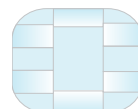


Mise en œuvre de l'acceptation  
des Cartes à puce EMV<sup>MC</sup>  
American Express sur un terminal

outils EMV<sup>MC</sup>



**A** | **M**ERICAN  
**E** | **X**PRESS  
**I** | **I**ntegrated Circuit Card  
**P** | **P**ayment  
**S** | **S**pecification

American Express peut en tout temps modifier les lignes directrices, les méthodes et les règles énoncées dans le présent guide.

© American Express Travel Related Services Company, Inc., 2008.

Tous droits réservés. Aucune partie du présent document ne peut être reproduite sous quelque forme que ce soit ni par aucun moyen électronique ou mécanique, y compris par un système de stockage et d'extraction de données, sans le consentement préalable écrit et explicite d'American Express Travel Related Services Company, Inc. EMV est une marque de commerce d'EMVCo, LLC. PCI Security Standards Council est une marque de commerce de PCI Security Standards Council, LLC. Toutes les autres marques et marques de commerce appartiennent à leurs propriétaires respectifs.

# TABLE DES MATIÈRES

<b>SECTION 1 : INTRODUCTION</b>	<b>5</b>
1.1. Aperçu	5
1.2. Comment utiliser le présent guide	5
1.3. Documents de référence	5
1.4. Expressions qualifiant les exigences	6
<b>SECTION 2 : SPÉCIFICATIONS EMV</b>	<b>7</b>
2.1. Spécifications de l'industrie	7
2.2. Spécifications (PCPAE (AEIPS)) : Spécifications pour le paiement par Carte à puce American Express	7
<b>SECTION 3 : EXIGENCES EMV RELATIVES AU TERMINAL, PAR ÉTAPE DU TRAITEMENT D'UNE OPÉRATION</b>	<b>9</b>
3.1. Introduction	9
3.2. Étapes du traitement d'une opération par Carte à puce (EMV)	10
Étape 1 : sélection de l'application	10
Étape 2 : lancement du traitement de l'application	11
Étape 3 : lecture des données relatives à l'application	11
Étape 4 : authentification des données hors ligne	11
Étape 5 : traitement des restrictions	12
Étape 6 : vérification de l'identité du titulaire de la Carte	12
Étape 7 : gestion du risque à partir du terminal	14
Étape 8 : première analyse des actions du terminal	14
Étape 9 : première analyse des actions de la Carte	15
Étape 10 : traitement des opérations en ligne	15
Étape 11 : authentification de l'émetteur	17
Étape 12 : deuxième analyse des actions du terminal	17
Étape 13 : deuxième analyse des actions de la Carte	18
Étape 14 : traitement du script de l'émetteur	18
Étape 15 : traitement final de l'opération	20

## SECTION 4 : TRAITEMENT SPÉCIAL D'UNE OPÉRATION . . . . . 25

4.1. Exigences des spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) relatives aux cas d'ordre technique. . . . .	25
4.1.1. Traitement de rechange . . . . .	25
4.1.2. Retrait prématuré de la Carte . . . . .	26
4.1.3. Opérations avec autorisation verbale . . . . .	27
4.1.4. Opérations refusées . . . . .	27
4.1.5. Autorisation par intervention du marchand . . . . .	28
4.1.6. Annulations . . . . .	30
4.2. Exigences des spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) relatives aux cas d'ordre circonstanciel . . . . .	31
4.2.1. Remboursements . . . . .	31
4.2.2. Opération sans présentation de la Carte . . . . .	32
4.2.3. Opération avec présentation à venir de la Carte . . . . .	32
4.2.4. Montant de l'opération encore inconnu . . . . .	32
4.2.5. Carte non accessible . . . . .	33
4.2.6. Carte présentée à nouveau pour compléter l'opération . . . . .	33
4.2.7. Ajout d'un pourboire . . . . .	34
4.3. Exigences des spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) relatives aux terminaux de paiement sans surveillance (TPSS) . . . .	34
4.3.1. Vérification de l'identité du titulaire à un TPSS . . . . .	35
4.3.2. Traitement de rechange à un TPSS . . . . .	35
4.3.3. Capacité de connexion à un TPSS . . . . .	35

## SECTION 5 : CERTIFICATION AEIPS (SPCPAE) DU TERMINAL . . . . . 37

5.1. Introduction . . . . .	37
5.2. Processus de certification AEIPS (SPCPAE) du terminal . . . . .	38
5.3. Plan d'essai [AEIPS-TEST] pour la certification AEIPS (SPCPAE) du terminal . . . . .	40
5.4. Programmation du terminal avant sa certification AEIPS (SPCPAE). . . . .	41
5.4.1. Exigences et paramètres supplémentaires pour la certification du processus d'autorisation par intervention du marchand . . . . .	42

5.4.2. Données obligatoires aux fins du diagnostic . . . . .	42
5.4.3. Essai de la connexion . . . . .	43
5.5. Exécution du plan d'essai . . . . .	43
5.5.1. Documentation . . . . .	43
5.5.2. Exigences relatives aux paramètres des champs « Résultats de vérification du terminal (TVR) » et « Renseignements sur les résultats de l'opération (TSI) » . . . . .	44
5.6. Aperçu des essais pour l'obtention d'une certification AEIPS (SPCPAE) du terminal . . . . .	44
5.6.1. Essais obligatoires . . . . .	45
5.6.2. Essais fondés sur les fonctions du terminal . . . . .	50
5.6.3. Essais effectués quand la liaison de communication a été modifiée . . . . .	56
<b>SECTION 6 : FORMATION DU MARCHAND . . . . .</b>	<b>57</b>
6.1. Directives pour un programme de formation réussi . . . . .	57
<b>ANNEXE A : RENSEIGNEMENTS SUR LES CLÉS RÉVÉLÉES DE L'ORGANISME DE CERTIFICATION . . . . .</b>	<b>59</b>
<b>ANNEXE B : MESSAGES AFFICHÉS . . . . .</b>	<b>63</b>
<b>ANNEXE C : GLOSSAIRE ET ACRONYMES . . . . .</b>	<b>67</b>



## SECTION 1 : INTRODUCTION

### 1.1. Aperçu

Le présent guide est conçu pour vous aider (le fournisseur de terminal, le marchand, le revendeur ou la société de traitement externe) à mettre en œuvre l'acceptation des Cartes à puce EMV American Express sur un terminal, au moyen des spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)). La lecture du présent guide exige une compréhension de base des spécifications EMV. En consultant le guide et les documents de référence, vous serez en mesure de bien comprendre les exigences, les lignes directrices et les méthodes – ainsi que les options de configuration – qui s'appliquent spécifiquement à American Express. Vous trouverez également des conseils pratiques, sous la rubrique « Meilleures pratiques », qui vous aideront à comprendre quelle est la meilleure façon de mettre en œuvre l'acceptation de la Carte à puce EMV American Express.

Le guide ne présente en détail que les exigences et les options propres à American Express en ce qui a trait à la mise en œuvre de la technologie EMV. Sauf indication contraire dans le présent document, veuillez traiter les opérations de la façon décrite dans les spécifications d'EMVCo. De plus, le présent guide ne traite que des exigences normalisées à l'échelle mondiale concernant la mise en œuvre des spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)). Un pays ou une banque administratrice peut afficher des exigences supplémentaires qui lui sont propres.

Pour obtenir de plus amples renseignements sur la mise en œuvre des spécifications EMV, veuillez communiquer avec votre banque administratrice ou votre représentant d'American Express ou visiter le site Web d'EMVCo ([www.emvco.com](http://www.emvco.com)).

### 1.2. Comment utiliser le présent guide

Bien que le présent guide ne constitue pas une spécification technique définitive, il offre une feuille de route vous permettant de mieux comprendre la mise en œuvre des spécifications d'American Express pour le passage à la technologie EMV. Les documents de référence techniques mentionnés dans la section 1.3 offrent un soutien supplémentaire. Pour plus de commodité, nous avons également inclus une section « Glossaire et acronymes » à la fin du présent document. Vous pouvez la consulter si vous lisez des phrases, des acronymes ou des termes qui ne vous sont pas familiers. Les termes définis au glossaire figurent en lettres majuscules dans le corps du texte.

### 1.3. Documents de référence

Tous les documents mentionnés dans le présent guide sont énumérés dans le tableau 1. Les références à ces documents seront faites au moyen des abréviations fournies. Il ne s'agit pas d'une liste exhaustive de tous les documents disponibles. Veuillez communiquer avec votre représentant d'American Express pour connaître les autres documents de référence disponibles.

Tableau 1 : Documents de référence

Abréviation	Nom complet du document	Source
[AEIPS-TEST]	Plan d'essai spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) v. 5.2, American Express	Communiquez avec votre représentant d'American Express
[AEIPS-TERM]	Spécifications – Terminal traitant les opérations portées à une Carte à puce American Express (PCPAE (AEIPS) 4.1), American Express	Communiquez avec votre représentant d'American Express
[AEIPS-CARD]	Spécifications – Carte à puce American Express (PCPAE (AEIPS) 4.1), American Express	Communiquez avec votre représentant d'American Express
[ISO-9564]	Banque – Gestion et sécurité du numéro personnel d'identification (NIP)	www.iso.org
[ISO-11568]	Banque – Gestion de clés (services aux particuliers)	www.iso.org
[ISO-11770]	Technologies de l'information – Techniques de sécurité – Gestion de clés	www.iso.org
[ISO-13492]	Services financiers – Élément de données lié à la gestion des clés (services aux particuliers)	www.iso.org
[ISO-15782]	Gestion de certificats pour les services financiers	www.iso.org
[ISO-15408]	Technologies de l'information – Techniques de sécurité – Critères d'évaluation pour la sécurité des TI	www.iso.org
[ISO-7813]	Cartes d'identification – Cartes de transactions financières	www.iso.org

#### 1.4. Expressions qualifiant les exigences

Dans le présent guide, la nature obligatoire des exigences est mise en évidence au moyen de l'italique et de caractères gras, comme suit :

- **Les exigences** sont mises en évidence au moyen des mots ***doit (doivent), exige (exigent)*** ou ***obligatoire(s)***.
- **Les recommandations** sont mises en évidence au moyen des mots ***devrait (devraient), facultatif(s) (facultative(s))*** ou ***recommande (recommandent, recommandé(es))***.

Dans le présent guide, seules **les exigences** dépassant **les exigences** relatives aux spécifications EMV, ainsi que les options pouvant être offertes par les fournisseurs de services de paiement, sont mises en évidence.



## SECTION 2 : SPÉCIFICATIONS EMV

### 2.1. Spécifications de l'industrie

Aux fins du présent document, « EMV » sert à décrire un ensemble de spécifications relatives aux Cartes à puce qui est géré par EMVCo. Ces spécifications facilitent la mise en œuvre d'un cadre interopérable dans lequel les opérations de paiement par Carte à puce peuvent être traitées partout dans le monde. Les spécifications EMV offrent aux fournisseurs de services de paiement et aux émetteurs de cartes la souplesse permettant de fixer leurs exigences précises en ce qui a trait à la sécurité, à la gestion du risque et à la vérification de l'identité du titulaire de Carte, et ce, afin de mieux atteindre leurs propres objectifs.

Les spécifications EMV s'appliquent à pratiquement tous les aspects touchant la Carte à puce, dont les suivants :

- les caractéristiques physiques;
- l'interface électronique entre la Carte à puce et le terminal;
- l'établissement de protocoles pour l'échange de données entre une Carte à puce et un terminal; et
- les caractéristiques de l'application de paiement.

EMVCo explique en détail et gère l'autorisation du type de terminal afin d'en assurer la conformité avec les spécifications. Les fournisseurs de services de paiement établissent leurs propres exigences relatives à la mise en œuvre de la technologie EMV et définissent les processus d'essai pour l'obtention d'une certification en vertu de ces exigences. Les associations du secteur bancaire de certains pays peuvent également établir des exigences locales. Celles-ci sont souvent liées aux mises en œuvre nationales visant à assurer une démarche cohérente dans un pays (p. ex., l'établissement d'exigences communes pour l'utilisation du NIP).

### 2.2. Spécifications (PCPAE (AEIPS)) : Spécifications pour le paiement par Carte à puce American Express

Les spécifications EMV contiennent des options de mise en œuvre que les fournisseurs de services de paiement précisent dans leurs propres spécifications. Afin de permettre l'utilisation la plus efficace possible de la technologie EMV, American Express a élaboré les spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)). Ces spécifications sont divisées en deux catégories :

- Spécifications – Carte à puce American Express [AEIPS-CARD], qui définissent les éléments de données techniques et les fonctionnalités au moment de mettre en œuvre les Cartes à puces conformes aux normes EMV.
- Spécifications – Terminal traitant les opérations portées à une Carte à puce American Express [AEIPS-TERM], qui décrivent les fonctionnalités du terminal exigées afin de traiter les opérations par Carte à puce EMV American Express.

**MEILLEURE PRATIQUE :** il est **recommandé** de lire les documents « Spécifications – Carte à puce American Express » et « Spécifications – Terminal traitant les opérations portées à une Carte à puce American Express » afin de comprendre pleinement comment mettre en œuvre l'acceptation des Cartes à puce EMV American Express.

Comme les spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) s'appuient sur les spécifications d'EMVCo, la mise en œuvre pour les Cartes à puce EMV American Express et celle pour les cartes à puce EMV des autres fournisseurs de services de paiement ne présentent aucune différence technique. Les seules différences concernent les options de configuration qu'American Express a choisies en se fondant sur les spécifications d'EMVCo. American Express ne fait pas exception; il existe des différences de configuration semblables entre les diverses autres fournisseurs de services de paiement.

Par conséquent, il est tout aussi facile de mettre en œuvre l'acceptation des Cartes à puce EMV American Express que celle des cartes d'autres fournisseurs de services de paiement. Cela offre de nombreux avantages; cela permet notamment de se conformer simultanément aux spécifications de tous les fournisseurs de services de paiement, d'économiser les efforts liés à l'ajout des spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) après avoir déjà entrepris le passage à la technologie EMV, et d'assurer la satisfaction de tous les clients potentiels.

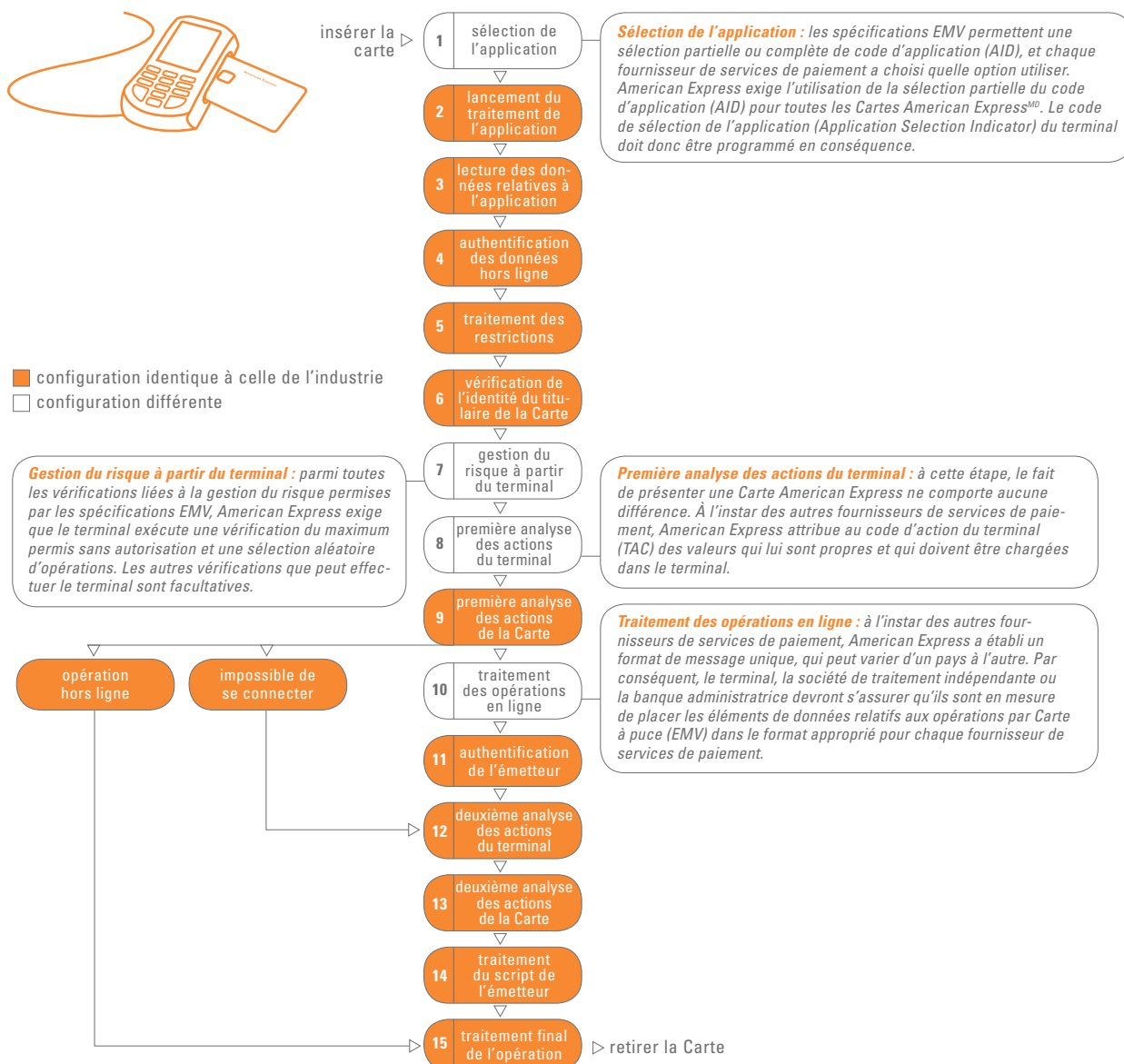
## SECTION 3 : EXIGENCES EMV RELATIVES AU TERMINAL, PAR ÉTAPE DU TRAITEMENT D'UNE OPÉRATION

### 3.1. Introduction



La présente section traite de chaque étape d'une opération par Carte à puce (EMV). Comme le montre la figure 1, le système d'American Express est interopérable et s'aligne également de très près sur le système des autres fournisseurs de services de paiement. American Express présente des différences de configuration par rapport à l'industrie à seulement quatre étapes du traitement d'une opération par Carte à puce EMV.

Figure 1 : Traitement d'une opération par Carte à puce (EMV)



### 3.2. Étapes du traitement d'une opération par Carte à puce (EMV)

Voici une description détaillée de chaque étape du traitement d'une opération par Carte à puce (EMV). Quand la configuration d'American Express diffère, les exigences propres à la Société sont notées et expliquées en détail. De plus, à certaines étapes, des exigences supplémentaires ont été ajoutées pour des fonctions opérationnelles non prévues par les spécifications EMV (p. ex., la dispense de NIP). Ces exigences supplémentaires sont aussi décrites aux étapes appropriées.

Les symboles suivants permettront de facilement repérer les étapes présentant une configuration propre aux spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) :

- ▲ Indique qu'il y a une différence de configuration propre aux spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS))
- so Indique qu'il n'y a pas eu de personnalisation au-delà des spécifications EMV normales

Une description générale des étapes figure au début de chaque section, entre deux lignes pointillées.

#### Étape 1 : sélection de l'application

##### ▲ Configuration d'American Express différente

Lorsqu'une Carte à puce est insérée dans un terminal, celui-ci dresse – et peut avoir l'option d'afficher – une liste d'applications prises en charge à la fois par la Carte à puce et le terminal. Cela se fait en jumelant le code de l'application (AID) chargé dans le terminal à une valeur semblable chargée dans la Carte.

- ▲ La sélection de l'application pour les Cartes conformes aux spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) s'effectue en fonction des spécifications EMV. American Express **exige** que les terminaux prennent en charge et permettent la sélection partielle du nom en fixant le code de sélection de l'application (Application Selection Indicator).

En ce qui concerne la sélection partielle du nom, la commande est transmise avec le code de l'application (AID) partiel American Express chargé dans le terminal, qui est constitué du code du fournisseur enregistré de l'application (RID) American Express et du premier octet de l'extension du code d'application de propriété exclusive (PIX).

Le code du fournisseur enregistré de l'application (RID) American Express est : « A0 00 00 00 25 » et le premier octet du PIX pour une application de paiement conforme aux spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) est « 01 ». Par conséquent, la valeur du code d'application (AID) contenu dans le terminal aux fins d'utilisation pour la sélection partielle du nom **doit** être « A0 00 00 00 25 01 ».

