CONTRAT D'ACCEPTATION EN PAIEMENT DE PROXIMITE
PAR CARTES DE PAIEMENT AVEC PREAUTORISATION (HORS AUTOMATES)

PARTIE 1

CONDITIONS GENERALES COMMUNES A TOUS LES SCHEMAS

ARTICLE 1 - DEFINITIONS

1) L'"Accepteur" peut être tout commerçant, tout prestataire de services, toute personne exerçant une profession libérale, et d'une manière générale tout professionnel, en l'espèce le professionnel exploitant un établissement de soins et qui, afin d'assurer le bon règlement des frais de séjour dus par sa clientèle, est susceptible d'utiliser un Système d'Acceptation reconnu par le(s) Schéma(s) dûment convenu(s) avec la Banque, et dont les modalités de paiement par Carte présente la particularité que le montant exact desdits frais n'est pas connu lorsque le titulaire de la Carte donne son consentement.

L'Accepteur dispose de toute liberté pour domicilier ses remises à l'encaissement auprès de l'établissement de crédit ou de paiement de son choix, membre du Schéma, et avec lequel il a passé un contrat pour ce faire.

L'Accepteur déclare disposer de toutes les informations déterminantes pour son consentement et que toutes ses demandes d'informations afférentes, notamment aux stipulations du présent Contrat et à la qualité des Parties, ont été satisfaites par la Banque.

2) Par "Paiement de proximité avec préautorisation", il faut entendre une opération de paiement comportant deux étapes :

- Avant le début de la prestation, l'Accepteur effectue une demande d'autorisation pour le montant estimé des frais réels.

  Cette opération est effectuée en présence physique du titulaire de la Carte dans les conditions visées à l'article 5.2 ci-après,

  L'enregistrement de cette opération est conservé jusqu'à l'échéance visée ci-après.
- La clôture de l'opération de paiement doit être effectuée au jour où le paiement des frais susvisés est dû, et au plus tard à l'expiration d'un délai de 30 (trente) jours calendaires courant à compter du jour de la demande d'autorisation susvisée.

  Elle est effectuée pour le montant final desdits frais, **qui ne peut être supérieur au montant estimé des frais réels**.

  La demande d'autorisation et la clôture de l'opération de paiement doivent être effectuées avec la même Carte.

  Si le titulaire de la Carte est présent lors de la clôture de l'opération de paiement et que le montant de la prestation est supérieur au montant estimé des frais réels, le paiement de la différence est possible selon les modalités du contrat d'acceptation en paiement de proximité par cartes de paiement que l'Accepteur doit avoir conclu par ailleurs.

  Après la clôture de l'opération de paiement, l'Accepteur peut, en l'absence physique du titulaire de la Carte et à distance, réaliser une nouvelle opération de paiement appelée **"facture complémentaire"** qui est destinée au paiement des frais qui n'ont pu être identifiés lors de ladite clôture.

  Un numéro de dossier, tel que visé à l'article 2.6 ci-après, doit être attribué à la facture complémentaire. Il doit être identique à celui de l'opération de paiement clôturée à laquelle la facture complémentaire fait suite.

  Pour cette facture complémentaire, l'Accepteur ne bénéficie **d'aucune garantie de paiement** et n'est donc réglé que sous bonne fin d'encaissement et en l'absence de contestation.

3) Par "Marque", il faut entendre tout nom, terme, sigle, symbole matériel ou numérique ou la combinaison de ces éléments susceptible de désigner le Schéma.

Les Marques pouvant être acceptées entrant dans le champ d'application du présent Contrat sont CB, Visa et MasterCard.

4) Par "Banque", il faut entendre l'établissement de crédit habilité à organiser l'acceptation des Cartes portant la(les) Marque(s) du(des) Schéma(s) visé(s) en partie 2 du présent Contrat.

5) Par "Système d'Acceptation", il faut entendre les logiciels, protocoles et équipements conformes aux spécifications définies par chaque Schéma et nécessaires à l'enregistrement, à la transmission et au traitement sécurisé des ordres de paiement par Cartes portant l'une des Marques dudit Schéma. L'Accepteur doit s'assurer que le Système d'Acceptation a fait l'objet d'un agrément par l'entité responsable du Schéma, le cas échéant en consultant la liste des Systèmes d'Acceptation reconnus par l'entité responsable du Schéma.

6) Par "Equipement Electronique", il faut entendre tout dispositif de paiement capable de lire la Carte équipée d'une puce au standard EMV ou d'une piste magnétique permettant l'authentification du titulaire de la Carte.

L'Equipement Electronique est soit agréé soit approuvé par l'entité responsable de chacun des Schémas dont les Cartes sont acceptées sur cet équipement.

Actuellement, ce contrôle est opérationnel avec les Cartes portant les Marques CB, Visa, MasterCard, VPAY, Maestro et ELECTRON.

L'agrément ou l'approbation de l'Equipement Electronique est une attestation de conformité avec des spécifications techniques et fonctionnelles définies par chaque Schéma concerné, qui dispose de la liste des Equipements Electroniques agréés ou approuvés.

7) Par "Règlement", il faut entendre le Règlement UE n°2015/751 du 29 avril 2015.

8) Par "Catégorie de carte", on entend les catégories de Carte suivantes:
- crédit ou carte de crédit,
- carte de débit,
- carte prépayée
- carte commerciale.

9) Par "Carte", on entend un instrument de paiement qui permet au payeur d'initier une opération de paiement. Elle porte une ou plusieurs Marques.

Lorsque la Carte est émise dans l'Espace Economique Européen (ci-après l'"EEE" - Il comprend les Etats membres de l'Union Européenne, l'Islande, le Liechtenstein et la Norvège), elle porte au moins l'une des mentions suivantes:
- crédit ou carte de crédit
- débit,
- prépayé,
- commercial,

ou l'équivalent dans une langue étrangère.

10) Par "Schéma", il faut entendre un ensemble de règles régissant l'exécution d'opérations de paiement liées à une carte tel que défini à l'article 2 du Règlement.

Les Schémas CB, Visa et MasterCard reposent sur l'utilisation de Cartes CB, Visa et MasterCard auprès des Accepteurs acceptant les Marques desdits Schémas, et cela dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits Schémas.

11) Par "Point d'acceptation", on entend le lieu physique où est initié l'ordre de paiement.

12) Par "Contrat ", il faut entendre ensemble les Conditions Générales communes à tous les Schémas (partie 1), les dispositions spécifiques à chaque Schéma (partie 2) et les conditions particulières convenues entre les Parties (ci-après les "Conditions Particulières").

13) Par "Instrument de paiement « sans contact »", il faut entendre un instrument de paiement disposant de la technologie « sans contact » constitué d'un logiciel de paiement mobile en mode «sans contact » intégré pour partie dans l'élément sécurisé d'un téléphone mobile, pour partie dans le téléphone mobile lui-même, et permettant de réaliser quelle que soit la Marque des opérations de paiement.

14) Par "Parties", il faut entendre la Banque et l'Accepteur.

