Paiements mobiles NFC au Canada

Modèle de référence

Version : 1.04

Date : 01-NOV-2012

Remarque : Version publique mise à jour

1 INTRODUCTION

Publié en août 2011, le rapport intermédiaire du Groupe de travail sur l'examen du système de paiement du gouvernement du Canada (le « groupe de travail ») soulignait la nécessité pour les acteurs de l'industrie des services financiers de travailler de concert à l'élaboration d'un cadre relatif aux paiements mobiles. C'est dans ce contexte qu'a été créée une initiative visant l'industrie des institutions financières (« IF ») canadiennes.

Les banques et les coopératives de crédit canadiennes ont collaboré à l'élaboration des normes contenues dans le présent document, qui visent l'adoption accélérée des paiements mobiles au pays, afin que tous les Canadiens puissent profiter de cette avancée technologique. L'élaboration de normes visant les paiements mobiles se situe dans la foulée des travaux réalisés par le groupe de travail du gouvernement fédéral. Ce dernier a demandé aux IF d'élaborer des normes à cet égard et les institutions participantes ont travaillé d'arrache-pied d'octobre 2011 à janvier 2012 pour atteindre cet objectif.

Les IF canadiennes participant à cette initiative (les « participants à l'initiative ») reconnaissent que les utilisateurs finaux s'attendent à ce qu'elles offrent des services sûrs et sécuritaires. De plus, les utilisateurs finaux exigent de garder le contrôle sur le type de paiement utilisé et sur le moyen d'y accéder. À cette fin, le présent modèle de référence des paiements mobiles fait en sorte que les consommateurs aient le dernier mot concernant la protection de leurs paiements par un mot de passe et les types de paiement pouvant être exécutés à l'aide de leur appareil mobile. Les marchands et les consommateurs s'attendent également à ce que la transparence au point de vente (« PDV ») soit assurée. Le présent document a été élaboré dans le but de répondre à cette attente et d'accélérer l'adoption des paiements mobiles.

Pour fonctionner efficacement, l'écosystème des paiements mobiles exige les efforts concertés de nombreuses parties prenantes. Il est à souhaiter que le fait de fournir tôt des lignes directrices claires à l'égard de la participation de l'industrie au sein de l'écosystème aidera à stabiliser le déploiement futur des paiements mobiles au Canada et en améliorera l'efficacité. Une fois opérationnel, l'écosystème des paiements mobiles permettra à un utilisateur final de sauvegarder des justificatifs de paiement (c'est-à-dire, les renseignements relatifs à une carte) dans un appareil mobile, puis de simplement effleurer le lecteur de son appareil pour effectuer un paiement. L'utilisateur jouira ainsi d'une expérience d'achat fluide et plus commode et sécuritaire.

Dans le cadre du présent document, les participants à l'initiative établissent un modèle de référence relatif aux paiements mobiles effectués au moyen de la technologie de communication en champ proche (« NFC », pour *near field communication*, en anglais) et dressent une liste d'attentes à l'intention des participants à l'écosystème. Ces attentes et les interactions connexes jettent des bases communes, établies de façon volontaire, qui permettront d'offrir des services de paiement mobile NFC au Canada.

Même si d'autres intervenants ont été consultés dans le cadre de la création de ce document, les participants à l'initiative demeurent responsables de sa version définitive.

2 REGISTRE DES MODIFICATIONS

Le présent document peut être passé en revue et mis à jour périodiquement, à mesure que l'écosystème évolue. L'objet de cette section est d'énumérer les changements apportés, au profit du lecteur.

Date (J/M/A)	Section(s)	Description des changements	Version
12-05-14	s. o.	Version publique initiale	1.03
12-11-01	s. o.	Réédition de la version publique initiale à laquelle on a intégré la rétroaction fournie par les participants à l'écosystème, dont les gestionnaires de service de confiance (GSC), les exploitants de réseau mobile (ERM), les réseaux de paiements et les fournisseurs de services de traitement des paiements.	1.04

3 VISION ET PRINCIPES DIRECTEURS

La vision et les principes directeurs en matière de paiements mobiles au Canada ont servi de base à la rédaction du présent document et ils ont orienté les participants à l'initiative dans le cadre de l'élaboration du Modèle de référence des paiements mobiles NFC au Canada.

L'énoncé de vision et les principes directeurs reposent sur la conviction que les consommateurs s'attendent à ce que les IF canadiennes offrent des services sûrs et sécuritaires. Afin de répondre à cette attente et d'accélérer l'adoption des paiements mobiles au Canada, les participants à l'initiative ont formulé l'énoncé de vision et les principes directeurs ci-dessous.

3.1 ÉNONCÉ DE VISION

Assurer le caractère pratique, ouvert, sûr et sécuritaire de l'écosystème des paiements mobiles au Canada à l'aide d'un cadre opérationnel axé sur des normes. Ce cadre permettra d'accroître les choix offerts aux consommateurs et d'accélérer l'adoption des paiements mobiles.

3.2 PRINCIPES DIRECTEURS

Le cadre opérationnel des paiements mobiles au Canada est :

Ouvert :

- s'adapte à divers modèles d'affaires;
- favorise l'innovation;
- assure la concurrence entre les différents joueurs du marché.

Sûr et sécuritaire :

- protège les renseignements confidentiels, qu'ils soient d'ordre personnel, financier ou transactionnel, au sein de l'écosystème des paiements mobiles;
- facilite les interactions sécuritaires entre les IF et l'écosystème.

Adapté aux besoins des utilisateurs finaux et des marchands :

- offre aux utilisateurs les caractéristiques suivantes : facilité d'utilisation, vitesse, disponibilité, sécurité, transparence, choix et cohérence.

Fondé sur des normes :

- établit des normes bien définies qui constituent la base des interactions entre les IF et l'écosystème des paiements mobiles;
- respecte le cadre réglementaire canadien et évite l'empiétement sur les normes existantes;
- respecte les normes internationales afin de faciliter l'interopérabilité.

Durable :

- trace la voie de façon à ce que les normes permettent d'assurer la viabilité à long terme des paiements mobiles au Canada;
- encadre les échanges réalisés entre les IF et l'écosystème des paiements mobiles;
- s'adapte au fil du temps en fonction de l'évolution de la technologie et de l'écosystème;
- permet l'utilisation de modèles d'affaires économiquement viables qui accélèrent l'adoption des paiements mobiles.

Axé sur les transactions effectuées à l'aide de technologie mobile :

- met l'accent sur les transactions de paiement et sur les fonctions créant des conditions favorables;
- tient compte des services de prépaiement et de postpaiement qui favorisent les transactions;
- permet l'utilisation de plusieurs devises et types de paiement;
- met l'accent sur les appareils mobiles munis de la fonction NFC et sur les technologies connexes.

4 TABLE DES MATIÈRES

1 INTRODUCTION 2

2 REGISTRE DES MODIFICATIONS 3

3 VISION ET PRINCIPES DIRECTEURS 4

3.1 ÉNONCÉ DE VISION 4
3.2 PRINCIPES DIRECTEURS 4

4 TABLE DES MATIÈRES 5

5 RENSEIGNEMENTS GÉNÉRAUX 7

5.1 OBJET 7
5.2 PAIEMENTS PAR CARTE ET PAIEMENTS MOBILES : COMPARAISON 7
5.3 PORTÉE 7
5.4 DÉFINITION DES ÉNONCÉS NORMALISÉS 8
5.5 RESPECT DES ÉNONCÉS NORMALISÉS 9
5.6 GOUVERNANCE ET CONSERVATION DU DOCUMENT 9
5.7 PUBLIC-CIBLE 9
5.8 RÈGLEMENTS ET CONTRATS 11
5.9 EXIGENCES EN MATIÈRE DE TESTS ET D'APPROBATION 11

6 CADRE RELATIF À LA SOLUTION DE PAIEMENTS MOBILES AU CANADA 12

6.1 RÈGLES DE VALORISATION DE LA MARQUE 12
6.2 EXIGENCES RELATIVES AUX SOCIÉTÉS OFFRANT DES SERVICES DE PAIEMENT MOBILE SANS CONTACT 12
6.3 EXIGENCES RELATIVES AU TRAITEMENT DES TRANSACTIONS 13
6.4 EPA 13
6.5 GMA/EPC 13
6.6 EMVCO 13
6.7 NFC 14
6.8 NORMES DE MESSAGERIE DE GLOBALPLATFORM 14
6.9 ÉNONCÉS NORMALISÉS 15

7 APERÇU DE L'ÉCOSYSTÈME DES PAIEMENTS MOBILES NFC 16

7.1 APERÇU DE L'ÉCOSYSTÈME 17
7.2 MODÈLE DE RÉFÉRENCE DES PAIEMENTS MOBILES NFC – DESCRIPTION DE LA SOLUTION 17
7.3 APERÇU DE L'ARCHITECTURE 18
7.4 RÔLES ET DESCRIPTION DES RÔLES 19
7.5 APERÇU DES LOGICIELS ET DES APPAREILS 21
7.6 EXIGENCES RELATIVES AU LECTEUR SANS CONTACT/PDV 23
7.7 INTEROPÉRABILITÉ 23
7.8 ÉNONCÉS NORMALISÉS 24

8 CARACTÉRISTIQUES ET FONCTIONS DU PORTE-MONNAIE ET DE L'APPLICATION DE PAIEMENT 25

8.1 TERMINOLOGIE ET STRUCTURE DE LA SOLUTION 25
8.2 OUVERTURE ET INTEROPÉRABILITÉ 26
8.3 CARACTÉRISTIQUES ET FONCTIONS DU PORTE-MONNAIE 27
8.4 APPLICATION ET JUSTIFICATIFS DE PAIEMENT 28
8.5 CARACTÉRISTIQUES ET FONCTIONS DU PORTE-MONNAIE ET DE L'APPLICATION DE PAIEMENT – RÉSUMÉ 31
8.6 ÉNONCÉS NORMALISÉS 31

9 TRAITEMENT DES TRANSACTIONS 35

9.1 TRANSACTIONS UTILITAIRES EFFECTUÉES À L'AIDE D'UN APPAREIL MOBILE 37

9.2 TRANSACTIONS DE VALEUR ÉLEVÉE OU À RISQUE ÉLEVÉ EFFECTUÉES À L'AIDE D'APPAREILS MOBILES 37
9.3 REÇUS ÉLECTRONIQUES 41
9.4 TRANSACTIONS DE REMISE D'ACHAT EFFECTUÉES À L'AIDE D'UN APPAREIL MOBILE 45
9.5 TRAITEMENT DES TRANSACTIONS – RÉSUMÉ 47
9.6 ÉNONCÉS NORMALISÉS 47

10 HABILITATION ET GESTION DU CYCLE DE VIE 49

10.1 RELATIONS COMMERCIALES ENTRE PARTICIPANTS À L'ÉCOSYSTÈME 50
10.2 GESTION DES CLÉS 50
10.3 INSTALLATION DU PORTE-MONNAIE MOBILE 54
10.4 INSTALLATION DE L'APPLICATION ET DES JUSTIFICATIFS DE PAIEMENT 56
10.5 ACTIVITÉS DE MAINTENANCE ASSOCIÉES À L'UTILISATEUR FINAL 61
10.6 ACTIVITÉS DE SOUTIEN ASSOCIÉES À L'UTILISATEUR FINAL 68
10.7 SUPPRESSION DE L'APPLICATION DE PAIEMENT ET DES JUSTIFICATIFS CONNEXES 69
10.8 HABILITATION ET GESTION DU CYCLE DE VIE – RÉSUMÉ 70
10.9 ÉNONCÉS NORMALISÉS 70

11 FIDÉLISATION ET RÉCOMPENSES 76

11.1 APERÇU DES PROGRAMMES DE FIDÉLISATION 76
11.2 INTERACTION AU PDV – PROGRAMMES DE FIDÉLISATION 79
11.3 ÉCHANGE DE POINTS DE FIDÉLISATION 83
11.4 FIDÉLISATION ET RÉCOMPENSES – RÉSUMÉ 85
11.5 ÉNONCÉS NORMALISÉS 86

12 DONNÉES ET SÉCURITÉ 87

12.1 DONNÉES 87
12.2 FRAUDE, LOGICIELS MALVEILLANTS ET SÉCURITÉ 98
12.3 DONNÉES ET SÉCURITÉ – RÉSUMÉ 98
12.4 ÉNONCÉS NORMALISÉS 98

13 RÉSUMÉ DU DOCUMENT 105

14 GLOSSAIRE 106

15 RÉFÉRENCES 113

15.1 RÉFÉRENCES ISO 113
15.2 RÉFÉRENCES DE GSM 114
15.3 RÉFÉRENCES DE L'ETSI 115
15.4 RÉFÉRENCES DE GLOBALPLATFORM 115
15.5 RÉFÉRENCES JAVA 116
15.6 RÉFÉRENCES D'EMVCO 116
15.7 RÉFÉRENCES DU EPC 117
15.8 RÉFÉRENCES DE PAYEZ MOBILE 117
15.9 RÉFÉRENCES DE AFSCM 118

16 SÉLECTION DE LA MÉTHODE DE VÉRIFICATION DE CARTES – RÉSUMÉ 119

17 ÉNONCÉS NORMALISÉS 120

5 RENSEIGNEMENTS GÉNÉRAUX

5.1 OBJET

L'objet du Modèle de référence des paiements mobiles NFC au Canada consiste à établir des lignes directrices à l'intention des participants à l'écosystème des paiements mobiles. À cette fin, les intervenants ayant participé à l'élaboration de ce document ont cherché à promouvoir une vision précise à l'égard des paiements mobiles au Canada. Cette vision consiste à assurer le caractère pratique, ouvert, sûr et sécuritaire de l'écosystème des paiements mobiles à l'aide d'un cadre opérationnel axé sur des normes.

Les participants à l'initiative ont la ferme conviction qu'en définissant des processus, des rôles, des responsabilités et des attentes sous forme d'énoncés normalisés, et en les communiquant, il en résultera un écosystème offrant plus de choix aux utilisateurs tout en accélérant l'adoption des paiements mobiles.

5.2 PAIEMENTS PAR CARTE ET PAIEMENTS MOBILES : COMPARAISON

Habituellement, un consommateur désirant se procurer une carte de crédit présente une demande auprès d'une IF qui, en cas d'acceptation de la demande, s'adresse à une société chargée de la délivrance des cartes. Cette dernière envoie alors une carte de crédit au consommateur. Lorsque le consommateur reçoit la carte, il doit l'activer et il peut ensuite l'utiliser chez un marchand, qui la glisse ou l'insère dans le lecteur.

Dans le contexte des paiements mobiles, le consommateur (appelé « utilisateur final ») demande à une IF (appelée « émetteur de justificatifs de paiement » ou « EJP ») de lui accorder l'accès aux services de paiement mobile à l'aide de son appareil portatif. L'EJP demande alors à son gestionnaire de service de confiance (le « GSC », qui a remplacé le spécialiste de traitement des cartes) de transmettre les justificatifs de paiement à l'appareil mobile de l'utilisateur final. Pour ce faire, le GSC de l'émetteur de justificatifs communique avec l'exploitant de réseau mobile (« ERM ») pertinent. Après la transmission des justificatifs à l'appareil, l'accès aux services de paiement mobile est accordé à l'utilisateur final en suivant un processus très similaire à celui de l'activation d'une carte de crédit. À la suite d'une vérification, l'utilisateur final peut utiliser son téléphone ou un autre appareil mobile de la même façon qu'il utiliserait une carte de paiement sans contact.

En résumé, les étapes pour configurer et utiliser les services de paiement mobile sont semblables à celles devant être franchies pour obtenir une carte de crédit traditionnelle.

5.3 PORTÉE

Ce document décrit les paiements mobiles NFC, notamment les éléments fonctionnels, les rôles, les responsabilités et les modèles d'interaction requis pour l'établissement d'un écosystème de paiements mobiles NFC.

Les paiements mobiles NFC, ou paiements sans contact, désignent des transactions exigeant que l'appareil mobile effleure le lecteur. À l'inverse d'autres modes de paiement mobile tels que les codes à barres et les paiements entre homologues, les paiements mobiles de type NFC exigent l'installation du matériel et du logiciel dans le même appareil mobile.

Ce document porte sur les éléments requis pour effectuer des paiements mobiles NFC et traiter ce type de transaction. L'installation de justificatifs de paiement dans un appareil mobile est sans nul doute plus complexe que la fourniture de tels justificatifs pour une carte de plastique, mais ces deux processus ne sont pas totalement différents. Le processus de délivrance de cartes de crédit a servi comme l'un des

nombreux modèles utilisés dans l'élaboration de ce document. Toutefois, dans le présent document, une importance particulière a été accordée aux cartes SIM (notamment aux cartes universelles à circuits intégrés, ou Universal Integrated Circuit Card [UICC], en anglais) et aux puces NFC intégrées à l'appareil mobile, qui permettent d'effectuer des paiements mobiles sans contact.

Autre point commun entre les paiements mobiles NFC et les paiements traditionnels par carte : le point de vente (PDV). Dans le présent document, il est présumé que dès que la connexion sans contact est établie au PDV, toutes les autres étapes de traitement de la transaction font appel aux réseaux de paiement existants. Ainsi, ce document ne redéfinit pas le rôle des réseaux de paiement.

5.3.1 DÉFINITION DES ÉLÉMENTS VISÉS

Pour déterminer les domaines d'application du présent document, les participants à l'initiative se sont basés sur la vision et les principes directeurs (consultez la section Vision et principes directeurs), l'interaction entre les participants à l'écosystème et les éléments qui diffèrent par rapport aux modes de paiement existants. À partir de ces facteurs, le présent document a été divisé dans les sections suivantes : Caractéristiques et fonctions du porte-monnaie et de l'application de paiement, Traitement des transactions, Habilitation et gestion du cycle de vie, Fidélisation et récompenses, Données et sécurité.

5.3.2 DÉFINITION DES ÉLÉMENTS NON VISÉS

Ce document ne porte pas sur les paiements mobiles à distance (soit les transactions initiées à l'aide d'un appareil mobile, peu importe où se trouvent le payeur et le bénéficiaire). De même, ce document ne porte pas sur d'autres technologies NFC, comme les cartes microSD et les autocollants de paiement sans contact.

Par ailleurs, les éléments ci-dessous ont été intentionnellement exclus du rayon d'action de ce document :

- **Paiements NFC non mobiles :** les types de paiements mobiles exclus du présent document sont les suivants : paiements effectués à l'aide de codes à barres ou par Bluetooth, paiements NFC ou RFID en mode passif (p. ex., autocollants et porte-clé), outils permettant le passage en mode NFC actif (y compris les cartes MicroSD et les étuis NFC), paiements entre homologues et paiements en nuage.
- **Processus de paiement non visés :** dans ce document, il est présumé que les paiements mobiles NFC seront effectués à l'aide de l'infrastructure de paiement existante. Ainsi, nombre d'éléments du traitement des paiements qui ne sont pas visés par les paiements mobiles, ainsi que ceux qui sont la propriété d'institutions particulières, n'ont pas été définis. Ces éléments comprennent l'acquisition d'utilisateurs finaux, l'acquisition de marchands, la facturation et le règlement, les recouvrements, le déploiement et la certification aux PDV, la gestion des comptes, les rapprochements et le traitement des paiements essentiels.
- **Monnaies non traditionnelles :** les monnaies émergentes et virtuelles, comme celles qui sont offertes dans les réseaux sociaux et les programmes de fidélisation, ne sont pas encore d'usage courant. Ces monnaies n'ont pas été évaluées dans le présent document.

5.4 DÉFINITION DES ÉNONCÉS NORMALISÉS

Ce document contient plusieurs types de renseignements, dont des lignes directrices et des normes. Les énoncés normalisés sont numérotés entre crochets (« **[EN1] ») ** et énumérés à la fin de chaque section. Dans ce document, les éléments qui ne sont pas désignés comme étant des normes sont présentés à titre informatif.

5.5 RESPECT DES ÉNONCÉS NORMALISÉS

Tous les énoncés normalisés doivent être respectés par les participants à l'initiative et par leurs partenaires faisant partie de l'écosystème. Dans le cas de ce groupe, le respect des énoncés normalisés se traduit par la conformité à l'ensemble d'entre eux.

Dans le cas des autres participants à l'écosystème, l'application des énoncés normalisés est facultative. Une fois que les énoncés seront rendus publics, les autres participants à l'écosystème pourront choisir de s'y conformer. Aucun examen officiel ou processus de certification n'est prévu pour évaluer le respect des énoncés normalisés.

5.6 GOUVERNANCE ET CONSERVATION DU DOCUMENT

Ce document a été rédigé par les participants à l'initiative. La publication et l'intendance du document seront gérées par l'Association des banquiers canadiens (ABC).

Le propriétaire du document est responsable de son affichage sur un site Web public et de son examen périodique en vue d'assurer sa pertinence, et il agit à titre de principale personne-ressource à l'égard du document et des normes qu'il contient.

5.7 PUBLIC-CIBLE

Enfin, ce document, le Modèle de référence des paiements mobiles NFC au Canada, s'adresse aux fournisseurs canadiens de services de paiement mobile, y compris les suivants, sans s'y limiter : EJP, GSC, réseaux mobiles, fabricants de matériel d'origine (« FMO »), réseaux de paiement (« ERP », p. ex., Interac, Visa, MasterCard), marchands, acquéreurs, fournisseurs de services de fidélisation, fournisseurs de porte-monnaie, organismes de réglementation et toutes les autres parties intéressées par les paiements mobiles NFC. Cependant, ce document permettra à tous les lecteurs de s'informer de la façon dont les participants à l'initiative abordent les paiements mobiles et, par conséquent, de mieux circonscrire leur propre approche à l'égard du nouvel écosystème.

Ce document contient de nombreux renseignements relatifs aux paiements mobiles NFC. Par conséquent, les lecteurs trouveront certaines sections plus pertinentes que d'autres en fonction de leur rôle. Le tableau ci-dessous présente des recommandations à l'égard de l'interprétation de ce document, en fonction du rôle des intervenants.

Pour obtenir les définitions des rôles, consultez la section Cadre relatif à la solution de paiements mobiles au Canada ou au glossaire. Dans le tableau ci-dessous, les participants à l'écosystème sont présentés en ordre alphabétique.

Participants à l'écosystème	**Sections suggérées**
Acquéreur	Les sections Traitement des transactions et Données et sécurité portent sur les étapes de traitement d'un paiement mobile NFC, y compris l'interaction de l'appareil mobile et du lecteur au PDV. La section Données et sécurité donne un aperçu des types de données auxquelles chaque participant à l'écosystème a accès.
Émetteur de justificatifs de paiement (EJP)	Le présent document, dans sa totalité, sera utile aux intervenants jouant le rôle d'EJP.

Participants à l'écosystème	Sections suggérées
Utilisateur final (aussi connu comme le « consommateur » ou le « client »)	Ce document ne s'adresse pas directement aux utilisateurs finaux de services de paiement mobile NFC. Une bonne partie du vocabulaire, de la phraséologie et des concepts contenus dans ce document peut être inconnue de l'utilisateur moyen de cartes de paiement ou de services de paiement mobile. Toutefois, si un utilisateur final choisit de consulter ce document, la section Caractéristiques et fonctions du porte-monnaie et de l'application de paiement l'aidera à comprendre ce qu'est un porte-monnaie et comment il fonctionne. La section Traitement des transactions l'informera du fonctionnement des paiements mobiles NFC au PDV. Enfin, la section Données et sécurité l'informera du type de données utilisées dans le cadre des paiements mobiles NFC et des données auxquelles chaque participant à l'écosystème a accès.
Fournisseur de services de fidélisation	Les sections Fidélisation et récompenses et Données et sécurité seront utiles aux fournisseurs de services de fidélisation. La section Fidélisation et récompenses donne un aperçu des types de programmes de fidélisation qui devraient être offerts à l'égard des appareils permettant d'effectuer des paiements mobiles NFC. Cette section tient compte du fait qu'il s'agit d'un milieu en évolution rapide assujetti à un degré important d'incertitude. La section Données et sécurité informera les fournisseurs de services de fidélisation du type de renseignements auxquels ils auront accès.
Marchand	Les sections Traitement des transactions et Données et sécurité seront utiles aux marchands. Dans la section Traitement des transactions, les marchands trouveront de l'information sur les exigences relatives aux PDV et sur la réduction prévue des temps d'attente. Dans la section Données et sécurité, ils trouveront de l'information sur l'accès aux données et les mesures de sécurité connexes.
Exploitant de réseau mobile (ERM)	Une grande partie de ce document intéressera les ERM. La section Caractéristiques et fonctions du porte-monnaie et de l'application de paiement décrit les mesures de stockage et d'association des justificatifs de paiement. La section Habilitation et gestion du cycle de vie décrit la participation de l'ERM au processus d'approvisionnement ainsi que les attentes relatives aux services offerts aux utilisateurs finaux. La section Données et sécurité présente les données auxquelles chaque participant à l'écosystème a accès. La section Traitement des transactions concerne surtout le marchand, l'utilisateur final et les réseaux de paiement; elle ne s'adresse pas aux ERM.
Fabricant de matériel d'origine (FMO)	Selon le rôle qu'ils jouent, les FMO peuvent trouver des renseignements utiles dans ce document. Si un FMO participe directement à la gestion d'un élément sécurisé ou d'une UICC (consultez le glossaire ou le Cadre relatif à la solution de paiements mobiles au Canada pour obtenir les définitions), il trouvera pertinentes les sections qui s'adressent aux ERM. Toutefois, si le rôle du FMO se limite à la fabrication du matériel et que la gestion de l'élément sécurisé ou

Participants à l'écosystème	Sections suggérées
	de l'UICC est déléguée à un ERM, seules les spécifications de GlobalPlatform contenues dans ce document risquent de l'intéresser.
Réseau de paiement	Ce document a été conçu pour être utilisé en parallèle avec les services fournis par les ERP, tels que Interac, Visa et MasterCard, et non de manière indépendante. La totalité de ce document peut présenter un intérêt aux yeux des ERP; cependant, les sections suivantes risquent d'être les plus utiles : Habilitation et gestion du cycle de vie (approvisionnement), Traitement des transactions (processus relatifs au PDV) et Données et sécurité.
Organismes de réglementation	Le présent document, dans sa totalité, sera utile aux organismes de réglementation. S'il est vrai que les paiements mobiles NFC empruntent aux caractéristiques actuelles du domaine bancaire et des domaines des paiements et des télécommunications, les paiements mobiles du futur feront appel à de nouvelles combinaisons de ces caractéristiques. Les organismes de réglementation voudront se tenir au courant de l'évolution de l'écosystème pour assurer la sûreté et la sécurité globales du marché canadien des services financiers et être au fait du rôle des paiements mobiles.
Gestionnaire de service de confiance (GSC)	Les sections Caractéristiques et fonctions du porte-monnaie et de l'application de paiement, Habilitation et gestion du cycle de vie et Données et sécurité intéresseront les GSC. La première décrit les mesures de stockage des justificatifs de paiement ainsi que le processus d'association du porte-monnaie et des justificatifs. La deuxième présente le processus d'approvisionnement, dont le GSC constitue une partie intégrante. La troisième décrit les données auxquelles chaque participant à l'écosystème a accès.
Fournisseur de porte-monnaie	Les sections Caractéristiques et fonctions du porte-monnaie et de l'application de paiement et Données et sécurité intéresseront les fournisseurs de porte-monnaie. La première présente les caractéristiques générales d'un porte-monnaie, notamment sur le plan de la sécurité, des fonctions et des interfaces, ainsi que les attentes connexes. La deuxième décrit les données auxquelles chaque participant à l'écosystème a accès.

5.8 RÈGLEMENTS ET CONTRATS

Il incombe à tous les participants à l'écosystème qui adoptent les présentes normes de s'assurer que leur application ne contrevient à aucune exigence d'ordre juridique, réglementaire ou contractuel.

5.9 EXIGENCES EN MATIÈRE DE TESTS ET D'APPROBATION

Par ailleurs, il incombe aux fabricants d'appareils, aux développeurs de logiciels, aux intégrateurs, aux banques, aux fournisseurs, aux ERM, aux tiers participant à des activités de traitement et aux autres participants à l'écosystème d'effectuer des tests d'assurance qualité exhaustifs relativement aux produits et services de paiement mobile.

6 CADRE RELATIF À LA SOLUTION DE PAIEMENTS MOBILES AU CANADA[1]

Cette section fournit une description générale du cadre ayant servi à la conception du Modèle de référence des paiements mobiles NFC au Canada.

Au moment de la rédaction de ce document, il n'existait pas de norme mondiale relative aux paiements mobiles. Il existait cependant une série de normes régionales et fonctionnelles portant sur des événements précis du cycle de vie des paiements mobiles. Ce document a été créé en utilisant d'autres normes comme point de départ et en mettant l'accent sur le cycle de vie des paiements mobiles, et il a comme seul objectif de favoriser les intérêts des Canadiens. Même s'il s'agit d'un document unique en son genre, il est largement inspiré du travail d'autres organismes rédacteurs de normes, notamment PayEz, l'Association française du sans contact mobile (AFSCM), GlobalPlatfom et EMVCo. Des références ont été indiquées au besoin.

6.1 RÈGLES DE VALORISATION DE LA MARQUE

Ce document ne modifie aucunement les règles de valorisation de la marque. Les règles de valorisation de la marque établies par les réseaux de paiement doivent être respectées **[EN1]**.

- **MasterCard :** l'utilisation de l'application MasterCard et des justificatifs de paiement associés à un appareil mobile ne peuvent être acceptés que par un marchand dont le système PDV affiche le logo d'acceptation MasterCard.
- **Visa :** l'utilisation de l'application Visa et des justificatifs de paiement associés à un appareil mobile ne peuvent être acceptés que par un marchand dont le système PDV affiche le logo d'acceptation Visa.
- **Interac :** l'utilisation de l'application Interac et des justificatifs de paiement associés à un appareil mobile ne peuvent être acceptés que par un marchand dont le système PDV affiche le logo d'acceptation Interac.

6.2 EXIGENCES RELATIVES AUX SOCIÉTÉS OFFRANT DES SERVICES DE PAIEMENT MOBILE SANS CONTACT

Des sociétés nationales et internationales émettrices de cartes, comme MasterCard, Visa et Interac, ont élaboré une série de spécifications relatives aux transactions de paiement mobile sans contact. Ces spécifications visent principalement à définir les règles et les exigences relatives au facteur de forme mobile et à l'exécution d'une transaction d'achat à l'aide d'un lecteur sans contact conforme à la norme ISO 14443 (cartes à puce de type A ou de type B) ([ISO-8], [ISO-9]).

Pour être conformes aux spécifications de paiement mobile sans contact MasterCard PayPass, Visa PayWave et Flash Interac, les appareils mobiles doivent prendre en charge les modes EMV et MSD (dans le cas de Visa et de MasterCard); il est ainsi possible d'exécuter des transactions de paiement mobile sans contact à l'aide de ces appareils.

Le Modèle de référence des paiements mobiles NFC au Canada s'applique aux technologies EMV et MSD :

[1] Cette section est tirée du document intitulé *Mobile Contactless Proximity Payment de PayEz Mobile, Part 1: Product Definition*, troisième version, avril 2011, page 19

Dans le cas de transactions sans contact effectuées au moyen de MasterCard PayPass, les spécifications relatives à l'appareil mobile et au lecteur sans contact doivent prendre en charge le profil PayPass Mag Stripe, tel que défini dans les spécifications PayPass Mag Stripe, ainsi que le profil Pass M/Chip ou Mobile M/Chip, tel que défini dans les spécifications PayPass M/Chip **[EN2]**.

Dans le cas de transactions sans contact effectuées au moyen de Visa PayWave, les spécifications relatives à l'appareil mobile et au lecteur sans contact doivent prendre en charge les modes MSD, VMPA et qVSDC tels que définis dans les spécifications Visa Mobile **[EN3]**.

Dans le cas de transactions sans contact effectuées au moyen de Flash Interac, l'appareil mobile et le lecteur sans contact doivent être conformes aux spécifications Interac Flash Mobile **[EN4]**.

6.3 EXIGENCES RELATIVES AU TRAITEMENT DES TRANSACTIONS

MasterCard, Visa et Interac ont conçu des transactions de paiement mobile sans contact, déclenchées au moyen d'un appareil mobile, de manière à ce qu'elles aient le moins de répercussions possible sur l'infrastructure actuelle de paiement par carte.

Le traitement de paiements mobiles de proximité par un réseau de paiement particulier exige le respect des exigences de ce réseau. Les autres règles opérationnelles applicables doivent être établies en fonction du même réseau d'autorisation et du même système de compensation que les transactions standards par carte de débit ou de crédit **[EN5]**. Parmi les exemples de règles opérationnelles applicables, on retrouve les lignes directrices de MasterCard, de Visa et d'Interac, ainsi que les règles connexes de l'Association canadienne des paiements.

6.4 EPA

Les groupes de travail du SEPA ont publié plusieurs documents qui établissent les exigences et les lignes directrices relatives aux transactions de paiement. Le Modèle de référence des paiements mobiles NFC au Canada est conforme aux publications du SEPA ci-dessous :

- SEPA Card Framework [EPC-1]
- SEPA Cards Standardization Volume – Book of Requirements [EPC-2]

6.5 GMA/EPC

Le Modèle de référence des paiements mobiles NFC au Canada est conforme aux lignes directrices de GSMA et du European Payments Council (EPC) ainsi qu'aux documents fournis par ces organismes.

- GSMA – EPX TSM Requirements [SPC-3]

6.6 EMVCO

Le Modèle de référence des paiements mobiles NFC au Canada est conforme aux documents publiés par EMVCo, notamment les suivants :

- EMVCo Contactless Mobile Payment Architecture Overview [EMV-11]
- EMVCo Handset Requirements for Contactless Mobile Payments [EMV-12]
- EMVCo Application Activation User Interface Contactless Activation/Deactivation Scenarios, Overview, Usage Guidelines and PPSE Requirements [EMV-13]
- EMVCo EMV Profiles of GlobalPlatform UICC Configuration [EMV-14]

6.7 NFC

La communication en champ proche désigne une technologie de connectivité de courte distance, sans fil, qui permet la communication sécuritaire entre des appareils électroniques situés à proximité.

Trois modes d'échange de données entre appareils électroniques sont actuellement pris en charge :

- Mode émulation de carte NFC
- Mode pair à pair (non abordé dans ce document)
- Mode lecture-écriture (non abordé dans ce document)

Le mode émulation de carte NFC doit être utilisé pour exécuter une transaction de paiement mobile sans contact entre l'appareil mobile de l'utilisateur final et un lecteur sans contact du marchand, au moyen d'une couche de communication liée à une radiofréquence respectant la norme ISO 14443 (cartes à puce de type A ou de type B) **[EN6]**.

6.8 NORMES DE MESSAGERIE DE GLOBALPLATFORM[2]

À des fins d'harmonisation et d'interopérabilité, les normes de messagerie de GlobalPlatform ont été adoptées. GlobalPlatform définit trois modes de messagerie :

Mode	Description
Mode simple	En mode simple, l'ERM ou le GDS autorise l'émetteur de justificatifs à utiliser son domaine sécurisé pour l'hébergement de l'application de paiement. Le droit d'accès au domaine sécurisé demeure la propriété de l'ERM ou du GDS. Toute mise à jour ou modification de l'application de paiement doit être effectuée par l'entremise du GDS ou de l'ERM.
Mode de délégation	En mode de délégation, l'ERM ou le GDS loue une section de l'élément sécurisé à l'émetteur de justificatifs ou lui donne accès à cette section. L'ERM ou le GDS demeure propriétaire de l'élément sécurisé et décide quelles applications peuvent être installées dans l'élément sécurisé. L'ERM ou le GDS et l'émetteur de justificatifs (ou l'installateur de justificatifs) échangent des clés permettant d'accéder à l'élément sécurisé.
Mode bimodal	En mode bimodal, l'ERM ou le GDS vend une section de l'élément sécurisé à l'émetteur de justificatifs. Ce dernier détient alors à part entière les droits d'accès relatifs à cette section de l'élément sécurisé. Dans le cadre de la vente, l'ERM ou le GDS et l'émetteur de justificatifs (ou l'installateur de

[2] GPS_Messaging_Specification_for_Mobile_NFC_Services-v1.0.

Mode	Description
	justificatifs) échangent des clés d'accès. L'émetteur de justificatifs peut donc installer toutes les applications qu'il désire dans la section de l'élément sécurisé qui lui appartient, sans avoir besoin de la permission de l'ERM ou du GDS.

Toutes les activités de messagerie doivent être exécutées conformément aux lignes directrices pertinentes. Consultez le document GPS_Messaging_Specification_for_Mobile_NFC_Services-v1.0.

Le présent document et les normes de GlobalPlatform tiennent compte des trois modes ci-dessus (mode simple, mode de délégation et mode bimodal); cependant, les organismes qui adoptent les présentes normes ne doivent utiliser que le mode de délégation ou le mode bimodal, tels que définis par GlobalPlatform **[EN7]**. Le mode de délégation et le mode bimodal permettent aux EJP d'assurer la sécurité des justificatifs de paiement; par conséquent, ils contribuent à la sûreté et à la sécurité de l'écosystème.

6.9 ÉNONCÉS NORMALISÉS

Numéro	Énoncé	Section
1	Les règles de valorisation de la marque établies par les réseaux de paiement doivent être respectées.	6.1 Règles de valorisation de la marque
2	Dans le cas de transactions sans contact effectuées au moyen de MasterCard PayPass, les spécifications relatives à l'appareil mobile et au lecteur sans contact doivent prendre en charge le profil PayPass Mag Stripe, tel que défini dans les spécifications PayPass Mag Stripe, ainsi que le profil Pass M/Chip ou Mobile M/Chip, tel que défini dans les spécifications PayPass M/Chip.	6.2 Exigences relatives aux sociétés offrant des services de paiement mobile sans contact
3	Dans le cas de transactions sans contact effectuées au moyen de Visa PayWave, les spécifications relatives à l'appareil mobile et au lecteur sans contact doivent prendre en charge les modes MSD, VMPA et qVSDC tels que définis dans les spécifications Visa Mobile.	6.2 Exigences relatives aux sociétés offrant des services de paiement mobile sans contact
4	Dans le cas de transactions sans contact effectuées au moyen de Flash Interac, l'appareil mobile et le lecteur sans contact doivent être conformes aux spécifications Interac Flash Mobile.	6.2 Exigences relatives aux sociétés offrant des services de paiement mobile sans contact
5	Les autres règles opérationnelles applicables doivent être établies en fonction du même réseau d'autorisation et du même système de compensation que les transactions	6.3 Exigences relatives au traitement des

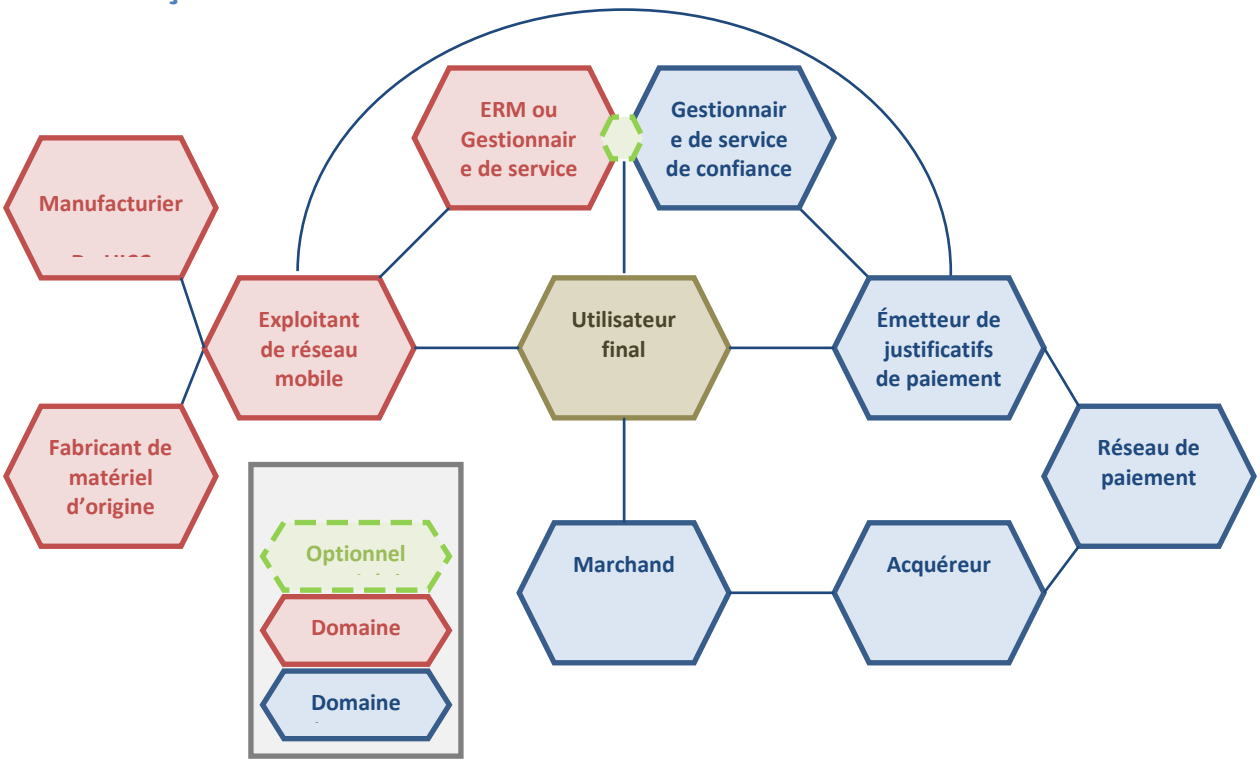
Numéro	Énoncé	Section
	standards par carte de débit ou de crédit.	transactions
6	Le mode émulation de carte NFC doit être utilisé pour exécuter une transaction de paiement mobile sans contact entre l'appareil mobile de l'utilisateur final et un lecteur sans contact du marchand, au moyen d'une couche de communication liée à une radiofréquence respectant la norme ISO 14443 (cartes à puce de type A ou de type B).	6.7 NFC
7	Le présent document et les normes de GlobalPlatform tiennent compte des trois modes ci-dessus (mode simple, mode de délégation et mode bimodal); cependant, les organismes qui adoptent les présentes normes ne doivent utiliser que le mode de délégation ou le mode bimodal, tels que définis par GlobalPlatform.	De la même façon, les GSC ne doivent utiliser que le mode de délégation ou le mode bimodal.

