le contrôleur NFC au moyen du protocole SWP ou S2C directement à l'application de la carte de débit MasterCard sur l'élément de sécurité. De même, les messages de l'application sont envoyés dans la direction opposée au terminal PDV. N'importe quelle autre application sur l'appareil mobile peut s'inscrire pour recevoir un avis lorsqu'une opération NFC est effectuée[77], mais cet avis indique uniquement que l'opération se fait (sans fournir les données transmises dans le message). De plus, pour pouvoir recevoir ce type d'avis, l'application doit être soumise à une vérification par le cadre de contrôle d'accès pour l'application de l'élément de sécurité utilisée pour l'opération[78].
- Après l'opération de paiement : Le contrôleur NFC reconnaît que le flux des messages NFC est terminé (ou que l'antenne se trouve hors de la portée du terminal PDV) et met l'élément de sécurité en mode arrêt. De plus, l'utilisateur peut fermer l'application de la carte de débit MasterCard ou du portefeuille électronique.

Les deux prochaines sous-sections portent sur les logiciels de paiement sur un appareil mobile NFC.

[77] BlackBerry Support Community Forums, *BlackBerry 10 – NFC Card Emulation*, 2 novembre 2012. Voir http://supportforums.blackberry.com/t5/Native-Development/BlackBerry-10-NFC-Card-Emulation/ta-p/1940867 (consulté le 20 mars 2013). Voir aussi *NFC Primer for Developers*, 14 février 2012, http://supportforums.blackberry.com/t5/Java-Development/NFC-Primer-for-Developers/ta-p/1334857 (consulté le 20 mars 2013).

[78] *Ibid.*

3.3.1.3 Portefeuille électronique

Comme nous l'avons mentionné à la partie 1 du présent rapport, un portefeuille électronique est une application qui gère les différents instruments de paiement et interfaces avec le payeur (p. ex. pour lui permettre de choisir l'instrument de paiement particulier à utiliser au moment d'un achat). Un certain nombre d'organisations ont choisi de devenir des fournisseurs de portefeuille électronique (dans le cadre de leurs activités commerciales), notamment Google, Isis, Visa, MasterCard et différentes banques. Comme on pouvait s'y attendre, cette concurrence a donné lieu à différents types d'applications, soit les portefeuilles mobiles, numériques et hybrides[79].

- Un portefeuille électronique mobile est une application sur le téléphone qui gère les instruments de paiement. Il est généralement installé par l'utilisateur (mais il peut aussi être déjà installé au moment de l'achat de l'appareil) et il faudra le déplacer ou le transférer d'une façon quelconque si l'utilisateur change d'appareil par la suite. Exemple : le portefeuille électronique mobile Rogers-CIBC.
- Un portefeuille électronique numérique (appellation qui porte à confusion, car toutes les applications logicielles sont numériques) est une application hébergée à l'extérieur du téléphone, par exemple sur un serveur ou dans le nuage. Ce portefeuille électronique n'est pas installé par l'utilisateur; on y a accès par le Web en demandant une connexion. Si l'utilisateur change d'appareil par la suite, il n'a rien à faire pour continuer de l'utiliser. Exemple : le portefeuille électronique PayPal Digital.
- Un portefeuille électronique hybride est un portefeuille installé sur un serveur ou dans le nuage dont un composant ou un segment se trouve sur le téléphone. L'utilisateur doit installer ce segment, qui permet d'automatiser la connexion au segment hébergé sur le serveur ou dans le nuage, si bien que l'utilisateur n'a pas à savoir que le portefeuille comporte deux segments. Exemple : le portefeuille électronique Google.

Les portefeuilles électroniques (mobiles, numériques ou hybrides) ont évolué et offrent maintenant des services qui vont bien au-delà de la simple gestion des instruments de paiement, par exemple la gestion du portefeuille financier de l'utilisateur, le suivi et l'utilisation des points de récompense ou de fidélité, la réception des offres spéciales de commerçants ainsi que le stockage des reçus numériques et de l'information sur les garanties[80]. Tous ces renseignements sensibles sont généralement protégés au moyen d'un mot de passe ou d'un numéro d'identification personnel (NIP) que l'utilisateur saisit pour déverrouiller le portefeuille électronique. Mentionnons à cet égard qu'au moins une entreprise (Inside Secure) permet la coexistence de plusieurs portefeuilles électroniques sur le même appareil mobile[81], de sorte que la quantité de renseignements sensibles sur un seul appareil mobile peut être encore plus importante.

---

[79] M. Crowe et E. Tavilla (Federal Reserve Bank of Boston), *Mobile Phone Technology: "Smarter" Thank We Thought: How Technology Platforms are Security Mobile Payments in the U.S.,* 16 novembre 2012. Voir http://www.bos.frb.org/bankinfo/payment-strategies/publications/2012/mobile-phone-technology.pdf (consulté le 21 mars 2013).

[80] Visa, *Digital Wallet Security: Just "LOK" it*. Voir http://www.cimbbank.com.my/creditcard/index.php?ch=2&pg=14&ac=9&bb=attachment (consulté le 21 mars 2013).

[81] M. Ricknas, « Inside Secure Opens Door for Multiple Wallets on One Smartphone », *CIO Drilldowns*, 29 octobre 2012. Voir http://www.cio.com/article/720174/Inside_Secure_Opens_Door_for_Multiple_Wallets_on_One_Smartphone (consulté le 21 mars 2013).

3.3.1.4 Applications de paiement et authentifiant

Comme nous l'avons déjà mentionné dans la section précédente, les applications de paiement et les authentifiants (données), qui appartiennent à la marque de paiement et sont personnalisés pour l'utilisateur, sont téléchargés et installés sur l'élément de sécurité de l'appareil mobile au moment du provisionnement. En règle générale, le propriétaire de l'application de paiement ou des données et le propriétaire de l'élément de sécurité sont des entités différentes (p. ex. Visa possède l'application de paiement et Rogers possède la carte UICC renfermant l'élément de sécurité). Par conséquent, ces entités doivent conclure une entente avant que l'application et les données puissent être installées – autrement, les protections cryptographiques bloqueraient l'accès à l'élément de sécurité. D'autres instruments de paiement, qui sont téléchargés sur l'appareil mobile sans se trouver sur l'élément de sécurité (p. ex. des coupons et des cartes de fidélité, qui sont stockés dans la mémoire du portefeuille électronique), ne nécessitent pas ce type d'entente. L'utilisateur ou d'autres entités (p. ex. les commerçants) peuvent les installer à tout moment.

Il est possible de verrouiller les applications de paiement hébergées sur l'élément de sécurité. On a besoin d'un mot de passe ou d'un NIP pour les déverrouiller avant de les utiliser. En règle générale, l'application de portefeuille électronique permet d'assurer cette protection (car l'utilisateur peut choisir de verrouiller ou non chaque instrument de paiement[82]). Toutefois, le portefeuille électronique permet aussi généralement à l'utilisateur de choisir un authentifiant par défaut : [traduction] « Grâce à l'authentifiant par défaut, les utilisateurs finals peuvent effectuer le paiement tout en laissant l'appareil mobile en mode veille sans avoir à choisir manuellement un portefeuille électronique[83]. ».

Signalons que le NIP ou le mot de passe utilisés pour verrouiller des applications de paiement particulières ne sont pas ceux qui servent à verrouiller l'application de portefeuille électronique dans son ensemble (ils sont également différents du NIP, du mot de passe et des données biométriques qui permettent de verrouiller l'appareil mobile proprement dit). Plusieurs niveaux de protection sont donc possibles, mais l'utilisation d'un plus grand nombre de niveaux peut rendre l'expérience frustrante pour l'utilisateur.

3.3.2 Risques d'atteinte à la sécurité et à la vie privée sur l'appareil

Les risques d'atteinte à la sécurité et à la vie privée sur l'appareil mobile se divisent en deux grandes catégories, soit les attaques de matériel (nécessitant un accès physique à l'appareil ciblé) et les attaques de logiciel.

3.3.2.1 Attaques de matériel

Avec l'architecture décrite ci-dessus, les attaques physiques sont possibles : si un fraudeur met la main sur le téléphone d'une victime et qu'il connaît les interfaces HCI, SWP ou S2C et ISO 7816 (normalisées ou autrement accessibles au public), il peut placer des clips ou des sondes sur ces fils (voir, par exemple,

[82] Institutions financières canadiennes (participants à l'initiative de l'industrie), *Canadian NFC Mobile Payments Reference Model*, version 1.03, 14 mai 2012, p. 2. Voir http://www.cba.ca/contents/files/misc/msc_20120514_mobile_en.pdf (consulté le 14 février 2013).

[83] *Ibid.,* p. 26.

Roland et coll.[84]) et transmettre au contrôleur NFC et aux éléments de sécurité des messages qui semblent authentiques. Le fraudeur peut ainsi imputer des frais sur les comptes de la victime et transférer des fonds à un « commerçant » de son choix (p. ex. son propre compte inscrit). Signalons que toute la protection de sécurité inhérente à ce système de paiement NFC (par exemple les NIP ou les mots de passe permettant de verrouiller le portefeuille électronique ou les instruments de paiement) se trouve presque toujours dans le logiciel (c.-à-d. dans l'application de portefeuille électronique, parce que l'utilisateur peut choisir d'exiger ou non le NIP lorsque ces applications sont utilisées). Ainsi, l'attaque de matériel contournera toute cette protection et communiquera directement avec les éléments de sécurité et leurs applications de paiement.

3.3.2.2 Attaques de logiciel

Il existe une différence fondamentale entre le paiement mobile au moyen de la technologie NFC et le paiement par carte utilisant cette technologie. Les deux modes de règlement sont assez semblables en ce qui a trait au provisionnement et semblent identiques pour ce qui est du processus de paiement réel. Le risque inhérent à une borne de lecture truquée, à une attaque de l'intercepteur ou à un intermédiaire entre l'appareil ou la carte et la borne de lecture est également identique. Même une attaque de matériel sur les fils entre les composants du circuit intégré peut être menée de manière similaire pour les appareils mobiles et les cartes. Il semble donc que la différence réelle tient à la possibilité qu'un fraudeur installe un maliciel sur l'appareil mobile d'un utilisateur (à l'heure actuelle, un fraudeur ne peut installer un maliciel sur la carte de crédit NFC d'un utilisateur).

Puisque la puce NFC et celle de l'élément de sécurité sont des circuits intégrés physiquement distincts reliés uniquement par des fils entre eux et avec le contrôleur hôte, aucun logiciel sur le téléphone n'a directement accès à ces puces. Les attaques de logiciel malveillant doivent donc passer par un contrôleur hôte corrompu ou une autre application corrompue faisant en sorte que le contrôle hôte non corrompu donne des instructions en son nom.

Contrôleur hôte corrompu

Comme nous l'avons vu à la section 3.3.1.2, le contrôleur hôte est situé entre les applications de l'appareil mobile (notamment le portefeuille électronique) et les applications de paiement installées sur l'élément de sécurité. Plus précisément, ce contrôleur répond au portefeuille électronique qui demande de l'informer de l'emplacement de chaque application de paiement installée et de fournir un identifiant pour localiser une application de paiement donnée et interagir avec elle (voir, par exemple, le modèle de référence[85] [p. 68], où le contrôleur hôte est considéré comme une « application-cadre » quand l'élément de sécurité se trouve sur une carte UICC). Le contrôleur hôte communique aussi avec le contrôleur NFC pour définir son mode de fonctionnement et lui indiquer avec quelle application de paiement il doit établir le contact afin que le paiement puisse être effectué.

[84] M. Roland, C. Saminger et J. Langer, *Packet Sniffer for the Physical Layer of the Single Wire Protocol*, rapport de recherche, Université des sciences appliquées de la Haute-Autriche. Voir http://research.fh-ooe.at/files/publications/941_PacketSnifferPhysicalLayerSWP.pdf (consulté le 19 mars 2013).

[85] Institutions financières canadiennes (participants à l'initiative de l'industrie), *Canadian NFC Mobile Payments Reference Model*, version 1.03, 14 mai 2012. Voir http://www.cba.ca/contents/files/misc/msc_20120514_mobile_en.pdf (consulté le 14 février 2013).

Comme le contrôleur hôte ne voit aucune donnée des applications de paiement (parce que ces données passent par ce contrôleur au moment de l'installation, mais uniquement sous une forme chiffrée) et ne voit aucun détail des opérations de paiement (parce que ces opérations vont directement du contrôleur NFC à l'application de paiement sur l'élément de sécurité sans passer par le contrôleur hôte), il vaut la peine d'examiner ce qu'un contrôleur hôte corrompu pourrait faire en réalité pour porter atteinte à la sécurité ou à la vie privée dans les paiements mobiles. De toute évidence, le contrôleur corrompu peut communiquer au portefeuille électronique ou au contrôleur NFC l'identifiant de la mauvaise application de paiement (par exemple pour faire croire à l'utilisateur que le paiement est effectué au moyen de MasterCard alors que c'est par Visa en fait). Naturellement, l'utilisateur pourra s'en étonner ou trouver cela ennuyeux lorsqu'il recevra sa facture plus tard au cours du mois (s'il s'en aperçoit), mais comme il s'agit de deux instruments de paiement associés à l'utilisateur en toute légitimité, il ne peut s'agir d'une atteinte à la sécurité ou à la vie privée. En revanche, le contrôleur hôte pourrait mettre le contrôleur NFC en un mode inapproprié à un moment inopportun (p. ex. le mettre en mode actif afin que le téléphone lise une étiquette NFC truquée lorsqu'il ne s'y attend pas ou en mode émulation de carte pour permettre qu'une opération de paiement soit effectuée sans que l'utilisateur l'ait demandé). Ce comportement pourrait à coup sûr entraîner des atteintes à la sécurité ou à la vie privée. Signalons toutefois que le contrôleur hôte corrompu devrait agir en concertation avec un appareil externe (p. ex. une étiquette NFC, une borne de lecture NFC ou un terminal PDV corrompu) pour que l'atteinte ait lieu. Le contrôleur hôte corrompu ne peut à lui seul causer des problèmes de sécurité ou de protection de la vie privée.

Application de paiement corrompue sur un élément de sécurité

Il peut arriver que l'application de paiement que l'utilisateur souhaite utiliser soit corrompue. Il s'agit là d'un autre exemple d'attaque de logiciel. Par exemple, une application Visa corrompue a été installée sur l'appareil et une activité malveillante prend place lorsque l'utilisateur essaie d'effectuer un paiement par Visa (p. ex. les frais sont imputés au compte d'une autre personne parce que le mauvais numéro de compte est transmis au terminal PDV ou des frais trop élevés sont imputés au compte de l'utilisateur).

On peut présumer que le risque de ce type d'attaque est très faible, mais pas forcément nul. D'après le *Canadian NFC Mobile Payments Reference Model*[86] (p. 14, section 6.8), les applications de paiement et les données connexes sont installées par la marque de paiement (p. ex. Visa) elle-même (par l'intermédiaire de l'exploitant de réseau mobile sous une forme chiffrée), après la conclusion d'une entente avec le propriétaire de l'élément de sécurité (p. ex. l'exploitant). Il est fort peu probable que Visa installe elle-même une application Visa corrompue sur les appareils mobiles de ses propres clients ou que l'exploitant du réseau mobile autorise l'installation d'une application de paiement par une marque de paiement suspecte ou indigne de confiance.

Autre application corrompue sur l'élément de sécurité

Dans une variante de l'attaque décrite ci-dessus, une autre application (c.-à-d. une application différente de celle que l'utilisateur souhaite utiliser) est corrompue. Par exemple, une application MasterCard corrompue a été installée sur l'appareil de sorte qu'une activité malveillante se produit lorsque l'utilisateur essaie d'effectuer un paiement au moyen de Visa (p. ex. des détails concernant le paiement sont communiqués à MasterCard).

[86] Ibid.

Là encore, le risque est très faible. En fait, plusieurs mécanismes de protection sont en place contre ce type d'attaque. Premièrement, comme dans le cas de l'attaque décrite ci-dessus, il faudrait que l'application MasterCard piratée soit installée par MasterCard avec l'accord du propriétaire de l'élément de sécurité. Deuxièmement, le *Canadian NFC Mobile Payments Reference Model*[87] (p. 28, section 8.4.1) précise qu'une seule application de paiement à la fois peut être ouverte (disponible pour le paiement). Si une application de paiement est ouverte, les autres doivent être fermées. Donc, si l'utilisateur a choisi Visa comme instrument de paiement pour une opération, l'application MasterCard (piratée ou non) ne fonctionnera pas. Enfin, en raison de l'aménagement de l'élément de sécurité proprement dit, les applications qui s'y trouvent sont compartimentées (c.-à-d. qu'elles ne peuvent se voir l'une l'autre ni voir les données des autres).

Portefeuille électronique corrompu

Une autre possibilité serait que l'application de portefeuille électronique soit corrompue. Signalons que le portefeuille n'est pas installé sur l'élément de sécurité et qu'il y a par conséquent moins de contraintes quant à la façon dont on l'installe sur l'appareil (p. ex. l'utilisateur peut choisir de télécharger un portefeuille électronique gratuit à partir d'un site Web quelconque). Un portefeuille électronique corrompu peut essayer d'obtenir de l'information concernant une opération de paiement et la communiquer à une autre partie (p. ex. le fournisseur du portefeuille). Il peut aussi essayer de modifier les messages relatifs au paiement (p. ex. changer les numéros de compte ou le montant des opérations) ou manipuler des données sensibles stockées (p. ex. les données sur le solde dans un programme de fidélité).

D'après le modèle de référence canadien[88] (p. 31), un portefeuille électronique mobile peut saisir les données des opérations pour toutes les applications de paiement auxquelles il est relié. Toutefois, en pareil cas, l'accès aux données et leur utilisation doivent être limités conformément aux normes énoncées dans la section du modèle consacrée aux données et à la sécurité. Or, selon cette section (p. 82 à 90), le portefeuille électronique peut recueillir et stocker toutes sortes de données financières, les données des programmes de fidélité (notamment le solde de points) et les données sur les types de paiement, mais personne d'autre (pas même le fournisseur du portefeuille) ne devrait y avoir accès. Ces précisions constituent une ligne directrice importante pour la mise en œuvre d'un portefeuille électronique lorsque l'on souhaite se conformer au modèle, mais qu'en est-il dans le cas d'un portefeuille truqué? En particulier, qu'est-ce qui empêche ce portefeuille de faire ce qui lui plaît avec les données qu'il détient?

Le chiffrement des données de paiement et des programmes de fidélité stockées dans le portefeuille électronique (au moyen d'une clé connue uniquement de l'application de paiement ou celle du programme de fidélité) constitue une mesure de protection possible. Cette approche est certainement utile, mais il est important de signaler que le chiffrement n'est pas obligatoire (l'application peut choisir de chiffrer ces données ou non) et même si l'on a recours au chiffrement, certaines données demeurent non chiffrées, notamment le numéro de carte de crédit, le nom sur la carte de crédit et la valeur de vérification de la carte. Un portefeuille électronique truqué peut donc y avoir accès. Autre mesure de protection, le portefeuille électronique ne peut voir les détails des opérations (c.-à-d. le contenu des

[87] Ibid.

[88] Ibid.

messages du protocole, par exemple le montant de l'achat) parce qu'ils sont transmis directement du contrôleur NFC à l'application sur l'élément de sécurité. Ainsi, le portefeuille électronique n'y a pas accès.

Autre application corrompue sur le téléphone (non installée sur l'élément de sécurité)

Enfin, une autre application quelconque (différente du portefeuille électronique) installée sur le téléphone (et non sur l'élément de sécurité) peut aussi être corrompue. Est-il possible que cette application ait accès aux messages concernant les opérations de paiement (p. ex. qu'elle puisse lire ou modifier les données entre la puce NFC et l'application de paiement légitime sur l'élément de sécurité) de sorte que l'utilisateur voie et approuve un paiement de 2 $ à Starbucks par Visa, mais qu'un montant de 200 $ soit en fait imputé à son compte Visa? Comme dans le cas ci-dessus, plusieurs mécanismes de protection sont en place contre ce type de fraude. Premièrement, les messages concernant les opérations de paiement sont transmis par fil du contrôleur NFC à l'élément de sécurité et aucun logiciel sur l'appareil ne peut y avoir accès[89,90]. Comme nous l'avons mentionné à la section 3.3.1.2, une application peut s'inscrire pour recevoir des avis en cas de transmission NFC, mais ces avis indiquent seulement qu'une transmission se fait (sans en révéler le contenu). Deuxièmement, même si une application pouvait avoir accès aux messages concernant les paiements, ceux-ci sont généralement chiffrés, par exemple entre l'application Visa sur le terminal PDV et l'application Visa sur l'élément de sécurité; toute autre application qui intercepterait les messages ne connaîtrait pas la clé et serait par conséquent incapable d'en déchiffrer le contenu.

3.3.2.3 Autres considérations

Différentes préoccupations en matière de sécurité et de protection de la vie privée s'ajoutent à celles que nous avons déjà évoquées. Premièrement, certains instruments de paiement (p. ex. les coupons et les cartes de fidélité) peuvent être stockés dans la mémoire habituelle de l'appareil (p. ex. dans la mémoire de l'application mobile de portefeuille électronique) et non sur l'élément de sécurité. Comme nous l'avons déjà signalé, un portefeuille corrompu pourrait avoir accès à ces données et les manipuler à des fins malveillantes (si elles ne sont pas chiffrées), mais d'autres applications pourraient-elles voir, utiliser ou modifier ces instruments? Sur certains appareils (p. ex. les téléphones Android), on a compartimenté les applications afin qu'elles ne puissent pas voir les données ou l'état interne de n'importe quelle autre application. Signalons toutefois que si le téléphone a été « rooté » (ou débridé), les applications pourraient accroître leurs privilèges et contourner ces protections. Par conséquent, le chiffrement des données de l'instrument de paiement s'avère une bonne façon d'atténuer ce risque. Autrement, un portefeuille électronique numérique (par opposition à un portefeuille électronique mobile) peut offrir une certaine protection : si ces instruments de paiement sont stockés sur un serveur ou dans le nuage, et non sur l'appareil, les autres applications se trouvant sur l'appareil n'auront pas accès à ces données stockées, même si l'appareil a été « rooté » (signalons toutefois que ces applications peuvent avoir accès aux données au moment elles sont transmises du nuage au commerçant en passant par l'appareil au cours d'une opération de paiement).