Si une Carte à puce est insérée dans un terminal et qu'aucune application correspondante ne peut être trouvée – p. ex., si le terminal peut prendre en charge les opérations par Carte à puce (EMV), mais n'a pas encore fait l'objet d'une certification à cette fin, ou s'il peut prendre en charge les opérations par carte à puce (EMV) d'autres fournisseurs de services de paiement, mais pas encore celles d'American Express – l'opération **doit** être traitée au moyen de la bande magnétique. Vous ne devez pas traiter l'opération à l'aide du traitement de rechange (voir la section 4.1.1. Traitement de rechange, pour une définition). Pour permettre le traitement de l'opération au moyen de la bande magnétique, le terminal **ne doit pas** effectuer une vérification complète du code de service (p. ex., il **ne devrait pas**

demander l'insertion d'une Carte quand il détecte un code de service commençant par 2 ou 6). Dans ce cas, les codes de données du PdV ou des codes semblables **doivent** indiquer que le terminal ne prend pas en charge les Cartes à puce (p. ex., position 1 [code de capacité de saisie des données de la Carte]  $\neq$  5 [Carte à puce]). Pour ce faire, le terminal **doit** pouvoir fixer le code des données du PdV en fonction du fournisseur de services de paiement.

## Étape 2 : lancement du traitement de l'application

### so Configuration d'American Express identique

Si une application PCPAE (AEIPS) est sélectionnée, le terminal demande que la Carte à puce fournisse l'emplacement des données à utiliser pour l'opération en cours et dresse une liste des fonctions prises en charge.

## Étape 3 : lecture des données relatives à l'application

### so Configuration d'American Express identique

Le terminal lit les données exigées à partir des emplacements fournis par la Carte à puce et utilise la liste des fonctions prises en charge pour déterminer le type de traitement à effectuer. Les renseignements exigés pour effectuer une authentification des données hors ligne se trouvent dans les données lues à partir de la Carte à puce à cette étape de l'opération.

## Étape 4 : authentification des données hors ligne

### so Configuration d'American Express identique. Toutefois, des exigences supplémentaires sont fournies pour les fonctionnalités opérationnelles non prévues par les spécifications EMV.

L'authentification des données hors ligne permet de vérifier si la Carte utilisée pour une opération est la Carte qui a été émise initialement et si les données qui y figurent n'ont pas été modifiées. Il existe différents types d'authentification hors ligne des données. Les plus utilisées sont l'authentification des données permanentes (SDA) et l'authentification de données dynamiques (DDA). Le terminal détermine s'il authentifie la Carte à puce hors ligne, au moyen soit de l'authentification des données permanentes (SDA), soit de l'authentification de données dynamiques (DDA), en fonction de la capacité de la Carte à puce et du terminal de prendre en charge ces méthodes.

American Express **exige** que les terminaux prennent en charge l'authentification des données permanentes (SDA) et l'authentification de données dynamiques (DDA). Toutefois, la prise en charge à la fois de l'authentification de données dynamiques (DDA) et de la production du cryptogramme d'application (AC) est **facultative**.

Les clés révélées de l'organisme de certification (CAPK) sont nécessaires pour l'authentification de données hors ligne. L'utilisation des mauvaises clés révélées de l'organisme de certification (CAPK) mènera à des échecs d'authentification de données hors ligne et possiblement au refus de l'opération. Les terminaux **doivent** être en mesure de stocker jusqu'à six clés révélées de l'organisme de certification (CAPK) par fournisseur de services de paiement.

Le tableau 2 fournit des renseignements détaillés sur les dates d'expiration des clés révélées de l'organisme de certification (CAPK), les dates prescrites de chargement dans le terminal, les premières dates d'utilisation par l'émetteur et les dates prescrites de retrait des clés.

Tableau 2 : cycle de vie de la gestion des clés révélées de l'organisme de certification (CAPK)

Taille des clés	Date d'expiration	Date de chargement prescrite pour les banques administratrices	Première date d'utilisation par l'émetteur	Date de retrait prescrite des terminaux
1024	31 décembre 2009	31 décembre 2003	1 <sup>er</sup> janvier 2004	30 juin 2010
1152	31 décembre 2014	31 décembre 2005	1 <sup>er</sup> mars 2006	30 juin 2015
1408	31 décembre 2017 ou après	31 décembre 2006	1 <sup>er</sup> janvier 2007	six mois après l'expiration
1984	31 décembre 2017 ou après	31 décembre 2006	1 <sup>er</sup> janvier 2007	six mois après l'expiration

**MEILLEURE PRATIQUE :** American Express, à l'instar des autres fournisseurs de services de paiement, évalue le cycle de vie des clés révélées de l'organisme de certification (CAPK) chaque année. Par conséquent, les dates d'expiration indiquées dans le tableau 2 peuvent changer. American Express **recommande** que les terminaux ne stockent pas la date d'expiration, à moins qu'elle puisse facilement être mise à jour.

Les clés révélées de l'organisme de certification (CAPK) d'American Express sont envoyées par courriel aux fournisseurs de terminaux lorsque ceux-ci communiquent avec American Express afin de lancer le processus de certification du terminal pour sa conformité aux spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)). Les clés révélées de l'organisme de certification (CAPK) d'American Express sont distribuées dans un format fixe. Les clés révélées de l'organisme de certification (CAPK) et le format fixe sont expliqués en détail à l'annexe A.

## Étape 5 : traitement des restrictions

### so Configuration d'American Express identique

Le terminal exécute un certain nombre de vérifications afin de déterminer s'il doit autoriser ou non une opération ou si des restrictions géographiques propres à un produit (p. ex., utilisation dans le pays d'origine seulement) ou des restrictions relatives à un type de service (p. ex., ne peut être utilisée pour des retraits de fonds) s'appliquent.

## Étape 6 : vérification de l'identité du titulaire de la Carte



**so Configuration d'American Express identique. Toutefois, des exigences supplémentaires sont fournies pour les fonctionnalités opérationnelles non prévues par les spécifications EMV.**

La vérification de l'identité du titulaire de la Carte sert à déterminer si ce dernier est un titulaire légitime et si la Carte à puce a été volée ou non. Voici les différents types de vérification de l'identité du titulaire de la Carte (CVM) prises en charge par le terminal dans un environnement de vente de détail :

- NIP crypté hors ligne
- NIP en clair hors ligne
- Signature
- Aucune vérification de l'identité du titulaire de la Carte (CVM) exigée

Les vérifications de l'identité du titulaire de la Carte (CVM) prises en charge par une Carte à puce ou un terminal conforme aux spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) dépendront de la mise en œuvre des spécifications EMV dans le pays visé.

**Exigences relatives au NIP.** L'utilisation d'un NIP – en clair ou crypté – avec les Cartes à puce (EMV) entraîne de nouvelles exigences techniques et opérationnelles. Les sections ci-après exposent en détail les exigences relatives au NIP d'American Express.

- American Express **exige** que le terminal soit en mesure de prendre en charge à la fois les NIP en clair et les NIP cryptés.
- Le terminal **doit** afficher le montant de l'opération (ou une estimation exacte) à l'intention du titulaire de la Carte avant que celui-ci ne saisisse son NIP.
- Les claviers de composition du NIP **devraient** être conçus pour tenir compte des besoins de tous les titulaires de Carte (p. ex., inclure un point en relief sur la touche 5 afin d'aider les clients atteints de cécité partielle, etc.)
- Les claviers de composition du NIP **devraient** être placés à des endroits pouvant satisfaire aux besoins de tous les titulaires de Carte (p. ex., afin de permettre aux clients en fauteuil roulant de saisir leur NIP). De plus, le titulaire de la Carte **devrait** être en mesure de voir sa Carte en tout temps.
- Si un clavier de composition du NIP est utilisé, il **doit** être conforme aux spécifications EMV, aux normes de sécurité des données du secteur des Cartes de paiement (normes PCI DSS) relatives aux appareils de saisie du NIP et aux exigences du pays dans lequel il est utilisé. American Express n'a aucune exigence minimale en ce qui concerne les claviers de composition du NIP autres que celles prévues dans ces spécifications, ces normes et ces exigences.

**Erreurs d'entrée du NIP.** Si le titulaire de la Carte se trompe en saisissant son NIP, des messages doivent guider le marchand et le titulaire de la Carte.

*Exigences propres aux spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) concernant les erreurs d'entrée du NIP*

Si une Carte est présentée à un terminal et si le compteur d'essais de saisie du NIP affiche « 1 » – il vous reste un essai pour saisir votre NIP correctement – le terminal **devrait** produire un message-guide approprié afin d'informer le marchand et le titulaire de la Carte de la situation (pour obtenir des renseignements sur les messages affichés par le terminal, voir l'annexe B). Si le compteur d'essais de saisie du NIP affiche « 0 », le terminal **devrait** poursuivre l'opération, ayant inscrit les octets applicables dans le champ « Résultats de vérification du terminal (TVR) », qui indique que la limite d'essais de saisie du NIP a été dépassée.

**Dispense de NIP.** La dispense de NIP est une option qui vise à faciliter la tâche des consommateurs au cours de la mise en œuvre de la fonction de saisie du NIP. Elle peut être activée si le titulaire de la Carte ne peut se souvenir de son NIP ou s'il est temporairement incapable de le saisir. Dans ce cas, le marchand peut avoir l'option de « dispenser » le client de saisir son NIP et permettre à la puce et au terminal de lancer la prochaine vérification de l'identité du titulaire de la Carte (CVM), qui sera probablement la signature.



La dispense de NIP **doit** être possible seulement si toutes les exigences suivantes sont remplies :

- le terminal est surveillé;
- le terminal est configuré pour offrir la dispense de NIP;
- le marchand et la banque administratrice acceptent de prendre en charge la dispense de NIP; et
- la liste des vérifications de l'identité du titulaire de la Carte (CVM) indiquée sur la Carte à puce permet le lancement d'une autre vérification de l'identité du titulaire de la Carte (CVM) prise en charge par le terminal.

Si la dispense de NIP est utilisée, le champ « Résultats de vérification du terminal (TVR) » **doit** enregistrer que « le NIP a été demandé, le terminal était muni d'un clavier de composition du NIP qui fonctionnait, mais le NIP n'a pas été saisi (octet 3, bit 4) ».

**MEILLEURE PRATIQUE :** American Express **recommande** que la fonction de dispense de NIP soit une option configurable du terminal et que cette fonction puisse être désactivée au moment opportun, p. ex., si un pays a complété le déploiement de la technologie relative au NIP.

**Remarque importante :** la dispense de NIP limite à la fois la réduction des fraudes et les avantages opérationnels liés à l'utilisation du NIP. Par conséquent, il s'agit d'une fonction qui **devrait** servir seulement au cours de la période de transition vers l'utilisation du NIP comme vérification de l'identité du titulaire de la Carte (CVM) normale. Il est en outre important de noter que les émetteurs refuseront probablement les opérations avec dispense de NIP, étant donné qu'elles comportent plus de risques que les opérations avec saisie du NIP.

### Étape 7 : gestion du risque à partir du terminal

#### ▲ Configuration d'American Express différente

À l'étape de gestion du risque à partir du terminal, un nombre de vérifications fondées sur les renseignements fournis par la Carte et la banque administratrice sont exécutées. Les spécifications EMV expliquent de nombreuses vérifications qui peuvent être effectuées dans le cadre de la gestion du risque à partir du terminal.

- ▲ American Express **exige** que la vérification du maximum permis sans autorisation et la sélection aléatoire d'opérations soient exécutées. Tous les autres types de vérifications sont **facultatifs**, en fonction de la configuration du terminal. Le terminal inscrit les résultats de ces vérifications dans le champ « Résultats de vérification du terminal (TVR) » aux fins d'utilisation future.

### Étape 8 : première analyse des actions du terminal

#### ▲ Configuration d'American Express différente

La première analyse des actions du terminal permet de comparer les résultats de l'authentification de données hors ligne, du traitement des restrictions, de la vérification de l'identité du titulaire de la Carte et de la gestion du risque à partir du terminal aux règles fixées par l'émetteur et American Express. Ce processus permet de déterminer si le terminal doit demander que l'opération soit autorisée hors ligne, envoyée en ligne aux fins d'autorisation ou refusée hors ligne.

Les règles fixées par l'émetteur sont inscrites dans les champs « Code d'action de l'émetteur (IAC) » de la Carte à puce, et les règles fixées par American Express sont inscrites dans les champs « Code d'action



du terminal (TAC) » du terminal. Le terminal compare les valeurs inscrites dans le champ « Résultats de vérification du terminal (TVR) » au cours du traitement hors ligne à celles inscrites dans les champs « Code d'action de l'émetteur (IAC) » et « Code d'action du terminal (TAC) » afin de déterminer si l'une ou l'autre des conditions d'opération énoncées dans le champ « Résultats de vérification du terminal (TVR) » indique que le terminal doit demander que l'opération soit refusée ou envoyée en ligne. Si ce n'est pas le cas, le terminal demandera que l'opération soit approuvée hors ligne au moyen de la Carte à puce.

Après avoir déterminé s'il doit demander que l'opération soit autorisée, refusée ou envoyée en ligne à la banque administratrice, le terminal demande que la Carte à puce produise un cryptogramme. Le type de cryptogramme à produire n'est pas le même si le terminal demande un certificat d'opération (TC) aux fins d'autorisation, un cryptogramme de demande d'autorisation (ARQC) aux fins d'une demande d'aller en ligne ou un cryptogramme d'authentification de l'application (AAC) aux fins de refus.

- ▲ Comme pour les autres fournisseurs de services de paiement, des valeurs précises **doivent** être saisies pour American Express dans le champ « Code d'action du terminal (TAC) »; des valeurs qui doivent être chargées dans les terminaux. Ces valeurs sont indiquées dans le tableau ci-après :

Tableau 3 : Valeurs à saisir dans le champ « Code d'action du terminal (TAC) » pour American Express

Par défaut	C8 00 00 00 00
En ligne	C8 00 00 00 00
Refus	00 00 00 00 00

### Étape 9 : première analyse des actions de la Carte

#### so Configuration d'American Express identique

Après avoir reçu la demande du terminal, la Carte à puce effectue la première analyse des actions à effectuer. À cette étape-ci, la Carte à puce effectue les vérifications relatives à la gestion du risque afin de déterminer la réponse appropriée à donner à la demande du terminal. La Carte à puce peut rejeter la demande du terminal. Par exemple, la Carte à puce pourrait recevoir une demande du terminal concernant une autorisation hors ligne, mais pourrait retourner un cryptogramme indiquant qu'une opération en ligne ou un refus hors ligne est exigé. Les paramètres associés à la fonction de gestion du risque de la Carte à puce (tels qu'ils sont choisis par l'émetteur) dictent la marche à suivre. La Carte à puce inscrit les résultats de cette analyse dans le champ « Résultats de vérification de la Carte (CVR) » pour utilisation future.

### Étape 10 : traitement des opérations en ligne

#### ▲ Configuration d'American Express différente

Si la Carte à puce ou le terminal détermine que l'opération exige une autorisation en ligne (et si le terminal peut traiter les opérations en ligne), le terminal transmet un message de demande d'autorisation en ligne à la banque administratrice. Si la Carte à puce ou le terminal détermine que l'opération exige une autorisation hors ligne, le terminal terminera le traitement de l'opération (voir l'étape 15).

Si l'opération doit être envoyée en ligne, mais que le terminal ne peut exécuter cette tâche pour des raisons techniques, le terminal procédera à une deuxième analyse des actions à effectuer (voir l'étape 12).

Le message envoyé à la banque administratrice inclut le cryptogramme produit par la Carte à puce (p. ex., l'ARQC), les données ayant servi à produire le cryptogramme et les codes présentant les résultats relatifs au traitement hors ligne, y compris les « Résultats de vérification du terminal (TVR) » et les « Résultats de vérification de la Carte (CVR) ».

Si l'émetteur a validé avec succès le cryptogramme fourni par la Carte à puce, les données d'authentification de l'émetteur (IAD) seront incluses dans le message de réponse à la demande d'autorisation. Ces données comprennent un cryptogramme produit par l'émetteur appelé « ARPC » et un code de réponse à la demande d'autorisation (ARC) qui décrit la décision de l'émetteur relativement à l'opération. La réponse peut également inclure des mises à jour pour la Carte à puce, appelées « scripts de l'émetteur » (voir l'étape 14 : traitement du script de l'émetteur).

Si un terminal reçoit une réponse à la demande d'autorisation qui contient des renseignements valides sur le résultat de l'opération, mais ne contient pas les données de la puce requises pour effectuer une authentification de l'émetteur, il s'agit d'une opération simplifiée (voir l'étape 12 : deuxième analyse des actions du terminal).

- ▲ À l'instar des autres fournisseurs de services de paiement, American Express a établi un format de message unique, qui peut varier d'un pays à l'autre. Le tableau ci-dessous illustre les éléments de données **obligatoires** et **facultatifs** pour les opérations par Cartes American Express.

Tableau 4 : éléments de données **obligatoires** et **facultatifs**

### Éléments de données obligatoires

#### MESSAGE DE DEMANDE D'AUTORISATION

- Code des capacités de traitement du terminal
- Code de méthode de saisie des données de la Carte
- Montant, montant autorisé de l'opération (autorisation) et montant de l'opération finale (règlement)
- Autre montant
- Profil du système d'échange de l'application
- Numéro de compte principal (PAN)
- Numéro de séquence du PAN
- Compteur d'opérations de l'application
- ARQC
- Données sur l'application de l'émetteur
- Code de pays du terminal
- Résultats de vérification du terminal (TVR)
- Code de devise de l'opération
- Date de l'opération
- Type d'opération
- Numéro imprévisible

#### MESSAGE DE RÉPONSE À LA DEMANDE D'AUTORISATION

- Données d'authentification de l'émetteur (IAD) (inclut l'ARPC et le code de réponse à la demande d'autorisation (ARC))
- Données relatives au script de l'émetteur

## Éléments de données supplémentaires facultatifs

### MESSAGE DE DEMANDE D'AUTORISATION

- Code de traitement de rechange
- Code de l'application (AID) (terminal)
- Numéro de version de l'application (terminal)
- Données sur le cryptogramme
- Résultats relatifs aux vérifications de l'identité du titulaire de la Carte (CVM)
- Codes d'action de l'émetteur (IAC) : refus, en ligne et par défaut

## Étape 11 : authentification de l'émetteur

### so Configuration d'American Express identique

Si la réponse à la demande d'autorisation contient un ARPC, la Carte à puce **doit** effectuer une authentification de l'émetteur en validant le cryptogramme de réponse. Après avoir reçu une réponse à la demande d'autorisation contenant un ARPC, le terminal présente ce dernier à la Carte à puce au moyen de la commande d'authentification externe. Cela permet de vérifier si la réponse a été envoyée par le véritable émetteur et d'empêcher les criminels de déjouer les dispositifs de sécurité de la Carte à puce en simulant un traitement en ligne et en autorisant frauduleusement une opération.

## Étape 12 : deuxième analyse des actions du terminal

### so Configuration d'American Express identique

À cette étape de l'opération, le terminal peut faire face à trois scénarios différents.

- **Les données relatives à la Carte à puce (EMV) ont été reçues dans la réponse à la demande d'autorisation** : si l'émetteur a authentifié la Carte avec succès puis retourné les données d'authentification de l'émetteur (IAD), le terminal peut utiliser soit le code de réponse à la demande d'autorisation (ARC) contenu dans les données d'authentification de l'émetteur (IAD), soit le message de réponse à la demande d'autorisation afin de déterminer s'il doit demander que la Carte à puce autorise ou refuse l'opération.
- **Aucunes données relatives à la Carte à puce (EMV) n'ont été reçues dans la réponse à la demande d'autorisation** : si le terminal ne reçoit aucunes données d'authentification de l'émetteur (IAD) dans le message de réponse, il détermine s'il doit demander que la Carte à puce autorise ou refuse l'opération. Cela se fait en utilisant le résultat de l'opération tel qu'il est inscrit dans le message de réponse provenant de la banque administratrice.

Le terminal **doit** alors remplir le champ « Code de réponse à la demande d'autorisation (ARC) » (étiquette EMV « 8A ») pour qu'il soit retourné à la Carte à puce à partir du terminal par suite de la deuxième commande visant à produire un cryptogramme d'application (AC), comme suit :

- « 00 » pour une autorisation (p. ex., « 3030 » dans le format ASCII)
- « 02 » pour une autorisation verbale (p. ex., « 3032 » dans le format ASCII)
- « 05 » pour un refus (p. ex., « 3035 » dans le format ASCII)

- **Le terminal a été incapable de se connecter** : si le terminal est incapable de se connecter, il détermine s'il doit demander une autorisation ou un refus hors ligne à la Carte à puce, en fonction du fait que le code d'action du terminal (TAC) (valeur par défaut) est inscrit ou non dans le terminal et que le code d'action de l'émetteur (IAC) (valeur par défaut) a été obtenu de la Carte à puce.

### Étape 13 : deuxième analyse des actions de la Carte

#### so Configuration d'American Express identique

Après la deuxième analyse des actions du terminal, le terminal demandera à la Carte à puce d'autoriser ou de refuser l'opération. La Carte à puce exécutera alors sa propre analyse des actions à effectuer et prendra la décision finale concernant l'autorisation ou le refus de l'opération.