ARTICLE 2 - OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur s'engage à:

2.1 Afficher visiblement chaque Marque qu'il accepte notamment en apposant de façon apparente à l'extérieur et à l'intérieur de son Point d'acceptation des panonceaux, vitrophanies et enseignes qui lui sont fournis par la Banque ou le Schéma.

Pour la(les) Marque(s) qu'il accepte, l'Accepteur doit accepter toutes les Cartes émises hors de l'EEE sur lesquelles figure(nt) cette(ces) Marque(s) quelle qu'en soit la Catégorie de carte.

2.2 Afficher visiblement chaque Catégorie de carte qu'il accepte ou refuse de façon apparente à l'extérieur et à l'intérieur de son Point d'acceptation.

2.3 Afficher visiblement le montant minimum éventuel à partir duquel la Carte ou la Catégorie de carte est acceptée afin que le titulaire de la Carte en soit préalablement informé.

2.4 En cas de présence de plusieurs Marques sur la Carte, respecter la Marque choisie par le titulaire de la Carte pour donner l'ordre de paiement.

2.5 Afin que le titulaire de la Carte n'ait pas de difficulté à vérifier et identifier les opérations de paiement qu'il a effectuées, vérifier avec la Banque la conformité des informations transmises pour identifier son Point d'acceptation. Les informations doivent indiquer une dénomination commerciale connue du titulaire de la Carte et permettre de dissocier ce mode de paiement par rapport aux autres modes de paiement (automate, vente à distance, etc.) dans ce Point d'acceptation.

2.6 Attribuer à l'occasion de l'initialisation de l'opération de paiement un numéro de dossier indépendant du numéro de la Carte

2.7 Accepter les paiements effectués avec les Cartes portant la(les) Marque(s) et Catégorie(s) de carte qu'il a choisi d'accepter ou qu'il doit accepter des Schémas en contrepartie d'actes de location de biens et de services offerts à sa clientèle et qu'il fournit ou réalise lui-même.

2.8 Ne pas collecter au titre du présent Contrat une opération de paiement pour laquelle il n'a pas reçu lui-même le consentement du titulaire de la Carte.

2.9 Transmettre les enregistrements des opérations de paiement à la Banque, dans les délais prévus dans les Conditions Particulières convenues avec lui.

2.10 Régler, selon les Conditions Particulières convenues avec la Banque, les commissions, frais et d'une manière générale toute somme due au titre de l'acceptation des Cartes.

2.11 Utiliser obligatoirement l'Equipement Electronique muni de l'extension de service « Paiement de proximité pour la location de biens et de services (PLBS) » et ne pas modifier les paramètres de son fonctionnement.

2.12 Assurer lui-même directement l'achat ou la location, l'installation, le fonctionnement, la maintenance et la mise à niveau de l'Equipement Electronique.

Il doit par ailleurs:
- Veiller à ce que sa police d'assurance couvre bien:
  - les risques inhérents à la garde de l'Equipement Electronique dont la Banque ne saurait être responsable, ainsi que les dommages directs ou indirects résultant de sa destruction ou de son altération,
  - les dommages directs ou indirects sur les Cartes utilisées et sur les équipements annexes qui auraient pu lui être confiés,
- Laisser libre accès au constructeur, à la Banque ou à toute personne désignée par cette dernière pour les différents travaux à effectuer, et à la Banque ou aux Schémas pour audit,

- Ne pas utiliser l'Equipement Electronique à des fins illicites ou non autorisées par le constructeur ou la Banque, et n'y apporter aucune modification de logiciel ayant un impact sur les Schémas sans accord préalable de la Banque et sans nouvelle procédure d'agrément par l'entité responsable de chacun des Schémas dont les Cartes sont acceptées sur cet équipement,
- assurer, selon le mode d'emploi, les conditions de bon fonctionnement de l'Equipement Electronique.

2.13 Prendre toutes les mesures propres à assurer la garde de son Equipement Electronique et être vigilant quant à l'utilisation qui en est faite.

2.14 Prévoir, dans ses relations contractuelles avec les tiers, tels que les prestataires de services techniques ou sous-traitants intervenant dans le traitement et le stockage des données liées à l'utilisation des Cartes, que ces derniers s'engagent à respecter tant le référentiel Sécuritaire Accepteur annexé au présent Contrat que le Référentiel Sécuritaire PCI/DSS, acceptent que les audits visés à l'article 2.15 ci-dessous soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé audit article.

2.15 Permettre à la Banque de faire procéder, aux frais de l'Accepteur dans les locaux de l'Accepteur ou dans ceux des tiers visés à l'article 2.14 ci-dessus, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences du Référentiel Sécuritaire Accepteur annexé au présent Contrat et/ou de celles du Référentiel Sécuritaire PCI/DSS. Cette vérification, appelée « procédure d'audit », peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée.

L'Accepteur autorise la communication du rapport à la Banque et aux Schémas concernés.

Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquements à ces clauses ou exigences, la Banque, le cas échéant à la demande d'un(des) Schéma(s), peut procéder à une suspension de l'acceptation des Cartes portant ses Marques par l'Accepteur, voire à une demande de résiliation du présent Contrat telle que prévue à l'article 9 de la présente partie 1.

2.16 L'Accepteur doit respecter les exigences du Référentiel Sécuritaire Accepteur annexé au présent Contrat et celles du Référentiel Sécuritaire PCI/DSS dont il peut prendre connaissance à l'adresse suivante:
https://fr.pcisecuritystandards.org/minisite/en/
ou qui lui sera communiqué par la Banque à première demande.

2.17 Faire son affaire personnelle des litiges liés à la relation sous-jacente qui existe entre lui et le titulaire de la Carte (litige commercial par exemple), et de leurs conséquences financières.

2.18 En cas de survenance d'un incident de sécurité majeur, notamment en cas de collecte/utilisation frauduleuse des données, coopérer avec la Banque et, le cas échéant, avec les autorités compétentes. Le refus ou l'absence de coopération de la part de l'Accepteur pourra conduire la Banque à résilier le présent Contrat conformément à l'article 9 de la présente partie 1.

2.19 **Ne pas faire usage de la Carte pour s'octroyer une caution ou un dépôt de garantie.**

2.20 En cas de manquement de l'Accepteur aux dispositions du présent Contrat concernant les mesures de sécurité ou en cas de taux d'impayés constaté anormalement élevé ou d'utilisation anormalement élevée de Cartes/d'Instruments de paiement « sans contact » volé(e)s, perdu(e)s ou contrefait(e)s ayant entraîné , le cas échéant, l'application de pénalités par les Schémas à la Banque, indemniser la Banque du montant desdites pénalités versées par la Banque aux Schémas.

ARTICLE 3 - OBLIGATIONS DE LA BANQUE

La Banque s'engage à :

3.1 Fournir à l'Accepteur les informations le concernant directement sur le fonctionnement du(des) Schéma(s) visé(s) dans la partie 2 et son/leur évolution, les Catégories de carte et les Marques dont il assure l'acceptation ainsi que les frais applicables à chacune des Catégories de carte et Marques acceptées par lui, y compris les commissions d'interchange et les frais versés au(x) Schéma(s).