[89] B. Jackson, « Google Wallet and NFC security: guarding against 'sharks with lasers », *IT Business*, 29 septembre 2011. Voir http://www.itbusiness.ca/news/google-wallet-and-nfc-security-guarding-against-sharks-with-lasers/16531 (consulté le 4 avril 2013).

[90] N. Pipenbrinck, « Secure Element communication with PCD/reader », *stackoverflow*, 22 juin 2012. Voir http://stackoverflow.com/questions/11152614/secure-element-communication-with-pcd-reader (consulté le 4 avril 2013).

Deuxièmement, il vaut la peine de se demander si les différents types de portefeuilles électroniques ont des répercussions sur la sécurité, la protection de la vie privée ou la responsabilité. Par exemple, avec un portefeuille électronique mobile, toutes les données de paiement se trouvent sur l'appareil proprement dit et peuvent être vulnérables en cas de perte ou de vol. En revanche, avec un portefeuille électronique numérique, toutes ces données sont stockées sur le serveur ou dans le nuage, de sorte que les autres peuvent y avoir accès si elles ne sont pas bien protégées. Autre exemple, l'utilisateur pourrait choisir de n'utiliser aucun NIP pour déverrouiller le portefeuille électronique mobile sur l'appareil, alors qu'il faut toujours utiliser un NIP ou un mot de passe pour établir la connexion avec un portefeuille électronique numérique sur un serveur (l'utilisateur n'a pas le choix). Autre exemple encore, un portefeuille électronique mobile (c.-à-d. installé sur l'appareil) communique avec les éléments de sécurité en passant par le contrôleur hôte, tandis qu'un portefeuille électronique numérique (c.-à-d. hébergé dans le nuage) communique avec eux par l'intermédiaire du navigateur et du contrôleur hôte. Par conséquent, il pourrait y avoir un risque d'atteinte à la sécurité ou à la vie privée si le navigateur présente des failles de sécurité.

Troisièmement, selon le *Canadian NFC Mobile Payments Reference Model* (p. 2, 3^{e} par.), le consommateur doit avoir le dernier mot quant à savoir si les données relatives à ses paiements sont protégées par un mot de passe et aux types de paiements possibles sur l'appareil mobile. Il est certainement utile de déterminer si le consommateur moyen prendra les bonnes décisions.

Quatrièmement, d'après le modèle de référence canadien (p. 63, section 10.6.1), même si le service mobile est déconnecté, l'application de paiement peut continuer de fonctionner pour les paiements NFC. Il vaut la peine de vérifier si c'est toujours une bonne chose. Y a-t-il un risque que des opérations de paiement puissent se faire lorsque l'utilisateur ne s'y attend pas?

Enfin, le modèle décrit non seulement les paiements effectués simplement en plaçant la carte devant la borne de lecture (p. ex. pour les opérations courantes), mais aussi les remboursements obtenus de la même manière (p. ex. pour les retours), parfois avec un reçu électronique. On ne demande à l'utilisateur aucune signature, aucun mot de passe ni aucun NIP pour retourner de la marchandise (p. 45). Dans le cas des reçus transmis par message texte ou par communication mobile OTA (*over-the-air,* par liaison radio) ou NFC, il est recommandé d'émettre des reçus en format texte. Pour les reçus transmis par courriel sur l'appareil, on peut utiliser le format texte ou PDF (p. 42). Bien entendu, il reste à savoir s'il est possible de voler le reçu d'une autre personne (p. ex. en l'interceptant sur le canal NFC ou sans fil au moment de l'opération de paiement ou en piratant le compte de courriel) et de retourner au magasin ultérieurement pour obtenir un remboursement (p. ex. pour un article volé similaire à celui acheté par le véritable client).

3.4 Sommaire

Le paiement de personne à personne NFC semble reposer sur une conception du matériel et des logiciels bien pensée intégrant plusieurs mesures de protection dans l'architecture et le flux des opérations en général. Toutefois, aucun mode n'est invulnérable (en particulier lorsque l'on souhaite qu'il puisse être mis en œuvre d'une façon facilitant son utilisation et déployé à grande échelle au bénéfice des consommateurs et des utilisateurs commerciaux). La présente section a mis en évidence plusieurs sources de préoccupations en matière de sécurité et de protection de la vie privée – bornes de lecture truquées et fraudeurs sur le canal NFC sans fil ou utilisant des outils matériels ou logiciels pour trafiquer le fonctionnement de l'appareil mobile. Enfin, des questions sont soulevées concernant le stockage des

données de certains instruments de paiement, les différents types de portefeuilles électroniques, la protection par mot de passe, la disponibilité continue des paiements lorsque le service mobile a été déconnecté et les remboursements sur présentation d'un reçu électronique.

4. Quelques modes de paiement de personne à personne

Dans la présente section, nous examinons brièvement deux types de paiement de personne à personne, soit M-Pesa et Cybermonnaie.

4.1 M-Pesa

M-Pesa, système de paiement articulé autour de la messagerie texte sur les téléphones mobiles, est utilisé au Kenya depuis 2007 et il a été déployé par la suite dans plusieurs autres pays d'Asie, d'Afrique et du Moyen-Orient. (On trouvera une analyse intéressante du déploiement initial de M-Pesa dans les régions rurales du Kenya dans l'analyse du projet M-Pesa présentée par Télécoms Sans Frontières[91].)

À tous les égards, M-Pesa a obtenu un taux d'acceptation élevé et un immense succès au Kenya et ailleurs, en particulier en mettant les transferts de fonds à la portée d'utilisateurs n'ayant pas accès aux services bancaires traditionnels. Toutefois, comme on pouvait s'y attendre, là où il y a de l'argent, il y a des fraudeurs qui essaient de pirater le système d'une façon quelconque afin de voler des fonds. Les deux exemples suivants font état d'attaques contre le système M-Pesa qui se sont réellement produites et qui sont documentées. Toutefois, il est important de signaler qu'aucune de ces attaques ne peut être pleinement automatisée : la participation d'un fraudeur ou d'un complice est obligatoire, ce qui limite la possibilité de les transposer à grande échelle.

Une attaque intéressante a été documentée en 2010[92]. Le 1er février 2010, deux personnes ont abordé un agent de M-Pesa dans la banlieue de Nairobi en prétendant être des employés de Safaricom (exploitant de réseau mobile au Kenya) chargés d'effectuer une vérification (les deux fraudeurs ont présenté du matériel publicitaire de M-Pesa et des pièces d'identité de Safaricom). L'agent n'a rien soupçonné, car ce type de vérification se fait régulièrement au Kenya. Après avoir demandé à voir les comptes et eu le loisir de les examiner pendant une certaine période, les fraudeurs ont quitté les lieux. Une vingtaine de minutes plus tard, un autre homme s'est adressé à l'agent pour lui demander un montant d'argent. Il a fait semblant de lancer l'opération M-Pesa sur un appareil mobile. L'agent a ensuite reçu un faux message autorisant une opération, qui indiquait le solde de son propre compte courant. L'agent a alors vérifié le nom de l'homme sur sa carte d'identité nationale et lui a donné le montant demandé. Plus tard, au moment de traiter une autre opération M-Pesa (légitime), l'agent a constaté que l'opération précédente n'avait pas été enregistrée, si bien qu'il avait perdu environ 450 $. Cette attaque a fonctionné parce qu'un faux message d'autorisation transmis par le fraudeur a été accepté comme étant un message d'autorisation authentique de Safaricom. Il s'avère que le « secret partagé » (entre Safaricom et un agent) qui authentifie ces messages constitue le solde du compte de l'agent à Safaricom. En se faisant passer pour des vérificateurs de Safaricom, les deux hommes ont pu examiner les livres de l'agent pour

[91] S. Hermon-Duc (chargé de projet pour TSF), *MPESA project analysis: Exploring the use of cash transfers using cell phones in pastoral areas*, rapport de projet de Télécoms sans frontières, 2012. Voir http://www.alnap.org/pool/files/mpesa-project-analysis-tsf-vsfg.pdf (consulté le 12 avril 2013).

[92] *Telco 2.0 News Review* (blogue), « Security Breach at M-PESA: Telco 2.0 Crash Investigation », Telco 2.0, 12 février 2010. Voir http://www.telco2.net/blog/2010/02/security_breach_at_mpesa_telco.html (consulté le 12 avril 2013).

connaître ce solde, ce qui leur a permis de créer un message d'autorisation convaincant et d'obtenir que l'agent remette les fonds à leur complice. Comme en fait état le rapport de Telco[93], il est intéressant de signaler que les fraudeurs ont utilisé le système de sécurité même de M-Pesa – vérifications régulières – afin d'obtenir l'information requise pour le pirater. Comme nous l'avons signalé ci-dessus, cette attaque ne peut être pleinement automatisée (il faut à tout le moins qu'un complice rencontre l'agent ciblé), ce qui limite la possibilité de fraude à grande échelle.

Un deuxième type de piratage contre le système M-Pesa a aussi été documenté[94]. Au moment du lancement de M-Pesa, les anciennes cartes SIM ne fonctionnaient pas avec le nouveau service. Seuls les clients ayant de nouvelles cartes SIM pouvaient s'inscrire comme utilisateurs de M-Pesa (les utilisateurs de téléphones dotés d'anciennes cartes SIM pouvaient avoir recours au service, mais uniquement en tant que clients non inscrits, et devaient payer des frais plus élevés pour obtenir des fonds auprès d'un agent). Des fraudeurs ont tiré avantage du fait que de nombreux utilisateurs ayant des téléphones dotés d'anciennes cartes SIM utilisaient des services prépayés. Un fraudeur achetait une nouvelle carte SIM et s'inscrivait au nom de l'utilisateur d'une ancienne carte SIM. Ainsi, toute personne qui se connectait à la base de données des utilisateurs de Safaricom voyait le nom de l'utilisateur légitime comme étant associé au numéro de téléphone correspondant, alors que le fraudeur était en fait l'utilisateur de M-Pesa inscrit sous ce numéro. D'après les règles de Safaricom, les fonds transférés par M-Pesa sont renvoyés à l'expéditeur s'ils ne sont pas retirés dans les sept jours. À l'intérieur de ce délai, le fraudeur retirait rapidement les fonds envoyés à l'utilisateur légitime (c.-à-d. l'utilisateur non inscrit ayant l'ancienne carte SIM). Par la suite, lorsque l'utilisateur légitime s'adressait à un agent M-Pesa pour prendre possession des fonds qui lui avaient été transférés, il découvrait que l'argent avait déjà été retiré. Là encore, ce piratage nécessite une intervention en personne et ne peut être pleinement automatisé et mené à grande échelle.

Compte tenu de la raison d'être première de M-Pesa (qui est de mettre les transferts de fonds à la portée d'un grand nombre d'utilisateurs n'ayant pas accès aux services bancaires traditionnels), il est peu probable que ce mode de paiement se répande au Canada. Mais un examen de M-Pesa fait ressortir des points qui peuvent s'appliquer également à d'autres modes de paiement (p. ex. les failles imputables aux fraudeurs ou l'utilisation (abusive) d'un mécanisme de sécurité comme une vérification pour parvenir à déjouer le système). Par conséquent, les leçons à tirer du cas de M-Pesa peuvent être utiles pour analyser la sécurité d'autres modes de paiement.

4.2 Cybermonnaie

Comme nous l'avons expliqué à la partie 1 du présent rapport, Cybermonnaie de la Monnaie royale canadienne est un mode de paiement de personne à personne qui permet de transférer un montant de Cybermonnaie par message texte, courriel ou communication NFC. Les appareils échangent des messages faisant état de la demande et du montant d'argent. Le message faisant état de la demande indique (entre autres) le montant à verser, la devise, l'identité du payé, l'adresse où envoyer l'argent ainsi qu'un nombre entier aléatoire de 32 bits. Le message faisant état du montant d'argent (signé numériquement) comprend essentiellement la même information de même que la date et l'heure, l'identité du payeur et son certificat de clé publique (pour vérifier sa signature). Quand le payeur crée un message faisant état

[93] *Ibid.*

[94] R. Wanjiku, « Security issues hit African mobile money providers », *Computerworld*, 17 novembre 2009. Voir http://news.idg.no/cw/art.cfm?id=03381EE0-1A64-6A71-CE896C46D67B6FFC (consulté le 12 avril 2013).

du montant, son solde de Cybermonnaie diminue. Quand le payé vérifie la validité de ce message, son solde augmente.

Puisque le système Cybermonnaie est à l'état de projet et qu'il n'a pas encore été déployé au Canada, on ne peut analyser la sécurité et la protection de la vie privée que sur la base des quelques détails de la mise en œuvre affichés dans le site Web de Cybermonnaie[95]. Toutefois, le système soulève certaines préoccupations ou questions. Mentionnons d'entrée de jeu que le message faisant état de la demande de Cybermonnaie ne semble protégé d'aucune façon (le message faisant état du montant d'argent est signé numériquement, mais non celui faisant état de la demande). Par conséquent, n'importe qui peut créer des messages de demande à volonté. Qui plus est, n'importe qui peut modifier le message de demande en transit entre l'expéditeur (le payé) et le récepteur (le payeur). Plus précisément, il est probable que le payeur recevra un message de demande, qu'une réponse s'affichera pour que l'utilisateur confirme l'opération et que le message de demande sera ensuite traité afin de créer le message affichant le montant correspondant. Un logiciel malveillant installé sur l'appareil de l'utilisateur pourrait donc modifier le message de demande entre la confirmation et le traitement afin que le payeur verse un montant plus élevé que prévu.

Deuxièmement, il est étonnant qu'un nombre entier non signé de 24 bits représentant le montant de l'opération en cents figure dans le champ du montant des messages faisant état de la demande et du montant d'argent. Avec 24 bits, ce champ peut renfermer des valeurs de l'ordre de 0 à 16777215. Il s'agit d'un montant supérieur à 167 000 $ – ce qui ne correspond absolument pas à un micropaiement ou à un nanopaiement! Il est difficile de comprendre pourquoi ce champ est si grand, alors que la Monnaie royale canadienne souhaite que sa cybermonnaie soit utilisée pour les opérations ayant une valeur de moins de 10 $.

Troisièmement, une fois que le message faisant état du montant a été créé et envoyé, la valeur est soustraite du compte et l'opération est irrévocable. Plus précisément, si le payé ne reçoit pas le message affichant le montant ou qu'il reçoit un message corrompu (p. ex. si la signature numérique n'est pas authentique), le payeur aura perdu les fonds, mais le destinataire ne les aura pas reçus. C'est un peu comme si une personne laissait tomber des pièces de monnaie dans un drain au moment où elle essayait de payer quelqu'un en argent liquide. Cela semble quelque peu risqué, mais rien ne prouve qu'il existe de meilleures solutions (p. ex. on pourrait envisager un protocole prévoyant trois messages, où le message final serait une confirmation du payé qui déclencherait le retrait dans le compte du payeur. Toutefois, en cas de perte ou de corruption du message final, le montant serait crédité au compte du bénéficiaire sans être débité de celui du payeur, si bien que les fonds auraient été créés à partir de rien). En revanche, le protocole de deux messages donne manifestement prise à une attaque par refus de service où les messages faisant état du montant sont corrompus au cours de la transmission, de sorte que le montant est retiré du compte du payeur sans qu'il reçoive les biens ou les services correspondants.

Quatrièmement, le message faisant état du montant indique l'identité du payeur et celle du payé ainsi que le certificat du payeur (requis pour permettre de vérifier la signature numérique). Même si personne ne stocke ces valeurs à long terme (pas même le système Cybermonnaie ni les différents payés), on peut se demander si des payeurs pourraient effectuer de façon anonyme des opérations de Cybermonnaie

95 Monnaie royale canadienne, « Ressources pour développeurs d'applications Cybermonnaie : MintChip Messages », 4 avril 2012. Voir http://developer.deficybermonnaie.com/devguide/developing/common/mintchip-messages.html (consulté le 8 avril 2013).

(comme on peut manifestement le faire avec l'argent liquide, ce que le système tente de reproduire dans l'économie numérique).

Enfin, dans son site Web[96], la Monnaie royale canadienne affirme que les messages affichant le montant de Cybermonnaie utilisent les signatures numériques RSA SHA-1. Or, étant donné que la fonction de hachage cryptographique SHA-1 est proscrite depuis janvier 2011 et qu'elle ne devra plus être utilisée après 2013 pour générer des signatures numériques[9798] (et que les variantes SHA-2 suscitent des doutes), cette norme a été remplacée par la nouvelle fonction de hachage SHA-3 en date d'octobre 2012[99]. On passera très bientôt à la fonction SHA-3 pour les procédures de signature numérique, qui continueront d'évoluer en faveur de solutions améliorant la sécurité et la protection des données.

5. Acceptation mobile

Dans le mode d'acceptation mobile, le commerçant a un appareil mobile (p. ex. une tablette ou un téléphone intelligent) qui a été mis à niveau d'une façon quelconque pour permettre l'acceptation des cartes de crédit traditionnelles (à bande magnétique). Une variante de ce mode permet au consommateur d'utiliser un appareil mobile au lieu d'une carte de crédit traditionnelle, mais le fait que le commerçant a remplacé le terminal PDV par un appareil mobile constitue la caractéristique qui distingue le mode d'acceptation mobile dans tous les cas.

Square[100], créée par Jack Dorsey, l'un des cofondateurs de Twitter, est une entreprise montante qui propose une technologie émergente dans le domaine. Plus de 200 000 entreprises acceptent les paiements effectués au moyen de cette technologie, qui ont récemment franchi le cap des 10 milliards de dollars. Entre autres, en vertu d'un partenariat conclu avec Starbucks, les clients peuvent utiliser la technologie de paiement Square dans plus de 7 000 cafés de la chaîne (Starbucks a aussi investi 25 millions de dollars dans Square et elle est représentée au sein de son conseil d'administration)[101]. Le système de paiement Square comporte deux volets, soit la Caisse Square (pour le commerçant) et le Portefeuille Square (facultatif – pour le client).

---

96 Monnaie royale canadienne, « Ressources pour développeurs d'applications Cybermonnaie : Message Validation », 4 avril 2012. Voir http://developer.Cybermonnaiechallenge.com/devguide/developing/common/message-validation.html (consulté le 8 avril 2013).

97 E. Barker et A. Roginsky, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, publication spéciale du NIST 800-131A, janvier 2011, p. 13-14. Voir http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf (consulté le 13 mai 2013).

98 T. Moffa (Centre de la sécurité des télécommunications Canada), *Algorithmes cryptographiques approuvés par le CSTC pour la protection des renseignements sensibles et pour les applications d'authentification et d'autorisation électroniques au sein du GC*, ALERTE ITSA-11 DU CSTC, mars 2011, section « Algorithmes de hachage et situation de l'algorithme SHA-1 ». Voir http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11e-fra.html (consulté le 13 mai 2013).

99 National Institute of Standards and Technology (NIST) des États-Unis, « NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition », *NIST Tech Beat*, 2 octobre 2012. Voir http://www.nist.gov/itl/csd/sha-100212.cfm (consulté le 8 avril 2013).

100 Square, Inc. Voir https://squareup.com/ca?country_code=ca (consulté le 5 avril 2013).

101 D. Terdiman, « Prowling the streets of San Francisco with Square Wallet », *CNET News*, 20 novembre 2012. Voir http://news.cnet.com/8301-1023_3-57552199-93/prowling-the-streets-of-san-francisco-with-square-wallet/ (consulté le 5 avril 2013).

La Caisse Square se compose d'une application logicielle installée sur l'appareil du commerçant et d'un petit cube en plastique que l'on branche dans la prise casque d'un iPhone, d'un iPad ou d'un appareil Android. Le cube comporte une petite fente où l'on peut glisser une carte de crédit ou de débit. L'application et le cube sont gratuits, mais le commerçant verse à Square des frais de 2,75 % par opération de paiement. Une fois l'achat terminé, le client peut obtenir un reçu numérique par courriel ou par message texte ou bien un reçu papier imprimé sur place. Le principal avantage de la Caisse Square tient au fait qu'elle permet d'accepter les paiements par carte de crédit ou de débit n'importe quand et n'importe où (p. ex. dans une vente de garage, dans un marché de producteurs ou à un stand de vente de fleurs au bord de la route); du point de vue du client, l'opération semble similaire à l'utilisation d'une carte traditionnelle à un terminal PDV. Toutefois, contrairement à ce qui se fait dans le cas du terminal PDV traditionnel, les données comptables du commerçant sont stockées sur les serveurs de Square, et non sur l'appareil mobile (le but étant, bien entendu, d'éviter des ennuis au commerçant en cas de perte ou de vol de l'appareil). Les renseignements tels que les paramètres du profil de l'entreprise, le calendrier des dépôts, les programmes de récompenses, les paramètres des comptes bancaires, les analyses commerciales approfondies, les autorisations conférées aux employés, l'historique des opérations et les données sur la gestion du personnel sont par conséquent tous stockés dans Square[102]. Cette situation peut être une source de préoccupations en matière de sécurité ou de protection de la vie privée, en particulier quant à la mesure dans laquelle le stockage de ces données est sécuritaire et qui y a accès.