La Carte à puce peut refuser une opération autorisée par l'émetteur en fonction des résultats de l'authentification de l'émetteur et des paramètres relatifs à l'émetteur inscrits sur la Carte à puce. La Carte à puce produit un cryptogramme de type TC (certificat d'opération) pour les opérations autorisées et de type AAC (cryptogramme d'authentification de l'application) pour les opérations refusées.

### Étape 14 : traitement du script de l'émetteur

#### so Configuration d'American Express identique. Toutefois, des exigences supplémentaires sont fournies pour les fonctionnalités opérationnelles non prévues par les spécifications EMV.

En vertu des spécifications EMV, l'émetteur est en mesure d'envoyer des mises à jour à la Carte à puce grâce à des scripts inscrits dans le message de réponse à la demande d'autorisation. Un script de l'émetteur est une série de commandes élaborée et envoyée par l'émetteur aux fins de mise à jour et de gestion des Cartes à puce.

Voici, expliquées en détail, les exigences d'American Express pour le traitement du script de l'émetteur.

- Le terminal **doit** traiter le script, que l'opération ait été autorisée ou refusée. Le terminal envoie les commandes définies dans le script à la Carte à puce, avant ou après avoir renvoyé le cryptogramme d'application (AC) final, en fonction du type de script envoyé.
- Le terminal **doit** traiter les scripts de l'émetteur avec la Carte à puce, que l'authentification de l'émetteur ait réussi ou non ou que l'opération ait été autorisée ou refusée. Le terminal **ne doit pas** envoyer un message au marchand indiquant soit la fin de l'opération, soit le retrait de la Carte, et ce, jusqu'à ce que la Carte à puce ait traité le script.
- Dans toute réponse à la demande d'autorisation, l'émetteur peut envoyer plus d'un script. Ces scripts peuvent contenir plusieurs commandes, qui **doivent** être traitées dans l'ordre de présentation de ces dernières dans le script. Si la Carte répond à une commande par un script de l'émetteur indiquant une opération réussie ou une mise en garde, le terminal **doit** traiter les commandes restantes. Si la Carte renvoie un message d'erreur, le terminal **doit** cesser le traitement de toute commande restante.
- Les terminaux **doivent** prendre en charge le traitement du script de l'émetteur au cours de cette étape de l'opération, ainsi qu'à l'étape 13, avant le lancement de la deuxième commande visant à produire un cryptogramme d'application (AC) (p. ex., il doit prendre en charge les étiquettes « 71 » et « 72 »).

Voici un exemple d'une vérification d'un script de l'émetteur présentant plus d'une commande.

#### Données de vérification

```
72459F18048000000086158424000210FEBF34F00B7CE770DC
61DA847BFB1E59862504DA8E002000000000000000000420141
035E031F020000000000000000AC7F4DF1D624A0E
```

Tableau 5 : éléments de données contenus dans le script de l'émetteur

Élément de données	Description
72	Étiquette du script
45H (69D)	Taille
9F18	Étiquette
04H (4D)	Taille de l'étiquette
80000000	Code du script
86	Étiquette de la commande
15H (21D)	Taille
8424	Commande de modification du NIP
0002	P1 P2
10H (16D)	Taille
FEBF34F00B7CE770	Données
DC61DA847BFB1E59	CAM
86	Étiquette de la commande
25H (37D)	Taille
04DA	Put data command (commande envoyée à la Carte à puce)
8E00	Mise à jour de la liste des vérifications de l'identité du titulaire de la Carte (CVM)
20H (32D)	Taille
0000000000000000420141035E031F020000000000000000	Données
AC7F4DF1D624A0ED	CAM

*H = Hexadécimale*

*D = Représentation décimale de la valeur hexadécimale*

Voici un exemple d'une vérification d'un script de l'émetteur présentant une seule commande.

#### Données de vérification

72179F180400004000860E04DA9F580900C7356286E3779889

Tableau 6 : éléments de données contenus dans le script de l'émetteur

Élément de données	Description
72	Étiquette du script
17H (23D)	Taille
9F18	Étiquette
04H (4D)	Taille de l'étiquette
00004000	Code du script
86	Étiquette de la commande
0EH (14D)	Taille
04DA	Put data command (commande envoyée à la Carte à puce)
9F58	Mise à jour de la liste des vérifications de l'identité du titulaire de la Carte (CVM)
09H (9D)	Taille
00	Données
C7356286E3779889	CAM

*H = Hexadécimale*

*D = Représentation décimale de la valeur hexadécimale*

### Étape 15 : traitement final de l'opération

**so** Configuration d'American Express identique. Toutefois, des exigences supplémentaires sont fournies pour les fonctionnalités opérationnelles non prévues par les spécifications EMV.

Le terminal exécute le traitement final afin de compléter l'opération. Si la signature a été désignée comme vérification de l'identité du titulaire de la Carte (CVM), c'est également à cette étape de l'opération que le terminal imprime le reçu et que le client doit le signer.

Exigences relatives au reçu en vertu des spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)). Les terminaux **doivent** satisfaire à certaines exigences relatives aux formats et aux données en ce qui a trait aux reçus d'opération. Ces exigences sont énoncées dans les tableaux suivants et les textes qui les accompagnent.

Légende pour le tableau 7, colonne titrée O, P, F ou C : **O : obligatoire** (exigé en tout temps), **P : privilégié** (meilleure pratique), **F : facultatif** (peut être présent) et **C : conditionnel** (en fonction de la situation)

Tableau 7 : Tableau sur les données devant figurer sur le reçu d'opération

Description du champ	O/P/F/C
Numéro de l'établissement	O*
Nom de l'établissement	O*
Adresse de l'établissement	O*
Type d'opération (p. ex., vente ou remboursement)	O*
Numéro de compte principal (PAN)	O* <sup>1</sup>
Date d'expiration de la Carte (MMAA)	O*
Source des données de l'opération (p. ex., bande magnétique, saisie manuelle, puce)	O*
Date de l'opération	O*
Code du terminal	O*
Numéro de l'opération	O*
Réponse pour l'opération (p. ex., code d'autorisation)	O*
Montant de l'opération (incluant le symbole de devise)	O*
Demande de signature (n'est pas requise pour les opérations avec saisie d'un NIP)	C
Espace pour la signature (n'est pas requise pour les opérations avec saisie d'un NIP)	C
Déclaration (p. ex., « Veuillez porter au débit de mon compte »)	O
Message pour rappeler au titulaire de conserver son reçu	O
État du NIP (requis uniquement pour les opérations avec saisie du NIP) (p. ex., NIP vérifié, NIP verrouillé)	C
Code de l'application (AID)	O
Montant du pourboire	F
Message de diagnostic	P
Date d'entrée en vigueur de la Carte (MMAA)	P
Heure de l'opération	P
Nom privilégié de l'application	C <sup>2</sup>
Nom du fournisseur de services de paiement/indicateur de l'application	O
Type de Carte	F
Nom du titulaire	F <sup>3</sup>
Message de courtoisie	F
Numéro d'inscription aux fins de la taxe	F
Numéro du reçu (différent du numéro de l'opération)	F

Description du champ	O/P/F/C
Montant des biens	F
Description des biens	F
Taux des taxes	F
Numéro de version du fichier d'exceptions	F
Numéro de version du logiciel du terminal	F
Type de cryptogramme/valeur	P
<i>*Indique les éléments de données qui <b>doivent</b> être inscrits sur un support électronique au cours d'une opération avec saisie d'un NIP.</i>	

#### Remarques sur le tableau 7

1. Le numéro de compte principal (PAN) inscrit sur le reçu du titulaire de la Carte **doit** être masqué conformément aux normes PCI DSS et aux prescriptions des lois de votre région.
2. Si le nom privilégié de l'application est inscrit et si le terminal prend en charge l'index du tableau de codes de l'émetteur approprié, cet élément de données est **obligatoire**.
3. Le nom du titulaire de la Carte, s'il est imprimé, **devrait** l'être conformément à la norme [ISO-7813]. Le nom du titulaire de la Carte provient de la puce dans le cas d'une opération par Carte à puce (EMV) ou de la piste 1 dans le cas d'une opération par Carte à bande magnétique.

**MEILLEURE PRATIQUE :** l'impression d'un reçu **devrait** se faire dès que possible, de façon à coïncider avec le traitement de l'opération. Cela permet de réduire au minimum le temps d'attente du marchand et du titulaire de la Carte.

Exigences relatives à la mise en page du reçu en vertu des spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)). La seule exigence **obligatoire** touchant la mise en page du texte sur un reçu consiste à placer la plage de signature et le montant près l'un de l'autre. Tous les efforts **devraient** également être déployés afin d'assurer que les autres renseignements sont présentés logiquement et clairement (p. ex., placer la date et l'heure près l'une de l'autre, faire de même pour le numéro de Carte masqué et la date d'expiration, etc.)

La mise en page du reçu présentée à la figure 2 met en évidence les exigences supplémentaires relatives à un terminal traitant une opération par Carte à puce American Express. Le texte en rouge indique les exigences relatives à la mise en page propres aux opérations par Carte à puce (EMV).



Figure 2 : exigences relatives à la mise en page du reçu

### Mise en page du reçu

LOGO(S), LE CAS ÉCHÉANT  
COMMERCE DE DÉTAIL  
154, RUE PRINCIPALE  
MONTRÉAL (QUÉBEC)  
BN2 2LP

NUMÉRO D'ÉTABLISSEMENT : 999 999 999  
CODE DU TERMINAL : 12345

LOT N° 0001                      REÇU N° 125  
XXXXXXXXXX1003 – (C)

AMERICAN EXPRESS              DATE D'EXP. 05/12

AMEX OR

A000000025010001  
19 OCT. 07    15:33  
VENTE  
NRE : 1234567890  
NOM DE L'ARTICLE/ DESCRIPTION (FACULTATIF)  
NOM DE L'ARTICLE/ DESCRIPTION (FACULTATIF)  
CODE DE L'UTILISATEUR : 9999 (FACULTATIF)

MONTANT DE BASE                      250,00 \$  
POURBOIRE                                      \$  
TOTAL    \$

NIP VÉRIFIÉ

X \_\_\_\_\_  
Y DUPONT

TC – A2E51245C4D7E551  
CODE D'AUTORISATION : 252525

J'ACCEPTE DE PAYER LE MONTANT TOTAL  
INDIQUÉ CI-DESSUS CONFORMÉMENT À  
L'ENTENTE AVEC L'ÉMETTEUR DE LA CARTE.

COPIE DU MARCHAND

### Données figurant sur le reçu

Nom de l'établissement  
Adresse de l'établissement

Numéro de l'établissement  
Code du terminal

Numéro de l'opération  
PAN masqué et source des données de l'opération :  
(S) bande magnétique (M) saisie manuelle ou  
**(C) puce.**

Type de Carte et date d'expiration

**Indicateur de l'application ou nom privilégié  
de l'application**

**Code de l'application (AID) de la Carte**

Date et heure de l'opération

Type d'opération

Numéro du reçu

Montant de l'opération (incluant le  
symbole de devise)

Montant du pourboire

**État du NIP ou**

espace pour la signature et  
demande de signature

Nom du titulaire

**Type de cryptogramme et valeur**

Réponse pour l'opération (p. ex., code  
d'autorisation)

Déclaration



## SECTION 4 : TRAITEMENT SPÉCIAL D'UNE OPÉRATION

Malgré les répercussions importantes des spécifications EMV sur le matériel et les logiciels de terminal, les processus relatifs à la prise en charge d'une opération normale effectuée par un titulaire de Carte sont sensiblement les mêmes pour les opérations par Carte à bande magnétique que pour celles par Carte à puce (EMV). Toutefois, avec l'introduction de la Carte à puce, et plus particulièrement de la fonction de saisie du NIP, certaines opérations survenant dans des scénarios uniques exigent une attention particulière. La présente section définit les exigences d'American Express dans de tels cas.

4.1. Cas d'ordre technique	4.2. Cas d'ordre circonstanciel	4.3. Terminal de paiement sans surveillance
4.1.1. Traitement de recharge	4.2.1. Remboursements	4.3.1. Vérification de l'identité du titulaire à un TPSS
4.1.2. Retrait prématuré de la Carte	4.2.2. Opération sans présentation de la Carte	4.3.2. Traitement de recharge à un TPSS
4.1.3. Opérations avec autorisation verbale	4.2.3. Opération avec présentation à venir de la Carte	4.3.3. Capacité de connexion à un TPSS
4.1.4. Opérations refusées	4.2.4. Montant de l'opération encore inconnu	
4.1.5. Autorisation par intervention du marchand	4.2.5. Carte non accessible	
4.1.6. Annulations	4.2.6. Carte présentée à nouveau pour compléter l'opération	
	4.2.7. Ajout d'un pourboire	

### 4.1. Exigences des spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) relatives aux cas d'ordre technique

#### 4.1.1. Traitement de recharge

Si un terminal certifié par American Express choisit une application avec succès, mais ne peut compléter l'opération par Carte à puce (EMV) pour des raisons techniques, il peut traiter l'opération au moyen d'une méthode moins sécuritaire (p. ex., lecture de la bande magnétique); c'est ce qu'on appelle un traitement de recharge. Le terminal peut utiliser le traitement de recharge du moment que l'erreur technique survient avant la réponse de la Carte à la première commande visant à produire un cryptogramme d'application (AC). Si l'erreur survient après cette étape, l'opération **doit** être refusée et le traitement de recharge n'est pas permis. De plus, avant que le traitement de recharge soit autorisé, American Express **exige** qu'il y ait plusieurs essais d'utilisation de la puce (p. ex., un premier essai, puis de nouveaux essais). American Express **recommande** qu'en cas d'échec de l'utilisation de la puce, un terminal procède à deux autres essais visant à lire les données de la puce avant d'utiliser un traitement de recharge pour l'opération.

Le terminal **devrait** répondre au premier et au deuxième essai infructueux en affichant un message cohérent (p. ex., « VEUILLER INSÉRER DE NOUVEAU »). À la suite du dernier essai infructueux, le terminal **doit** inviter le marchand à tenter une lecture de la bande magnétique pour effectuer un traitement de recharge (p. ex., « VEUILLER GLISSER LA CARTE »).

Si le traitement de recharge vise une opération par Carte à puce (EMV), le terminal **doit** exécuter les vérifications normalement exécutées pour toutes les opérations par Carte à bande magnétique.

Il **ne doit pas** y avoir de traitement de rechange dans les situations suivantes :

- si la Carte est bloquée;
- si toutes les applications activées sont bloquées;
- si l'opération par Carte à puce (EMV) a déjà été refusée; ou
- si l'opération est traitée à un terminal de paiement sans surveillance (TPSS).

**Signalement d'un traitement de rechange.** L'interface reliant le terminal à la banque administratrice **doit** être munie d'un indicateur permettant de signaler clairement les opérations résultant d'un traitement de rechange. Il existe deux façons d'indiquer à American Express les opérations résultant d'un traitement de rechange.

#### Option 1 : indicateur de traitement de rechange

- p. ex., position 7 du code des données relatives au PdV (code de méthode de saisie des données sur la Carte) = 9 (traitement de rechange)

#### Option 2 : descripteur dérivé (utilise les codes des données relatives au PdV)

- Position 1 (code de capacité de saisie des données de la Carte) = 5 (Carte à puce)
- Position 6 (code pour opération avec présentation de la Carte) = 1 (opération avec présentation de la Carte)
- Position 7 (code de méthode de saisie des données sur la Carte)  $\neq$  5 (Carte à puce). Voici quelques exemples de valeurs possibles :
  - 2 (lecture de la bande magnétique)
  - 6 (saisie au clavier)
  - S (code de sécurité de la Carte de quatre chiffres [CSC4] ou code de lot de quatre chiffres [C4C], saisi au clavier)

**MEILLEURE PRATIQUE :** American Express **recommande** l'option 1, car elle permet de relever les opérations résultant d'un traitement de rechange avec plus d'exactitude.

**Maximum permis sans autorisation.** American Express **exige** qu'un maximum permis sans autorisation de zéro soit imposé pour toutes les opérations faisant l'objet d'un traitement de rechange, ce qui signifie que ces opérations **doivent** faire l'objet d'une demande d'autorisation en ligne.

**Saisie du numéro de compte principal (PAN).** Si l'opération ne peut être complétée au moyen de la puce ou de la bande magnétique, elle peut l'être en saisissant au clavier le PAN, sous réserve d'une entente avec votre banque administratrice.

#### 4.1.2. Retrait prématuré de la Carte

Dans le cadre d'une opération par Carte à puce (EMV), la Carte **doit** demeurer dans le terminal tout au long de l'opération; si le titulaire de la Carte ou le marchand la retire avant que le terminal ait complété l'opération, le terminal **doit** annuler celle-ci.

Si une autorisation a déjà été accordée, le terminal **doit** envoyer un message d'annulation si la banque administratrice et le terminal prennent en charge les annulations.

S'il est impossible d'envoyer un message d'annulation, le terminal **doit** annuler l'opération. Dans ce cas, aucunes données de règlement ne seront envoyées.

#### 4.1.3. Opérations avec autorisation verbale



Comme c'est actuellement le cas avec les opérations par Carte à bande magnétique, l'émetteur peut répondre à une demande d'autorisation en vous demandant d'appeler pour obtenir une autorisation verbale. Ce ne sont pas tous les terminaux qui prennent en charge ce type de message. Un terminal ne prenant pas en charge ce type de message **doit** traiter une réponse demandant une autorisation verbale comme un refus d'autorisation.

Dans ce cas, American Express exige ce qui suit :

le marchand **doit** retirer la Carte du terminal et la conserver aux fins d'utilisation durant le processus d'autorisation verbale, compte tenu que des renseignements ne figurant pas sur le reçu produit par le terminal peuvent être requis au cours de ce processus (par exemple, le CSC4 au recto de la Carte). Toutefois, le terminal **doit** compléter l'opération avec la Carte avant d'afficher tout message demandant le retrait de la Carte.

Cela peut se faire des deux façons suivantes.

**Option 1 :** le terminal et la puce complètent l'opération comme si elle avait été refusée (p. ex., si le terminal demande un cryptogramme d'authentification de l'application (AAC)).

- Le terminal **doit** conserver les données de l'opération jusqu'à ce que l'état de celle-ci ait été déterminé.
- Si l'opération est par la suite autorisée, le terminal **doit** permettre au marchand de saisir le code d'autorisation au moment de compléter l'opération. Le code d'autorisation **doit** être inclus dans la présentation de l'opération, tout comme l'ARQC que la Carte a produit avant l'autorisation en ligne.
- Si l'opération est par la suite refusée, elle **doit** l'être pendant qu'elle est dans le terminal, sans autre traitement des données de la Carte.

**Option 2 :** le terminal et la puce complètent l'opération comme si elle avait été autorisée (p. ex., si le terminal demande un certificat d'opération (TC)).

- Le terminal **doit** conserver les données de l'opération jusqu'à ce que l'état de celle-ci ait été déterminé.
- Si l'opération est par la suite autorisée, le terminal **doit** permettre au marchand de saisir le code d'autorisation au moment de compléter l'opération. Le code d'autorisation **doit** être inclus dans la présentation de l'opération, tout comme le certificat d'opération (TC) que la Carte a produit.
- Si l'opération est par la suite refusée, elle **doit** l'être pendant que la Carte est dans le terminal, sans autre traitement des données de la Carte.

**MEILLEURE PRATIQUE :** American Express **recommande** l'option 1, car elle est plus appropriée sur le plan technique. À l'étape de l'autorisation verbale, l'opération n'a pas encore réellement été autorisée.

#### 4.1.4. Opérations refusées

Normalement, quand un émetteur refuse une opération, le terminal effectue tout de même la deuxième analyse des actions du terminal et de la Carte.

Si l'opération est refusée, le marchand en est averti grâce à un message à l'écran du terminal. Si une opération est refusée par la Carte, le terminal ou l'émetteur, elle **ne doit pas** être traitée par une autre méthode de saisie des données (p. ex., lecture de la bande magnétique ou saisie au clavier du PAN).

**Opération refusée et conservation de la Carte.** Dans des cas exceptionnels, on peut demander au marchand (grâce à un code envoyé dans le message de réponse) de conserver la Carte. Cela est appelé « refuser et conserver » (ou « refuser et ramasser »). Ce code est généralement envoyé avec un script de l'émetteur, pour empêcher que d'autres opérations soient effectuées au moyen de la Carte à puce (EMV). Le message indiquant de conserver la Carte **ne doit pas** être affiché avant que la puce ait traité le script.

