

ADHÉSION AU SYSTÈME DE PAIEMENT PAR CARTE BANCAIRE SUR AUTOMATE EN LIBRE-SERVICE (ALS)



CONDITIONS GÉNÉRALES

Conditions Générales d'adhésion au système de paiement par carte Bancaire sur Automate Libre-Service.

ARTICLE PRELIMINAIRE

1) L'Accepteur "CB" peut être tout commerçant, tout prestataire de services, toute personne exerçant une profession libérale, susceptible d'utiliser le Système "CB", et d'une manière générale tout professionnel vendant ou louant des biens ou des prestations de services.

L'Accepteur "CB" 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 GIE "CB" ou Entité de Groupe au sens des Statuts du GIE "CB" et avec lequel il a passé un contrat d'acceptation.

2) Par "Acquéreur "CB" il faut entendre tout établissement de crédit ou de paiement, Membre du GIE "CB" ou Entité de Groupe au sens des Statuts du GIE "CB", avec lequel l'Accepteur "CB" a signé un contrat d'acceptation, et cela quel que soit son statut, (banque, etc....).

3) Par "Équipement Électronique", il faut entendre tout dispositif de paiement qui comporte un système permettant le contrôle du code confidentiel, placé sous la maîtrise d'un Accepteur "CB", permettant à celui-ci d'accepter les paiements par Carte. Actuellement, ce contrôle est opérationnel avec les cartes portant la marque "CB" et certaines cartes portant la marque Visa ou MasterCard. Toute extension de l'application de ce contrôle à d'autres cartes sera notifiée par l'Acquéreur "CB" à l'Accepteur "CB", conformément à l'article 9 des présentes Conditions Générales.

4) Par "Automate de paiement en libre-service", il faut entendre tout Équipement Électronique agréé par le GIE "CB", permettant la distribution automatique de biens et services, acceptant le paiement par Carte en libre-service, impliquant la présence du Titulaire de la Carte au point d'acceptation et sans intervention directe de l'Accepteur "CB".

L'agrément est une attestation de conformité avec des spécifications techniques et fonctionnelles définies par le GIE "CB", qui dispose de la liste des Équipements Électroniques agréés et qui peut la communiquer à l'Accepteur "CB" sur sa demande.

Les Automates de paiement en libre-service sont désignés ci-après par le terme générique "Automate".

ARTICLE 1 : DEFINITION DU SYSTÈME

Le système de paiement par Carte "CB" repose sur l'utilisation de Cartes "CB" ou agréées "CB" pour le paiement d'achats de biens ou de prestations de services auprès des Accepteurs adhérant au Système "CB" et cela dans le cadre des seules dispositions et procédures définies ou homologuées par 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 de Cartes agréées "CB" et la suspension de l'adhésion au Système "CB". Il établit les Conditions Générales du contrat d'adhésion, l'Acquéreur "CB" définissant certaines Conditions Particulières de fonctionnement.

Lorsque l'Acquéreur "CB" représente le GIE "CB", le terme de "représentation" ne concerne que l'ensemble des conditions techniques d'acceptation de la Carte "CB" et de Cartes agréées "CB" et de remise des opérations à l'Acquéreur "CB", et non la mise en jeu de la garantie du paiement visée à l'article 5 des présentes Conditions Générales.

ARTICLE 2 : DISPOSITIONS RELATIVES AUX CARTES

Sont utilisables dans le Système "CB":

- les cartes sur lesquelles figure la marque "CB"

- les cartes agréées "CB" c'est-à-dire :

- cartes portant uniquement les marques Visa ou MasterCard dont l'acceptation dans le Système "CB" a été agréée par le GIE "CB",
- cartes émises dans le cadre de réseaux étrangers ou internationaux homologuées par le GIE "CB" et dont l'Accepteur

"CB" peut obtenir les signes de reconnaissance auprès de l'Acquéreur "CB".

L'ensemble de ces cartes précitées est désigné ci-après par le terme générique de "Carte".