Le Portefeuille Square est une extension optionnelle du système Square, qui permet aux clients d'effectuer des paiements aux entreprises figurant dans le répertoire de Square (c.-à-d. celles équipées de la Caisse Square) en utilisant un appareil mobile au lieu d'une carte à bande magnétique. (Le Portefeuille Square devrait être offert au Canada au cours de 2013.) L'utilisateur télécharge l'application du portefeuille, s'inscrit au service et entre les données d'une carte de crédit ou de débit (les cartes de plusieurs émetteurs sont acceptées, notamment Visa, MasterCard, AMEX et Discover). Au moment de l'inscription, l'utilisateur peut télécharger sa photo. Le client pourra ensuite utiliser l'outil d'exploration intégré pour trouver un commerçant à proximité qui accepte les paiements par Square. Au moment de l'achat, il lui suffit de cliquer sur le nom de ce commerçant et d'ouvrir l'onglet (« Slide to Pay » – signalons qu'il est possible de laisser cet onglet ouvert pour les entreprises où le client fait régulièrement des achats). Quand l'appareil se trouve à la distance requise de l'application Caisse Square du commerçant, le nom et la photo du client s'affichent sur l'écran du commerçant sur une liste de payeurs possibles (fait intéressant, le client peut laisser son téléphone dans sa poche ou son sac à main). Le client indique son nom au caissier, qui compare ensuite la photo avec le visage de la personne devant lui et sélectionne le payeur, après quoi l'opération est conclue[103]. En ce qui a trait aux préoccupations en matière de sécurité ou de protection de la vie privée, mentionnons que l'application du Portefeuille Square n'utilise aucun mot de passe ni aucun NIP (la seule façon d'empêcher les paiements consiste à fermer l'onglet). De plus, le commerçant voit la photo et le nom des acheteurs éventuels (ceux qui utilisent l'application et qui ont ouvert l'onglet – par exemple comme cela pourrait se faire dans les cafés Starbucks), même s'ils décident de payer comptant. Enfin, signalons que l'entreprise Square prend connaissance du nom du client, de sa photo et de l'historique de ses achats (y compris l'endroit précis et les articles achetés). À l'heure actuelle, les compagnies de cartes de crédit n'ont pas accès à toute cette information.

[102] Square, Inc., Square Register. Voir https://squareup.com/ca/register (consulté le 5 avril 2013).

[103] J. Duffy, J., « Pay With Square (for iPhone) », *PC Magazine* (pcmag.com), 9 août 2012. Voir http://www.pcmag.com/article2/0,2817,2408287,00.asp (consulté le 5 avril 2013).

L'utilisation de Square, en particulier la fonction permettant de payer en déclinant son nom, suscite également des préoccupations au chapitre de la sécurité. Supposons qu'un dénommé Robert se présente dans un café Starbucks et qu'il aperçoit son collègue Éric assis à une table de coin en train de prendre un chocolat chaud et un muffin. Les deux hommes se ressemblent. Robert sait Éric a un onglet ouvert pour Starbucks dans Square et il pourrait se présenter au comptoir, commander un café au lait et dire au caissier qu'il souhaite effectuer le paiement au moyen de Square en affirmant qu'il s'appelle Éric. Le café au lait sera imputé à la carte de crédit d'Éric (lequel n'en saura rien avant de recevoir son relevé de carte de crédit suivant; et même à ce moment, il risque de ne pas s'en apercevoir : il pourrait fort bien ne pas se rappeler s'il a commandé un café au lait quelques semaines auparavant et ne pas voir que l'opération a eu lieu le jour où il a acheté un chocolat chaud et un muffin). Plus grave encore, en faisant la queue, Robert pourrait voir un étranger qui lui ressemble en train de régler un achat au moyen de Square et l'entendre décliner son nom. En se présentant au comptoir (à plus forte raison si le café Starbucks est bondé ou que le caissier n'est pas le même), Robert pourrait utiliser le nom de l'étranger pour payer son café au lait. On peut imaginer que cette fraude aurait des répercussions encore plus grandes si le commerçant était un établissement où les paiements sont généralement beaucoup plus élevés que chez Starbucks.

Manifestement, la fonction qui permet d'effectuer un paiement en déclinant son nom est pratique et conviviale, mais elle semble vulnérable à une fraude par usurpation d'identité. L'entreprise s'efforce d'atténuer ce risque en demandant à chaque utilisateur de télécharger une photo au moment de son inscription à Square, mais tout le monde sait qu'une photo peut représenter de façon très approximative le visage d'une personne, en particulier si le client a changé de coiffure, s'il s'est rasé la barbe ou l'a fait pousser ou encore s'il porte un chapeau ou des verres fumés. Le message envoyé à l'appareil mobile d'Éric confirmant que le paiement a été mené à bien est également utile, mais il pourrait bien ne pas empêcher tout à fait ce type de fraude si Robert a déjà quitté l'établissement en emportant son café au lait.

6. Risques technologiques généraux liés aux opérations financières électroniques

Comme le montre clairement la partie 1 du présent rapport, différents modes de paiement ont été proposés ou déployés. Tout porte à croire que de nouveaux modes continueront de voir le jour au fil du temps[104]. L'industrie des paiements mobiles, qui est déjà assez importante, devrait continuer de prendre une expansion considérable au cours des prochaines années (p. ex. voir l'article de Collins[105], selon lequel Visa prévoit que d'ici 2020 plus de la moitié des achats effectués par des clients en Europe utiliseront les paiements mobiles). Par conséquent, même si les sections précédentes du présent rapport ont analysé certains modes et technologies de paiement en particulier, il est utile de se pencher globalement sur les risques d'atteinte à la sécurité et à la vie privée liés à tous les modes de paiement (ou à un grand nombre d'entre eux). Dans la présente section, nous analysons certains risques et dangers liés aux systèmes de paiement purement électronique sur les appareils mobiles.

[104] M. Bradley, « Digital Wallets Executive Briefing », *Information Technology Association of Canada (ITAC) Digital Commerce Forum: How Your Wallet is Going Digital*, 16 avril 2013. Voir http://itac.ca/files/2013_april_16_digital_wallet_presentation.pdf (consulté le 1er mai 2013).

[105] J. Collins, « Mobile payments deal between Visa and Monitise is formed », *Mobile Commerce News*, 11 mars 2013. Voir http://www.qrcodepress.com/mobile-payments-deal-between-visa-and-monitise-is-formed/8518094/ (consulté le 16 avril 2013).

En général, les préoccupations concernant la protection de la vie privée analysées ci-après se rapportent aux principes de l'OCDE relatifs à l'équité dans le traitement de l'information en matière de mesures de sécurité, de consentement, d'exactitude et d'accès aux renseignements personnels. Le cas échéant, les principes pertinents de la Loi sur la protection des renseignements personnels et les documents électroniques *seront mentionnés expressément au bénéfice des lecteurs qui pourraient s'intéresser particulièrement à une perspective canadienne.*

6.1 Suivi des paiements

Le suivi des paiements présente le risque d'atteinte à la vie privée le plus évident qui est commun à de nombreux modes de paiement électronique (c.-à-d. la capacité de suivre le mouvement de l'argent dans une opération de paiement, qui fait en réalité que le consommateur n'a plus le choix ou la possibilité d'effectuer un paiement de façon anonyme). Tout le monde sait que les émetteurs de cartes de crédit savent quand et auprès de quel commerçant une personne a utilisé sa carte de crédit, mais, comme nous l'avons déjà mentionné, certains autres modes de paiement permettent à d'autres parties d'obtenir des renseignements beaucoup plus détaillés sur les achats. Avec l'argent liquide, un consommateur a toujours l'option d'acheter des biens ou des services en toute confidentialité, alors que l'adoption des opérations électroniques (y compris pratiquement toutes les formes de paiement mobile) élimine cette possibilité. Les paiements anonymes ont certainement été envisagés dès le début des mécanismes utilisant de l'argent électronique (par exemple, voir Chaum, Fiat et Naor[106]), mais les identifiants qui figurent dans les messages faisant état de la demande et du montant de Cybermonnaie semblent exclure l'anonymat dans la formule proposée par ce système.

Une approche consiste à examiner des solutions de rechange à l'anonymat à l'intérieur du cadre juridique en place. Si les modes et les protocoles de paiement ne permettent pas l'anonymat sur le plan technique, il est d'autant plus important de s'assurer que les données de paiement, dans la mesure où il s'agit de renseignements personnels, seront protégées conformément à la législation de protection de la vie privée en vigueur, notamment la *Loi sur la protection des renseignements personnels et les documents électroniques* (pour les marchands, les marques de paiement, etc.) et la *Loi sur la protection des renseignements personnels* (p. ex. pour les montants remboursés aux citoyens par le gouvernement). De cette façon, la loi impose des contraintes quant aux entités qui peuvent découvrir les opérations financières et à ce qu'elles peuvent en faire. Manifestement, il n'est pas question d'anonymat dans ce cas, mais la collecte, l'utilisation, la communication et la conservation des renseignements sont soumises à certains contrôles, ce qui constitue à tout le moins un pas dans la bonne direction. En revanche, des solutions techniques permettent d'appuyer et d'appliquer les solutions législatives, si bien que les modes de paiement assurant un anonymat véritable dans les opérations financières présenteraient un intérêt considérable.

6.2 Petite taille de l'écran des appareils mobiles

La taille des appareils mobiles suscite une préoccupation en matière de protection de la vie privée que l'on oublie parfois. Plus précisément, la petite taille de l'écran d'un téléphone intelligent ou d'une tablette, comparativement à celui d'un ordinateur de bureau ou même d'un ordinateur portatif, peut compliquer l'affichage de la politique de confidentialité ou d'autres avis à l'intention des utilisateurs, si

[106] D. Chaum, A. Fiat et M. Naor, « Untraceable Electronic Cash », dans *Advances in Cryptology: Proceedings of CRYPTO '88*, S. Goldwasser (sous la dir. de), Springer-Verlag, 1989, p. 319-327.

bien qu'il est difficile d'obtenir un consentement valable (car il est peu probable que les utilisateurs lisent en entier des pages de texte sur un petit écran).

Les principes 4.8 (Transparence : « Une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne ») et 4.3 (Consentement : « Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire. ») de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) peuvent être pertinents pour donner suite à cette préoccupation.

6.3 Employés du fournisseur d'instruments de paiement

Comme nous l'avons mentionné à la section 5, dans certains modes de paiement mobile, l'entreprise qui offre l'instrument ou le service de paiement obtient beaucoup plus d'information sur le consommateur ou le commerçant que dans une opération de paiement effectuée au moyen d'une carte de crédit traditionnelle et d'un terminal PDV. Cet état de choses peut susciter des préoccupations en matière de la vie privée du fait que les employés du fournisseur pourraient avoir accès à cette information ou l'utiliser sans autorisation. Ces employés peuvent tenter d'avoir accès à cette information ou de l'utiliser d'une façon qui pourrait contrevenir aux principes de la LPRPDE, en particulier les principes 4.3 (Consentement : « Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire. ») et 4.5 (Limitation de l'utilisation, de la communication et de la conservation : « Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. »). L'accès ou l'utilisation non autorisés peuvent aussi faire ressortir des failles dans les mesures de sécurité mises en place par l'organisation, comme l'exige le principe 4.7 (Mesures de sécurité : « Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. »).

Des contrôles de vérification rigoureux et d'autres technologies et procédures concernant l'accès des employés aux données de paiement peuvent être nécessaires pour atténuer le risque.

6.4 Catastrophes naturelles ou d'origine humaine

À l'ère électronique, les sociétés sont de plus en plus vulnérables et dépourvues en cas de panne de courant : presque tous les appareils à la maison, au travail et dans les lieux publics cessent de fonctionner – y compris, bien entendu, toutes les formes d'opérations de paiement électronique.

Des pannes de courant peuvent être provoquées par de nombreux types de catastrophes naturelles (tremblements de terre, orages violents, activité extrême des taches solaires, etc.) de même que par des catastrophes d'origine humaine (explosions nucléaires, activités terroristes, etc.). Certaines catastrophes peuvent également rendre illisibles en permanence les systèmes de mémoire (disques durs des ordinateurs, clés USB, etc.). Quels sont les dangers de ne pas avoir de trace écrite des opérations financières : pas de fichiers de secours, pas d'information sur les comptes bancaires, pas de reçus d'achat, en fait rien du tout sous une forme pouvant résister à une désactivation de la mémoire électronique? Sous toutes ses formes, le commerce serait pratiquement impossible. Et pourtant, c'est le

risque vers lequel la société se dirige à grands pas à mesure que les opérations financières se font uniquement par voie électronique.

Vers la fin de 2012, le système M-Pesa a fait l'objet d'une mini-étude de cas intéressante illustrant cette situation. D'après Walubengo[107], une panne de courant touchant le serveur de Vodafone, en Allemagne, a endommagé les disques du serveur, ce qui a empêché la prestation des services de transfert de fonds M-Pesa de Safaricom au Kenya pendant près de 24 heures de la nuit du samedi au dimanche soir. [traduction] « Les rendez-vous ont été annulés, les gens ont commencé à avoir faim, ils ne pouvaient plus acheter de médicaments, ils se querellaient, leurs plans de voyage tombaient à l'eau, il était impossible de payer des réservations et de payer à temps les services publics et personne n'a vraiment pu profiter de la fin de semaine. » La panne a eu d'autres répercussions financières concrètes : les agents de M-Pesa ont dû passer la journée entière sans travailler et certains d'entre eux se sont plaints dans les médias des énormes pertes attribuables à la panne. Comme le signale Walubengo[108], [traduction] « si une panne de quelques heures peut causer d'énormes pertes, un arrêt complet des systèmes entraînerait une perte de revenus et priverait d'emploi une bonne partie des 49 079 agents. »

Les questions que soulève cette panne à l'égard des plateformes monétaires et des organismes de réglementation de l'industrie en général suscitent peut-être plus d'intérêt encore. Par exemple, Walubengo[109] (citant une présentation donnée en 2008 par Ananda et Kiptum[110]) affirme que le paragraphe 2(1) de la Loi sur les banques (il s'agit de la loi kenyane, mais on peut imaginer que la situation est similaire à tout le moins dans certains autres pays) définit l'« activité bancaire » comme étant l'acceptation de fonds du public dans un compte de dépôt ou un compte courant ET l'utilisation de ces fonds sous forme de prêts, d'investissements ou de toute autre manière pour le compte et au risque de la personne qui utilise ces fonds. Toujours d'après Walubengo, les fonds perçus par Safaricom auprès des titulaires de compte M-Pesa sont détenus par la M-Pesa Trust Company Limited dans un compte commun et l'intérêt que rapporte ce compte ne semble apparemment pas revenir ou profiter à Safaricom Limited. Par conséquent, Safaricom n'utilise pas les dépôts M-Pesa pour en tirer des bénéfices, de sorte qu'elle n'est pas considérée comme une organisation menant des « activités bancaires ». Puisque les lois régissant les principales institutions bancaires au Kenya pourraient ne pas s'appliquer aux opérations mobiles financières de Safaricom, le risque pour les utilisateurs peut être très différent. Il est peu probable que la plupart des utilisateurs kenyans l'avaient compris avant la panne.

Dans l'ensemble, les questions qu'a fait ressortir M-Pesa au Kenya[111] peuvent s'appliquer à d'autres modes de paiement mobile dans le monde. De nombreux pays auraient donc intérêt à se les poser.

- Qui indemnisera les clients si une plateforme mobile s'effondre (L'exploitant? La marque de paiement? La banque? L'État?)?

[107] N. Walubengo, « The Mobile Money Apocalypse; What Would Happen to Your Money? », *PesaTalk*, 2 novembre 2012. Voir http://pesatalk.com/the-mobile-money-apocalypse-what-would-happen-to-your-money/ (consulté le 17 avril 2013).

[108] *Ibid.*

[109] *Ibid.*

[110] F. Ananda et J. Kiptum, *Security Issues in M-Banking*, présentation donnée lors de la Information Security and Cyber Forensics Conference, du 29 au 31 octobre 2008. Voir http://www.strathmore.edu/pdf/M-Pesa.pdf (consulté le 12 juin 2013).

[111] N. Walubengo, « The Mobile Money Apocalypse; What Would Happen to Your Money? », *PesaTalk*, 2 novembre 2012. Voir http://pesatalk.com/the-mobile-money-apocalypse-what-would-happen-to-your-money/ (consulté le 17 avril 2013).

- Si l'on a mis en place un système quelconque pour rembourser les millions d'utilisateurs de fonds mobiles, comment s'y prendra-t-on sur le plan pratique alors que le système qu'ils utilisaient se sera effondré (rappelons qu'une forte proportion de la population kenyane n'a pas accès à des services bancaires)?
- Comment les exploitants se préparent-ils en prévision de problèmes de sécurité sur les serveurs pour protéger l'argent des abonnés?

Signalons que les conséquences d'une catastrophe naturelle ou d'origine humaine ne se limitent pas aux préoccupations en matière de sécurité. À cet égard, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE[112]) du Canada énonce les principes 4.7 (Mesures de sécurité : « Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. ») et 4.9 (Accès aux renseignements personnels : « Une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. »), qui se rapportent aux préoccupations en matière de protection des renseignements personnels. Il vaut la peine de se demander si une organisation qui ne conserve aucun registre papier pourrait avoir de la difficulté à satisfaire à ces exigences après une catastrophe qui aurait détruit tous les systèmes de mémoire électronique.

6.5 Mise en œuvre insuffisante de mesures de sécurité

Les avancées technologiques dans le monde des paiements mobiles permettraient d'accroître la sécurité de l'information financière (comparativement aux systèmes de paiement traditionnels par carte et terminal PDV), à tout le moins de trois façons particulières[113].

- Dans un système de paiement traditionnel, les données financières sont souvent transmises ou stockées sans chiffrement à une étape de la procédure de paiement. En revanche, la technologie des paiements mobiles permet de chiffrer les données tout au long de la chaîne de paiement (on parle alors de « chiffrement de bout en bout »). Signalons que la conformité aux normes PCI exige une sécurité de bout en bout. Or, dans la norme PCI, « de bout en bout » (en anglais *end-to-end*) renvoie au trajet allant du terminal PDV du commerçant à la destination finale de l'opération de paiement[114]. Dans le contexte des paiements mobiles, « de bout en bout » part de l'appareil mobile du consommateur et non du terminal du commerçant.
- Dans un système de paiement traditionnel, l'information financière figurant sur la bande magnétique d'une carte est transmise exactement sous la même forme chaque fois qu'un consommateur effectue un paiement. Si cette information est interceptée, le fraudeur pourra l'utiliser à répétition pour effectuer par la suite des opérations non autorisées. Toutefois, les

[112] *Loi sur la protection des renseignements personnels et les documents électroniques*. Voir http://laws-lois.justice.gc.ca/fra/lois/P-8.6/index.html; analyse des dispositions de la *Loi*, voir http://www.LPRPDE.info/a/1.html (consultés le 12 juin 2013).

[113] Federal Trade Commission (FTC) des États-Unis, Division of Financial Practices (D. Pozza, P. Poss, J. Chen et coll.), *Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments*, rapport du personnel de la FTC, mars 2013, p. 11-12. Voir http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (consulté le 5 avril 2013).

[114] Payment Card Industry (PCI) Security Standards Council, *Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance for Transmissions of Cardholder Data and Sensitive Authentication Data*, livre blanc d'Emerging Technology, Guide de programme, version 1.0, 5 octobre 2010. Voir https://www.pcisecuritystandards.org/pdfs/pci_ptp_encryption.pdf (consulté le 1er mai 2013).

paiements mobiles peuvent faire appel à une authentification dynamique des données, où une série unique d'information sur le paiement est générée pour chaque opération. De cette façon, même si un fraudeur intercepte les données, il ne pourra les utiliser pour une opération ultérieure.

- Sur un appareil mobile, l'information relative aux paiements peut être stockée sur l'élément de sécurité résistant à la falsification, qui est distinct du reste de la mémoire de l'appareil. Par conséquent, les pirates qui accèdent à l'appareil (physiquement ou uniquement au moyen d'un logiciel) ne peuvent obtenir ou falsifier des données financières sensibles.

C'est pourquoi la technologie permettant d'améliorer la sécurité des paiements mobiles est disponible, mais, d'après le compte rendu de l'atelier de la FTC[115] (p. 11-12), rien ne prouve que toutes les entreprises du marché des paiements mobiles les utilisent. Si des entreprises peu responsables ne mettent pas en œuvre les technologies sécurisées disponibles pour recueillir et stocker l'information relative aux paiements, les consommateurs (et l'industrie dans son ensemble advenant que les consommateurs en arrivent à croire que des pratiques de sécurité inadéquates sont la norme) pourront en souffrir. Le principe 4.7 (Mesures de sécurité : « Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. ») de la LPRPDE peut être utile face à cette préoccupation.

6.6 Mise en œuvre boguée

Comme toutes les autres applications installées sur un appareil mobile, les applications de paiement sont mises en œuvre dans un logiciel. Il est de notoriété publique dans l'industrie du logiciel que la majorité des programmes informatiques sont lourds et complexes (même un programme comportant quelques lignes de code peut atteindre rapidement plusieurs kilo-octets, voire des méga-octets, par exemple en raison des bibliothèques de données et des progiciels qu'il recèle). Or, les programmes informatiques lourds et complexes sont rarement exempts de bogues : les entrées, utilisations et situations inattendues peuvent toutes faire en sorte qu'un programme se comporte d'une façon imprévue par le développeur d'origine. Il est par conséquent probable qu'à tout le moins certaines applications de paiement seront « boguées », ce qui crée un véritable risque que des fraudeurs détectent ces bogues et en tirent parti.