#### 4.1.5. Autorisation par intervention du marchand

Si la Carte à puce et le terminal ont établi qu'une opération doit être envoyée en ligne et s'il est impossible de communiquer avec la banque administratrice affiliée à American Express en raison de problèmes techniques, les valeurs par défaut du code d'action de l'émetteur (IAC) et du code d'action du terminal (TAC) font l'objet d'une vérification afin de déterminer si l'opération doit être autorisée ou refusée. Le marchand n'a aucun contrôle sur ce processus. Toutefois, dans le cas des opérations par Carte à bande magnétique, il peut décider d'accepter une telle opération à ses propres risques (sous réserve du contrat du marchand). C'est ce qu'on appelle l'autorisation par intervention du marchand.

American Express a élaboré un processus qui permettrait aux marchands qui effectuent actuellement des autorisations par intervention du marchand de continuer à le faire pour les opérations par Carte à puce (EMV). S'il est impossible de communiquer avec la banque administratrice affiliée à American Express et si le marchand souhaite effectuer une autorisation par intervention du marchand, un terminal **doit** exécuter les trois étapes suivantes :

**Étape 1 : vérification de l'admissibilité à l'autorisation par intervention du marchand.** Le terminal **doit** contenir une liste de tous les codes de l'application (AID), partiels ou complets, pour lesquels il prend en charge l'autorisation par intervention du marchand. Le terminal comparera le code de l'application (AID) inscrit sur la puce de la Carte aux codes de l'application (AID) figurant sur sa liste. S'il y a correspondance, la Carte peut faire l'objet d'une autorisation par intervention du marchand.

Si le terminal appartient à un marchand ou à une banque administratrice qui souhaite prendre en charge l'autorisation par intervention du marchand pour les opérations par Carte American Express, le terminal **doit** être muni d'un indicateur spécifiant que l'autorisation par intervention du marchand est permise pour toutes les applications de paiement valides d'American Express.

Si le terminal trouve une application qui est admissible à l'autorisation par intervention du marchand, il **doit** effectuer l'autorisation par intervention du marchand telle qu'elle est décrite aux étapes 2 et 3. Dans l'éventualité où le résultat de la vérification de l'admissibilité indique que l'autorisation par intervention du marchand n'est pas possible, le traitement de l'opération doit se poursuivre au moyen des valeurs par défaut du code d'action du terminal (TAC) et du code d'action de l'émetteur (IAC).

**Étape 2 : code d'action de l'autorisation par intervention du marchand (SAC).** Un terminal prenant en charge l'autorisation par intervention du marchand **devrait** avoir un code d'action de l'autorisation par intervention du marchand (SAC) aux seules fins de traiter l'autorisation par intervention du marchand (un code d'action (SAC) par code de l'application (AID) pris en charge). Afin de traiter l'autorisation par intervention du marchand, le terminal **devrait** comparer le contenu du champ « Résultats de vérification du terminal (TVR) » au code d'action de l'autorisation par intervention du marchand (SAC) relatif au code de l'application (AID) pris en charge. Si l'un au l'autre des bits du champ « Résultats de vérification du terminal (TVR) » correspondant est inscrit, le terminal **devrait** demander le refus de l'opération. Le tableau suivant présente les valeurs par défaut du code d'action de l'autorisation par intervention du marchand (SAC) d'American Express.

Tableau 8 : valeurs par défaut du code d'action de l'autorisation par intervention du marchand (SAC) d'American Express \*

Octet	Bit	Valeur
1	8	Authentification des données hors ligne non effectuée
1	7	L'authentification des données permanentes hors ligne a échoué
1	6	Données de la Carte à puce manquante
1	5	La Carte figure dans le fichier d'exception du terminal
1	4	L'authentification des données dynamiques hors ligne a échoué
2	7	Application échue
2	5	Le service demandé n'est pas permis pour cette Carte
3	8	La vérification de l'identité du titulaire de la Carte a échoué
3	6	La limite d'essais de saisie hors ligne du NIP a été dépassée
3	4	La saisie hors ligne du NIP est exigée, présence d'un clavier de composition du NIP, mais NIP non saisi
4	6	Limite hors ligne supérieure pour opérations consécutives dépassée

\*Ce tableau correspond à une valeur hexadécimale du code d'action de l'autorisation par intervention du marchand (SAC) de « F8 50 A8 20 00 ».

**Étape 3 : vérification du montant.** La dernière vérification que le terminal effectue dans le cadre d'une autorisation par intervention du marchand concerne le montant de l'opération. C'est ce qu'on appelle la vérification du montant. Le terminal **doit** prévoir un seuil propre aux autorisations par intervention du marchand (autre que zéro). Pour qu'une opération soit autorisée par intervention du marchand, le montant de l'opération **doit** être situé sous ce seuil. Si la valeur de l'opération dépasse ce seuil, l'opération **doit** faire l'objet d'une autorisation verbale.

**Exigences supplémentaires relatives à l'autorisation par intervention du marchand.** Les exigences supplémentaires définies par American Express en ce qui a trait au processus d'autorisation par intervention du marchand figurent ci-après.

*a. Validation supplémentaire à un terminal au cours de l'acceptation de l'opération*

Les exigences définies ci-dessus ne remplacent pas la validation normale qui **doit** être effectuée dans le cadre du processus d'autorisation par intervention du marchand; cela inclut le seuil établi pour l'autorisation par intervention du marchand.

*b. Messages affichés à l'écran des terminaux à l'intention des titulaires de la Carte*

Les messages affichés à l'intention des titulaires de la Carte et des marchands par les terminaux **devraient** être identiques à ceux utilisés quand le système est en mesure d'effectuer une autorisation en ligne auprès de la banque administratrice. Dans certains cas, l'autorisation d'un superviseur ou une autorisation verbale peut être requise. Toutefois, cette situation s'applique généralement aux opérations dont le montant est élevé, pour lesquelles une telle intervention est considérée comme normale.

*c. Codes d'autorisation*

Dans la mesure du possible, le terminal **devrait** produire un code d'autorisation aléatoire et en temps d'arrêt aux fins d'affichage au terminal et d'impression sur les reçus. Le pseudo-code d'autorisation **ne doit pas** être intégré aux données sur l'opération présentée pour laquelle il a été créé.

#### 4.1.6. Annulations

Les annulations servent à invalider les opérations effectuées qui contiennent une erreur (p. ex., l'opération a déjà été envoyée aux fins d'autorisation quand le marchand ou le titulaire de la Carte se rend compte que le montant de l'opération est inexact). Les terminaux doivent envoyer des messages d'annulation seulement quand l'opération doit être annulée une fois la communication établie avec la banque administratrice.








En fonction des protocoles spécifiques de messages d'annulation utilisés, le message d'annulation peut contenir ou non les données sur la Carte à puce (EMV), car ces données sont **facultatives** pour les messages d'annulation. Si elles figurent dans le message d'annulation, elles doivent être une copie des données sur la Carte à puce qui figurent dans le message de demande d'autorisation correspondant qui fait l'objet de l'annulation. Le terminal **ne devrait** établir **aucune** nouvelle communication avec la puce pour traiter l'annulation.

Dans tous les cas, le terminal **doit** annuler l'opération et produire un reçu pour le titulaire de la Carte, indiquant que l'opération initiale a été annulée.



## 4.2. Exigences des spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) relatives aux cas d'ordre circonstanciel

Tableau 9 : exemples de cas d'ordre circonstanciel

Cas	Exemple
4.2.1. Remboursements 	<ul style="list-style-type: none"> <li>Remboursement d'une vente</li> </ul>
4.2.2. Opération sans présentation de la Carte 	<ul style="list-style-type: none"> <li>Commandes postales et téléphoniques</li> <li>Dépôts effectués par téléphone pour une réservation d'hôtel ou de voiture</li> </ul>
4.2.3. Opération avec présentation à venir de la Carte 	<ul style="list-style-type: none"> <li>Réservation de chambre d'hôtel</li> <li>Location de voiture</li> </ul>
4.2.4. Montant de l'opération encore inconnu 	<ul style="list-style-type: none"> <li>Distributeur d'essence</li> <li>Ouverture d'une note de bar</li> <li>Enregistrement dans un hôtel</li> <li>Prise en charge d'un véhicule de location</li> </ul>
4.2.5. Carte non accessible 	<ul style="list-style-type: none"> <li>Départ express d'un hôtel</li> <li>Remises d'un véhicule de location</li> </ul>
4.2.6. Carte présentée à nouveau pour compléter l'opération 	<ul style="list-style-type: none"> <li>Règlement de la note d'un hôtel effectué en personne</li> <li>Remise d'un véhicule effectué en personne à l'agence de location</li> </ul>
4.2.7. Ajout d'un pourboire 	<ul style="list-style-type: none"> <li>Salon de coiffure/barbier</li> <li>Ventes dans un restaurant</li> </ul>

TRAITEMENT SPÉCIAL  
D'UNE OPÉRATION

### 4.2.1. Remboursements

Les remboursements présentent moins de risques de fraude que les opérations normales. Par conséquent, American Express impose moins de restrictions concernant le traitement des remboursements. On peut traiter les remboursements en utilisant la puce ou la bande magnétique, ou en saisissant manuellement le PAN dans le terminal.

Si vous choisissez d'utiliser la puce, il n'est pas nécessaire d'effectuer toutes les étapes possibles pour une opération par Carte à puce (EMV). Il y a deux façons de traiter un remboursement au moyen d'une Carte à puce; dans les deux cas, le terminal **ne doit pas** indiquer que l'opération a été complétée après le renvoi du cryptogramme en réponse à la deuxième commande visant à produire un cryptogramme d'application (AC).

**Option 1 : opération complète par Carte à puce (EMV).** Si vous choisissez d'effectuer une opération complète par Carte à puce (EMV), American Express **recommande** que le terminal demande l'autorisation hors ligne de l'opération par la Carte à puce (p. ex., qu'il demande un certificat d'opération (TC)). Toutefois, il est possible de traiter en ligne les remboursements, au besoin (p. ex., grâce à un ARQC). Si, pour quelque raison que ce soit, la Carte refuse le remboursement, le cryptogramme d'authentification de l'application (AAC) **devrait** être rejeté, et l'ARQC, présenté aux fins de remboursement. Le terminal **devrait** traiter l'opération comme si elle avait été autorisée.

**Option 2 : données de la piste 2.** Si vous choisissez de ne pas effectuer une opération complète par Carte à puce (EMV), le terminal **doit** lire les données de la piste 2 de la puce et les utiliser pour traiter le

remboursement. Au moment de programmer le remboursement, vous pouvez soit utiliser des parties d'éléments de la piste 2, soit extraire les éléments de l'image de la piste 2. Cependant, n'utilisez pas l'image comme telle, étant donné qu'il n'est pas nécessaire que le CSC4 sur la bande magnétique et celui sur la puce soient identiques. De plus, une exigence relative aux normes PCI DSS prescrit que l'ensemble du contenu des données de la piste 2 ne doit pas être consigné une fois l'opération terminée. Le fait de voir à ce que vos terminaux puissent extraire le PAN de l'application et la date d'expiration de la puce (plutôt que d'utiliser toutes les données de la piste 2) contribue à assurer que vous satisfaites à l'exigence relative aux normes PCI DSS.

#### MEILLEURE PRATIQUE :

- American Express **recommande** que le terminal effectue des remboursements au moyen de l'option 2.
- American Express **recommande** que la gestion du risque à partir du terminal et l'autorisation en ligne ne soient pas effectuées pour des remboursements.

#### 4.2.2. Opération sans présentation de la Carte



Certaines opérations peuvent devoir être autorisées et réglées sans que le marchand n'ait accès à la Carte à puce, mais celui-ci pourra tout de même profiter des dispositifs de sécurité de celle-ci. Par conséquent, aucune exigence ne s'applique aux opérations sans présentation de la Carte, et les marchands **devraient** traiter ces opérations au moyen des procédés existants.

**MEILLEURE PRATIQUE :** quand ils traitent des opérations sans présentation de la Carte, les marchands devraient s'assurer d'utiliser les dispositifs de sécurité existants auxquels ils ont accès, tels que la vérification d'adresse et le CSC4.

#### 4.2.3. Opération avec présentation à venir de la Carte



Dans certains cas, les activités d'un marchand peuvent faire en sorte que celui-ci exige une assurance quant à la validité d'un compte-Carte avant la présentation de la Carte. C'est pourquoi les marchands peuvent souhaiter obtenir des renseignements sur la Carte auprès du titulaire avant la présentation de celle-ci. Par conséquent, aucune exigence ne s'applique aux opérations avec présentation à venir de la Carte, et les marchands **devraient** traiter ces opérations au moyen des procédés existants.

**MEILLEURE PRATIQUE :** American Express **recommande** que les opérations avec présentation à venir de la Carte soient effectuées pour des montants limités, afin d'éviter de causer des désagréments au titulaire de la Carte en réduisant inutilement les fonds disponibles sur sa Carte.

#### 4.2.4. Montant de l'opération encore inconnu



Dans certains cas, un marchand doit effectuer une opération par Carte à puce (EMV) avant de connaître le montant final de l'opération. Dans un scénario où le montant de l'opération est encore inconnu, une estimation peut être affichée, mais le marchand **doit** alors informer le titulaire de la Carte que le montant correspond à une estimation et peut par conséquent faire l'objet d'une modification. Si la différence entre le montant réel de l'opération et le montant initial de l'autorisation est supérieure à 15 %, le marchand **doit** présenter une autre demande d'autorisation pour la différence entre les deux montants.

Si un terminal n'est pas en mesure de consigner les données de l'opération par Carte à puce (EMV), toute autorisation supplémentaire exige que le titulaire de la Carte présente à nouveau sa Carte, sans quoi l'autorisation **doit** être entrée dans le format « saisie au clavier du PAN ».

**MEILLEURE PRATIQUE :** American Express **recommande** que toutes les données pertinentes des opérations par Carte à puce (EMV) découlant de l'autorisation soient consignées aux fins du processus de règlement, y compris le cryptogramme produit par la Carte.

#### 4.2.5. Carte non accessible



Parfois, le marchand ne connaîtra le montant final à facturer qu'après le départ du titulaire. Par conséquent, il n'aura pas accès à la Carte à puce. Les seules données de l'opération par Carte à puce (EMV) que le marchand aura alors en sa possession seront les données recueillies au cours de l'autorisation initiale et de toute autorisation supplémentaire. Si un terminal n'est pas en mesure de consigner les données de l'opération par Carte à puce (EMV), l'opération finale peut être traitée en saisissant le PAN au clavier.

#### MEILLEURE PRATIQUE :

- American Express **recommande** que l'opération finale soit présentée aux fins de règlement au moyen des données de la Carte à puce (EMV) tirées de l'autorisation la plus récente.
- Le message de la présentation **devrait** comprendre ce qui suit :
  - l'ARQC;
  - le montant estimé ou supplémentaire relatif à l'ARQC; et
  - le montant final de l'opération.

TRAITEMENT SPÉCIAL  
D'UNE OPÉRATION

#### 4.2.6. Carte présentée à nouveau pour compléter l'opération



Dans les cas où la Carte à puce a servi initialement à autoriser une opération avant que le montant de celle-ci ne soit connu et où elle est par la suite présentée à nouveau après l'établissement du montant final de l'opération, l'opération est complétée comme suit.

- Si la différence entre le montant réel de l'opération et le montant initial de l'autorisation est supérieure à 15 %, une opération par Carte à puce (EMV) normale **doit** être complétée avec présentation de la Carte pour le montant en entier, et toute autorisation antérieure **doit** par ailleurs être annulée, dans la mesure du possible.
- Si la différence entre le montant réel de l'opération et le montant initial de l'autorisation est égale ou inférieure à 15 %, l'opération **devrait** être complétée hors ligne. Cela peut se faire des deux façons suivantes.

**Option 1 : opération complète par Carte à puce (EMV).** Si vous choisissez d'effectuer une opération complète par Carte à puce, American Express **recommande** que le terminal demande l'autorisation hors ligne de l'opération par la Carte (p. ex., qu'il demande un certificat d'opération (TC)). Toutefois, si l'opération est envoyée en ligne, American Express **recommande** qu'elle soit envoyée comme message d'avertissement, dans la mesure du possible.

**Option 2 : données de la piste 2.** Si vous choisissez de ne pas effectuer une opération complète par Carte à puce (EMV), le terminal **doit** lire les données de la piste 2 de la puce et les utiliser pour traiter l'opération. Au moment de programmer l'opération, vous pouvez utiliser des parties d'éléments de la piste 2 ou extraire les éléments de l'image de la piste 2. Cependant, n'utilisez pas l'image comme telle, étant donné qu'il n'est pas nécessaire que le CSC4 sur la bande magnétique et celui sur la puce soient identiques. De plus, une exigence relative aux normes PCI DSS prescrit que l'ensemble du contenu des données de la piste 2 ne doit pas être consigné une fois l'opération terminée. Le fait de voir à ce que vos terminaux puissent extraire le PAN de l'application et la date d'expiration de la puce (plutôt que d'utiliser toutes les données de la piste 2) contribue à assurer que vous satisfaites à l'exigence relative aux normes PCI DSS.

**MEILLEURE PRATIQUE :** dans la mesure du possible, les données de la Carte à puce (EMV) tirées du message d'autorisation **devraient** être jointes aux données de l'opération dans le message de compensation.

#### 4.2.7. Ajout d'un pourboire



Pour certaines catégories de marchand, comme les restaurants, il est courant de permettre aux clients d'ajouter un pourboire au montant de l'opération. Il y a différentes façons d'ajouter un pourboire. American Express ne définit aucune méthode spécifique quant à l'ajout de pourboires.

**MEILLEURE PRATIQUE :** American Express **recommande** que le logiciel du terminal permette au titulaire de la Carte d'ajouter le montant du pourboire à l'opération avant de saisir son NIP. Cela permet à l'opération d'être traitée comme une « opération avec présentation de la Carte » normale.

### 4.3. Exigences des spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) relatives aux terminaux de paiement sans surveillance (TPSS)

L'introduction de la technologie EMV et des dispositifs de sécurité qui y sont associés permet d'augmenter de façon importante l'analyse de rentabilisation relative aux TPSS. L'authentification de la Carte et la vérification de l'identité du titulaire – qui reposaient auparavant sur l'observation physique de la Carte et de la signature par les employés – peuvent maintenant être effectuées grâce à une interaction directe entre une Carte à puce et un terminal.

Une opération par Carte à puce (EMV) est traitée essentiellement de la même façon à un TPSS qu'à un terminal normal, sauf pour quelques exceptions. Les sections suivantes expliquent ces exceptions, ainsi que les exigences d'American Express relatives aux TPSS qui y sont liées.

### 4.3.1. Vérification de l'identité du titulaire à un TPSS

L'introduction de la capacité de saisie hors ligne du NIP qu'offre la technologie EMV accroît de beaucoup le potentiel lié à la vérification de l'identité du titulaire de la Carte à un TPSS. Le traitement de rechange **ne doit pas** être pris en charge aux TPSS (p. ex., si la vérification de l'identité du titulaire de la Carte (CVM) la plus importante prise en charge à la fois par le terminal et la Carte est la saisie du NIP, le NIP **doit** être utilisé ou l'opération **doit** être refusée).

### 4.3.2. Traitement de rechange à un TPSS

Si le terminal prend en charge les opérations par Carte à puce (EMV), mais n'a pas encore fait l'objet d'une certification, ou s'il prend en charge les opérations par Carte à puce (EMV) d'autres fournisseurs de services de paiement, mais pas encore d'American Express, l'opération **doit** être traitée au moyen de la bande magnétique. Le terminal **ne doit pas** traiter l'opération au moyen du traitement de rechange.

Le traitement de rechange « lecture de la bande magnétique » **ne doit pas** être offert aux TPSS prenant en charge les spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)). Ces terminaux **doivent** rejeter une Carte à bande magnétique dont le code de service commence par 2 ou 6 (qui indique la prise en charge de la technologie EMV) si les données de la puce ne peuvent être lues.

### 4.3.3. Capacité de connexion à un TPSS

Selon l'environnement dans lequel ils sont déployés et le type d'opérations effectuées, certains de vos TPSS peuvent être munis d'une capacité de connexion. Le terminal **doit** inscrire des codes dans les messages d'autorisation et de présentation des opérations, indiquant que l'opération a été traitée à un TPSS.

#### MEILLEURE PRATIQUE :

- Si votre TPSS possède une capacité de connexion, American Express **recommande** qu'il ait un seuil relatif au terminal de zéro et qu'il tente de traiter toutes les opérations en ligne.
- Si le TPSS peut traiter des opérations en ligne, American Express **recommande** qu'il soit en mesure de saisir les données de la Carte à la demande de l'émetteur.
- Si votre TPSS ne peut pas effectuer des opérations en ligne, American Express **recommande** l'utilisation de fichiers d'exception et la validation des renseignements sur la Carte (y compris la date d'expiration) avant que le terminal soit autorisé à poursuivre l'opération.