3.2 Respecter le choix de la Marque utilisée pour donner l'ordre de paiement effectué au Point d'acceptation conformément au choix de l'Accepteur ou du titulaire de la Carte.

3.3 Mettre à la disposition de l'Accepteur, selon les modalités convenues aux Conditions Particulières, les informations relatives à la sécurité des opérations de paiement, notamment l'accès au serveur d'autorisation.

3.4 Indiquer à l'Accepteur la liste et les caractéristiques des Cartes (Marques et Catégories de carte) pouvant être acceptées et lui fournir, à sa demande, le fichier des codes émetteurs (BIN).

3.5 Créditer le compte de l'Accepteur des sommes qui lui sont dues selon les modalités convenues aux Conditions Particulières.

3.6 Ne pas débiter, au-delà du délai maximum de 15 (quinze) mois à partir de la date du crédit initial porté au compte de l'Accepteur, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

3.7 Selon les modalités convenues avec l'Accepteur, communiquer au moins une fois par mois les informations suivantes:
- la référence lui permettant d'identifier l'opération de paiement,
- le montant de l'opération de paiement exprimé dans la devise dans laquelle son compte est crédité,
- le montant de tous les frais appliqués à l'opération de paiement et le montant de la commission de service acquittée par l'Accepteur et de la commission d'interchange.

L'Accepteur peut demander à ce que ces informations soient regroupées par Marque, application de paiement, Catégorie de carte et par taux de commission d'interchange applicable à l'opération.

3.8 Indiquer et facturer à l'Accepteur les commissions de services à acquitter séparément pour chaque Catégorie de carte et chaque Marque selon les différents niveaux de commission d'interchange.

L'Accepteur peut demander à ce que les commissions de services soient regroupées par Marque, application de paiement, Catégorie de carte et par taux de commission d'interchange applicable à l'opération.

ARTICLE 4 - GARANTIE DE PAIEMENT

4.1 Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées tant à l'article 5 de la présente partie 1 qu'en partie 2 du présent Contrat, ainsi qu'aux Conditions Particulières, sauf en cas de demande de remboursement du titulaire de la Carte fondée sur l'article L.133-25 du Code monétaire et financier.

4.2 Toutes les mesures de sécurité sont indépendantes les unes des autres.

Ainsi, l'autorisation donnée par le serveur d'autorisation ne vaut garantie que sous réserve du respect des autres mesures de sécurité, et notamment le contrôle du code confidentiel.

4.3 En cas de non-respect d'une seule de ces mesures, les opérations de paiement ne sont réglées que sous réserve de bonne fin d'encaissement.

4.4 En cas d'opération de paiement réalisée hors la présence physique du titulaire de la Carte à distance, les factures et les enregistrements ne sont réglés que sous réserve de bonne fin d'encaissement, et en l'absence de contestation.

ARTICLE 5 - MESURES DE SECURITE

5.1 L'Accepteur doit informer immédiatement la Banque en cas de fonctionnement anormal de l'Equipement Electronique et pour toutes autres anomalies.

5.2 **Lors du paiement**

L'Accepteur s'engage à:

5.2.1 Vérifier l'acceptabilité de la Carte, c'est-à-dire :

- la Marque, la Catégorie de carte du Schéma concerné par l'acceptation,
- le cas échéant l'hologramme sauf pour les Cartes n'en disposant pas,
- la puce sur les Cartes lorsqu'elle y est prévue par le Schéma,
- la Marque et Catégorie de carte définies dans les Conditions spécifiques au Schéma concerné figurant dans la partie 2 du présent Contrat ou dans les Conditions Particulières,
- le cas échéant, la période de validité (fin et éventuellement début).

5.2.2 Utiliser l'Equipement Electronique muni de l'extension de service «Paiement de proximité pour la location de biens et de services (PLBS) » conforme aux spécifications en vigueur, respecter les indications affichées sur son écran et suivre les procédures dont les modalités techniques lui ont été indiquées.

L'Equipement Electronique doit notamment:

- après la lecture de la puce de la Carte lorsqu'elle est présente:
  - permettre le contrôle du code confidentiel lorsque la puce le lui demande,
  - vérifier:
    - le code émetteur de la Carte (BIN),
    - le code service,
    - le cas échéant, la date de fin de validité de la Carte.
- lorsque la puce n'est pas présente sur une Carte, après lecture de la piste ISO 2, vérifier:
  - le code émetteur de la Carte (BIN),
  - le code service,
  - le cas échéant, la date de fin de validité de la Carte.

5.2.3 Contrôler le numéro de la Carte par rapport à la dernière liste des Cartes faisant l'objet d'un blocage ou d'une opposition diffusée par la Banque pour le Point d'acceptation concerné et selon les modalités convenues aux Conditions Particulières.

5.2.4 Lorsque la puce le demande à l'Equipement Electronique, faire composer par le titulaire de la Carte, dans les meilleures conditions de confidentialité, son code confidentiel. La preuve de la frappe du code confidentiel est apportée par le certificat qui doit figurer sur le ticket émis par l'Equipement Electronique conservé par l'Accepteur (ci-après "Ticket ").

Lorsque le code confidentiel n'est pas vérifié, l'opération n'est réglée que sous réserve de bonne fin d'encaissement, même en cas de réponse positive à la demande d'autorisation.

5.2.5 Obtenir systématiquement une autorisation d'un montant identique à celui connu et accepté par le titulaire de la Carte.

Lorsque la puce n'est pas présente sur une Carte, l'autorisation doit être demandée en transmettant l'intégralité des données de la piste ISO 2.

Une opération pour laquelle l'autorisation a été refusée par le serveur d'autorisation n'est jamais garantie.

Une demande de capture de Carte, faite par le serveur d'autorisation, annule la garantie pour toutes les opérations faites postérieurement le même jour et avec la même Carte dans le même Point d'acceptation.

5.2.6 Faire signer le Ticket:

- dans tous les cas où l'Equipement Electronique le demande,
- lorsque le montant de l'opération est supérieur à 1 500 euros.

5.2.7 Lorsque la signature est requise et que la Carte comporte un panonceau de signature, vérifier attentivement la conformité de celle-ci avec celle qui figure sur ledit panonceau.

Pour une Carte sur laquelle ne figure pas le panonceau de signature, vérifier la conformité de la signature utilisée avec celle qui figure sur la pièce d'identité présentée par le titulaire de la Carte.

5.2.8 Dans tous les cas où l'Equipement Electronique édite un Ticket, remettre au titulaire de la Carte l'exemplaire qui lui est destiné sur lequel doit figurer notamment :

- le montant final de la vente/la location dont le montant maximal estimé lui est précisé,
- le numéro de dossier,
- la mention de « ticket provisoire ».

5.2.9 Mode «sans contact»: en cas d'opération en mode « sans contact » permise par l'Equipement Electronique, l'opération de paiement est garantie même si le code confidentiel n'a pas à être vérifié, sous réserve du respect de toutes les autres mesures de sécurité.