Cette réflexion nous amène à ce qui se produit lorsqu'une application de paiement ne se comporte pas comme il se doit. En raison de bogues dans le logiciel, d'erreurs de transmission qui passent inaperçues ou de tout autre problème, on peut se trouver dans une situation où les deux parties sont en désaccord concernant une opération de paiement. Lorsque c'est la parole de l'un contre celle de l'autre, qui faut-il croire? Comment peut-on résoudre ce genre de divergence? Qui sera l'arbitre en fin de compte? À qui incombe la responsabilité à la fin? Bien entendu, des différends peuvent se produire aussi dans le cas des opérations en argent liquide, mais il y a alors à tout le moins un objet physique concret (l'argent) qui est transféré d'une partie à l'autre : après l'opération, le payeur a 10 $ de moins qu'avant, tandis que le payé a 10 $ de plus. Dans un paiement électronique, il est possible qu'une partie ait reçu à l'écran un message confirmant que 10 $ ont été payés, mais que l'autre partie en ait reçu un confirmant qu'un montant de 1 $ a été reçu. Auprès de qui les parties peuvent-elles porter plainte? Quelles mesures s'offrent à elles pour résoudre le problème? Il peut être utile d'examiner les registres des opérations qui sont conservés.

[115] Federal Trade Commission (FTC) des États-Unis, Division of Financial Practices (D. Pozza, P. Poss, J. Chen et coll.), Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments, rapport du personnel de la FTC, mars 2013. Voir http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (consulté le 5 avril 2013).

Toutefois, le degré de détail des renseignements consignés n'est pas toujours suffisant pour bien régler le différend.

La « mise en œuvre boguée » d'interventions menées par des humains, et non par des programmes informatiques, est à l'origine d'un autre problème connexe. Que se passe-t-il en cas d'erreurs humaines commises au cours d'une opération de paiement? On a vu un certain nombre d'exemples de cette situation dans le cadre du système de paiement M-Pesa au Kenya[116] : si l'utilisateur qui effectue un paiement transfère par erreur les fonds dans le mauvais compte, un mécanisme est prévu pour annuler le transfert (l'utilisateur appelle le Service à la clientèle de M-Pesa). Toutefois, cela peut fonctionner uniquement si celui qui a reçu par erreur les fonds transférés ne les a pas déjà encaissés ou utilisés pour faire un achat. S'il a déjà retiré les fonds, le payeur malchanceux les aura perdus. Des programmes informatiques bogués sont un autre exemple : après le transfert de fonds au mauvais compte en raison d'une erreur humaine, le payeur contacte M-Pesa pour faire annuler le transfert. Le représentant de M-Pesa lui donne alors l'assurance que l'opération a été annulée, mais le payeur ne voit pas les fonds dans son compte.

Un problème plus grave peut se produire si le payé est un fournisseur de services, et non un utilisateur, et que le payeur a des intentions malveillantes. Supposons que le payeur effectue un transfert M-Pesa au bénéfice d'un fournisseur de services, qu'il consomme le bien ou le service et contacte ensuite le Service à la clientèle de M-Pesa pour faire annuler le paiement (en alléguant que les fonds ont été transférés dans le mauvais compte par erreur). Ce stratagème peut fonctionner – on a documenté des cas où Safaricom avait accédé au compte d'un fournisseur de services et lancé l'annulation de l'opération sans aviser le fournisseur (par exemple, voir Yawe[117]).

Pour les cas de mise en œuvre boguée, en plus du principe 4.7 (Mesures de sécurité : « Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. ») de la LPRPDE, le principe 4.6 (Exactitude : « Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés. ») peut être pertinent. Il vaut la peine de vérifier si le propriétaire ou l'exploitant d'une application ou d'un service de paiement peut contrevenir à ce principe dans le cas où une mise en œuvre boguée donnerait lieu à des erreurs dans les opérations de paiement ou les montants versés.

6.7 Manque d'uniformité dans le règlement des différends

Compte tenu de la préoccupation décrite ci-dessus, une procédure de règlement des différends s'impose en cas de divergence dans une opération de paiement. Malheureusement, cette procédure varie d'un instrument de paiement à l'autre. D'après le compte rendu d'un récent atelier de la FTC sur les paiements mobiles aux États-Unis[118] (p. 5-7) :

---

[116] Bankelele (auteur de Nairobi s'intéressant à l'activité bancaire, aux finances, à la technologie et aux investissements), *How to Get n M-Pesa Refund and other Safaricom tales*, 29 juin 2009. Voir http://www.bankelele.co.ke/2009/06/how-to-get-M-Pesa-refund.html (consulté le 22 avril 2013).

[117] R. Yawe, *How secure is mpesa*, KICTAnet (Kenya ICT Action Network), juillet 2011. Voir http://www.kictanet.or.ke/?p=713 (consulté le 22 avril 2013).

[118] Federal Trade Commission (FTC) des États-Unis, Division of Financial Practices (D. Pozza, P. Poss, J. Chen et coll.), Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments, rapport du personnel de la FTC, mars 2013. Voir http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (consulté le 5 avril 2013).

> [traduction] L'une des préoccupations les plus importantes pour les utilisateurs des paiements mobiles réside dans le mode de résolution des différends en cas de paiement frauduleux ou de frais non autorisés. Selon la source de paiement utilisée pour financer le paiement mobile (p. ex. une carte de crédit, une carte prépayée ou la facture de l'entreprise de télécommunications mobiles), la loi peut protéger ou non les consommateurs contre les frais non autorisés. […]
>
> Les utilisateurs des paiements mobiles ne sont parfois pas conscients que leur protection contre les opérations frauduleuses ou non autorisées peut varier grandement en fonction de la source de financement visée. En règle générale, la protection offerte par la loi est la plus grande dans le cas du paiement par carte de crédit, car la responsabilité à l'égard d'une utilisation non autorisée est alors limitée à 50 $. Si un paiement mobile est effectué au moyen d'une carte de débit bancaire, la responsabilité du consommateur à l'égard d'un transfert non autorisé se limite à 50 $ pourvu que l'incident soit signalé dans les deux jours ouvrables, mais elle peut atteindre 500 $ après ce délai. Toutefois, si le consommateur ne signale pas les débits non autorisés sur son compte bancaire dans les 60 jours après que son relevé périodique lui a été envoyé par la poste, sa responsabilité peut devenir illimitée, peu importe que les frais découlent ou non de la perte ou du vol de sa carte ou d'un autre transfert électronique.
>
> Pour d'autres types de mécanismes de financement, la loi n'offre toutefois pas la même protection qu'avec les cartes de crédit ou de débit. Par exemple, aucune loi fédérale autre que la *FTC Act* ne protège les consommateurs contre les frais non autorisés si le paiement mobile est effectué au moyen d'un compte pré provisionné ou d'une carte à valeur stockée, par exemple une carte-cadeau ou une carte rechargeable polyvalente, aussi appelée « carte de débit prépayée ». […] Certes, le manque d'uniformité au chapitre de la protection complique la situation pour les consommateurs qui n'ont pas forcément conscience des différences entre ces sources de financement. […]
>
> Certaines entreprises ont comblé les lacunes dans la protection offerte par la loi en incluant dans le contrat des dispositions qui protègent les consommateurs en cas de différend concernant un paiement. […] Toutefois, comme elle est offerte sur une base volontaire, cette protection varie et les entreprises qui l'offrent pourraient la retirer ou la modifier à leur guise.

Les auteurs du compte rendu de l'atelier de la FTC concluent la section consacrée au règlement des différends en affirmant que les consommateurs [traduction] « devraient connaître leurs droits et leurs protections au moment de déterminer s'ils utiliseront un appareil mobile pour effectuer leurs paiements et, le cas échéant, de choisir le service de paiement mobile et le mécanisme de financement à utiliser. Pour les aider à faire ces choix, les entreprises devraient se doter de politiques clairement définies concernant les frais frauduleux et non autorisés et communiquer expressément ces politiques aux consommateurs ». Ce conseil s'applique manifestement aussi aux pays autres que les États-Unis, y compris le Canada.

6.8 Protocoles de paiement exclusifs

Selon une tendance qui s'amorce, des commerçants, des institutions financières et des marques de paiement créent des technologies de portefeuille électronique ou des modes de paiement exclusifs au lieu d'adopter les solutions existantes[119]. Certains d'entre eux peuvent y voir une façon d'offrir des caractéristiques ou une expérience à l'utilisateur se distinguant par rapport aux autres produits et leur conférant par le fait même un avantage concurrentiel. Cela n'a rien d'étonnant, à plus forte raison dans les sociétés qui privilégient une économie de libre marché.

Toutefois, les opérations de paiement figurent parmi les opérations les plus sensibles en matière de sécurité qui peuvent être effectuées sur un appareil mobile et les complexités avec lesquelles il faut

[119] M. Bradley, « Digital Wallets Executive Briefing », *Information Technology Association of Canada (ITAC) Digital Commerce Forum: How Your Wallet is Going Digital*, 16 avril 2013. Voir http://itac.ca/files/2013_april_16_digital_wallet_presentation.pdf (consulté le 1er mai 2013).

composer pour le faire dans les règles ne sont pas banales. Les commerçants, les institutions financières et les marques de paiement peuvent avoir une bonne compréhension des finances et du commerce, voire compter au sein de leur effectif des développeurs hautement qualifiés capables de créer des applications mobiles multifonctions adaptées, mais rien ne nous garantit qu'ils emploieront assez de personnes possédant une expertise suffisante en matière de sécurité et de protection de la vie privée pour s'assurer que les opérations de paiement mobile sont bien protégées. On ne sait donc pas très bien si les portefeuilles électroniques ou les modes de paiement exclusifs seront conçus, examinés et analysés par des spécialistes comme c'est nécessaire afin d'atténuer le risque pour les clients.

Les préoccupations concernant les offres exclusives s'articulent autour des failles imprévues des protocoles de paiement au chapitre de la sécurité et de la protection de la vie privée : Pourrait-il y avoir des façons de créer ou d'effacer des fonds? De blanchir de l'argent? De reproduire, de bloquer, d'ignorer ou de faire disparaître des paiements? De façon générale, la confidentialité, l'intégrité, l'authenticité et la disponibilité des paiements ne sont pas exemptes de risque. (Mentionnons à titre d'exemple les failles qui ont entraîné la perte de millions de dollars en Bitcoins en 2011[120].) Les principes 4.7 (Mesures de sécurité : « Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. ») et 4.6 (Exactitude : « Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés. ») de la LPRPDE peuvent être pertinents dans ce contexte, car il est important de s'assurer que les renseignements personnels des utilisateurs (p. ex. leurs opérations de paiement) ne peuvent être modifiées, supprimées ou reproduites dans un dessein malveillant.

En parallèle avec la protection offerte sous le régime de la LPRPDE, il pourrait être utile de vérifier si un paiement frauduleux ou malveillant constitue un vol ou une usurpation d'identité en vertu du *Code criminel* (le fraudeur prétend être l'utilisateur ou le commerçant).

6.9 Confiscation de fonds et blocage d'opérations

Une préoccupation concernant les systèmes de paiement électronique (notamment de paiement mobile) tient au fait que, exception faite du suivi des paiements, certaines parties pourraient être en mesure d'empêcher que des opérations se fassent. Il est facile d'imaginer un scénario où une personne ou un groupe de personnes serait ciblé comme étant « indésirable » : les autorités pourraient choisir d'empêcher ces personnes d'effectuer des paiements ou de recevoir des fonds (« Nous sommes désolés. Cette opération n'est pas autorisée… »), limitant ainsi dans les faits les mouvements et la liberté du groupe ciblé. C'est tout à fait possible : le *Canadian NFC Mobile Payments Reference Model*[121] (p. 29) indique que l'émetteur d'un authentifiant peut bloquer une application de paiement (p. ex. limiter l'utilisation au niveau de l'appareil ou du compte), de sorte qu'il n'aura pas accès à l'application pour effectuer des paiements tant que la procédure d'autorisation n'aura pas été exécutée entre l'utilisateur final et l'émetteur de l'authentifiant pour débloquer l'application de paiement. Signalons que les autorités faisant partie d'un gouvernement corrompu pourraient forcer un émetteur d'authentifiant à bloquer une application de paiement pour un utilisateur ou un groupe donné. Mais une simple erreur ou la négligence pourrait causer les mêmes torts à un citoyen complètement innocent, peut importe le régime politique.

---

[120] J. Mick, « Inside the Mega-Hack of Bitcoin: the Full Story », *DailyTech*, 19 juin 2011. Voir http://www.dailytech.com/Inside+the+MegaHack+of+Bitcoin+the+Full+Story/article21942.htm (consulté le 3 mai 2013).

[121] Institutions financières canadiennes (participants à l'initiative de l'industrie), *Canadian NFC Mobile Payments Reference Model*, version 1.03, 14 mai 2012. Voir http://www.cba.ca/contents/files/misc/msc_20120514_mobile_en.pdf (consulté le 14 février 2013).

Dans le même ordre d'idées, on peut se demander si une autorité pourrait « confisquer » l'argent numérique d'un individu (p. ex. essentiellement en le marquant comme « argent sale » afin qu'il ne puisse être dépensé nulle part). Cette fois encore, la chose semble faisable sur le plan technique et on peut aussi imaginer que des erreurs de ce genre auraient pour effet de pénaliser des personnes innocentes.

6.10 Vol d'un appareil

Manifestement, les appareils mobiles tels que les tablettes et les téléphones intelligents sont des produits convoités et par le fait même une cible attrayante pour les voleurs (qui souhaitent en tirer un bénéfice en vendant les appareils ou l'information qui y est stockée). Il vaut donc la peine de se demander si le fait qu'un appareil puisse être utilisé pour effectuer des paiements mobiles, à plus forte raison s'il renferme de l'argent numérique, accroît le risque de vol. Dans l'affirmative (ce qui semble probable), ceux qui ont ces appareils sur eux pourraient être exposés par le fait même à un risque de violence ou de préjudice accru.
Une mise en place généralisée de mesures de sécurité (notamment un mot de passe ou un NIP pour déverrouiller l'instrument de paiement, la suppression à distance des données sur un appareil perdu ou volé, etc.) revêt donc une importance accrue dans le monde des paiements mobiles (non seulement pour assurer la sécurité et la protection de la vie privée en général dans les opérations de paiement, mais aussi pour réduire le risque de vol de l'appareil et par le fait même renforcer la sécurité physique de son propriétaire).

6.11 Procédure de notification fastidieuse en cas de perte ou de vol

La préoccupation concernant le vol d'un appareil s'accompagne d'autres inquiétudes liées à la procédure de notification en cas de perte ou de vol. En effet, si un appareil est perdu ou volé, qui le propriétaire doit-il aviser? Si un seul appareil peut renfermer un bon nombre de cartes de crédit ou de débit, les cartes de rabais ou de fidélité ainsi que des coupons de nombreux émetteurs différents, comment le propriétaire se souviendra-t-il qui aviser pour bloquer ces divers instruments de paiement? Outre l'exploitant du réseau mobile, le propriétaire pourrait être contraint de communiquer avec chacune de ces marques de paiement et institutions financières individuellement (et ce, rapidement avant que la personne qui a trouvé ou volé l'appareil puisse s'en servir pour effectuer une opération de paiement). Les formalités peuvent être très lourdes pour un utilisateur ordinaire.
On pourrait bien entendu inciter les utilisateurs à verrouiller le portefeuille électronique et l'application de paiement au moyen d'un mot de passe ou d'un NIP afin d'éviter que ces applications soient immédiatement accessibles en cas de vol. Toutefois, il n'existe aucun moyen d'obliger les utilisateurs à se servir d'un NIP (il s'agit à l'heure actuelle d'une fonction optionnelle). Si l'utilisateur se sert d'un NIP, il n'existe aucun moyen de l'obliger à adopter un NIP différent pour chaque application de paiement et de garantir que tout NIP utilisé sera suffisamment difficile à deviner. Mais ce n'est pas tout : d'après une équipe de recherche allemande, en abaissant la température d'un appareil – à tout le moins pour certains types d'appareils (les expériences menées portaient sur un appareil Android Galaxy Nexus de Samsung) – au-dessous de moins 10 degrés Celsius et ensuite en connectant et en déconnectant la batterie, on rend le téléphone vulnérable[122]. Une fois le téléphone en mode vulnérable, un fraudeur pourrait le remettre en marche en utilisant un logiciel personnalisé au lieu du système Android interne et

[122] *BBC News Technology*, « Frozen Android phones give up data secrets », 7 mars 2013. Voir http://www.bbc.co.uk/news/technology-21697704 (consulté le 19 avril 2013).

par la suite trouver les clés de chiffrement afin de décrypter les données et de les copier sur un ordinateur distinct aux fins d'analyse. Les données de paiements effectués sur un appareil volé (c.-à-d. toute donnée qui n'est pas stockée sur l'élément de sécurité) peuvent être vulnérables même si elles sont chiffrées ou protégées par un NIP. Signalons qu'il s'agit d'une attaque récente, mais tout indique que les fraudeurs en mettront d'autres au point au fil du temps.

Le principe 4.7 (Mesures de sécurité : « Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. ») de la LPRPDE peut être pertinent dans cette situation. Plus précisément, il est utile de se demander si les fabricants d'appareils ou de systèmes d'exploitation pourraient contrevenir à ce principe étant donné que le fait de « congeler » l'appareil ou de commettre une autre forme d'attaque peut rendre vulnérables les renseignements personnels (p. ex. si les fabricants n'ont pas mis en place des mesures de sécurité adéquates pour assurer une protection contre ce type d'attaques). De plus, les fabricants pourraient contrevenir à ce principe s'ils prennent conscience de ces failles et omettent d'en faire part aux utilisateurs et de remédier à la situation.

6.12 Incertitudes entourant « l'effacement à distance »

Certains fabricants de systèmes d'exploitation pour appareils mobiles ont adopté « l'effacement à distance » pour rassurer leurs clients : en cas de perte ou de vol de son appareil, le client peut donner une commande à distance et supprimer les données qui y sont stockées, ce qui rend l'appareil beaucoup moins attrayant pour celui qui l'a trouvé ou volé. Il s'agit là d'une idée convaincante, en particulier dans le cas des paiements mobiles où un fraudeur qui prend possession du téléphone perdu ou volé pourrait avoir accès à des renseignements financiers sensibles (p. ex. les numéros de carte de crédit et leur date d'expiration, les coupons, les cartes de fidélité et même de l'argent numérique) et les utiliser.

Le concept d'effacement à distance soulève toutefois au moins deux préoccupations. Premièrement (peut-être l'aspect le plus important), cette technologie fonctionne-t-elle vraiment? Dans les premiers jours de l'informatique, des spécialistes suggéraient de supprimer les renseignements sensibles sur un disque dur avant de se défaire d'un ordinateur, mais on a rapidement découvert que la suppression pure et simple des fichiers ne les efface pas entièrement (elle supprime simplement l'indicateur de fichier et marque ainsi que le fichier comme « espace disque disponible » pouvant être utilisé pour le stockage d'autres données). Ce problème a conduit à la création de la fonction « suppression sécurisée » avec laquelle de nouvelles données complètement aléatoires sont utilisées pour écraser à plusieurs reprises l'information stockée sur le fichier choisi avant la suppression de l'indicateur de fichier. De cette façon, il est vraiment impossible de récupérer les données, même en effectuant une analyse technique poussée. Le fait que nous sommes peut-être encore néophytes pour ce qui est de la suppression de fichiers sur les plateformes mobiles (c.-à-d. que, sur certaines plateformes à tout le moins, la suppression à distance peut en fait ne rien effacer) est une source de préoccupation. D'après des recherches préliminaires menées à l'Université d'Ottawa, ce pourrait être le cas (voir l'annexe A). Par ailleurs, il est facile de faire échouer l'effacement à distance si la personne qui a désormais l'appareil en sa possession agit assez rapidement pour le bloquer d'une façon quelconque (p. ex. en plaçant l'appareil dans une boîte en métal) avant que le propriétaire s'aperçoive qu'il ne l'a plus. L'environnement « blindé » empêcherait le signal d'effacement à distance d'atteindre l'appareil. Dans les deux cas, il y a manifestement des répercussions sur le plan de la sécurité et de la protection de la vie privée si l'on peut encore récupérer des données financières sur l'appareil lorsque le propriétaire croit les avoir supprimées.

Deuxièmement, des interrogations demeurent même si l'effacement à distance fonctionne à la perfection. Ainsi, est-il vrai que l'effacement détruit tout l'argent numérique stocké sur l'appareil? Dans l'affirmative, cet argent est-il disparu pour toujours? Dans l'affirmative, le propriétaire a-t-il des recours – par exemple cette perte pourrait-elle être couverte par une assurance, en particulier s'il s'agit de montants considérables? S'il y a une possibilité de recours (p. ex. une assurance), comment le propriétaire peut-il prouver que le montant d'argent était stocké sur l'appareil? Il semble plus probable que l'argent numérique serait simplement perdu (comme si la personne avait égaré son portefeuille : il est impossible de récupérer l'argent, que le portefeuille renferme 10 $ ou 1 000 $). Compte tenu du nombre de téléphones mobiles perdus ou volés chaque jour[123], on peut se demander si les consommateurs seraient réticents à stocker sur leur téléphone des montants d'argent élevés ou à avoir recours à l'effacement à distance (dans l'espoir de trouver bientôt leur téléphone derrière les coussins du canapé). À cela s'ajoute une préoccupation connexe si le téléphone sert à la fois à des fins commerciales et personnelles : comme il est possible que l'effacement à distance exécuté par l'entreprise détruise les renseignements personnels (y compris l'argent numérique), cela pourrait inciter les utilisateurs à ne pas stocker des montants d'argent élevés sur leur appareil.