7 APERÇU DE L'ÉCOSYSTÈME DES PAIEMENTS MOBILES NFC[3]

Cette section donne un aperçu des différents éléments requis par le Modèle de référence des paiements mobiles NFC au Canada dans le cadre de l'exécution d'une transaction de paiement mobile sans contact.

[3] Cette section est tirée du document intitulé *Mobile Contactless Proximity Payment de PayEz Mobile, Part 1: Product Definition*, troisième version, avril 2011, page 19.

7.1 APERÇU DE L'ÉCOSYSTÈME



Reportez-vous à la section sur les rôles associés aux paiements mobiles et à celle sur la messagerie pour obtenir plus de renseignements sur les participants à l'écosystème.

7.2 MODÈLE DE RÉFÉRENCE DES PAIEMENTS MOBILES NFC – DESCRIPTION DE LA SOLUTION

Le Modèle de référence des paiements mobiles NFC au Canada permet l'exécution de transactions de paiement NFC par radiofréquences. Le présent document ne porte que sur les paiements mobiles NFC.

Pour effectuer un paiement mobile NFC, l'utilisateur final doit posséder le matériel et les logiciels adéquats. Dans ce contexte, « matériel » désigne un appareil mobile compatible avec la technologie NFC. Le terme « logiciels » englobe l'application porte-monnaie électronique, l'application de paiement et les justificatifs de paiement (reportez-vous à la section Caractéristiques et fonctions du porte-monnaie et de l'application de paiement pour consulter les définitions). Les vérifications relatives à l'admissibilité du matériel ne sont pas traitées en profondeur dans ce document; il est présumé que l'utilisateur final dispose du matériel nécessaire pour effectuer des paiements mobiles NFC. Par conséquent, la section Habilitation et gestion du cycle de vie porte essentiellement sur les exigences relatives aux logiciels.

En supposant que l'utilisateur final dispose du matériel approprié, il doit d'abord installer les logiciels pertinents dans son appareil pour ensuite effectuer des paiements mobiles NFC. Ce document présente les caractéristiques du porte-monnaie et décrit l'installation de l'application de paiement ainsi que le processus d'association connexe : il s'agit là des étapes de configuration préalables à l'exécution de paiements. Ces éléments sont présentés dans les sections Caractéristiques et fonctions du porte-monnaie et de l'application de paiement et Habilitation et gestion du cycle de vie.

Après la configuration initiale, il est possible d'effectuer des transactions de paiement mobile NFC. La section Traitement des transactions décrit les étapes d'un paiement mobile NFC. La solution est conçue pour faire la distinction entre les transactions de faible valeur, de valeur élevée ou à risque élevé. Elle se caractérise par l'utilisation d'une radiofréquence de courte portée qui exige que l'appareil mobile effleure le lecteur sans contact pour effectuer la transaction.

En plus de mettre l'accent sur la fonction de paiement de la solution, ce document tient compte du fait que les programmes de fidélisation et de récompenses, y compris l'échange de coupons et de points, joueront un rôle crucial quant à l'adoption et à l'efficacité des services de paiement mobile NFC. En effet, ce secteur évolue plus que tout autre; c'est pourquoi la section Fidélisation et récompenses porte essentiellement sur les règles et les lignes directrices susceptibles d'influer sur l'évolution de l'écosystème.

Les normes associées aux données et à la sécurité sont essentielles à la création d'un écosystème de paiements mobiles sûr et sécuritaire. Ces normes sont abordées dans la dernière section de ce document. La section Données et sécurité a été conçue en fonction d'un principe général selon lequel chaque participant à l'écosystème ne doit avoir accès qu'au minimum d'information requis pour remplir son rôle principal. Autrement dit, le but premier des participants à l'écosystème est de protéger les données de l'utilisateur final et du marchand. Si le participant à l'écosystème doit accéder à des données, obtenues au moyen d'un appareil mobile, au-delà de la limite permise afin de remplir son rôle principal, l'utilisateur final doit en être informé et il doit accorder explicitement son autorisation à cet effet **[8]**. Pour des raisons de sécurité et de prévention de la fraude, si le participant à l'écosystème doit accéder à des données, obtenues au moyen d'un appareil mobile, au-delà de la limite permise afin de remplir son rôle principal, l'émetteur de justificatifs doit également en être informé et ce dernier doit lui aussi accorder explicitement son autorisation à cet effet **[9]**.

Voici deux thèmes fondés sur la section Vision et principes directeurs qui ont eu une incidence importante sur l'élaboration du Modèle de référence des paiements mobiles NFC.

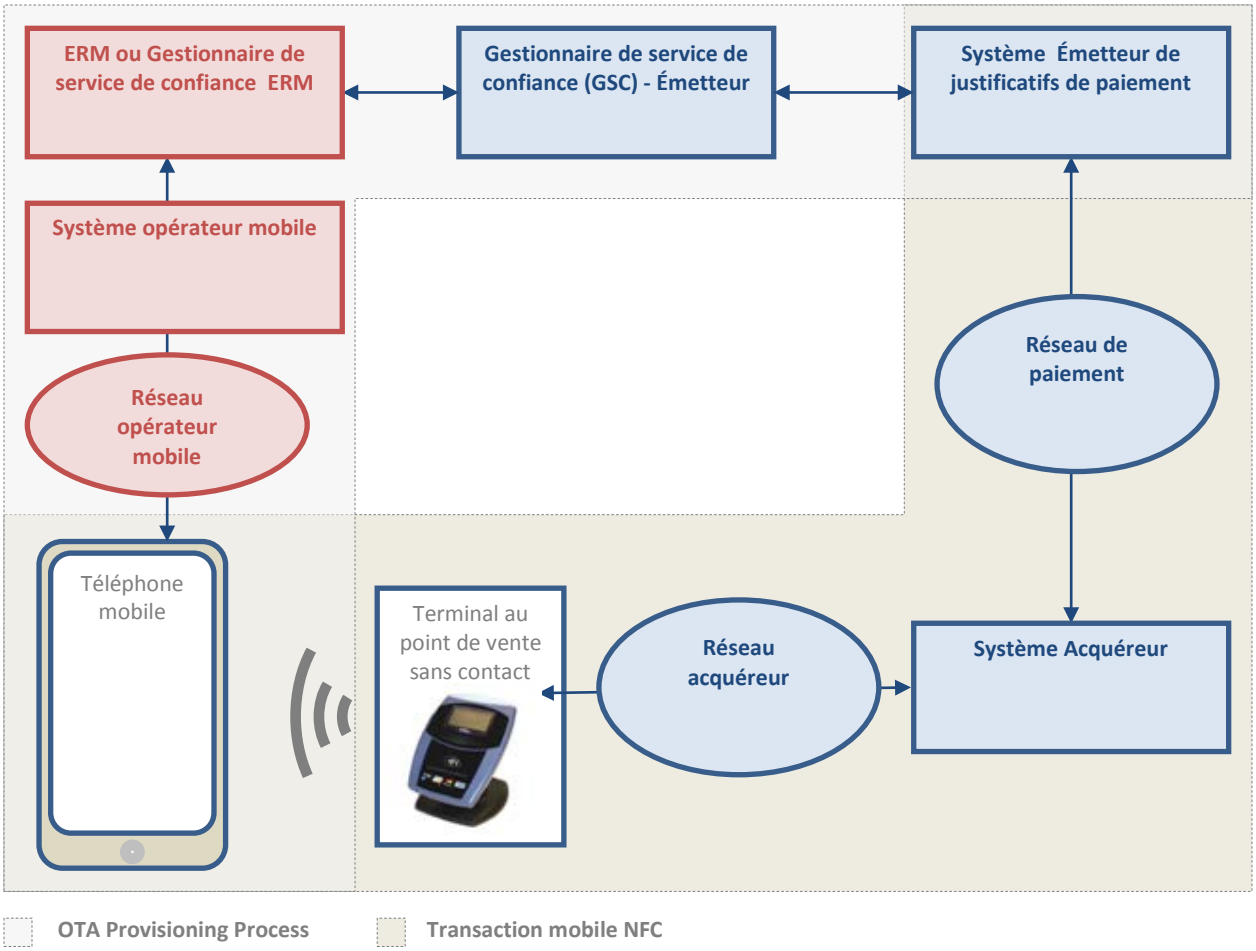
- Premièrement, les normes contenues dans ce document doivent assurer à la fois la protection des intérêts des utilisateurs finaux et des marchands. Quand c'est possible, les processus de ce document ont comme point de départ le souci de la protection des utilisateurs finaux.
- Deuxièmement, ces normes visent l'interopérabilité avec les autres écosystèmes de paiement en cours de développement au Canada. Afin de favoriser cette interopérabilité, le modèle de référence renvoie à des documents et à des décisions d'autres organismes intéressés par l'établissement d'un système de paiements mobiles, et s'en inspire. S'il y a lieu, le modèle de référence contient des citations relatives aux normes existantes mentionnées dans le document.

Le présent document a été structuré en supposant que le lecteur dispose d'une bonne connaissance des concepts abordés dans chacune des sections. Les principales sections du document sont les suivantes : Caractéristiques et fonctions du porte-monnaie et de l'application de paiement, Traitement des transactions, Habilitation et gestion du cycle de vie, Fidélisation et récompenses, Données et sécurité.

7.3 APERÇU DE L'ARCHITECTURE

La figure ci-dessous donne un aperçu de haut niveau des principales composantes requises pour :

- configurer une solution de paiement mobile NFC;
- exécuter et traiter une transaction de paiement mobile NFC.



7.4 RÔLES ET DESCRIPTION DES RÔLES

Le tableau ci-dessous présente les différents rôles au sein de l'écosystème des paiements mobiles au Canada. Ces rôles sont mentionnés tout au long du document.

Rôle	Description
Acquéreur	Désigne une institution qui traite les paiements par carte de débit ou de crédit au nom d'un marchand.
Émetteur de justificatifs de paiement (EJP)	L'EJP est responsable du chiffrement, de la sûreté et de la sécurité des justificatifs de paiement. La relation entre l'utilisateur final et l'EJP repose sur une offre de produits et de services financiers.
Autorité de contrôle (AC)	L'AC peut gérer les principaux échanges effectués relativement à un « porte-monnaie ouvert ». Il s'agit ici d'un modèle qui est reconnu dans le cadre du modèle de référence des paiements mobiles NFC, mais qui n'est pas obligatoire. Ce modèle est considéré comme étant une solution de rechange aux relations de type « plusieurs à plusieurs » entre le GSC d'un émetteur de

Rôle	Description
	justificatifs de paiement et le GSC d'un gestionnaire de domaine sécurisé.
Utilisateur final	(*aussi appelé client*) Consommateur de services de paiement et de connectivité mobiles.
Marchand	Désigne le fournisseur de biens ou de services en échange desquels l'utilisateur final effectue un paiement.
Exploitant de réseau mobile (ERM)	Fournisseur de services de connectivité associés à des appareils mobiles. Aux fins du présent document, ce rôle est parfois employé de manière interchangeable avec celui du FMO et du GDS.
Fabricant de matériel d'origine (FMO)	Le FMO fabrique l'appareil mobile utilisé par l'utilisateur final.
Réseau de paiement	Cet intervenant, aussi appelé *créateur de l'application de paiement,* crée une application de paiement qui n'est pas destinée à l'utilisateur final, en plus de gérer le réseau de paiement
Gestionnaire de domaine sécurisé (GDS)	Le GDS gère l'accès à l'élément sécurisé. Ce rôle est souvent combiné avec celui d'ERM, mais pas toujours. Aux fins du présent document, ce rôle est parfois employé de manière interchangeable avec celui du ERM et du FMO.
Gestionnaire de service de confiance (GSC)	(*aussi appelé application de paiement ou installateur de justificatifs de paiement*) Cet intervenant installe les justificatifs de paiement dans l'élément sécurisé. Le GSC joue le rôle de lien sécurisé entre plusieurs intervenants (p. ex., l'EJP et l'ERM) afin de faciliter l'installation des justificatifs de paiement.
Fournisseur de porte-monnaie	Le fournisseur de porte-monnaie est chargé de l'interface destinée à l'utilisateur final.

Les définitions de rôles contenues dans ce document ont été élaborées à partir de celles fournies par GlobalPlatform et PayEz[4] Les rôles désignent des acteurs qui exécutent des activités particulières; l'objectif n'est pas de préciser quels participants à l'écosystème rempliront les rôles en question.

[4] GPS_Messaging_Specification_for_Mobile_NFC_Services-v1.0 et PayEz Mobile, Mobile Contactless Proximity Payment; Part 1: Product Definition; troisième version, avril 2011, page 22.

7.5 APERÇU DES LOGICIELS ET DES APPAREILS[5]

L'appareil mobile permet la communication sans contact au moyen d'un protocole NFC (conforme à la norme ISO 14443 – cartes à puce de type A ou de type B) et d'un contrôleur NFC dédié, intégré à l'appareil mobile. Le contrôleur NFC est lié à l'UICC ou à l'élément sécurisé intégré.

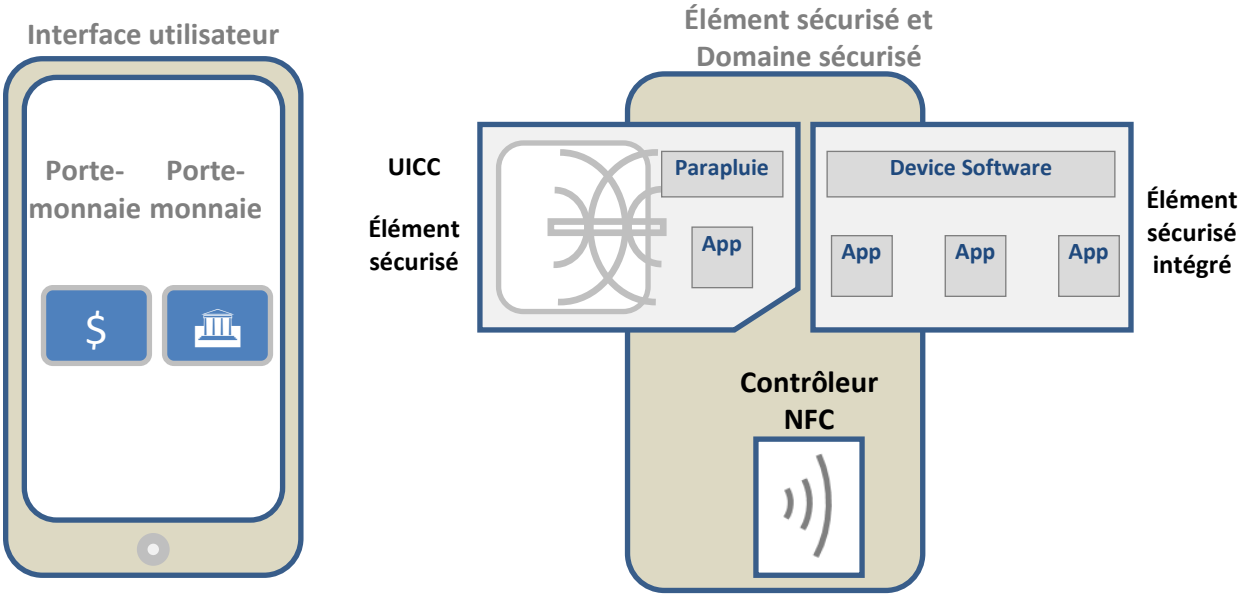
Le contrôleur NFC peut être utilisé en mode émulation, pour émuler des cartes sans contact, ou en mode lecture-écriture, pour lire des étiquettes RFID.

Les appareils mobiles doivent respecter les lignes directrices relatives aux réseaux de paiements et à la certification des ERM **[10]**. De plus, l'appareil mobile doit pouvoir accepter la réalisation d'activités d'installation de justificatifs et de maintenance, par l'entremise de radiofréquences **[11]**.

L'UICC et l'élément sécurisé intégré se composent de domaines sécurisés (DS) et de domaines sécurisés secondaires (DSS). Les DS et les DSS peuvent être affectés à des EJP distincts.

Les DS sont assortis de clés de chiffrement utilisées pour établir une voie de communication protégée entre le GSC de l'émetteur de justificatifs de paiement et le domaine sécurisé connexe.

La présente section décrit les éléments de l'appareil mobile associés à des paiements mobiles NFC.



Terme	Définition
Application compagnon (Companion Application)	Une application compagnon est liée à une application de paiement pour en accroître les fonctionnalités (p. ex., gestion des codes personnels ou registre des transactions). L'application compagnon est fournie à la discrétion de

[5] Spécifications PayEz Mobile, page 5.

Terme	Définition
	l'installateur de l'application de paiement.
Logiciel de l'appareil (Device Software)	Lorsqu'une application de paiement et des justificatifs de paiement sont stockés dans l'élément sécurisé intégré, le logiciel de l'appareil joue le rôle d'application parapluie (voir ci-dessous) en vue de localiser les justificatifs de paiement et de les associer au contrôleur NFC.
Contrôleur NFC (NFC Controller)	Désigne le matériel et le logiciel qui, ensemble, contrôlent les radio signaux NFC transmis en provenance et à destination de l'appareil mobile.
Application de paiement (Payment Application)	Une application de paiement permet de satisfaire aux exigences de sécurité en vue d'effectuer un paiement et de stocker les justificatifs de paiement.
Domaine sécurisé (Secure Domain)	Subdivision de l'élément sécurisé.
Élément sécurisé (Secure Element)	(Secure Element) Désigne la zone sécurisée intégrée ou la zone sécurisée de l'UICC où est stockée l'information chiffrée.
UICC	L'UICC (Universal Integrated Circuit Card ou carte universelle à circuits intégrés) désigne la carte à puce utilisée dans des terminaux mobiles, sur des réseaux GSM et UMTS, conformément aux définitions du European Telecommunications Standards Institute (ETSI Project Smart Card Platform [EP SCP]).
Application parapluie (Umbrella Application)	Une application parapluie est utilisée uniquement lorsqu'une application de paiement est stockée dans l'UICC. L'application parapluie permet la communication entre un porte-monnaie et toutes les applications de paiement associées à ce porte-monnaie. La relation entre l'application parapluie et les applications de paiement est une relation de type « un à plusieurs ». Dans le cas d'un élément sécurisé intégré, c'est le logiciel de l'appareil qui joue ce rôle.
Application porte-monnaie (Wallet Application)	Le porte-monnaie mobile désigne l'application destinée à l'utilisateur final, c'est-à-dire celle qui doit être installée sur l'appareil mobile. L'application permet à l'utilisateur de saisir et de gérer des renseignements précis liés à son compte, qui seront utilisés dans le cadre d'une transaction mobile NFC. Un appareil mobile peut contenir un ou plusieurs porte-monnaie mobiles à la fois, en tout temps.

7.6 EXIGENCES RELATIVES AU LECTEUR SANS CONTACT/PDV [6]

Les lecteurs sans contact au PDV doivent être conformes aux spécifications de paiement sans contact d'EMVCo [EMV-6] ainsi qu'à celles de MasterCard et/ou Visa et/ou Interac **[12]**.

Un lecteur sans contact au PDV est muni d'une antenne qui crée un champ électromagnétique permettant l'échange de données lorsqu'un appareil doté de fonctionnalités NFC se trouve à proximité. Le champ électromagnétique créé par le lecteur constitue la zone de réception.

Plus précisément, la zone de réception désigne la partie du lecteur sans contact où la radiofréquence transmise par le lecteur est la plus forte. La portée de la radiofréquence est connue sous le nom de « volume opérationnel ». La zone de réception est désignée à l'aide du symbole « sans contact ». Le lecteur extrait automatiquement les données d'un appareil NFC qui l'effleure.

Un lecteur sans contact au PDV peut être totalement intégré au terminal du commerçant ou bien fonctionner de façon indépendante, en étant branché à un terminal encastré du commerçant ou à une caisse enregistreuse électronique.

Un lecteur sans contact au PDV peut être muni de quatre lumières (p. ex., de type DEL) pour indiquer que le lecteur est prêt à échanger des données avec un appareil mobile et que la transaction de paiement mobile sans contact a été effectuée avec succès. De plus, un échange réussi de données est suivi d'un signal sonore.

Un faible signal sonore (signal d'avertissement) peut être utilisé pour aviser l'utilisateur final que le lecteur au PDV est en attente de la saisie d'un mot de passe. Ce dernier est utilisé dans le cas où l'utilisateur final doit autoriser des transactions de valeur élevée ou à risque élevé.

7.7 INTEROPÉRABILITÉ[7]

{§7} L'interopérabilité entre les divers éléments de l'écosystème des paiements mobiles représente l'un des principaux objectifs du Modèle de référence des paiements mobiles NFC. Aux fins des paiements mobiles NFC, le terme « interopérabilité » signifie que les différents éléments de l'écosystème évolueront de manière à s'intégrer les uns aux autres. En pratique, l'interopérabilité se traduit par les points ci-dessous :

- l'utilisateur final pourra choisir son appareil mobile NFC, son EJP et son ERM;
- les participants à l'écosystème et les appareils (p. ex., le terminal et les appareils au PDV) travailleront en collaboration;
- les appareils mobiles pourront communiquer avec toute plateforme de radiodiffusion;
- une plateforme de radiodiffusion sera en mesure de communiquer avec toute UICC ou tout élément sécurisé intégré;
- un appareil mobile NFC pourra communiquer avec tout lecteur sans contact qui respecte la norme ISO 14443 (cartes à puce de type A ou de type B);
- un EJP sera en mesure de communiquer avec toute plateforme de radiodiffusion.

[6] Spécifications PayEz Mobile, page 5
[7] Spécifications PayEz Mobile, page 5.

7.8 ÉNONCÉS NORMALISÉS

Numéro	Énoncé	Section
8	Si le participant à l'écosystème doit accéder à des données, obtenues au moyen d'un appareil mobile, au-delà de la limite permise afin de remplir son rôle principal, l'utilisateur final doit en être informé et il doit accorder explicitement son autorisation à cet effet.	7.2 Modèle de référence des paiements mobiles NFC – Description de la solution
9	Pour des raisons de sécurité et de prévention de la fraude, si le participant à l'écosystème doit accéder à des données, obtenues au moyen d'un appareil mobile, au-delà de la limite permise afin de remplir son rôle principal, l'émetteur de justificatifs doit également en être informé et ce dernier doit lui aussi accorder explicitement son autorisation à cet effet.	7.2 Modèle de référence des paiements mobiles NFC – Description de la solution
10	Les appareils mobiles doivent respecter les lignes directrices relatives aux réseaux de paiements et à la certification des ERM.	7.2 Modèle de référence des paiements mobiles NFC – Description de la solution
11	L'appareil mobile doit pouvoir accepter la réalisation d'activités d'installation de justificatifs et de maintenance, par l'entremise de radiofréquences.	7.5 Aperçu des logiciels et des appareils
12	Les lecteurs sans contact au PDV doivent être conformes aux spécifications de paiement sans contact d'EMVCo [EMV-6] ainsi qu'à celles de MasterCard et/ou Visa et/ou Interac.	7.6 Exigences relatives au lecteur sans contact/PDV

8 CARACTÉRISTIQUES ET FONCTIONS DU PORTE-MONNAIE ET DE L'APPLICATION DE PAIEMENT

Cette section présente les principales caractéristiques et fonctions d'une application porte-monnaie et d'une application de paiement.

Certains des éléments de cette section constituent des normes qui doivent être respectées. D'autres représentent des lignes directrices qui visent à influer sur l'évolution des paiements mobiles NFC au Canada.

Cette section repose sur les définitions et l'architecture présentées dans la section précédente.

8.1 TERMINOLOGIE ET STRUCTURE DE LA SOLUTION

Le porte-monnaie mobile désigne l'application utilisée par l'utilisateur final. Cette application peut être utilisée pour :

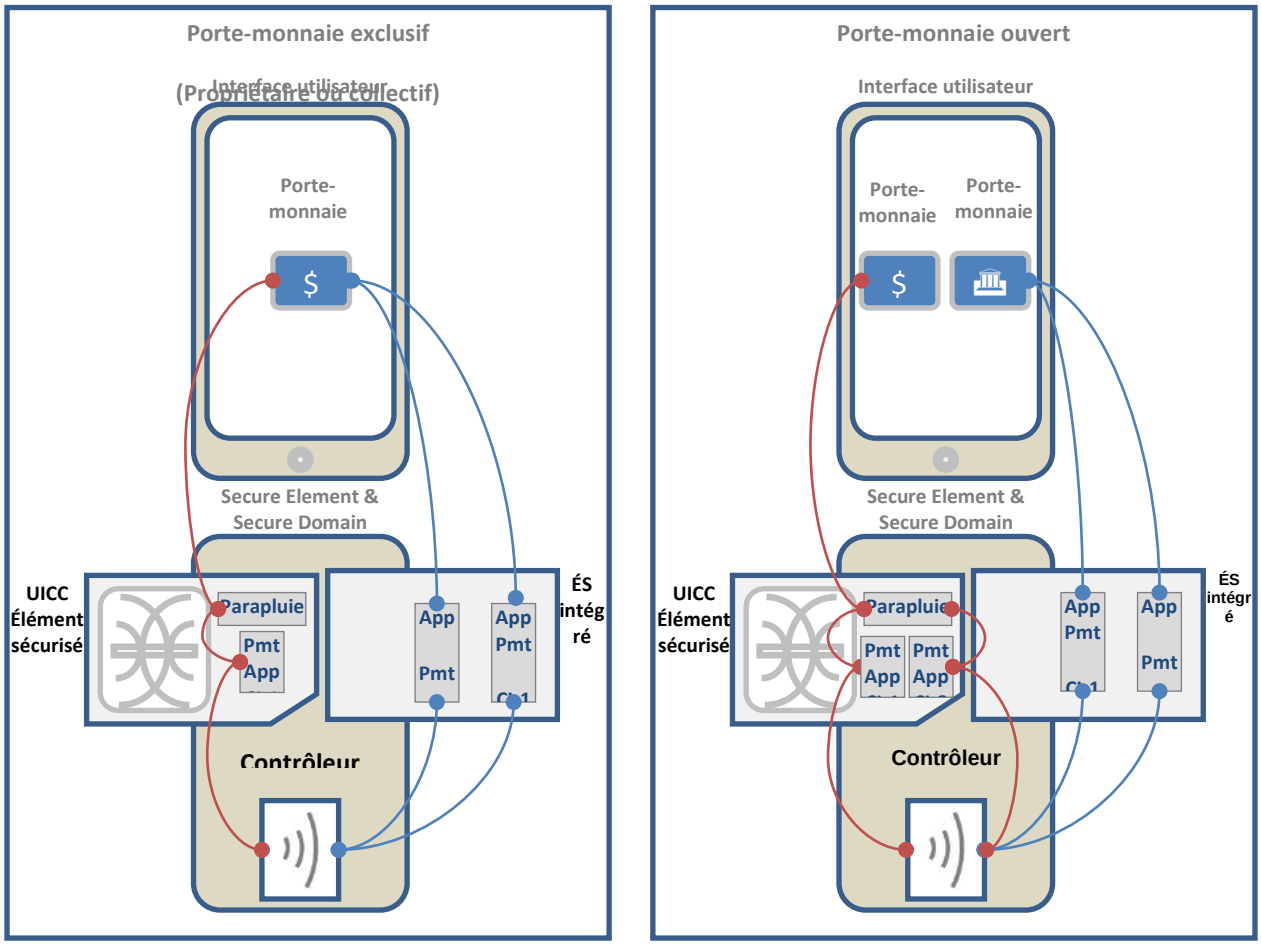
- exécuter des activités d'installation de produits et de justificatifs de paiement;
- communiquer avec l'utilisateur final;
- gérer les préférences de l'utilisateur final;
- jouer le rôle de dispositif mobile de saisie de mots de passe;
- gérer des activités d'installation de produits et de justificatifs de paiement;
- gérer de l'information associée aux programmes de fidélisation et de récompenses.

Les règles logiques et commerciales associées aux fonctions ci-dessus peuvent se trouver dans le porte-monnaie mobile ou dans d'autres applications non destinées à l'utilisateur final.

Le présent document porte sur les trois types de porte-monnaie ci-dessous.

Type de porte-monnaie	Définition
Porte-monnaie exclusif (Proprietary Wallet)	Porte-monnaie mobile conçu pour faire en sorte que seuls les justificatifs de paiement du fournisseur de porte-monnaie puissent y être associés pour effectuer des paiements mobiles NFC.
Porte-monnaie collectif (Collective Wallet)	Porte-monnaie mobile conçu par un groupe d'EJP pour faire en sorte que seuls les justificatifs de paiement de ce groupe puissent y être associés pour effectuer des paiements mobiles NFC.
Porte-monnaie ouvert (Open Wallet)	Porte-monnaie mobile conçu pour faire en sorte que les justificatifs de paiement de plusieurs EJP puissent y être associés pour effectuer des paiements mobiles NFC. Même s'il est « ouvert », ce type de porte-monnaie exige néanmoins la conclusion d'ententes et l'établissement de relations commerciales entre les EJP et les fournisseurs de porte-monnaie avant que des justificatifs de paiement puissent être associés à un porte-monnaie.

À gauche, un porte-monnaie exclusif ou collectif (porte-monnaie de type fermé, ou Closed Wallet) est délivré par l'EJP 1 et associé à des applications de paiement et à des justificatifs de paiement de l'EJP 1. À droite, un ou plusieurs porte-monnaie ouverts de l'EJP 1 et de l'EJP 2 sont associés à des applications de paiement et à des justificatifs de paiement de l'EJP 1 et de l'EJP 2.



Les auteurs du présent document reconnaissent que, à court terme, les porte-monnaie exclusifs et collectifs représenteront vraisemblablement, aux yeux des participants à l'écosystème, la solution la mieux adaptée aux conditions actuelles du marché. Indépendamment des fonctions mises au point dans le cadre de projets pilotes ou de lancements commerciaux initiaux, les organismes qui adoptent les présentes normes s'attendent à passer au modèle de porte-monnaie ouvert et à abandonner la structure de porte-monnaie exclusif ou collectif dans les dix-huit mois suivant le lancement du premier porte-monnaie ouvert au Canada.

8.2 OUVERTURE ET INTEROPÉRABILITÉ

Afin de respecter les objectifs en matière d'ouverture et d'interopérabilité, les porte-monnaie mobiles, les ERM, les FMO, les GDS et les EJP ne doivent pas limiter l'accès à des applications de paiement liées aux éléments ci-dessous :

- produits de paiement par carte de débit
- produits de paiement par carte de crédit
- produits de paiement prépayés;

- autres produits de paiement, y compris ceux associés à des titres de transport et à des programmes de fidélisation;
- produits de paiement créés en monnaie étrangère (p. ex., produits basés sur le dollar américain).

Le présent énoncé normalisé est assujetti à la mise en place des relations commerciales et des capacités techniques appropriées **[13]**.

Il n'existe pas de restrictions quant aux autres applications de paiement auxquelles un porte-monnaie peut donner accès. Si le propriétaire du porte-monnaie, l'EJP et l'utilisateur final l'approuvent et s'ils ont établi la relation commerciale appropriée, le porte-monnaie peut être associé à n'importe quelle autre forme de justificatif (de paiement ou autre). Les applications ou les justificatifs de paiement ne doivent pas être conçus de manière à interdire l'accès d'un porte-monnaie à d'autres applications ou justificatifs de paiement, si les relations commerciales appropriées ont été établies **[14]**.

8.3 CARACTÉRISTIQUES ET FONCTIONS DU PORTE-MONNAIE

Les principales caractéristiques et fonctions d'un porte-monnaie mobile sont décrites dans cette section. Les recommandations et les énoncés normalisés fournis ici visent à protéger l'utilisateur final.

La sécurité, toutefois, n'est pas l'unique préoccupation. Dans l'élaboration de cette section, l'accent a été mis sur l'équilibre entre la sûreté et sécurité et l'expérience de l'utilisateur final. Par exemple, il serait plus sûr de demander à un utilisateur final de saisir des mots de passe distincts pour activer son appareil mobile, accéder à son porte-monnaie, autoriser une transaction et confirmer l'exécution d'une transaction de valeur élevée ou à risque élevé. Le recours à un tel modèle, très sûr, aurait entraîné des résultats défavorables sur le plan de l'expérience de l'utilisateur final.

Cette section contient une série d'énoncés normalisés fondés sur des caractéristiques de base en matière de sécurité, qui permettent toutefois à l'utilisateur final d'ajouter des mesures de sécurité supplémentaires s'il le désire.

- **Approvisionnement en justificatifs :** un porte-monnaie mobile peut donner à l'utilisateur final la possibilité de demander l'approvisionnement en justificatifs de paiement, c'est-à-dire, déclencher un processus d'installation.
- **Accès au porte-monnaie mobile :** pour des raisons de sécurité, un porte-monnaie mobile doit donner à l'utilisateur final la possibilité de le verrouiller et de le déverrouiller à l'aide d'un mot de passe de son choix **[15]**. Cette norme n'oblige pas l'utilisateur final à utiliser un mot de passe, mais vise à lui donner la possibilité de le faire.
- **Sélection de justificatifs par défaut :** un porte-monnaie mobile doit donner à l'utilisateur final la possibilité d'activer et de désactiver les justificatifs de paiement par défaut **[16]**. Les justificatifs de paiement par défaut permettent à l'utilisateur final de déclencher un paiement en laissant l'appareil mobile en mode attente et sans avoir à choisir manuellement un porte-monnaie. Les porte-monnaie peuvent aussi être conçus de manière à permettre l'établissement de paramètres globaux par défaut : en tenant compte des justificatifs de paiement par défaut des autres porte-monnaie, il est possible de définir des justificatifs de paiement par défaut s'appliquant à tous les porte-monnaie de l'appareil mobile.
- **Annulation manuelle :** un porte-monnaie mobile doit donner à l'utilisateur final la possibilité d'annuler l'application de justificatifs de paiement par défaut et de les remplacer par des justificatifs de paiement choisis manuellement **[17]**.

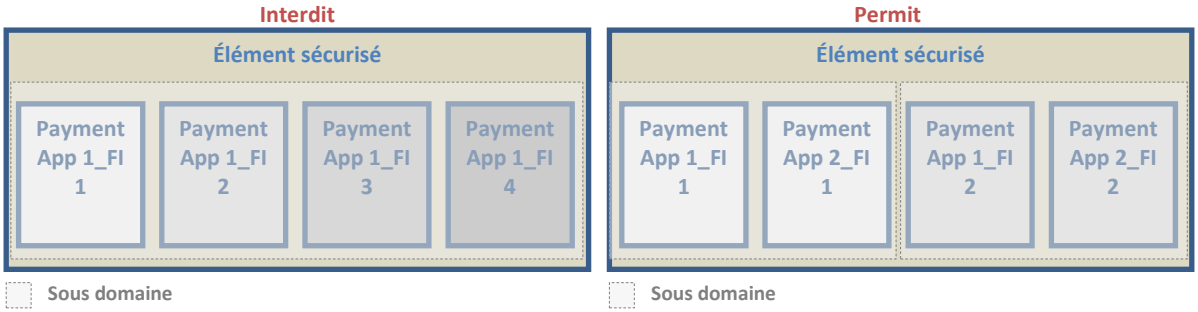
- **Paiements de valeur élevée ou à risque élevé :** un porte-monnaie mobile doit permettre à l'utilisateur final de saisir un mot de passe pour confirmer des paiements de valeur élevée ou à risque élevé **[18]**.
- **Données relatives aux transactions :** un porte-monnaie mobile peut collecter des données relatives aux transactions réalisées à l'aide de toutes les applications de paiement qui y sont liées; cependant, si de telles données sont recueillies, l'accès à ces données et leur utilisation doivent être limités selon les normes établies dans la section Données et sécurité du présent document **[19]**.
- **Reçus électroniques :** un porte-monnaie mobile peut stocker, extraire et transmettre des reçus électroniques. Si des reçus électroniques sont stockés, ils ne doivent pas sortir du porte-monnaie utilisé pour effectuer le paiement.
- **Transactions de remise d'achat :** les porte-monnaie mobiles et les applications de paiement doivent autoriser l'exécution de transactions de remise d'achat **[20]**. Dans le cas de telles transactions, l'utilisateur final choisit l'application de paiement à utiliser, puis il effleure le lecteur au PDV à l'aide de l'appareil mobile.
- **Fidélisation et récompenses :** un appareil mobile peut être utilisé pour stocker et gérer l'information relative aux programmes de fidélisation et de récompenses.

8.4 APPLICATION ET JUSTIFICATIFS DE PAIEMENT

L'application et les justificatifs de paiement sont essentiels au traitement de paiements mobiles NFC. L'application de paiement est semblable à celle qui est installée dans une carte sans contact (p ex., PayWave et PayPass). Les justificatifs de paiement désignent des renseignements personnalisés associés à cette application, renseignements qui ne correspondent qu'à un seul produit de paiement précis. L'application et les justificatifs de paiement sont des éléments non destinés à l'utilisateur final qui sont installés dans l'appareil mobile NFC. Sauf indication contraire, les expressions « application de paiement » et « justificatifs de paiement » sont utilisées comme synonymes dans le présent document.

- **Emplacement de l'application de paiement :** tous les éléments de l'application de paiement et des justificatifs de paiement (y compris l'application de paiement personnalisée et le mot de passe associé) doivent être regroupés dans l'appareil mobile, soit dans un élément sécurisé de l'UICC, soit dans une zone de l'élément sécurisé intégré **[21]**. Plusieurs possibilités ont été examinées concernant le stockage de l'application de paiement. Cependant, pour des raisons de sécurité, une seule méthode est privilégiée dans le cadre de ce document. Chaque EJP doit stocker l'application de paiement dans un domaine sécurisé secondaire (DSS) au sein de l'élément sécurisé **[22]**. La présente norme n'empêche pas la sauvegarde de plusieurs justificatifs ou applications de paiement d'un EJP donné dans le même DSS. Chaque DSS doit être assorti de clés de chiffrement particulières qui sont requises pour établir une voie de communication protégée entre le GSC de l'EJP et le domaine sécurisé approprié[8] **[23].**

[8] Spécifications PayEz Mobile, page 5.



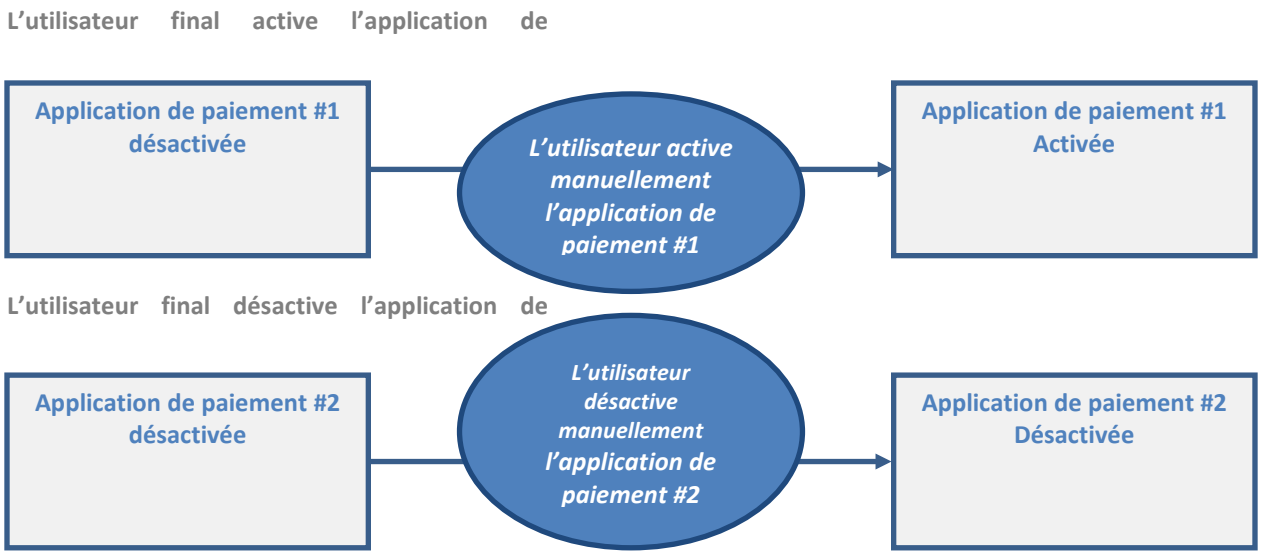
- **Partage de l'application de paiement** : une application de paiement doit contenir de l'information provenant d'un seul EJP **[24]**. Le partage d'une application de paiement entre plusieurs EJP est interdit (cette norme s'applique aux mises en œuvre initiales dans l'écosystème; elle pourrait être revue à mesure que le système évolue et que de nouvelles technologies sont implantées).
- **Caractère ouvert de l'application de paiement :** si les relations commerciales et contractuelles appropriées ont été établies, une application de paiement ne doit pas prévenir l'association à plusieurs porte-monnaie **[25]**.
- **Repérage des justificatifs :** les applications et les justificatifs de paiement contiennent des renseignements sécurisés et chiffrés. Aucune autre application ne doit avoir accès à ces renseignements **[26]**. Cependant, afin de permettre à l'utilisateur final de repérer et de choisir des justificatifs de paiement, il peut être nécessaire d'associer des renseignements à des justificatifs de paiement pouvant être utilisés par un porte-monnaie mobile ou par une autre application. Afin d'assurer une expérience utilisateur cohérente, dans le cadre du présent document, il est recommandé que seuls les renseignements suivants soient partagés : nom de l'établissement émetteur des justificatifs de paiement, nom du réseau de paiement, images associées à la carte, numéro de compte masqué, type de produit de paiement (c'est-à-dire carte de débit ou de crédit) et date d'expiration (s'il y a lieu).
- **Protocoles de stockage liés à l'application de paiement** : une application de paiement et les justificatifs de paiement connexes doivent être stockés selon les directives appropriées d'EMVCo et du réseau de paiement **[27]**
- **Activation et désactivation de l'application de paiement :** il est possible qu'une application de paiement doive être activée pour transmettre des justificatifs de paiement ou désactivée pour empêcher leur transmission. L'application de paiement peut être activée et désactivée de plusieurs façons. Un moyen consiste à empêcher l'application de paiement de recevoir les radio signaux NFC. Un autre moyen consiste à empêcher l'application de paiement d'accéder aux justificatifs de paiement. (Pour en savoir plus sur les normes visant l'activation et la désactivation de l'application de paiement, consultez la section 8.4.1, Activation et désactivation de l'application de paiement.)
- **Application compagnon** : des services supplémentaires peuvent être ajoutés à une application de paiement à l'aide d'une application compagnon. Pour qu'une application compagnon soit ajoutée, l'EJP doit approuver cet ajout et l'application compagnon doit respecter les mêmes protocoles de sécurité que l'application de paiement **[28]**
- **Application parapluie ou logiciel de l'appareil :** une application de paiement est associée à une application porte-monnaie (et parfois à des radio signaux NFC) au moyen d'une application parapluie, dans le cas de l'UICC, et du logiciel de l'appareil, dans le cas d'un élément sécurisé intégré. L'application parapluie et le logiciel de l'appareil (utilisés comme synonymes dans ce document) jouent le rôle de répertoire afin que l'application de paiement puisse être repérée. L'application porte-monnaie, l'application parapluie (s'il y a lieu) et l'application de paiement sont assujetties à un processus d'association sécurisé **[29]**. Les normes relatives au processus d'association sont décrites dans la section 8.4.2, Association de l'application porte-monnaie et de l'application de paiement.