5.3 **Après le paiement**

L'Accepteur s'engage à :

5.3.1 Transmettre à la Banque dans les délais et selon les modalités prévus dans les Conditions Particulières, les enregistrements électroniques des opérations, et s'assurer que les opérations de paiement ont bien été portées au crédit du compte dans les délais et selon les modalités prévus dans les Conditions Particulières. Toute opération ayant fait l'objet d'une autorisation transmise par la Banque doit être obligatoirement remise à cette dernière.

5.3.2 Archiver et conserver, à titre de justificatif, pendant la durée requise par les règles du Schéma après la date de l'opération:

- un exemplaire du Ticket comportant, lorsqu'elle est requise, la signature du titulaire de la Carte,
- l'enregistrement électronique représentatif de l'opération ou le journal de fond lui-même.

5.3.3 Communiquer, à la demande de la Banque et dans les délais prévus dans les Conditions Particulières, tout justificatif des opérations de paiement.

5.3.4 L'Accepteur s'engage à ne stocker, sous quelque forme que ce soit, aucune des données de la Carte suivantes:

- le cryptogramme visuel,
- la piste magnétique dans son intégralité,
- le code confidentiel.

Les mesures de sécurité énumérées à l'article 5 ci-dessus pourront être modifiées et complétées pendant toute la durée du présent Contrat, selon la procédure prévue à l'article 8 de la présente partie 1.

ARTICLE 6 - MODALITES ANNEXES DE FONCTIONNEMENT

6.1 Réclamation

Toute réclamation doit être formulée par écrit à la Banque dans un délai maximum de 6 (six) mois à compter de la date de l'opération contestée, sous peine de forclusion.

Ce délai est réduit à une durée de 15 (quinze) jours calendaires à compter de la date de débit en compte d'une opération non garantie.

6.2 Convention de preuve

De convention expresse entre les Parties, les enregistrements électroniques constituent la preuve des opérations de paiement remises à l'Acquéreur. En cas de conflit, les enregistrements électroniques produits par la Banque ou le Schéma dont les règles s'appliquent à l'opération de paiement concernée prévaudront sur ceux produits par l'Accepteur, à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des enregistrements produits par la banque ou le Schéma.

6.3 Retrait à son titulaire d'une Carte faisant l'objet d'un blocage ou en opposition

En cas de retrait à son titulaire d'une Carte faisant l'objet d'un blocage ou en opposition (le retrait ayant eu lieu sur instruction du serveur d'autorisation), l'Accepteur utilise la procédure de gestion et de renvoi des Cartes capturées (disponible sur demande auprès de la Banque).

Pour toute capture de Carte, une prime pourra être versée à l'Accepteur ou à toute personne indiquée par lui et exerçant une activité au sein de son Point d'acceptation.

6.4 Oubli d'une Carte par son titulaire

En cas d'oubli de sa Carte par le titulaire, l'Accepteur peut la lui restituer dans un délai maximum de 2 (deux) jours ouvrables après la date d'oubli de la Carte, sur justification de son identité et après obtention d'un accord demandé selon la procédure communiquée par la Banque. Au-delà de ce délai, l'Accepteur utilise la procédure de gestion et de restitution des Cartes oubliées (disponible sur demande auprès de la Banque).

6.5 « Transaction crédit »

Le remboursement partiel ou total d'un achat d'un bien ou d'un service, d'un don ou d'une cotisation réglé(e) par Carte doit, avec l'accord de son titulaire, être effectué au titulaire de la Carte utilisée pour l'opération initiale.

L'Accepteur doit alors utiliser la procédure dite de « transaction crédit » et, dans le délai prévu dans les conditions convenues avec elle, effectuer la remise correspondante à la Banque à qui il avait remis l'opération initiale. Le montant de la « transaction crédit » ne doit pas dépasser le montant de l'opération initiale.

6.6 Carte non signée

En cas de Carte non signée, et si le panonceau de signature est présent sur la Carte, l'Accepteur doit demander au titulaire de la Carte de justifier de son identité et d'apposer sa signature sur le panonceau de signature prévu à cet effet au verso de la Carte et enfin vérifier la conformité de cette signature avec celle figurant sur la pièce d'identité présentée par le titulaire de la Carte. Si le titulaire de la Carte refuse de signer sa Carte, l'Accepteur doit refuser le paiement par Carte.

6.7 Dysfonctionnement

La Banque et l'Accepteur ne peuvent être tenus pour responsable de l'impossibilité d'effectuer le paiement en cas de dysfonctionnement de la Carte et/ou de son support.

ARTICLE 7 - PAIEMENT « SANS CONTACT »

Cet article s'applique si l'Accepteur utilise un Equipement Electronique disposant de la technologie « sans contact ».

Sauf disposition contraire prévue dans le présent article, l'ensemble des dispositions du présent Contrat sont applicables aux opérations de paiement réalisées avec une Carte équipée de la technologie « sans contact » ou un Instrument de paiement « sans contact.

Lorsque l'Accepteur dispose d'un Equipement Electronique disposant de la technologie dite « sans contact », ledit Equipement Electronique permet le paiement rapide grâce à une lecture à distance de la Carte équipée de la technologie « sans contact » ou de l'Instrument de paiement « sans contact ».

L'Accepteur s'engage à signaler au public l'acceptation du paiement « sans contact » par l'apposition sur l'Equipement Electronique, au niveau du lecteur « sans contact », de façon apparente, d'un pictogramme permettant d'identifier le paiement « sans contact ».

En toutes circonstances, l'Accepteur doit se conformer aux directives qui apparaissent sur l'Equipement Electronique, notamment la frappe du code confidentiel dans les meilleures conditions de confidentialité.

Le montant unitaire maximum de chaque opération de paiement en mode « sans contact » est limité:

- à 20 euros lorsque l'opération de paiement est réalisée par une Carte équipée de la technologie « sans contact ». Au-delà de ce montant unitaire maximum, les conditions de l'opération de paiement telles que prévues dans la présente partie 1 restent inchangées.

Lorsqu'un certain nombre de règlements successifs en mode « sans contact » est atteint, l'Accepteur peut être amené à passer en mode contact même pour une opération d'un montant inférieur au montant unitaire maximum d'une opération en mode « sans contact ».

- à 300 euros lorsque l'opération de paiement est réalisée par un Instrument de paiement « sans contact ». Au-delà de ce montant unitaire maximum, l'opération de paiement « sans contact » ne peut être effectuée.

Lorsque l'opération de paiement est réalisée à l'aide d'un Instrument de paiement « sans contact », les articles 5.2.1, 6.3, 6.4, et 6.6 de la présente partie 1 ne sont pas applicables.

ARTICLE 8 - MODIFICATIONS

8.1 La Banque peut modifier à tout moment les présentes Conditions Générales, les conditions spécifiques ainsi que les Conditions Particulières.