Que l'effacement à distance ne fonctionne pas ou qu'il fonctionne et détruise tout l'argent numérique, les coupons, les cartes de fidélité, etc., stockés sur l'appareil, les principes 4.1 (Responsabilité : « Une organisation est responsable des renseignements personnels dont elle a la gestion […]. ») et 4.7 (« Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. ») de la LPRPDE peuvent être pertinents. Toute entité qui offre un service d'effacement à distance a implicitement la maîtrise de l'information stockée sur l'appareil (à tout le moins la maîtrise de son existence) et doit en assumer la responsabilité si l'utilisateur estime que l'information a été détruite alors qu'il était en fait possible de la récupérer.

6.13 Intérêt croissant des pirates informatiques pour les appareils mobiles

Depuis quelques années, les appareils mobiles présentent un attrait croissant pour les pirates informatiques, les auteurs de maliciels et les autres fraudeurs et tout indique que cette tendance se maintiendra. Comme un plus grand nombre d'appareils mobiles renferment des instruments de paiement de toutes sortes, notamment de l'argent numérique, ces appareils deviennent une cible encore plus attrayante. On peut donc s'attendre à ce que la diversité, l'ampleur et la complexité des risques d'atteinte à la sécurité et à la vie privée liés aux appareils mobiles en général et aux paiements mobiles en particulier ne fassent qu'augmenter au fil du temps.

7. Conclusion

À la partie 2 du présent rapport, nous proposons une analyse de certains modes de paiement mobile. Nous analysons aussi de façon détaillée le paiement à un terminal de point de vente NFC et d'autres modes de paiement, notamment le paiement de personne à personne (p. ex. M-Pesa et Cybermonnaie) et l'acceptation mobile (p. ex. la technologie Square). Nous y analysons aussi dans une optique générale les préoccupations en matière de sécurité et de protection de la vie privée se rapportant à l'ensemble ou à la plupart des modes de paiement électronique. Par souci d'exhaustivité, nous y explorons d'abord

[123] S. Knight, « Americans lost $30 billion worth of mobile phones in 2011 », *TechSpot*, 23 mars 2012. Voir http://www.techspot.com/news/47930-americans-lost-30-billion-worth-of-mobile-phones-in-2011.html (consulté le 23 avril 2013).

l'étape de transition vers les paiements mobiles véritables, qui sont largement utilisés dans de nombreuses sociétés (opérations bancaires ou achats en ligne et paiements mobiles par l'intermédiaire des entreprises de télécommunications mobiles).

De façon générale, la sécurité et la protection de la vie privée suscitent de nombreuses préoccupations, très mineures (p. ex. la modification de messages sur le canal sans fil NFC) ou plus importantes (subtilisation de fonds sur des appareils NFC, installation de maliciels – notamment d'un portefeuille électronique piraté – sur l'appareil mobile, possibilité d'usurpation d'identité dans Square, perte d'anonymat dans les opérations de paiement, procédure de notification fastidieuse en cas de perte ou de vol, incertitudes entourant l'effacement à distance, par exemple). Nous nous sommes efforcés de décrire ces problèmes aussi clairement que possible (à la fois sur le plan technique et général) et d'expliquer les risques correspondants. La dernière partie du présent rapport, la partie 3, fait état de recommandations découlant de l'analyse exposée à la partie 2.

Les paiements mobiles en tout temps et en tout lieu : bref survol du paysage des paiements mobiles

Partie 3 – Recommandations

Résumé

La dernière des trois parties présente des recommandations au chapitre de la sécurité et de la protection de la vie privée qui découlent de l'analyse de divers modes de paiement mobiles présentée à la partie 2. Certaines recommandations sont classées en fonction des groupes auxquels elles s'adressent, notamment les fabricants d'appareils mobiles, les fournisseurs d'instruments de paiement, les organismes de normalisation et les utilisateurs finals.

Les recommandations formulées reflètent le point de vue de l'auteur, l'objectif étant de contribuer à la recherche sur la sécurité et la protection de la vie privée menée par le Commissariat à la protection de la vie privée du Canada et d'autres parties intéressées. En ce sens, elles devraient être considérées comme une information que le Commissariat et d'autres parties peuvent prendre en compte au moment de formuler leurs propres politiques et lignes directrices dans le domaine des paiements mobiles.

1. Introduction

Le présent rapport sur les paiements mobiles est divisé en trois parties : contexte, analyse et recommandations. La partie 3, « Recommandations », examine des façons d'atténuer les risques d'atteinte à la sécurité et à la vie privée liés aux divers modes de paiement analysés à la partie 2.

Le reste de la partie 3 est structuré comme suit. Nous présentons à la section 2 des recommandations émanant d'autres sources qui s'appliquent aux appareils et aux paiements mobiles. Nous formulons à la section 3 des recommandations découlant de l'analyse présentée à la partie 2, qui se rapportent à des modes de paiement en particulier, et à la section 4 celles visant tous les modes de paiement électronique, classées en fonction des groupes auxquelles elles s'adressent : fabricants d'appareils et de systèmes d'exploitation, exploitants de réseau mobile, développeurs de portefeuilles électroniques ou d'applications, organismes de normalisation, commerçants et utilisateurs finals. Enfin, nous présentons les conclusions à la section 5.

2. Recommandations pertinentes émanant d'autres sources

Plusieurs groupes différents ont formulé des recommandations au chapitre de la sécurité et de la protection de la vie privée dans les environnements mobiles. Certaines se rapportent à des modes de paiement mobile en particulier, tandis que d'autres visent à définir les pratiques exemplaires pour les appareils mobiles en général. Nous présentons, dans un ordre aléatoire, plusieurs exemples dans les prochaines sous-sections.

2.1 Federal Trade Commission

En avril 2012, la Federal Trade Commission (FTC) des États-Unis a tenu un atelier sur les paiements mobiles [traduction] « pour en apprendre davantage sur l'industrie des paiements mobiles et son incidence sur les consommateurs ». Les pages 11 à 13 du compte rendu de l'atelier[124] portent sur la sécurité des données des consommateurs dans les paiements mobiles et recommandent différentes mesures, par exemple utiliser des mots de passe différents afin de déverrouiller l'appareil et d'accéder aux applications de paiement et contacter immédiatement l'entreprise de télécommunications mobiles en cas de vol de l'appareil afin de faire désactiver l'appareil proprement dit et toutes les applications de paiement. Les pages 13 à 15 traitent de la protection de la vie privée et recommandent des mesures à adopter par les entreprises du marché des paiements mobiles : prise en compte de la protection de la vie privée dès la conception, notamment à l'étape du développement des produits, et restriction de la collecte des données en fonction du contexte de l'interaction d'un consommateur avec l'entreprise visée; et simplification du choix pour les entreprises et les consommateurs, en particulier concernant la communication de renseignements non nécessaires pour effectuer une opération de paiement; et transparence accrue quant aux pratiques touchant les données.

2.2 LAP et M^{3}AAWG

Des membres de l'International Cybersecurity Enforcement Network, connu sous le nom de « Plan d'action de Londres » (London Action Plan [LAP]) ont fait équipe avec des membres du Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG) pour produire un rapport intitulé *Best Practices to Address Online and Mobile Threats* (Pratiques exemplaires pour régler la question des menaces mobiles et en ligne)[125]. Ce rapport, qui a été publié le 15 octobre 2012, ne porte pas expressément sur les paiements mobiles, mais il fait état de recommandations et de pratiques exemplaires utiles pour donner suite à toute une gamme de sujets de préoccupation, notamment les maliciels et les réseaux d'ordinateurs zombies, l'hameçonnage et le piratage psychologique, l'exploitation du protocole Internet (IP) et du système de noms de domaine (DNS) ainsi que les menaces mobiles. En ce qui a trait aux menaces mobiles, le rapport présente le cas d'un fraudeur qui a mis sur pied une station de base truquée et un réseau sans fil illicite, une escroquerie axée sur une facturation frauduleuse à taux majoré (p. ex. des services à taux majoré sont imputés au compte d'un abonné sans son consentement), les pourriels et les maliciels sur appareils mobiles, la sécurité (ou le manque de sécurité) des magasins d'applications et la modification des appareils mobiles (débridage, « rootage » et déverrouillage).

2.3 Commissariat à la protection de la vie privée du Canada

Le Commissariat à la protection de la vie privée du Canada a publié plusieurs lignes directrices et recommandations portant sur les appareils mobiles et la protection de la vie privée en ligne. Plus

[124] Federal Trade Commission (FTC) des États-Unis, Division of Financial Practices (D. Pozza, P. Poss, J. Chen et coll.), *Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments*, rapport de la FTC, mars 2013. Voir http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (consulté le 17 mai 2013).

[125] London Action Plan (LAP) et Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG), *Best Practices to Address Online and Mobile Threats*, 15 octobre 2012. Voir http://www.maawg.org/sites/maawg/files/news/M3AAWG_LAP_Best_Practices_to_Address_Online_and_Mobile_Threats_0.pdf (consulté le 17 mai 2013).

précisément, le site Web principal du Commissariat (http://www.priv.gc.ca/) présente, entre autres, les ressources suivantes :

- *La protection de la vie privée à l'air libre : 10 conseils à suivre pour aider les particuliers à protéger les renseignements personnels sur les appareils mobiles* (http://www.priv.gc.ca/resource/fs-fi/02_05_d_47_dpd_f.asp), janvier 2011.
- *La transformation du système de paiements canadiens : pourquoi la protection de la vie privée est essentielle à la confiance à l'égard du système de paiements et son innovation* (http://www.priv.gc.ca/information/research-recherche/sub/sub_psr_1109_f.asp, septembre 2011.
- Document d'orientation du CPVP – *Le vol d'identité et vous* (http://www.priv.gc.ca/information/pub/guide_idt_f.asp), mars 2009.
- *Comment reconnaître les menaces contre les données personnelles : Quatre façons de détourner vos renseignements personnels sur Internet* (http://www.priv.gc.ca/resource/fs-fi/id/phishing_f.asp), mars 2007.
- *Protection des renseignements personnels en ligne : Foire aux questions* (http://www.priv.gc.ca/resource/fs-fi/02_05_d_13_rev_01_f.asp), dernière modification : septembre 2011.
- Document d'orientation du CPVP – *Une occasion à saisir : Développer des applis mobiles dans le respect du droit à la vie privée* (http://www.priv.gc.ca/information/pub/gd_app_201210_f.asp), octobre 2012.
- *Protéger les renseignements personnels : Un outil d'auto-évaluation à l'intention des organisations* (http://www.priv.gc.ca/resource/tool-outil/security-securite/francais/AssessRisks.asp?x=1), mars 2011.

En ce qui a trait aux appareils mobiles, le Commissariat a notamment recommandé de se familiariser avec les réglages de sécurité et de protection de la vie privée sur l'appareil, de supprimer les renseignements personnels non nécessaires qui y sont stockés, d'utiliser un mot de passe difficile à deviner, de verrouiller l'appareil lorsqu'on ne l'utilise pas, d'installer des logiciels de sécurité (antivirus, anti-logiciel espion, pare-feu et logiciels de chiffrement) sur l'appareil, de désactiver les fonctions Wi-Fi et Bluetooth par défaut, de préparer un plan en cas de perte ou de vol, d'utiliser un écran assurant un affichage confidentiel, de toujours installer les derniers correctifs de sécurité et de limiter le nombre de personnes qui ont accès au numéro de l'appareil mobile.

2.4 Payment Card Industry Security Standards Council

Le Payment Card Industry (PCI) Security Standards Council a publié un document[126] qui a pour ambition de donner une orientation aux commerçants sur la façon de mettre en œuvre une solution d'acceptation mobile sécurisée. Les sections 4, 5 et 6 (Objectifs et orientation pour la sécurité d'une opération de paiement, Orientation pour sécuriser l'appareil mobile et Orientation pour sécuriser la solution d'acceptation des paiements) constituent la partie centrale du rapport (voir aussi l'annexe B : Pratiques exemplaires et responsabilités) et elles présentent des lignes directrices recommandant par exemple de

[126] Payment Card Industry (PCI) Security Standards Council, Emerging Technologies, PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users, version 1.0, février 2013. Voir https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf (consulté le 17 mai 2013).

prévenir l'accès physique non autorisé à l'appareil, de le protéger contre les maliciels, de s'assurer qu'il est sécurisé, de désactiver les fonctions non nécessaires sur l'appareil, d'inspecter les journaux du système et les rapports, d'effacer de façon sécuritaire les données sur l'appareil et de se défaire de l'appareil de façon sécuritaire.

Signalons toutefois que ce présent rapport met l'accent sur l'appareil mobile utilisé par le commerçant pour l'opération de paiement (p. ex. un terminal PDV ou un appareil d'acceptation des paiements). Il ne propose pas de lignes directrices visant expressément l'appareil mobile utilisé par le consommateur (payeur). Toutefois, nombre des lignes directrices analysées s'appliqueraient aussi à l'appareil de l'utilisateur.

3. Recommandations découlant du présent rapport (modes de paiement mobile précis)

À la partie 2 du présent rapport, nous nous sommes penchés sur quelques modes de paiement mobile et nous avons analysé plus particulièrement certaines technologies de paiement mobile. Les sous-sections suivantes font état des recommandations issues de cette analyse.

3.1 Activités bancaires ou achats en ligne au moyen d'un navigateur mobile

Comme nous l'avons signalé à la partie 2, section 2.1, les failles des navigateurs mobiles peuvent entraîner une perte ou une utilisation abusive des données ou permettre le téléchargement de logiciels malveillants sur l'appareil. Les recommandations d'usage sont donc pertinentes pour ce mode de paiement :

- toujours télécharger les dernières corrections et mises à jour et du navigateur et du système d'exploitation;
- télécharger des logiciels uniquement à partir de sources dignes de confiance;
- utiliser un appareil qui n'a pas été débridé ni « rooté ».

3.2 Facturation par l'entreprise de télécommunications mobiles

La facturation par l'entreprise de télécommunications mobiles suscite deux grands sujets de préoccupation, soit la possibilité que l'entreprise utilise à mauvais escient les renseignements supplémentaires recueillis concernant ses clients (p. ex. l'historique détaillé de leurs achats et l'identité des commerçants visés); et la possibilité accrue de bourrage de factures (frais non autorisés, qui peuvent être présentés ou désignés de façon ambiguë ou trompeuse, par exemple « frais de service » ou « autres frais »). Les recommandations se rapportant à ce mode de paiement sont les suivantes (les trois premières sont issues du compte rendu de l'atelier de la FTC[127] [p. 8-9]) :

- Les entreprises de télécommunications mobiles devraient permettre à leurs clients de bloquer tous les frais de tiers sur leur compte de téléphonie mobile (p. ex. les clients devraient pouvoir choisir de ne pas autoriser ou utiliser les services de tiers).
- Il faudrait établir une procédure uniforme et clairement définie pour la contestation de frais suspects et l'obtention d'un remboursement par les clients.

[127] Federal Trade Commission (FTC) des États-Unis, Division of Financial Practices (D. Pozza, P. Poss, J. Chen et coll.), *Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments*, rapport du personnel de la FTC, mars 2013. Voir http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (consulté le 17 mai 2013).

- Les entreprises de télécommunications devraient normaliser et mettre en évidence la désignation des frais imputés par des tiers.
- Les clients devraient vérifier minutieusement leur facture chaque mois en étant à l'affût des frais suspects ou mal expliqués.
- Les entreprises de télécommunications mobiles devraient s'efforcer de protéger la vie privée de leurs clients et la confidentialité des renseignements personnels recueillis à leur sujet en prélevant des paiements sur leur facture.

3.3 Terminal PDV NFC

Les appareils mobiles qui permettent d'effectuer des paiements en utilisant un terminal au point de vente sans contact muni de la technologie de communication en champ proche (NFC) suscitent plusieurs préoccupations en matière de sécurité et de protection de la vie privée, que nous avons analysées à la partie 2, section 3, du présent rapport. Ces préoccupations donnent lieu aux recommandations suivantes :

- Pour éviter qu'un fraudeur effectue une opération de paiement à l'insu ou sans le consentement du propriétaire de l'appareil ou bien qu'il s'approprie en douce un numéro de carte de crédit et sa date d'expiration sur l'appareil, la fonction NFC devrait être désactivée lorsque l'écran est éteint et la confirmation de l'utilisateur devrait être exigée pour toutes les opérations de paiement (et non seulement celles de valeur élevée). L'autorisation de l'utilisateur devrait aussi être exigée pour l'exécution des instructions se trouvant dans une étiquette NFC.
- Afin d'éviter les attaques par canal corrompu (p. ex. les attaques de l'intercepteur ou par relais), les utilisateurs devraient faire preuve de vigilance et observer les personnes se trouvant tout près d'eux pendant qu'ils effectuent des opérations (p. ex. il faut se méfier d'un badaud muni d'un appareil comportant une longue antenne!). En outre, la confirmation de l'utilisateur devrait être exigée pour toutes les opérations de paiement afin de réduire le risque qu'un fraudeur commette une attaque par relais et fasse ainsi payer ses achats par un utilisateur légitime.
- En énonçant des normes à respecter, le *Canadian NFC Mobile Payments Reference Model*[128] (p. 2, 3e par., et p. 30-31, S15-S17) veille à ce que le consommateur ait le dernier mot quant à savoir si ses paiements seront protégés au moyen d'un mot de passe et aux types de paiement qui sont activés sur son appareil mobile. Comme il est impossible d'avoir l'assurance que le consommateur moyen prendra des décisions judicieuses à cet égard, les applications des portefeuilles devraient comporter des paramètres par défaut qui privilégient la sécurité et la protection de la vie privée (p. ex. mot de passe exigé par défaut pour toutes les applications de paiement).
- D'après le modèle de référence (p. 26), [traduction] « un authentifiant par défaut permet à l'utilisateur final d'effectuer un paiement tout en laissant l'appareil mobile en mode veille sans avoir à sélectionner manuellement un portefeuille électronique ». Étant donné les risques d'atteinte à la sécurité liés à ce type de procédure d'authentification par défaut (p. ex. opérations frauduleuses effectuées au moyen de bornes de lecture truquées), les utilisateurs devraient bien connaître toutes les conséquences éventuelles du réglage de l'authentification par défaut sur leur appareil.
- Toujours d'après le modèle de référence (p. 41), les reçus électroniques devraient indiquer aux fins de suivi non seulement le numéro de carte de crédit ou de débit (tronqué aux quatre

[128] Institutions financières canadiennes (participants à l'initiative de l'industrie), *Canadian NFC Mobile Payments Reference Model*, version 1.03, 14 mai 2012. Voir http://www.cba.ca/contents/files/misc/msc_20120514_mobile_en.pdf (consulté le 23 mai 2013).

derniers chiffres), mais aussi le numéro d'appareil mobile (tronqué). Toutefois, comme un fraudeur ayant obtenu le reçu d'un utilisateur aurait probablement beaucoup plus de facilité à trouver le numéro du téléphone mobile que le numéro de la carte à partir des valeurs tronquées (puisque le numéro de téléphone comprend moins de chiffres et que plusieurs d'entre eux peuvent être faciles à deviner), il vaut mieux que le numéro de téléphone tronqué ne figure pas sur le reçu.

- Le modèle de référence (p. 45) décrit les « remboursements effectués simplement en plaçant l'appareil mobile devant la borne de lecture » : aucune signature, aucun mot de passe ni aucun NIP n'est exigé pour obtenir un remboursement. Cette situation peut exposer les commerçants à un risque (p. ex. si un fraudeur utilise un reçu volé afin d'obtenir un remboursement pour un article volé) et c'est pourquoi il y a lieu de se pencher sur le niveau d'authentification pertinent pour les retours, en particulier d'examiner des pratiques ne portant pas atteinte à la vie privée.
- D'après le modèle de référence (p. 63, section 10.6.1), même si le service mobile est déconnecté, l'application de paiement peut continuer à fonctionner pour les paiements NFC. Cette fonction n'est pas nécessairement intuitive pour les utilisateurs (qui pourraient naturellement penser qu'en l'absence de service mobile, ils ne pourront utiliser leur téléphone pour effectuer des paiements), ce qui peut donner lieu à une situation où des opérations de paiement se font lorsque l'utilisateur ne s'y attend pas. Par conséquent, les entreprises de télécommunications mobiles ne devraient pas offrir cette fonction ou elles devraient s'assurer que les utilisateurs sont parfaitement au courant de cette possibilité.
- Les données de paiement et des cartes de fidélité stockées dans le portefeuille électronique (et non sur l'élément de sécurité) devraient être chiffrées par ceux qui les fournissent afin de réduire le risque d'utilisation abusive par un logiciel malveillant sur l'appareil.
- Les utilisateurs devraient prendre le maximum de précautions et télécharger et installer uniquement des applications de portefeuille électronique fiables (p. ex. une application d'un fournisseur connu et digne de confiance), car un portefeuille truqué peut recueillir les données de paiement qui ne sont pas chiffrées (p. ex. le numéro de carte de crédit et la valeur de vérification de la carte [CVV]) et les utiliser à mauvais escient.
- Les utilisateurs ne devraient jamais « rooter » ou débrider leur appareil mobile, ce qui le rendrait plus vulnérable aux maliciels.
- Les applications de paiement installées sur l'élément de sécurité devraient toujours chiffrer les données des opérations de paiement transmises à un terminal PDV (pour atténuer le risque découlant des bornes de lecture corrompues et des intercepteurs sur le canal NFC; voir, par exemple, la section 4.2 du livre blanc de Kremer[129]).
- Comme il est mentionné dans le modèle de référence (p. 91), chaque participant à l'écosystème devrait mettre en place des procédures pour suivre, surveiller et atténuer les préoccupations en matière de fraude et de sécurité, notamment les maliciels, le piratage et le vol d'appareils mobiles.
- Selon un article paru dans *CNN Money*[130], [traduction], « les appareils devraient à tout le moins demander une autorisation avant d'accepter des données provenant d'une étiquette NFC se trouvant à proximité par hasard ou d'un appareil inconnu ». Il est vrai que les utilisateurs ne

[129] J. Kremer, *NFC: Near Field Communication White Paper*, Jan Kremer Consulting Services. Voir http://jkremer.com/White%20Papers/Near%20Field%20Communication%20White%20Paper%20JKCS.pdf (consulté le 23 mai 2013).