## SECTION 5 : CERTIFICATION AEIPS (SPCPAE) DU TERMINAL



### 5.1. Introduction

L'intégration de la technologie EMV aux terminaux et aux systèmes hôtes peut accroître la complexité et les possibilités de problèmes liés à l'interopérabilité. Pour minimiser ces problèmes, nous avons établi un processus de certification qui **doit** être suivi.

Plusieurs parties peuvent devoir participer au processus de certification AEIPS (SPCPAE – spécifications pour le paiement par Carte à puce American Express) du terminal. Par exemple, American Express peut accorder une certification directement à un fournisseur de terminaux. Ou encore, une certification peut devoir être accordée par l'entremise d'une société indépendante, comme un revendeur ou une banque administratrice. Bien que les rôles joués par de nombreuses parties peuvent sous-entendre diverses responsabilités, le processus de certification AEIPS (SPCPAE) du terminal ne sera pas modifié de façon importante. Aux fins du présent document, nous ferons référence à chacune de ces parties comme étant un responsable de la certification.

La présente section n'énonce que les exigences normalisées à l'échelle mondiale en ce qui a trait à la certification SPCPAE d'un terminal; d'autres tests et exigences propres aux pays et aux banques administratrices peuvent exister. Le processus de certification peut également différer légèrement en fonction de la présence ou non de ces différences régionales. Veuillez communiquer avec votre représentant d'American Express afin de déterminer si des exigences supplémentaires s'appliquent à votre situation.

La présente section permettra aux responsables de la certification de réussir facilement leur mise en œuvre des spécifications pour le paiement par Carte à puce American Express à un terminal.

**Remarque importante :** avant d'obtenir une certification AEIPS (SPCPAE), le terminal **doit** déjà avoir fait l'objet d'une certification de niveau 1 et 2 par EMVCo. Bien que vous puissiez entamer le processus de certification AEIPS (SPCPAE) du terminal avant d'avoir reçu la certification de niveau 2 d'EMVCo, vous ne recevrez pas officiellement la certification AEIPS (SPCPAE) du terminal avant qu'EMVCo ne confirme sa certification.

**Obligations** des responsables de la certification

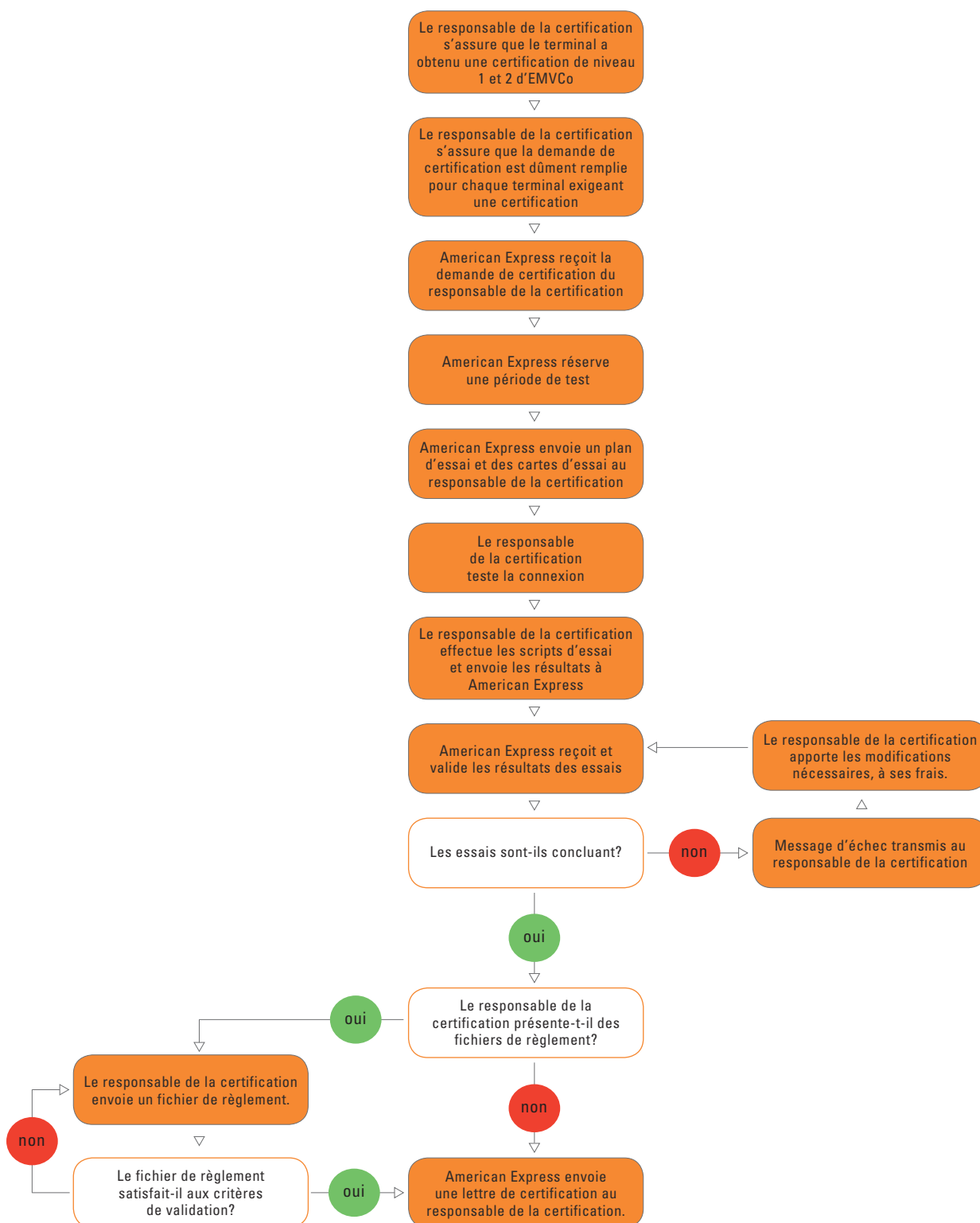
- s'assurer qu'American Express a certifié tous les terminaux pouvant prendre en charge les opérations par Carte à puce (EMV);
- s'assurer que la certification s'applique à chaque version du logiciel du terminal (et non seulement au noyau du logiciel de la puce) dans chaque pays où cette version est mise en œuvre pour qu'aucun problème pouvant causer le besoin d'une nouvelle certification du terminal ne survienne après le développement du logiciel d'application locale;
- s'assurer qu'American Express est mise au courant de toute modification apportée au logiciel.

**5.2. Processus de certification AEIPS (SPCPAE) du terminal**

Le diagramme suivant montre le processus de haut niveau de certification AEIPS (SPCPAE – spécifications pour le paiement par Carte à puce American Express) du terminal. Le processus débute quand un responsable de la certification présente une demande de certification dûment remplie à American Express. Ce formulaire peut être obtenu auprès de votre représentant d'American Express.



Figure 3 : étapes du processus de certification AEIPS (SPCPAE) du terminal



L'ensemble du processus de certification AEIPS (SPCPAE) du terminal prend généralement de quatre à six semaines. La durée de ce processus ne dépend pas que d'American Express, mais aussi du responsable de la certification. American Express prend les engagements suivants en ce qui concerne les délais liés à la certification AEIPS (SPCPAE) du terminal :

- American Express fera part au responsable de la certification de la réception de la demande de certification et lui fournira le document [AEIPS-TEST] ainsi que les cartes d'essai nécessaires dans la semaine suivant la réception de la demande.
- Une fois qu'elle a reçu les résultats des essais relatifs à la certification, American Express les validera et informera le responsable de la certification de l'état de cette validation dans les deux semaines suivant la réception des résultats.

Veuillez communiquer avec votre représentant d'American Express pour obtenir une demande de certification ainsi que le plan d'essai détaillé et les cartes d'essai. Vous pouvez obtenir des renseignements à jour sur les certifications de niveau 1 et 2 d'EMVCo en consultant le [www.emvco.com](http://www.emvco.com).

**Remarque importante :** au début de 2008, American Express a l'intention de mettre en place un outil de certification qui permettra d'éliminer l'obligation de se connecter au réseau American Express pour obtenir une certification AEIPS (SPCPAE) du terminal. Une fois cette obligation éliminée, les essais seront effectués sur le simulateur du système hôte, et les résultats seront présentés à American Express aux fins de validation. Si vous préférez utiliser cet outil plutôt que de vous connecter au réseau d'American Express, veuillez communiquer avec votre représentant d'American Express afin de déterminer s'il est disponible. Il peut être encore nécessaire de se connecter au réseau d'American Express afin de procéder à une certification quand des exigences propres à un pays ne sont pas prises en charge par cet outil.

### 5.3. Plan d'essai [AEIPS-TEST] pour la certification AEIPS (SPCPAE) du terminal



Le plan d'essai a été divisé en quatre sections. Les essais prévus à la première section sont **obligatoires**, ceux prévus aux deux sections suivantes peuvent devoir être effectués ou non, selon les fonctions prises en charge par le terminal. Les essais prévus à la dernière section **doivent** être effectués si la liaison de communication pour l'obtention des autorisations est modifiée. Le plan d'essai ci-dessous ne présente que les essais normalisés à l'échelle mondiale en ce qui a trait à la certification AEIPS (SPCPAE) d'un terminal; d'autres tests et exigences propres aux pays et aux banques administratrices peuvent exister.

#### Plan d'essai – section 1 (obligatoire)

- Section 1. Essais pour le processus d'autorisation – La présente section comprend neuf essais en ligne qui permettent de vérifier les fonctions AEIPS de base et l'interaction avec le système hôte d'American Express. Elle comprend également deux essais qui permettent de vérifier la fonctionnalité du terminal en matière de bandes magnétiques.

**Remarque importante :** American Express émet des Cartes dans les formats définis par l'Organisation internationale de normalisation (ISO) et l'American National Standards Institute (ANSI). Par conséquent, il est important de vérifier si le terminal est en mesure de lire les deux formats.

### Plan d'essai – sections 2 et 3 (selon les fonctions du terminal)

- **Section 2. Essais pour le processus d'autorisation par intervention du marchand** – La présente section prévoit neuf essais qui permettent de vérifier la fonctionnalité d'autorisation par intervention du marchand. Seuls les terminaux qui prennent en charge l'autorisation par intervention du marchand et qui intègre un code d'action de l'autorisation par intervention du marchand (SAC) doivent effectuer ces essais.
- **Section 3. Essais pour le processus de présentation des opérations** – Si vous devez créer un fichier d'opérations aux fins de présentation, vous devrez effectuer les essais prévus dans la présente section. Les deux essais permettent d'assurer que les données pertinentes sont transmises à American Express. Ces essais ne sont pas nécessaires si la présentation se fait par l'entremise d'une société de traitement indépendante. Toutefois, aucune certification officielle ne sera accordée tant que la liaison avec cette société de traitement indépendante n'aura pas été certifiée.

### Plan d'essai – section 4 (si la liaison de communication entre le terminal et American Express est modifiée)

- **Section 4. Essais à la suite d'une modification de la liaison de communication** – Si la liaison de communication pour l'obtention des autorisations a été modifiée, les essais de la présente section devront être effectués afin de vérifier si le terminal et American Express sont toujours en mesure d'établir une communication.

## 5.4. Programmation du terminal avant sa certification AEIPS (SPCPAE)

Avant de procéder au processus de certification AEIPS (SPCPAE) du terminal, il faut s'assurer que les paramètres du terminal sont appropriés et que les clés révélées de l'organisme de certification (CAPK) sont chargées. De plus, le terminal doit également être en mesure de fournir les bons renseignements diagnostiques. Une fois cela fait, une opération d'essai doit être effectuée pour vérifier la connexion entre le terminal et le réseau d'American Express. Une liste de vérification est jointe au document [AEIPS-TEST] pour vous aider à vous assurer que vous avez bien configuré votre terminal.

Le tableau ci-dessous présente les éléments de données auxquels sont associées des valeurs spécifiques aux fins d'essai.

Tableau 10 : valeurs spécifiques aux fins d'essai

Description	Valeurs d'essai
Intervalles des NIB d'American Express	340000–349999, 370000–379999
Code de l'application (AID) d'American Express	
Code du fournisseur enregistré de l'application (RID) :	A0 00 00 00 25
Extension du code d'application de propriété exclusive (PIX) :	01
Code de sélection de l'application (Application Selection Indicator)	La fonction de sélection partielle du code de l'application (AID) <b>doit</b> être activée
Code d'action du terminal (TAC) – valeur par défaut	00 00 00 00 00
Code d'action du terminal (TAC) – en ligne	00 00 00 00 00
Code d'action du terminal (TAC) – refus	00 00 00 00 00

Description	Valeurs d'essai
Code d'action de l'autorisation par intervention du marchand (SAC) – valeur par défaut <sup>1</sup>	F8 50 A8 20 00
Numéro de version de l'application	0001
Liste d'objets de données relative aux certificats d'opération (TDOL)	Non utilisée
Liste d'objets de données relative à l'authentification de données dynamiques (DDOL)	9F3704
Valeur limite pour la sélection aléatoire biaisée	Sélection aléatoire désactivée (que des zéros)
Pourcentage cible pour la sélection aléatoire	0
Pourcentage cible maximal pour la sélection aléatoire biaisée	0
Seuils pour le terminal	Fournis par votre représentant d'American Express
Clés révélées de l'organisme de certification (CAPK) <sup>2</sup>	Lca00003 Lca0000E Lca0000F Lca00010
Numéro d'établissement	Fourni par votre représentant d'American Express

<sup>1</sup> Utilisée seulement si la fonction de traitement de l'autorisation par intervention du marchand a été installée.

<sup>2</sup> Le format des clés révélées de l'organisme de certification (CAPK) d'American Express et d'autres renseignements sur celles-ci sont fournis dans l'annexe A.

#### 5.4.1. Exigences et paramètres supplémentaires pour la certification du processus d'autorisation par intervention du marchand

- Le code de l'application (AID) d'American Express **devrait** indiquer que le processus d'autorisation par intervention du marchand est pris en charge, sauf indication contraire au moment de l'essai.
- Aucune connexion au système hôte d'American Express **ne devrait** être possible au cours de tout essai du processus d'autorisation par intervention du marchand.

##### Seuils liés à l'autorisation par intervention du marchand

- Seuil lié à l'autorisation par intervention du marchand, avant la communication = 0.
- Seuil lié à l'autorisation par intervention du marchand, après la communication = 150.

#### 5.4.2. Données obligatoires aux fins du diagnostic

Les données présentées ci-après sont essentielles à la certification AEIPS (SPCPAE) du terminal. Elles peuvent être présentées sur le reçu ou le journal des transmissions. Les renseignements **doivent** être disponibles seulement durant le processus de certification et, s'ils sont fournis par l'entremise d'un reçu diagnostique, ils **ne doivent pas** être présentés au cours des opérations réelles.

- Résultats de vérification du terminal (TVR)
- Renseignements sur l'état de l'opération
- Résultats de vérification de la Carte (CVR)
- Type de cryptogramme
- Valeur du cryptogramme

- Codes d'action de l'émetteur (IAC)
- Codes d'action du terminal (TAC)
- Capacités du terminal
- Capacités supplémentaires du terminal
- Profil du système d'échange de l'application
- Données d'authentification de l'émetteur (IAD)
- Numéro de version de l'application (Carte)
- Numéro de version de l'application (terminal)
- Renseignements sur la version du logiciel du terminal
- Index des clés révélées de l'organisme de certification (CAPK)
- Résultats – Script de l'émetteur

### 5.4.3. Essai de la connexion

L'opération suivante peut être effectuée au moyen de la Carte d'essai SPCPAE (AEIPS) 10 afin de vérifier la connexion.

Montant de l'opération	Réponse
8.00	Autorisée

D'autres opérations aux fins d'essai de la connexion produisant différentes réponses peuvent également être effectuées (p. ex., autorisation verbale). Communiquez avec votre représentant d'American Express pour en savoir plus.

## 5.5. Exécution du plan d'essai

### 5.5.1. Documentation

Au moment d'effectuer une certification AEIPS (SPCPAE) du terminal, vous devrez remplir une fiche des résultats pour chaque essai effectué [AEIPS-TEST]. Afin d'aider American Express à vérifier les résultats – et d'accélérer le processus –, il est important que les personnes qui effectuent les essais fournissent le plus de preuves documentaires possibles. Cette preuve sera constituée, au minimum, des éléments suivants :

- un reçu par opération (ou un commentaire indiquant qu'aucun reçu n'a été produit);
- une confirmation imprimée des principaux messages-guides affichés à l'écran du terminal et du clavier de composition du NIP;
- une preuve des paramètres des champs « Résultats de vérification du terminal (TVR) » et « Renseignements sur l'état de l'opération (TSI) » (sur le reçu).
- Si les résultats d'un essai ne correspondent pas aux résultats prévus, des explications **devraient** être fournies. Le fait de fournir ces explications permettra d'accélérer la vérification des résultats.

De plus, fournir l'un ou l'autre des éléments suivants contribuera à simplifier le processus :

- les enregistrements produits par le matériel faisant l'objet de l'essai, indiquant le flot des données pour l'opération ou tout autre renseignement utile;
- tout commentaire supplémentaire qui, selon le responsable de la certification, aidera American Express à vérifier les résultats.

#### **5.5.2. Exigences relatives aux paramètres des champs « Résultats de vérification du terminal (TVR) » et « Renseignements sur les résultats de l'opération (TSI) »**

Pour certains essais, American Express exige que des valeurs précises soient inscrites dans le champ « Résultats de vérification du terminal (TVR) » ou « Renseignements sur les résultats de l'opération (TSI) ». Cela est indiqué dans le document [AEIPS-TEST] par l'inscription de ces valeurs précises dans ces champs (p. ex., le champ « Résultats de vérification du terminal (TVR) » – 00 xx xx xx xx). Si d'autres bits que ceux correspondant aux valeurs requises sont inscrits, cela ne signifie pas que l'essai a échoué. Toutefois, la présence de ces bits supplémentaires **doit** être expliquée.

Quand les renseignements sur les résultats de l'opération sont présentés, seules les valeurs pertinentes pour l'essai sont affichées (p. ex., 8x xx). Cependant, le terminal inscrira toujours des bits supplémentaires. Encore une fois, cela ne signifie pas que l'essai a échoué.

#### **5.6. Aperçu des essais pour l'obtention d'une certification AEIPS (SPCPAE) du terminal**

La présente section offre un aperçu des essais relatifs aux Cartes à puce (EMV) American Express pour les processus d'autorisation (plan d'essai – section 1), d'autorisation par intervention du marchand (plan d'essai – section 2), de présentation des opérations (plan d'essai – section 3) et de vérification à la suite d'une modification de la liaison de communication (plan d'essai – section 4). Elle n'inclut aucun essai propre à un pays ou à une banque administratrice que vous pourriez devoir effectuer. Veuillez communiquer avec votre représentant d'American Express afin de déterminer si des exigences supplémentaires s'appliquent à votre situation. Les tableaux présentant les aperçus commencent à la page suivante.