8.2 La Banque peut notamment apporter:

- des modifications techniques telles que l'acceptation de nouvelles Cartes, les modifications de logiciel, le changement de certains paramètres, la remise en état de l'Equipement Electronique suite à un dysfonctionnement, etc.
- des modifications sécuritaires telles que:
  - la modification du seuil de demande d'autorisation,
  - la suppression de l'acceptabilité de certaines Cartes,
  - la suspension de l'acceptation des Cartes portant certaines Marques.

8.3 Les nouvelles conditions entrent généralement en vigueur au terme d'un délai minimum fixé à 1 (un) mois à compter de la notification sur support papier ou sur tout autre support durable.

8.4 Ce délai est exceptionnellement réduit à 5 (cinq) jours calendaires lorsque la Banque ou le Schéma concerné constate, dans le Point d'acceptation, une utilisation anormale de Cartes/d'Instruments de paiement « sans contact » perdu(e)s, volé(e)s ou contrefait(e)s.

8.5 Passés les délais visés au présent article, les modifications sont réputées acceptées par l'Accepteur s'il n'a pas résilié le présent Contrat. Elles lui sont dès lors opposables.

8.6 Le non-respect des nouvelles conditions techniques ou sécuritaires, dans les délais impartis, peut entraîner la résiliation du présent Contrat.

8.7 Sans préjudice des autres stipulations du présent Contrat, tout risque d'exécution excessivement onéreuse du présent Contrat résultant d'un changement des circonstances imprévisibles est assumée par les Parties. Chacune des Parties consent à ne pas se prévaloir des dispositions de l'article 1195 du Code civil. À défaut d'accord entre les parties dans un délai de 8 (huit) jours calendaires à compter de l'entrée en négociation, le présent contrat sera résilié de plein droit.

ARTICLE 9 - DUREE ET RESILIATION DU CONTRAT

9.1 Le présent Contrat est conclu pour une durée indéterminée, sauf dispositions contraires visées dans les Conditions Particulières.

L'Accepteur d'une part, la Banque d'autre part, peuvent, à tout moment, sans justificatif ni préavis (sauf dérogation particulière convenue entre les deux Parties), sous réserve du dénouement des opérations en cours, résilier le présent Contrat, sans qu'il soit nécessaire d'accomplir aucune autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception.

L'Accepteur garde alors la faculté de continuer à accepter les Cartes de tout Schéma avec tout autre acquéreur de son choix.

Lorsque cette résiliation fait suite à un désaccord sur les modifications prévues à l'article 8 ci-dessus, elle ne peut intervenir qu'au-delà du délai prévu dans cet article pour l'entrée en vigueur de ces modifications.

9.2 En outre, à la demande de tout Schéma, la Banque peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à la résiliation du présent Contrat. Elle peut être décidée notamment pour l'une des raisons visées à l'article 10.2 ci-dessous.

Elle est notifiée par lettre recommandée avec demande d'avis de réception et doit être motivée. Son effet est immédiat.

9.3 Toute cessation d'activité de l'Accepteur, cession ou mutation du fonds de commerce, entraîne la résiliation immédiate de plein droit du présent Contrat, sous réserve du dénouement des opérations en cours.

Dans le cas où, après résiliation du présent Contrat, il se révélerait des impayés, ceux-ci seront à la charge de l'Accepteur ou pourront faire l'objet d'une déclaration de créances.

9.4 L'Accepteur sera tenu de restituer à la Banque l'Equipement Electronique, les dispositifs techniques et sécuritaires et les documents en sa possession dont la Banque est propriétaire. Sauf dans le cas où il a conclu un ou plusieurs autres contrats d'acceptation en paiement de proximité pour la location de biens et de services par cartes de paiement, l'Accepteur s'engage à retirer immédiatement de son Point d'acceptation tout signe d'acceptation des Cartes ou Marques des Schémas concernés.

ARTICLE 10 - SUSPENSION DE L'ACCEPTATION

10.1 La Banque peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'acceptation des Cartes/Instrument de paiement « sans contact » portant certaines Marques par l'Accepteur. La suspension est précédée, le cas échéant, d'un avertissement à l'Accepteur, voire d'une réduction de son seuil de demande d'autorisation. Elle est notifiée par tout moyen et doit être motivée. Son effet est immédiat.

Elle peut également intervenir à l'issue d'une procédure d'audit telle que visée à l'article 2.15 de la présente partie 1, au cas où le rapport révélerait un ou plusieurs manquements tant aux clauses du présent Contrat qu'aux exigences du Référentiel Sécuritaire Accepteur annexé au présent Contrat et/ou du Référentiel Sécuritaire PCI/DSS.

10.2 La suspension peut être décidée en raison notamment:

10.2.1 du non-respect répété des obligations du présent Contrat et du refus d'y remédier, notamment d'une utilisation non agréée de l'Equipement Electronique permettant à l'Accepteur d'accéder au Système d'Acceptation et d'un risque de dysfonctionnement important du Système d'Acceptation du Schéma,

10.2.2 d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes/d'Instrument de paiement « sans contact » perdu(e)s, volé(e)s ou contrefait(e)s,

10.2.3 d'un refus d'acceptation répété et non motivé des Cartes et/ou des Catégories de carte du Schéma qu'il a choisi d'accepter ou qu'il doit accepter,

10.2.4 de plaintes répétées d'autres membres ou partenaires d'un Schéma et qui n'ont pu être résolues dans un délai raisonnable,

10.2.5 de retard volontaire ou non motivé de transmission des justificatifs,

10.2.6 d'un risque aggravé en raison des activités de l'Accepteur.

10.3 L'Accepteur s'engage alors à restituer à la Banque l'Equipement Electronique, les dispositifs techniques et sécuritaires et les documents en sa possession dont la Banque est propriétaire, et à retirer immédiatement de son Point d'acceptation tout signe d'acceptation des Cartes du Schéma concerné.

10.4 La période de suspension est au minimum de 6 (six) mois, éventuellement renouvelable. A l'expiration de ce délai, l'Accepteur peut demander la reprise du présent Contrat auprès de la Banque ou souscrire un nouveau contrat d'acceptation en paiement de proximité pour la location de biens et de services par cartes de paiement avec un autre acquéreur de son choix.

ARTICLE 11 - MESURES DE PREVENTION ET DE SANCTION PRISES PAR LA BANQUE

11.1 En cas de manquement de l'Accepteur aux stipulations du présent Contrat ou aux lois en vigueur, ou en cas de constat d'un taux d'impayés anormalement élevé ou d'utilisation anormale de Cartes/d'instruments de paiement « sans contact » perdu(e)s, volé(e)s ou contrefait(e)s, la Banque peut prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement à l'Accepteur valant mise en demeure précisant les mesures à prendre pour remédier au manquement ou résorber le taux d'impayés anormalement élevé constaté.

11.2 Si, dans un délai de 30 (trente) jours, l'Accepteur n'a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté, la Banque peut soit procéder à une suspension de l'acceptation des Cartes dans les conditions précisées à l'article 10 ci-dessus, soit résilier de plein droit avec effet immédiat, sous réserve du dénouement des opérations en cours, le présent Contrat par lettre recommandée avec demande d'avis de réception.