[130] S. Cowley, « NFC exploit: Be very, very careful what your smartphone gets near », *CNNMoney*, 26 juillet 2013. Voir http://money.cnn.com/2012/07/26/technology/nfc-hack/index.htm (consulté le 23 mai 2013).

peuvent pas toujours évaluer adéquatement le risque lié aux étiquettes ou aux appareils inconnus, mais il n'en reste pas moins préférable que l'utilisateur donne une autorisation au lieu de laisser l'appareil accepter les données de toute origine sans aucune évaluation de la part de l'utilisateur.

Enfin, le livre blanc de la GSMA[131] présente une analyse de la raison d'être et des avantages de l'utilisation de la technologie NFC dans le secteur du commerce de détail. Les sections 8 et 9 (Définition des rôles et des responsabilités et Éléments à prendre en compte) mettent l'accent sur la façon de promouvoir l'utilisation de la technologie mobile NFC dans le commerce et présentent un bon nombre de recommandations s'adressant à divers acteurs de l'écosystème du commerce de détail (entre autres, renseigner les consommateurs sur le mode d'utilisation de la technologie mobile NFC; établir un cadre robuste et sécurisé pour la gestion des données des clients; déterminer ce qui doit être sécurisé et ce qui n'a pas à l'être; avoir recours à des solutions normalisées pour assurer l'interopérabilité et permettre des économies d'échelle; et veiller à ce qu'un téléphone NFC dont la pile est déchargée puisse établir un contact avec un terminal NFC). Il vaut la peine de lire ces sections pour en savoir plus sur les points résumés ci-dessus à l'égard des recommandations portant sur le paiement mobile à un terminal NFC.

3.4 Paiement mobile de personne à personne

L'analyse présentée à la partie 2, section 4.1, donne lieu aux recommandations suivantes pour les technologies d'acceptation mobile.

- Si des renseignements secrets partagés par deux entités authentifient le message autorisant une opération, il ne doit pas s'agir d'une information facile à obtenir par un fraudeur (ou à tout le moins ils ne doivent pas se limiter à ce type d'information)[132]. Une solution plus appropriée consisterait à utiliser la cryptographie (p. ex. signer numériquement le message d'autorisation sur le serveur de l'entreprise de paiement et faire vérifier par le logiciel agent la signature des messages d'autorisation entrants).
- Une authentification rigoureuse s'impose lorsqu'un utilisateur essaie d'ouvrir un compte ou d'y apporter des modifications (p. ex. enregistrer une nouvelle carte SIM en utilisant un numéro existant [celui d'une ancienne carte SIM]). Ainsi, un fraudeur pourrait plus difficilement obtenir de l'argent transmis à un autre utilisateur.
- Il faudrait être très attentif aux moyens qui s'offrent aux fraudeurs d'utiliser les mécanismes de sécurité (p. ex. les vérifications) afin de pirater le système de paiement et aux aspects où des failles peuvent exister en raison de la présence d'acteurs malveillants à une étape quelconque de l'opération de paiement. En outre, dans les pays où l'on pourrait considérer que le fournisseur d'applications de paiement pratique des « activités bancaires », alors qu'il n'en est rien selon une interprétation stricte de la loi, les clients devraient être bien connaître les responsabilités ou les risques auxquels ils s'exposeraient si leurs opérations ou leurs comptes subissaient des pertes imprévues.

[131] Groupe Speciale Mobile Association (GSMA), *Mobile NFC in Retail*, livre blanc, version 1.0, septembre 2012. Voir http://www.gsma.com/mobilenfc/wp-content/uploads/2012/10/Mobile-NFC-in-Retail-White-Paper-Oct-2012.pdf (consulté le 23 mai 2013).

[132] Par exemple, dans le cas présenté à la partie 2, section 4.1, le solde du compte courant est utilisé comme information secrète partagée. Cette valeur est stockée – probablement de façon sécurisée – sur le serveur du fournisseur de la solution de paiement, mais elle peut aussi figurer dans un document connu de tous : le livre de comptes de l'agent. Quiconque a accès à ce livre (soit en se faisant passer pour un vérificateur ou en y jetant un coup d'œil en douce pendant que l'agent est distrait par autre chose) pourra créer un message autorisant une opération truquée que l'agent acceptera comme étant légitime.

3.5 Systèmes de cybermonnaie

Comme nous l'avons montré à la partie 3, section 4.2, les systèmes de cybermonnaie peuvent susciter certaines préoccupations en matière de sécurité et de protection de la vie privée. Ces préoccupations donnent lieu aux recommandations suivantes.

- Tous les messages devraient être protégés (cryptographiquement) d'une façon quelconque, peut-être par une signature numérique de l'expéditeur du message. Cette mesure empêcherait de modifier un message de demande ou de réponse en transit (respectivement au détriment du payeur ou du payé).
- Dans les messages de demande et de réponse, le champ du montant devrait avoir une taille appropriée pour l'usage visé (p. ex. les micropaiements). On peut laisser un peu d'espace supplémentaire en prévision d'une croissance éventuelle, mais une taille excessive ouvre la voie à des utilisations abusives (en particulier si les messages ne sont pas protégés comme nous l'avons signalé au paragraphe précédent).
- Pour ressembler davantage à l'argent liquide, les systèmes de cybermonnaie devraient comporter une option permettant d'effectuer des paiements de façon totalement anonyme. Pour certaines propositions, la façon de procéder à cette fin n'est pas évidente (puisque les messages sont signés numériquement et que les participants doivent avoir une clé publique digne de confiance permettant de vérifier que les signatures sont valides), mais il faudrait explorer certains autres paramètres de conception dans le domaine.
- Il faudrait examiner périodiquement tous les algorithmes cryptographiques utilisés dans les protocoles de paiement pour s'assurer que les pratiques exemplaires sont toujours suivies (p. ex. le passage du protocole SHA-1 [proscrit] à la version SHA-3).

3.6 Acceptation mobile

L'analyse présentée à la partie 2, section 5, conduit aux recommandations suivantes concernant l'acceptation mobile.

- Pour certaines technologies proposées, une quantité appréciable de données sensibles du commerçant sont stockées sur les serveurs du fournisseur de services de paiement (incluant potentiellement les paramètres des comptes bancaires, le calendrier des dépôts, les analyses commerciales approfondies, les autorisations conférées aux employés, l'historique des opérations et les données sur la gestion du personnel). Il est donc recommandé aux fournisseurs de services de paiement de faire preuve de vigilance pour protéger la vie privée de leurs clients et la confidentialité de tous les renseignements recueillis à leur sujet (c.-à-d. sur les commerçants et, indirectement, leurs clients).
- En ce qui a trait au payeur, autrement dit le client, il est recommandé de prendre des précautions supplémentaires pour atténuer le risque d'attaque par usurpation d'identité. Plus précisément, il faut s'assurer que le paiement est bien effectué par la personne qui passe à la caisse (et non par l'un des autres « payeurs disponibles » qui se trouvent à proximité). À cette fin, on pourrait obliger tous les utilisateurs d'applications qui s'inscrivent à un service de paiement à télécharger une photo. Toutefois, en raison des préoccupations en matière de vie privée que cela pose, cette mesure n'est pas recommandée. Il faudrait explorer d'autres mécanismes techniques d'authentification. Dans le même ordre d'idées, même si c'est pratique, les utilisateurs ne devraient pas laisser leur application de paiement activée en permanence (le but étant de réduire la possibilité qu'ils paient sans le vouloir les achats d'un fraudeur). Il est préférable d'activer

l'application uniquement lorsqu'ils sont prêts à effectuer un achat et de la désactiver immédiatement après.

4. Recommandations découlant du présent rapport (tous les modes de paiement électronique)

À la partie 2 du présent rapport, nous avons analysé quelques technologies de paiement mobile précises ainsi que certaines préoccupations en matière de sécurité et de protection de la vie privée qui s'appliquent généralement à l'ensemble ou à la plupart des modes de paiement électronique. Dans les sous-sections qui suivent, nous présentons les recommandations découlant de cette partie de l'analyse, classées en fonction des groupes auxquels elles s'adressent (en particulier les fabricants d'appareils ou de systèmes d'exploitation, les exploitants de réseau mobile, les développeurs de portefeuilles électroniques ou d'applications, les organismes de réglementation, les commerçants et les utilisateurs finals).

Nota : Certaines recommandations sont reprises dans différentes sous-sections. Ces répétitions sont volontaires, car les lecteurs ne liront probablement que la sous-section s'adressant au groupe dont ils font partie.

4.1 Fabricants d'appareils ou de systèmes d'exploitation

Les recommandations dont nous faisons état dans la présente sous-section s'adressent principalement aux fabricants d'appareils mobiles et de systèmes d'exploitation utilisés sur ces appareils (parfois la même entité, mais pas toujours).

4.1.1 Écrans de petite taille

Même les tablettes et les téléphones mobiles les plus gros sont munis d'un écran beaucoup plus petit que ceux dont sont généralement équipés les ordinateurs portatifs. Comme nous l'avons signalé à la partie 2, en raison de la petite taille de ces écrans, il est difficile d'obtenir un consentement valable des utilisateurs, du fait notamment qu'il est peu probable qu'ils lisent attentivement une longue politique de confidentialité sur un appareil mobile. Nous encourageons les fabricants à explorer des façons de résoudre ce problème, peut-être en adoptant d'autres méthodes pour communiquer l'information de façon utile à un utilisateur (p. ex. en présentant leur politique par étapes ou au fil des besoins).

4.1.2 Mise en œuvre boguée

Comme nous l'avons mentionné à la partie 2, la probabilité que les systèmes logiciels lourds et complexes (comme les systèmes d'exploitation) contiennent des bogues est élevée. Il en va de même pour les gros systèmes matériels complexes (comme les circuits intégrés). Nous encourageons les fabricants à conserver leurs procédures rigoureuses de conception et d'essais, voire à les renforcer pour s'assurer dans la mesure du possible de livrer des systèmes exempts de bogues. Une certification par un organisme externe (comme un laboratoire d'évaluation des critères communs – on trouvera dans le site Web du CSTC[133] une liste de produits certifiés au Canada) peut s'avérer très utile dans ce processus.

[133] Centre de la sécurité des télécommunications Canada (CSTC), Produits certifiés selon les critères communs, voir http://www.cse-cst.gc.ca/its-sti/services/cc/cp-pc-fra.html (consulté le 12 juin 2013).

4.1.3 Perte ou vol d'un appareil

Le risque de perte ou de vol d'un appareil mobile est élevé. Parfois, les données stockées sont vulnérables et peuvent être piratées. Nous encourageons les fabricants à maintenir, voire à renforcer leurs efforts afin de fournir des mécanismes de protection utiles dans ces situations, par exemple le verrouillage à distance de l'appareil ainsi que le chiffrement et l'effacement à distance des données.

4.1.4 Défaillance des mécanismes de protection

Comme le montre l'attaque par « congélation du téléphone » décrite à la partie 2 section 6.11, il est possible de porter atteinte aux mécanismes de protection tels que le chiffrement des données par des moyens inattendus. Nous encourageons les fabricants à maintenir, voire à renforcer leurs procédures rigoureuses de mise à l'essai des mécanismes de protection des données, en particulier lorsque l'appareil est soumis à des conditions de fonctionnement inhabituelles ou extrêmes.

4.1.5 Effacement à distance

Comme nous l'avons signalé à la partie 2, section 6.12, et dans l'annexe, on ne sait pas avec certitude si l'effacement à distance est efficace pour empêcher toute récupération des données. Nous encourageons les fabricants à explorer ce domaine attentivement pour voir s'il est possible de trouver des techniques qui effaceront les données de façon sécuritaire tout en évitant d'épuiser sans raison la mémoire flash.

4.1.6 Intérêt croissant des pirates informatique

À la partie 2, section 6.13, nous avons souligné que les appareils mobiles présentent depuis quelques années un attrait croissant pour les pirates informatiques, les auteurs de maliciels et les autres fraudeurs et tout indique que cette tendance se maintiendra. Nous encourageons les fabricants à poursuivre énergiquement leurs efforts afin que leurs systèmes d'exploitation et leur matériel soient exempts de failles susceptibles de porter atteinte à la sécurité et à la protection de la vie privée, et à contribuer activement à faire en sorte que les appareils soient exempts de maliciels en créant et en diffusant les correctifs, les mises à jour, etc., aussi rapidement que possible.

4.2 Exploitants de réseau mobile

Les recommandations dont nous faisons état dans la présente sous-section s'adressent principalement aux exploitants de réseau mobile.

4.2.1 Perte ou vol d'un appareil

En cas de perte ou de vol d'un appareil mobile, l'utilisateur avise généralement l'exploitant du réseau mobile (et d'autres entités). Nous encourageons les exploitants à poursuivre leurs efforts afin que la procédure soit la plus simple et la moins fastidieuse possible. Entre autres, il peut s'agir d'aider l'utilisateur à verrouiller l'appareil, à chiffrer ou effacer les données, à localiser l'appareil et à l'inscrire dans un registre national[134]. Le *Canadian NFC Mobile Payments Reference Model*[135] (p. 59-61,

[134] M. Lewis, « Registry targets smartphone black market », *The Toronto Star: Business*, 8 novembre 2012. Voir http://www.thestar.com/business/2012/11/08/registry_targets_smartphone_black_market.html (consulté le 12 juin 2013).

section 10.5.4), présente un diagramme de haut niveau montrant les principales tâches incombant à l'exploitant de réseau mobile après qu'un utilisateur l'a informé de la perte ou du vol d'un appareil.

4.2.2 Effacement à distance

Comme nous l'avons signalé à la partie 2, section 6.12, et dans l'annexe, on ne sait pas avec certitude si l'effacement à distance est efficace pour empêcher toute récupération des données. Nous encourageons les fabricants à explorer ce domaine attentivement pour voir s'il est possible de trouver des techniques qui permettront d'effacer les données de façon sécuritaire sur demande.

4.2.3 Intérêt croissant des pirates informatiques

À la partie 2, section 6.13, nous avons souligné que les appareils mobiles présentent depuis quelques années un attrait croissant pour les pirates informatiques, les auteurs de maliciels et les autres fraudeurs, et tout indique que cette tendance se maintiendra. Nous encourageons les exploitants de réseau mobile à poursuivre leurs efforts afin que les appareils soient exempts de maliciels en transmettant les correctifs, les outils antivirus, etc., à leurs clients aussi rapidement que possible et à aider les utilisateurs à mettre en place ces mesures de protection dès qu'elles sont disponibles.

4.3 Développeurs de portefeuilles électroniques et d'applications

Les recommandations dont nous faisons état dans la présente sous-section s'adressent principalement aux développeurs et aux fournisseurs de portefeuilles électroniques et d'applications de paiement.

4.3.1 Suivi des paiements

À la partie 2, section 6.1, nous avons traité du suivi dans les systèmes de paiement électronique et du fait que les utilisateurs ne peuvent effectuer ou recevoir des paiements de façon anonyme. Bien que le suivi soit utile, notamment aux fins de vérification, pour des raisons fiscales et pour d'autres fins, les systèmes de paiement électronique modernes semblent n'offrir aucun mécanisme permettant les opérations anonymes (comme c'est possible avec l'argent liquide, qu'ils remplacent). Nous encourageons les développeurs de portefeuilles électroniques et d'applications à explorer des façons d'ajouter aux modes de paiement actuels l'option de paiement totalement anonyme.

4.3.2 Écrans de petite taille

Comme nous en avons fait état à la section 4.1.1, les écrans de petite taille font en sorte qu'il est difficile d'obtenir un consentement valable des utilisateurs, du fait notamment qu'il est peu probable qu'ils lisent attentivement une longue politique de confidentialité sur un appareil mobile. Nous encourageons les développeurs de portefeuilles électroniques et d'applications de paiement à explorer des façons de résoudre ce problème, notamment peut-être en adoptant d'autres méthodes pratiques pour communiquer l'information aux utilisateurs.

---

[135] Institutions financières canadiennes (participants à l'initiative de l'industrie), *Canadian NFC Mobile Payments Reference Model*, version 1.03, 14 mai 2012. Voir http://www.cba.ca/contents/files/misc/msc_20120514_mobile_en.pdf (consulté le 23 mai 2013).

4.3.3 Employés malveillants

À la partie 2, section 6.3, nous avons expliqué qu'une entreprise offrant un instrument ou un service de paiement recueille beaucoup plus d'information sur le client ou le commerçant que l'émetteur de carte de crédit dans les paiements effectués au moyen d'une carte de crédit traditionnelle à un terminal PDV. Si un employé de cette entreprise est mal intentionné, on peut craindre qu'il ait accès à ces renseignements et en fasse un usage qui contrevient aux principes de protection de la vie privée. Nous encourageons les développeurs et les fournisseurs de portefeuilles électroniques et d'applications de paiement à mettre en place des contrôles de vérification rigoureux et d'autres procédures et mesures technologiques concernant l'accès des employés aux données de paiement et autres renseignements sensibles.

4.3.4 Catastrophes naturelles ou d'origine humaine

À la partie 2, section 6.4, nous avons analysé les conséquences éventuelles des catastrophes naturelles ou d'origine humaine, en particulier celles qui rendent illisibles en permanence les systèmes de mémoire. Nous encourageons les développeurs de portefeuilles électroniques et d'applications de paiement à stocker sous une forme récupérable, à tout le moins périodiquement, les documents essentiels (p. ex. les soldes des comptes) pour assurer la continuité des activités en cas de catastrophe. Ces développeurs pourraient indiquer dans leur politique l'endroit où ces documents seront stockés, sous quelle forme, pendant combien de temps et qui y aura accès.

4.3.5 Mise en œuvre insuffisante de mesures de sécurité

Comme nous l'avons mentionné à la partie 2, section 6.5, la technologie permettant d'améliorer la sécurité dans les paiements mobiles existe mais, pour différentes raisons, certaines entreprises en activité sur ce marché ne les adoptent pas. Nous encourageons les développeurs de portefeuilles électroniques et d'applications à utiliser tous les mécanismes de sécurité à leur disposition pour s'assurer que les données de paiement et les autres renseignements sensibles sont protégés comme il se doit en tout temps.

4.3.6 Protocoles de paiement exclusifs

Comme nous l'avons signalé à la partie 2, section 6.8, certains commerçants, institutions financières et marques de paiement envisagent de créer des technologies de portefeuille électronique ou des modes de paiement exclusifs au lieu d'adopter les solutions existantes, peut-être dans le but d'offrir des caractéristiques ou une expérience utilisateur qui semblent leur conférer un avantage concurrentiel. Mais il est de notoriété publique que les opérations de paiement sont très sensibles pour ce qui est de la sécurité et de la protection de la vie privée et qu'il peut être très difficile de les effectuer de façon appropriée. Nous encourageons les développeurs de portefeuilles électroniques et d'applications de paiement à adopter des solutions normalisées ou soumises à un examen minutieux dans la mesure du possible et à s'assurer que des spécialistes de la sécurité et de la protection de la vie privée conçoivent, examinent et analysent tous les aspects exclusifs avant le déploiement auprès des consommateurs afin d'atténuer les risques.

4.3.7 Règlement des différends

À la partie 2, section 6.7, nous avons parlé du manque d'uniformité des pratiques de règlement des différends entre les commerçants et entre les instruments de paiement. En accord avec la position énoncée dans le compte rendu de l'atelier de la FTC sur les paiements mobiles[136] (p. 5-7), nous encourageons les développeurs de portefeuilles électroniques et d'applications de paiement à définir clairement leur politique concernant les frais frauduleux et non autorisés et à la communiquer explicitement aux consommateurs.

4.3.8 Confiscation de fonds et blocage d'opérations

À la partie 2, section 6.9, nous avons fait état de la possibilité que des comptes de cybermonnaie et des opérations de paiement soient bloqués, confisqués ou marqués comme « inacceptables » à la demande d'une autorité ou par erreur. Nous encourageons les développeurs et les fournisseurs de portefeuilles électroniques et d'applications de paiement à s'assurer que leur politique à cet égard est claire pour les utilisateurs et à faire le nécessaire afin d'éviter qu'une telle situation se produise en raison d'erreurs ou de négligence de la part de l'une des entités participantes.

4.3.9 Perte ou vol d'un appareil

En cas de perte ou de vol d'un appareil mobile, l'utilisateur doit généralement aviser les fournisseurs d'applications de paiement (et d'autres entités). Nous encourageons les développeurs et les fournisseurs à poursuivre leurs efforts afin que la procédure soit le plus simple et le moins fastidieuse possible pour les utilisateurs. Entre autres, il peut s'agir de faciliter le verrouillage à distance des applications de paiement et l'effacement à distance des données de l'application. L'utilisateur aura peut-être de la difficulté à trouver qui aviser étant donné que l'appareil mobile peut renfermer de nombreux instruments de paiement et beaucoup plus de données de paiement qu'un portefeuille traditionnel. Nous encourageons les fournisseurs à trouver des façons de faciliter la procédure de notification pour les utilisateurs, peut-être notamment en envoyant périodiquement à leur adresse postale les coordonnées des services à contacter en cas d'urgence.