## 5.6.1. Essais obligatoires

### Plan d'essai – section 1. Essais pour le processus d'autorisation

Jeu d'essai	Description	Prérequis et paramètres	Tâches	Critères de réussite des essais
<b>AXP – POS 001</b>	Opération en ligne avec lecture de la puce et saisie du NIP	Le terminal est configuré pour la certification AEIPS (SPCPAE) du terminal	<ul style="list-style-type: none"> <li>Effectuez une vente au moyen de la Carte d'essai SPCPAE (AEIPS) 10 et entrez le montant requis</li> <li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li> </ul>	<ul style="list-style-type: none"> <li>Le terminal demande que la Carte à puce soit insérée</li> <li>Le terminal demande la saisie du NIP</li> <li>Le NIP est validé avec succès</li> <li>Le champ « Résultats de vérification du terminal (TVR) » affiche la valeur 00 xx xx 0x 0x (l'authentification des données n'a pas échoué, l'authentification de l'émetteur a réussi)</li> <li>Le champ « Renseignements sur les résultats de l'opération (TSI) » affiche la valeur 8x xx (p. ex., bit 8 = 1, authentification des données effectuée)</li> <li>L'ARPC est renvoyé dans le message de réponse à la demande d'autorisation de la banque administratrice affiliée à American Express</li> <li>La Carte renverra un certificat d'opération (TC) afin de lancer une deuxième commande visant à produire un cryptogramme d'application (AC)</li> <li>L'authentification de l'émetteur est effectuée (le terminal envoie le message d'authentification externe à la Carte)</li> <li>La vérification hors ligne du NIP est effectuée (Résultats de vérification de la Carte (CVR) : octet 1, bit 3 = 1)</li> <li>L'opération est autorisée</li> <li>Le terminal imprime ou affiche l'indicateur de l'application</li> <li>La case de signature n'est pas imprimée sur le reçu</li> </ul>

Jeu d'essai	Description	Prérequis et paramètres	Tâches	Critères de réussite des essais
<b>AXP – POS 002</b>	Opération en ligne avec lecture de la puce et saisie du NIP – Trois scripts de l'émetteur renvoyés dans le message de réponse à la demande d'autorisation	Le terminal est configuré pour la certification AEIPS (SPCPAE) du terminal	<ul style="list-style-type: none"> <li>Effectuez une vente au moyen de la Carte d'essai SPCPAE (AEIPS) 10 et entrez le montant requis</li> <li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li> <li>Effectuez une deuxième vente au moyen de la Carte d'essai SPCPAE (AEIPS) 10 et entrez le montant requis</li> <li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li> </ul>	<p>Première opération</p> <ul style="list-style-type: none"> <li>Le terminal demande la saisie du NIP</li> <li>Le NIP est validé avec succès</li> <li>Le système hôte d'American Express renvoie trois scripts d'émetteur au terminal pour la limite hors ligne inférieure pour opérations consécutives (LHLOC) dans le message de réponse à la demande d'autorisation</li> <li>Le terminal envoie à la Carte les scripts pour la LHLOC</li> <li>La Carte accepte les scripts pour la LHLOC</li> <li>L'authentification de l'émetteur est effectuée (le terminal envoie la commande d'authentification externe à la Carte)</li> <li>L'authentification de l'émetteur est réussie</li> <li>L'opération est autorisée par le système hôte</li> <li>Le terminal imprime ou affiche l'indicateur de l'application</li> </ul> <p>Deuxième opération</p> <ul style="list-style-type: none"> <li>Le champ « Résultats de vérification de la Carte (CVR) » indique trois commandes concernant le script de l'émetteur, qui contiennent des messages de sécurité traités avec succès au cours de la dernière opération (octet 4, bits 5 à 8)</li> <li>Le champ « Résultats de vérification de la Carte (CVR) » indique « Authentification de l'émetteur réussi pour la dernière opération » (octet 3, bit 4 = 0)</li> </ul>
<b>AXP – POS 003</b>	L'authentification de l'émetteur est effectuée avec succès après la réception d'une réponse de la banque administratrice demandant une autorisation verbale	Le terminal est configuré pour la certification AEIPS (SPCPAE) du terminal et prend en charge le traitement des autorisations verbales	<ul style="list-style-type: none"> <li>Effectuez une vente au moyen de la Carte d'essai SPCPAE (AEIPS) 10 et entrez le montant requis</li> <li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li> <li>Entrez le code d'autorisation 55 lorsqu'on vous le demande</li> <li>Effectuez une deuxième vente au moyen de la Carte d'essai SPCPAE (AEIPS) 10 et entrez le montant requis</li> <li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li> </ul>	<p>Première opération</p> <ul style="list-style-type: none"> <li>Le terminal demande la saisie du NIP</li> <li>Le NIP est validé avec succès</li> <li>L'opération doit faire l'objet d'une autorisation verbale</li> <li>L'ARPC est renvoyé dans le message de réponse à la demande d'autorisation de la banque administratrice affiliée à American Express</li> <li>Soit le certificat d'opération (TC) soit le cryptogramme d'authentification de l'application (AAC) est renvoyé par la Carte en réponse à la deuxième commande visant à produire un cryptogramme d'application (AC)</li> <li>L'authentification de l'émetteur est effectuée (le terminal envoie la commande d'authentification externe à la Carte)</li> <li>L'authentification de l'émetteur est réussie</li> <li>Le terminal imprime ou affiche l'indicateur de l'application</li> <li>L'écran du terminal et le reçu présentent le message « VEUILLEZ APPELER L'ÉMETTEUR » et la valeur du code de réponse</li> </ul> <p>Deuxième opération</p> <ul style="list-style-type: none"> <li>Le champ « Résultats de vérification de la Carte (CVR) » indique « Authentification de l'émetteur réussie pour la dernière opération » (Résultats de vérification de la Carte (CVR) : octet 3, bit 4 = 0)</li> </ul>





Jeu d'essai	Description	Prérequis et paramètres	Tâches	Critères de réussite des essais
<b>AXP – POS 004</b>	Opération effectuée au moyen d'une Carte d'essai dont le NIB commence par 34 et dont la clé révélée de l'organisme de certification (CAPK) AXP est 1408 – le terminal <b>doit</b> considérer le PAN valide	<ul style="list-style-type: none"><li>Le terminal est configuré pour la certification AEIPS (SPCPAE) du terminal</li><li>Le terminal est configuré pour accepter les NIB American Express commençant par 34 et 37</li></ul>	<ul style="list-style-type: none"><li>Effectuez une vente au moyen de la Carte d'essai SPCPAE (AEIPS) 11 et entrez le montant requis</li></ul>	<ul style="list-style-type: none"><li>Le terminal demande la saisie du NIP</li><li>Le NIP est validé avec succès</li><li>Le terminal accepte un NIB commençant par 34</li><li>Les données de l'opération sont envoyées en ligne et l'opération est autorisée</li><li>L'ARPC est renvoyé dans le message de réponse à la demande d'autorisation de la banque administratrice affiliée à American Express</li><li>Le certificat d'opération (TC) est généré par la Carte à puce en réponse à la deuxième commande visant à créer un cryptogramme d'application (AC)</li><li>L'authentification de l'émetteur est effectuée avec succès</li><li>Le champ « Résultats de vérification du terminal (TVR) » affiche la valeur 00 xx xx 0x xx (l'authentification des données n'a pas échoué)</li><li>Le champ « Renseignements sur les résultats de l'opération (TSI) » affiche la valeur 8x xx (p. ex., bit 8 = 1, authentification des données effectuée)</li></ul>
<b>AXP – POS 005</b>	Opération effectuée au moyen d'une Carte d'essai dotée de plusieurs applications exigeant la confirmation de l'identité du titulaire de la Carte	Le terminal est configuré pour la certification AEIPS (SPCPAE) du terminal	Effectuez une vente au moyen de la Carte d'essai SPCPAE (AEIPS) 12 et entrez le montant requis	<p>Si la fonction de confirmation de l'identité du titulaire de la Carte est prise en charge</p> <ul style="list-style-type: none"><li>La Carte demande la confirmation de l'identité du titulaire de la Carte</li><li>Le terminal <b>doit</b> afficher une invite pour une application d'AMEX</li><li>Choisissez l'application AMEX.</li><li>L'opération est autorisée.</li><li>Le champ « Résultats de vérification du terminal (TVR) » affiche la valeur 00 xx xx 0x xx (l'authentification des données n'a pas échoué)</li><li>Le champ « Renseignements sur les résultats de l'opération (TSI) » affiche la valeur 8x xx (p. ex., bit 8 = 1, authentification des données effectuée)</li><li>L'indicateur de l'application est imprimé sur le reçu</li></ul> <p>Si la fonction de confirmation de l'identité du titulaire de la Carte n'est pas prise en charge</p> <ul style="list-style-type: none"><li>La Carte demande la confirmation de l'identité du titulaire de la Carte</li><li>La fonction de confirmation de l'identité du titulaire de la Carte n'est pas prise en charge</li><li>L'opération est refusée</li></ul>

Jeu d'essai	Description	Prérequis et paramètres	Tâches	Critères de réussite des essais
<b>AXP – POS 006</b>	Opération en ligne par Carte à puce avec authentification de données dynamiques (DDA)	Le terminal est configuré pour la certification AEIPS (SPCPAE) du terminal	Effectuez une vente au moyen de la Carte d'essai SPCPAE (AEIPS) 13 et entrez le montant requis	<ul style="list-style-type: none"> <li>Le champ « Résultats de vérification du terminal (TVR) » affiche la valeur 00 xx xx xx – authentification hors ligne des données effectuée</li> <li>L'authentification de données dynamiques (DDA) n'a pas échoué</li> <li>Le champ « Renseignements sur les résultats de l'opération (TSI) » affiche la valeur 8x xx (p. ex., bit 8 = 1, authentification des données effectuée)</li> <li>L'authentification de l'émetteur est effectuée (le terminal envoie la commande d'authentification externe à la Carte)</li> <li>L'authentification de l'émetteur est réussie</li> <li>La Carte renvoie le cryptogramme d'authentification de l'application (AAC) afin de produire le premier cryptogramme d'application (AC)</li> <li>L'opération est refusée</li> </ul>
<b>AXP – POS 007</b>	Opération en ligne par Carte à puce, effectuée au moyen de la clé révélée de l'organisme de certification (CAPK) AXP 1984 et d'un script de 126 octets envoyé dans un message de réponse à la demande d'autorisation	<ul style="list-style-type: none"> <li>Le terminal est configuré pour la certification AEIPS (SPCPAE) du terminal</li> <li>Le terminal est en mesure de traiter plusieurs scripts de l'émetteur et plusieurs commandes inscrites dans ces scripts</li> </ul>	<ul style="list-style-type: none"> <li>Effectuez une vente au moyen de la Carte d'essai SPCPAE (AEIPS) 14 et entrez le montant requis</li> <li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li> <li>Effectuez une deuxième vente au moyen de la Carte d'essai SPCPAE (AEIPS) 14 et entrez le montant requis</li> <li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li> </ul>	<p>Première opération</p> <ul style="list-style-type: none"> <li>Le terminal demande la saisie du NIP</li> <li>Le NIP est validé avec succès</li> <li>Le script est renvoyé au terminal par le système hôte d'American Express dans le message de réponse à la demande d'autorisation</li> <li>Le terminal a envoyé une commande de mise à jour « extra longue » (126 octets) à la Carte (2 scripts intégrés)</li> <li>Le terminal demande la saisie du NIP</li> <li>Le champ « Résultats de vérification du terminal (TVR) » affiche la valeur 00 xx xx 0x xx (l'authentification des données n'a pas échoué)</li> <li>Le champ « Renseignements sur les résultats de l'opération (TSI) » affiche la valeur 8x xx (p. ex., bit 8 = 1, authentification des données effectuée)</li> <li>L'authentification de l'émetteur est effectuée (le terminal envoie la commande d'authentification externe à la Carte)</li> <li>L'authentification de l'émetteur est réussie</li> <li>La vérification hors ligne du NIP est effectuée (octet 1, bit 3 = 1)</li> <li>L'opération est autorisée</li> </ul> <p>Deuxième opération</p> <ul style="list-style-type: none"> <li>Le champ « Résultats de vérification de la Carte (CVR) » indique deux commandes dans le script de l'émetteur, qui contiennent des messages de sécurité traités avec succès au cours de la dernière opération (octet 4, bits 5 à 8)</li> <li>Le champ « Résultats de vérification de la Carte (CVR) » indique que l'authentification de l'émetteur a été réussie pour la dernière opération (octet 3, bit 4 = 0)</li> </ul>

Jeu d'essai	Description	Prérequis et paramètres	Tâches	Critères de réussite des essais
<b>AXP – POS 008</b>	Vérification des remboursements	<ul style="list-style-type: none"> <li>Le terminal est configuré pour la certification AEIPS (SPCPAE) du terminal</li> <li>Le terminal prend en charge le remboursement complet des opérations par Carte à puce (EMV)</li> </ul>	<ul style="list-style-type: none"> <li>Effectuez une vente au moyen de la Carte d'essai SPCPAE (AEIPS) 10 et entrez le montant requis</li> <li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li> <li>Effectuez un remboursement au moyen de la Carte d'essai SPCPAE (AEIPS) 10 et entrez le montant requis</li> </ul>	<ul style="list-style-type: none"> <li>Le remboursement a réussi soit en ligne, soit hors ligne</li> <li>Le remboursement est autorisé</li> <li>Les données relatives au remboursement sont saisies au terminal</li> </ul>
<b>AXP – POS 009</b>	Opération en ligne effectuée et autorisée, mais la validation de l'émetteur a échoué, et la Carte a refusé l'opération. Le terminal effectue alors une annulation	Le terminal est configuré pour la certification AEIPS (SPCPAE) et peut prendre en charge la fonction d'annulation en ligne	<ul style="list-style-type: none"> <li>Effectuez une vente au moyen de la Carte d'essai SPCPAE (AEIPS) 10 et entrez le montant requis</li> <li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li> <li>Annulez l'opération</li> </ul>	<ul style="list-style-type: none"> <li>L'ARPC est renvoyé dans le message de réponse à la demande d'autorisation du système hôte d'American Express</li> <li>Le système hôte d'American Express autorise l'opération</li> <li>L'authentification de l'émetteur est effectuée</li> <li>Le terminal demande un certificat d'opération (TC) dans la deuxième commande visant à produire un cryptogramme d'application (AC)</li> <li>Le cryptogramme d'authentification de l'application (AAC) est généré par la Carte à puce en réponse à la deuxième commande visant à créer un cryptogramme d'application (AC)</li> <li>L'authentification de l'émetteur a réussi (résultats de vérification du terminal (TVR) : octet 5, bit 7 = 0)</li> <li>L'authentification de l'émetteur a été effectuée (renseignements sur les résultats de l'opération : octet 1, bit 5 = 1)</li> <li>L'opération est refusée</li> <li>Une opération d'annulation est générée</li> </ul>
<b>AXP – POS 010</b>	Opération avec lecture de la bande magnétique; Carte formatée conformément aux normes ISO	Le terminal est configuré pour la certification AEIPS (SPCPAE) du terminal	Effectuez une vente au moyen de la Carte d'essai d'AEIPS conforme aux normes ISO et entrez le montant requis	<ul style="list-style-type: none"> <li>Le terminal est en mesure de lire les données de la piste 2 de la bande magnétique</li> <li>Le terminal est en mesure de reconnaître le code de service 101 de la norme ISO</li> <li>Le terminal ne demande pas que la Carte à puce soit insérée</li> <li>L'opération est autorisée</li> </ul>
<b>AXP – POS 011</b>	Opération avec lecture de la bande magnétique; Carte formatée conformément aux normes ANSI	Le terminal est configuré pour le terminal	Effectuez une vente au moyen de la Carte d'essai d'AEIPS conforme aux normes ANSI et entrez le montant requis	<ul style="list-style-type: none"> <li>Le terminal est en mesure de lire les données de la piste 2 de la bande magnétique</li> <li>Le terminal ne demande pas que la Carte à puce soit insérée</li> <li>L'opération est autorisée</li> </ul>

## 5.6.2. Essais fondés sur les fonctions du terminal

### Plan d'essai – section 2. Essais pour le processus d'autorisation par intervention du marchand

Jeu d'essai	Description	Prérequis et paramètres	Tâches	Critères de réussite des essais
<b>STP-020 – Non configuré pour l'autorisation par intervention du marchand</b>	L'opération est refusée, car l'autorisation par intervention du marchand n'est pas prise en charge	<ul style="list-style-type: none"> <li>Le terminal ne peut se connecter au système hôte de la banque administratrice</li> <li>La fonction de traitement de l'autorisation par intervention du marchand n'est pas configurée pour le code de l'application (AID) d'American Express</li> </ul>	Effectuez une vente au moyen de la Carte d'essai STP-0020 et entrez le montant 150,01 (montant supérieur au maximum permis sans autorisation pour une opération par intervention du marchand après l'établissement de la communication)	<ul style="list-style-type: none"> <li>Le terminal n'envoie pas de commande d'authentification externe à la Carte</li> <li>Le terminal demande la production d'un cryptogramme d'authentification de l'application (AAC) dans la deuxième commande visant à produire un cryptogramme d'application (AC)</li> <li>Au moment de demander un cryptogramme d'authentification de l'application (AAC), le terminal programme le code de réponse à la demande d'autorisation (ARC) (étiquette 8A) à « Z3 »</li> <li>L'opération est refusée au terminal</li> <li>Le montant de l'opération dépasse le maximum permis sans autorisation pour une opération par intervention du marchand (Résultats de vérification du terminal (TVR) : octet 4, bit 8 = 1)</li> </ul>
<b>STP-021a – Montant inférieur au maximum permis sans autorisation pour une opération par intervention du marchand après l'établissement de la communication</b>	Opération autorisée par intervention du marchand	<ul style="list-style-type: none"> <li>Le terminal ne peut se connecter au système hôte de la banque administratrice</li> <li>La fonction d'autorisation par intervention du marchand est configurée pour le code de l'application (AID) d'American Express et le code d'action de l'autorisation par intervention du marchand (SAC) est inscrit</li> </ul>	Effectuez une vente au moyen de la Carte d'essai STP-0021 et entrez le montant 50,01 (montant inférieur au maximum permis sans autorisation pour une opération par intervention du marchand après l'établissement de la communication, mais supérieur à celui avant l'établissement de la communication)	<ul style="list-style-type: none"> <li>Le terminal n'envoie pas de commande d'authentification externe à la Carte</li> <li>Le terminal demande la production d'un certificat d'opération (TC) dans la deuxième commande visant à produire un cryptogramme d'application (AC)</li> <li>Au moment de demander un certificat d'opération (TC), le terminal programme le code de réponse à la demande d'autorisation (ARC) (étiquette 8A) à « 00 »</li> <li>Le terminal autorise l'opération</li> <li>Le terminal demande une signature</li> <li>Le montant de l'opération dépasse le maximum permis sans autorisation pour une opération par intervention du marchand (Résultats de vérification du terminal (TVR) : octet 4, bit 8 = 1)</li> </ul>
<b>STP-021b – Montant inférieur au maximum permis sans autorisation pour une opération par intervention du marchand après l'établissement de la communication (opérations présentées)</b>	Présentation de l'opération créée lors de l'essai STP-021a	Aucun	Présentez les données de l'opération créées lors de l'essai STP-021a à American Express	Les données de l'opération ont été présentées correctement dans le fichier de lots

Jeu d'essai	Description	Prérequis et paramètres	Tâches	Critères de réussite des essais
<b>STP-022 – Montant supérieur au maximum permis sans autorisation pour une opération par intervention du marchand après l'établissement de la communication</b>	Réponse exigeant une autorisation verbale reçue à la suite d'une autorisation par intervention du marchand	<ul style="list-style-type: none"> <li>Le système du terminal ne peut se connecter au système hôte de la banque administratrice</li> <li>La fonction d'autorisation par intervention du marchand est configurée pour le code de l'application (AID) d'American Express et le code d'action de l'autorisation par intervention du marchand (SAC) est inscrit</li> </ul>	<p>Effectuez une vente au moyen de la Carte d'essai STP-0022 et entrez le montant 150,02 (montant supérieur au maximum permis sans autorisation pour une opération par intervention du marchand avant et après l'établissement de la communication)</p>	<ul style="list-style-type: none"> <li>Le terminal n'envoie pas de commande d'authentification externe à la Carte</li> <li>Le terminal demande la création d'un certificat d'opération (TC) dans la deuxième commande visant à produire un cryptogramme d'application (AC) (il peut s'agir d'un cryptogramme d'authentification de l'application (AAC))</li> <li>Au moment de demander le certificat d'opération (TC), le terminal programme le code de réponse à la demande d'autorisation (ARC) (étiquette 8A) à « 02 »</li> <li>Le terminal demande que l'opération fasse l'objet d'une autorisation verbale</li> <li>Le montant de l'opération dépasse le maximum permis sans autorisation pour une opération par intervention du marchand (Résultats de vérification du terminal (TVR) : octet 4, bit 8 = 1)</li> </ul>
<b>STP-023 – Condition de refus remplie (échec de l'authentification des données permanentes (SDA))</b>	Opération refusée lors de l'autorisation par intervention du marchand, en raison de l'échec de l'authentification des données permanentes (SDA)	<ul style="list-style-type: none"> <li>Le système du terminal ne peut se connecter au système hôte de la banque administratrice</li> <li>La fonction d'autorisation par intervention du marchand est configurée pour le code de l'application (AID) d'American Express et le code d'action de l'autorisation par intervention du marchand (SAC) est inscrit</li> </ul>	<p>Effectuez une vente au moyen de la Carte d'essai STP-0023 et entrez le montant 50,03 (montant inférieur au maximum permis sans autorisation pour une opération par intervention du marchand après l'établissement de la communication, mais supérieur à celui avant l'établissement de la communication)</p>	<ul style="list-style-type: none"> <li>Le système hôte du marchand refuse la réponse à la demande d'autorisation avec le code de réponse « 05 »</li> <li>Le terminal n'envoie pas de commande d'authentification externe à la Carte</li> <li>Le terminal demande la production d'un cryptogramme d'authentification de l'application (AAC) dans la deuxième commande visant à produire un cryptogramme d'application (AC)</li> <li>Au moment de demander un cryptogramme d'authentification de l'application (AAC), le terminal programme le code de réponse à la demande d'autorisation (ARC) (étiquette 8A) à « 05 »</li> <li>L'opération est refusée au terminal</li> <li>L'authentification hors ligne des données permanentes (SDA) a échoué (Résultats de vérification du terminal (TVR) : octet 1, bit 7 = 1)</li> <li>Le montant de l'opération dépasse le maximum permis sans autorisation pour une opération par intervention du marchand (Résultats de vérification du terminal (TVR) : octet 4, bit 8 = 1)</li> </ul>