11.3 De même, si dans un délai de 3 (trois) mois à compter de l'avertissement, l'Accepteur est toujours confronté à un taux d'impayés anormalement élevé, la Banque peut décider la résiliation de plein droit avec effet immédiat, sous réserve des opérations en cours, du présent Contrat, notifiée par lettre recommandée avec demande d'avis de réception.

ARTICLE 12 - SECRET BANCAIRE ET PROTECTION DES DONNEES A CARACTERE PERSONNEL

Conformément aux dispositions de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, il est précisé que les données à caractère personnel recueillies aux présentes sont obligatoires pour la conclusion du présent Contrat et son exécution et, qu'à ce titre, elles feront l'objet d'un traitement dont le responsable est la Banque, ce qu'acceptent les personnes sur lesquelles portent lesdites données.

Ces données ainsi que l'ensemble des données à caractère personnel détenues par la Banque dans le cadre des opérations réalisées par les signataires des présentes pourront être utilisées pour les besoins de gestion de ces opérations, d'octroi de crédit, de détection et d'évaluation du risque, de sécurité et de prévention des impayés, de lutte contre la fraude et le blanchiment d'argent, et des actions commerciales de la Banque et des sociétés du Groupe HSBC. Elles pourront être communiquées aux sociétés dudit groupe ou à des tiers, notamment sous-traitants, partenaires, les Schémas visés en partie 2, sociétés pour lesquelles la Banque intervient dans le cadre d'opérations de courtage situés en France ou à l'étranger, notamment dans des Etats n'appartenant pas à l'Union Européenne, pour l'exécution du présent Contrat ou pour répondre aux obligations légales, fiscales ou réglementaires de la Banque.

Dans le cadre d'un transfert vers des pays tiers à l'Union européenne (actuellement l'Inde, la Chine, l'Égypte, la Malaisie, le Sri Lanka, les Philippines ou les États-Unis sont des pays destinataires à des fins de sous-traitance), des règles assurant la protection des données ont été mises en place et peuvent être consultées sur le site www.hsbc.fr. La liste mise à jour des pays destinataires des données est également consultable sur le même site.

Les personnes susvisées consentent à ce que lesdites données soient communiquées dans les conditions décrites ci-dessus et délient la Banque du secret professionnel.

Les personnes sur lesquelles portent les données à caractère personnel ci-dessus recueillies auront le droit d'en obtenir communication auprès de la Banque (Direction Expérience Client et Qualité - 103, avenue des Champs-Elysées - 75008 Paris), d'en exiger, le cas échéant, la rectification, de s'opposer à leur utilisation à des fins de prospection, notamment commerciale.

Les titulaires de Cartes sur lesquels des données à caractère personnel ont été recueillies doivent pouvoir disposer desdits droits de communication, de rectification ou d'opposition auprès de l'Accepteur. A cet égard, l'Accepteur s'engage d'ores et déjà à leur permettre d'exercer ces droits.

ARTICLE 13 - NON RENONCIATION

Le fait pour l'Accepteur ou pour la Banque de ne pas exiger à un moment quelconque l'exécution stricte d'une disposition du présent Contrat ne peut en aucun cas être considéré comme constituant de sa part une renonciation, quelle qu'elle soit, à l'exécution de celle-ci.

ARTICLE 14 - AUTONOMIE DES DISPOSITIONS

Chaque stipulation du présent Contrat est divisible et si une stipulation est ou devient illégale, nulle ou inopposable, l'application de cette stipulation sera alors écartée, toutes les autres stipulations continuant à produire leurs effets.

ARTICLE 15 – IMPREVISION

Sans préjudice des autres stipulations du présent Contrat, tout risque d'exécution excessivement onéreuse du présent Contrat résultant d'un changement des circonstances imprévisibles est assumée par les Parties. Chacune des Parties consent à ne pas se prévaloir des dispositions de l'article 1195 du Code civil. À défaut d'accord entre les parties dans un délai de 8 (huit) jours calendaires à compter de l'entrée en négociation, le présent Contrat sera résilié de plein droit.

ARTICLE 16 - LOI APPLICABLE / TRIBUNEAUX COMPETENTS

Le présent Contrat et toutes les questions qui s'y rapportent seront régis par le droit français et tout différend relatif à l'interprétation, la validité et/ou l'exécution du présent Contrat est soumis à la compétence des Tribunaux français, y compris les procédures tendant à obtenir des mesures d'urgence ou conservatoires, en référé ou sur requête.

ARTICLE 17 - LANGUE DU PRESENT CONTRAT

Le présent Contrat est le contrat original rédigé en langue française qui est le seul qui fait foi.

PARTIE 2

DISPOSITIONS SPECIFIQUES A CHAQUE SCHEMA

DISPOSITIONS SPECIFIQUES AUX SCHEMAS VISA ET MASTERCARD

ARTICLE 1 - FONCTIONNEMENT DES SCHEMAS

Les entités responsables des Schémas Visa et MasterCard sont:
- VISA Inc.et VISA Europe ,
- MasterCard International Inc.

Les Schémas reposent sur l'utilisation des Cartes portant les Marques suivantes:
- Pour VISA Inc. et VISA Europe:
  - Visa
  - VPAY
  - ELECTRON
- Pour MasterCard International Inc.:
  - MasterCard
  - Maestro

ARTICLE 2 - OBLIGATION DE LA BANQUE

Par dérogation à l'article 3.6 de la partie 1, la Banque s'engage à ne pas débiter, au-delà du délai maximum de 24 (vingt-quatre) mois à partir de la date du crédit initial porté au compte de l'Accepteur les opérations de paiement non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

ARTICLE 3 - GARANTIE DE PAIEMENT

Pour les opérations de paiement réalisées à l'aide d'une Carte émis(e) hors de l'EEE, la garantie de paiement n'est pas acquise en cas de contestation du titulaire de la Carte liée à la relation sous-jacente.

DISPOSITIONS SPECIFIQUES AU SCHEMA CB

ARTICLE 1 - DEFINITION DU SCHEMA CB

Le Schéma CB repose sur l'utilisation de Cartes portant la Marque CB (ci-après les « Cartes CB ») auprès des Accepteurs adhérant au Schéma CB dans le cadre des seules dispositions et procédures définies ou homologuées par le Groupement des Cartes Bancaires CB (ci-après le « GIE CB »).

Le GIE CB intervient notamment, pour des raisons sécuritaires, dans les modifications du seuil de demande d'autorisation, la suppression de l'acceptabilité de certaines Cartes CB ou application de paiement CB et la suspension de l'adhésion au Schéma CB. Il établit les conditions du contrat d'adhésion, la banque définissant certaines conditions spécifiques de fonctionnement. Lorsque la Banque représente le GIE CB, le terme de "représentation" ne concerne que l'ensemble des conditions techniques d'acceptation de la Carte CB et de remise des opérations à la Banque, et non la mise en jeu de la garantie du paiement visée à l'article 4 de la partie 1.