4.3.10 Intérêt croissant des pirates informatiques

À la partie 2, section 6.13, nous avons signalé que les appareils mobiles présentent depuis quelques années un attrait croissant pour les pirates informatiques, les auteurs de maliciels et les autres fraudeurs, et tout indique que cette tendance se maintiendra. Nous encourageons les développeurs à poursuivre leurs efforts afin que les applications et les portefeuilles électroniques installés sur les appareils mobiles soient dans la mesure du possible exempts de failles susceptibles de porter atteinte à la sécurité et à la protection de la vie privée.

[136] Federal Trade Commission (FTC) des États-Unis, Division of Financial Practices (D. Pozza, P. Poss, J. Chen et coll.), *Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments*, rapport du personnel de la FTC, mars 2013. Voir http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (consulté le 17 mai 2013).

4.4 Organismes de réglementation

Les recommandations dont nous faisons état dans la présente sous-section s'adressent principalement aux organismes qui élaborent des protocoles ou des interfaces standards pour le traitement et la communication dans le cadre des opérations de paiement mobile.

4.4.1 Authentifiant par défaut

D'après le *Canadian NFC Mobile Payments Reference Model*[137] (p. 26), [traduction] « un authentifiant par défaut permet à l'utilisateur final d'effectuer un paiement tout en laissant l'appareil mobile en mode veille sans avoir à sélectionner manuellement un portefeuille électronique ». Cette fonction pourrait accroître le risque qu'un fraudeur utilise une borne de lecture pour s'approprier en douce l'information d'une carte de crédit ou de débit ou effectuer une opération de paiement à l'insu de l'utilisateur. Nous encourageons les organismes de normalisation (en particulier les éditeurs de la prochaine version du modèle de référence le cas échéant) à reconsidérer l'inclusion de cette fonction ou à exiger le consentement de l'utilisateur avant qu'une opération puisse se faire sur un appareil en mode veille.

4.4.2 Service mobile désactivé

D'après le modèle de référence[138] (p. 63, section 10.6.1), [traduction] « même si le service mobile est déconnecté, l'application de paiement peut continuer de fonctionner pour les paiements NFC. » Cette fonction pourrait accroître le risque qu'une opération de paiement frauduleuse soit effectuée à l'insu de l'utilisateur. Nous encourageons les organismes de réglementation (en particulier les éditeurs de la prochaine version du modèle de référence le cas échéant) à reconsidérer l'inclusion de cette fonction ou à exiger le consentement de l'utilisateur avant qu'une opération puisse se faire sur un appareil lorsque le service mobile est déconnecté.

4.5 Commerçants

Les recommandations dont nous faisons état dans la présente sous-section s'adressent principalement aux commerçants.

4.5.1 Catastrophes naturelles ou d'origine humaine

À la partie 2, section 6.4, nous avons analysé les conséquences éventuelles de catastrophes naturelles ou d'origine humaine, en particulier celles qui rendent illisibles en permanence les systèmes de mémoire. Nous encourageons les commerçants à stocker sous une forme récupérable, à tout le moins périodiquement, les documents essentiels pour assurer la continuité des activités en cas de catastrophe. Ils pourraient indiquer dans leur politique l'endroit où ces documents seront stockés, sous quelle forme, pendant combien de temps et qui y aura accès.

---

[137] Institutions financières canadiennes (participants à l'initiative de l'industrie), *Canadian NFC Mobile Payments Reference Model*, version 1.03, 14 mai 2012. Voir http://www.cba.ca/contents/files/misc/msc_20120514_mobile_en.pdf (consulté le 23 mai 2013).

[138] *Ibid.*

4.5.2 Mise en œuvre boguée d'interventions humaines

À la partie 2, section 6.6, nous avons fait état du risque de mise en œuvre boguée. Ce type de faille peut entraîner des différends ou des pertes à la fois pour les commerçants et les clients. Nous encourageons les commerçants à adopter des politiques succinctes et énoncées clairement pour gérer ces situations et à s'assurer de que leurs clients en prennent connaissance (p. ex. en leur envoyant périodiquement des rappels).

4.5.3 Règlement des différends

À la partie 2, section 6.7, nous avons fait état du manque d'uniformité des pratiques de règlement des différends entre les commerçants et entre les instruments de paiement. Conformément à la position énoncée dans le compte rendu de l'atelier de la FTC sur les paiements mobiles[139] (p. 5-7), nous encourageons les commerçants à définir clairement leur politique concernant les frais frauduleux et non autorisés et à la communiquer explicitement aux consommateurs.

4.5.4 Intérêt croissant des pirates informatiques

À la partie 2, section 6.13, nous avons souligné que les appareils mobiles présentent depuis quelques années un attrait croissant pour les pirates informatiques, les auteurs de maliciels et les autres fraudeurs, et tout indique que cette tendance se maintiendra. Nous encourageons les commerçants à poursuivre leurs efforts afin que le système d'exploitation et les applications installés sur tout appareil mobile utilisé comme terminal PDV soient exempts de maliciels en installant les correctifs, les outils antivirus, etc., aussi rapidement que possible (voir la partie 3, section 2.4).

4.6 Utilisateurs finals

Les recommandations dont nous faisons état dans la présente sous-section s'adressent principalement aux utilisateurs finals.

4.6.1 Petite taille de l'écran

Comme nous l'avons signalé à la partie 2, section 6.2, en raison de la petite taille des écrans, les utilisateurs ont de la difficulté à lire attentivement la politique de confidentialité ou toute autre information connexe. Nous encourageons les utilisateurs à s'efforcer d'examiner systématiquement et minutieusement cette information, peut-être en la lisant sur une autre plateforme (p. ex. un PC) pour pouvoir donner un consentement aussi valable que possible.

[139] Federal Trade Commission (FTC) des États-Unis, Division of Financial Practices (D. Pozza, P. Poss, J. Chen et coll.), *Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments*, rapport du personnel de la FTC, mars 2013. Voir http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (consulté le 17 mai 2013).

4.6.2 Mise en œuvre boguée d'interventions humaines

À la partie 2, section 6.6, nous avons fait état du risque de mise en œuvre boguée. Ce type de faille peut entraîner des différends ou des pertes à la fois pour les commerçants et les clients. Nous encourageons les utilisateurs à s'assurer qu'ils comprennent la politique des commerçants applicables à ces situations afin d'avoir conscience des risques auxquels ils sont exposés et des droits afférents.

4.6.3 Règlement des différends

À la partie 2, section 6.7, nous avons fait état du manque d'uniformité des pratiques en matière de règlement des différends entre les commerçants et entre les instruments de paiements. Conformément à la position énoncée dans le compte rendu de l'atelier de la FTC sur les paiements mobiles[140] (p. 5-7), nous encourageons les utilisateurs à se familiariser avec la politique des commerçants au sujet des frais frauduleux et non autorisés afin de bien comprendre leurs droits et responsabilités à cet égard.

4.6.4 Confiscation de fonds et blocage d'opérations

À la partie 2, section 6.9, nous avons fait état de la possibilité que des comptes de cybermonnaie et des opérations de paiement soient bloqués, confisqués ou marqués comme « inacceptables » à la demande d'une autorité ou par erreur. Nous encourageons les utilisateurs à se familiariser avec les politiques sur les portefeuilles électroniques et les applications de paiement (et peut-être les lois pertinentes) applicables à ces situations afin de bien connaître les risques auxquels ils sont exposés ainsi que les droits et protections connexes.

4.6.5 Perte ou vol d'un appareil

En cas de perte ou de vol d'un appareil mobile, l'utilisateur avise généralement l'exploitant du réseau mobile et les fournisseurs d'applications de paiement (voire d'autres entités). Nous encourageons les utilisateurs à tirer parti de toutes les protections qui leur sont offertes par les fabricants de l'appareil et du système d'exploitation, l'exploitant du réseau mobile et les fournisseurs de portefeuilles électroniques et d'applications. Il peut s'agir d'utiliser un mot de passe ou un NIP pour verrouiller l'appareil, le portefeuille électronique et les applications de paiement, d'utiliser un outil de localisation, de chiffrer les données à distance et d'utiliser une fonction d'effacement à distance. L'utilisateur aura de la difficulté à trouver qui aviser étant donné que l'appareil mobile peut contenir de nombreux instruments de paiement et beaucoup plus de données de paiement qu'un portefeuille traditionnel. Nous encourageons les utilisateurs à stocker à un endroit facilement accessible, ailleurs que sur l'appareil mobile, les coordonnées des services à contacter en cas d'urgence. Le *Canadian NFC Mobile Payments Reference Model*[141] (p. 59-61, section 10.5.4), présente un diagramme de haut niveau montrant les principales tâches qui incombent à l'exploitant de réseau mobile après qu'un utilisateur l'a informé de la perte ou du vol d'un appareil.

---

[140] Federal Trade Commission (FTC) des États-Unis, Division of Financial Practices (D. Pozza, P. Poss, J. Chen et coll.), *Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments*, rapport du personnel de la FTC, mars 2013. Voir http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (consulté le 17 mai 2013).

[141] Institutions financières canadiennes (participants à l'initiative de l'industrie), *Canadian NFC Mobile Payments Reference Model*, version 1.03, 14 mai 2012. Voir http://www.cba.ca/contents/files/misc/msc_20120514_mobile_en.pdf (consulté le 23 mai 2013).

4.6.6 Effacement à distance

Comme nous l'avons signalé à la partie 2, section 6.12 et dans l'annexe, on ne sait pas avec certitude si l'effacement à distance est efficace pour empêcher toute récupération des données. Nous encourageons les utilisateurs à ne pas trop compter sur ce mécanisme, qui n'effacera peut-être pas les données comme prévu, et à prendre des mesures pour réduire la quantité de renseignements personnels stockées inutilement sur l'appareil. En outre, les utilisateurs jugeront peut-être utile d'explorer d'autres mécanismes pour supprimer les données de façon sécuritaire, notamment un éventail d'applications ou de services (par exemple voir Blancco[142] ou la section 3.4.3 de la note du CSTC sur l'effacement des supports de stockage électronique[143]).

4.6.7 Intérêt croissant des pirates informatiques

À la partie 2, section 6.13, nous avons souligné que les appareils mobiles présentent depuis quelques années un attrait croissant pour les pirates informatiques, les auteurs de maliciels et les autres fraudeurs, et tout indique que cette tendance se maintiendra. Nous encourageons les utilisateurs à prendre toutes les précautions possibles pour protéger leur appareil, notamment à télécharger et à installer uniquement un portefeuille électronique fiable (c.-à-d. provenant d'une source digne de confiance) et à faire le nécessaire afin que leur appareil soit exempt de maliciels (p. ex. en installant les derniers correctifs de sécurité, les outils antivirus, etc.). Nous les encourageons également à ne pas « rooter » ni débrider leur appareil mobile, ce qui le rendrait plus vulnérable aux logiciels malveillants.

5. Conclusion

La partie 3 du rapport présente des recommandations au chapitre de la sécurité et de la protection de la vie privée qui se rapportent à différents modes de paiement mobile particuliers ou de façon générale à l'ensemble ou à la plupart des modes de paiement électronique. Certaines recommandations sont classées en fonction des groupes auxquels elles s'adressent, notamment les fabricants d'appareils et de systèmes d'exploitation, les exploitants de réseau mobile, les développeurs de portefeuilles électroniques et d'applications, les organismes de normalisation, les commerçants et les utilisateurs finals.

[142] Blancco Mobile, *Erase all data securely from smartphones and tablets*, 2011. Voir http://www.blancco.com/en/products/total-data-erasure/mobile/ (consulté le 27 mai 2013).

[143] Centre de la sécurité des télécommunications Canada (CSTC), *Effacement et déclassification des supports d'information électroniques – ITSG-06*, juillet 2006. Voir http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg06-fra.html (consulté le 12 juin 2013).

Références

Ananda, F. et J. Kiptum. *Security Issues in M-Banking*, présentation donnée lors de l'Information Security and Cyber Forensics Conference, du 29 au 31 octobre 2008. Voir http://www.strathmore.edu/pdf/M-Pesa.pdf (consulté le 12 juin 2013).

Bankelele (auteur de Nairobi s'intéressant aux opérations bancaires, aux finances, à la technologie et aux investissements). *How to Get n M-Pesa Refund and other Safaricom tales*, 29 juin 2009. Voir http://www.bankelele.co.ke/2009/06/how-to-get-M-Pesa-refund.html (consulté le 22 avril 2013).

Barker, E. et A. Roginsky. *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, publication spéciale du NIST n° 800-131A, janvier 2011, p. 13-14. Voir http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf (consulté le 13 mai 2013).

BBC News Technology. « Frozen Android phones give up data secrets », 7 mars 2013. Voir http://www.bbc.co.uk/news/technology-21697704 (consulté le 19 avril 2013).

Berkes, J. *Side-Channel Monitoring of Contactless Java Cards*, mémoire de maîtrise, Département de génie électrique et informatique,Université de Waterloo, 2008. Voir http://www.berkes.ca/archive/jb-thesis-final-electronic.pdf (consulté le 26 mars 2013).

BlackBerry Support Community Forums. « BlackBerry 10 – NFC Card Emulation », 2 novembre 2012. Voir http://supportforums.blackberry.com/t5/Native-Development/BlackBerry-10-NFC-Card-Emulation/ta-p/1940867 (consulté le 20 mars 2013). Voir aussi « NFC Primer for Developers », 14 février 2012, http://supportforums.blackberry.com/t5/Java-Development/NFC-Primer-for-Developers/ta-p/1334857 (consulté le 20 mars 2013).

Blancco Mobile. *Erase all data securely from smartphones and tablets*, 2011. Voir http://www.blancco.com/en/products/total-data-erasure/mobile/ (consulté le 27 mai 2013).

Bradley, M. *Digital Wallets Executive Briefing*, Information Technology Association of Canada (ITAC) Digital Commerce Forum: How Wallet is Going Digital, 16 avril 2013. Voir http://itac.ca/files/2013_april_16_digital_wallet_presentation.pdf (consulté le 1er mai 2013).

Canada Newswire. « La Banque CIBC et Rogers présentent le futur en matière de paiements mobiles au Canada », 15 mai 2012. Voir http://www.newswire.ca/fr/story/974983/la-banque-cibc-et-rogers-presentent-le-futur-en-matiere-de-paiements-mobiles-au-canada (consulté le 22 février 2013).

Carrington, D., *US Mobile Payments Forecast 2013 – 2017: Mobile Payments to Reach $90B by 2017*. Forrester Research, Inc., 16 janvier 2013. Voir http://blogs.forrester.com/denee_carrington/13-01-16-us_mobile_payments_forecast_2013_2017_mobile_payments_to_reach_90b_by_2017 (consulté le 27 février 2013).

Centre de la sécurité des télécommunications Canada (CSTC). *Effacement et déclassification des supports d'information électroniques – ITSG-06*, juillet 2006. Voir http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg06-fra.html (consulté le 12 juin 2013).

Centre de la sécurité des télécommunications Canada (CSTC). Produits certifiés selon les critères communs. Voir http://www.cse-cst.gc.ca/its-sti/services/cc/cp-pc-fra.html (consulté le 12 juin 2013).

Charrat, B. *Debunking NFC Peer-to-Peer Myths*, Inside Secure, février 2012. Voir http://insidesecure.com/eng/Media/White-papers (consulté le 20 février 2013).

Chaum, D., A. Fiat et M. Naor. « Untraceable Electronic Cash », dans *Advances in Cryptology: Proceedings of CRYPTO '88*, S. Goldwasser (sous la dir. de), Springer-Verlag, 1989, p. 319-327.

Collins, J. « Mobile payments deal between Visa and Monitise is formed », *Mobile Commerce News*, 11 mars 2013. Voir http://www.qrcodepress.com/mobile-payments-deal-between-visa-and-monitise-is-formed/8518094/ (consulté le 16 avril 2013).

Comité technique conjoint ISO/IEC n° 1, sous-comité n° 17. *ISO/IEC 7816 : Cartes d'identification – cartes à circuit(s) imprimé(s)- Cartes avec contact.*

Comité technique conjoint ISO/IEC n° 1, sous-comité n° 17, groupe de travail n° 8. *Cartes d'identification ISO/IEC 14443 – Cartes à circuit(s) imprimé(s) sans contact – Cartes de proximité*.

CommTech Knowledge. *NFC-Near Field Communication: General Architecture of NFC Enabled Mobile Phones*. Voir http://mp-nfc.org/nfc_near_field_communication_architecture.html (consulté le 15 mars 2013).

Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC). *Vous avez des droits – Renseignements sur vos services téléphoniques locaux de résidence*, section « Votre droit de contester les frais ou de déposer une plainte ». Voir http://www.bell.ca/web/common/fr/all_regions/pdfs/wireline/SCR_Final.pdf (consulté le 10 mai 2013).

Constine, J. « Bump Pay Lets You PayPal Someone With A Tap, But Only In-Person », *TechCrunch Hot Topics*, 29 mars 2012. Voir http://techcrunch.com/2012/03/29/bump-pay/ (consulté le 20 février 2013).

Cowley, S. « NFC exploit: Be very, very careful what your smartphone gets near », *CNNMoney*, 26 juillet 2012. Voir http://money.cnn.com/2012/07/26/technology/nfc-hack/index.htm (consulté le 23 mai 2013).

Crowe, M. et E. Tavilla (Federal Reserve Bank of Boston). *Mobile Phone Technology: "Smarter" Thank We Thought: How Technology Platforms are Security Mobile Payments in the U.S.*, 16 novembre 2012. Voir http://www.bos.frb.org/bankinfo/payment-strategies/publications/2012/mobile-phone-technology.pdf (consulté le 21 mars 2013).

Dolcourt, J. « Making Sense of Mobile Payment », *CNET*, 13 août 2010. Voir http://www.cnet.com/8301-17918_1-20013480-85.html (consulté le 14 février 2013).

Dolcourt, J. « Start Your Own Business with Square for Android », *CNET*, 19 mai 2010. Voir http://www.cnet.com/8301-19736_1-20005441-251.html (consulté le 14 février 2013).

Dolcourt, J. « Who Will Profit from NFC, Mobile Payments? », *CNET*, 7 avril 2011. Voir http://www.cnet.com/8301-17918_1-20049894-85.html (consulté le 14 février 2013).

Duffy, J. « Pay with Square (for iPhone) », *PC Magazine* (pcmag.com), 9 août 2012. Voir http://www.pcmag.com/article2/0,2817,2408287,00.asp (consulté le 5 avril 2013). [Cette technologie est aussi mentionnée sans détails à l'adresse https://squareup.com/ca/portefeuille électronique.]

Elenkov, N. *Accessing the embedded secure element in Android 4.x*, 22 août 2012. Voir http://nelenkov.blogspot.ca/2012/08/accessing-embedded-secure-element-in.html#!/2012/08/accessing-embedded-secure-element-in.html (consulté le 12 mars 2013).

Ericsson, D. *The role of SIM OTA and the Mobile Operator in the NFC environment*, livre blanc de SmartTrust, avril 2009. Voir http://www.paymentscardsandmobile.com/research/reports/SIM-OTA-Mobile-Operator-role-NFC.pdf (consulté le 12 mars 2013).

Evans, P. Rogers Wants to Start a Bank », *CBC News*, 6 septembre 2011. Voir http://www.cbc.ca/news/business/story/2011/09/06/rogers-bank.html (consulté le 22 février 2013).

Federal Communications Commission (FCC) des États-Unis. Matériel infographique sur le bourrage de factures. Voir http://www.ftc.gov/os/2011/12/111227crammingcomment.pdf (consulté le 8 avril 2013).

Federal Trade Commission (FTC) des États-Unis, Division of Financial Practices (D. Pozza, P. Poss, J. Chen et coll.). *Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments*, rapport du personnel de la FTC, mars 2013. Voir http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (consulté le

17 mai 2013).
Gabriel, C. « PayPal extends mobile wallet, but no NFC », *Rethink Wireless*, 15 janvier 2013. Voir http://www.rethink-wireless.com/2013/01/15/paypal-extends-mobile-wallet-nfc.htm (consulté le 22 février 2013).
Global Platform. *Card Specification*, version 2.2, mars 2006. Voir http://www.win.tue.nl/pinpasjc/docs/GPCardSpec_v2.2.pdf (consulté le 15 mars 2013).
Google Play. *Achats avec facturation par l'opérateur*. Voir https://support.google.com/googleplay/answer/167794?hl=fr&ctx=topic (consulté le 8 avril 2013).
Groupe de travail sur l'examen du système de paiement. *Le passage au numérique : Faire la transition vers les paiements numériques,* rapport présenté au ministre des Finances, 2011. Voir http://paymentsystemreview.ca/wp-content/themes/psr-esp-hub/documents/r03_fra.pdf (consulté le 13 février 2013).
Groupe Speciale Mobile Association (GSMA). *Mobile NFC in Retail*, livre blanc, version 1.0, septembre 2012. Voir http://www.gsma.com/mobilenfc/wp-content/uploads/2012/10/Mobile-NFC-in-Retail-White-Paper-Oct-2012.pdf (consulté le 23 mai 2013).
Hardy, I. « WIND Mobile goes live with BlackBerry World carrier billing », *MobileSyrup*, 1er avril 2013. Voir http://mobilesyrup.com/2013/04/01/wind-mobile-goes-live-with-blackberry-world-carrier-billing/(consulté le 30 avril 2013).
Hermon-Duc, S. (chef du projet TSF). *MPESA project analysis: Exploring the use of cash transfers using cell phones in pastoral areas*, rapport de projet de Télécoms sans frontières, 2012. Voir http://www.alnap.org/pool/files/mpesa-project-analysis-tsf-vsfg.pdf (consulté le 12 avril 2013).
Holly, R. « How to use NFC to automate your mobile routine », *geek.com*, 8 février 2012. Voir http://www.geek.com/articles/mobile/how-to-use-nfc-to-automate-your-mobile-routine-2012028/ (consulté le 25 mars 2013).
Inside Secure. *Opening the NFC stack to Java and native applications*, document d'information de l'entreprise, novembre 2010. Voir http://www.insidesecure.com/content/download/1095/12802/version/6/file/WHITE%20PAPER_NEW%20CHARTE-3.pdf (consulté le 15 mars 2013).
Institutions financières canadiennes (participants à l'initiative de l'industrie). *Canadian NFC Mobile Payments Reference Model*, version 1.03, 14 mai 2012. Voir http://www.cba.ca/contents/files/misc/msc_20120514_mobile_en.pdf (consulté le 23 mai 2013).
Isis Mobile Wallet (Isis a été fondée par AT&T Mobility, T-Mobile USA et Verizon Wireless pour réaliser leur vision commune du commerce mobile). Voir http://www.paywithisis.com/ (consulté le 28 février 2013).
Jackson, B. « Google Wallet and NFC security: guarding against "sharks with lasers" », *IT Business*, 29 septembre 2011. Voir http://www.itbusiness.ca/news/google-wallet-and-nfc-security-guarding-against-sharks-with-lasers/16531 (consulté le 4 avril 2013).
Kerschberger, M. *Near Field Communication: A survey of safety and security measures*, Bachelorarbeit, Université technique de Vienne, 17 juillet 2011. Voir https://www.auto.tuwien.ac.at/bib/pdf_TR/TR0156.pdf (consulté le 26 mars 2013).
Kessler, S. *Bank Lets Customers Pay Friends By Bumping iPhones*, 29 avril 2011. Voir http://mashable.com/2011/04/29/ing-direct-customers-bump/ (consulté le 20 février 2013).
Kharif, O. « NFC Stickers Make Smartphones Smarter », *Bloomberg Businessweek: Technology*, 12 juillet 2012. Voir http://www.businessweek.com/articles/2012-07-12/nfc-stickers-make-smartphones-smarter (consulté le 25 mars 2013).