8.4.1 ACTIVATION ET DÉSACTIVATION DE L'APPLICATION DE PAIEMENT[9]

L'activation et la désactivation de l'application de paiement constituent des moyens de prévenir l'utilisation fautive de justificatifs pour effectuer un paiement. Les solutions de paiement mobile NFC doivent faire en sorte qu'il soit impossible d'activer plus d'une application de paiement mobile (soit une application permettant d'effectuer des paiements), à la fois **[30]**. L'application de paiement activée sera utilisée pour exécuter toutes les transactions de paiement.

L'application de paiement activée doit être clairement indiquée sur la liste d'applications de paiement affichée dans le porte-monnaie mobile **[31]**. Afin de promouvoir une expérience utilisateur cohérente, les justificatifs de paiement activés peuvent être en gras, surlignés ou accompagnés d'un crochet.

L'utilisateur final a aussi la possibilité de désigner une application ou des justificatifs de paiement par défaut dans le porte-monnaie mobile. Si l'utilisateur final définit une application de paiement par défaut, cette dernière sera activée, sauf si l'utilisateur choisit d'en activer une autre. Dès qu'une application porte-monnaie est fermée, l'application de paiement par défaut est activée et les autres applications de paiement sont désactivées, pour faire en sorte qu'une seule application de paiement soit activée à la fois.



Si une application de paiement par défaut a été définie, elle doit être désactivée avant qu'une autre application de paiement puisse être activée **[32]**.

Si un EJP bloque une application de paiement (p. ex., au niveau de l'appareil ou du compte), elle ne peut pas être utilisée pour effectuer un paiement. L'utilisateur final ne doit pas être en mesure de choisir une application bloquée pour effectuer un paiement. Pour que cette application puisse être choisie, l'utilisateur final et l'EJP doivent appliquer la marche à suivre appropriée en vue de débloquer l'application de paiement **[33]**

[9] Spécifications PayEz Mobile 2.1.

8.4.2 ASSOCIATION D'UNE APPLICATION PORTE-MONNAIE ET D'UNE APPLICATION DE PAIEMENT

Avant que des justificatifs puissent être utilisés pour effectuer un paiement, une application de paiement et un porte-monnaie doivent être associés au moyen d'un processus sécurisé qui permet au porte-monnaie d'accéder à l'application de paiement. Ce processus est appelé « association » **[34]**

Avant que l'application porte-monnaie et l'application de paiement puissent être associées, le réseau de paiement et l'EJP, puis l'EJP et le fournisseur de porte-monnaie doivent établir une relation commerciale valide **[35]**. Il est recommandé que cette relation soit documentée dans un contrat décrivant la procédure de sécurité ainsi que les règles en matière de confidentialité des données, de responsabilité, de service à la clientèle et de gestion de la relation avec l'utilisateur final.

Le porte-monnaie mobile et l'application de paiement peuvent être associés directement au moyen d'une application parapluie. Le processus d'association d'une application porte-monnaie et d'une application de paiement est décrit dans la section Habilitation et gestion du cycle de vie.

8.5 CARACTÉRISTIQUES ET FONCTIONS DU PORTE-MONNAIE ET DE L'APPLICATION DE PAIEMENT – RÉSUMÉ

La présente section décrit les principales caractéristiques et fonctions d'une application porte-monnaie et d'une application de paiement. Les normes de cette section visent à protéger l'utilisateur final, à promouvoir la sûreté et la sécurité de l'écosystème et à assurer la cohérence de l'expérience utilisateur.

La prochaine section présente les normes liées au traitement des transactions.

8.6 ÉNONCÉS NORMALISÉS

Numéro	Énoncé	Section
13	Afin de respecter les objectifs en matière d'ouverture et d'interopérabilité, les porte-monnaie mobiles, les ERM, les FMO, les GDS et les EJP ne doivent pas limiter l'accès à des applications de paiement liées aux éléments ci-dessous : • produits de paiement par carte de débit • produits de paiement par carte de crédit • produits de paiement prépayés; • autres produits de paiement, y compris ceux associés à des titres de transport et à des programmes de fidélisation; • produits de paiement créés en monnaie étrangère (p. ex., produits basés sur le dollar américain). Le présent énoncé normalisé est assujetti à la mise en place des relations commerciales et des capacités techniques appropriées.	8.2 Ouverture et interopérabilité
14	Les applications ou les justificatifs de paiement ne doivent pas être conçus de manière à interdire l'accès d'un porte-monnaie à d'autres applications ou justificatifs de paiement, si les relations commerciales appropriées ont été établies.	8.2 Ouverture et interopérabilité

Numéro	Énoncé	Section
15	Accès au porte-monnaie mobile : pour des raisons de sécurité, un porte-monnaie mobile doit donner à l'utilisateur final la possibilité de le verrouiller et de le déverrouiller à l'aide d'un mot de passe de son choix.	8.3 Caractéristiques et fonctions du porte-monnaie
16	Sélection de justificatifs par défaut : un porte-monnaie mobile doit donner à l'utilisateur final la possibilité d'activer et de désactiver les justificatifs de paiement par défaut.	8.3 Caractéristiques et fonctions du porte-monnaie
17	Annulation manuelle : un porte-monnaie mobile doit donner à l'utilisateur final la possibilité d'annuler l'application de justificatifs de paiement par défaut et de les remplacer par des justificatifs de paiement choisis manuellement.	8.3 Caractéristiques et fonctions du porte-monnaie
18	Paiements de valeur élevée ou à risque élevé : un porte-monnaie mobile doit permettre à l'utilisateur final de saisir un mot de passe pour confirmer des paiements de valeur élevée ou à risque élevé.	8.3 Caractéristiques et fonctions du porte-monnaie
19	Données relatives aux transactions : un porte-monnaie mobile peut collecter des données relatives aux transactions réalisées à l'aide de toutes les applications de paiement qui y sont liées; cependant, si de telles données sont recueillies, l'accès à ces données et leur utilisation doivent être limitées selon les normes établies dans la section Données et sécurité du présent document.	8.3 Caractéristiques et fonctions du porte-monnaie
20	Transactions de remise d'achat : les porte-monnaie mobiles et les applications de paiement doivent autoriser l'exécution de transactions de remise d'achat.	8.3 Caractéristiques et fonctions du porte-monnaie
21	Emplacement de l'application de paiement : tous les éléments de l'application de paiement et des justificatifs de paiement (y compris l'application de paiement personnalisée et le mot de passe associé) doivent être regroupés dans l'appareil mobile, soit dans un élément sécurisé de l'UICC, soit dans une zone de l'élément sécurisé intégré. [Suite à l'EN22]	8.4 Application et justificatifs de paiement
22	[Suite de l'EN21] Cependant, pour des raisons de sécurité, une seule méthode est privilégiée dans le cadre de ce document. Chaque EJP doit stocker l'application de paiement dans un domaine sécurisé secondaire (DSS) au	8.4 Application et justificatifs de paiement

Numéro	Énoncé	Section
	sein de l'élément sécurisé.	
23	Chaque DSS doit être assorti de clés de chiffrement particulières qui sont requises pour établir une voie de communication protégée entre le GSC de l'EJP et le domaine sécurisé approprié.	8.4 Application et justificatifs de paiement
24	Partage de l'application de paiement : une application de paiement doit contenir de l'information provenant d'un seul EJP.	8.4 Application et justificatifs de paiement
25	Caractère ouvert de l'application de paiement : si les relations commerciales et contractuelles appropriées ont été établies, une application de paiement ne doit pas prévenir l'association à plusieurs porte-monnaie.	8.4 Application et justificatifs de paiement
26	Repérage des justificatifs : les applications et les justificatifs de paiement contiennent des renseignements sécurisés et chiffrés. Aucune autre application ne doit avoir accès à ces renseignements.	8.4 Application et justificatifs de paiement
27	Protocoles de stockage liés à l'application de paiement : une application de paiement et les justificatifs de paiement connexes doivent être stockés selon les directives appropriées d'EMVCo et du réseau de paiement.	8.4 Application et justificatifs de paiement
28	[Contexte – Application compagnon : des services supplémentaires peuvent être ajoutés à une application de paiement à l'aide d'une application compagnon.] Pour qu'une application compagnon soit ajoutée, l'EJP doit approuver cet ajout et l'application compagnon doit respecter les mêmes protocoles de sécurité que l'application de paiement.	8.4 Application et justificatifs de paiement
29	L'application porte-monnaie, l'application parapluie (s'il y a lieu) et l'application de paiement sont assujetties à un processus d'association sécurisé.	8.4 Application et justificatifs de paiement
30	Les solutions de paiement mobile NFC doivent faire en sorte qu'il soit impossible d'activer plus d'une application de paiement mobile (soit une application permettant d'effectuer des paiements) à la fois.	8.4.1 Activation et désactivation de l'application de paiement
31	L'application de paiement activée doit être clairement indiquée sur la liste d'applications de paiement affichée	8.4.1 Activation et désactivation de

Numéro	Énoncé	Section
	dans le porte-monnaie mobile.	l'application de paiement
32	Si une application de paiement par défaut a été définie, elle doit être désactivée avant qu'une autre application de paiement puisse être activée.	8.4.1 Activation et désactivation de l'application de paiement
33	L'utilisateur final ne doit pas être en mesure de choisir une application bloquée pour effectuer un paiement. Pour que cette application puisse être choisie, l'utilisateur final et l'EJP doivent appliquer la marche à suivre appropriée en vue de débloquer l'application de paiement.	8.4.1 Activation et désactivation de l'application de paiement
34	Avant que des justificatifs puissent être utilisés pour effectuer un paiement, une application de paiement et un porte-monnaie doivent être associés au moyen d'un processus sécurisé qui permet au porte-monnaie d'accéder à l'application de paiement. Ce processus est appelé « association ».	8.4.2 Association d'une application porte-monnaie et d'une application de paiement
35	Avant que l'application porte-monnaie et l'application de paiement puissent être associées, le réseau de paiement et l'EJP, puis l'EJP et le fournisseur de porte-monnaie doivent établir une relation commerciale valide.	8.4.2 Association d'une application porte-monnaie et d'une application de paiement

9 TRAITEMENT DES TRANSACTIONS

La section Traitement des transactions porte sur les aspects du processus de traitement des transactions de paiement mobile NFC qui constituent des nouveautés, c'est-à-dire des aspects qui diffèrent du processus de traitement par carte sans contact. Cette section présente des lignes directrices et des normes qui renforcent la sûreté et la sécurité de l'écosystème, protègent l'utilisateur final et assurent une expérience utilisateur cohérente dans le cadre de transactions de paiement NFC.

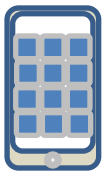
Cette section a été rédigée en présumant que les paiements mobiles NFC seront exécutés au moyen des réseaux de paiement existants (p. ex., Interac, Visa et MasterCard). Ce modèle a été spécialement conçu pour réduire les effets sur les marchands, les utilisateurs finaux et les autres participants à l'écosystème. Cette section est basée sur les étapes habituelles d'une transaction de paiement et elle vise à réduire les effets sur le marchand en offrant une expérience utilisateur cohérente.

Voici un aperçu du processus d'achat dans le cadre de paiements mobiles :

***L'usager final** présente ses achats au **marchand** pour effectuer le paiement.*

*Le **marchand** calcule la somme due et informe **l'usager final**.*

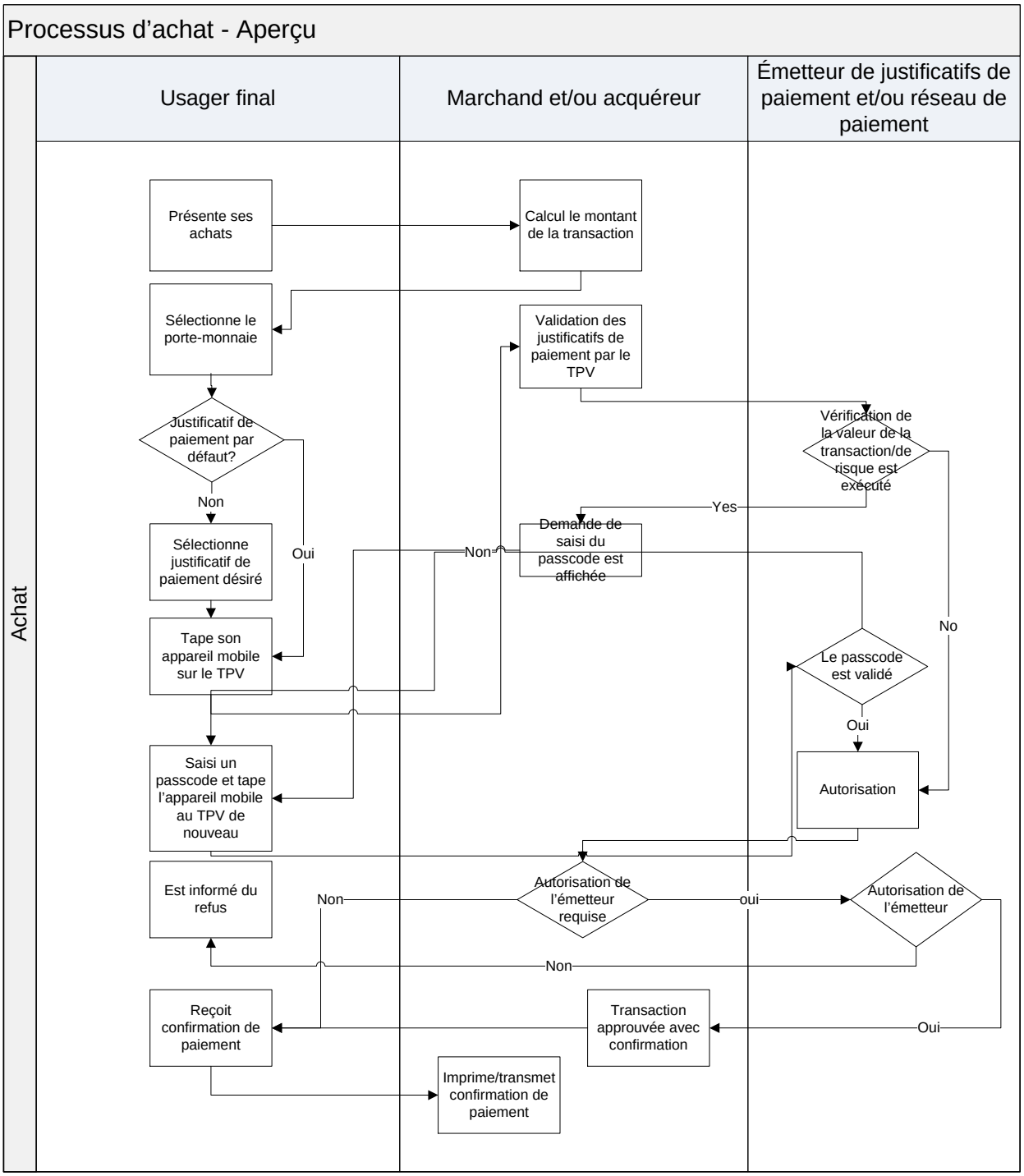
*The **L'usager final** active le porte-monnaie, sélectionne le justificatif de paiement à utiliser et tape son téléphone au TPV*



*Si le montant du paiement excède les valeurs prescrites, **l'usager final** devra entrer un passcode et taper son téléphone au TPV de nouveau*

***Le réseau de paiement** autorise les paiements, le **marchand** et **l'usager final** sont informés et le reçu est transmis ou imprimé.*

Vous trouverez à la page suivante une illustration plus détaillée du déroulement de la transaction.



Nota : même si les étapes de la MVC figurent sous la rubrique Émetteur de justificatifs, en réalité, ces étapes sont franchies localement par l'application de paiement.

À quelques différences près, le déroulement d'une transaction mobile est semblable à celui d'une transaction par carte sans contact. Les différences ci-dessous sont abordées dans la présente section :

- transactions utilitaires;

- transactions de valeur élevée ou à risque élevé;
- transactions de remise d'achat;
- reçus électroniques.

9.1 TRANSACTIONS UTILITAIRES EFFECTUÉES À L'AIDE D'UN APPAREIL MOBILE

Une transaction utilitaire désigne une transaction qui satisfait à certains critères en matière de valeur monétaire et de catégorie de dépenses. Les transactions utilitaires sont habituellement des transactions effectuées de manière fréquente et rapide (p. ex., l'achat d'un titre de transport ou d'un café). Les transactions utilitaires ne doivent pas dépasser les limites établies à l'égard des transactions de valeur élevée ou à risque élevé, selon les définitions des réseaux de paiement **[36]**. Par ailleurs, une transaction de remise d'achat n'est pas une transaction utilitaire.

Une transaction utilitaire doit respecter les lignes directrices existantes des réseaux de paiement à l'égard des paiements sans contact; sauf si les règles de sécurité l'exigent (p. ex., un compteur de transactions), la transaction utilitaire ne doit pas exiger plus qu'un simple « tapez et partez » pour la réalisation d'un paiement et elle ne doit pas être assujettie à une MVC supplémentaire **[37]**.

9.2 TRANSACTIONS DE VALEUR ÉLEVÉE OU À RISQUE ÉLEVÉ EFFECTUÉES À L'AIDE D'APPAREILS MOBILES

9.2.1 APERÇU

L'EJP et/ou les réseaux de paiement définissent les transactions de valeur élevée ou à risque élevé. L'utilisateur final doit approuver les transactions de valeur élevée ou à risque élevé en appliquant une MVC **[38]**.

Il existe diverses options pour vérifier la validité d'une transaction de valeur élevée ou à risque élevé effectuée à l'aide d'un appareil mobile. Après l'analyse de plusieurs d'entre elles, une seule a été retenue à des fins d'autorisation par l'utilisateur final. Une fois qu'elles sont jugées acceptables par les réseaux de paiement, les transactions de valeur élevée ou à risque élevé doivent être approuvées à l'aide de la MVC dénommée « tapez et confirmez » (une première tape de l'écran de l'appareil, suivie de la saisie du mot de passe, puis d'une deuxième tape) **[39]**. Les autres MVC examinées et rejetées en tant que méthode cible sont énumérées en annexe.

À mesure que la popularité et l'omniprésence des paiements mobiles NFC augmentent et que les offres de programmes de fidélisation et de récompenses sont adaptées aux appareils mobiles, on s'attend à ce que les paiements mobiles NFC soient utilisés pour effectuer des achats de valeur croissante.

9.2.2 APERÇU DES DIFFÉRENTES MVC

Il existe sept MVC communément acceptées relativement aux transactions de valeur élevée ou à risque élevé. Après analyse, la méthode « tapez et confirmez » a été choisie comme méthode cible dans le cadre des paiements mobiles NFC au Canada.

- **Tapez et partez –** L'utilisateur final tape l'écran de l'appareil une seule fois. Aucune MVC supplémentaire n'est requise; cette méthode est utilisée pour exécuter des transactions utilitaires.
- **Saisie du mot de passe et vérification par radiofréquence –** L'utilisateur final tape l'écran de l'appareil comme pour effectuer une transaction utilitaire et, quand on le lui demande, il saisit le mot de passe dans l'appareil. Ce dernier est alors transmis par radiofréquence au moyen du réseau mobile, puis vérifié par le réseau de paiement.

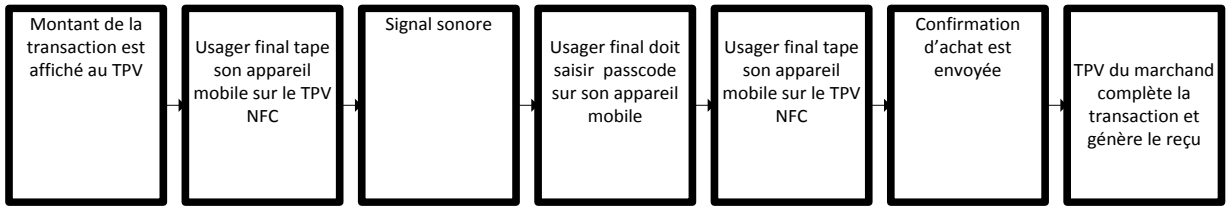
- **Saisie du mot de passe dans le terminal au point de vente (TPV) du marchand – L'utilisateur final tape l'écran de l'appareil comme pour effectuer une transaction utilitaire et, quand on le lui demande, il saisit le mot de passe dans le TPV du marchand.** Le mot de passe est alors vérifié par le réseau de paiement.
- **Tapez et confirmez (méthode cible) – L'utilisateur final tape l'écran de l'appareil comme pour effectuer une transaction utilitaire et, quand on le lui demande, il saisit le mot de passe dans l'appareil, puis tape l'écran de nouveau.** L'application de paiement vérifie alors le mot de passe et l'acceptation ou le refus de la transaction est communiqué à un tiers. La méthode « tapez et confirmez » est la seule méthode de vérification de cartes approuvée; elle doit être utilisée dès qu'une transaction est jugée acceptable par un réseau de paiement [**40.**
- **Tapez, confirmez et reconfirmez –** L'utilisateur final tape l'écran de l'appareil comme pour effectuer une transaction utilitaire et, quand on le lui demande, il saisit le mot de passe dans l'appareil puis, à l'aide de ce dernier, effleure le lecteur au PDV. En dernier lieu, l'utilisateur final est invité à taper l'écran une fois de plus pour recevoir une confirmation de paiement.
- **Tapez et branchez-vous –** L'utilisateur final tape l'écran de l'appareil mobile puis, quand on le lui demande, il tape l'écran de nouveau, établissant ainsi une connexion bidirectionnelle. Une fois cette connexion établie, il saisit le mot de passe dans l'appareil mobile. Dans le cas de cette MVC, une connexion ouverte doit être maintenue pendant toute la durée du processus de vérification.
- **Tapez et explorez –** Il s'agit d'une version étendue de la méthode « tapez et branchez-vous ». Ici, l'utilisateur final tape l'écran de l'appareil mobile et établit une connexion qui est utilisée à des fins de vérification et de transmission de renseignements associés à un programme de fidélisation.

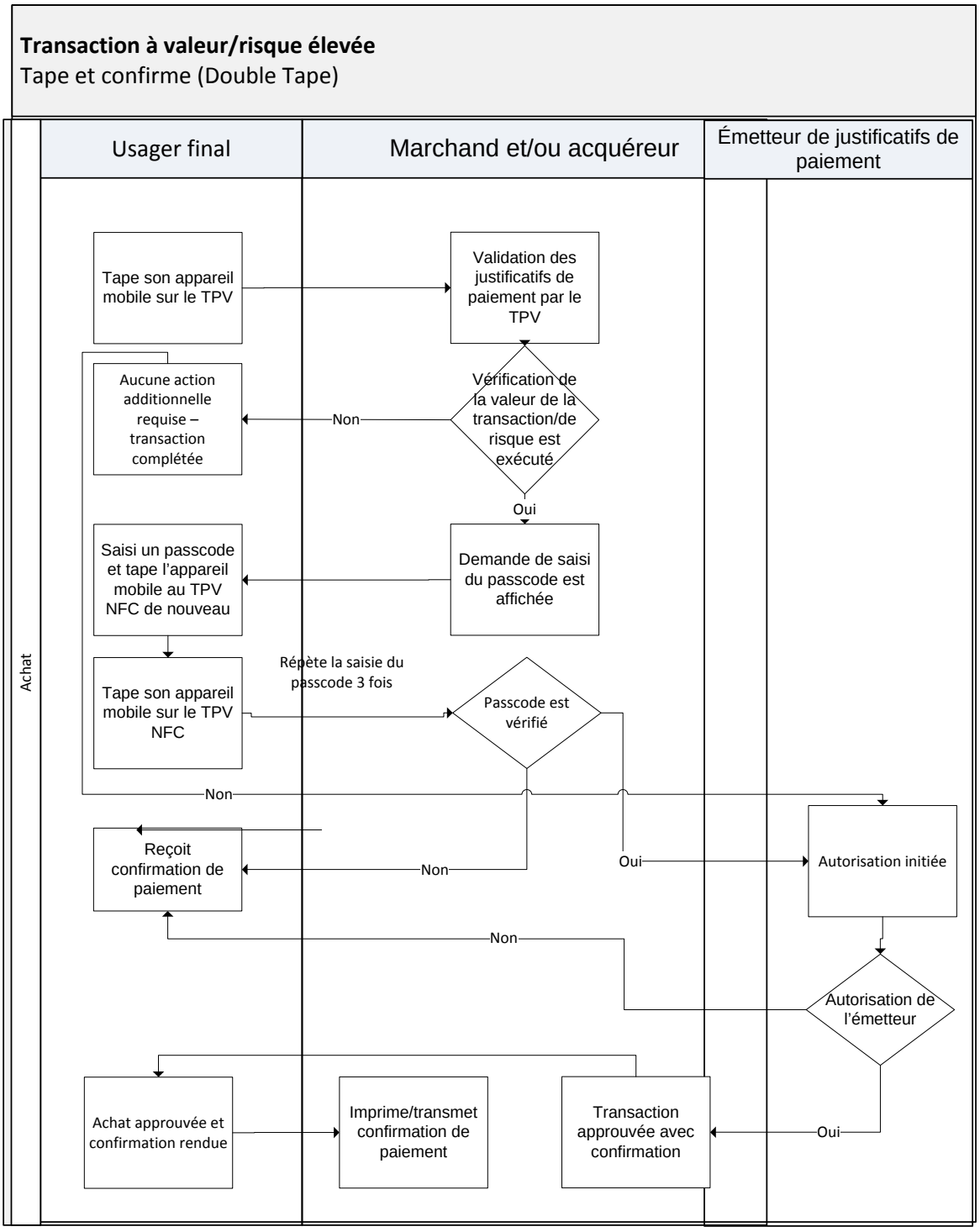
Dans la présente section, il est présumé que l'utilisateur final a défini un type de paiement par défaut. Si l'utilisateur final souhaite choisir un autre type de paiement pour la transaction en cours, il peut le faire avant d'effleurer le PDV de son appareil mobile. Une fois la transaction terminée, la méthode de paiement par défaut est rétablie.

La MVC standard au Canada relativement aux paiements de valeur élevée ou à risque élevé est la méthode **« tapez et confirmez »** (**méthode requérant deux tapes)** [**41]**. Compte tenu des limites actuelles associées aux TPV NFC et des plans de mise en œuvre des réseaux, il faudra un certain temps avant que cette norme puisse être adoptée. D'autres MVC (tapez et signez, etc.) seront acceptées jusqu'à ce que les EJP et les réseaux de paiement déterminent que la méthode « tapez et confirmez » sera la seule acceptée. Cette norme est conforme aux normes de Visa, de MasterCard et d'Interac ainsi qu'aux normes européennes, et elle contribuera à assurer l'interopérabilité à l'échelle mondiale.

9.2.3 TAPEZ ET CONFIRMEZ – DOUBLE TAPE

Il s'agit de la norme adoptée par l'European Payments Council à l'égard des transactions de valeur élevée. L'exécution d'une transaction de valeur élevée uniquement fondée sur la technologie NFC exige deux tapes au minimum. L'utilisateur final doit taper une seule fois l'écran dans le cas de transactions de faible valeur et deux fois dans le cas de transactions de valeur élevée. Toutes les mises à jour relatives à l'application de paiement et au processus de confirmation se font par radiofréquence.


Montant de la transaction est affiché au TPV
Usager final tape son appareil mobile sur le TPV NFC
Signal sonore
Usager final doit saisir passcode sur son appareil mobile
Usager final tape son appareil mobile sur le TPV NFC
Confirmation d'achat est envoyée
TPV du marchand complète la transaction et génère le reçu



Nota : même si les étapes de la MVC figurent sous la rubrique Émetteur de justificatifs, en réalité, ces étapes sont franchies localement par l'application de paiement.

Consultez l'annexe pour en savoir plus sur le processus d'évaluation des MVC.

9.3 REÇUS ÉLECTRONIQUES

La délivrance du reçu est la dernière étape du traitement d'une transaction mobile NFC. Il n'existe pas de normes particulières quant à la délivrance de reçus relativement aux paiements mobiles. Cette section vise à souligner qu'il y a différentes façons de délivrer des reçus pour les paiements mobiles NFC. La délivrance des reçus doit être conforme aux lignes directrices en vigueur. **[42]** Les reçus peuvent être délivrés en format imprimé, électronique ou autre.

Certains marchands donnent à l'utilisateur final la possibilité de recevoir des reçus électroniques. Habituellement, ces reçus sont envoyés du TPV du marchand à l'adresse de courriel de l'utilisateur. Compte tenu de l'arrivée du porte-monnaie mobile, il est possible que les utilisateurs finaux demandent aux marchands de leur fournir des reçus électroniques au lieu de reçus imprimés. Dans ces cas, le marchand doit envoyer le reçu au porte-monnaie mobile de l'utilisateur final. Après réception, le reçu électronique peut être sauvegardé dans le porte-monnaie en toute sécurité.

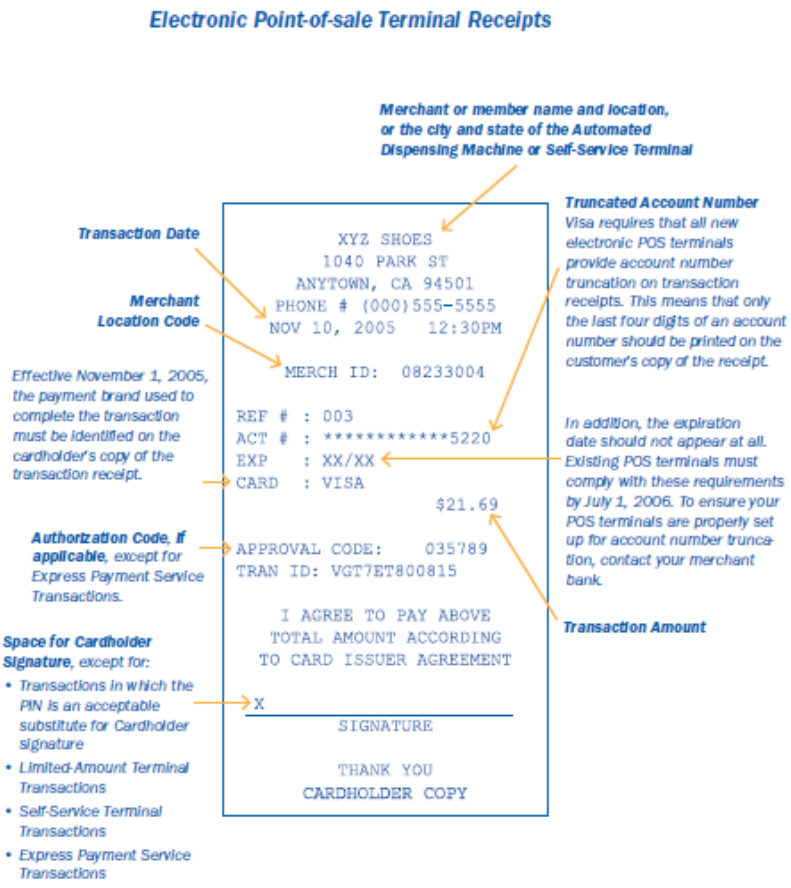
Cette section porte sur les différents éléments associés aux reçus électroniques : utilisation, transmission de données, sauvegarde et stockage et renseignements obligatoires.

9.3.1 EXEMPLES DE REÇUS

Les reçus électroniques varient selon le marchand, l'EJP, le réseau de paiement et même le fournisseur de porte-monnaie. Cette section porte sur la forme et la structure des reçus électroniques.

9.3.2 NORMES ACTUELLES DE VISA RELATIVEMENT AUX REÇUS IMPRIMÉS

À titre d'exemple de reçu électronique, l'image ci-dessous illustre les exigences de Visa à l'égard de tous les reçus de transaction générés à partir de TPV :



[10]

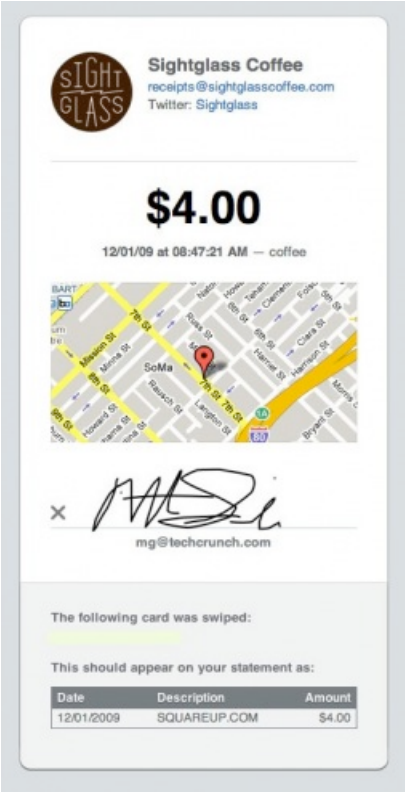
Visa exige que les renseignements ci-dessous figurent sur les reçus électroniques :

- Nom du marchand
- établissement du marchand (texte);
- code d'établissement du marchand;
- numéro de compte tronqué;
- montant de la transaction;
- date de la transaction;
- code d'autorisation (s'il y a lieu);
- espace pour la signature du titulaire du compte (utilisateur final);

9.3.3 NORMES ACTUELLES DE SQUARE RELATIVEMENT AUX REÇUS (MODE D'ACCEPTATION PAIR À PAIR)

L'entreprise Square offre un autre exemple de l'utilisation de reçus électroniques. Les exigences de Square à l'égard de tous les reçus de transaction générés à partir de TPV (y compris les terminaux activés par l'utilisateur final) sont présentées ci-dessous :

[10] Site Web de VISA



Les renseignements ci-dessous doivent figurer sur les reçus de Square :

- Nom du marchand
- établissement du marchand (texte);
- établissement du marchand (carte);
- courriel et compte Twitter du marchand;
- description de la transaction;
- montant de la transaction;
- date et heure de la transaction;
- espace pour la signature du titulaire du compte (utilisateur final);
- courriel du titulaire du compte (utilisateur final).

9.3.4 LIGNES DIRECTRICES RELATIVES AUX REÇUS ÉLECTRONIQUES

Avantages et désavantages des reçus électroniques : les reçus électroniques comportent des avantages et des désavantages. Le présent document n'impose pas l'utilisation de reçus électroniques; cependant, les intervenants devraient passer en revue leurs ententes pour comprendre leurs propres exigences en matière de reçus, et ils doivent déterminer si les reçus électroniques leur conviennent.

Champs de données : compte tenu de ces exemples et d'autres recherches, si un marchand choisit de délivrer des reçus électroniques, on lui suggère d'inclure les renseignements ci-dessous :

Champs obligatoires	Description
Nom du marchand	Nom du marchand et information relative au contrat. Ces renseignements permettent d'identifier le marchand.
Établissement du marchand	Adresse permettant d'identifier le marchand.
Numéro ou code de référence	Numéro de référence de la transaction : ce renseignement permet à l'utilisateur final de repérer la transaction et il est utilisé dans le cadre de transactions de remise d'achat.
Numéro ou code d'autorisation	Code d'autorisation bancaire utilisé à des fins de vérification et de suivi.
Montant	Montant de la transaction : ce renseignement est utilisé à des fins de vérification et de rapprochement avec le relevé correspondant, et il sert également de preuve d'achat.
Statut	Résumé de toute mesure devant être prise par le marchand.
Date et heure	Date et heure auxquelles la transaction a été effectuée.
Numéro de carte (tronqué; quatre derniers chiffres)	Le numéro de carte est tronqué pour des raisons de sécurité, mais les quatre derniers chiffres sont indiqués à des fins de suivi.
Numéro de téléphone (tronqué)	Le numéro de téléphone est tronqué pour des raisons de sécurité, mais il est partiellement indiqué à des fins de suivi.
Numéro de carte de fidélité	Numéro de la carte relative au programme de fidélisation.
Numéro de coupon	Numéro de coupon ou code à barres.

Méthodes de transmission : par ailleurs, il est recommandé que les reçus électroniques soient transmis selon les méthodes suivantes :

Méthode de transmission	Description
Courriel	Courriel dans un format pouvant être lu à l'aide de l'appareil mobile.
Texto	Texto envoyé au numéro de cellulaire lié au compte.
Radiofréquence	Le reçu électronique est envoyé à l'utilisateur final par radiofréquence, au moyen du réseau mobile. Il contient de l'information permettant de l'associer au marchand pertinent.

Méthode de transmission	Description
NFC	Le reçu est transmis au PDV par NFC. L'utilisateur final doit effleurer le lecteur de son appareil pour obtenir le reçu.

Format des données : dans le cas des reçus envoyés par texto, radiofréquence ou NFC, il est recommandé qu'ils soient transmis en format texte. Dans le cas des reçus envoyés par courriel, il est recommandé qu'ils soient transmis en format texte ou pdf.

Format des données	Description	Format texte (.txt)/(.csv)	Texte non formaté
PDF (.pdf)	Texte formaté et images		

9.4 TRANSACTIONS DE REMISE D'ACHAT EFFECTUÉES À L'AIDE D'UN APPAREIL MOBILE

Une transaction de remise d'achat vise la présentation pour acceptation des justificatifs de paiement liés à une remise de biens ou de services. L'utilisation d'un porte-monnaie mobile pour traiter une transaction de remise d'achat offrira à l'utilisateur final une expérience unique.

Cette section porte sur les normes et les lignes directrices liées aux transactions de remise d'achat. On y aborde notamment les exigences en matière d'expérience utilisateur à l'égard des remises d'achat, les exigences liées aux MVC à l'égard des remises d'achat, ainsi que la présentation pour acceptation de reçus électroniques dans le cadre de ces transactions.

9.4.1 REÇUS ÉLECTRONIQUES ET TRANSACTIONS DE REMISE D'ACHAT

Habituellement, les processus de remise d'achat sont déclenchés en présentant le reçu imprimé auprès du marchand. Ce dernier utilise alors les renseignements figurant sur le reçu pour retrouver la transaction dans le système PDV. Or, à mesure que les paiements mobiles NFC deviendront plus populaires, les utilisateurs finaux présenteront de plus en plus de reçus électroniques pour entamer le processus de remise d'achat. Les reçus électroniques seront vraisemblablement présentés de trois façons :

- **Mode visuel :** l'utilisateur final extrait le reçu du porte-monnaie mobile et le présente au marchand. Ce dernier peut soit numériser un code à barres à partir du reçu, soit saisir manuellement les renseignements qui y figurent.
- **Mode électronique :** l'utilisateur final envoie le reçu au marchand par voie électronique (par radiofréquence) au moyen de données de routage fournies par le marchand ou inscrites sur le reçu sous forme de code.
- **Par NFC :** le reçu est transmis au PDV par NFC. L'utilisateur final effleure le lecteur de son appareil pour transmettre le reçu électronique et entamer le processus de remise d'achat.

Dans le cas de remises d'achat, la norme proposée consiste à faire en sorte que l'utilisateur final et le marchand aient la possibilité d'accepter les reçus électroniques soit selon le mode visuel, soit selon le mode électronique.