ARTICLE 2 - DISPOSITIONS RELATIVES AUX CARTES CB ET SOLUTIONS DE PAIEMENT CB

Sont utilisables dans le Schéma CB et dans le cadre du présent Contrat:
- les Cartes sur lesquelles figure la Marque CB,
- les solutions de paiement CB.

ARTICLE 3 - DISPOSITIONS SUR L'ACCEPTATION DE CARTES CB

En complément des dispositions de la partie 1, l'Accepteur s'engage:

- à accepter les Cartes CB pour le PLBS offerts à sa clientèle et réellement effectués,
- à transmettre les enregistrements des opérations de paiement à la Banque dans les délais prévus dans les Conditions Particulières convenues avec lui. Au-delà d'un délai maximum de 6 (six) mois après la date de l'opération, l'encaissement des opérations de paiement n'est plus réalisable dans le cadre du Schéma CB,
- en cas de demande d'audit par le GIE CB, à permettre à la Banque de faire procéder, aux frais de l'Accepteur, dans les locaux de l'Accepteur ou dans ceux des tiers visés à l'article 2.15 de la partie 1, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI/DSS. Cette vérification, appelée « procédure d'audit », peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée.

  Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquements à ces clauses ou exigences, le GIE CB peut procéder à une suspension de l'adhésion, voire à une radiation du Schéma CB telle que prévue à l'article 4 ci-après.

  L'Accepteur autorise la communication du rapport à la Banque et au GIE CB.

ARTICLE 4 - RECLAMATION

Toute réclamation doit être formulée par écrit à la Banque dans un délai maximum 6 (six) mois à compter de la date de l'opération contestée, sous peine de forclusion.

Ce délai est réduit à une durée 15 (quinze) jours calendaires à compter de la date de débit en compte résultant d'une opération non garantie.

ARTICLE 5 - SUSPENSION DE L'ADHESION ET RADIATION DU SCHEMA CB

5.1 Le GIE CB peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'adhésion au Schéma CB. Elle est précédée, le cas échéant, d'un avertissement à l'Accepteur, voire d'une réduction de son seuil de demande d'autorisation. Cette suspension est notifiée par tout moyen. Son effet est immédiat.

Elle peut être décidée en raison notamment:

- d'une utilisation anormale de Cartes/d'instruments de paiement « sans contact » perdu(e)s, volé(e)s ou contrefait(e)s,
- d'une utilisation d'un Equipement Electronique non agréé,
- d'un risque de dysfonctionnement important du Schéma CB.

5.2 L'Accepteur s'engage alors à restituer à l'Acquéreur l'Equipement Electronique, les dispositifs techniques et sécuritaires et les documents en sa possession dont la Banque est propriétaire, et à retirer immédiatement de son Point d'acceptation tout signe d'acceptation des Cartes CB.

5.3 La période de suspension est au minimum de 6 (six) mois, éventuellement renouvelable.

5.4 A l'expiration de ce délai, l'Accepteur peut, sous réserve de l'accord préalable du GIE CB, demander la reprise d'effet du présent Contrat auprès de la Banque, ou souscrire un nouveau contrat d'acceptation en paiement de proximité pour la location de biens et de services par cartes de paiement avec un autre acquéreur de son choix.

Cette reprise d'effet ou cette nouvelle d'adhésion pourra être subordonnée à la mise en œuvre de recommandations d'un auditeur désigné par le GIE CB ou la Banque.

5.5 En cas de comportement frauduleux de la part de l'Accepteur, il peut être immédiatement radié du Schéma CB ou la suspension être convertie en radiation.

Les exigences présentées ci-après constituent le référentiel sécuritaire de la Banque qui doit être respecté à tout moment par l'Accepteur.

Exigence 1 (E1) - Gérer la sécurité du système commercial et de paiement au sein de l'entreprise

Pour assurer la sécurité des données des transactions et notamment, des données du porteur de Carte, une organisation, des procédures et des responsabilités doivent être établies par l'Accepteur.

En particulier, un responsable de la sécurité du système commercial et de paiement doit être désigné. Il est chargé, entre autres, d'appliquer la législation sur la protection des données à caractère personnel et des données bancaires dans le cadre de leur utilisation et de leur environnement.

Les détenteurs de droits d'usage des informations et du système doivent être identifiés et sont responsables de l'attribution des droits d'accès au système.

Le contrôle du respect des exigences de sécurité relatives au système commercial et de paiement doit être assuré.
Une organisation chargée du traitement des incidents de sécurité, de leur suivi et de leur historisation doit être établie.

Exigence 2 (E2) - Gérer l'activité humaine et interne

Les obligations et les responsabilités du personnel de l'Accepteur quant à l'utilisation des données bancaires et confidentielles, à leur stockage et à leur circulation en interne ou à l'extérieur doivent être établies.

Il en est de même pour l'utilisation des postes de travail et du réseau interne comme du réseau Internet.

Les obligations et les responsabilités du personnel de l'Accepteur quant à la protection des données bancaires et confidentielles doivent être établies. L'ensemble de ces règles doit s'appliquer à tous les personnels impliqués : salariés de l'entreprise et tiers.

Les personnels de l'Accepteur doivent être sensibilisés aux risques encourus, notamment sur la divulgation d'informations confidentielles, l'accès non autorisé aux informations, aux supports et aux documents. Ils doivent être régulièrement sensibilisés aux risques particuliers liés à l'usage des moyens informatiques (postes de travail en réseau, serveurs, accès depuis ou vers Internet) et notamment, à l'introduction de virus.

Il convient que les personnels de l'Accepteur reçoivent une formation appropriée sur l'utilisation correcte du système d'exploitation et du système applicatif commercial et de paiement.

Exigence 3 (E3) - Gérer les accès aux locaux et aux informations

Tout dispositif (équipement réseau, serveur, ...) qui stocke ou qui traite des données relatives à une transaction, et notamment des données du porteur de la Carte, doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les recommandations de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Les petits matériels ou supports informatiques sensibles doivent être rendus inaccessibles à des tiers en période de non utilisation. Notamment, les cartouches de sauvegarde doivent être stockées dans un coffre.

Dans le cas où ces petits matériels ou supports informatiques sensibles ne sont plus opérationnels, ils doivent être obligatoirement détruits et la preuve de leur destruction doit être établie.

La politique d'accès aux locaux sensibles doit être formalisée et les procédures doivent être établies et contrôlées.

Exigence 4 (E4) - Assurer la protection logique du système commercial et de paiement

Les règles de sécurité relatives aux accès et sorties depuis et vers le système commercial et de paiement doivent être établies et leur respect doit être contrôlé.

Seul le serveur supportant l'application commerciale doit être accessible par les internautes.

Le serveur de base de données client ainsi que le serveur hébergeant le système de paiement ne doivent être accessibles que par le serveur commercial front-office et seulement par l'intermédiaire d'un pare-feu.