Knight, S. « Americans lost $30 billion worth of mobile phones in 2011 », *TechSpot*, 23 mars 2012. Voir http://www.techspot.com/news/47930-americans-lost-30-billion-worth-of-mobile-phones-in-2011.html (consulté le 23 avril 2013).

Kremer, J. *NFC: Near Field Communication White Paper*, Jan Kremer Consulting Services. Voir http://jkremer.com/White%20Papers/Near%20Field%20Communication%20White%20Paper%20JKCS.pdf (consulté le 23 mai 2013).

Lewis, M. « Registry targets smartphone black market », *The Toronto Star: Business*, 8 novembre 2012. Voir http://www.thestar.com/business/2012/11/08/registry_targets_smartphone_black_market.html (consulté le 12 juin 2013).

Loi sur la protection des renseignements personnels et les documents électroniques. Voir http://laws-lois.justice.gc.ca/fra/lois/P-8.6/index.html; analyse des dispositions de la Loi, voir http://www.LPRPDE.info/a/1.html (consultés le 12 juin 2013).

London Action Plan (LAP) et Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG). *Best Practices to Address Online and Mobile Threats*, 15 octobre 2012. Voir http://www.maawg.org/sites/maawg/files/news/M3AAWG_LAP_Best_Practices_to_Address_Online_and_Mobile_Threats_0.pdf (consulté le 17 mai 2013).

Mick, J. « Inside the Mega-Hack of Bitcoin: the Full Story », *DailyTech*, 19 juin 2011. Voir http://www.dailytech.com/Inside+the+MegaHack+of+Bitcoin+the+Full+Story/article21942.htm (consulté le 3 mai 2013).

Mobile Transaction. *Growing Use of SMS Payments Around the World*. Voir http://www.mobiletransaction.org/sms-payments/around-the-world (consulté le 20 février 2013).

Moffa, T. (Centre de la sécurité des télécommunications Canada). *Algorithmes cryptographiques approuvés par le CSTC pour la protection des renseignements sensibles et pour les applications d'authentification et d'autorisation électroniques au sein du GC*, ALERTE ITSA-11 DU CSTC, mars 2011, section « Algorithmes de hachage et situation de l'algorithme SHA-1 ». Voir http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11e-fra.html (consulté le 13 mai 2013).

Monnaie royale canadienne. *Ressources pour développeurs d'applications Cybermonnaie*. Voir http://developer.mintchipchallenge.com/devguide/index.php (consulté le 14 février 2013).

Monnaie royale canadienne. *Ressources pour développeurs d'applications Cybermonnaire : Message Validation*, 4 avril 2012. Voir http://developer.deficybermonnaie.com/devguide/developing/common/message-validation.html (consulté le 8 avril 2013).

Monnaie royale canadienne. *Ressources pour développeurs d'applications Cybermonnaie : Cybermonnaie Messages*, 4 avril 2012. Voir http://developer.deficybermonnaie.com/devguide/developing/common/mintchip-messages.html (consulté le 8 avril 2013).

National Institute of Standards and Technology (NIST) des États-Unis. « NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition », *NIST Tech Beat*, 2 octobre 2012. Voir http://www.nist.gov/itl/csd/sha-100212.cfm (consulté le 8 avril 2013).

NFC Times. « Topic: "Trusted Service Manager" », 2013 (recueil de contrats conclus récemment avec des gestionnaires de services de confiance). Voir http://nfctimes.com/tags/trusted-service-manager (consulté le 28 février 2013).

NFC World. « A Definitive List of NFC Phones », mis à jour le 19 février 2013. Voir http://www.nfcworld.com/nfc-phones-list/ (consulté le 19 février 2013).

Pauli, D. « Android app steals contactless credit card data », *SC Magazine*, 21 juin 2012. Voir http://www.scmagazine.com.au/News/305881,android-app-steals-contactless-credit-card-data.aspx (consulté le 22 mars 2013).

Payment Card Industry (PCI) Security Standards Council, Emerging Technologies. *PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users*, version 1.0, février 2013. Voir https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf (consulté le 17 mai 2013).

Payment Card Industry (PCI) Security Standards Council. *Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance for Transmissions of Cardholder Data and Sensitive Authentication Data*, livre blanc d'Emerging Technology, Guide de programme, version 1.0, 5 octobre 2010. Voir https://www.pcisecuritystandards.org/pdfs/pci_ptp_encryption.pdf (consulté le 1er mai 2013).

Payment Card Industry Security Standards Council, Emerging Technologies. *PCI Mobile Payment Acceptance Security Guidelines*, version 1.0, février 2013. Voir https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Commerçants_v1.pdf (consulté le 1er mars 2013).

PayPal. *Texting with PayPal – easy as lifting a finger*. Voir https://personal.paypal.com/ca/cgi-bin/?cmd=_render-content&content_ID=marketing_ca/mobile_text (consulté le 20 février 2013).

Pipenbrinck, N. « Secure Element communication with PCD/reader », *stackoverflow*, 22 juin 2012. Voir http://stackoverflow.com/questions/11152614/secure-element-communication-with-pcd-reader (consulté le 4 avril 2013).

Ricknas, M. « Inside Secure Opens Door for Multiple Wallets on One Smartphone », *CIO Drilldowns*, 29 octobre 2012. Voir http://www.cio.com/article/720174/Inside_Secure_Opens_Door_for_Multiple_Wallets_on_One_Smartphone (consulté le 21 mars 2013).

Roland, M., C. Saminger et J. Langer. *Packet Sniffer for the Physical Layer of the Single Wire Protocol*, rapport de recherche, Universités de sciences appliquées de la Haute-Autriche. Voir http://research.fh-ooe.at/files/publications/941_PacketSnifferPhysicalLayerSWP.pdf (consulté le 19 mars 2013).

Rosa, T. *RFID Wormholes: The Case of Contactless Smartcards*, SmartCard Forum, Prague (République tchèque), 2011. Voir http://crypto.hyperlink.cz/files/rosa_wormhole_v1a.pdf (consulté le 26 mars 2013).

Samuel, S. « New in the Android Market: Updated PayPal Mobile App Featuring P2P NFC Capabilities », *The PayPal Blog*, 8 novembre 2011. Voir https://www.thepaypalblog.com/2011/11/new-in-the-android-market-updated-paypal-mobile-app-featuring-p2p-nfc-capabilities-2/ (consulté le 20 février 2013).

Sequent, définitions dans le site Web. Voir http://www.sequent.com/glossary/s (consulté le 12 mars 2013).

Sequent, définitions dans le site Web. Voir http://www.sequent.com/glossary/n (consulté le 15 mars 2013).

Smart Card Alliance. *Security of Proximity Mobile Payments*, livre blanc du Smart Card Alliance Contactless and Mobile Payments Council, publication CPMC-09001, mai 2009. Voir http://collaboration/lib-bib/Library%20Document%20Collection/Security%20of%20Proximity%20Mobile%20Payments.pdf (consulté le 14 février 2013).

Snopes.com. « Electronic Pickpocketing », 4 octobre 2012. Voir http://www.snopes.com/fraud/identity/pickpocket.asp (consulté le 22 mars 2013). Voir aussi http://www.youtube.com/watch?v=EKks3vfiy6Q

Square, Inc. *Caisse Square*. Voir https://squareup.com/ca/register (consulté le 5 avril 2013).

Square, Inc. *Square Pricing.* Voir https://squareup.com/ca/pricing (consulté le 27 février 2013).

Square, Inc. Voir https://squareup.com/ca?country_code=ca (consulté le 5 avril 2013).

Stark, J. *Mobile Payments: Starbucks App*, 20 juin 2011. Voir http://jonathanstark.com/blog/mobile-payments-starbucks-app (consulté le 27 février 2013). Voir aussi http://www.starbucks.ca/coffeehouse/mobile-apps/mystarbucks.

Telco 2.0 News Review (blogue). « Security Breach at M-PESA: Telco 2.0 Crash Investigation », Telco 2.0, 12 février 2010. Voir http://www.telco2.net/blog/2010/02/security_breach_at_mpesa_telco.html (consulté le 12 avril 2013).

Terdiman, D. « Prowling the streets of San Francisco with Square Wallet », *CNET News*, 20 novembre 2012. Voir http://news.cnet.com/8301-1023_3-57552199-93/prowling-the-streets-of-san-francisco-with-square-wallet/ (consulté le 5 avril 2013).

The Paypers: Insights in Payments. « Brazil: PagSeguro, Nokia to introduce NFC P2P payments », 3 mai 2012. Voir http://www.thepaypers.com/news/mobile-payments/brazil-pagseguro-nokia-to-introduce-nfc-p2p-payments/747502-16 (consulté le 22 février 2013).

VeriFone. *PAYware Mobile e100*. Voir http://www.paywaremobile.com/ (consulté le 14 février 2013).

Visa. *Digital Wallet Security: Just 'LOK' it*. Voir http://www.cimbbank.com.my/creditcard/index.php?ch=2&pg=14&ac=9&bb=attachment (consulté le 21 mars 2013).

Walubengo, N. « The Mobile Money Apocalypse; What Would Happen to Your Money? », *PesaTalk*, 2 novembre 2012. Voir http://pesatalk.com/the-mobile-money-apocalypse-what-would-happen-to-your-money/ (consulté le 17 avril 2013).

Wanjiku, R. « Security issues hit African mobile money providers », *Computerworld,* 17 novembre 2009. Voir http://news.idg.no/cw/art.cfm?id=03381EE0-1A64-6A71-CE896C46D67B6FFC (consulté le 12 avril 2013).

Whitwam, R. « How To Have Fun with Near Field Communication on Android », *Tested*, 27 avril 2011. Voir http://www.tested.com/tech/android/2234-how-to-have-fun-with-near-field-communication-on-android/ (consulté le 25 mars 2013).

Wikipedia, the Free Encyclopedia. « Digital Wallet ». Voir http://en.wikipedia.org/wiki/Digital_wallet (consulté le 15 février 2013). Voir aussi *A Global Overview of Digital Wallet Technologies*, publié par le ID Lab, Université de Toronto, 28 mai 2011. Voir http://propid.ischool.utoronto.ca/digiportefeuille électronique_overview/ (consulté le 15 février 2013).

Wikipedia, the Free Encyclopedia. « NFC-WI ». Voir http://en.wikipedia.org/wiki/NFC-WI (consulté le 15 mars 2013).

Wikipedia, the Free Encyclopedia. « PayPal ». Voir http://en.wikipedia.org/wiki/PayPal (consulté le 20 février 2013).

Wikipedia, the Free Encyclopedia. « Single Wire Protocol ». Voir http://en.wikipedia.org/wiki/Single_Wire_Protocol (consulté le 15 mars 2013).

Yawe, R. *How secure is mpesa*, KICTAnet (Kenya ICT Action Network), juillet 2011. Voir http://www.kictanet.or.ke/?p=713 (consulté le 22 avril 2013).

Annexe : Effacement à distance sur les appareils mobiles

[Les deux premiers paragraphes ci-après résument un courriel personnel envoyé à l'un de mes collègues par un membre du personnel de recherche-développement d'une entreprise de gestion d'appareils mobiles.]

Les appareils mobiles font généralement appel à la technologie de la mémoire flash, qui est extrêmement différente de celle du disque dur utilisée sur les ordinateurs de bureau et (certains) ordinateurs portatifs. Plus précisément, la mémoire flash comporte une caractéristique singulière : chaque emplacement de mémoire a une durée de vie prévue correspondant au nombre d'écritures qui peuvent être effectuées. Pour prolonger la durée de vie de ce type de mémoire, l'appareil comporte un algorithme qui répartit les données uniformément de manière à prévenir l'usure. Les données sont ensuite réparties sur l'ensemble des puces de mémoire flash et une logique intelligente les convertit en un format lisible analogue à un système de fichiers de disque dur.

Examinons maintenant la suppression de fichiers sur la mémoire flash d'un appareil mobile. Pour mettre en œuvre la fonction de « suppression sécurisée » (dont il est question à la partie 2, section 6.12, en utilisant de nouvelles données purement aléatoires pour écraser à plusieurs reprises l'information stockée sur le fichier choisi), il serait nécessaire d'inscrire beaucoup de données un peu partout dans la mémoire, ce qui userait prématurément la mémoire flash. C'est pourquoi cette option est exclue. Il semble donc probable que si un fraudeur voulait récupérer des données en lisant chaque emplacement de mémoire, il pourrait récupérer les fichiers qui y sont stockés.

En outre, dans le système d'exploitation de certains appareils mobiles (p. ex. iOS et Android), les applications sont compartimentées, si bien qu'une application peut inscrire des données uniquement dans l'espace qui lui est réservé; elle n'a pas accès aux fichiers des autres applications. Il est donc tout à fait impossible de créer dans ces systèmes d'exploitation une application permettant d'effacer l'information à distance sur l'appareil entier.

Signalons qu'Apple fournit son propre logiciel de gestion à distance, qui comprend une option pour rétablir les réglages d'usine. D'après les premiers essais, il s'agit d'une procédure sécuritaire concernant la récupération de données (peu de données sont récupérables après l'utilisation de cette fonction, ou peut-être même aucune). Toutefois, l'option d'effacement du contenu de l'appareil après un certain nombre de tentatives de saisie du mot de passe n'est pas sécuritaire et la plus grande partie des données peuvent être récupérées.

Enfin, la fonction d'effacement à distance d'Apple est efficace (à tout le moins pour les réglages d'usine), mais la plupart des entreprises de gestion d'appareils mobiles mettent en œuvre leur propre version, qui est souvent peu sécuritaire. Par exemple, l'ancien propriétaire d'une tablette Android (Acer Iconia) achetée d'occasion sur eBay avait supposément rétabli les réglages d'usine. Or, une récupération aux fins d'examen prospectif a permis de voir les fichiers encore accessibles : l'analyse a révélé que des photos de l'ancien propriétaire figuraient parmi les fichiers récupérés, ainsi que des images de pages Web consultées.

Liste des sigles

AES	Advanced Encryption Standard
CPVP	Commissariat à la protection de la vie privée du Canada
CSTC	Centre de la sécurité des télécommunications Canada
DES	Data Encryption Standard
EEPROM	Electrically-Erasable Programmable Read-Only Memory
FIPS	Federal Information Processing Standards des États-Unis
FTC	Federal Trade Commission des États-Unis
HCI	Host Controller Interface
IP	Internet Protocol
ISO	Organisation internationale de normalisation
LAP	London Action Plan
LPRPDE	*Loi sur la protection des renseignements personnels et les documents électroniques*
M^3AAWG	Messaging, Malware and Mobile Anti-Abuse Working Group
mAccept	Acceptation mobile
mCommerce	Commerce mobile
MicroSD	(Micro-sized) Secure Digital memory card
mP2P	Paiement mobile de personne à personne
mPOS	Paiement mobile à un terminal de point de vente
NFC	Communication en champ proche (*Near Field Communication)*
NFC-WI	NFC Wired Interface
NIP	Numéro d'identification personnel
OTA	Over-the-Air
PC	Ordinateur personnel (*Personal Computer*)
PCISSC	Payment Card Industry Security Standards Council
PDV	Point de vente
RAM	Mémoire vive (*Random Access Memoray*)
RSA	Rivest-Shamir-Adleman Cryptographic Algorithm
SHA-1	Secure Hash Algorithm 1 (de même SHA-2 et SHA-3)
SIM	Module d'identification de l'abonné (*Subscriber Identity Module*)
SWP	Single Wire Protocol
TLS	Transport Layer Security
UICC	Carte de circuit intégré universelle (*Universal Integrated Circuit Card*)
USB	Universal Serial Bus
VVC	Valeur de vérification de la carte

Définitions

Acceptation mobile (mAccept) : Mode de paiement mobile où les opérations financières se font entre un individu et un commerçant qui utilise un appareil mobile (et non un terminal de point de vente traditionnel).

Appareil mobile : Appareil informatique de petite taille (p. ex. un téléphone intelligent ou une tablette) généralement équipé d'un écran d'affichage tactile et/ou d'un clavier miniature. Cet appareil est équipé d'un système d'exploitation et peut exécuter divers types de logiciels d'application. Il est souvent doté d'une connexion Internet, d'une caméra et d'un lecteur multimédia.

Attaque de l'intercepteur : Forme d'attaque où le fraudeur établit une connexion distincte avec les victimes pour relayer les messages entre elles en leur faisant croire qu'elles se parlent directement sur une connexion privée alors qu'il contrôle en fait toute la conversation.

Commerce mobile (mCommerce) : Mode de paiement mobile où un individu utilise une application ou le navigateur d'un appareil mobile pour effectuer un achat ou une opération bancaire en ligne dans un site Web à distance.

Débridage d'un appareil mobile : Élimination des restrictions mises en place sur les appareils Apple utilisant le système d'exploitation iOS. Le débridage donne accès au système d'exploitation comme super-utilisateur, permettant ainsi de télécharger des applications, des extensions et des thèmes supplémentaires qui ne sont pas offerts par l'App Store officiel d'Apple. Il s'agit d'une forme d'augmentation des privilèges.

Déverrouillage d'un appareil mobile : Contournement des contraintes mises en place pour limiter l'utilisation d'un appareil à certains pays et fournisseurs de réseau.

Élément de sécurité : Circuit intégré inviolable permettant d'héberger des applications de façon sécuritaire (y compris des applications de paiement) et les données confidentielles et cryptographiques s'y rapportant (p. ex. les clés de chiffrement).

Étiquette NFC : Puce d'identification par radiofréquence (RFID) de faible portée qui communique avec un lecteur utilisant la technologie NFC. Il s'agit d'un dispositif passif, c'est-à-dire que l'étiquette NFC n'a pas sa propre source d'énergie (pile), mais qu'elle puise dans l'appareil qui la lit l'énergie nécessaire pour fonctionner.

Maliciel (logiciel malveillant) : Logiciel hostile ou intrusif utilisé ou programmé par un fraudeur pour perturber le fonctionnement d'un ordinateur, recueillir des renseignements sensibles ou avoir accès à des systèmes informatiques privés.

Paiement mobile à un terminal de point de vente (mPOS) : Mode de paiement mobile où les opérations financières se font entre une personne utilisant un appareil mobile et un commerçant utilisant un terminal de point de vente (parfois sans contact).

Paiement mobile de personne à personne (mP2P) : Mode de paiement mobile où les opérations financières (généralement des transferts de fonds) se font entre deux personnes qui ne sont pas des commerçants enregistrés. Les deux personnes utilisent un appareil mobile pour ces opérations.

Portefeuille électronique : Application (portefeuille électronique mobile) ou service sur un serveur ou dans un nuage (portefeuille électronique numérique) qui gère les instruments de paiement et les données connexes. Le portefeuille électronique possède une interface utilisateur de sorte que l'utilisateur peut choisir et activer des instruments de paiement particuliers (notamment des cartes de crédit et de débit, des cartes de fidélité et des coupons) au moment d'une opération de paiement.

« Rootage » d'un appareil mobile : Intervention similaire au débridage (voir ci-dessus), mais utilisée pour les appareils mobiles équipés du système d'exploitation Android. Le « rootage » confère aux applications installées par l'utilisateur les privilèges de l'administrateur, ce qui leur permet d'exécuter des commandes privilégiées généralement inaccessibles dans la configuration de série, notamment la modification ou la suppression de fichiers système, la suppression d'applications installées par l'exploitant ou le fabricant et l'accès aux composants du matériel.

Valeur de vérification de la carte (VVC) : Numéro de trois ou quatre chiffres imprimé sur la carte de crédit ou de débit ou sur la bande de signature au dos de la carte. Ce numéro, qui n'est pas encodé sur la banque magnétique, constitue une mesure de sécurité (les commerçants peuvent le demander pour les opérations sans carte).