9.4.2 PROCESSUS DE REMISE D'ACHAT

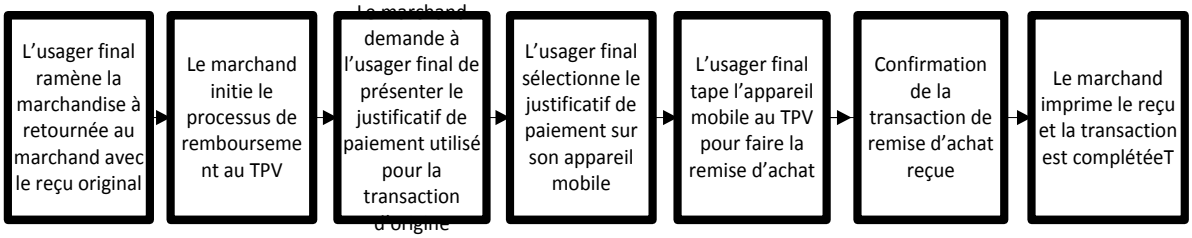
Le processus de remise (le contraire d'une transaction de paiement, qui entraîne un crédit porté au compte) doit respecter les définitions des réseaux de paiement. **[43]**. Ainsi, les transactions de remise

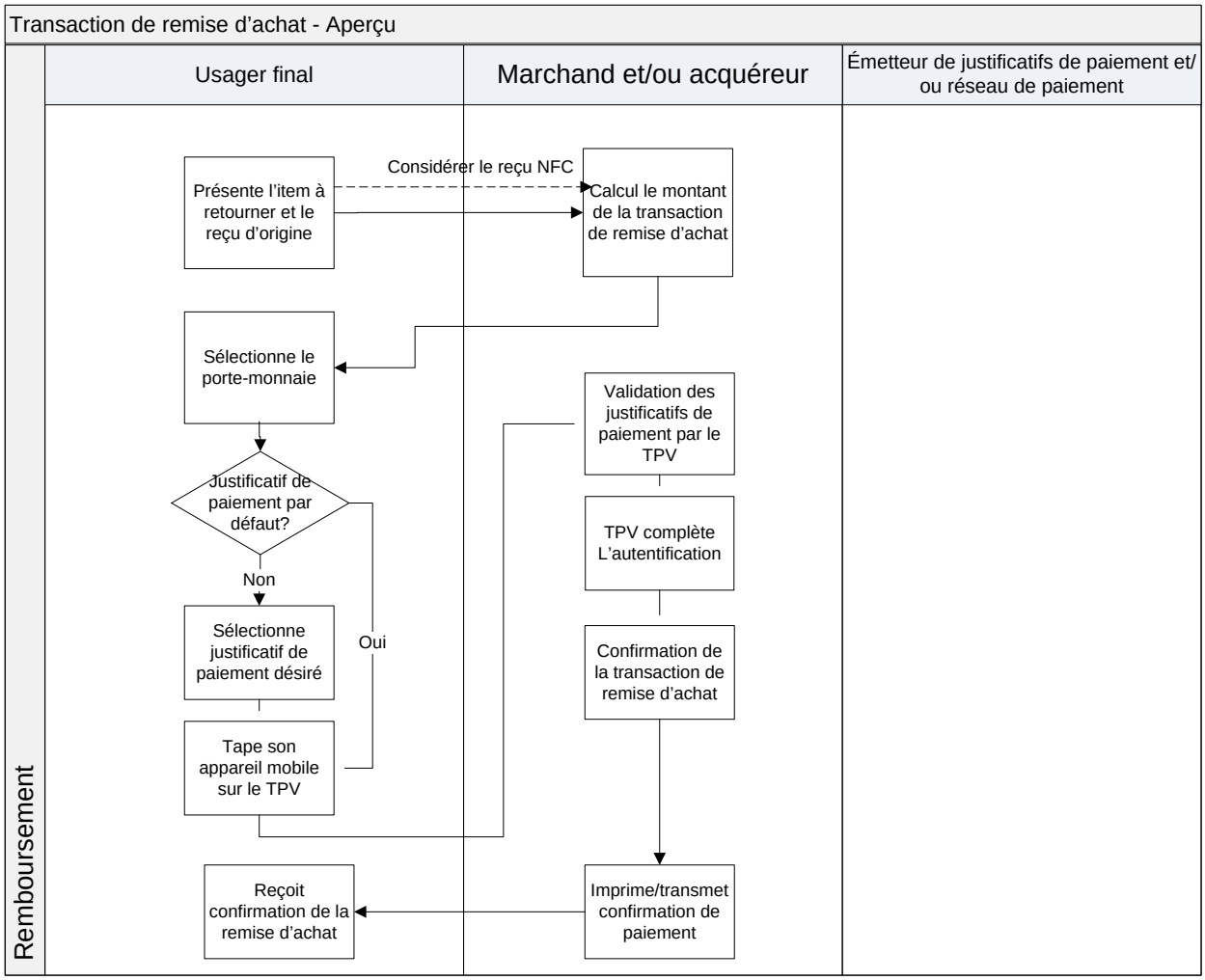
d'achat effectuées par NFC n'exigent pas systématiquement l'application d'une MVC (p. ex., signature ou mot de passe) à moins que les réseaux de paiement l'exigent.

Pour en savoir plus sur les autres méthodes de traitement de transactions de remise d'achat ayant été évaluées, veuillez vous reporter à l'annexe.

9.4.3 PROCESSUS DE REMISE D'ACHAT

Ci-après la démarche adoptée pour le traitement des transactions de remise d'achat effectuées par NFC au Canada.





9.5 TRAITEMENT DES TRANSACTIONS – RÉSUMÉ

La section Traitement des transactions résume les principales étapes du traitement des transactions de paiement mobile NFC. Elle donne un aperçu du traitement des paiements, de la MVC relative aux paiements de valeur élevée ou à risque élevé, des lignes directrices à l'égard des reçus électroniques et des remises d'achat effectuées à l'aide d'un appareil mobile. Les normes de la présente section sont conformes aux règles existantes et aux lignes directrices publiées par les réseaux de paiement. En s'harmonisant avec la structure existante, ces normes permettront de réduire au minimum les répercussions sur les utilisateurs finaux, les marchands et les réseaux de paiement.

9.6 ÉNONCÉS NORMALISÉS

Numéro	Énoncé	Section
36	Les transactions utilitaires ne doivent pas dépasser les limites établies à l'égard des transactions de valeur élevée ou à risque élevé, selon les définitions des réseaux de paiement.	9.1 Transactions utilitaires effectuées à l'aide d'un appareil mobile
37	Une transaction utilitaire doit respecter les lignes directrices existantes des réseaux de paiement à l'égard des paiements sans contact; sauf si les règles de sécurité l'exigent (p. ex., un compteur de transactions), la transaction utilitaire ne doit pas exiger plus qu'un simple « tapez et partez » pour la réalisation d'un paiement et elle ne doit pas être assujettie à une MVC supplémentaire.	9.1 Transactions utilitaires effectuées à l'aide d'un appareil mobile
38	L'EJP et/ou les réseaux de paiement définissent les transactions de valeur élevée ou à risque élevé. L'utilisateur final doit approuver les transactions de valeur élevée ou à risque élevé en appliquant une MVC.	9.2 Transactions de valeur élevée ou à risque élevé effectuées à l'aide d'appareils mobiles
39	Une fois qu'elles sont jugées acceptables par les réseaux de paiement, les transactions de valeur élevée ou à risque élevé doivent être approuvées à l'aide de la MVC dénommée « tapez et confirmez » (une première tape de l'écran de l'appareil, suivie de la saisie du mot de passe, puis d'une deuxième tape).	9.2 Transactions de valeur élevée ou à risque élevé effectuées à l'aide d'appareils mobiles
40	La méthode « tapez et confirmez » est la seule méthode de vérification de cartes approuvée; elle doit être utilisée dès qu'une transaction est jugée acceptable par un réseau de paiement.	9.2.2 Aperçu des différentes MVC
41	La MVC standard au Canada relativement aux paiements de valeur élevée ou à risque élevé est la méthode « tapez et confirmez » (méthode requérant deux tapes).	9.2.2 Aperçu des différentes MVC

Numéro	Énoncé	Section
42	La délivrance du reçu est la dernière étape du traitement d'une transaction mobile NFC. Il n'existe pas de normes particulières quant à la délivrance de reçus relativement aux paiements mobiles. La délivrance des reçus doit être conforme aux lignes directrices en vigueur.	9.3 Reçus électroniques
43	Le processus de remise (le contraire d'une transaction de paiement, qui entraîne un crédit porté au compte) doit respecter les définitions des réseaux de paiement.	9.4.2 Processus de remise d'achat

10 HABILITATION ET GESTION DU CYCLE DE VIE

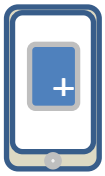
La section Habilitation et gestion du cycle de vie établit un cadre de référence commun relativement à l'installation d'une application porte-monnaie, d'applications de paiement et des justificatifs de paiement de l'utilisateur final, ainsi qu'à la mise à jour de ces derniers pendant que l'utilisateur demeure actif. Les activités décrites dans cette section nécessitent des efforts de coordination entre plusieurs participants à l'écosystème (EJP, ERM et GSC, notamment). Les normes qui y sont présentées tiennent compte à la fois de l'expérience utilisateur et des relations de base devant être établies pour créer un écosystème de paiements mobiles. Cette section suppose que les participants à l'écosystème coordonnent et approuvent entre eux les activités qu'ils entreprennent relativement à l'Habilitation et gestion du cycle de vie.

La section Habilitation et gestion du cycle de vie est divisée dans les sous-sections suivantes :

- Relations commerciales entre participants à l'écosystème
- Gestion des clés
- Installation du porte-monnaie mobile
- Installation de l'application de paiement et des justificatifs de paiement
- Activités de soutien associées à l'utilisateur final
- Annulation du service

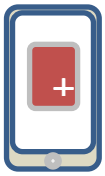
L'habilitation constitue un prérequis en vue de l'utilisation d'un appareil mobile pour effectuer des paiements NFC; les activités d'habilitation doivent être exécutées avant toute activité liée aux transactions.

***L'usager final** installe le porte-monnaie et l'application de paiement.*



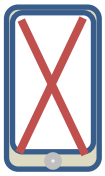
***L'usager final** (ou Émetteur de justificatifs) relie les justificatifs au porte-monnaie*

***L'usager final** utilise son téléphone mobile pour faire des transactions d'achat et de remboursement NFC.*



***L'usager final** ajoute les informations des programmes de fidélisation à son téléphone mobile.*

L'usager final** demande et reçoit des services **de l'opérateur mobile, le l'émetteur de justificatifs et fournisseur de programmes de fidélisation



À la fin du cycle de vie le compte de l'usager final est fermé et les services annulés.

10.1 RELATIONS COMMERCIALES ENTRE PARTICIPANTS À L'ÉCOSYSTÈME

La section Habilitation et gestion du cycle de vie repose sur le principe selon lequel les interactions entre les participants à l'écosystème (réseau de paiement et EJP, fournisseur de porte-monnaie et EJP, EJP et GSC, EJP et ERM, etc.) doivent être précédées d'étapes visant à établir des relations commerciales contractuelles **[44]**.

Les relations commerciales peuvent être établies directement ou par l'entremise d'un organisme comme une autorité de contrôle (AC).

10.2 GESTION DES CLÉS

Le présent document, tout comme le processus d'approvisionnement prévu, repose sur les protocoles de communication ainsi que les rôles et responsabilités établis par GlobalPlatform. Ce document ne

tient pas compte de tous les processus de gestion des clés comme ceux entre le réseau de paiement et l'EJP. En plus des lignes directrices énumérées dans cette section, les processus de gestion des clés établis par les réseaux de paiement doivent être respectés **[45]**.

Comme il est décrit à la section 6.8, toutes les activités de messagerie doivent être exécutées conformément aux lignes directrices pertinentes tirées du document GPS_Messaging_Specification_for_Mobile_NFC_Services-v1.0 **[46]**.

Les intervenants qui appliquent les normes contenues dans ce document acceptent de n'utiliser que le mode de délégation ou le mode bimodal, tels que définis par GlobalPlatform, dans le cadre de toutes les activités associées à l'habilitation et à la gestion du cycle de vie **[47]**. Cette norme est fondamentale à l'égard de toutes les activités liées à l'habilitation et à la gestion du cycle de vie, car le mode de délégation et le mode bimodal permettent aux EJP d'assurer la sécurité des justificatifs de paiement; par conséquent, ils contribuent à la sûreté et à la sécurité de l'écosystème.

Par ailleurs, avant l'application du processus d'approvisionnement, il faut établir un processus de gestion des clés. Le processus de gestion des clés vise à établir des protocoles de gestion des données sécurisées entre le GSC de l'émetteur de justificatifs et le GSC du gestionnaire de domaine sécurisé.

10.2.1 GESTION DES CLÉS SÉCURISÉES

La présente section porte sur l'échange de clés entre l'EJP et son GSC. Ce processus est nécessaire afin de faciliter les étapes d'installation de l'application, d'installation des justificatifs de paiement et d'association, énumérées plus haut.

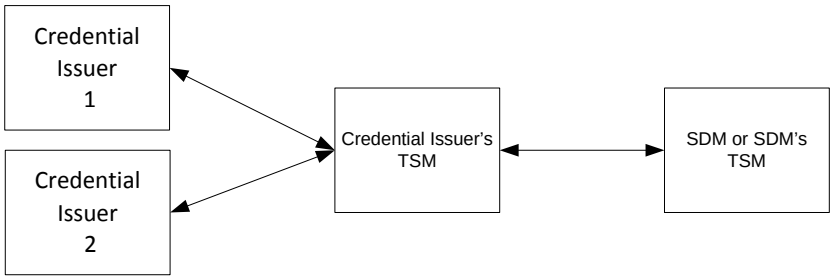
S'il s'agit d'un porte-monnaie exclusif, un processus de gestion des clés sécurisées doit être établi entre l'EJP, son GSC, le GDS et son GSC. **[48]**. S'il s'agit d'un porte-monnaie ouvert, des protocoles doivent être établis de manière à ce que les clés soient gérées par plusieurs intervenants **[49]**. Cette tâche peut être accomplie en ajoutant un GSC tiers, un GSC agissant à titre de plaque tournante ou une AC.

Dans le processus, l'EJP, son GSC et le GSC du GDS, le GDS et le GSC de l'EJP et le GSC du GDS doivent avoir établi une relation commerciale, directement ou indirectement. **[50]**

Les clés pourront être échangées une fois cette relation établie. L'échange de clés permet la transmission sûre des données nécessaires pour assurer l'envoi sécurisé des justificatifs à l'application de paiement. Cette interaction ne concerne que l'EJP et son GSC. L'utilisateur final ne participe pas à ce processus. Des processus supplémentaires de gestion des clés (p. ex., l'échange de clés entre le FMO et l'ERM ou son GSC) sont exclus du rayon d'action de ce document.

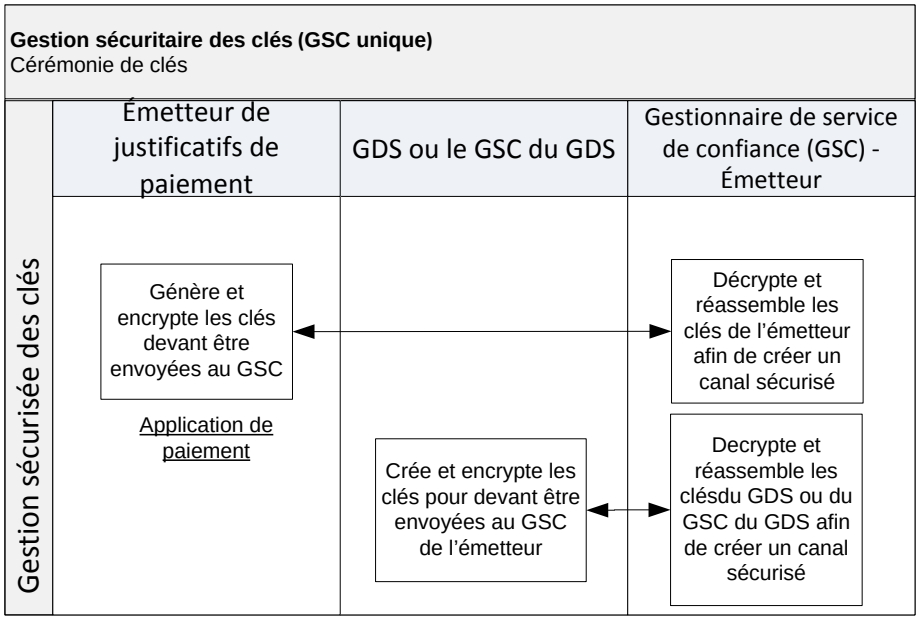
10.2.2 INSTALLATEUR UNIQUE DE JUSTIFICATIFS DE PAIEMENT

L'image suivante présente les relations dans un modèle axé sur un GSC unique. Un tel modèle est utilisé lorsque chaque participant à l'écosystème des paiements mobiles NFC établit des relations commerciales sur une base individuelle.



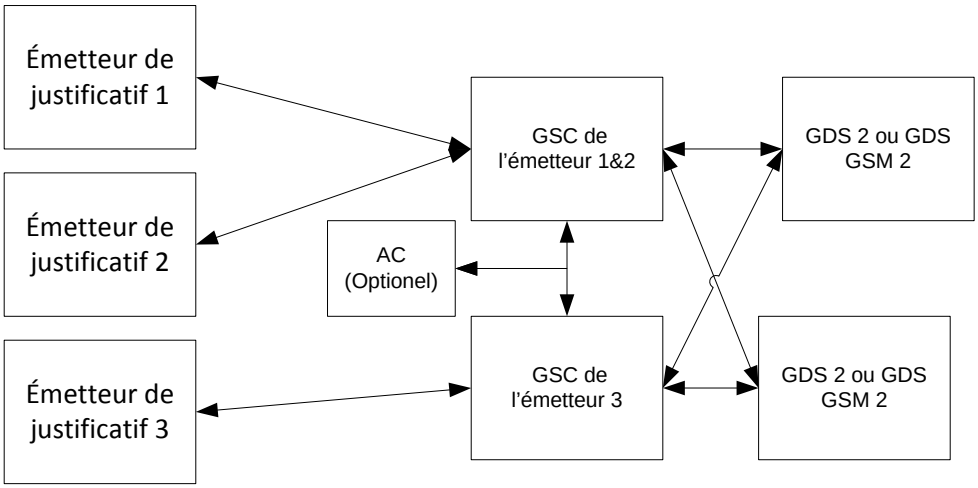
Ce processus d'installation des justificatifs visant un seul EJP est déclenché lorsque l'EJP établit une nouvelle relation avec un GSC (cette relation facilite l'approvisionnement et la gestion initiaux des clés sécurisées). Le GSC de l'EJP travaille avec l'intervenant chargé du traitement des paiements de l'EJP (p. ex., TSYS) en vue de la création d'un ensemble de clés chiffrées. Les clés sont ensuite envoyées au GSC de l'EJP sous forme d'un ensemble de fichiers de données chiffrées. Le même processus est appliqué par le GDS et le GSC du GDS.

L'échange de clés doit être réalisé conformément aux lignes directrices de GlobalPlatform **[51]**. Une fois ce processus terminé, l'échange de clés permettra de mettre en place une voie de communication protégée dédiée à la transmission de données entre l'EJP, son GSC et le GSC du GDS. Cette voie de communication protégée constitue une exigence minimale et doit être en place afin que puissent être exécutées des activités d'installation par radiofréquences. **[52]** Des processus d'installation supplémentaires peuvent également être utilisés une fois l'exigence minimale satisfaite.



10.2.3 INSTALLATEURS MULTIPLES DE JUSTIFICATIFS DE PAIEMENT (RÉSEAU EN ÉTOILE)

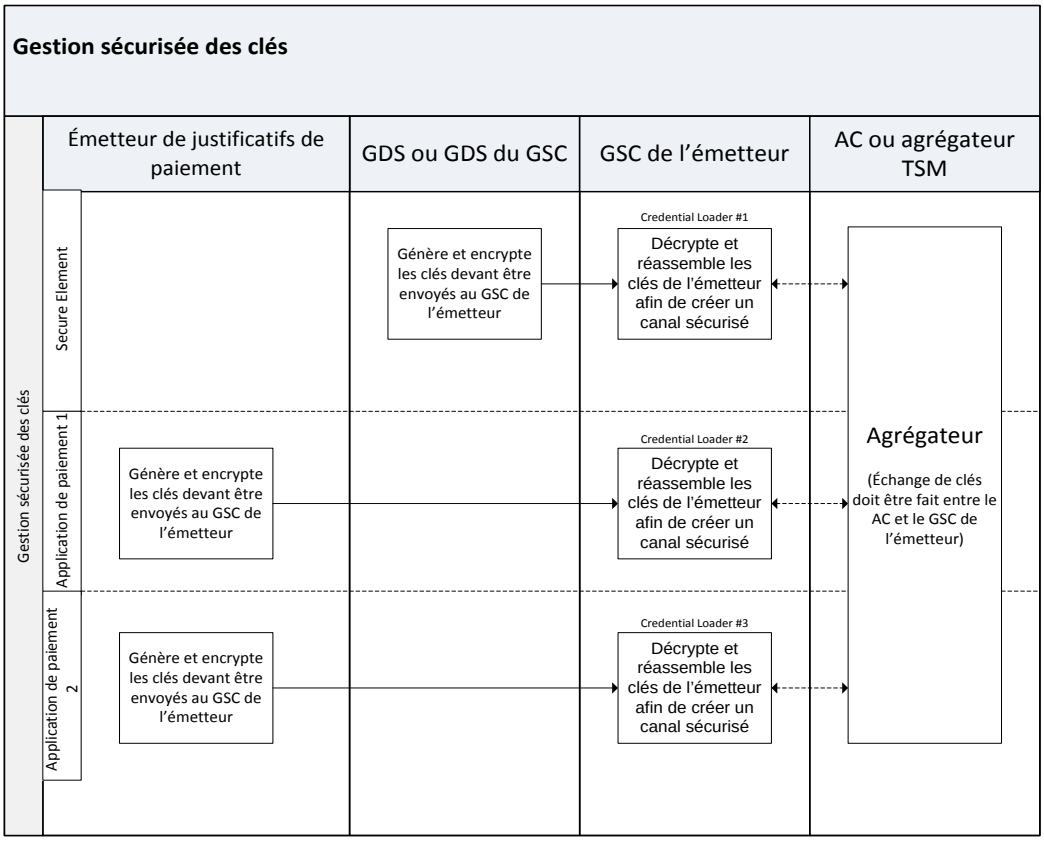
Le scénario ci-dessous, plus complexe, présente les relations dans un modèle axé sur plusieurs GSC. Cette section décrit un scénario dans lequel un ou plusieurs GSC d'EJP jouent le rôle de plaque tournante à l'égard de l'industrie. Ce modèle pourrait être utilisé pour regrouper plusieurs EJP dans une seule application porte-monnaie.



Dans ce modèle, l'EJP établit une relation avec son GSC pour échanger des clés et s'assurer qu'il existe un moyen sécurisé de transmission de données entre les participants à l'écosystème.

Dans un modèle basé sur plusieurs installateurs de justificatifs, un groupe d'installateurs établit une relation commerciale autorisant la transmission sécurisée de données entre les participants. Ensuite, les GSC des EJP échangent des clés entre eux pour s'assurer de mettre en place des voies de communication protégées. Cet échange de clés doit avoir lieu pour permettre l'installation de justificatifs de paiement dans un porte-monnaie ouvert ou collectif **[53]**

Dans ce modèle, tous les intervenants doivent échanger les clés conformément aux lignes directrices de GlobalPlatform. L'AC ou la plaque tournante de GSC des EJP doit élaborer et diffuser des protocoles destinés à faciliter ces interactions **[54]**

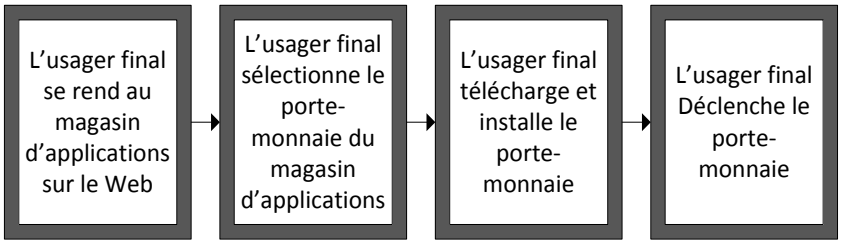


10.3 INSTALLATION DU PORTE-MONNAIE MOBILE

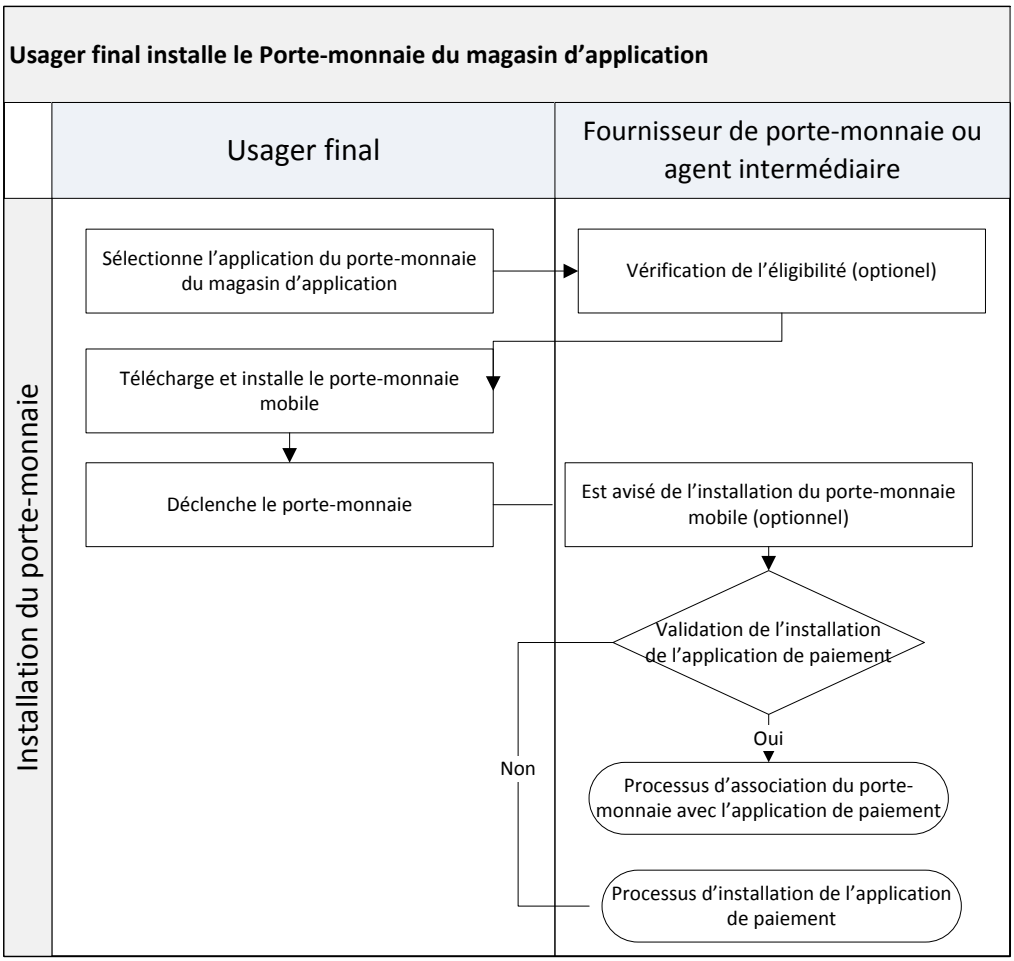
Du point de vue de l'utilisateur final, l'habilitation commence lorsqu'il obtient l'accès à l'application porte-monnaie. Pour entamer le processus d'habilitation des paiements mobiles, le porte-monnaie mobile doit être installé dans l'appareil de l'utilisateur final. Dans le cadre du présent document, les deux méthodes d'installation de l'application porte-monnaie ci-dessous sont prises en considération :

- **Installation déclenchée par l'utilisateur final :** l'utilisateur final installe le porte-monnaie mobile à partir d'un magasin d'applications ou d'un site Web.
- **Application préinstallée :** l'EJP, l'ERM, le fournisseur de porte-monnaie ou un autre intervenant préinstalle le porte-monnaie mobile dans l'appareil avant que l'utilisateur final y accède.

On peut également avoir recours à la préinstallation au lieu de l'installation déclenchée par le porte-monnaie mobile. Le processus de préinstallation n'est pas décrit dans ce document. Cette section décrit l'installation déclenchée par l'utilisateur final, qui visite d'abord un magasin d'applications ou un site Web. Cette étape peut être franchie avant ou après l'installation de l'application et des justificatifs de paiement dans l'appareil mobile.



Le processus ci-dessous illustre l'installation déclenchée par l'utilisateur final. Il existe d'autres moyens d'installation : le porte-monnaie mobile peut notamment être installé dans l'appareil par l'EJP ou l'ERM.



10.3.1 VÉRIFICATION DE L'ADMISSIBILITÉ EN VUE DE LA PRÉINSTALLATION

Une vérification d'admissibilité doit être réalisée à l'égard de certains magasins d'applications, sites Web et fournisseurs de services avant l'installation d'un porte-monnaie mobile. Cette vérification vise à s'assurer que le matériel de l'utilisateur final lui permettra d'effectuer des paiements mobiles NFC, c'est-à-dire que l'appareil peut envoyer et recevoir des radio signaux NFC.

Si la vérification de l'admissibilité n'est pas obligatoire, elle est fortement encouragée. Le recours à une telle vérification permettra d'atténuer la confusion des utilisateurs finaux, de réduire au minimum les coûts de dépannage liés à l'installation du porte-monnaie et d'éviter des problèmes de sécurité potentiels (p. ex., hameçonnage).

10.4 INSTALLATION DE L'APPLICATION ET DES JUSTIFICATIFS DE PAIEMENT

L'installation de l'application de paiement et l'installation de l'application porte-monnaie désignent deux processus distincts. L'application et les justificatifs de paiement sont personnalisés par l'EJP et contiennent des données chiffrées très sensibles.

Cette section porte sur plusieurs processus secondaires liés à l'installation de l'application et des justificatifs de paiement :

- Demande d'accès de l'utilisateur final à l'application et aux justificatifs de paiement
- Vérification et validation des renseignements relatifs à l'utilisateur final
- Installation de l'application de paiement
- Association de l'application de paiement au porte-monnaie mobile (au moyen d'une application parapluie)
- Installation de justificatifs de paiement au moyen de radiofréquences

10.4.1 DEMANDE D'ACCÈS DE L'UTILISATEUR FINAL À L'APPLICATION DE PAIEMENT

À titre d'exigence minimale, l'utilisateur final doit être en mesure de demander l'installation de l'application de paiement à l'aide de son porte-monnaie mobile **[55]**. Outre cette méthode, la demande d'installation de l'application de paiement peut être présentée en ligne, dans une succursale bancaire, en appelant à un centre d'appels ou au moyen d'une application de services bancaires mobiles. Quelle que soit la méthode utilisée pour télécharger l'application et les justificatifs de paiement, l'utilisateur final doit donner son consentement avant l'installation **[56]**.

Comme il est expliqué ci-dessus, la demande d'installation peut être présentée de plusieurs façons :

- demande présentée par l'utilisateur final au moyen du porte-monnaie mobile;
- demande présentée par l'utilisateur final par un autre moyen;
- demande présentée par l'EJP.

Dans le cas des demandes présentées à l'aide du porte-monnaie mobile, ce dernier doit afficher le nom de l'EJP dont les justificatifs de paiement vont être installés dans le porte-monnaie **[57]**

Après la présentation de la demande d'installation de l'application et des justificatifs de paiement, mais avant l'installation comme telle, l'identité de l'utilisateur final doit être vérifiée (consultez la section suivante pour consulter les énoncés normalisés.)

10.4.2 VÉRIFICATION ET VALIDATION DES RENSEIGNEMENTS RELATIFS À L'UTILISATEUR FINAL

Avant l'installation de l'application et des justificatifs de paiement dans l'appareil mobile, l'identité de l'utilisateur final doit être validée **[58]**.

Le processus de vérification et de validation de l'identité différera en fonction de l'EJP. Ce dernier a la responsabilité de définir le processus de vérification et de validation de l'identité de l'utilisateur final

[59]. Le présent document ne décrit pas les exigences associées à ce processus. Parmi les éléments à prendre en considération, on retrouve la propriété de l'appareil mobile et l'autorisation de l'utilisateur final en vue de l'installation de justificatifs.

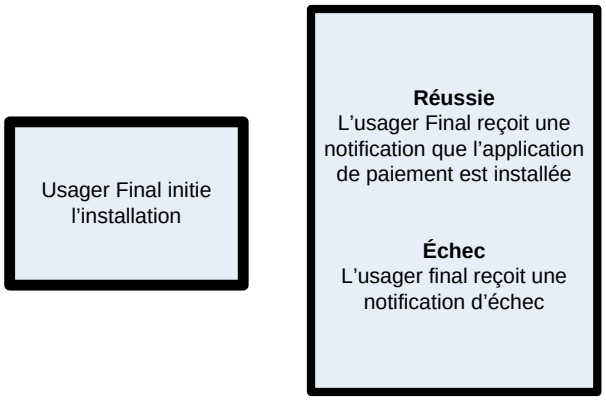
Les présentes normes autorisent le déclenchement du processus d'approvisionnement à l'aide du porte-monnaie. L'EJP demeure responsable de la validation de l'identité de l'utilisateur final, conformément à l'énoncé ci-dessus.

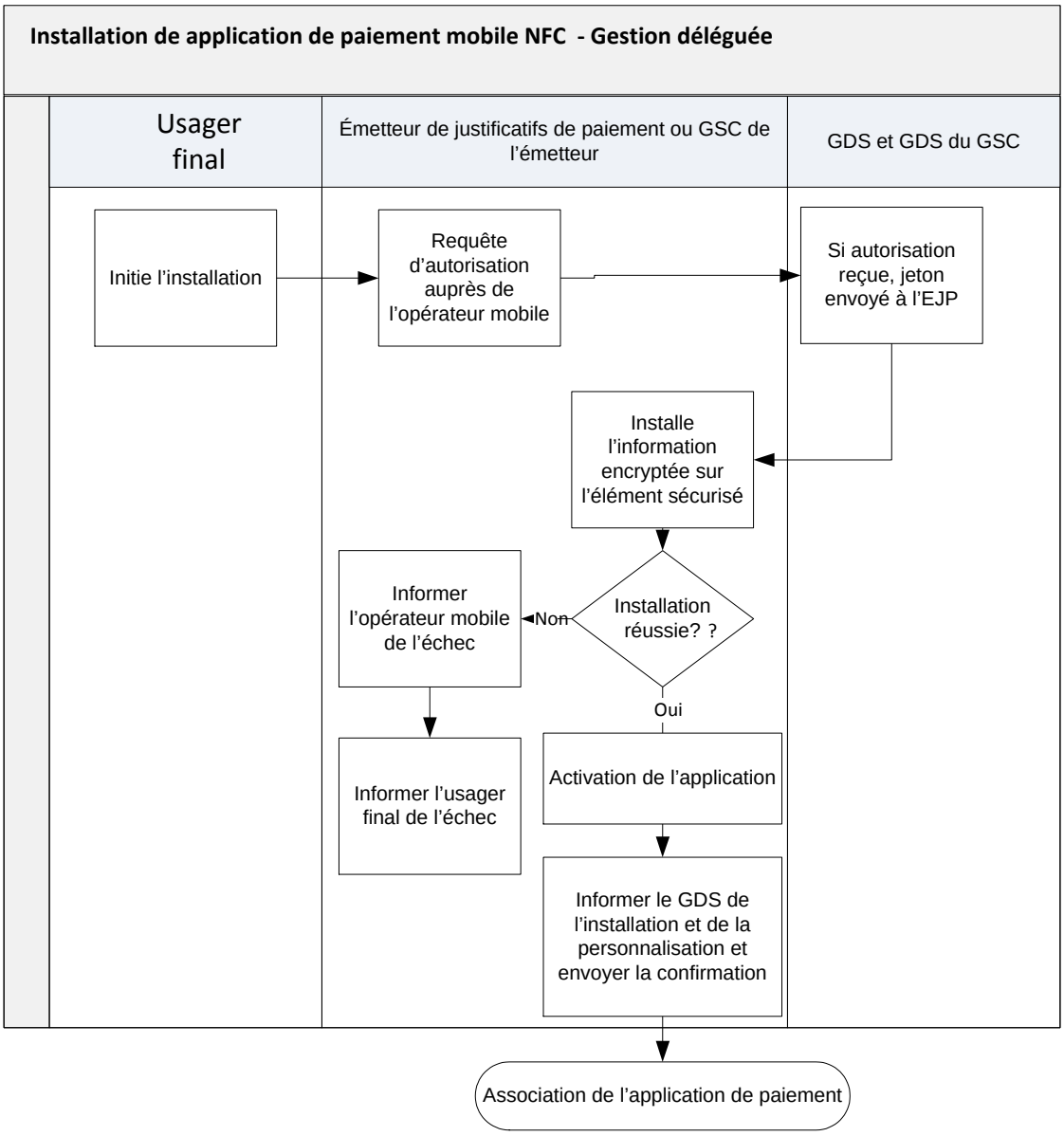
Après la vérification et la validation, l'EJP doit envoyer à l'utilisateur final un message décrivant la prochaine étape **[60]**. Si les renseignements relatifs à l'utilisateur final sont validés, l'étape suivante est celle de l'installation de l'application de paiement.

10.4.3 INSTALLATION DE L'APPLICATION DE PAIEMENT

Une fois l'identité de l'utilisateur final vérifiée et approuvée en vue de l'accès aux services de paiement mobile NFC, la prochaine étape est celle de l'installation, de la personnalisation et de l'activation du service dans l'appareil mobile de l'utilisateur final. Dans ce document, il est présumé que l'installation, la personnalisation et l'activation sont effectuées en même temps. Toutefois, cette étape peut aussi être exécutée avant l'installation d'une application porte-monnaie.

Dans le modèle ci-dessous, l'installation et l'activation des services de paiement mobile NFC ont été déléguées au GSC de l'EJP et au GSC du GDS. Pour que l'application et les justificatifs de paiement puissent être installés, tous les intervenants doivent établir une voie de communication protégée avec l'EJP et le GDS. **[61]** Une fois la voie de communication protégée établie, le GSC doit prendre en charge toutes les activités, y compris l'installation et l'activation des services de paiement mobile NFC dans l'appareil. **[62]**





Après l'installation de l'application de paiement, cette dernière doit être associée au porte-monnaie mobile et les justificatifs de paiement doivent être téléchargés avant que l'application puisse être utilisée pour effectuer un paiement (consultez la section Association de l'application de paiement au porte-monnaie mobile pour connaître les énoncés normalisés connexes).

10.4.4 ASSOCIATION DE L'APPLICATION DE PAIEMENT AU PORTE-MONNAIE MOBILE

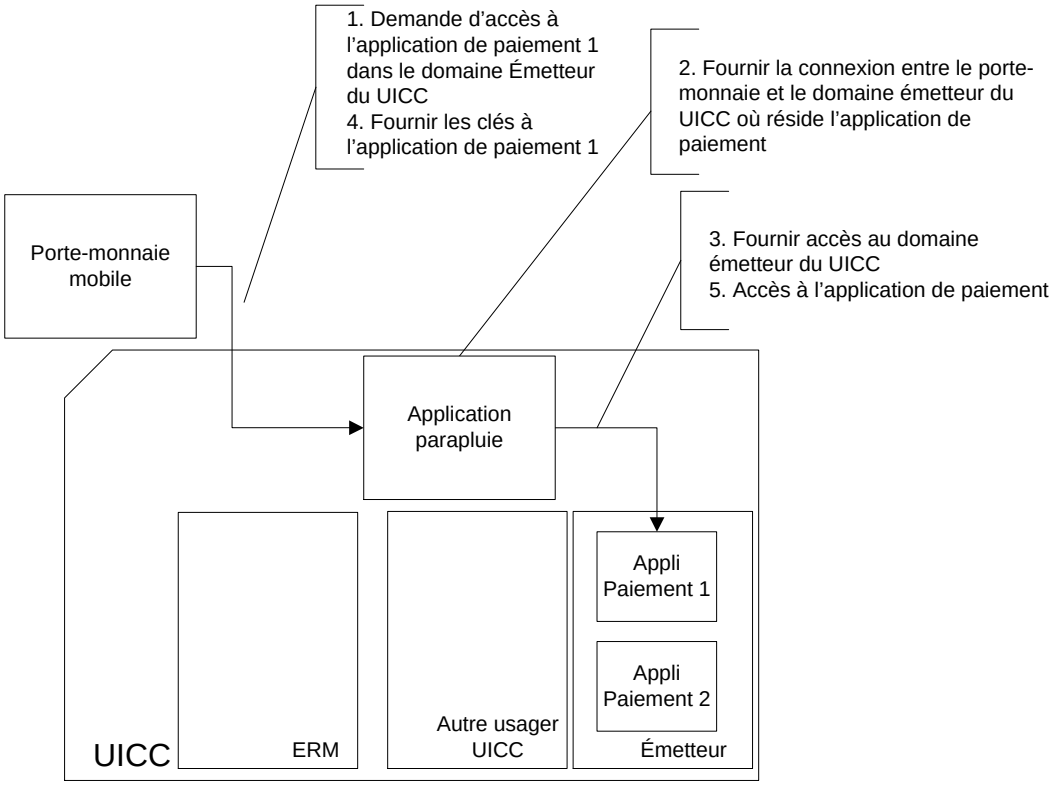
Le processus d'association met en cause un porte-monnaie mobile et une ou plusieurs applications de paiement. Le but de l'association est d'indiquer au porte-monnaie mobile à quel endroit de l'UICC ou de l'élément sécurisé intégré se trouvent les applications de paiement. L'association est nécessaire pour qu'un porte-monnaie mobile puisse accéder à une application de paiement. **[63]**

Le processus d'association diffère selon l'endroit où l'application de paiement est stockée.

10.4.5 ÉLÉMENT SÉCURISÉ DANS L'UICC

Afin qu'une application de paiement installée dans l'UICC puisse être utilisée pour effectuer un paiement, le porte-monnaie mobile et l'application de paiement doivent être soumis à un processus d'association Lorsque l'application de paiement est stockée dans l'UICC, le porte-monnaie se sert de l'application parapluie de l'UICC pour localiser l'application de paiement. L'application parapluie sert de répertoire de l'UICC et doit être fournie par le GDS. **[64]**

Pendant le processus d'association, le porte-monnaie mobile communique avec l'application parapluie pour déterminer où se trouve l'application de paiement. Ensuite, l'application parapluie informe le porte-monnaie de l'endroit où se trouve l'application de paiement et lui fournit un identificateur permettant de la repérer. Le GDS doit fournir la structure de l'identificateur. **[65]**.