ARTICLE 3 : OBLIGATIONS DE L'ACCEPTEUR "CB"

L'Accepteur "CB" s'engage:

3.1 - Signaler au public l'acceptation des Cartes par l'apposition de façon apparente sur l'Automate des panonceaux, vitrophanies et enseignes qui lui seront fournis par l'Acquéreur "CB".

3.2 - Afficher visiblement le montant maximum de 1500 euros au-delà duquel aucune opération ne peut être réalisée ainsi que le montant minimum éventuel à partir duquel la Carte est acceptée afin que les Titulaires de la Carte en soient préalablement informés. Ce montant minimum doit être raisonnable et ne pas être un frein à l'acceptation des Cartes.

3.3 - Informer clairement les clients des procédures et conditions avec lesquelles ils peuvent utiliser leur Carte pour le règlement de leurs achats de biens ou de prestations de services via l'Automate.

3.4 - S'identifier clairement par le numéro SIRET et le code activité (NAF/APE) que l'INSEE lui a attribués. Si l'Accepteur "CB" n'est pas immatriculable, il doit utiliser un numéro d'identification spécifique, fourni par l'Acquéreur "CB", lui permettant l'accès au Système "CB".

3.5 - 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 l'Acquéreur "CB" la conformité des informations transmises pour identifier son point de vente, les informations doivent indiquer une dénomination commerciale connue des Titulaires de Cartes et permettre de dissocier le mode de paiement sur Automate par rapport aux autres modes de paiement (vente à distance et vente en présence physique de l'Accepteur "CB") dans ce point de vente.

3.6 - Recevoir des paiements en contrepartie d'actes de vente ou de fournitures de prestations de services offerts à sa clientèle et qu'il fournit ou réalise lui-même avec l'Automate.

3.7 - Accepter les Cartes telles que définies à l'article 2 ci-dessus pour le paiement d'achats de biens ou de prestations de services offerts à sa clientèle et réellement effectués (à l'exclusion de toute délivrance d'espèces ou de tout titre convertible en espèces pour leur valeur faciale).

3.8 - Transmettre les enregistrements des opérations de paiement à l'Acquéreur "CB", dans le délai prévu dans les Conditions Particulières convenues avec lui. Au-delà d'un délai maximum de 6 mois après la date de l'opération, l'encaissement des opérations de paiement n'est plus réalisable dans le cadre du Système "CB".

3.9 - Faire son affaire personnelle des litiges commerciaux et de leurs conséquences financières pouvant survenir avec des clients et concernant des biens et services dont l'achat a été réglé par Carte au titre du présent Contrat.

3.10 - Régler, selon les Conditions Particulières convenues avec l'Acquéreur "CB", les commissions, frais et d'une manière générale, toute somme due au titre de l'adhésion et du fonctionnement du Système "CB".

3.11 - Utiliser obligatoirement l'Automate tel que défini par l'article Préliminaire ci-dessus et agréé par le GIE "CB". Ne pas modifier les paramètres de son fonctionnement et ne pas y installer de nouvelles applications notamment en acceptant l'intervention de tiers, sans avoir au préalable obtenu l'autorisation de l'Acquéreur "CB".

3.12 - Prendre toutes les mesures propres à assurer la garde de son Automate et être vigilant quant à l'utilisation qui en est faite.

3.13 - Permettre à l'Acquéreur "CB" et au GIE "CB" de faire procéder aux frais de l'Accepteur "CB" dans ses locaux ou ceux de ses prestataires, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences du Référentiel Sécuritaire Accepteur figurant en annexe.

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 Système "CB" tel que prévu à l'article 11.

L'Accepteur "CB" autorise la communication du rapport à l'Acquéreur "CB", au GIE "CB" et aux réseaux étrangers ou internationaux mentionnés sur les Cartes acceptées par l'Accepteur "CB" et définies à l'article 2.

3.14 - 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 le référentiel de sécurité PCI DSS et acceptent que les audits visés à l'article 3.13 soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé dans cet article.

3.15 - Respecter les exigences du Référentiel Sécuritaire Accepteur PCI DSS figurant en annexe du présent Contrat.