Jeu d'essai	Description	Prérequis et paramètres	Tâches	Critères de réussite des essais
<b>STP-024 – Condition de refus remplie (fichier d'exceptions)</b>	L'opération a été refusée lors de l'autorisation par intervention du marchand, car le numéro de la Carte est inscrit dans le fichier d'exceptions du terminal	<ul style="list-style-type: none"> <li>Le système du terminal ne peut se connecter au système hôte de la banque administratrice</li> <li>La fonction d'autorisation par intervention du marchand est configurée pour code de l'application (AID) d'American Express et le code d'action de l'autorisation par intervention du marchand (SAC) est inscrit</li> <li>Le numéro de Carte « 37 42 00 00 00 00 4 » figure dans le fichier d'exceptions du terminal</li> </ul>	Effectuez une vente au moyen de la Carte d'essai STP-0024 et entrez le montant 50,04 (montant inférieur au maximum permis sans autorisation pour une opération par intervention du marchand après l'établissement de la communication, mais supérieur à celui avant l'établissement de la communication)	<ul style="list-style-type: none"> <li>Le système hôte du marchand refuse la réponse à la demande d'autorisation avec le code de réponse « 05 »</li> <li>Le terminal n'envoie pas de commande d'authentification externe à la Carte</li> <li>Le terminal demande la production d'un cryptogramme d'authentification de l'application (AAC) dans la deuxième commande visant à produire un cryptogramme d'application (AC)</li> <li>Au moment de demander un cryptogramme d'authentification de l'application (AAC), le terminal programme le code de réponse à la demande d'autorisation (ARC) (étiquette 8A) à « 05 »</li> <li>L'opération est refusée au terminal</li> <li>Le numéro de la Carte figure dans le fichier d'exceptions (Résultats de vérification du terminal (TVR) : octet 1, bit 5 = 1)</li> <li>Le montant de l'opération dépasse le maximum permis sans autorisation pour une opération par intervention du marchand (Résultats de vérification du terminal (TVR) : octet 4, bit 8 = 1)</li> </ul>
<b>STP-025 – Condition de refus remplie (application expirée)</b>	L'opération a été refusée lors de l'autorisation par intervention du marchand, car l'application de la Carte est expirée	<ul style="list-style-type: none"> <li>Le système du terminal ne peut se connecter au système hôte de la banque administratrice</li> <li>La fonction d'autorisation par intervention du marchand est configurée pour code de l'application (AID) d'American Express et le code d'action de l'autorisation par intervention du marchand (SAC) est inscrit</li> </ul>	Effectuez une vente au moyen de la Carte d'essai STP-0025 et entrez le montant 50,05 (montant inférieur au maximum permis sans autorisation pour une opération par intervention du marchand après l'établissement de la communication, mais supérieur à celui avant l'établissement de la communication)	<ul style="list-style-type: none"> <li>Le système hôte du marchand refuse la réponse à la demande d'autorisation avec le code de réponse « 05 »</li> <li>Le terminal n'envoie pas de commande d'authentification externe à la Carte</li> <li>Le terminal demande la production d'un cryptogramme d'authentification de l'application (AAC) dans la deuxième commande visant à produire un cryptogramme d'application (AC)</li> <li>Au moment de demander un cryptogramme d'authentification de l'application (AAC), le terminal programme le code de réponse à la demande d'autorisation (ARC) (étiquette 8A) à « 05 »</li> <li>L'opération est refusée au terminal</li> <li>Application expirée (Résultats de vérification du terminal (TVR) : octet 2, bit 7 = 1)</li> <li>Le montant de l'opération dépasse le maximum permis sans autorisation pour une opération par intervention du marchand (Résultats de vérification du terminal (TVR) : octet 4, bit 8 = 1)</li> </ul>



Jeu d'essai	Description	Prérequis et paramètres	Tâches	Critères de réussite des essais
<b>STP-026a – Condition de refus NON remplit</b>	L'opération a été autorisée lors de l'autorisation par intervention du marchand, car le code d'action de l'autorisation par intervention du marchand (SAC) n'est pas programmé pour refuser une application expirée	<ul style="list-style-type: none"> <li>Le système du terminal ne peut se connecter au système hôte de la banque administratrice</li> <li>La fonction de traitement de l'autorisation par intervention du marchand est configurée pour le code de l'application (AID) d'American Express</li> <li>Un code d'action de l'autorisation par intervention du marchand (SAC) dont la valeur est « 0000000000 » est chargé dans le terminal</li> </ul>	Effectuez une vente au moyen de la Carte d'essai STP-0026 et entrez le montant 50,06 (montant inférieur au maximum permis sans autorisation pour une opération par intervention du marchand après l'établissement de la communication, mais supérieur à celui avant l'établissement de la communication)	<ul style="list-style-type: none"> <li>Le système hôte du marchand autorise la réponse à la demande d'autorisation avec le code de réponse « 00 »</li> <li>Le terminal n'envoie pas de commande d'authentification externe à la Carte</li> <li>Le terminal demande la production d'un certificat d'opération (TC) dans la deuxième commande visant à produire un cryptogramme d'application (AC)</li> <li>Au moment de demander un certificat d'opération (TC), le terminal programme le code de réponse à la demande d'autorisation (ARC) (étiquette 8A) à « 00 »</li> <li>Le terminal autorise l'opération</li> <li>Application expirée (Résultats de vérification du terminal (TVR) : octet 2, bit 7 = 1)</li> <li>Le montant de l'opération dépasse le maximum permis sans autorisation pour une opération par intervention du marchand (Résultats de vérification du terminal (TVR) : octet 4, bit 8 = 1)</li> <li>Les données de l'opération ont été présentées correctement dans le fichier de lots</li> </ul>
<b>STP-026b – Condition de refus NON remplit (opérations présentées)</b>	Présentation des données de l'opération créées lors de l'essai STP-026a	Aucun	Présentez les données de l'opération créées lors de l'essai STP-026a à American Express	
<b>STP-027 – Condition de refus remplit (nombre d'essais permis de saisie du NIP dépassé)</b>	L'opération a été refusée lors de l'autorisation par intervention du marchand, car le nombre d'essais permis de saisie du NIP a été dépassé	<ul style="list-style-type: none"> <li>Le système du terminal ne peut se connecter au système hôte de la banque administratrice</li> <li>La fonction d'autorisation par intervention du marchand est configurée pour code de l'application (AID) d'American Express et le code d'action de l'autorisation par intervention du marchand (SAC) est inscrit</li> </ul>	<ul style="list-style-type: none"> <li>Effectuez une vente au moyen de la Carte d'essai STP-0027 et entrez le montant 50,07 (montant inférieur au maximum permis sans autorisation pour une opération par intervention du marchand après l'établissement de la communication, mais supérieur à celui avant l'établissement de la communication)</li> <li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li> </ul>	<ul style="list-style-type: none"> <li>L'hôte du marchand refuse la réponse à la demande d'autorisation avec le code de réponse « 05 »</li> <li>Le terminal n'envoie pas de commande d'authentification externe à la Carte</li> <li>Le terminal demande la production d'un cryptogramme d'authentification de l'application (AAC) dans la deuxième commande visant à produire un cryptogramme d'application (AC)</li> <li>Au moment de demander un cryptogramme d'authentification de l'application (AAC), le terminal programme le code de réponse à la demande d'autorisation (ARC) (étiquette 8A) à « 05 »</li> <li>L'opération est refusée au terminal</li> <li>Nombre d'essais permis de saisie hors ligne du NIP dépassé (Résultats de vérification du terminal (TVR) : octet 3, bit 6 = 1)</li> <li>Le montant de l'opération dépasse le maximum permis sans autorisation pour une opération par intervention du marchand (Résultats de vérification du terminal (TVR) : octet 4, bit 8 = 1)</li> </ul>

Jeu d'essai	Description	Prérequis et paramètres	Tâches	Critères de réussite des essais
<b>STP-028 – Condition de refus remplies (NIP non saisi)</b>	L'opération a été refusée lors de l'autorisation par intervention du marchand, car la saisie hors ligne du NIP a été requise, mais non effectuée	<ul style="list-style-type: none"> <li>Le système du terminal ne peut se connecter au système hôte de la banque administratrice</li> <li>La fonction d'autorisation par intervention du marchand est configurée pour code de l'application (AID) d'American Express et le code d'action de l'autorisation par intervention du marchand (SAC) est inscrit</li> </ul>	<ul style="list-style-type: none"> <li>Effectuez une vente au moyen de la Carte d'essai STP-0028 et entrez le montant 50,08 (montant inférieur au maximum permis sans autorisation pour une opération par intervention du marchand après l'établissement de la communication, mais supérieur à celui avant l'établissement de la communication)</li> <li>Lorsque le NIP est demandé, demandez une dispense de NIP</li> </ul>	<ul style="list-style-type: none"> <li>La dispense de NIP se fait au terminal</li> <li>Le système hôte du marchand refuse la réponse à la demande d'autorisation avec le code de réponse « 05 »</li> <li>Le terminal n'envoie pas de commande d'authentification externe à la Carte</li> <li>Le terminal demande la production d'un cryptogramme d'authentification de l'application (AAC) dans la deuxième commande visant à produire un cryptogramme d'application (AC)</li> <li>Au moment de demander un cryptogramme d'authentification de l'application (AAC), le terminal programme le code de réponse à la demande d'autorisation (ARC) (étiquette 8A) à « 05 »</li> <li>L'opération est refusée au terminal</li> <li>Saisie hors ligne du NIP requise, clavier de composition du NIP présent, mais NIP non saisi (Résultats de vérification du terminal (TVR) : octet 3, bit 4 = 1)</li> <li>Le montant de l'opération dépasse le maximum permis sans autorisation pour une opération par intervention du marchand (Résultats de vérification du terminal (TVR) : octet 4, bit 8 = 1)</li> </ul>





Plan d'essai – section 3. Essais pour le processus de présentation des opérations

Si vous devez fournir un fichier de lots afin de présenter des opérations dans le cadre des essais d'autorisation, vous devez le faire au moyen des opérations indiquées dans la présente section.

Jeu d'essai	Description	Prérequis et paramètres	Tâches	Critères de réussite des essais
<b>Règlement – opération de débit</b>	Opération autorisée en ligne, dont les données sont présentées correctement dans le fichier de lots	Le terminal est configuré pour la certification AEIPS (SPCPAE) du terminal	<ul style="list-style-type: none"><li>Effectuez une vente au moyen de la Carte d'essai SPCPAE (AEIPS) 10 et entrez le montant requis</li><li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li><li>Inscrivez les données de l'opération autorisée dans le fichier de lots et présentez ce dernier à American Express (si vous êtes le présentateur direct), à votre banque administratrice ou au bureau administrateur</li></ul>	<ul style="list-style-type: none"><li>L'opération par Carte à puce a été autorisée en ligne</li><li>Les données de l'opération ont été inscrites dans le fichier de lots</li><li>Le fichier de lots a été présenté dans le format convenu</li></ul>
<b>Règlement – Opération de crédit</b>	Remboursement d'une opération autorisée en ligne, dont les données ont été inscrites correctement dans le fichier de lots	Le terminal est configuré pour la certification AEIPS (SPCPAE) du terminal	<ul style="list-style-type: none"><li>Effectuez une vente au moyen de la Carte d'essai SPCPAE (AEIPS) 10 et entrez le montant requis</li><li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li><li>Remboursez le montant requis de l'opération autorisée</li><li>Inscrivez les données de l'opération et du remboursement dans le fichier de lots et présentez ce dernier à American Express (si vous êtes le présentateur direct) ou à votre banque administratrice</li></ul>	<ul style="list-style-type: none"><li>L'opération par Carte à puce a été autorisée en ligne</li><li>L'opération autorisée a été remboursée</li><li>Les données de l'opération ont été inscrites dans le fichier de lots</li><li>Le fichier de lots a été présenté dans le format convenu</li></ul>

### 5.6.3. Essais effectués quand la liaison de communication a été modifiée

#### Plan d'essai – section 4 : essais à la suite d'une modification de la liaison de communication

Les essais suivants sont effectués quand une modification a été apportée à la liaison de communication entre le terminal et American Express.

Jeu d'essai	Description	Prérequis et paramètres	Tâches	Critères de réussite des essais
<b>AXP – COM 001</b>	L'authentification de l'émetteur est effectuée avec succès après la réception d'une réponse demandant une autorisation verbale	Le terminal est configuré pour la certification AEIPS (SPCPAE) du terminal	<ul style="list-style-type: none"> <li>Effectuez une vente au moyen de la Carte d'essai SPCPAE (AEIPS) 10 et entrez le montant requis</li> <li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li> <li>Entrez le code d'autorisation 55 lorsqu'on vous le demande</li> </ul>	<ul style="list-style-type: none"> <li>L'opération doit faire l'objet d'une autorisation verbale</li> <li>Le NIP est validé avec succès</li> <li>L'ARPC est envoyé dans la réponse par la banque administratrice affiliée à American Express</li> <li>Le certificat d'opération (TC) est généré par la Carte à puce en réponse à la deuxième commande visant à créer un cryptogramme d'application (AC)</li> <li>L'authentification de l'émetteur est effectuée avec succès</li> <li>L'indicateur de l'application est imprimé sur le reçu</li> </ul>
<b>AXP – COM 002</b>	Opération en ligne par Carte à puce, effectuée au moyen de la clé révélée de l'organisme de certification AXP 1984 et d'un script de 126 octets envoyé dans un message de réponse à la demande d'autorisation	Le terminal est configuré pour la certification AEIPS (SPCPAE) du terminal	<ul style="list-style-type: none"> <li>Effectuez une vente au moyen de la Carte d'essai SPCPAE (AEIPS) 14 et entrez le montant requis</li> <li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li> <li>Effectuez une deuxième vente au moyen de la Carte d'essai SPCPAE (AEIPS) 14 et entrez le montant requis</li> <li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li> </ul>	<ul style="list-style-type: none"> <li>L'opération est autorisée en ligne</li> <li>L'authentification des données permanentes (SDA) est effectuée avec succès</li> <li>Le NIP est validé avec succès</li> <li>L'authentification de l'émetteur est réussie</li> <li>L'indicateur de l'application est imprimé sur le reçu</li> <li>Le champ « Résultats de vérification de la Carte (CVR) » de la deuxième opération en ligne indique que le script a été traité avec succès lors de la dernière opération</li> </ul>
<b>AXP – COM 003</b>	Opération en ligne avec saisie de NIP refusée par le système hôte	Le terminal est configuré pour la certification AEIPS (SPCPAE) du terminal	<ul style="list-style-type: none"> <li>Effectuez une vente au moyen de la Carte d'essai SPCPAE (AEIPS) 10 et entrez le montant requis</li> <li>Lorsqu'on vous le demandera, saisissez le NIP 1234</li> </ul>	<ul style="list-style-type: none"> <li>L'opération est refusée</li> <li>Le NIP est validé avec succès</li> <li>L'authentification de l'émetteur est effectuée avec succès</li> <li>L'indicateur de l'application est imprimé sur le reçu</li> </ul>

## SECTION 6 : FORMATION DU MARCHAND



Pour que la nouvelle technologie soit efficace, il est essentiel que les personnes qui doivent l'utiliser, la gérer ou s'occuper de son entretien reçoivent la formation adéquate. Notre expérience nous a prouvé qu'au moment de la mise en œuvre de la technologie EMV, on ne peut offrir trop de formation.

L'adoption d'une nouvelle technologie de paiement constitue un changement important pour un marchand, et les clients peuvent se montrer insatisfaits si les opérations ne sont pas prises en charge adéquatement. Il est essentiel que les marchands qui passent à la technologie EMV prévoient, élaborent et mettent en œuvre un programme de formation du personnel.

### 6.1. Directives pour un programme de formation réussi

Il convient de donner la formation relative à la technologie EMV avant la mise en œuvre de celles-ci chez le marchand et de façon continue pour les nouveaux employés. Le matériel de formation **devrait** également être disponible en tout temps pour que le personnel puisse le consulter au besoin.

**MEILLEURE PRATIQUE :** nous **recommandons** la création d'un aide-mémoire contenant les renseignements importants sur l'acceptation des Cartes à puce et des Cartes à bande magnétique, qui devrait être conservé près du terminal.

- Nous **recommandons** que la formation sur la technologie EMV soit interactive et qu'elle inclue des exercices pratiques d'acceptation à la fois des Cartes à puce et des Cartes à bande magnétique.
- De plus, il est **recommandé** que les marchands collaborent avec leur banque administratrice s'ils ont des questions ou s'ils requièrent un soutien supplémentaire relativement au traitement d'opérations par Carte à puce (EMV).

Voici quelques sujets clés qui **devraient** être inclus dans la formation sur la technologie EMV :

- les avantages de la technologie EMV en ce qui a trait aux risques de fraude et à la responsabilité en matière de fraude;
- l'insertion de la Carte à puce;
- la réponse aux demandes du terminal;
- le traitement de rechange;
- la saisie du NIP et la dispense de NIP (selon l'utilisation locale);
- les réponses aux questions courantes des clients;
- l'obligation de continuer d'accepter tous les types de Carte.



## ANNEXE A : RENSEIGNEMENTS SUR LES CLÉS RÉVÉLÉES DE L'ORGANISME DE CERTIFICATION

### Renseignements détaillés sur le format des clés révélées de l'organisme de certification (CAPK)

Sauf indication contraire, les valeurs sont présentées en format hexadécimal.

Tableau A-1 : Format des clés révélées de l'organisme de certification

Nom du champ	Taille (nombre d'octets)	Haché	Description
En-tête	1	Non	Programmé à « 20 »
Code de service	4	Non	Code du produit American Express. Programmé à « 00 00 00 00 »
Taille du modulo relatif aux clés révélées de l'organisme de certification	2	Non	Taille du modulo relatif aux clés révélées de l'organisme de certification.  Valeurs valides actuelles = 00 80 (1024 bits), 0090 (1152 bits), 00B0 (1408 bits), 00F8 (1984 bits)
Code de l'algorithme relatif aux clés révélées de l'organisme de certification	1	Non	Code de l'algorithme cryptographique servant à produire les clés révélées de l'organisme de certification. Programmé à « 01 »
Taille de l'exposant des clés révélées de l'organisme de certification	1	Non	Taille de l'exposant des clés révélées de l'organisme de certification. Programmé à « 01 »
Code du fournisseur enregistré de l'application (RID)	5	Oui	Programmé à « A0 00 00 00 25 »
Index des clés révélées de l'organisme de certification	1	Oui	Numéro d'index des clés révélées de l'organisme de certification
Modulo relatif aux clés révélées de l'organisme de certification	Variable	Oui	Modulo relatif aux clés révélées de l'organisme de certification
Exposant des clés révélées de l'organisme de certification	Variable	Oui	Exposant des clés révélées de l'organisme de certification. Programmé à « 03 »
Valeur de hachage	20	Non	Hachage d'éléments indiqué dans la colonne « Haché »

## Clés révélées de l'organisme de certification

Il existe quatre clés révélées de l'organisme de certification. Elles sont envoyées dans un fichier compressé, en format texte ou binaire.

Tableau A-2 : clés révélées de l'organisme de certification

Nom du fichier de la clé	Index des clés révélées de l'organisme de certification	Taille des clés révélées de l'organisme de certification
Lca00003.dat Lca00003.txt	03	00 80 (hex.) = 128 octets = 1024 bits
Lca0000E.dat Lca0000E.txt	0E	00 90 (hex.) = 144 octets = 1152 bits
Lca0000F.dat Lca0000F.txt	0F	00 B0 (hex.) = 176 octets = 1408 bits
Lca00010.dat Lca00010.txt	10	00 F8 (hex.) = 248 octets = 1984 bits

Les versions texte de ces clés sont présentées ci-dessous.