Les accès internes des utilisateurs comme des administrateurs à ces mêmes serveurs doivent se faire par l'intermédiaire du pare-feu. L'architecture réseau doit être organisée de manière à ce que les règles de sécurité définies soient mises en oeuvre et contrôlées. Le pare-feu doit être mis à jour systématiquement lorsque des vulnérabilités sont identifiées sur ses logiciels (logiciel pare-feu et logiciel d'exploitation) et corrigeables.

Le serveur supportant le pare-feu doit être doté d'un outil de contrôle de l'intégrité.

Le pare-feu doit assurer l'enregistrement des accès et des tentatives d'accès dans un journal d'audit. Celui-ci doit être analysé quotidiennement.

Exigence 5 (E5) - Contrôler l'accès au système commercial et de paiement

Le principe d'autorisation d'utilisation du système doit être défini et reposer sur la notion d'accès des classes d'utilisateurs aux classes de ressources définition des profils d'utilisateurs et des droits accordés.

Les responsabilités et rôles quant à l'attribution, l'utilisation et le contrôle doivent être identifiés. Notamment, les profils, les droits et les privilèges associés doivent être validés par les propriétaires des informations et du système commercial et de paiement.

Les droits des utilisateurs et des administrateurs ainsi que de leurs privilèges, doivent être gérés et mis à jour conformément à la politique de gestion des droits.

Exigence 6 (E6) - Gérer les accès autorisés au système commercial et de paiement

Aucune ouverture de droits ne peut se faire en dehors des procédures d'autorisation adéquates. Les autorisations données doivent être archivées et contrôlées régulièrement.

Outre les accès clients, tout accès au système commercial et de paiement doit se faire sur la base d'une identification et d'une authentification.
L'identification doit être nominative y compris pour les administrateurs et les personnels de maintenance. Les droits accordés à ceux-ci doivent être restreints aux opérations qui leur sont autorisées.

L'utilisation de codes d'identification attribués à des groupes ou des fonctions (process techniques comme l'alimentation automatique des signatures antivirales) n'est autorisée que si elle est appropriée au travail effectué.

Les changements de situation (changement de poste, départ...) des personnels doivent systématiquement entraîner un contrôle des droits d'accès attribués.

La suppression des droits d'accès doit être immédiate en cas de départ d'une personne.

Le contrôle d'accès doit être assuré au niveau réseau par le pare-feu, au niveau système par les systèmes d'exploitation des machines accédées et au niveau applicatif par le logiciel applicatif et par le gestionnaire de base de données.

Les tentatives d'accès doivent être limitées en nombre. Les mots de passe doivent être changés régulièrement.

Les mots de passe doivent comporter au minimum 8 caractères dont des caractères spéciaux.

Exigence 7 (E7) - Surveiller les accès au système commercial et de paiement

Les accès et tentatives d'accès au système doivent être enregistrés dans des journaux d'audit.

L'enregistrement doit comporter au minimum la date et l'heure de l'accès (ou tentative) et l'identification de l'acteur et de la machine.

Les opérations privilégiées comme la modification des configurations, la modification des règles de sécurité, l'utilisation d'un compte administrateur doivent également être enregistrées.

Les systèmes assurant l'enregistrement doivent au minimum être le pare-feu, le système supportant la base de données clients ainsi que celui supportant la base de données paiements.

Les journaux d'audit doivent être protégés contre des risques de désactivation, modification ou suppression non autorisées.

Les responsabilités et rôles quant à l'audit des données enregistrées sont identifiés. Celui-ci doit être effectué quotidiennement.

Exigence 8 (E8) - Contrôler l'introduction de logiciels pernicieux

Les procédures et les responsabilités de gestion ayant trait à la protection anti-virus et à la restauration des données et des logiciels en cas d'attaque par virus doivent être définies et formalisées.

L'installation et la mise à jour régulière des logiciels de détection et d'élimination des virus doivent être effectuées sur la totalité des machines ayant accès au système commercial et de paiement.

La vérification anti-virus doit être exécutée quotidiennement sur la totalité des machines.

Exigence 9 (E9) - Appliquer les correctifs de sécurité (patches de sécurité) sur les logiciels d'exploitation

Les correctifs de sécurité doivent être systématiquement appliqués sur les équipements de sécurité et les serveurs applicatifs frontaux pour fixer le code lorsque des vulnérabilités pourraient permettre des accès non autorisés et non visibles.

Ces correctifs doivent être appliqués sur la base d'une procédure formelle et contrôlée.

Exigence 10 (El0) - Gérer les changements de version des logiciels d'exploitation

Une procédure d'installation d'une nouvelle version doit être établie et contrôlée.

Cette procédure doit prévoir entre autres, des tests de non régression du système et un retour arrière en cas de dysfonctionnement.

Exigence 11 (E11) - Maintenir l'intégrité des logiciels applicatifs relatifs au système commercial et de paiement

Il convient d'établir les responsabilités et les procédures concernant les modifications opérationnelles touchant aux applications.

Les modifications apportées aux logiciels applicatifs doivent faire l'objet d'une définition précise.

La demande de modification doit être approuvée par le responsable fonctionnel du système.

Les nouvelles versions de logiciels applicatifs doivent être systématiquement soumises à recette et approuvées par le responsable fonctionnel de l'application concernée avant toute mise en production.

Exigence 12 (E12) - Assurer la traçabilité des opérations techniques (administration et maintenance)

Les opérations techniques effectuées doivent être enregistrées de manière chronologique, dans un cahier de bord pour permettre la reconstruction, la revue et l'analyse en temps voulu des séquences de traitement et des autres activités liées à ces opérations.

Exigence 13 (E13) - Maintenir l'intégrité des informations relatives au système commercial et de paiement

La protection et l'intégrité des éléments de la transaction doivent être assurés ainsi lors de leur stockage et lors de leur routage sur les réseaux (internes ou externes). Il en est de même pour les éléments secrets servant à chiffrer ces éléments.

Le dossier de sécurité propre au système commercial et de paiement doit décrire les moyens mis en place pour répondre à cette exigence.

Exigence 14 (E14) - Protéger la confidentialité des données bancaires

Les données du porteur de Carte ne peuvent être utilisées que pour exécuter l'ordre de paiement et les réclamations.

Le cryptogramme visuel d'un porteur de Carte ne doit en aucun cas être stocké par le commerçant.

Les données bancaires et à caractère personnel relatives à une transaction, et notamment les données du porteur de Carte, doivent être protégées lors de leur stockage et lors de leur routage sur les réseaux internes et externes au site d'hébergement conformément aux recommandations de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Il en est de même pour l'authentifiant du commerçant et les éléments secrets servant à chiffrer.

Le dossier de sécurité propre au système commercial et de paiement doit décrire les moyens mis en place pour répondre à cette exigence.

Exigence 15 (E15) - Protéger la confidentialité des identifiants/authentifiants des utilisateurs et des administrateurs

La confidentialité des identifiants - authentifiants doit être protégée lors de leur stockage et de leur circulation.

Il convient de s'assurer que les données d'authentification des administrateurs ne puissent être réutilisées.

Dans le cadre d'une intervention extérieure pour maintenance, les mots de passe utilisés doivent être systématiquement changés à la suite de l'intervention.