Une fois que l'application porte-monnaie et l'application de paiement ont été soumises au processus d'association, l'application porte-monnaie communique avec l'application parapluie afin d'accéder aux justificatifs, à des fins de paiement et de maintenance.

10.4.6 ÉLÉMENT SÉCURISÉ INTÉGRÉ

De même, afin que des applications de paiement installées dans un élément sécurisé intégré puissent être utilisées pour effectuer un paiement, le porte-monnaie mobile et l'application de paiement doivent être soumis à un processus d'association.

Quand le porte-monnaie mobile fait partie du processus d'approvisionnement en justificatifs, c'est lui qui détermine l'endroit où est stockée l'application de paiement. Lorsque l'application et les justificatifs de paiement sont téléchargés avant l'installation du porte-monnaie ou avant l'association avec ce dernier, l'EJP ou son GSC détermine l'endroit où est stockée l'application de paiement.

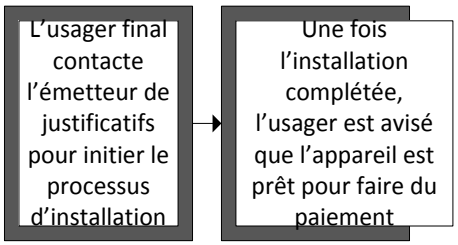
10.4.7 INSTALLATION DE JUSTIFICATIFS DE PAIEMENT AU MOYEN DE RADIOFRÉQUENCES

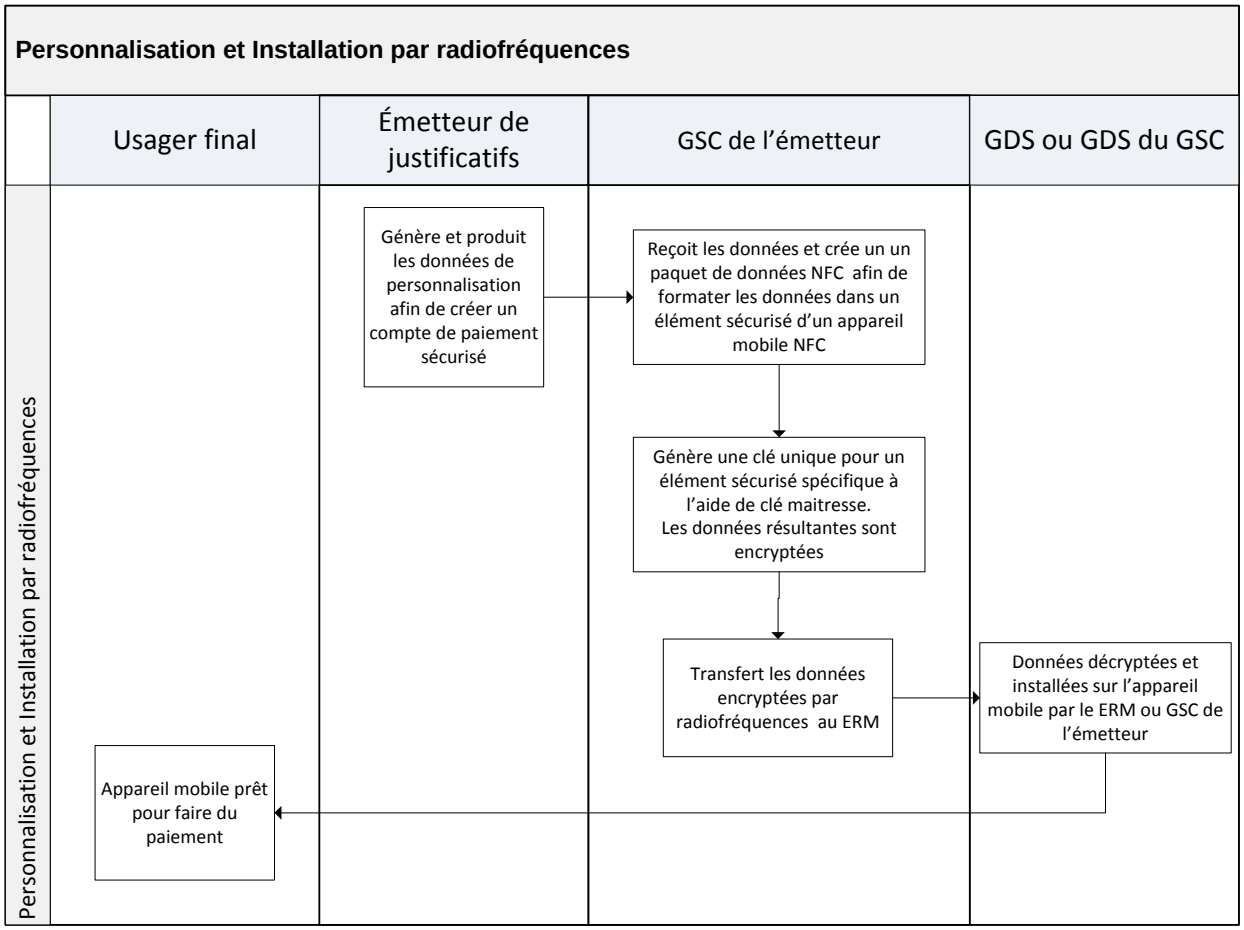
Même si les justificatifs de paiement peuvent être installés en même temps que l'application de paiement, ces deux éléments peuvent être installés séparément. Cette section porte sur l'installation de justificatifs dans l'application de paiement, au moyen de radiofréquences. Pour réaliser l'installation, le GSC de l'EJP et le GSC de l'ERM peuvent coordonner l'installation et la personnalisation de l'application de paiement dans l'appareil de l'utilisateur final.

Les justificatifs peuvent être préinstallés ou envoyés à un appareil mobile au moyen de radiofréquences. L'exemple ci-dessous illustre le processus d'installation et de personnalisation au moyen de radiofréquences. Les justificatifs de paiement sont stockés dans l'appareil mobile et doivent pouvoir être installés et mis à jour au moyen de radiofréquences. **[66]**

Dans le cadre du processus d'installation et de personnalisation par radiofréquences :

- l'EJP génère les justificatifs de paiement;
- le GSC de l'EJP est ensuite responsable de l'ensemble de fichiers de données chiffrées;
- l'ensemble de données chiffrées est alors installé dans un domaine sécurisé secondaire de l'UICC ou de l'élément sécurisé intégré.





Dès que le porte-monnaie, l'application et les justificatifs de paiement ont été installés et associés, l'appareil mobile peut être utilisé pour effectuer des paiements.

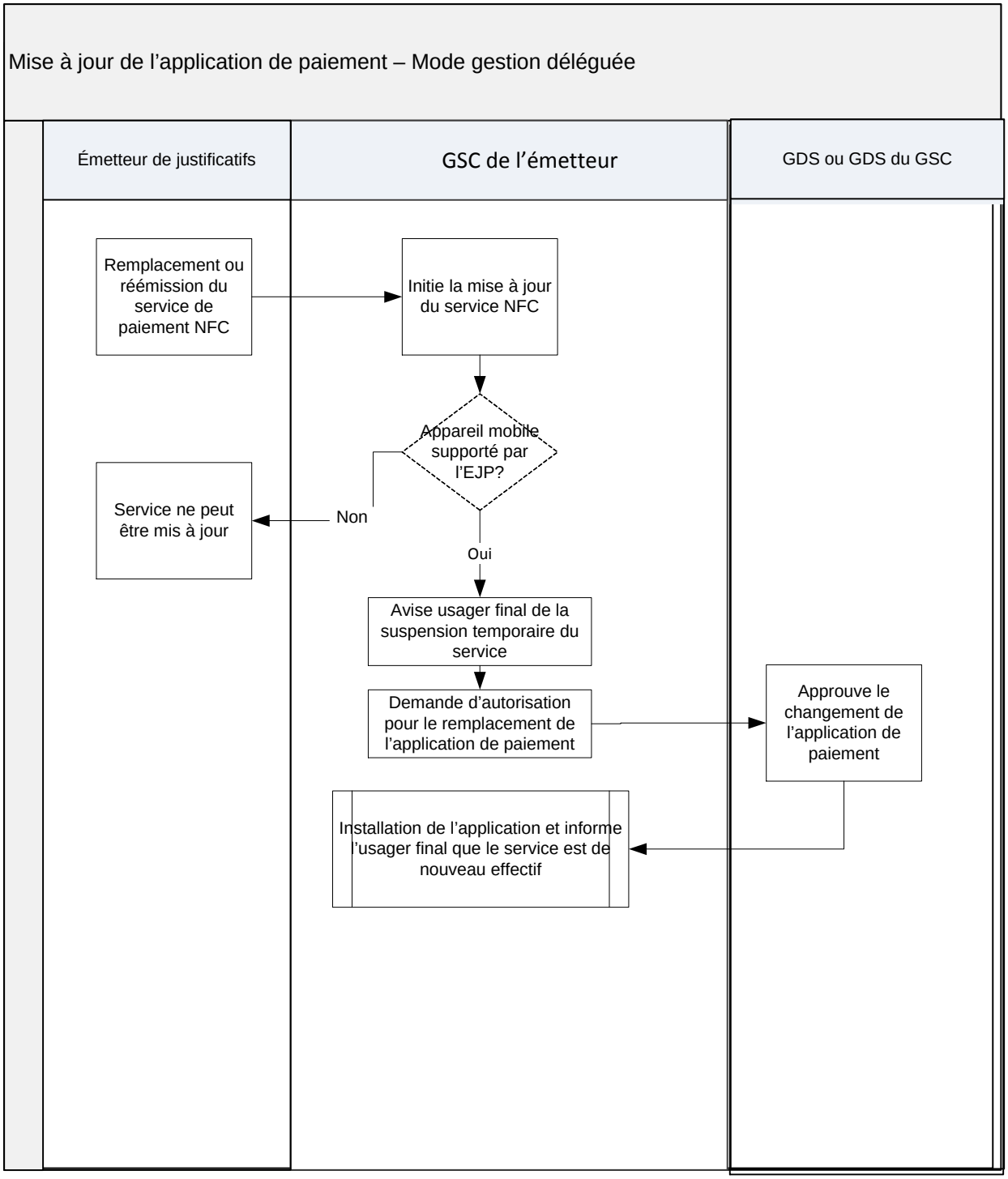
10.5 ACTIVITÉS DE MAINTENANCE ASSOCIÉES À L'UTILISATEUR FINAL

La présente section porte sur les événements importants pouvant survenir entre le moment où l'utilisateur final active les services de paiement mobile NFC et le moment où ces services sont désactivés. Cette section englobe les processus de maintenance ainsi que les autres activités liées à la gestion du cycle de vie. Ces activités visent à s'assurer que l'utilisateur final est en mesure d'utiliser son appareil mobile de façon continue pour effectuer des paiements mobiles NFC. Les éléments suivants sont abordés dans cette section :

- Mise à jour de l'application de paiement
- Mise à jour ou modification de l'élément sécurisé
- Changement d'appareil mobile
- Perte ou vol de l'appareil mobile
- Remplacement de l'appareil mobile

10.5.1 MISE À JOUR DE L'APPLICATION DE PAIEMENT

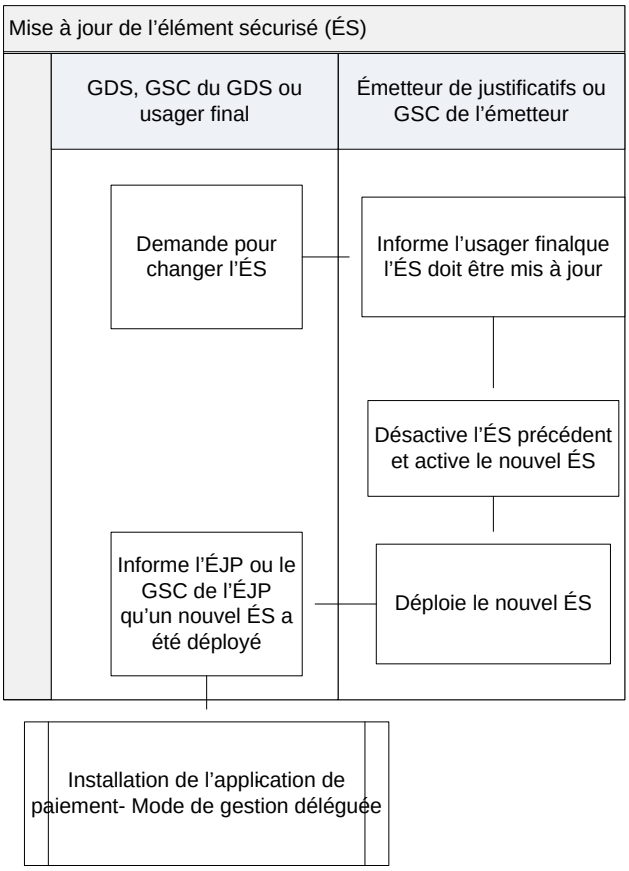
L'image ci-dessous illustre la façon dont l'EJP met à jour l'application de paiement d'utilisateurs existants de services de paiement mobile.



10.5.2 MISE À JOUR DE L'ÉLÉMENT SÉCURISÉ

Ce processus décrit la mise à jour de l'élément sécurisé, notamment à la suite d'une panne ou d'une insuffisance relative à sa mémoire. Ce processus peut être déclenché par l'utilisateur final ou par le GDS. Si l'élément sécurisé intégré tombe en panne, l'utilisateur final doit remplacer l'appareil mobile. Si l'élément sécurisé de l'UICC tombe en panne ou si sa mémoire fait défaut, l'UICC doit être mise à jour. Il

est recommandé que les parties intéressées établissent et documentent leurs responsabilités et les étapes de validation associées à la mise à jour de l'élément sécurisé.



Si le GDS (ou le GSC du GDS) demande la mise à jour de l'élément sécurisé, la partie intéressée doit communiquer avec le GSC de l'EJP pour réinstaller l'application de paiement après la mise à jour de l'élément sécurisé. **[67]** L'application de paiement doit également être personnalisée dans le cadre du processus d'installation de l'application de paiement (consultez plus haut les sections associées à ces étapes).

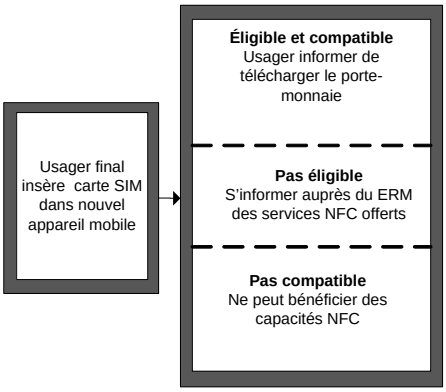
10.5.3 CHANGEMENT D'APPAREIL MOBILE

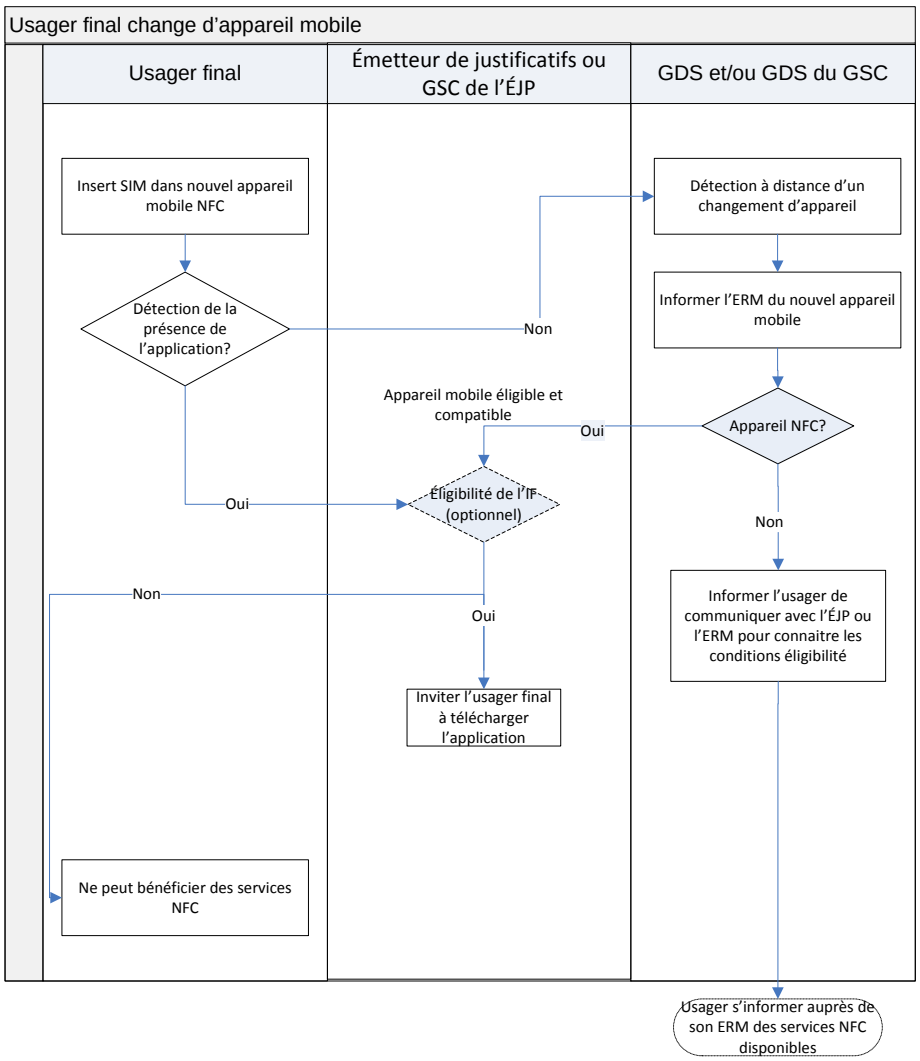
Ce processus décrit les étapes devant être franchies lorsque l'utilisateur final change d'appareil mobile.

Changement d'appareil mobile (élément sécurisé intégré) : si l'application de paiement mobile est stockée dans l'élément sécurisé intégré, l'utilisateur final doit appliquer de nouveau tout le processus d'installation du porte-monnaie mobile et de l'application de paiement (étapes de configuration d'un nouvel appareil). **[68]** Cependant, si l'application de paiement mobile est stockée dans l'UICC, l'utilisateur final doit suivre les étapes ci-dessous :

- transférer l'UICC de l'ancien au nouvel appareil;
- installer l'application porte-monnaie, vérifier l'identité de l'utilisateur final et associer le porte-monnaie et l'application de paiement.

Changement d'appareil mobile (élément sécurisé dans l'UICC) : si l'utilisateur final change d'appareil mobile ou ajoute un appareil secondaire, il doit effectuer la configuration initiale de nouveau, y compris la vérification de l'identité de l'utilisateur final et l'association du porte-monnaie mobile et des justificatifs de paiement. **[69]**

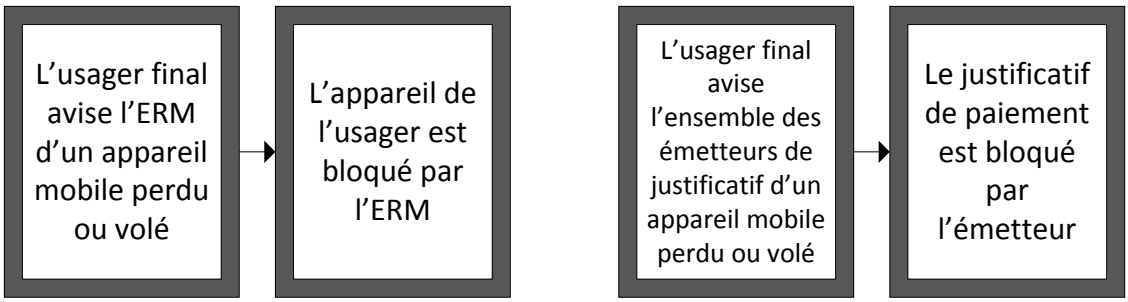


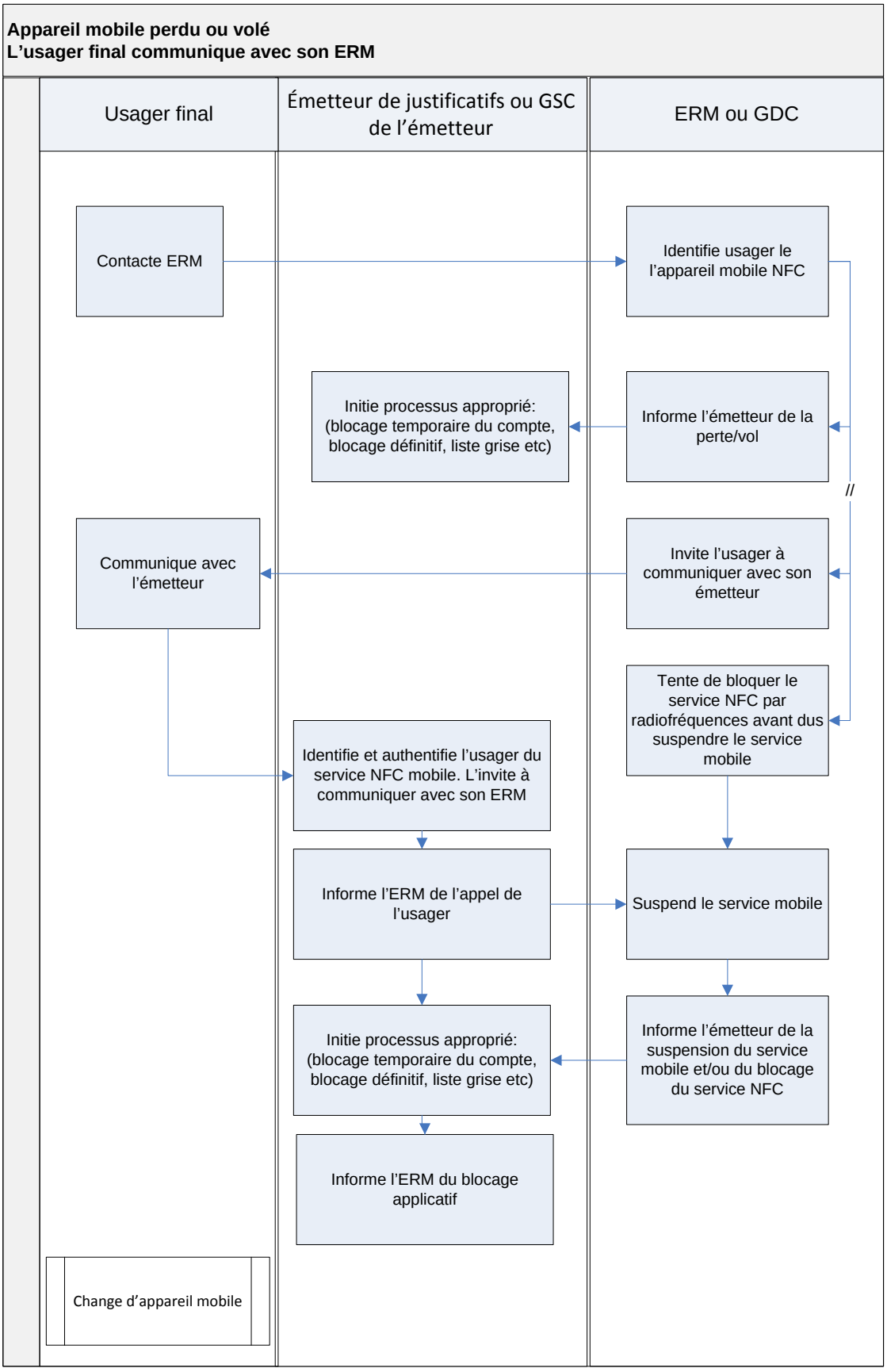


10.5.4 PERTE OU VOL DE L'APPAREIL MOBILE (L'UTILISATEUR FINAL COMMUNIQUE AVEC L'ERM ET L'EJP)

Ce processus définit la marche à suivre si un utilisateur final perd un appareil mobile doté d'une application de paiement mobile NFC activée.

- En cas de perte ou de vol d'un appareil mobile, l'utilisateur final doit être invité à communiquer avec l'ERM et l'EJP **[70]**.
- Lorsqu'il est mis au courant de la perte ou du vol d'un appareil mobile, l'ERM ou le GDS (s'ils sont différents) doit tenter d'interrompre le service de l'appareil mobile ou de le bloquer (dans le cas d'appareils dotés d'une carte SIM, la carte doit également être bloquée; autrement, la zone sécurisée de l'élément sécurisé intégré doit être bloquée, au besoin) **[EN71]**.
- Lorsqu'il est mis au courant de la perte ou du vol d'un appareil mobile, l'EJP doit bloquer la méthode de paiement. (d'autres étapes, ressemblant aux étapes actuelles d'inscription de produits de cartes sur une liste noire, peuvent être suivies à l'interne) **[72]**.
- Après l'annulation du service, l'utilisateur final peut entamer le processus de remplacement de l'appareil mobile et de réinstallation du porte-monnaie et des justificatifs de paiement.



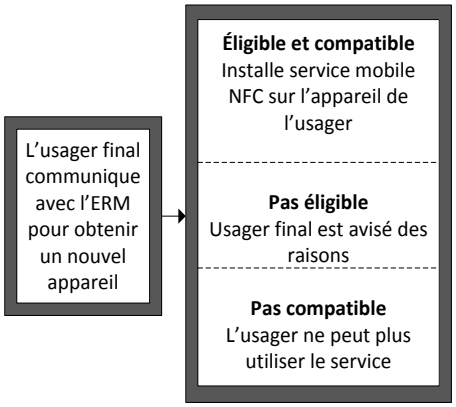

Appareil mobile perdu ou volé
L'usager final communique avec son ERM
Usager final
Émetteur de justificatifs ou GSC de l'émetteur
ERM ou GDC
Contacte ERM
Identifie usager le l'appareil mobile NFC
Initie processus approprié: (blocage temporaire du compte, blocage définitif, liste grise etc)
Informe l'émetteur de la perte/vol
//
Communique avec l'émetteur
Invite l'usager à communiquer avec son émetteur
Tente de bloquer le service NFC par radiofréquences avant dus suspendre le service mobile
Identifie et authentifie l'usager du service NFC mobile. L'invite à communiquer avec son ERM
Informe l'ERM de l'appel de l'usager
Suspend le service mobile
Initie processus approprié: (blocage temporaire du compte, blocage définitif, liste grise etc)
Informe l'émetteur de la suspension du service mobile et/ou du blocage du service NFC
Informe l'ERM du blocage applicatif
Change d'appareil mobile

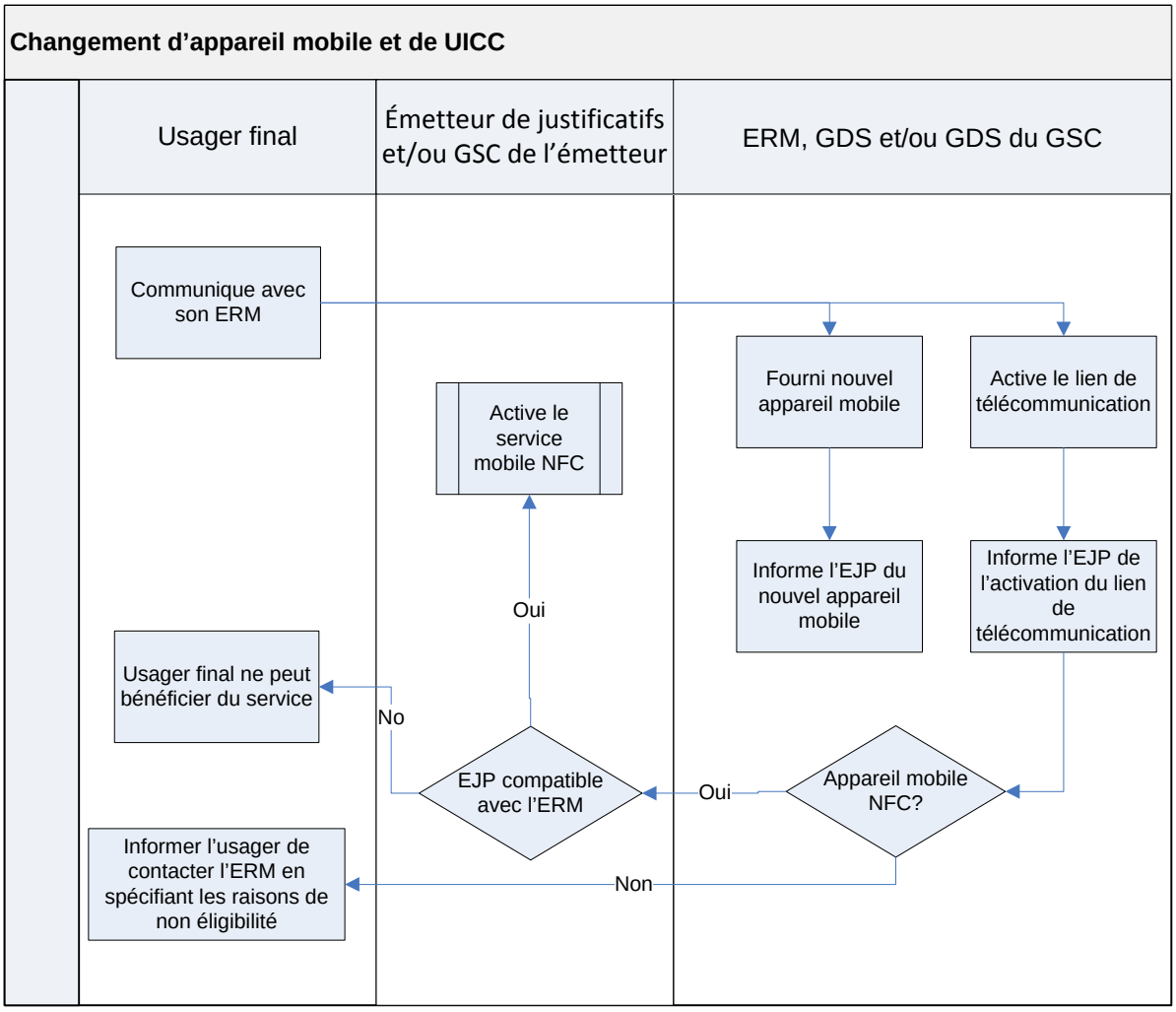
10.5.5 REMPLACEMENT DE L'APPAREIL MOBILE PAR L'UTILISATEUR FINAL (À LA SUITE DE L'ACHAT D'UN NOUVEL APPAREIL OU APRÈS UNE PERTE OU UN VOL)

Ce processus décrit l'activation d'un nouvel appareil mobile. Cette activation peut faire suite à un choix de l'utilisateur final ou à la perte ou au vol d'un appareil mobile. Avant l'activation d'un nouvel appareil mobile et l'installation des justificatifs de paiement, le GSC de l'EJP ou le GSC du GDS de l'ancien appareil ou de l'appareil perdu ou volé doit tenter de retirer toute l'information relative aux justificatifs de paiement et doit fournir un avis concernant le résultat de cette opération à l'ERM et au GDS (s'ils sont différents) et à l'EJP **[73]**.

Ce processus se déroule comme suit :

- l'ERM fournit un nouvel appareil mobile ou ajoute le nouvel appareil à son réseau;
- l'ERM fournit la connectivité mobile;
- l'utilisateur final demande l'accès aux services de paiement mobile NFC (en suivant les mêmes étapes que lors de la configuration initiale).





10.6 ACTIVITÉS DE SOUTIEN ASSOCIÉES À L'UTILISATEUR FINAL

Pendant qu'il demeure actif, l'utilisateur final aura besoin de services de maintenance et de soutien relativement à l'application de paiement. Les services de paiement mobile NFC sont complexes compte tenu du nombre d'intervenants. Afin d'offrir à l'utilisateur final une expérience satisfaisante à ce chapitre, il pourra obtenir de l'aide selon les modalités ci-dessous.

10.6.1 APPAREIL ET SERVICES MOBILES

En cas de questions liées à l'appareil ou aux services mobiles, l'utilisateur final sera invité à communiquer avec l'ERM. **[74]**. Même si le service est désactivé, l'application de paiement pourrait continuer de fonctionner et d'autoriser les paiements mobiles. Une entente doit être conclue avec l'ERM ou le GDS en vue de l'exécution d'activités d'approvisionnement et de maintenance même lorsque les services mobiles de l'utilisateur final sont interrompus ou inactifs **[75]**.

10.6.2 INSTALLATION DES JUSTIFICATIFS DE PAIEMENT ÉCHOUÉE

Si l'installation des justificatifs de paiement échoue, l'utilisateur final sera invité à communiquer avec l'EJP. **[76]**

10.6.3 TRANSACTION ÉCHOUÉE

Si une transaction échoue, l'utilisateur final sera invité à communiquer avec l'EJP responsable de l'instrument de paiement utilisé. **[77]**

10.6.4 ACTIVITÉS DE MAINTENANCE LIÉES AU COMPTE

Dans le cas de toutes les activités de maintenance associées à un compte, l'utilisateur final sera invité à communiquer avec l'EJP**. [78]**

10.6.5 APPAREIL MOBILE PERDU OU VOLÉ

En cas de perte ou de vol d'un appareil mobile, l'utilisateur final sera invité à communiquer avec l'ERM et le ou les EJP. **[79]**

10.6.6 PROCESSUS D'ASSOCIATION

Si le porte-monnaie fonctionne normalement, mais que l'application de paiement connaît des ratés, l'utilisateur final sera invité à appeler l'EJP. **[80]**

10.6.7 MAINTENANCE DE L'APPLICATION DE PAIEMENT

En cas de problèmes associés à la maintenance de l'application de paiement, l'utilisateur final sera invité à communiquer avec l'EJP. **[81]**

10.7 SUPPRESSION DE L'APPLICATION DE PAIEMENT ET DES JUSTIFICATIFS CONNEXES

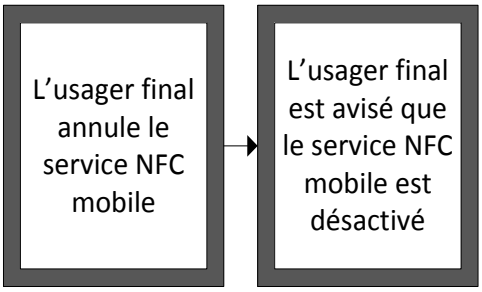
Le dernier élément de la section Habilitation et gestion du cycle de vie porte sur l'annulation des services de paiement mobile. Cette section décrit les lignes directrices pour mettre fin à ces services. Les services de paiement mobile peuvent être annulés par l'utilisateur final, l'ERM ou l'EJP. Cette section ne tient pas compte des différences entre les processus d'annulation des services mobiles NFC des participants à l'écosystème : il est présumé que tous les processus d'annulation sont identiques.

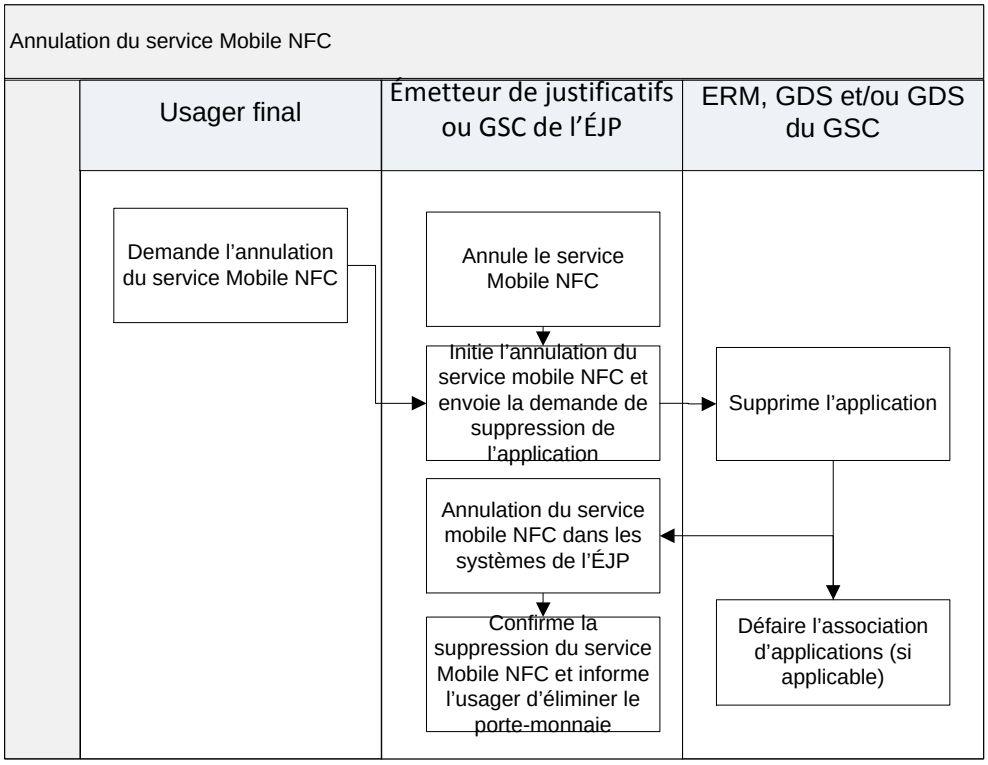
Si l'ERM met fin aux services mobiles, l'application de paiement continue de fonctionner. Des ententes doivent être conclues entre l'ERM et l'EJP en vue d'établir des protocoles visant une telle situation (voir section 10.6.1) **[82]** Même si l'application mobile continue de fonctionner, il est recommandé que l'on mette fin aux services mobiles NFC dès que le service de l'ERM est annulé, que l'ERM nettoie l'élément sécurisé et que l'EJP est informé de la prise de ces mesures. En l'absence d'une entente à cet effet, l'utilisateur final pourrait continuer d'utiliser son appareil mobile comme instrument de paiement. Cependant, l'EJP ou son GSC ne serait pas en mesure d'installer des justificatifs de paiement au moyen de radiofréquences dans un appareil mobile non doté d'une connexion mobile active.

10.7.1 ANNULATION DES SERVICES DE PAIEMENT MOBILE NFC PAR L'EJP OU L'UTILISATEUR FINAL

Ce scénario illustre l'annulation des services de paiement mobile NFC par l'EJP ou l'utilisateur final.

- Ce processus définit la manière sûre d'éliminer de l'appareil mobile l'application de paiement et les justificatifs connexes. Pour mettre fin aux services de paiement mobile, l'utilisateur final doit communiquer avec l'EJP.
- L'EJP peut utiliser ce processus pour éliminer l'application de paiement et les justificatifs connexes qui se trouvent dans l'appareil mobile à l'égard duquel l'utilisateur final a déjà annulé le produit de paiement.





10.8 HABILITATION ET GESTION DU CYCLE DE VIE – RÉSUMÉ

La section Habilitation et gestion du cycle de vie contient des énoncés normalisés concernant le téléchargement d'une application de porte-monnaie mobile, l'installation de justificatifs de paiement dans un appareil mobile et la maintenance de ces justificatifs pendant le cycle de vie de l'utilisateur final.