### Index de la clé 03 (1024)

En-tête	20
Code de service	00 00 00 00
Taille du modulo relatif aux clés révélées de l'organisme de certification	00 80
Code de l'algorithme relatif aux clés révélées de l'organisme de certification	01
Taille de l'exposant des clés révélées de l'organisme de certification	01
Code du fournisseur enregistré de l'application (RID)	A0 00 00 00 25
Index des clés révélées de l'organisme de certification	03
Modulo relatif aux clés révélées de l'organisme de certification	B0C2C6E2A6386933CD17C239496BF48C57E389164F2A96BFF133439AE8A77B20498BD4DC6959AB0C2D05D0723AF3668901937B674E5A2FA92DD5E78EA9D75D79620173CC269B35F463B3D4AAFF2794F92E6C7A3FB95325D8AB95960C3066BE548087BCB6CE12688144A8B4A66228AE4659C634C99E36011584C095082A3A3E3
Exposant des clés révélées de l'organisme de certification	03
Valeur de hachage	8708A3E3BBC1BB0BE73EBD8D19D4E5D20166BF6C

### Index de la clé 0E (1152)

En-tête	20
Code de service	00 00 00 00
Taille du modulo relatif aux clés révélées de l'organisme de certification	00 90
Code de l'algorithme relatif aux clés révélées de l'organisme de certification	01
Taille de l'exposant des clés révélées de l'organisme de certification	01
Code du fournisseur enregistré de l'application (RID)	A0 00 00 00 25
Index des clés révélées de l'organisme de certification	0E
Modulo relatif aux clés révélées de l'organisme de certification	AA94A8C6DAD24F9BA56A27C09B01020819568B81A026BE9FD0A3416CA9A71166ED5084ED91CED47DD457DB7E6CBCD53E560BC5DF48ABC380993B6D549F5196CFA77DFB20A0296188E969A2772E8C4141665F8BB2516BA2C7B5FC91F8DA04E8D512EB0F6411516FB86FC021CE7E969DA94D33937909A53A57F907C40C22009DA7532CB3BE509AE173B39AD6A01BA5BB85
Exposant des clés révélées de l'organisme de certification	
Valeur de hachage	A7266ABAE64B42A3668851191D49856E17F8FBCD

### Index de la clé 0F (1408)

En-tête	20
Code de service	00 00 00 00
Taille du modulo relatif aux clés révélées de l'organisme de certification	00 B0
Code de l'algorithme relatif aux clés révélées de l'organisme de certification	01
Taille de l'exposant des clés révélées de l'organisme de certification	01
Code du fournisseur enregistré de l'application (RID)	A0 00 00 00 25
Index des clés révélées de l'organisme de certification	0F
Modulo relatif aux clés révélées de l'organisme de certification	C8D5AC27A5E1FB89978C7C6479AF993AB3800EB243996FBB2AE26B67B23AC482C4B746005A51AF A7D2D83E894F591A2357B30F85B85627FF15DA12290F70F05766552BA11AD34B7109FA49DE29DCB0109670875A17EA95549E92347B948AA1F045756DE56B707E3863E59A6CBE99C1272EF65FB66CBB4CFF070F36029DD76218B21242645B51CA752AF37E70BE1A84FF31079DC0048E928883EC4FADD497A719385C2BBBEBBC5A66AA5E5655D18034EC5
Exposant des clés révélées de l'organisme de certification	03
Valeur de hachage	A73472B3AB557493A9BC2179CC8014053B12BAB4

### Index de la clé 10 (1984)

En-tête	20
Code de service	00 00 00 00
Taille du modulo relatif aux clés révélées de l'organisme de certification	00 F8
Code de l'algorithme relatif aux clés révélées de l'organisme de certification	01
Taille de l'exposant des clés révélées de l'organisme de certification	01
Code du fournisseur enregistré de l'application (RID)	A0 00 00 00 25
Index des clés révélées de l'organisme de certification	10
Modulo relatif aux clés révélées de l'organisme de certification	CF98DFEDB3D3727965EE7797723355E0751C81D2D3DF4D18EBAB9FB9D49F38C8C4A826B99DC9DEA3F01043D4BF22AC3550E2962A59639B1332156422F788B9C16D40135EFD1BA94147750575E636B6EBC618734C91C1D1BF3EDC2A46A43901668E0FFC136774080E888044F6A1E65DC9AAA8928DACBE B0DB55EA3514686C6A732CEF55EE27CF877F110652694A0E3484C855D882AE191674E25C296205BB B599455176FDD7BBC549F27BA5FE35336F7E29E68D783973199436633C67EE5A680F05160ED12D16 65EC83D1997F10FD05BDBBF9433E8F797AEE3E9F02A34228ACE927ABE62B8B9281AD08D3DF5C737 9685045D7BA5FCDE58637
Exposant des clés révélées de l'organisme de certification	03
Valeur de hachage	C729CF2FD262394ABC4CC173506502446AA9B9FD



## ANNEXE B : MESSAGES AFFICHÉS

Le tableau B-1 présente les messages qu'un terminal peut afficher au cours d'une opération par Carte à puce. Il fournit également des renseignements sur le moment où chaque message peut être utilisé. Ce tableau sert de guide, mais ne constitue pas une liste exhaustive.

Tableau B-1 : messages affichés par le terminal

Message	Fonction
APPELER L'ÉMETTEUR	Utilisé quand une réponse exigeant une autorisation verbale est envoyée au terminal, indiquant que le marchand doit communiquer avec l'émetteur.
APPELER LE CENTRE D'AUTORISATION	Sert à aviser le marchand qu'une autorisation verbale doit être obtenue à la demande de la banque administratrice ou en raison de problèmes de connexion.
APPELER LE SOUTIEN TECHNIQUE	Utilisé quand le terminal présente un problème technique dont la résolution nécessite un soutien technique.
AUTORISATION VERBALE	Sert à aviser le marchand qu'une autorisation verbale est exigée ou en cours.
CARTE DE CONTRÔLE	Sert à demander l'insertion ou le glissement de la Carte de contrôle pour l'exécution de certaines fonctions.
CARTE NON AUTORISÉE	Opération non autorisée (voir REFUSÉE).
CHARGEMENT	Indique que le terminal reçoit les données de configuration d'un ordinateur distant.
CHOISIR LE TYPE DE PAIEMENT	Message utilisé quand de multiples options de paiement s'appliquent à une seule Carte (p. ex., débit ou crédit).
CODE D'AUTORISATION : nnnnn	Sert à afficher le code d'autorisation réel ou, si une opération est autorisée par le terminal, à afficher le code qui est créé par celui-ci.
CONNEXION ÉTABLIE	Indique que la connexion a été établie avec succès entre le terminal et le système hôte de la banque administratrice.
DATE D'EXPIRATION : MM/AA	Sert à demander l'entrée de la date d'expiration de la Carte.
DEMANDE INVALIDE	Indique que l'opération demandée n'est pas prise en charge pour le type de Carte présenté.
DERNIER ESSAI DE SAISIE DU NIP	Avertit le titulaire de la Carte qu'il n'a plus qu'un seul essai pour saisir son NIP avant que celui-ci ne soit bloqué.
NIP INEXACT – DERNIER ESSAI DE SAISIE DU NIP	
EN TRAITEMENT – UN MOMENT S.V.P.	Utilisé durant l'interaction entre le terminal et la Carte, au cours de laquelle la Carte <b>ne devrait pas</b> être retirée.
ENTRÉE EN VIGUEUR : MM/AA	Sert à demander la saisie de la date d'entrée en vigueur de la Carte.
ENTRER LE MONTANT	Sert à demander le montant.
ENTRER LE NUMÉRO DE LA CARTE	Indique que la bande magnétique n'a pas été lue avec succès trois fois de suite.

<b>Message</b>	<b>Fonction</b>
ERREUR DE SAISIE DE NIP ou NIP INVALIDE	Indique qu'un NIP inexact a été saisi.
NIP INEXACT – RÉESSAYER	
GLISSER À NOUVEAU	Indique que la bande magnétique n'a pas été lue avec succès.
GLISSER LA CARTE	Message utilisé à l'étape du processus où les données de la Carte à bande magnétique sont exigées.
IMPOSSIBLE D'ÉTABLIR LA CONNEXION, OPÉRATION AUTORISÉE HORS LIGNE	Peut servir à fournir d'autres renseignements sur le traitement de l'opération.
IMPOSSIBLE D'ÉTABLIR LA CONNEXION, OPÉRATION REFUSÉE HORS LIGNE	
INSÉRER DE NOUVEAU	Indique que la puce n'a pas été lue avec succès.
INSÉRER LA CARTE	Sert à demander que la Carte soit insérée plutôt que glissée.
LE TITULAIRE DE LA CARTE DOIT SAISIR SON NIP	L'un ou l'autre de ces messages est affiché quand le titulaire de la Carte doit saisir son NIP.
SAISIR LE NIP	
LIGNE OCCUPÉE	Indique que la ligne téléphonique à laquelle se connecte le terminal est occupée.
LIMITE D'ESSAIS DE SAISIE DU NIP DÉPASSÉE – APPELER L'ÉMETTEUR	Quand le compteur d'essais de saisie du NIP affiche « 0 ».
MAXIMUM COMPTE OUVERT XX,XX \$ SAISIR LE NIP	Message utilisé dans les bars et les restaurants pour indiquer au titulaire de la Carte le montant maximal pour lequel il peut être facturé si la Carte est conservée par le marchand jusqu'au paiement final.
MAXIMUM XX \$ – VEUILLEZ SAISIR VOTRE NIP	Indique le montant maximal pour lequel une opération peut être effectuée.
MÉMOIRE PLEINE	Sert à aviser le marchand que la mémoire d'opérations est remplie et que le terminal doit communiquer avec la banque administratrice.
MONTANT ESTIMATIF MAXIMAL XXX,XX	Utilisé dans les hôtels, les agences de location de voiture, les restaurants et les bars lorsque que le titulaire de la Carte effectue une opération pour laquelle le montant final n'est pas encore connu.
MONTANT MAXIMAL XXX,XX	
MAXIMUM POUR COMPTE OUVERT XXX,XX SAISIR LE NIP	

<b>Message</b>	<b>Fonction</b>
NE PAS RETIRER LA CARTE	Avertit le titulaire de la Carte ou le marchand de ne pas retirer la Carte.
NIP BLOQUÉ	Indique que le NIP associé à la Carte à puce a été bloqué relativement à l'opération en cours ou à une opération antérieure.
NIP OK	Indique que le NIP a été saisi correctement.
OPÉRATION ANNULÉE	Message utilisé si l'opération est annulée par le terminal avant une autorisation verbale.
OPÉRATION TERMINÉE	Indique que l'opération a été terminée.
POURBOIRE? ENTRER/ANNULER	Permet aux titulaires de la Carte d'ajouter un pourboire.
REFUSÉE	Message imprimé ou affiché à la suite d'une autorisation verbale si la banque administratrice, l'émetteur ou la Carte a refusé l'opération et que le marchand a transmis ce renseignement au terminal.
REFUSÉE PAR L'ÉMETTEUR – LE TITULAIRE DEVRAIT COMMUNIQUER AVEC L'ÉMETTEUR	Avisé le marchand et le titulaire de la Carte du résultat de l'opération et de la marche à suivre.
REFUSÉE PAR LA CARTE – LE TITULAIRE DEVRAIT COMMUNIQUER AVEC L'ÉMETTEUR	
REMETTRE CARTE AU MARCHAND	Sert à demander au titulaire de passer la Carte au commis à la caisse.
RETIRER LA CARTE	Sert à demander au marchand ou au titulaire de la Carte de retirer la Carte du terminal.
TERMINÉE	Indique que l'opération est terminée.
TOTAUX DE LA SESSION NON ACCEPTÉE NON CONFIRMÉE NE PEUT CONFIRMER	Message utilisé au cours d'un rapprochement afin d'aviser le marchand de l'état de l'opération de rapprochement.
UN MOMENT S.V.P.	Utilisé sur réception d'un message « en attente » avec un élément de données de message vide. Sans la présence de ce message, le terminal <b>devrait</b> afficher le contenu des éléments de données du message.
VÉRIFIER LA SIGNATURE	Sert à demander la vérification de visu de la signature.
VEUILLEZ INITIALISER	Indique que le terminal doit être initialisé afin de télécharger un nouveau logiciel ou de nouveaux paramètres (« INITIALISER SVP » si le terminal ne peut afficher plus de 16 caractères).



## ANNEXE C : GLOSSAIRE ET ACRONYMES

<b>AAC</b>	Cryptogramme d'authentification de l'application. Type de cryptogramme indiquant que la Carte à puce a refusé l'opération
<b>AID</b>	Code de l'application. Valeur définie par [ISO 7816-5] et servant à identifier l'application du terminal
<b>ANSI</b>	American National Standards Institute
<b>ARPC</b>	Cryptogramme de réponse à la demande d'autorisation. Type de cryptogramme produit par l'émetteur, utilisé pour permettre à la Carte à puce de valider la réponse à la demande d'autorisation
<b>ARQC</b>	Cryptogramme de demande d'autorisation. Type de cryptogramme produit par une Carte à puce lorsque celle-ci établit que les données de l'opération devraient être envoyées en ligne
<b>ASCII</b>	American Standard Code for Information Interchange. Code pour représenter les caractères en nombres binaires
<b>Authentification de la Carte</b>	Processus par lequel les Cartes à puce conformes aux normes EMV s'authentifient auprès des systèmes des terminaux et des émetteurs
<b>Autorisation par intervention du marchand</b>	Si une opération ne peut être autorisée par un émetteur, le marchand peut le faire à la place de ce dernier et décider s'il est prêt ou non à accepter les risques et à autoriser l'opération
<b>AXP</b>	American Express
<b>Banque administratrice</b>	Entité ayant conclu un contrat avec un marchand, en vertu duquel : i. un titulaire de Carte est autorisé à porter à une Carte des achats de biens ou de services qu'il a effectués auprès de ce marchand et ii. le marchand accepte de transférer ces opérations à la banque administratrice
<b>C4C</b>	Code de lot de quatre chiffres
<b>CA</b>	Cryptogramme d'application
<b>CAM</b>	Code d'authentification du message
<b>CAPK</b>	Clé révélée de l'organisme de certification
<b>Carte à puce</b>	Carte munie d'une puce de silicium intégrée
<b>Clavier de composition du NIP</b>	Composante d'un terminal dont se sert le titulaire de la Carte pour saisir son NIP aux fins de vérifications de son identité
<b>Code de sélection de l'application</b> (Application Selection Indicator)	Code inscrit dans le logiciel du terminal, qui détermine si une sélection partielle de l'application est possible

<b><i>Cryptogramme</i></b>	Données de sécurité créées par la Carte à puce ou le système de l'émetteur et servant à valider une opération ou un message de réponse à une demande d'autorisation
<b><i>CSC4</i></b>	Code de sécurité de la Carte de quatre chiffres
<b><i>CVM</i></b>	Méthode de vérification de l'identité du titulaire de la Carte
<b><i>DDA</i></b>	Authentification des données dynamiques. Méthode par laquelle un terminal peut authentifier une Carte à puce, telle qu'elle est définie dans les spécifications EMV
<b><i>DDOL</i></b>	Liste d'objets de données relative à l'authentification de données dynamiques (DDA)
<b><i>Dispense du NIP</i></b>	Programme permettant aux marchands supervisant une opération par Carte à puce avec saisie du NIP de dispenser les titulaires de la Carte d'une saisie de NIP afin d'empêcher un nombre élevé de refus d'autorisation en raison de l'incapacité des titulaires de la Carte à se souvenir de leur NIP
<b><i>Données sur l'application de l'émetteur</i></b>	Données relatives à l'authentification de l'émetteur
<b><i>Émetteur</i></b>	Toute entité émettant une carte de paiement ou exploitant une entreprise d'émission de cartes de paiement
<b><i>EMV</i></b>	Terme utilisé pour faire référence aux spécifications mondiales d'EMVCo. L'application sur la Carte à puce et celle dans le terminal, qui servent à effectuer des opérations. « EMV » est une marque de commerce d'EMVCo, LLC.
<b><i>EMVCo</i></b>	EMVCo LLC, l'organisation qui gère les spécifications EMV ainsi que le processus d'autorisation relatif aux cartes et aux terminaux
<b><i>En ligne</i></b>	Désigne une opération dont les données sont envoyées à la banque administratrice avant que l'opération ne soit terminée
<b><i>Fichier d'exceptions</i></b>	Fichier de numéros de compte utilisé au cours de l'autorisation par intervention du marchand, pour lequel l'émetteur a prédéterminé la décision finale relative à l'autorisation ou au refus (p. ex., état négatif) ou exige un traitement spécial (p. ex., VIP)
<b><i>Fournisseur de terminaux</i></b>	Société qui fabrique et vend des terminaux
<b><i>Fournisseurs de services de paiement</i></b>	Partie exploitant un réseau de paiement par carte
<b><i>Hors ligne</i></b>	Désigne une opération qui est effectuée sans que le terminal ne communique avec le système de la banque administratrice
<b><i>ISO</i></b>	International Organization for Standardization
<b><i>LHLIOC</i></b>	Limite hors ligne inférieure pour opérations consécutives
<b><i>LHLSOC</i></b>	Limite hors ligne supérieure pour opérations consécutives

<b>Marchand ou établissement</b>	Toute personne ou entreprise ayant conclu un contrat avec une banque administratrice, en vertu duquel cette personne accepte de satisfaire aux exigences suivantes : i. permettre au titulaire de la Carte de porter à sa Carte les achats de biens et de services qu'il a effectués auprès du marchand ou de l'établissement et ii. transférer ces opérations à une banque administratrice
<b>Maximum permis</b>	Montant d'argent maximal pour une opération unique, à partir duquel une autorisation doit être obtenue avant de terminer l'opération
<b>Maximum permis au terminal</b>	Montant d'argent maximal pour une opération unique, programmé dans le terminal, à partir duquel le terminal doit obtenir une autorisation avant de terminer l'opération
<b>Maximum permis sans autorisation pour une opération par intervention du marchand</b>	Montant d'argent maximal pour une opération unique, à partir duquel le marchand doit obtenir une autorisation avant de terminer l'opération. Cette valeur n'est utilisée qu'au moment de l'autorisation par intervention du marchand et peut être chargée dans le système hôte du terminal ou de la société de traitement indépendante
<b>NIB</b>	Numéro d'identification de la banque. Numéro de six chiffres désignant l'institution de l'émetteur. Constitue également les six premiers chiffres d'un numéro de compte-Card attribué par l'émetteur.
<b>NIP</b>	Numéro d'identification personnel
<b>Normes PCI DSS</b>	Normes de sécurité des données du secteur des cartes de paiement
<b>PAN</b>	Numéro du compte principal
<b>PCPAE (AEIPS)</b>	Spécifications pour les paiements par Cartes à puce American Express. Il y a deux types de spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)) : <ul style="list-style-type: none"><li>• Spécifications – Carte à puce American Express [AEIPS-CARD], qui définissent les éléments de données techniques et la fonctionnalité au moment de la mise en œuvre des Cartes à puce, et ce, pour tous les établissements affiliés à American Express.</li><li>• Spécifications – Terminal traitant les opérations portées à une Carte à puce American Express [AEIPS-TERM], qui soulignent les fonctions que le terminal doit pouvoir effectuer pour le traitement des opérations par Carte à puce American Express.</li></ul>
<b>PdV</b>	Point de vente; voir « Terminal »
<b>PIX</b>	Code d'application (AID) de propriété exclusive
<b>Revendeur</b>	Entité qui achète des terminaux d'un fournisseur de terminaux, qui développe et met en œuvre un logiciel propre à un pays, puis revend les terminaux aux marchands ou à d'autres clients
<b>Script de l'émetteur</b>	Ensemble de commandes relatives aux cartes, créées et envoyées par l'émetteur afin de gérer et de mettre à jour des cartes

<b><i>SDA</i></b> ( <i>authentification des données permanentes</i> )	Méthode par laquelle un terminal peut authentifier une Carte à puce, telle qu'elle est définie dans les spécifications EMV
<b><i>Société de traitement indépendante</i></b>	Entreprise qui traite les opérations par Carte American Express au nom des marchands, des banques administratrices ou des émetteurs
<b><i>SPCPAE (AEIPS)</i></b>	Spécifications pour le paiement par Carte à puce American Express (spécifications PCPAE (AEIPS)); voir PCPAE (AEIPS).
<b><i>TC</i></b>	Certificat de l'opération. Signature numérique composée d'objets de données choisis par l'émetteur. Le certificat d'opération (TC), produit par la Carte à puce à la fin d'une opération autorisée, permet à l'émetteur de vérifier qu'aucunes données sensibles contenues sur la puce n'ont été modifiées avant la validation de la Carte
<b><i>TDOL</i></b>	Liste d'objets de données relative aux certificats d'opération
<b><i>Terminal</i></b>	Appareil prenant en charge les Cartes American Express pour le paiement de produits et de services
<b><i>Titulaire ou titulaire de la Carte</i></b>	Personne ayant conclu un contrat avec un émetteur et ayant ouvert un compte chez celui-ci, ou personne dont le nom figure sur une Carte
<b><i>TPSS</i></b>	Terminal de paiement sans surveillance. Appareil non surveillé muni d'un lecteur de cartes, qui distribue un produit ou fournit un service (p. ex., un distributeur d'essence) payé au moyen d'une Carte valide, après activation par celle-ci. Également appelé « terminal activé par Carte »
<b><i>Traitement de rechange</i></b>	Si une opération par Carte à puce ne peut être terminée à un terminal prenant en charge la technologie EMV, le terminal lit la bande magnétique
<b><i>Vérification de l'identité du titulaire de la Carte</i></b>	Processus permettant de vérifier l'identité du titulaire de la Carte





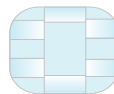




outils EMV<sup>MC</sup>



MD



**A** | **MERICAN**  
**E** | **XPRESS**  
**I** | Integrated Circuit Card  
**P** | Payment  
**S** | Specification