10.9 ÉNONCÉS NORMALISÉS

Numéro	Énoncé	Section
44	La section Habilitation et gestion du cycle de vie repose sur le principe selon lequel les interactions entre les participants à l'écosystème (ERP et EJP, fournisseur de porte-monnaie et EJP, EJP et GSC, EJC et ERM, etc.) doivent être précédées d'étapes visant à établir des relations commerciales contractuelles.	10.1 Relations commerciales entre participants à l'écosystème

Numéro	Énoncé	Section
45	[Contexte : Ce document ne tient pas compte de tous les processus de gestion des clés comme ceux entre le réseau de paiement et l'EJP.] En plus des lignes directrices définies dans cette section, les processus de gestion des clés définis par les réseaux de paiement doivent être respectés.	10.2 Gestion des clés
46	Comme il est décrit à la section 6.8, toutes les activités de messagerie doivent être exécutées conformément aux lignes directrices pertinentes tirées du document GPS_Messaging_Specification_for_Mobile_NFC_Services-v1.0.	10.2 Gestion des clés
47	Les intervenants qui appliquent les normes contenues dans ce document acceptent de n'utiliser que le mode de délégation ou le mode bimodal, tels que définis par GlobalPlatform, dans le cadre de toutes les activités associées à l'habilitation et à la gestion du cycle de vie.	10.2 Gestion des clés
48	S'il s'agit d'un porte-monnaie exclusif, un processus de gestion des clés sécurisées doit être établi entre l'EJP, son GSC, le GDS et son GSC.	10.2 Gestion des clés
49	S'il s'agit d'un porte-monnaie ouvert, des protocoles doivent être établis de manière à ce que les clés soient gérées par plusieurs intervenants.	10.2 Gestion des clés
50	Dans le cadre de ce processus [le processus de gestion des clés], le GSC de l'EJP et l'EJP, le GSC du GDS et le GDS et le GSC de l'EJP et le GSC du GDS doivent avoir établi une relation commerciale, directement ou indirectement.	10.2 Gestion des clés
51	L'échange de clés doit être réalisé conformément aux lignes directrices de GlobalPlatform.	10.2.2 Installateur unique de justificatifs de paiement
52	[Contexte : une fois ce processus terminé, l'échange de clés permettra de mettre en place une voie de communication protégée dédiée à la transmission de données entre l'EJP, son GSC et le GSC du GDS.] Cette voie de communication protégée constitue une exigence minimale et doit être en place afin que puissent être exécutées des activités d'approvisionnement par radiofréquences.	10.2.2 Installateur unique de justificatifs de paiement
53	Ensuite, les GSC des EJP échangent des clés entre eux pour s'assurer de mettre en place des voies de communication protégées. Cet échange de clés doit avoir lieu pour permettre l'installation de justificatifs de paiement dans un porte-monnaie ouvert ou collectif.	10.2.3 Installateurs multiples de justificatifs de paiement (réseau en étoile)

Numéro	Énoncé	Section
54	Dans ce modèle, tous les intervenants doivent échanger les clés conformément aux lignes directrices de GlobalPlatform. L'AC ou la plaque tournante de GSC des EJP doit élaborer et diffuser des protocoles destinés à faciliter ces interactions.	10.2.3 Installateurs multiples de justificatifs de paiement (réseau en étoile)
55	À titre d'exigence minimale, l'utilisateur final doit être en mesure de demander l'installation de l'application de paiement à l'aide de son porte-monnaie mobile.	10.4.1 Demande d'accès de l'utilisateur final à l'application de paiement
56	Outre cette méthode, la demande d'installation de l'application de paiement peut être présentée en ligne, dans une succursale bancaire, en appelant à un centre d'appels ou au moyen d'une application de services bancaires mobiles. Quelle que soit la méthode utilisée pour télécharger l'application et les justificatifs de paiement, l'utilisateur final doit donner son consentement avant l'installation.	10.4.1 Demande d'accès de l'utilisateur final à l'application de paiement
57	Dans le cas des demandes présentées à l'aide du porte-monnaie mobile, ce dernier doit afficher le nom de l'EJP dont les justificatifs de paiement vont être installés dans le porte-monnaie.	10.4.1 Demande d'accès de l'utilisateur final à l'application de paiement
58	Avant l'installation de l'application et des justificatifs de paiement dans l'appareil mobile, l'identité de l'utilisateur final doit être validée.	10.4.2 Vérification et validation des renseignements relatifs à l'utilisateur final
59	Le processus de vérification et de validation de l'identité différera en fonction de l'EJP. Ce dernier a la responsabilité de définir le processus de vérification et de validation de l'identité de l'utilisateur final.	10.4.2 Vérification et validation des renseignements relatifs à l'utilisateur final
60	Après la vérification et la validation, l'EJP doit envoyer à l'utilisateur final un message décrivant la prochaine étape.	10.4.2 Vérification et validation des renseignements relatifs à l'utilisateur final
61	Pour que l'application et les justificatifs de paiement puissent être installés, tous les intervenants doivent établir une voie de communication protégée avec l'EJP et le GDS.	10.4.3 Installation de l'application de paiement

Numéro	Énoncé	Section
62	Une fois la voie de communication protégée établie, le GENC doit prendre en charge toutes les activités, y compris l'installation et l'activation des services de paiement mobile NFC dans l'appareil.	10.4.3 Installation de l'application de paiement
63	L'association est nécessaire pour qu'un porte-monnaie mobile puisse accéder à une application de paiement.	10.4.4 Association de l'application de paiement au porte-monnaie mobile
64	L'application parapluie sert de répertoire de l'UICC et doit être fournie par le GDS.	10.4.5 Élément sécurisé dans l'UICC
65	[Contexte : ensuite, l'application parapluie informe le porte-monnaie de l'endroit où se trouve l'application de paiement et lui fournit un identificateur permettant de la repérer.] Le GDS doit fournir la structure de l'identificateur.	10.4.5 Élément sécurisé dans l'UICC
66	Les justificatifs de paiement sont stockés dans l'appareil mobile et doivent pouvoir être installés et mis à jour au moyen de radiofréquences.	10.4.7 Installation de justificatifs de paiement au moyen de radiofréquences
67	Si le GDS (ou le GSC du GDS) demande la mise à jour de l'élément sécurisé, la partie intéressée doit communiquer avec le GSC de l'EJP pour réinstaller l'application de paiement après la mise à jour de l'élément sécurisé.	10.5.2 Mise à jour de l'élément sécurisé
68	Changement d'appareil mobile (élément sécurisé intégré) : si l'application de paiement mobile est stockée dans l'élément sécurisé intégré, l'utilisateur final doit appliquer de nouveau tout le processus d'installation du porte-monnaie mobile et de l'application de paiement (étapes de configuration d'un nouvel appareil).	10.5.3 Changement d'appareil mobile
69	Changement d'appareil mobile (élément sécurisé dans l'UICC) : si l'utilisateur final change d'appareil mobile ou ajoute un appareil secondaire, il doit effectuer la configuration initiale de nouveau, y compris la vérification de l'identité de l'utilisateur final et l'association du porte-monnaie mobile et des justificatifs de paiement.	10.5.3 Changement d'appareil mobile
70	En cas de perte ou de vol d'un appareil mobile, l'utilisateur final doit être invité à communiquer avec l'ERM et l'EJP.	10.5.4 Appareil mobile perdu ou volé

Numéro	Énoncé	Section
71	Lorsqu'il est mis au courant de la perte ou du vol d'un appareil mobile, l'ERM ou le GDS (s'ils sont différents) doit interrompre le service de l'appareil mobile ou le bloquer (dans le cas d'appareils dotés d'une carte SIM, la carte doit également être bloquée; autrement, la zone sécurisée de l'élément sécurisé intégré doit être bloquée, au besoin).	10.5.4 Appareil mobile perdu ou volé
72	Lorsqu'il est mis au courant de la perte ou du vol d'un appareil mobile, l'EJP doit bloquer la méthode de paiement (d'autres étapes, ressemblant aux étapes actuelles d'inscription de produits de cartes sur une liste noire, peuvent être suivies à l'interne).	10.5.4 Appareil mobile perdu ou volé
73	[Contexte : ce processus décrit l'activation d'un nouvel appareil mobile. Cette activation peut faire suite à un choix de l'utilisateur final ou à la perte ou au vol d'un appareil mobile.] Avant l'activation d'un nouvel appareil mobile et l'installation des justificatifs de paiement, le GSC de l'EJP ou le GSC du GDS de l'ancien appareil ou de l'appareil perdu ou volé doit tenter de retirer toute l'information relative aux justificatifs de paiement et doit fournir un avis concernant le résultat de cette opération à l'ERM et au GDS (s'ils sont différents) et à l'EJP.	10.5.5 Remplacement de l'appareil mobile par l'utilisateur final
74	En cas de questions liées à l'appareil ou aux services mobiles, l'utilisateur final sera invité à communiquer avec l'ERM.	10.6.1 Appareil et services mobiles
75	Une entente doit être conclue avec l'ERM ou le GDS en vue de l'exécution d'activités d'approvisionnement et de maintenance même lorsque les services mobiles de l'utilisateur final sont interrompus ou inactifs.	10.6.2 Installation des justificatifs de paiement échouée
76	Si l'installation des justificatifs de paiement échoue, l'utilisateur final sera invité à communiquer avec l'EJP.	10.6.3 Transaction échouée
77	Si une transaction échoue, l'utilisateur final sera invité à communiquer avec l'EJP responsable de l'instrument de paiement utilisé.	10.6.3 Transaction échouée
78	Dans le cas de toutes les activités de maintenance associées à un compte, l'utilisateur final sera invité à communiquer avec l'EJP.	10.6.4 Activités de maintenance liées au compte
79	En cas de perte ou de vol d'un appareil mobile, l'utilisateur final sera invité à communiquer avec l'ERM et le ou les EJP.	10.6.5 Appareil mobile perdu ou volé
80	Si le porte-monnaie fonctionne normalement, mais que l'application de paiement connaît des ratés, l'utilisateur final sera invité à appeler l'EJP.	10.6.6 Processus d'association

Numéro	Énoncé	Section
81	En cas de problèmes associés à la maintenance de l'application de paiement, l'utilisateur final sera invité à communiquer avec l'EJP.	10.6.7 Maintenance de l'application de paiement
82	Si l'ERM met fin aux services mobiles, l'application de paiement continue de fonctionner. Des ententes doivent être conclues entre l'ERM et l'EJP en vue d'établir des protocoles visant une telle situation (voir section 10.6.1).	10.7 Suppression de l'application de paiement et des justificatifs connexes

11 FIDÉLISATION ET RÉCOMPENSES

Le domaine de la fidélisation et des récompenses est en évolution rapide. C'est pourquoi, au lieu d'énoncer des directives strictes, ce document présente des lignes directrices. Une partie importante de cette section est consacrée à l'élaboration d'une vision commune du marché actuel et du rôle de la fidélisation et des récompenses relativement à l'avenir des paiements mobiles. À mesure que l'écosystème évolue, ce document peut être mis à jour dans le but d'établir des normes en matière de fidélisation et de récompenses.

La section Fidélisation et récompenses est divisée dans les sous-sections suivantes :

- Aperçu des programmes de fidélisation
- Interaction au PDV
- Échange de points de fidélisation (programmes de fidélisation, coupons, bons d'achat et incitatifs)
- Fidélisation et récompenses – Résumé

Cette section porte sur les types de programmes de fidélisation actuellement offerts et ceux qui pourraient être pris en charge au moyen de la technologie de paiements mobiles NFC, les normes relatives aux données liées à ces programmes, les récompenses, les coupons, les bons d'achat, les incitatifs et l'expérience de l'utilisateur final en matière d'interaction au PDV en ce qui a trait aux programmes de fidélisation.

11.1 APERÇU DES PROGRAMMES DE FIDÉLISATION

11.1.1 INTRODUCTION

Plusieurs programmes de fidélisation sont actuellement en vigueur dans le marché. Chacun de ces programmes a des caractéristiques différentes en matière de financement et d'échange.

Le tableau qui suit décrit les différents types de programmes de fidélisation offerts. Le but de cette section est d'informer le lecteur relativement au milieu actuel de la fidélisation et des récompenses et de présenter les effets possibles de la prise en charge de programmes de fidélisation et de récompenses dans la structure des paiements mobiles.

11.1.2 ANALYSE DES PROGRAMMES DE FIDÉLISATION

La présente section donne un aperçu des programmes de fidélisation. Chacun de ces programmes pourrait être utilisé conjointement avec un porte-monnaie mobile.

Type de programme de fidélisation	Description	Caractéristiques de financement
Programmes partiellement financés par les marchands	Ces programmes sont offerts conjointement avec des produits de cartes de crédit ou de débit. Dans le cadre de ces programmes, les utilisateurs finaux accumulent des points ou reçoivent des remises en argent auprès de marchands participants. Habituellement, ces programmes sont de courte durée.	En général, les rabais sont financés par les marchands. La délivrance de points et les remises en argent liées à ces programmes sont habituellement financées par les émetteurs de produits de paiement.

Type de programme de fidélisation	Description	Caractéristiques de financement
Programmes de points et de remises en argent fondés sur le produit de paiement	Ces programmes sont habituellement offerts par les émetteurs de produits de paiement. Il s'agit en général de programmes permanents dans le cadre desquels les utilisateurs finaux accumulent des points ou reçoivent des remises en argent de la part des émetteurs de produits de paiement.	Ces programmes sont financés par les émetteurs de produits de paiement et visent à inciter les utilisateurs finaux à dépenser.
Programmes offerts par un groupe de marchands	Programmes ponctuels ou permanents dans le cadre desquels les utilisateurs finaux enregistrent des produits de paiement afin de recevoir des rabais et d'accumuler des points auprès de marchands participants. Ces programmes sont offerts par des associations mutuelles, des réseaux de paiement et des administrateurs de programmes de fidélisation.	Ces programmes sont habituellement financés par les marchands ou les fabricants.
Programmes offerts en ligne seulement, financés par les marchands	Programmes permanents dans le cadre desquels les utilisateurs finaux accumulent des points ou reçoivent des remises en argent grâce à l'utilisation d'un produit de paiement pour effectuer des achats en ligne auprès de certains marchands.	Ces programmes sont habituellement financés par les marchands ou les fabricants.
Programmes de rabais financés par les marchands	Programmes ponctuels prenant la forme de rabais en ligne et de coupons en magasin. Ces programmes sont habituellement offerts par des émetteurs de produits de paiement, des réseaux de paiement ou des associations mutuelles.	Ces programmes sont habituellement financés par les marchands ou les fabricants.
Programmes entièrement financés par les marchands	Programmes ponctuels ou permanents parrainés par les marchands. Ces programmes ne sont pas associés à un produit de paiement et n'exigent pas la participation d'une institution financière.	Ces programmes sont entièrement financés par les marchands.

Comme il est souligné dans le tableau ci-dessus, la plupart des programmes de fidélisation concernent plusieurs intervenants, ce qui sous-entend l'utilisation de plusieurs moyens de gestion du processus d'échange. Compte tenu de la nature de ces programmes, seuls quelques-uns d'entre eux sont

considérés comme étant compatibles avec les services de paiement mobile NFC, du point de vue de l'interaction au PDV et du processus d'échange.

Les programmes considérés comme étant compatibles avec les services de paiement mobile NFC sont ceux qui font appel à des produits de paiement :

- Programmes partiellement financés par les marchands
- Programmes de points et de remises en argent fondés sur le produit de paiement
- Programmes offerts par un groupe de marchands

Ces programmes permettent une interaction directe au PDV et font appel à un produit de paiement. Les autres programmes ne répondent pas à ces critères.

11.1.3 APERÇU DES COUPONS, DES BONS D'ACHAT ET DES INCITATIFS

La présente section porte sur le concept de « couponnage ». Les marchands et les fabricants utilisent le couponnage pour accroître leurs ventes. Il est prévu que l'utilisation de coupons, de bons d'achat et d'autres incitatifs à l'aide d'appareils mobiles représentera une augmentation de valeur importante pour les utilisateurs finaux et les marchands.

Compte tenu de la hausse de la popularité des appareils mobiles, les spécialistes du marketing ont cherché de nouveaux moyens permettant la prise en charge de coupons par ces appareils. Ainsi, plusieurs services sont offerts aux utilisateurs finaux pour leur permettre d'obtenir et d'échanger des coupons à l'aide de leur appareil mobile.

Le tableau ci-dessous présente les différents types de coupons, de bons d'achat et d'incitatifs offerts sur le marché.

11.1.4 ANALYSE DES COUPONS, DES BONS D'ACHAT ET DES INCITATIFS

Cette section donne un aperçu des programmes de fidélisation; ces programmes pourraient être utilisés conjointement avec un porte-monnaie mobile.

Type de coupon ou de bon d'achat	Description	Caractéristiques de financement
Rabais ou réductions	Les rabais sont déduits du coût d'un article ou du total d'un achat. Habituellement, les rabais sont appliqués avant le paiement; les réductions, après le paiement.	Ces rabais et réductions sont financés par les marchands ou les fabricants.
Deux pour le prix d'un	Les marchands et les fabricants utilisent ces offres pour encourager l'achat de biens ou de services.	Ces offres sont habituellement financées par les marchands ou les fabricants.
Carte de membre	Les rabais sont réservés aux membres d'une association mutuelle (p. ex., clubs-entrepôts).	Ces rabais sont habituellement financés par les fabricants ou les marchands.
Biens ou services offerts (p. ex., article, frais d'envoi,	À la suite de l'achat d'un bien ou d'un service particulier par l'utilisateur final, des biens ou des services	Ces offres sont habituellement financées par les fabricants ou les

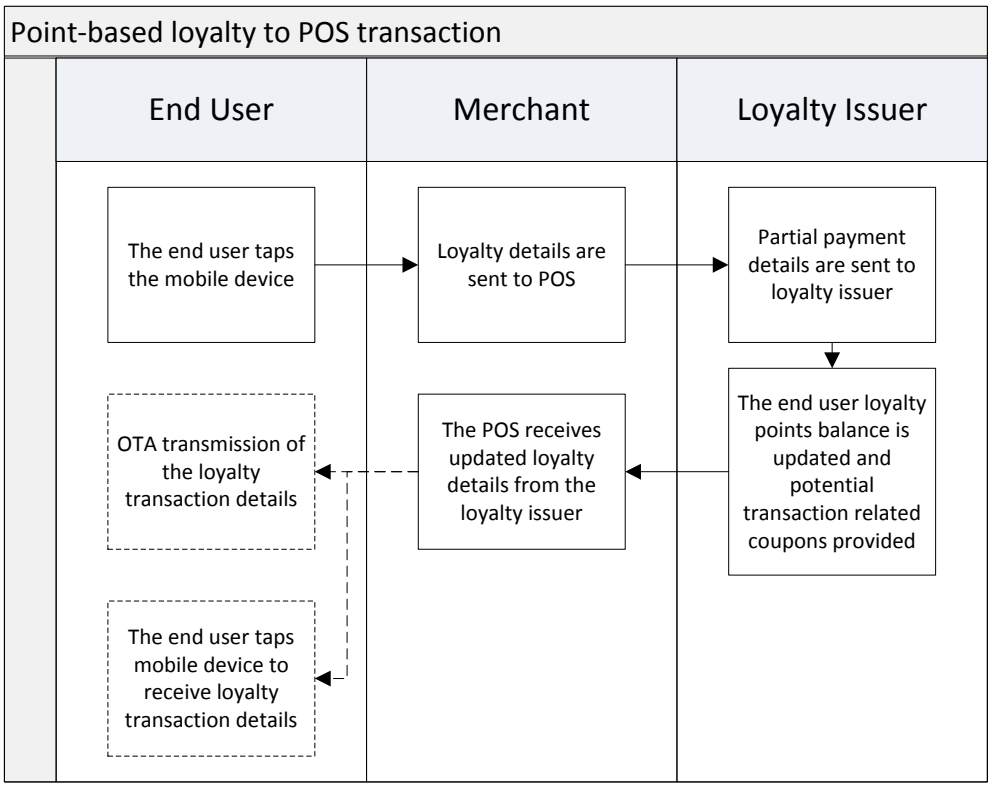
Type de coupon ou de bon d'achat	Description	Caractéristiques de financement
équivalent des taxes)	supplémentaires sont ajoutés à sa commande.	marchands.

11.2 INTERACTION AU PDV – PROGRAMMES DE FIDÉLISATION

La communication entre le PDV et les appareils mobiles est un autre domaine exigeant l'établissement de normes précises. Cette section porte sur les différents procédés et principes directeurs sous-jacents à la prise en charge du processus d'échange de coupons, de bons d'achat et d'incitatifs par le PDV. Il est souhaitable que les PDV soient en mesure d'extraire et de traiter les données de l'utilisateur final relatives aux programmes de fidélisation à partir de son appareil mobile. Si un marchand décide d'accepter la transmission NFC de renseignements liés aux programmes de fidélisation, cette section établit les lignes directrices à respecter.

11.2.1 INTERACTION AU PDV – SCHÉMA DU PROCESSUS

Le processus ci-dessous décrit la transmission de renseignements entre l'utilisateur final, le marchand et le responsable du programme de fidélisation. L'utilisateur final utilise une méthode de paiement standard (p. ex., Visa ou MasterCard) et présente son produit de paiement par points de fidélisation pour connaître son solde de points. En fonction des préférences configurées dans le porte-monnaie mobile, l'utilisateur final peut recevoir des coupons liés à cette transaction en vue d'une utilisation future.



Selon la méthode de réception des reçus électroniques établie, le détail de la transaction de fidélisation est envoyé par radiofréquence lorsque l'utilisateur final tape l'écran de son appareil.

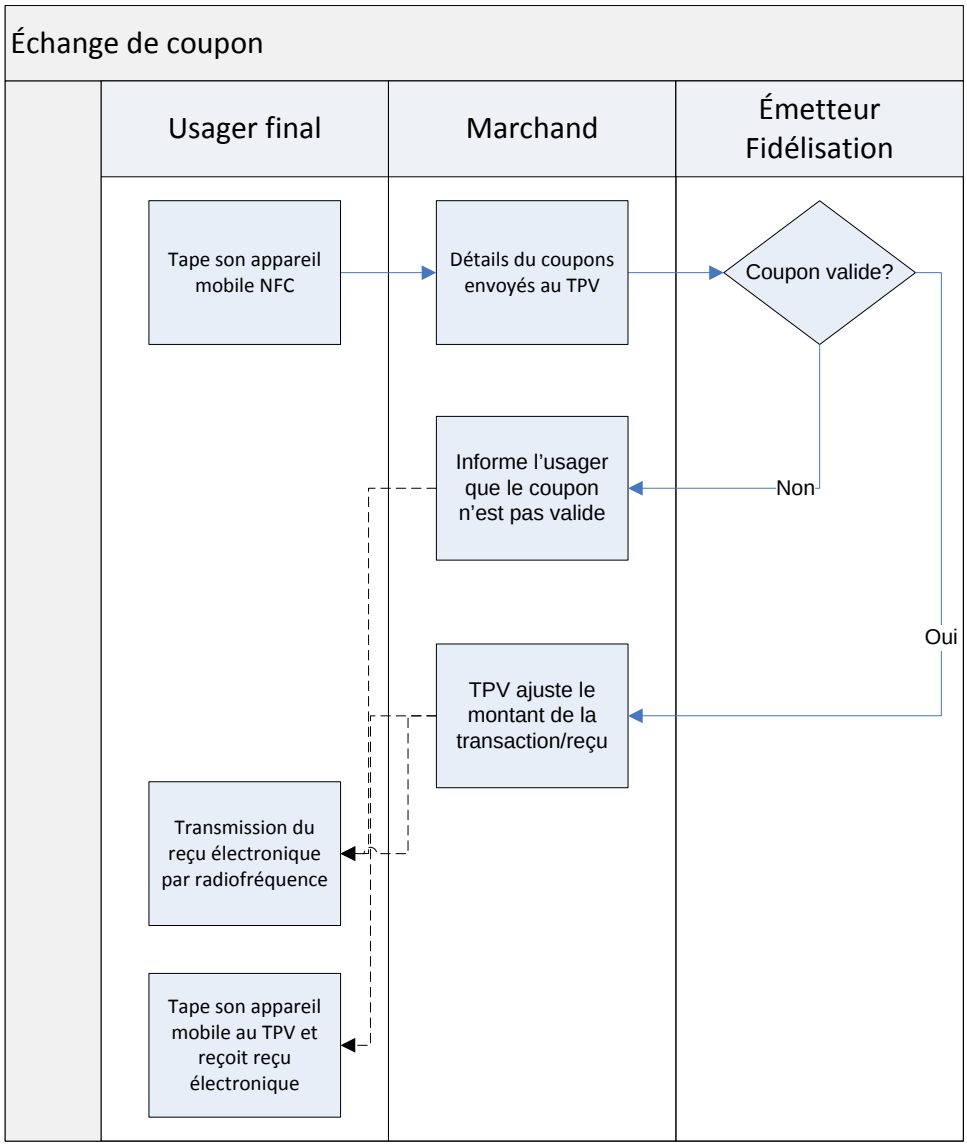
11.2.2 ANALYSE DE L'EXPÉRIENCE LIÉE À L'INTERACTION AU PDV DANS LE CADRE DE PROGRAMMES DE FIDÉLISATION

Cette section présente une comparaison de l'expérience de fidélisation habituelle avec l'expérience de fidélisation liée à l'utilisation d'un appareil mobile NFC. Cette dernière peut être bien plus intéressante pour l'utilisateur final.

Programme utilisé	Interaction actuelle	Interaction à l'aide d'un appareil mobile	Répercussions
Échange de points de fidélisation dans le cadre d'un achat	L'utilisateur final paie avec le produit de fidélisation et l'émetteur du produit de paiement ajoute des points dans son compte au moyen du système de points de fidélisation.	Les renseignements liés au programme de fidélisation sont transférés dans le porte-monnaie mobile et envoyés au PDV au moment de l'achat.	Pendant une transaction de paiement, le PDV doit être en mesure d'extraire et de traiter les données de l'utilisateur final relatives aux programmes de fidélisation.

11.2.3 ÉCHANGE DE COUPONS, DE BONS D'ACHAT ET D'INCITATIFS – SCHÉMA DU PROCESSUS

Le coupon est envoyé pendant le processus de paiement et il est déduit du total de la facture.



Selon la méthode de réception des reçus électroniques établie, les reçus électroniques mis à jour sont envoyés par radiofréquence lorsque l'utilisateur final tape l'écran de son appareil.

11.2.4 INTERACTION AU PDV – ANALYSE DES COUPONS, DES BONS D'ACHAT ET DES INCITATIFS

Type d'incitatif	Interaction actuelle	Interaction à l'aide d'un appareil mobile	Répercussions

Type d'incitatif	Interaction actuelle	Interaction à l'aide d'un appareil mobile	Répercussions
Rabais ou réductions, deux pour le prix d'un, remboursement de l'équivalent des taxes	L'utilisateur final reçoit un coupon imprimé. Le coupon est numérisé au PDV et le prix total est ajusté.	L'utilisateur final paie à l'aide de son appareil mobile. Le porte-monnaie mobile recherche des coupons pouvant s'appliquer à la transaction et les envoie au PDV. Avant que l'utilisateur final mette à jour la méthode de paiement de son appareil mobile, le PDV doit extraire et traiter les coupons associés à la transaction de paiement. Une fois que tous les coupons ont été traités, le paiement est effectué.	Le PDV doit extraire les coupons et les traiter avant la réalisation du paiement, sans que l'utilisateur ait à taper l'écran à plusieurs reprises.

Les répercussions ci-dessus entraînent l'établissement de certaines lignes directrices :

Les coupons et bons d'achat contenus dans le porte-monnaie mobile qui transmettent de l'information au PDV NFC au moyen de la technologie NFC ou d'une autre méthode (p. ex., code à barres) doivent respecter les normes pertinentes du présent document. **[83]**. Le PDV du marchand doit être en mesure de traiter les coupons et les bons d'achat transmis par NFC ou par un autre moyen et d'appliquer les rabais appropriés à la transaction de l'utilisateur final.

Technologies liées au PDV

Des protocoles ont été établis relativement à la transmission de renseignements liés aux programmes de fidélisation et aux coupons entre le PDV et l'appareil mobile. La norme internationale ISO/CEI 14443 définit les cartes de proximité employées à des fins d'identification et les protocoles de transmission utilisés pour communiquer. Cette norme doit être respectée dans le cadre de la transmission de renseignements liés aux programmes de fidélisation et de récompenses de l'appareil mobile au PDV au moyen de la technologie NFC. **[84]**.

En confirmant que la norme ISO/CEI 14443 est la norme à respecter dans le cadre de la transmission de renseignements liés aux programmes de fidélisation au Canada, le présent document cherche à limiter les répercussions sur les marchands. Ces derniers doivent tout de même moderniser leurs PDV de manière à assurer le bon acheminement de la transaction de fidélisation, mais le respect de cette norme limitera les coûts de modernisation du matériel ainsi que les coûts de conservation du personnel.

Plusieurs cartes de proximité permettent la transmission de données dans le cadre de services mobiles NFC, dont MiFare, FeliCa et Calypso. Le présent document ne fait la promotion d'aucune de ces cartes;

les organismes souhaitant offrir des programmes de fidélisation et de récompenses adaptés aux appareils mobiles sont encouragés à étudier ces cartes et l'architecture connexe.

11.3 ÉCHANGE DE POINTS DE FIDÉLISATION

L'échange de points de fidélisation désigne le processus qui consiste à récompenser les utilisateurs finaux de leur fidélité en leur offrant de la valeur sous forme de points, de coupons ou d'incitatifs. Les paiements mobiles NFC offrent la possibilité de faciliter le processus d'échange.

Dans cette section, l'expérience d'échange actuelle sera décrite en détail en ce qui a trait aux différents programmes de fidélisation, aux coupons, aux bons d'achat et aux incitatifs. Dans un premier temps, le portrait de la situation actuelle en matière d'échange sera dressé. Ensuite seront présentées l'expérience d'échange relative aux appareils mobiles ainsi que les mesures nécessaires pour mettre le processus en application.

Actuellement, l'échange de points de fidélisation peut se faire de trois façons :

- **Échange automatique :** le paiement est effectué au moyen des points de fidélisation de l'utilisateur final (en présumant que son solde de points est suffisant pour payer la totalité de l'achat).
- **Échange déclenché par l'utilisateur final :** avant d'effectuer le paiement, l'utilisateur final vérifie son solde de points et choisit de payer au moyen de ses points de fidélisation.
- **Échange déclenché par le marchand :** l'utilisateur final tente de payer en utilisant sa méthode de paiement habituelle et le marchand l'avise qu'il dispose d'un nombre suffisant de points. L'utilisateur final choisit alors de payer au moyen de ses points de fidélisation ou de la méthode standard.

11.3.1 ANALYSE DE L'EXPÉRIENCE D'ÉCHANGE DE POINTS DE FIDÉLISATION

Description	Expérience d'échange actuelle	Expérience d'échange relative aux transactions mobiles NFC	Répercussions
Programme partiellement financé par le marchand	Au PDV, l'utilisateur final échange ses points contre des produits sélectionnés, des nuitées ou d'autres prix, par l'entremise du site Web du programme de fidélisation. Les points peuvent servir à régler l'achat en totalité ou en partie.	L'utilisateur final paie à l'aide de l'appareil mobile : il choisit la carte pertinente dans son porte-monnaie mobile et ses points accumulés sont immédiatement appliqués à l'achat en question.	L'utilisateur final peut avoir à choisir au PDV l'option de paiement au moyen de ses points pour déclencher le processus d'échange.
Programme de points et de remises en argent (traditionnellement offert par une	L'utilisateur final échange ses points ou obtient sa remise en argent soit à la fin de son cycle de	À la fin du cycle de facturation, l'utilisateur final reçoit, dans son porte-monnaie mobile, un	Aucun changement n'est requis à l'égard de l'activation de ce mode d'échange à l'aide d'un appareil

Description	Expérience d'échange actuelle	Expérience d'échange relative aux transactions mobiles NFC	Répercussions
institution financière [IF])	facturation, soit à la fin de l'année. L'échange est fait automatiquement par l'IF sous forme d'un rabais sur facture ou d'un chèque à la fin de l'année.	relevé à jour faisant état de la remise en argent.	mobile NFC, car le processus est entièrement géré par l'IF.
Programme offert par un groupe de marchands et programme d'enregistrement	L'utilisateur final reçoit un rabais sur son achat après avoir montré au marchand les renseignements relatifs au programme.	L'utilisateur final paie en utilisant son porte-monnaie mobile et ses points accumulés sont immédiatement appliqués à l'achat en question.	L'utilisateur final peut avoir à taper l'écran de son appareil de nouveau pour déclencher immédiatement le processus d'échange avec le marchand, sauf si une connexion bidirectionnelle a été établie.
Programme de rabais financé par le marchand	Au PDV, l'utilisateur final échange ses points contre des produits sélectionnés, des nuitées ou d'autres prix, par l'entremise du site Web du programme de fidélisation. Autrement, l'utilisateur final peut échanger ses points au magasin du marchand lorsqu'il effectue son achat. Les points peuvent servir à régler l'achat en totalité ou en partie.	L'utilisateur final paie à l'aide de l'appareil mobile : il choisit le produit de paiement pertinent dans son porte-monnaie mobile et ses points accumulés sont immédiatement appliqués à l'achat en question.	L'utilisateur final peut avoir à choisir au PDV l'option de paiement au moyen de ses points pour déclencher le processus d'échange.
Programme entièrement financé par le marchand	Au PDV, l'utilisateur final échange ses points contre tout produit disponible dans les magasins	L'utilisateur final paie à l'aide de l'appareil mobile : il choisit le produit de paiement pertinent dans son	L'utilisateur final peut avoir à choisir au PDV l'option de paiement au moyen de ses points pour

Description	Expérience d'échange actuelle	Expérience d'échange relative aux transactions mobiles NFC	Répercussions
	participants. Les points peuvent servir à régler l'achat en totalité ou en partie.	porte-monnaie mobile et ses points accumulés sont immédiatement appliqués à l'achat en question.	déclencher le processus d'échange.

L'échange immédiat de points au PDV dans le cadre de programmes de fidélisation (en utilisant les points de fidélisation comme monnaie d'échange) est un service facultatif offert à la discrétion des participants à l'écosystème. Si les points de fidélisation et les récompenses sont utilisés comme monnaie d'échange, les justificatifs associés aux points de fidélisation et aux récompenses doivent être traités comme des justificatifs de paiement; ils doivent donc être installés et stockés de façon sécurisée dans l'appareil mobile. **[85]**. Pour procéder à l'échange immédiat de points de fidélisation, l'utilisateur final doit être tenu de présenter ses points comme mode de paiement en sélectionnant le programme de fidélisation approprié dans le porte-monnaie mobile. **[86]**

11.3.2 ANALYSE DE L'EXPÉRIENCE D'ÉCHANGE DE COUPONS, DE BONS D'ACHAT ET D'INCITATIFS

	Expérience d'échange actuelle	Expérience d'échange relative aux transactions mobiles NFC	Répercussions
Coupons, bons d'achat et incitatifs	L'utilisateur final présente le coupon au marchand; ce dernier le numérise et le PDV le traite.	Les coupons sont stockés dans le porte-monnaie mobile et ils sont envoyés au PDV au cours de la transaction de paiement.	La prise en charge des coupons par le porte-monnaie mobile est requise. Le PDV doit être modernisé pour traiter les coupons envoyés au cours de la transaction de paiement.

En fonction du consentement de l'utilisateur final, les coupons et les bons d'achat devraient pouvoir être automatiquement échangés par le porte-monnaie mobile dans le cadre d'une transaction de paiement.

11.4 FIDÉLISATION ET RÉCOMPENSES – RÉSUMÉ

Les programmes de fidélisation et de récompenses actuellement offerts sont évalués dans cette section, ainsi que le processus d'intégration potentiel de ces programmes dans le cadre de transactions de paiement mobile NFC. Cette section contient très peu d'énoncés normalisés; elle vise plutôt à fournir des recommandations quant à la mise en œuvre d'une solution en matière de fidélisation et de récompenses.

Il s'agit d'un domaine en évolution rapide. À mesure que l'écosystème évoluera, il faudra évaluer et mettre à jour les normes en matière de fidélisation et de récompenses.

La section finale, qui suit, porte sur les normes en matière de données et de sécurité visant tous les aspects des paiements mobiles, y compris la fidélisation et les récompenses.

11.5 ÉNONCÉS NORMALISÉS

Numéro	Énoncé	Section
83	Les coupons et bons d'achat contenus dans le porte-monnaie mobile qui transmettent de l'information au PDV NFC au moyen de la technologie NFC ou d'une autre méthode (p. ex., code à barres) doivent respecter les normes pertinentes du présent document.	11.2.4 Interaction au PDV – Analyse des coupons, des bons d'achat et des incitatifs
84	La norme internationale ISO/CEI 14443 définit les cartes de proximité employées à des fins d'identification et les protocoles de transmission utilisés pour communiquer. Cette norme doit être respectée dans le cadre de la transmission de renseignements liés aux programmes de fidélisation et de récompenses de l'appareil mobile au PDV au moyen de la technologie NFC.	11.2.5 Technologies liées au PDV
85	Si les points de fidélisation et les récompenses sont utilisés comme monnaie d'échange, les justificatifs associés aux points de fidélisation et aux récompenses doivent être traités comme des justificatifs de paiement; ils doivent donc être installés et stockés de façon sécurisée dans l'appareil mobile.	11.3.1 Analyse de l'expérience d'échange de points de fidélisation
86	Pour procéder à l'échange immédiat de points de fidélisation, l'utilisateur final doit être tenu de présenter ses points comme mode de paiement en sélectionnant le programme de fidélisation approprié dans le porte-monnaie mobile.	11.3.1 Analyse de l'expérience d'échange de points de fidélisation

12 DONNÉES ET SÉCURITÉ

La section Données et sécurité a été conçue en fonction d'un principe général selon lequel chaque participant à l'écosystème ne doit avoir accès qu'au minimum d'information requis pour remplir son rôle principal à moins que l'utilisateur final et les autres participants à l'écosystème autorisent explicitement le partage d'information. Le but premier des participants à l'écosystème est de protéger les données de l'utilisateur final et du marchand. L'accès aux données ainsi que leur utilisation doivent être communiqués à l'utilisateur final, qui doit accorder explicitement son autorisation à cet effet **[87]**. Conformément à l'EN9, qui s'applique à l'ensemble du présent document, l'EJP doit lui aussi accorder explicitement son autorisation à l'égard de l'utilisation des données.

12.1 DONNÉES

Les porte-monnaie mobiles représentent un élément relativement nouveau au sein de l'écosystème des paiements, qui va vraisemblablement évoluer. Beaucoup de nouveaux fournisseurs de porte-monnaie développent des porte-monnaie mobiles et les installent dans les appareils des utilisateurs finaux. Afin d'assurer le caractère sûr et sécuritaire de l'écosystème des paiements canadien, il est très important que les porte-monnaie mobiles soient conformes aux lignes directrices de l'industrie des paiements. Un élément essentiel de ces lignes directrices consiste à déterminer à quelles données peut accéder le porte-monnaie mobile. La présente section porte sur les différents types de données visées et contient les normes définissant les données auxquelles les différents intervenants ont accès.

Les tableaux et les énoncés normalisés font état de l'accès initial aux données, avant que l'utilisateur final et les autres participants à l'écosystème n'aient explicitement accordé leur autorisation.

En plus de respecter les lignes directrices en matière de données contenues dans cette section, tous les porte-monnaie mobiles doivent être conformes aux normes PCI DSS. En cas de conflit, les normes les plus strictes prévalent.

12.1.1 ACCÈS AUX DONNÉES CONTENUES DANS LE PORTE-MONNAIE

Cette section décrit quels participants à l'écosystème peuvent avoir accès aux différents types de données contenues dans le porte-monnaie.

Type de données	EJP	Fournisseur de porte-monnaie	Marchand	Utilisateur final	ERM ou GDS	Responsable du programme de fidélisation	Autres applications
Produits de paiement contenus dans le porte-monnaie	NON	OUI[11]	NON	OUI	NON	NON	NON
Produits de fidélisation contenus dans le porte-monnaie	NON	OUI[12]	NON	OUI	NON	NON	NON
Coupons contenus dans le porte-monnaie	NON	OUI	NON	OUI	NON	NON	OUI

- **Produits de paiement contenus dans le porte-monnaie** – seuls le **fournisseur de porte-monnaie** et **l'utilisateur final** ont accès aux **produits de paiement** contenus dans un porte-monnaie. Aucun autre intervenant ne doit avoir accès aux **produits de paiement**. **[88]**.

[11] Seuls les émetteurs de justificatifs chiffrés ont accès à cette information. Le fournisseur de porte-monnaie n'a accès qu'au minimum d'information nécessaire pour assurer la maintenance des produits. L'accent doit être mis sur le fait que l'EJP et l'utilisateur final doivent accorder explicitement leur consentement à l'égard de l'accès aux renseignements et de leur utilisation.

[12] Seuls les émetteurs de justificatifs chiffrés ont accès à cette information. Le fournisseur de porte-monnaie n'a accès qu'au minimum d'information nécessaire pour assurer la maintenance des produits. L'accent doit être mis sur le fait que l'EJP et l'utilisateur final doivent accorder explicitement leur consentement à l'égard de l'accès aux renseignements et de leur utilisation.

L'accès du fournisseur de porte-monnaie à l'information liée aux **produits de paiement** doit se limiter à l'information nécessaire pour assurer la maintenance du porte-monnaie **[89]**.

- **Produits de fidélisation contenus dans le porte-monnaie** – seuls le **fournisseur de porte-monnaie** et **l'utilisateur final** ont accès à la l**iste de produits de fidélisation** contenue dans un porte-monnaie. Aucun autre intervenant ne doit avoir accès à la **liste de produits de fidélisation [].** L'accès du fournisseur de porte-monnaie à **l'information liée aux produits de fidélisation** doit se limiter à l'information nécessaire pour assurer la maintenance du porte-monnaie **[91].**
- **Coupons contenus dans le porte-monnaie** – seuls le **fournisseur de porte-monnaie**, **l'utilisateur final** et **quelques autres applications de fidélisation approuvées** par l'utilisateur final ont accès à la **liste de coupons** contenue dans un porte-monnaie. Aucun autre intervenant ne doit avoir accès à la **liste de coupons. [92]**

Les énoncés ci-dessus sont fondés sur le principe selon lequel seuls l'utilisateur final et les intervenants à l'égard desquels ils ont donné leur accord explicite peuvent accéder à l'information contenue dans le porte-monnaie. Cette information englobe notamment le nombre et le type de produits de paiement dont dispose l'utilisateur final.

12.1.2 ACCÈS AUX DONNÉES LIÉES AUX JUSTIFICATIFS

Cette section décrit quels participants à l'écosystème peuvent avoir accès aux données liées aux justificatifs, peu importe où ces données sont stockées.

Type de données	EJP	Fournisseur de porte-monnaie	Marchand	Utilisateur final	ERM ou GDS	Responsable du programme de fidélisation	Autres applications
Données non chiffrées liées au produit de paiement	OUI	NON	OUI[13]	OUI	NON	NON	NON
Données chiffrées liées au produit de paiement	OUI	NON	NON	NON	NON	NON	NON
Données non chiffrées associées aux justificatifs liés aux programmes de fidélisation	NON	NON	OUI[14]	OUI	NON	OUI	NON
Données chiffrées associées aux justificatifs liés aux programmes de fidélisation	NON	NON	NON	NON	NON	OUI	NON

[13] Consultez les précisions dans l'énoncé normalisé.
[14] Consultez les précisions dans l'énoncé normalisé.

- **Données non chiffrées liées au produit de paiement** – seuls l'**EJP**, les **marchands** et l'**utilisateur final** ont accès aux **données non chiffrées liées au produit de paiement**. Aucun autre intervenant ne doit avoir accès aux **données non chiffrées liées au produit de paiement [93]**. Exemples de données financières non chiffrées liées aux produits de paiement : numéro de carte de crédit, nom figurant sur la carte et code de vérification de carte. Les marchands ont accès à ces renseignements uniquement dans le cadre du traitement du paiement. La collecte et le stockage de **données non chiffrées liées aux produits de paiement par les marchands** doivent être conformes aux lignes directrices du réseau de paiement. **[94]**.
- **Données chiffrées liées au produit de paiement** – seul l'**EJP** a accès aux **données chiffrées liées au produit de paiement**. Aucun autre intervenant ne doit avoir **accès aux données chiffrées liées au produit de paiement. [95]**.
- **Données non chiffrées associées aux justificatifs liés aux programmes de fidélisation** – seuls le **responsable du programme de fidélisation**, les **marchands** et l'**utilisateur final** ont accès aux **données non chiffrées associées aux justificatifs liés aux programmes de fidélisation**. Aucun autre intervenant ne doit avoir accès aux **données non chiffrées associées aux justificatifs liés aux programmes de fidélisation [96]**. Les **données non chiffrées associées aux justificatifs liés aux programmes de fidélisation** collectées et stockées par les marchands doivent être traitées de la même manière que les justificatifs de paiement. De plus, ces données ne doivent servir qu'à l'octroi de récompenses et à l'échange de points de fidélisation **[97]**.
- **Données chiffrées associées aux justificatifs liés aux programmes de fidélisation** – si des points de fidélisation sont échangés au PDV, seul le **responsable du programme de fidélisation** a accès aux **données chiffrées associées aux justificatifs liés aux programmes de fidélisation**. Aucun autre intervenant ne doit avoir accès aux **données chiffrées associées aux justificatifs liés aux programmes de fidélisation**. **[98]**.

12.1.3 ACCÈS AUX DONNÉES FINANCIÈRES

Cette section décrit quels participants à l'écosystème peuvent avoir accès aux données liées aux transactions financières.

Type de données	Acquéreur	EJP	Fournisseur de porte-monnaie[15]	Marchand	Utilisateur final	ERM ou GDS	Responsable du programme de fidélisation	Autres applications
Montant	OUI	OUI	NON	OUI	OUI	NON	NON	NON
Heure	OUI	OUI	NON	OUI	OUI	NON	NON	NON
Marchand	OUI	OUI	NON	OUI	OUI	NON	NON	NON
Produit (quel justificatif)	OUI	OUI	NON	OUI	OUI	NON	NON	NON
Lieu	OUI	OUI	NON	OUI	OUI	NON	NON	NON
Détail de la transaction	NON	NON	NON	OUI	OUI	NON	NON	NON
Reçu électronique	NON	NON	NON	OUI	OUI	NON	NON	NON

**Veuillez prendre note que l'EN9 s'applique à toute la présente section.

- **Données financières, montant** – seuls l'**acquéreur**, l'**EJP**, le **marchand** et l'**utilisateur final** ont accès au **montant de la transaction**. Aucun autre intervenant ne doit avoir accès au **montant de la transaction** [**99]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le **montant de la transaction [100]**.

[15] Consultez les précisions dans l'énoncé normalisé.

- **Données financières, heure** – seuls l'**acquéreur**, l'**EJP**, le **marchand** et l'**utilisateur final** ont accès à l'**heure de la transaction**. Aucun autre intervenant ne doit avoir accès à l'**heure de la transaction**. **[101]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer l'**heure de la transaction** [**102]**.
- **Données financières, marchand** – seuls l'**acquéreur**, l'**EJP**, le **marchand** et l'**utilisateur final** peuvent connaître l'identité du **marchand ayant effectué la transaction**. Aucun autre intervenant ne doit connaître l'identité du **marchand ayant effectué la transaction**. **[103]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer l'identité du **marchand ayant effectué la transaction**. **[104]**.
- **Données financières, produit** – seuls l'**acquéreur**, l'**EJP**, le **marchand** et l'**utilisateur final** ont accès au **produit utilisé pour effectuer une transaction**. Aucun autre intervenant ne doit avoir accès au **produit utilisé pour effectuer une transaction**. **[105]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le **produit utilisé pour effectuer une transaction [106]**.
- **Données financières, lieu – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final ont accès au lieu de la transaction. Aucun autre intervenant ne doit avoir accès au lieu de la transaction. [107]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le **lieu de la transaction [108]**.
- **Données financières, détail de la transaction** – seuls le **marchand** et l'**utilisateur final** ont accès au **détail de la transaction** (p. ex., numéro d'article). Aucun autre intervenant ne doit avoir accès au **détail de la transaction [109]**. Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et le marchant accordent explicitement leur autorisation de communiquer le **détail de la transaction [110]**.
- **Données financières, reçus électroniques** – seuls le **marchand** et l'**utilisateur final** ont accès aux **reçus électroniques** liés à une transaction. Aucun autre intervenant ne doit avoir accès aux **reçus électroniques [111]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de transmettre les **reçus électroniques** [**112]**.

12.1.4 ACCÈS AUX DONNÉES LIÉES AUX PROGRAMMES DE FIDÉLISATION

Cette section décrit quels participants à l'écosystème peuvent avoir accès aux données liées aux transactions de fidélisation.

Type de données	Acquéreur	EJP	Fournisseur de porte-monnaie[16]	Marchand	Utilisateur final	ERM ou GDS	Responsable du programme de fidélisation	Autres applications
Montant	OUI	NON	NON	OUI	OUI	NON	OUI	NON
Heure	OUI	NON	NON	OUI	OUI	NON	OUI	NON
Marchand	OUI	NON	NON	OUI	OUI	NON	OUI	NON
Produit (quel justificatif)	OUI	NON	NON	OUI	OUI	NON	OUI	NON
Lieu	OUI	NON	NON	OUI	OUI	NON	OUI	NON
Détail de la transaction	NON	NON	NON	OUI	OUI	NON	NON	NON
Reçu électronique	NON	NON	NON	OUI	OUI	NON	NON	NON

**Veuillez prendre note que l'EN9 s'applique à toute la présente section.

- **Données liées aux programmes de fidélisation, montant** – seuls l'**acquéreur**, l'**EJP**, le **marchand** et l'**utilisateur final** ont accès au **montant d'une transaction de fidélisation**. Aucun autre intervenant ne doit avoir accès au **montant d'une transaction de fidélisation [113]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au

[16] Consultez les précisions dans l'énoncé normalisé.

fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le **montant d'une transaction de fidélisation [114]**.

- **Données liées aux programmes de fidélisation, heure** – seuls l'**acquéreur**, l'**EJP**, le **marchand** et l'**utilisateur final** ont accès à l'**heure d'exécution d'une transaction de fidélisation**. Aucun autre intervenant ne doit avoir accès à l'**heure d'exécution d'une transaction de fidélisation**. **[115]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer l'**heure d'exécution d'une transaction de fidélisation [116]**.
- **Données liées aux programmes de fidélisation, marchand** – seuls l'**acquéreur**, l'**EJP**, le **marchand** et l'**utilisateur final** peuvent connaître l'**identité du marchand ayant effectué la transaction de fidélisation**. Aucun autre intervenant ne doit connaître l'**identité du marchand ayant effectué la transaction de fidélisation**. **[117]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer l'**identité du marchand ayant effectué la transaction de fidélisation [118]**.
- **Données liées aux programmes de fidélisation, produit** – seuls l'**acquéreur**, l'**EJP**, le **marchand** et l'**utilisateur final** peuvent connaître le **produit utilisé pour effectuer une transaction de fidélisation**. Aucun autre intervenant ne doit connaître le **produit utilisé pour effectuer une transaction de fidélisation. [119]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le **produit utilisé pour effectuer une transaction de fidélisation [120]**.
- **Données liées aux programmes de fidélisation, lieu** – seuls l'**acquéreur**, l'**EJP**, le **marchand** et l'**utilisateur final** peuvent connaître le **lieu d'exécution d'une transaction de fidélisation**. Aucun autre intervenant ne doit connaître le **lieu d'exécution d'une transaction de fidélisation. [121]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le **lieu d'exécution d'une transaction de fidélisation [122]**.
- **Données liées aux programmes de fidélisation, détail de la transaction** – seuls le **marchand** et l'**utilisateur final** ont accès au **détail de la transaction de fidélisation** (p. ex., numéro d'article). Aucun autre intervenant ne doit avoir accès au **détail de la transaction de fidélisation [123]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le **détail de la transaction de fidélisation. [124]**.
- **Données liées aux programmes de fidélisation, reçus électroniques** – seuls le **marchand** et l'**utilisateur final** ont accès aux **reçus électroniques liés à une transaction de fidélisation**. Aucun autre intervenant ne doit avoir accès aux **reçus électroniques liés à une transaction de fidélisation [125]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de transmettre les **reçus électroniques liés à une transaction de fidélisation [126]**.

12.1.5 ACCÈS AUX DONNÉES LIÉES AUX PRODUITS DE PAIEMENT ET AU COMPTE DE FIDÉLISATION

Cette section décrit quels participants à l'écosystème peuvent avoir accès aux données liées aux produits de paiement et au compte de fidélisation et de récompenses.

Type de données		EJP	Fournisseur de porte-monnaie[17]	Marchand	Utilisateur final	ERM ou GDS	Responsable du programme de fidélisation	Autres applications
Produit de paiement	**Solde**	OUI	NON	NON	OUI	NON	NON	NON
	Détail du compte	OUI	NON	NON	OUI	NON	NON	NON
Produit de fidélisation	**Solde**	NON	NON	NON[18]	OUI	NON	OUI	NON
	Détail du compte	NON	NON	NON[19]	OUI	NON	OUI	NON

**Veuillez prendre note que l'EN9 s'applique à toute la présente section.

- **Produit de paiement, solde** – seuls l'**EJP** et l'**utilisateur final** ont accès au **solde du produit de paiement**. Aucun autre intervenant ne doit avoir accès au **solde du produit de paiement. [127]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le **solde du produit de paiement [128]**.
- **Produit de paiement, détail du compte** – seuls l'**EJP** et l'**utilisateur final** ont accès au **détail du compte lié au produit de paiement**. Aucun autre intervenant ne doit avoir accès au **détail du compte lié au produit de paiement [129]** Le porte-monnaie peut collecter et

[17] Consultez les précisions dans l'énoncé normalisé.
[18] OUI – seulement pour les échanges.
[19] OUI – seulement pour les échanges.

stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le **détail du compte lié au produit de paiement [130]**.

- **Produit de fidélisation, solde** – seuls l'**EJP** et l'**utilisateur final** ont accès au **solde du produit de fidélisation**. Aucun autre intervenant ne doit avoir accès au **solde du produit de fidélisation**. **[131]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le **solde du produit de fidélisation** [**132]**.
- **Produit de fidélisation, détail du compte** – seuls l'**EJP** et l'**utilisateur final** ont accès au **détail du compte lié au produit de fidélisation**. Aucun autre intervenant ne doit avoir accès au **détail du compte lié au produit de fidélisation**. **[133]** Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le **détail du compte lié au produit de fidélisation [134]**.

12.2 FRAUDE, LOGICIELS MALVEILLANTS ET SÉCURITÉ

La fraude et la sécurité représentent des préoccupations importantes dans le cadre des paiements mobiles. Même si ce document ne contient pas de normes précises en matière de fraude et de sécurité, il est recommandé que chaque participant à l'écosystème établisse des processus en vue d'assurer le suivi des problèmes de fraude et de sécurité et de les atténuer, particulièrement en ce qui concerne les logiciels malveillants ainsi que le piratage et le vol d'appareils mobiles.

Les participants à l'écosystème sont encouragés à travailler de concert pour combattre les risques en matière de sûreté et de sécurité auxquels fait face l'écosystème de paiements mobiles.

12.3 DONNÉES ET SÉCURITÉ – RÉSUMÉ

Cette section porte sur les questions liées aux données et à la sécurité. Elle a été conçue en fonction d'un principe général selon lequel chaque participant à l'écosystème ne doit avoir accès qu'au minimum d'information requis pour remplir son rôle principal.

Il est primordial que tous les participants à l'écosystème travaillent ensemble pour assurer le caractère sûr et sécuritaire des paiements mobiles.

12.4 ÉNONCÉS NORMALISÉS

Numéro	Énoncé	Section
87	Le but premier des participants à l'écosystème est de protéger les données de l'utilisateur final et du marchand. L'accès aux données ainsi que leur utilisation doivent être communiqués à l'utilisateur final, qui doit accorder explicitement son autorisation à cet effet.	12 Données et sécurité
88	Produits de paiement contenus dans le porte-monnaie – seuls le fournisseur de porte-monnaie et l'utilisateur final ont accès à la liste de produits de paiement contenue dans un porte-monnaie. Aucun autre intervenant ne doit avoir accès à la liste de produits de paiement. [Suite à l'EN89]	12.1.1 Accès aux données contenues dans le porte-monnaie
89	[Suite de l'EN88] L'accès du fournisseur de porte-monnaie à l'information liée aux produits de paiement doit se limiter à l'information nécessaire pour assurer la maintenance du porte-monnaie.	12.1.1 Accès aux données contenues dans le porte-monnaie
90	Produits de fidélisation contenus dans le porte-monnaie – seuls le fournisseur de porte-monnaie et l'utilisateur final ont accès à la liste de produits de fidélisation contenue dans un porte-monnaie. Aucun autre intervenant ne doit avoir accès à la liste de produits de fidélisation. [Suite à l'EN91]	12.1.1 Accès aux données contenues dans le porte-monnaie
91	[Suite de l'EN90] L'accès du fournisseur de porte-monnaie à l'information liée aux produits de fidélisation doit se limiter à l'information nécessaire pour assurer la maintenance du porte-monnaie.	12.1.1 Accès aux données contenues dans le porte-monnaie

Numéro	Énoncé	Section
92	Coupons contenus dans le porte-monnaie – seuls le fournisseur de porte-monnaie, l'utilisateur final et quelques autres applications de fidélisation approuvées par l'utilisateur final ont accès à la liste de coupons contenue dans un porte-monnaie. Aucun autre intervenant ne doit avoir accès à la liste de coupons.	12.1.1 Accès aux données contenues dans le porte-monnaie
93	Données non chiffrées liées au produit de paiement – seuls l'EJP, les marchands et l'utilisateur final ont accès aux données non chiffrées liées au produit de paiement. Aucun autre intervenant ne doit avoir accès aux données non chiffrées liées au produit de paiement. [Suite à l'EN94]	12.1.2 Accès aux données liées aux justificatifs
94	[Suite de l'EN93] Exemples de données financières non chiffrées liées aux produits de paiement : numéro de carte de crédit, nom figurant sur la carte et code de vérification de carte. Les marchands ont accès à ces renseignements uniquement dans le cadre du traitement du paiement. La collecte et le stockage de données non chiffrées liées aux produits de paiement par les marchands doivent être conformes aux lignes directrices du réseau de paiement.	12.1.2 Accès aux données liées aux justificatifs
95	Données chiffrées liées au produit de paiement – seul l'EJP a accès aux données chiffrées liées au produit de paiement. Aucun autre intervenant ne doit avoir accès aux données chiffrées liées au produit de paiement.	12.1.2 Accès aux données liées aux justificatifs
96	Données non chiffrées associées aux justificatifs liés aux programmes de fidélisation – seuls le responsable du programme de fidélisation, les marchands et l'utilisateur final ont accès aux données non chiffrées associées aux justificatifs liés aux programmes de fidélisation. Aucun autre intervenant ne doit avoir accès aux données non chiffrées associées aux justificatifs liés aux programmes de fidélisation. [Suite à l'EN97]	12.1.2 Accès aux données liées aux justificatifs
97	[Suite de l'EN96] Les données non chiffrées associées aux justificatifs liés aux programmes de fidélisation collectées et stockées par les marchands doivent être traitées de la même manière que les justificatifs de paiement. De plus, ces données ne doivent servir qu'à l'octroi de récompenses et à l'échange de points de fidélisation.	12.1.2 Accès aux données liées aux justificatifs
98	Données chiffrées associées aux justificatifs liés aux programmes de fidélisation – si des points de fidélisation sont échangés au PDV, seul le responsable du programme de fidélisation a accès aux données chiffrées associées aux justificatifs liés aux programmes de fidélisation. Aucun autre intervenant ne doit avoir accès aux données chiffrées associées aux justificatifs liés aux programmes de fidélisation.	12.1.2 Accès aux données liées aux justificatifs

Numéro	Énoncé	Section
99	Données financières, montant – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final ont accès au montant de la transaction. Aucun autre intervenant ne doit avoir accès au montant de la transaction. [Suite à l'EN100]	12.1.3 Accès aux données financières
100	[Suite de l'EN99] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le montant de la transaction.	12.1.3 Accès aux données financières
101	Données financières, heure – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final ont accès à l'heure de la transaction. Aucun autre intervenant ne doit avoir accès à l'heure de la transaction. [Suite à l'EN102]	12.1.3 Accès aux données financières
102	[Suite de l'EN101] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer l'heure de la transaction.	12.1.3 Accès aux données financières
103	Données financières, marchand – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final peuvent connaître l'identité du marchand ayant effectué la transaction. Aucun autre intervenant ne doit connaître l'identité du marchand ayant effectué la transaction. [Suite à l'EN104]	12.1.3 Accès aux données financières
104	[Suite de l'EN103] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer l'identité du marchand ayant effectué la transaction.	12.1.3 Accès aux données financières
105	Données financières, produit – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final ont accès au produit utilisé pour effectuer une transaction. Aucun autre intervenant ne doit avoir accès au produit utilisé pour effectuer une transaction. [Suite à l'EN106]	12.1.3 Accès aux données financières
106	[Suite de l'EN105] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le produit utilisé pour effectuer une transaction.	12.1.3 Accès aux données financières
107	Données financières, lieu – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final ont accès au lieu de la	12.1.3 Accès aux données

Numéro	Énoncé	Section
	transaction. Aucun autre intervenant ne doit avoir accès au lieu de la transaction. [Suite à l'EN108]	financières
108	[Suite de l'EN107] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le lieu de la transaction.	12.1.3 Accès aux données financières
109	Données financières, détail de la transaction – seuls le marchand et l'utilisateur final ont accès au détail de la transaction (p. ex., numéro d'article). Aucun autre intervenant ne doit avoir accès au détail de la transaction. [Suite à l'EN110]	12.1.3 Accès aux données financières
110	[Suite de l'EN109] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et le marchant accordent explicitement leur autorisation de communiquer le détail de la transaction.	12.1.3 Accès aux données financières
111	Données financières, reçus électroniques – seuls le marchand et l'utilisateur final ont accès aux reçus électroniques liés à une transaction. Aucun autre intervenant ne doit avoir accès aux reçus électroniques. [Suite à l'EN112]	12.1.3 Accès aux données financières
112	[Suite de l'EN111] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de transmettre les reçus électroniques.	12.1.3 Accès aux données financières
113	Données liées aux programmes de fidélisation, montant – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final ont accès au montant d'une transaction de fidélisation. Aucun autre intervenant ne doit avoir accès au montant d'une transaction de fidélisation. [Suite à l'EN114]	12.1.4 Accès aux données liées aux programmes de fidélisation
114	[Suite de l'EN113] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le montant d'une transaction de fidélisation.	12.1.4 Accès aux données liées aux programmes de fidélisation

Numéro	Énoncé	Section
115	Données liées aux programmes de fidélisation, heure – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final ont accès à l'heure d'exécution d'une transaction de fidélisation. Aucun autre intervenant ne doit avoir accès à l'heure d'exécution d'une transaction de fidélisation. [Suite à l'EN116]	12.1.4 Accès aux données liées aux programmes de fidélisation
116	[Suite de l'EN115] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer l'heure d'exécution d'une transaction de fidélisation.	12.1.4 Accès aux données liées aux programmes de fidélisation
117	Données liées aux programmes de fidélisation, marchand – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final peuvent connaître l'identité du marchand ayant effectué la transaction de fidélisation. Aucun autre intervenant ne doit connaître l'identité du marchand ayant effectué la transaction de fidélisation. [Suite à l'EN118]	12.1.4 Accès aux données liées aux programmes de fidélisation
118	[Suite de l'EN117] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer l'identité du marchand ayant effectué la transaction de fidélisation.	12.1.4 Accès aux données liées aux programmes de fidélisation
119	Données liées aux programmes de fidélisation, produit – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final peuvent connaître le produit utilisé pour effectuer une transaction de fidélisation. Aucun autre intervenant ne doit connaître le produit utilisé pour effectuer une transaction de fidélisation. [Suite à l'EN120]	12.1.4 Accès aux données liées aux programmes de fidélisation
120	[Suite de l'EN119] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le produit utilisé pour effectuer une transaction de fidélisation.	12.1.4 Accès aux données liées aux programmes de fidélisation
121	Données liées aux programmes de fidélisation, lieu – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final peuvent connaître le lieu d'exécution d'une transaction de fidélisation. Aucun autre intervenant ne doit connaître le lieu d'exécution d'une transaction de fidélisation. [Suite à l'EN122]	12.1.4 Accès aux données liées aux programmes de fidélisation

Numéro	Énoncé	Section
122	[Suite de l'EN121] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le lieu d'exécution d'une transaction de fidélisation.	12.1.4 Accès aux données liées aux programmes de fidélisation
123	Données liées aux programmes de fidélisation, détail de la transaction – seuls le marchand et l'utilisateur final ont accès au détail de la transaction de fidélisation (p. ex., numéro d'article). Aucun autre intervenant ne doit avoir accès au détail de la transaction de fidélisation. [Suite à l'EN124]	12.1.4 Accès aux données liées aux programmes de fidélisation
124	[Suite de l'EN 123]. Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le détail de la transaction de fidélisation.	12.1.4 Accès aux données liées aux programmes de fidélisation
125	Données liées aux programmes de fidélisation, reçus électroniques – seuls le marchand et l'utilisateur final ont accès aux reçus électroniques liés à une transaction de fidélisation. Aucun autre intervenant ne doit avoir accès aux reçus électroniques liés à une transaction de fidélisation. [Suite à l'EN126]	12.1.4 Accès aux données liées aux programmes de fidélisation
126	[Suite de l'EN125] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de transmettre les reçus électroniques liés à une transaction de fidélisation.	12.1.4 Accès aux données liées aux programmes de fidélisation
127	Produit de paiement, solde – seuls l'EJP et l'utilisateur final ont accès au solde du produit de paiement. Aucun autre intervenant ne doit avoir accès au solde du produit de paiement. [Suite à l'EN128]	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation
128	[Suite de l'EN127] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le solde du produit de paiement.	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation

Numéro	Énoncé	Section
129	Produit de paiement, détail du compte – seuls l'EJP et l'utilisateur final ont accès au détail du compte lié au produit de paiement. Aucun autre intervenant ne doit avoir accès au détail du compte lié au produit de paiement. [Suite à l'EN130]	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation
130	[Suite de l'EN129] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le détail du compte lié au produit de paiement.	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation
131	Produit de fidélisation, solde – seuls l'EJP et l'utilisateur final ont accès au solde du produit de fidélisation. Aucun autre intervenant ne doit avoir accès au solde du produit de fidélisation. [Suite à l'EN132]	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation
132	[Suite de l'EN131] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le solde du produit de fidélisation.	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation
133	Produit de fidélisation, détail du compte – seuls l'EJP et l'utilisateur final ont accès au détail du compte lié au produit de fidélisation. Aucun autre intervenant ne doit avoir accès au détail du compte lié au produit de fidélisation. [Suite à l'EN134]	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation
134	[Suite de l'EN133] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le détail du compte lié au produit de fidélisation.	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation

13 RÉSUMÉ DU DOCUMENT

Le Modèle de référence des paiements mobiles NFC contenu dans le présent document établit une série d'attentes à l'égard des participants à l'écosystème. Ces attentes et les interactions connexes jettent des bases communes qui permettront d'offrir des services de paiement mobile NFC au Canada.

Tous les participants à l'écosystème doivent décider s'ils souhaitent appliquer ces normes. S'ils choisissent de le faire, ils s'engagent non seulement à les respecter, mais aussi à mettre en place un écosystème de paiements mobiles ouvert, sûr et sécuritaire au Canada.

14 GLOSSAIRE

Termes	Définition
Acquéreur ou réseau acquéreur	Désigne une institution qui traite les paiements par carte de débit ou de crédit au nom d'un marchand.
Magasin d'applications	Magasin chargé de la distribution d'applications destinées à l'appareil mobile de l'utilisateur final.
Modèle de référence des paiements mobiles NFC au Canada	Désigne le présent document.
Paiement en nuage	Type de paiement permettant de stocker des justificatifs à distance. Pour qu'un utilisateur final puisse effectuer un paiement en nuage, il doit utiliser des logiciels et se connecter à des serveurs à distance. Les paiements en nuage NE SONT PAS abordés dans ce document.
Porte-monnaie collectif (Collective Wallet)	Porte-monnaie mobile conçu par un groupe d'EJP pour faire en sorte que seuls les justificatifs de paiement de ce groupe puissent y être associés pour effectuer des paiements mobiles NFC.
Application compagnon (Companion Application)	Une application compagnon est liée à une application de paiement pour en accroître les fonctionnalités (p. ex., gestion des codes personnels ou registre des transactions). L'application compagnon est fournie à la discrétion de l'installateur de l'application de paiement.
Sans contact	Méthode de communication qui n'exige pas de contact physique entre deux appareils (consultez la définition de « Communication en champ proche » pour en savoir plus).
Autocollant sans contact	Autocollant faisant appel à la technologie NFC pour transférer de l'information.
Autorité de contrôle (AC)	L'AC gère les principaux échanges effectués relativement à un « porte-monnaie ouvert ». Il s'agit ici d'un modèle qui est reconnu dans le cadre du modèle de référence des paiements mobiles NFC, mais qui n'est pas obligatoire. Ce modèle est considéré comme étant une solution de rechange aux relations de type « plusieurs à plusieurs » entre le GSC d'un émetteur de justificatifs de paiement et le GSC d'un gestionnaire de domaine sécurisé.
Justificatif	Désigne les renseignements chiffrés associés à un produit de paiement précis.

Termes	Définition
Émetteur de justificatifs de paiement (EJP)	Organisme chargé de la création et de la maintenance du produit de paiement.
Méthode de vérification des cartes (MVC)	Méthode visant à s'assurer que la personne qui présente la carte (par l'entremise de l'appareil mobile) est bel et bien la personne à qui la carte a été délivrée.
Code de vérification de carte	Désigne le code de trois chiffres imprimé au dos de la carte de crédit.
Par défaut	Expression visant une application ou des justificatifs de paiement configurés pour être utilisés dans le cadre d'une transaction, sauf si l'utilisateur final choisit une application ou des justificatifs de paiement différents.
Mode de délégation	En mode de délégation, l'ERM ou le GDS loue une section de l'élément sécurisé à l'émetteur de justificatifs ou lui donne accès à cette section. L'ERM ou le GDS demeure propriétaire de l'élément sécurisé et décide quelles applications peuvent être installées dans l'élément sécurisé. L'ERM ou le GDS et l'émetteur de justificatifs (ou l'installateur de justificatifs) échangent des clés permettant d'accéder à l'élément sécurisé.
Logiciel de l'appareil (Device Software)	Lorsqu'une application de paiement et des justificatifs de paiement sont stockés dans l'élément sécurisé intégré, le logiciel de l'appareil joue le rôle d'application parapluie (voir ci-dessous) en vue de localiser les justificatifs de paiement et de les associer au contrôleur NFC.
Mode bimodal	En mode bimodal, l'ERM ou le GDS vend une section de l'élément sécurisé à l'émetteur de justificatifs. Ce dernier détient alors à part entière les droits d'accès relatifs à cette section de l'élément sécurisé. Dans le cadre de la vente, l'ERM ou le GDS et l'émetteur de justificatifs (ou l'installateur de justificatifs) échangent des clés d'accès. L'émetteur de justificatifs peut donc installer toutes les applications qu'il désire dans la section de l'élément sécurisé qui lui appartient, sans avoir besoin de la permission de l'ERM ou du GDS.
Participants à l'écosystème	Organismes ou personnes jouant un rôle officiel dans le cadre de l'écosystème de paiements mobiles (p. ex., en offrant ou en utilisant des services de paiement mobile).
Reçu électronique	Reçu remis et sauvegardé sous forme de données numériques, sans

Termes	Définition
	qu'il n'y ait de reçu imprimé.
Utilisateur final	(*aussi appelé client*) Désigne le consommateur de services de paiement et de connectivité mobiles.
Paiement à risque élevé	Type de paiement qui satisfait à des critères de risque établis par les réseaux de paiement ou les EJP. Les paiements à risque élevés sont assujettis à des MVC plus élaborées.
Paiement de valeur élevée	Paiement dépassant certains critères de valeur établis par les réseaux de paiement ou les EJP ou une combinaison de critères de valeur et de catégorie de dépenses. Les paiements de valeur élevée sont assujettis à des MVC plus élaborées.
Participants à l'initiative	Organismes engagés dans l'élaboration de normes et de principes directeurs visant les paiements mobiles au Canada. Les organismes suivants ont participé à l'élaboration du présent document : Banque de Montréal (BMO), Banque Nationale du Canada (BNC), Banque Canadienne Impériale de Commerce (CIBC), Centrale des caisses de crédit du Canada (CCCC), Desjardins, Banque Royale du Canada (RBC), La Banque de Nouvelle-Écosse (Banque Scotia), La Banque Toronto-Dominion (TD).
Fournisseur de services de fidélisation	Administrateur de programmes de fidélisation et de récompenses.
Marchand	Désigne le fournisseur de biens ou de services en échange desquels l'utilisateur final effectue un paiement.
Carte microSD	Carte mémoire conçue pour être utilisée avec des téléphones cellulaires et d'autres appareils mobiles.
Appareil mobile	Téléphone intelligent doté de certaines fonctionnalités semblables à celles d'une tablette électronique. Ce document ne porte que sur les appareils mobiles compatibles avec la technologie NFC. Dans ce document, « appareil » est utilisé comme synonyme d'« appareil mobile ».
Exploitant de réseau mobile (ERM)	Fournisseur de services de connectivité associés à des appareils mobiles. Aux fins du présent document, ce rôle est parfois employé de manière interchangeable avec celui du FMO et du GDS.

Termes	Définition
Communication en champ proche (NFC)	La communication en champ proche permet la réalisation de transactions simplifiées, l'échange de données et l'établissement de connexions sans fil entre deux appareils situés à proximité, habituellement à une distance approximative d'au plus dix centimètres. Les transactions de paiement mobile NFC sont exécutées conformément à la norme ISO 14443 (cartes à puce de type A ou de type B).
Contrôleur NFC (NFC Controller)	Désigne le matériel et le logiciel qui, ensemble, contrôlent les radio signaux NFC transmis en provenance et à destination de l'appareil mobile.
Porte-monnaie ouvert (Open Wallet)	Porte-monnaie mobile conçu pour faire en sorte que les justificatifs de paiement de plusieurs EJP puissent y être associés pour effectuer des paiements mobiles NFC. Même s'il est « ouvert », ce type de porte-monnaie exige néanmoins la conclusion d'ententes et l'établissement de relations commerciales entre les EJP et les fournisseurs de porte-monnaie avant que des justificatifs de paiement puissent être associés à un porte-monnaie.
Volume opérationnel	Désigne la portée de la radiofréquence NFC d'un appareil mobile, à des fins de communication et de maintenance.
Fabricant de matériel d'origine (FMO)	Le FMO fabrique l'appareil mobile utilisé par l'utilisateur final. Aux fins du présent document, ce rôle est parfois employé de manière interchangeable avec celui du ERM et du GDS.
Radiofréquence	Moyen de transmission de données à l'aide d'un réseau sans fil.
PAN	(primary account number) Numéro de compte primaire composé de 16 chiffres : numéro d'identification de l'émetteur de 6 chiffres (NII), dont le premier désigne l'identificateur de la principale activité économique (MII); un identificateur de compte individuel de longueur variable (jusqu'à 12 chiffres); un numéro unique de vérification.
Mot de passe	L'utilisateur final saisit un mot de passe dans son appareil mobile dans le cadre d'une méthode de vérification de cartes.
Application de paiement (Payment Application)	Une application de paiement permet de satisfaire aux exigences de sécurité en vue d'effectuer un paiement et de stocker les justificatifs de paiement.
Émetteur de justificatifs de paiement (EJP)	(*ou propriétaire de l'application de paiement*) L'EJP est responsable du chiffrement, de la sûreté et de la sécurité des justificatifs de paiement. La relation entre l'utilisateur final et l'EJP repose sur une

Termes	Définition
	offre de produits et de services financiers.
Réseau de paiement	Cet intervenant, aussi appelé *créateur de l'application de paiement*, crée une application de paiement qui n'est pas destinée à l'utilisateur final, en plus de gérer le réseau de paiement *(p. ex., Visa, MasterCard, Interac, etc.).*
Groupe de travail sur l'examen du système de paiement du gouvernement du Canada	Le groupe de travail a été formé en 2011 par le gouvernement canadien pour évaluer l'avenir du système de paiement au pays.
Paiements entre homologues	Paiements réalisés directement entre deux utilisateurs finaux; aucun marchand ne participe à ce type de transaction.
Point de vente (PDV)	Désigne le matériel utilisé par le marchand pour obtenir les justificatifs de paiement dans le cadre d'une transaction.
Application de TPV	Le terminal de point de vente contient une application de paiement conforme aux spécifications de paiement sans contact MasterCard PayPass, Visa PayWave ou à d'autres normes locales.
Terminal de point de vente (TPV)	Expression générique désignant le terminal utilisé par le marchand pour exécuter et traiter une transaction financière en communiquant avec l'appareil mobile de l'utilisateur final.
Porte-monnaie exclusif (Proprietary Wallet)	Porte-monnaie mobile conçu pour faire en sorte que seuls les justificatifs de paiement du fournisseur de porte-monnaie puissent y être associés pour effectuer des paiements mobiles NFC.
Transaction de remise d'achat	Transaction de retour de marchandises effectuée au PDV. Domaine sécurisé
Domaine sécurisé (Secure Domain)	Subdivision de l'élément sécurisé.
Gestionnaire de domaine sécurisé (GDS)	Le GDS gère l'accès à l'élément sécurisé. Ce rôle est souvent combiné avec celui d'ERM, mais pas toujours. Aux fins du présent document, ce rôle est parfois employé de manière interchangeable avec celui du ERM et du FMO.
Élément sécurisé (Secure Element)	(Secure Element) Désigne la zone sécurisée intégrée ou la zone sécurisée de l'UICC où est stockée l'information chiffrée.

Termes	Définition
Clés sécurisées	La délivrance de clés sécurisées est une variante du chiffrement à base de pièces d'identité. Les clés sécurisées permettent de réduire le degré de confiance devant être accordé à un tiers en le répartissant entre plusieurs tiers.
Fournisseur de services	Le fournisseur de services désigne une banque, une société de transport, un détaillant, etc., qui fournit des services prenant en charge les paiements mobiles NFC.
Carte SIM	Carte d'identification d'abonné.
Mode simple	En mode simple, l'ERM ou le GDS autorise l'émetteur de justificatifs à utiliser son domaine sécurisé pour l'hébergement de l'application de paiement. Le droit d'accès au domaine sécurisé demeure la propriété de l'ERM ou du GDS. Toute mise à jour ou modification de l'application de paiement doit être effectuée par l'entremise du GDS ou de l'ERM.
Jeton d'authentification	Valeur chiffrée fournie par l'émetteur d'une carte pour prouver qu'une activité de délégation a été autorisée.
Transaction	Désigne l'exécution d'un paiement de proximité sans contact entre un PDV et un appareil mobile. Une transaction comprend l'achat au PDV et le traitement de l'autorisation et des messages connexes.
Gestionnaire de service de confiance (GSC)	(*aussi appelé application de paiement ou installateur de justificatifs de paiement*) Cet intervenant installe les justificatifs de paiement dans l'élément sécurisé.
UICC	L'UICC (Universal Integrated Circuit Card ou carte universelle à circuits intégrés) désigne la carte à puce utilisée dans des terminaux mobiles, sur des réseaux GSM et UMTS, conformément aux définitions du European Telecommunications Standards Institute (ETSI Project Smart Card Platform [EP SCP]).
Application parapluie (Umbrella Application)	Une application parapluie est utilisée uniquement lorsqu'une application de paiement est stockée dans l'UICC. L'application parapluie permet la communication entre un porte-monnaie et toutes les applications de paiement associées à ce porte-monnaie. La relation entre l'application parapluie et les applications de paiement est une relation de type « un à plusieurs ». Dans le cas d'un élément sécurisé intégré, c'est le logiciel de l'appareil qui joue ce rôle.

Termes	Définition
Application porte-monnaie ou porte-monnaie	Le porte-monnaie mobile désigne l'application destinée à l'utilisateur final, c'est-à-dire celle qui doit être installée sur l'appareil mobile. L'application permet à l'utilisateur de saisir et de gérer des renseignements précis liés à son compte, qui seront utilisés dans le cadre d'une transaction mobile NFC. Un appareil mobile peut contenir un ou plusieurs porte-monnaie mobiles à la fois, en tout temps.
Fournisseur de porte-monnaie	Le fournisseur de porte-monnaie fournit l'interface destinée à l'utilisateur final (p. ex., Google Wallet, ISIS, Visa, MasterCard, institutions financières ou autres tiers).

15 RÉFÉRENCES

Le présent document est fondé sur un ensemble de normes récemment créées dans le domaine des paiements mobiles NFC. Ces normes comprennent les documents ci-dessous :

- GlobalPlatform System Messaging Specification for Management of Mobile-NFC Services v1.0
- The GlobalPlatform Proposition for NFC Mobile: Secure Element Management & Messaging (White Paper)
- GSMA – Mobile NFC Technical Guidelines
- 101203 – AFSCM TECH – LIVBL – Interface Specification – V1.2.1
- Règlements Visa à l'intention des marchands
- http://techcrunch.com/2009/12/01/square-receipt/

15.1 RÉFÉRENCES ISO[20]

Norme	Description
ISO-1	ISO/IEC 7816-1: 1998/Amd 1:2003 Cartes d'identification – Cartes à circuit intégré – Partie 1 : Cartes à contacts – Caractéristiques physiques
ISO-2	ISO/IEC 7816-2:2007 Cartes d'identification – Cartes à circuit intégré – Partie 2 : Cartes à contacts – Dimensions et emplacements des contacts
ISO-3	ISO/IEC 7816-3:2006 Cartes d'identification – Cartes à circuit intégré – Partie 3 : Cartes à contacts – Interface électrique et protocoles de transmission
ISO-4	ISO/IEC 7816-4:2005 Cartes d'identification – Cartes à circuit intégré – Partie 4 : Cartes à contacts – Organisation, sécurité et commandes pour les échanges
ISO-5	ISO/IEC 7816-5:2004 Cartes d'identification – Cartes à circuit intégré – Partie 5 : Cartes à contacts – Enregistrement des fournisseurs d'application

[20] PayEz

Norme	Description
ISO-6	ISO/IEC 7816-6:2004/Cor 1: 2006 Cartes d'identification – Cartes à circuit intégré – Partie 6 : Cartes à contacts – Éléments de données intersectoriels pour les échanges
ISO-7	ISO/IEC 7816-15 Cartes d'identification – Cartes à circuit intégré – Partie 15 : Cartes à contacts – Application des informations cryptographiques
ISO-8	ISO/IEC 14443-3:2001 Cartes d'identification – Cartes à circuit(s) intégré(s) sans contact – Cartes de proximité – Partie 3 : Initialisation et anticollision
ISO-9	ISO/IEC 14443-4:2001 Cartes d'identification – Cartes à circuit(s) intégré(s) sans contact – Cartes de proximité – Partie 4 : Protocole de transmission

15.2 RÉFÉRENCES DE GSM[21]

Norme	Description
GSM-1	3GPP 31-111: Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)
GSM-2	3GPP 31-115: Secured packet structure for (Universal) Subscriber Identity Module (U) SIM Toolkit applications
GSM-3	3GPP 31-116: Remote APDU Structure for (Universal) Subscriber Identity Module (U) SIM Toolkit applications
GSM-4	3GPP TS 23.040: Technical realization of Short Message Service (SMS)
GSM-5	SGPP TS 23.048: Security mechanisms for the (U)SIM application toolkit; Stage 2
GSM-6	GSM 11.11: Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) Interface

[21] PayEz

15.3 RÉFÉRENCES DE L'ETSI[22]

Norme	Description
ETSI-1	ETSI TS 102-223: Smart Cards; Card Application Toolkit (CAT)
ETSI-2	ETSI TS 102 225: Secured packet structure for UICC applications
ETSI-3	ETSI TS 102 226: Remote APDU Structure for UICC based Applications
ETSI-4	ETSI TS 102 484 (Release 7): Smart Cards; Secure channel between a UICC and an end-point terminal
ETSI-5	ETSI TS 102 613 (Release 9): Smart Cards; UICC – Contactless Front-end (CLF) Interface Part 1: Physical and data link layer characteristics
ETSI-6	ETSI TS 102 622 (Release 10): Smart Cards UICC Contactless Front-end Interface (CLF): Host Controller Interface (HCI)
ETSI-7	ETSI TS 102 127: Reservation of CAT-TP <<well-known>> ports for standard applications

15.4 RÉFÉRENCES DE GLOBALPLATFORM[23]

Norme	Description
GP-1	GlobalPlatform Specification v2.2 – Mars 2006
GP-2	GlobalPlatform Specification v2.2 – Release Notes – 25 mars 2006
GP-3	GlobalPlatform Card – Confidential Card Content Management v1.0 (Amendment A) – Octobre 2007
GP-4	GlobalPlatform Specification 2.2 – UICC Configuration v1.0 – Octobre 2008
GP-5	GlobalPlatform Specification 2.2 – Contactless Services v1.0 (Amendment C) – Février 2010
GP-6	GlobalPlatform Key Management System Functional Requirements 1.0 – Novembre 2003
GP-7	GlobalPlatform Smart Card Management System Functional Requirements Version 4.0 21 décembre 2004

[22] PayEz
[23] PayEz.

15.5 RÉFÉRENCES JAVA[24]

Norme	Description
JAVA-1	Java Card Specifications v2.2.2
JAVA-2	JSR 118: Mobile Information Device Profile v2.1
JAVA-3	JSR 177: Security and Trust Services API for J2ME v1.0.1
JAVA-4	JSR 257: Contactless Communication API v1.1
JAVA-5	JSR 211: Content Handler API (CHAPI) v1.0.1

15.6 RÉFÉRENCES D'EMVCO[25]

Norme	Description
EMV-1	EMVCo – EMV Integrated Circuit Card Specifications for Payment Systems – Book 1, Application Independent ICC to Terminal Interface Requirements V4.2
EMV-2	EMVCo – EMV Integrated Circuit Card Specifications for Payment Systems – Book 2, Security and Key Management V4.2
EMV-3	EMVCo – EMV Integrated Circuit Card Specifications for Payment Systems – Book 3, Application Specifications V4.2
EMV-4	EMVCo – EMV Integrated Circuit Card Specifications for Payment Systems – Book 4, Cardholder, Attendant, and Acquirer Interface Requirements V4.2
EMV-5	EMV Contactless Specifications for Payment Systems Framework for Contactless Evolution V1.0 – Octobre 2007
EMV-6	EMVCo – EMV Contactless Specification for Payment – Entry Point V1.0 – Mai 2008
EMV-7	EMVCo Contactless Indicator Reproduction Standards for Cards and Payment Devices – Dernière mise à jour : 31 mai 2007
EMV-8	EMVCo Contactless Symbol at POS Specifications Reproduction Specifications – Last Revised 06.01.07

[24] PayEz.
[25] PayEz.

Norme	Description
EMV-9	EMVCo – EMV Card Personalization Specification V1.1 – Juillet 2007
EMV-10	EMVCo – PayPass – ISO/IEC 14443 Implementation Specification V1.1 – Mars 2006
EMV-11	EMVCo – Contactless Mobile Payment Architecture Overview v1.0 – Juin 2010
EMV-12	EMVCo – Handset Requirements for Contactless Mobile Payment V1.0 – Juin 2010
EMV-13	EMVCo – Application Activation User Interface – Overview, Usage Guidelines and PPSE Requirements V1.0 – Décembre 2010
EMV-14	EMVCo – EMV Profile of GlobalPlatform UICC Configuration v1.0 – Décembre 2010

15.7 RÉFÉRENCES DU EPC[26]

Norme	Description
EPC-1	SEPA Cards Framework Version 2.1 – Décembre 2009
EPC-2	SEPA cards standardization volume – book of requirements Payments and Withdrawals with Cards in SEPA: Applicable Standards and Certification Process Version 4.0 – Décembre 2009
EPC-3	EPC – GSMA – Trusted Service Manager – Service Management Requirements and Specifications – Version 1.0 – Janvier 2010

15.8 RÉFÉRENCES DE PAYEZ MOBILE[27]

Norme	Description
PM-1	Part I: Product Definition v1.0 – Avril 2011
PM-2	Part II: Technical Specification v1.0 – Avril 2011

[26] PayEz.
[27] PayEz.

Norme	Description
PM-3	Security Guidelines for Standard Operational Environment v1.0 – Juin 2009
PM-4	Guidance for Payment Application Package Security Target v2.1 – Juillet 2009
PM-5	(U)SIM Java Card TM Platform Protection Profile v2.0 – Juillet 2010
PM-6	Payez *Mobile* MasterCard Implementation Guide – Avril 2011
PM-7	Payez *Mobile* Visa Implementation Guide – Avril 2011

15.9 RÉFÉRENCES DE AFSCM[28]

Norme	Description
AFSCM-1	Guidelines for Interconnection of Service Providers' and MNOs' Information Systems – Current document v1.0
AFSCM-2	Interface Specification between Telecom Operators and NFC Services Providers v1.1
AFSCM-3	Rules and Recommendations for MIDLet Design and Development v1.0
AFSCM-4	Cardlet Development Guideline v1.0

[28] PayEz

16 SÉLECTION DE LA MÉTHODE DE VÉRIFICATION DE CARTES – RÉSUMÉ

Cette section présente les choix pris en considération dans la détermination de la méthode de vérification de cartes. La méthode « tapez et confirmez » a été choisie comme la méthode la plus appropriée dans le cadre des paiements mobiles NFC au Canada.

Méthode	Répercussions	Avantages	Désavantages
Tapez et partez (Exploitant de réseau mobile – radio-fréquences)	• Expérience utilisateur cohérente pour les transactions de valeur élevée ou faible • Meilleure option du point de vue de l'utilisateur final	• Commodité : une seule tape • Expérience similaire à celle des méthodes de paiement sans contact actuelles • Compatibilité avec d'autres porte-monnaie mobiles	• Exige une connectivité cellulaire à des fins de saisie du mot de passe et de confirmation • L'utilisateur final paie des frais supplémentaires liés aux données
Tapez et partez (PDV du marchand)	• Expérience utilisateur cohérente pour les transactions de valeur élevée ou faible	• Commodité : une seule tape	• Nécessité d'interagir avec deux interfaces • Exige une connectivité cellulaire à des fins de confirmation • L'utilisateur final paie des frais supplémentaires liés aux données
Tapez et confirmez (méthode approuvée)	• Nécessité d'informer l'utilisateur final sur la manière d'effectuer des transactions de valeur élevée • Utilisation équilibrée de la technologie NFC et des radiofréquences	• Conforme aux normes européennes • Confirmation du mot de passe effectuée par NFC	• Exige une connectivité par radiofréquences aux fins de confirmation et de mise à jour • Aucune mise à jour par NFC

Méthode	Répercussions	Avantages	Désavantages
Tapez, confirmez et reconfirmez	• Bonne méthode dans le cas d'un modèle fondé uniquement sur la technologie NFC • Répercussions sur l'expérience de l'utilisateur final	• Aucune nécessité de faire appel aux radiofréquences dans le cas de transactions de valeur élevée • L'appareil mobile peut être utilisé sans recourir à la connectivité cellulaire	• Trois touches requises : transaction longue • Les trois touches peuvent créer de la confusion chez l'utilisateur final
Tapez et branchez-vous	• Difficulté à maintenir la connectivité bidirectionnelle, car l'appareil mobile doit être maintenu à une distance de 10 cm du PDV NFC	• Expérience de l'utilisateur final transparente et cohérente dans le cadre de transactions de faible valeur	• L'appareil mobile doit être tenu très près du lecteur pendant toute la durée de la transaction • Utilisation accrue de la pile de l'appareil
Tapez et explorez	• Le marchand peut moduler l'expérience de l'utilisateur final, lui offrir des coupons et lui proposer des offres promotionnelles	• Expérience plus riche du point de vue de l'utilisateur final : possibilité de choisir parmi plusieurs méthodes de paiement et programmes de fidélisation	• Transaction longue • Les fournisseurs de porte-monnaie et les EJP n'ont pas d'avantage associé à l'utilisation de cette méthode

17 ÉNONCÉS NORMALISÉS

Certains énoncés normalisés peuvent être répétés si des concepts sont abordés dans des sections distinctes du document. À des fins de clarification et pour connaître le contexte, les sections pertinentes du document devraient être consultées.

Numéro	Énoncé	Section
1	Les règles de valorisation de la marque établies par les réseaux de paiement doivent être respectées.	6.1 Règles de valorisation de la marque
2	Dans le cas de transactions sans contact effectuées au moyen de MasterCard PayPass, les spécifications relatives à l'appareil mobile et au lecteur sans contact doivent prendre en charge le profil PayPass Mag Stripe, tel que défini dans les spécifications PayPass Mag Stripe, ainsi que le profil Pass M/Chip ou Mobile M/Chip, tel que défini dans les spécifications PayPass M/Chip.	6.2 Exigences relatives aux sociétés offrant des services de paiement mobile sans contact

Numéro	Énoncé	Section
3	Dans le cas de transactions sans contact effectuées au moyen de Visa PayWave, les spécifications relatives à l'appareil mobile et au lecteur sans contact doivent prendre en charge les modes MSD, VMPA et qVSDC tels que définis dans les spécifications Visa Mobile.	6.2 Exigences relatives aux sociétés offrant des services de paiement mobile sans contact
4	Dans le cas de transactions sans contact effectuées au moyen de Flash Interac, l'appareil mobile et le lecteur sans contact doivent être conformes aux spécifications Interac Flash Mobile.	6.2 Exigences relatives aux sociétés offrant des services de paiement mobile sans contact
5	Les autres règles opérationnelles applicables doivent être établies en fonction du même réseau d'autorisation et du même système de compensation que les transactions standards par carte de débit ou de crédit.	6.3 Exigences relatives au traitement des transactions
6	Le mode émulation de carte NFC doit être utilisé pour exécuter une transaction de paiement mobile sans contact entre l'appareil mobile de l'utilisateur final et un lecteur sans contact du marchand, au moyen d'une couche de communication liée à une radiofréquence respectant la norme ISO 14443 (cartes à puce de type A ou de type B).	6.7 NFC
7	Le présent document et les normes de GlobalPlatform tiennent compte des trois modes ci-dessus (mode simple, mode de délégation et mode bimodal); cependant, les organismes qui adoptent les présentes normes ne doivent utiliser que le mode de délégation ou le mode bimodal, tels que définis par GlobalPlatform.	De la même façon, les GSC ne doivent utiliser que le mode de délégation ou le mode bimodal.
8	Si le participant à l'écosystème doit accéder à des données, obtenues au moyen d'un appareil mobile, au-delà de la limite permise afin de remplir son rôle principal, l'utilisateur final doit en être informé et il doit accorder explicitement son autorisation à cet effet.	7.2 Modèle de référence des paiements mobiles NFC – Description de la solution
9	Pour des raisons de sécurité et de prévention de la fraude, si le participant à l'écosystème doit accéder à des données, obtenues au moyen d'un appareil mobile, au-delà de la limite permise afin de remplir son rôle principal, l'émetteur de justificatifs doit également en être informé et ce dernier doit lui aussi accorder explicitement son autorisation à cet effet.	7.2 Modèle de référence des paiements mobiles NFC – Description de la solution
10	Les appareils mobiles doivent respecter les lignes directrices relatives aux réseaux de paiements et à la certification des ERM.	7.5 Aperçu des logiciels et des appareils
11	L'appareil mobile doit pouvoir accepter la réalisation d'activités d'installation de justificatifs et de maintenance, par l'entremise de radiofréquences.	7.5 Aperçu des logiciels et des appareils

Numéro	Énoncé	Section
12	Les lecteurs sans contact au PDV doivent être conformes aux spécifications de paiement sans contact d'EMVCo [EMV-6] ainsi qu'à celles de MasterCard et/ou Visa et/ou Interac.	7.6 Exigences relatives au lecteur sans contact/PDV
13	Afin de respecter les objectifs en matière d'ouverture et d'interopérabilité, les porte-monnaie mobiles, les ERM, les FMO, les GDS et les EJP ne doivent pas limiter l'accès à des applications de paiement liées aux éléments ci-dessous : • produits de paiement par carte de débit • produits de paiement par carte de crédit • produits de paiement prépayés; • autres produits de paiement, y compris ceux associés à des titres de transport et à des programmes de fidélisation; • produits de paiement créés en monnaie étrangère (p. ex., produits basés sur le dollar américain). Le présent énoncé normalisé est assujetti à la mise en place des relations commerciales et des capacités techniques appropriées.	8.2 Ouverture et interopérabilité
14	Les applications ou les justificatifs de paiement ne doivent pas être conçus de manière à interdire l'accès d'un porte-monnaie à d'autres applications ou justificatifs de paiement, si les relations commerciales appropriées ont été établies.	8.2 Ouverture et interopérabilité
15	Accès au porte-monnaie mobile : pour des raisons de sécurité, un porte-monnaie mobile doit donner à l'utilisateur final la possibilité de le verrouiller et de le déverrouiller à l'aide d'un mot de passe de son choix.	8.3 Caractéristiques et fonctions du porte-monnaie
16	Sélection de justificatifs par défaut : un porte-monnaie mobile doit donner à l'utilisateur final la possibilité d'activer et de désactiver les justificatifs de paiement par défaut.	8.3 Caractéristiques et fonctions du porte-monnaie
17	Annulation manuelle : un porte-monnaie mobile doit donner à l'utilisateur final la possibilité d'annuler l'application de justificatifs de paiement par défaut et de les remplacer par des justificatifs de paiement choisis manuellement.	8.3 Caractéristiques et fonctions du porte-monnaie
18	Paiements de valeur élevée ou à risque élevé : un porte-monnaie mobile doit permettre à l'utilisateur final de saisir un mot de passe pour confirmer des paiements de valeur élevée ou à risque élevé.	8.3 Caractéristiques et fonctions du porte-monnaie

Numéro	Énoncé	Section
19	Données relatives aux transactions : un porte-monnaie mobile peut collecter des données relatives aux transactions réalisées à l'aide de toutes les applications de paiement qui y sont liées; cependant, si de telles données sont recueillies, l'accès à ces données et leur utilisation doivent être limités selon les normes établies dans la section Données et sécurité du présent document.	8.3 Caractéristiques et fonctions du porte-monnaie
20	Transactions de remise d'achat : les porte-monnaie mobiles et les applications de paiement doivent autoriser l'exécution de transactions de remise d'achat.	8.3 Caractéristiques et fonctions du porte-monnaie
21	Emplacement de l'application de paiement : tous les éléments de l'application de paiement et des justificatifs de paiement (y compris l'application de paiement personnalisée et le mot de passe associé) doivent être regroupés dans l'appareil mobile, soit dans un élément sécurisé de l'UICC, soit dans une zone de l'élément sécurisé intégré. [Suite à l'EN22]mm	8.4 Application et justificatifs de paiement
22	[Suite de l'EN21] Cependant, pour des raisons de sécurité, une seule méthode est privilégiée dans le cadre de ce document. Chaque EJP doit stocker l'application de paiement dans un domaine sécurisé secondaire (DSS) au sein de l'élément sécurisé.	8.4 Application et justificatifs de paiement
23	Chaque DSS doit être assorti de clés de chiffrement particulières qui sont requises pour établir une voie de communication protégée entre le GSC de l'EJP et le domaine sécurisé approprié.	8.4 Application et justificatifs de paiement
24	Partage de l'application de paiement : une application de paiement doit contenir de l'information provenant d'un seul EJP.	8.4 Application et justificatifs de paiement
25	Caractère ouvert de l'application de paiement : si les relations commerciales et contractuelles appropriées ont été établies, une application de paiement ne doit pas prévenir l'association à plusieurs porte-monnaie.	8.4 Application et justificatifs de paiement
26	Repérage des justificatifs : les applications et les justificatifs de paiement contiennent des renseignements sécurisés et chiffrés. Aucune autre application ne doit avoir accès à ces renseignements.	8.4 Application et justificatifs de paiement
27	Protocoles de stockage liés à l'application de paiement : une application de paiement et les justificatifs de paiement connexes doivent être stockés selon les directives appropriées d'EMVCo et du réseau de paiement.	8.4 Application et justificatifs de paiement

Numéro	Énoncé	Section
28	[Contexte – Application compagnon : des services supplémentaires peuvent être ajoutés à une application de paiement à l'aide d'une application compagnon.] Pour qu'une application compagnon soit ajoutée, l'EJP doit approuver cet ajout et l'application compagnon doit respecter les mêmes protocoles de sécurité que l'application de paiement.	8.4 Application et justificatifs de paiement
29	L'application porte-monnaie, l'application parapluie (s'il y a lieu) et l'application de paiement sont assujetties à un processus d'association sécurisé.	8.4 Application et justificatifs de paiement
30	Les solutions de paiement mobile NFC doivent faire en sorte qu'il soit impossible d'activer plus d'une application de paiement mobile (soit une application permettant d'effectuer des paiements) à la fois.	8.4.1 Activation et désactivation de l'application de paiement
31	L'application de paiement activée doit être clairement indiquée sur la liste d'applications de paiement affichée dans le porte-monnaie mobile.	8.4.1 Activation et désactivation de l'application de paiement
32	Si une application de paiement par défaut a été définie, elle doit être désactivée avant qu'une autre application de paiement puisse être activée.	8.4.1 Activation et désactivation de l'application de paiement
33	L'utilisateur final ne doit pas être en mesure de choisir une application bloquée pour effectuer un paiement. Pour que cette application puisse être choisie, l'utilisateur final et l'EJP doivent appliquer la marche à suivre appropriée en vue de débloquer l'application de paiement.	8.4.1 Activation et désactivation de l'application de paiement
34	Avant que des justificatifs puissent être utilisés pour effectuer un paiement, une application de paiement et un porte-monnaie doivent être associés au moyen d'un processus sécurisé qui permet au porte-monnaie d'accéder à l'application de paiement. Ce processus est appelé « association ».	8.4.2 Association d'une application porte-monnaie et d'une application de paiement
35	Avant que l'application porte-monnaie et l'application de paiement puissent être associées, le réseau de paiement et l'EJP, puis l'EJP et le fournisseur de porte-monnaie doivent établir une relation commerciale valide.	8.4.2 Association d'une application porte-monnaie et d'une application de paiement
36	Les transactions utilitaires ne doivent pas dépasser les limites établies à l'égard des transactions de valeur élevée ou à risque élevé, selon les définitions des réseaux de paiement.	9.1 Transactions utilitaires effectuées à l'aide d'un appareil mobile

Numéro	Énoncé	Section
37	Une transaction utilitaire doit respecter les lignes directrices existantes des réseaux de paiement à l'égard des paiements sans contact; sauf si les règles de sécurité l'exigent (p. ex., un compteur de transactions), la transaction utilitaire ne doit pas exiger plus qu'un simple « tapez et partez » pour la réalisation d'un paiement et elle ne doit pas être assujettie à une MVC supplémentaire.	9.1 Transactions utilitaires effectuées à l'aide d'un appareil mobile
38	L'EJP et/ou les réseaux de paiement définissent les transactions de valeur élevée ou à risque élevé. L'utilisateur final doit approuver les transactions de valeur élevée ou à risque élevé en appliquant une MVC.	9.2 Transactions de valeur élevée ou à risque élevé effectuées à l'aide d'appareils mobiles
39	Une fois qu'elles sont jugées acceptables par les réseaux de paiement, les transactions de valeur élevée ou à risque élevé doivent être approuvées à l'aide de la MVC dénommée « tapez et confirmez » (une première tape de l'écran de l'appareil, suivie de la saisie du mot de passe, puis d'une deuxième tape).	9.2 Transactions de valeur élevée ou à risque élevé effectuées à l'aide d'appareils mobiles
40	La méthode « tapez et confirmez » est la seule méthode de vérification de cartes approuvée; elle doit être utilisée dès qu'une transaction est jugée acceptable par un réseau de paiement.	9.2.2 Aperçu des différentes MVC
41	La MVC standard au Canada relativement aux paiements de valeur élevée ou à risque élevé est la méthode « tapez et confirmez » (méthode requérant deux tapes).	9.2.2 Aperçu des différentes MVC
42	La délivrance du reçu est la dernière étape du traitement d'une transaction mobile NFC. Il n'existe pas de normes particulières quant à la délivrance de reçus relativement aux paiements mobiles. La délivrance des reçus doit être conforme aux lignes directrices en vigueur.	9.3 Reçus électroniques
43	Le processus de remise (le contraire d'une transaction de paiement, qui entraîne un crédit porté au compte) doit respecter les définitions des réseaux de paiement.	9.4.2 Processus de remise d'achat
44	La section Habilitation et gestion du cycle de vie repose sur le principe selon lequel les interactions entre les participants à l'écosystème (ERP et EJP, fournisseur de porte-monnaie et EJP, EJP et GSC, EJC et ERM, etc.) doivent être précédées d'étapes visant à établir des relations commerciales contractuelles.	10.1 Relations commerciales entre participants à l'écosystème

Numéro	Énoncé	Section
45	[Contexte : Ce document ne tient pas compte de tous les processus de gestion des clés comme ceux entre le réseau de paiement et l'EJP.] En plus des lignes directrices définies dans cette section, les processus de gestion des clés définis par les réseaux de paiement doivent être respectés.	10.2 Gestion des clés
46	Comme il est décrit à la section 6.8, toutes les activités de messagerie doivent être exécutées conformément aux lignes directrices pertinentes tirées du document GPS_Messaging_Specification_for_Mobile_NFC_Services-v1.0.	10.2 Gestion des clés
47	Les intervenants qui appliquent les normes contenues dans ce document acceptent de n'utiliser que le mode de délégation ou le mode bimodal, tels que définis par GlobalPlatform, dans le cadre de toutes les activités associées à l'habilitation et à la gestion du cycle de vie.	10.2 Gestion des clés
48	S'il s'agit d'un porte-monnaie exclusif, un processus de gestion des clés sécurisées doit être établi entre l'EJP, son GSC, le GDS et son GSC.	10.2 Gestion des clés
49	S'il s'agit d'un porte-monnaie ouvert, des protocoles doivent être établis de manière à ce que les clés soient gérées par plusieurs intervenants.	10.2 Gestion des clés
50	Dans le cadre de ce processus [le processus de gestion des clés], le GSC de l'EJP et l'EJP, le GSC du GDS et le GDS et le GSC de l'EJP et le GSC du GDS doivent avoir établi une relation commerciale, directement ou indirectement.	10.2 Gestion des clés
51	L'échange de clés doit être réalisé conformément aux lignes directrices de GlobalPlatform.	10.2.2 Installateur unique de justificatifs de paiement
52	[Contexte : une fois ce processus terminé, l'échange de clés permettra de mettre en place une voie de communication protégée dédiée à la transmission de données entre l'EJP, son GSC et le GSC du GDS.] Cette voie de communication protégée constitue une exigence minimale et doit être en place afin que puissent être exécutées des activités d'installation par radiofréquences.	10.2.2 Installateur unique de justificatifs de paiement
53	Ensuite, les GSC des EJP échangent des clés entre eux pour s'assurer de mettre en place des voies de communication protégées. Cet échange de clés doit avoir lieu pour permettre l'installation de justificatifs de paiement dans un porte-monnaie ouvert ou collectif.	10.2.3 Installateurs multiples de justificatifs de paiement (réseau en étoile)

Numéro	Énoncé	Section
54	Dans ce modèle, tous les intervenants doivent échanger les clés conformément aux lignes directrices de GlobalPlatform. L'AC ou la plaque tournante de GSC des EJP doit élaborer et diffuser des protocoles destinés à faciliter ces interactions.	10.2.3 Installateurs multiples de justificatifs de paiement (réseau en étoile)
55	À titre d'exigence minimale, l'utilisateur final doit être en mesure de demander l'installation de l'application de paiement à l'aide de son porte-monnaie mobile.	10.4.1 Demande d'accès de l'utilisateur final à l'application de paiement
56	Outre cette méthode, la demande d'installation de l'application de paiement peut être présentée en ligne, dans une succursale bancaire, en appelant à un centre d'appels ou au moyen d'une application de services bancaires mobiles. Quelle que soit la méthode utilisée pour télécharger l'application et les justificatifs de paiement, l'utilisateur final doit donner son consentement avant l'installation.	10.4.1 Demande d'accès de l'utilisateur final à l'application de paiement
57	Dans le cas des demandes présentées à l'aide du porte-monnaie mobile, ce dernier doit afficher le nom de l'EJP dont les justificatifs de paiement vont être installés dans le porte-monnaie.	10.4.1 Demande d'accès de l'utilisateur final à l'application de paiement
58	Avant l'installation de l'application et des justificatifs de paiement dans l'appareil mobile, l'identité de l'utilisateur final doit être validée.	10.4.2 Vérification et validation des renseignements relatifs à l'utilisateur final
59	Le processus de vérification et de validation de l'identité différera en fonction de l'EJP. Ce dernier a la responsabilité de définir le processus de vérification et de validation de l'identité de l'utilisateur final.	10.4.2 Vérification et validation des renseignements relatifs à l'utilisateur final
60	Après la vérification et la validation, l'EJP doit envoyer à l'utilisateur final un message décrivant la prochaine étape.	10.4.2 Vérification et validation des renseignements relatifs à l'utilisateur final
61	Pour que l'application et les justificatifs de paiement puissent être installés, tous les intervenants doivent établir une voie de communication protégée avec l'EJP et le GDS.	10.4.3 Installation de l'application de paiement
62	Une fois la voie de communication protégée établie, le GSC doit prendre en charge toutes les activités, y compris l'installation et l'activation des services de paiement mobile NFC dans l'appareil.	10.4.3 Installation de l'application de paiement
63	L'association est nécessaire pour qu'un porte-monnaie mobile puisse accéder à une application de paiement.	10.4.4 Association de l'application de paiement au porte-monnaie mobile

Numéro	Énoncé	Section
64	L'application parapluie sert de répertoire de l'UICC et doit être fournie par le GDS.	10.4.5 Élément sécurisé dans l'UICC
65	[Contexte : ensuite, l'application parapluie informe le porte-monnaie de l'endroit où se trouve l'application de paiement et lui fournit un identificateur permettant de la repérer.] Le GDS doit fournir la structure de l'identificateur.	10.4.5 Élément sécurisé dans l'UICC
66	Les justificatifs de paiement sont stockés dans l'appareil mobile et doivent pouvoir être installés et mis à jour au moyen de radiofréquences.	10.4.7 Installation de justificatifs de paiement au moyen de radiofréquences
67	Si le GDS (ou le GSC du GDS) demande la mise à jour de l'élément sécurisé, la partie intéressée doit communiquer avec le GSC de l'EJP pour réinstaller l'application de paiement après la mise à jour de l'élément sécurisé.	10.5.2 Mise à jour de l'élément sécurisé
68	Changement d'appareil mobile (élément sécurisé intégré) : si l'application de paiement mobile est stockée dans l'élément sécurisé intégré, l'utilisateur final doit appliquer de nouveau tout le processus d'installation du porte-monnaie mobile et de l'application de paiement (étapes de configuration d'un nouvel appareil).	10.5.3 Changement d'appareil mobile
69	Changement d'appareil mobile (élément sécurisé dans l'UICC) : si l'utilisateur final change d'appareil mobile ou ajoute un appareil secondaire, il doit effectuer la configuration initiale de nouveau, y compris la vérification de l'identité de l'utilisateur final et l'association du porte-monnaie mobile et des justificatifs de paiement.	10.5.3 Changement d'appareil mobile
70	En cas de perte ou de vol d'un appareil mobile, l'utilisateur final doit être invité à communiquer avec l'ERM et l'EJP.	10.5.4 Appareil mobile perdu ou volé
71	Lorsqu'il est mis au courant de la perte ou du vol d'un appareil mobile, l'ERM ou le GDS (s'ils sont différents) doit interrompre le service de l'appareil mobile ou le bloquer (dans le cas d'appareils dotés d'une carte SIM, la carte doit également être bloquée; autrement, la zone sécurisée de l'élément sécurisé intégré doit être bloquée, au besoin).	10.5.4 Appareil mobile perdu ou volé

Numéro	Énoncé	Section
72	Lorsqu'il est mis au courant de la perte ou du vol d'un appareil mobile, l'EJP doit bloquer la méthode de paiement (d'autres étapes, ressemblant aux étapes actuelles d'inscription de produits de cartes sur une liste noire, peuvent être suivies à l'interne).	10.5.4 Appareil mobile perdu ou volé
73	[Contexte : ce processus décrit l'activation d'un nouvel appareil mobile. Cette activation peut faire suite à un choix de l'utilisateur final ou à la perte ou au vol d'un appareil mobile.] Avant l'activation d'un nouvel appareil mobile et l'installation des justificatifs de paiement, le GSC de l'EJP ou le GSC du GDS de l'ancien appareil ou de l'appareil perdu ou volé doit tenter de retirer toute l'information relative aux justificatifs de paiement et doit fournir un avis concernant le résultat de cette opération à l'ERM et au GDS (s'ils sont différents) et à l'EJP.	10.5.5 Remplacement de l'appareil mobile par l'utilisateur final
74	En cas de questions liées à l'appareil ou aux services mobiles, l'utilisateur final sera invité à communiquer avec l'ERM.	10.6.1 Appareil et services mobiles
75	Une entente doit être conclue avec l'ERM ou le GDS en vue de l'exécution d'activités d'approvisionnement et de maintenance même lorsque les services mobiles de l'utilisateur final sont interrompus ou inactifs.	10.6.2 Installation des justificatifs de paiement échouée
76	Si l'installation des justificatifs de paiement échoue, l'utilisateur final sera invité à communiquer avec l'EJP.	10.6.3 Transaction échouée
77	Si une transaction échoue, l'utilisateur final sera invité à communiquer avec l'EJP responsable de l'instrument de paiement utilisé.	10.6.3 Transaction échouée
78	Dans le cas de toutes les activités de maintenance associées à un compte, l'utilisateur final sera invité à communiquer avec l'EJP.	10.6.4 Activités de maintenance liées au compte
79	En cas de perte ou de vol d'un appareil mobile, l'utilisateur final sera invité à communiquer avec l'ERM et le ou les EJP.	10.6.5 Appareil mobile perdu ou volé
80	Si le porte-monnaie fonctionne normalement, mais que l'application de paiement connaît des ratés, l'utilisateur final sera invité à appeler l'EJP.	10.6.6 Processus d'association
81	En cas de problèmes associés à la maintenance de l'application de paiement, l'utilisateur final sera invité à communiquer avec l'EJP.	10.6.7 Maintenance de l'application de paiement

Numéro	Énoncé	Section
82	Si l'ERM met fin aux services mobiles, l'application de paiement continue de fonctionner. Des ententes doivent être conclues entre l'ERM et l'EJP en vue d'établir des protocoles visant une telle situation (voir section 10.6.1).	10.7 Suppression de l'application de paiement et des justificatifs connexes
83	Les coupons et bons d'achat contenus dans le porte-monnaie mobile qui transmettent de l'information au PDV NFC au moyen de la technologie NFC ou d'une autre méthode (p. ex., code à barres) doivent respecter les normes pertinentes du présent document.	11.2.4 Interaction au PDV – Analyse des coupons, des bons d'achat et des incitatifs
84	La norme internationale ISO/CEI 14443 définit les cartes de proximité employées à des fins d'identification et les protocoles de transmission utilisés pour communiquer. Cette norme doit être respectée dans le cadre de la transmission de renseignements liés aux programmes de fidélisation et de récompenses de l'appareil mobile au PDV au moyen de la technologie NFC.	11.2.5 Technologies liées au PDV
85	Si les points de fidélisation et les récompenses sont utilisés comme monnaie d'échange, les justificatifs associés aux points de fidélisation et aux récompenses doivent être traités comme des justificatifs de paiement; ils doivent donc être installés et stockés de façon sécurisée dans l'appareil mobile.	11.3.1 Analyse de l'expérience d'échange de points de fidélisation
86	Pour procéder à l'échange immédiat de points de fidélisation, l'utilisateur final doit être tenu de présenter ses points comme mode de paiement en sélectionnant le programme de fidélisation approprié dans le porte-monnaie mobile.	11.3.1 Analyse de l'expérience d'échange de points de fidélisation
87	Le but premier des participants à l'écosystème est de protéger les données de l'utilisateur final et du marchand. L'accès aux données ainsi que leur utilisation doivent être communiqués à l'utilisateur final, qui doit accorder explicitement son autorisation à cet effet.	12 Données et sécurité
88	Produits de paiement contenus dans le porte-monnaie – seuls le fournisseur de porte-monnaie et l'utilisateur final ont accès à la liste de produits de paiement contenue dans un porte-monnaie. Aucun autre intervenant ne doit avoir accès à la liste de produits de paiement. [Suite à l'EN89]	12.1.1 Accès aux données contenues dans le porte-monnaie
89	[Suite de l'EN88] L'accès du fournisseur de porte-monnaie à l'information liée aux produits de paiement doit se limiter à l'information nécessaire pour assurer la maintenance du porte-monnaie.	12.1.1 Accès aux données contenues dans le porte-monnaie

Numéro	Énoncé	Section
90	Produits de fidélisation contenus dans le porte-monnaie – seuls le fournisseur de porte-monnaie et l'utilisateur final ont accès à la liste de produits de fidélisation contenue dans un porte-monnaie. Aucun autre intervenant ne doit avoir accès à la liste de produits de fidélisation. [Suite à l'EN91]	12.1.1 Accès aux données contenues dans le porte-monnaie
91	[Suite de l'EN90] L'accès du fournisseur de porte-monnaie à l'information liée aux produits de fidélisation doit se limiter à l'information nécessaire pour assurer la maintenance du porte-monnaie.	12.1.1 Accès aux données contenues dans le porte-monnaie
92	Coupons contenus dans le porte-monnaie – seuls le fournisseur de porte-monnaie, l'utilisateur final et quelques autres applications de fidélisation approuvées par l'utilisateur final ont accès à la liste de coupons contenue dans un porte-monnaie. Aucun autre intervenant ne doit avoir accès à la liste de coupons.	12.1.1 Accès aux données contenues dans le porte-monnaie
93	Données non chiffrées liées au produit de paiement – seuls l'EJP, les marchands et l'utilisateur final ont accès aux données non chiffrées liées au produit de paiement. Aucun autre intervenant ne doit avoir accès aux données non chiffrées liées au produit de paiement. [Suite à l'EN94]	12.1.2 Accès aux données liées aux justificatifs
94	[Suite de l'EN93] Exemples de données financières non chiffrées liées aux produits de paiement : numéro de carte de crédit, nom figurant sur la carte et code de vérification de carte. Les marchands ont accès à ces renseignements uniquement dans le cadre du traitement du paiement. La collecte et le stockage de données non chiffrées liées aux produits de paiement par les marchands doivent être conformes aux lignes directrices du réseau de paiement.	12.1.2 Accès aux données liées aux justificatifs
95	Données chiffrées liées au produit de paiement – seul l'EJP a accès aux données chiffrées liées au produit de paiement. Aucun autre intervenant ne doit avoir accès aux données chiffrées liées au produit de paiement.	12.1.2 Accès aux données liées aux justificatifs
96	Données non chiffrées associées aux justificatifs liés aux programmes de fidélisation – seuls le responsable du programme de fidélisation, les marchands et l'utilisateur final ont accès aux données non chiffrées associées aux justificatifs liés aux programmes de fidélisation. Aucun autre intervenant ne doit avoir accès aux données non chiffrées associées aux justificatifs liés aux programmes de fidélisation. [Suite à l'EN97]	12.1.2 Accès aux données liées aux justificatifs

Numéro	Énoncé	Section
97	[Suite de l'EN96] Les données non chiffrées associées aux justificatifs liés aux programmes de fidélisation collectées et stockées par les marchands doivent être traitées de la même manière que les justificatifs de paiement. De plus, ces données ne doivent servir qu'à l'octroi de récompenses et à l'échange de points de fidélisation.	12.1.2 Accès aux données liées aux justificatifs
98	Données chiffrées associées aux justificatifs liés aux programmes de fidélisation – si des points de fidélisation sont échangés au PDV, seul le responsable du programme de fidélisation a accès aux données chiffrées associées aux justificatifs liés aux programmes de fidélisation. Aucun autre intervenant ne doit avoir accès aux données chiffrées associées aux justificatifs liés aux programmes de fidélisation.	12.1.2 Accès aux données liées aux justificatifs
99	Données financières, montant – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final ont accès au montant de la transaction. Aucun autre intervenant ne doit avoir accès au montant de la transaction. [Suite à l'EN100]	12.1.3 Accès aux données financières
100	[Suite de l'EN99] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le montant de la transaction.	12.1.3 Accès aux données financières
101	Données financières, heure – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final ont accès à l'heure de la transaction. Aucun autre intervenant ne doit avoir accès à l'heure de la transaction. [Suite à l'EN102]	12.1.3 Accès aux données financières
102	[Suite de l'EN101] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer l'heure de la transaction.	12.1.3 Accès aux données financières
103	Données financières, marchand – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final peuvent connaître l'identité du marchand ayant effectué la transaction. Aucun autre intervenant ne doit connaître l'identité du marchand ayant effectué la transaction. [Suite à l'EN104]	12.1.3 Accès aux données financières
104	[Suite de l'EN103] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final	12.1.3 Accès aux données financières

Numéro	Énoncé	Section
	et l'EJP accordent explicitement leur autorisation de communiquer l'identité du marchand ayant effectué la transaction.	
105	Données financières, produit – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final ont accès au produit utilisé pour effectuer une transaction. Aucun autre intervenant ne doit avoir accès au produit utilisé pour effectuer une transaction. [Suite à l'EN106]	12.1.3 Accès aux données financières
106	[Suite de l'EN105] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le produit utilisé pour effectuer une transaction.	12.1.3 Accès aux données financières
107	Données financières, lieu – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final ont accès au lieu de la transaction. Aucun autre intervenant ne doit avoir accès au lieu de la transaction. [Suite à l'EN108]	12.1.3 Accès aux données financières
108	[Suite de l'EN107] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le lieu de la transaction.	12.1.3 Accès aux données financières
109	Données financières, détail de la transaction – seuls le marchand et l'utilisateur final ont accès au détail de la transaction (p. ex., numéro d'article). Aucun autre intervenant ne doit avoir accès au détail de la transaction. [Suite à l'EN110]	12.1.3 Accès aux données financières
110	[Suite de l'EN109] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le détail de la transaction.	12.1.3 Accès aux données financières
111	Données financières, reçus électroniques – seuls le marchand et l'utilisateur final ont accès aux reçus électroniques liés à une transaction. Aucun autre intervenant ne doit avoir accès aux reçus électroniques. [Suite à l'EN112]	12.1.3 Accès aux données financières

Numéro	Énoncé	Section
112	[Suite de l'EN111] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de transmettre les reçus électroniques.	12.1.3 Accès aux données financières
113	Données liées aux programmes de fidélisation, montant – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final ont accès au montant d'une transaction de fidélisation. Aucun autre intervenant ne doit avoir accès au montant d'une transaction de fidélisation. [Suite à l'EN114]	12.1.4 Accès aux données liées aux programmes de fidélisation
114	[Suite de l'EN113] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le montant d'une transaction de fidélisation.	12.1.4 Accès aux données liées aux programmes de fidélisation
115	Données liées aux programmes de fidélisation, heure – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final ont accès à l'heure d'exécution d'une transaction de fidélisation. Aucun autre intervenant ne doit avoir accès à l'heure d'exécution d'une transaction de fidélisation. [Suite à l'EN116]	12.1.4 Accès aux données liées aux programmes de fidélisation
116	[Suite de l'EN115] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer l'heure d'exécution d'une transaction de fidélisation.	12.1.4 Accès aux données liées aux programmes de fidélisation
117	Données liées aux programmes de fidélisation, marchand – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final peuvent connaître l'identité du marchand ayant effectué la transaction de fidélisation. Aucun autre intervenant ne doit connaître l'identité du marchand ayant effectué la transaction de fidélisation. [Suite à l'EN118]	12.1.4 Accès aux données liées aux programmes de fidélisation
118	[Suite de l'EN117] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer l'identité du marchand ayant effectué la	12.1.4 Accès aux données liées aux programmes de fidélisation

Numéro	Énoncé	Section
	transaction de fidélisation.	
119	Données liées aux programmes de fidélisation, produit – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final peuvent connaître le produit utilisé pour effectuer une transaction de fidélisation. Aucun autre intervenant ne doit connaître le produit utilisé pour effectuer une transaction de fidélisation. [Suite à l'EN120]	12.1.4 Accès aux données liées aux programmes de fidélisation
120	[Suite de l'EN119] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le produit utilisé pour effectuer une transaction de fidélisation.	12.1.4 Accès aux données liées aux programmes de fidélisation
121	Données liées aux programmes de fidélisation, lieu – seuls l'acquéreur, l'EJP, le marchand et l'utilisateur final peuvent connaître le lieu d'exécution d'une transaction de fidélisation. Aucun autre intervenant ne doit connaître le lieu d'exécution d'une transaction de fidélisation. [Suite à l'EN122]	12.1.4 Accès aux données liées aux programmes de fidélisation
122	[Suite de l'EN121] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le lieu d'exécution d'une transaction de fidélisation.	12.1.4 Accès aux données liées aux programmes de fidélisation
123	Données liées aux programmes de fidélisation, détail de la transaction – seuls le marchand et l'utilisateur final ont accès au détail de la transaction de fidélisation (p. ex., numéro d'article). Aucun autre intervenant ne doit avoir accès au détail de la transaction de fidélisation. [Suite à l'EN124]	12.1.4 Accès aux données liées aux programmes de fidélisation
124	[Suite de l'EN 123]. Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le détail de la transaction de fidélisation.	12.1.4 Accès aux données liées aux programmes de fidélisation

Numéro	Énoncé	Section
125	Données liées aux programmes de fidélisation, reçus électroniques – seuls le marchand et l'utilisateur final ont accès aux reçus électroniques liés à une transaction de fidélisation. Aucun autre intervenant ne doit avoir accès aux reçus électroniques liés à une transaction de fidélisation. [Suite à l'EN126]	12.1.4 Accès aux données liées aux programmes de fidélisation
126	[Suite de l'EN125] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de transmettre les reçus électroniques liés à une transaction de fidélisation.	12.1.4 Accès aux données liées aux programmes de fidélisation
127	Produit de paiement, solde – seuls l'EJP et l'utilisateur final ont accès au solde du produit de paiement. Aucun autre intervenant ne doit avoir accès au solde du produit de paiement. [Suite à l'EN128]	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation
128	[Suite de l'EN127] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le solde du produit de paiement.	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation
129	Produit de paiement, détail du compte – seuls l'EJP et l'utilisateur final ont accès au détail du compte lié au produit de paiement. Aucun autre intervenant ne doit avoir accès au détail du compte lié au produit de paiement. [Suite à l'EN130]	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation
130	[Suite de l'EN129] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le détail du compte lié au produit de paiement.	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation
131	Produit de fidélisation, solde – seuls l'EJP et l'utilisateur final ont accès au solde du produit de fidélisation. Aucun autre intervenant ne doit avoir accès au solde du produit de fidélisation. [Suite à l'EN132]	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation

Numéro	Énoncé	Section
132	[Suite de l'EN131] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le solde du produit de fidélisation.	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation
133	Produit de fidélisation, détail du compte – seuls l'EJP et l'utilisateur final ont accès au détail du compte lié au produit de fidélisation. Aucun autre intervenant ne doit avoir accès au détail du compte lié au produit de fidélisation. [Suite à l'EN134]	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation
134	[Suite de l'EN133] Le porte-monnaie peut collecter et stocker cette information au nom de l'utilisateur final, mais elle ne doit pas être accessible au fournisseur de porte-monnaie ni à un autre tiers, sauf si l'utilisateur final et l'EJP accordent explicitement leur autorisation de communiquer le détail du compte lié au produit de fidélisation.	12.1.5 Accès aux données liées aux produits de paiement et au compte de fidélisation