ARTICLE 4 : OBLIGATIONS DE L'ACQUÉREUR "CB"

L'Acquéreur "CB" s'engage à :

4.1 - Fournir à l'Accepteur "CB" les informations le concernant directement sur le fonctionnement du Système "CB" et son évolution.

4.2 - Mettre à la disposition de l'Accepteur "CB", selon les Conditions Particulières convenues avec lui, les informations relatives à la sécurité des opérations de paiement, notamment l'accès au serveur d'autorisation.

4.3 - Indiquer à l'Accepteur "CB" la liste et les caractéristiques des Cartes pouvant être acceptées au titre du présent Contrat.

4.4 - Créditer le compte de l'Accepteur "CB" des sommes qui lui sont dues, selon les Conditions Particulières convenues avec lui.

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

4.6 - Communiquer, à la demande de l'Accepteur "CB", les éléments essentiels des procédures administratives annexes, notamment :

- gestion et renvoi des Cartes capturées par l'Accepteur "CB",
- gestion et restitution des Cartes oubliées par leurs Titulaires.

ARTICLE 5 : GARANTIE DU PAIEMENT

5.1 - Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées aux articles 6 et 7 des présentes Conditions Générales, ainsi qu'aux Conditions Particulières.

5.2 - 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.

5.3 - En cas de non-respect d'une seule de ces mesures, les enregistrements ne sont réglés que sous réserve de bonne fin d'encaissement.

ARTICLE 6 : MESURES DE SECURITE A LA CHARGE DIRECTE DE L'ACCEPTEUR "CB"

6.1 - L'Automate doit être clairement identifié par un numéro d'identification spécifique fourni par l'Acquéreur « CB » lui permettant l'accès au Système "CB".

6.2 - L'Accepteur "CB" doit suivre les procédures dont les modalités techniques lui ont été indiquées et informer immédiatement l'Acquéreur "CB" en cas de fonctionnement anormal de l'Automate, et pour toutes autres anomalies (absence de reçu ou de mise à jour de la liste noire, impossibilité de réparer rapidement, etc.).

6.3 - L'Accepteur "CB" doit fréquemment procéder à une inspection visuelle externe approfondie de l'Automate afin

de détecter l'éventuelle présence de matériels de capture de données placés à l'extérieur de ceux-ci.

En cas de présence anormale d'un matériel, l'Accepteur "CB"

doit le signaler immédiatement à l'Acquéreur "CB".

LORS DU PAIEMENT

L'Accepteur "CB" s'engage à :

6.4 - Utiliser l'Automate, respecter ou faire respecter les indications techniques affichées sur son écran et suivre les procédures dont les modalités techniques lui ont été indiquées.

APRES LE PAIEMENT

6.5 - L'Accepteur "CB" s'engage à :

6.5.1 - Transmettre à l'Acquéreur "CB", dans les délais et selon les modalités prévus dans les Conditions Particulières convenues avec l'Acquéreur "CB", les enregistrements électroniques des opérations, et s'assurer qu'ils ont bien été portés au crédit du compte dans les délais et selon les modalités prévus dans les Conditions Particulières convenues avec l'Acquéreur "CB".

Toute opération ayant fait l'objet d'une autorisation transmise par l'Acquéreur "CB" signataire du présent Contrat doit être obligatoirement remise à ce dernier.

6.5.2 - Archiver et conserver, à titre de justificatif, pendant 15 mois après la date de l'opération, l'enregistrement magnétique représentatif de chaque opération comprenant l'image du ticket fourni par l'Automate et notamment les numéros de certificat et s'il y a lieu d'autorisation ainsi que les éléments servant à leur calcul.

6.6 - Communiquer, à la demande de l'Acquéreur "CB" et dans le délai prévu dans les Conditions Particulières convenues avec lui, tout justificatif des opérations de paiement.

ARTICLE 7 : MESURES DE SECURITE A LA CHARGE DE L'ACCEPTEUR "CB" ET ASSUREES DIRECTEMENT PAR L'AUTOMATE

L'Automate doit notamment, après lecture de la puce de la Carte, assurer automatiquement les opérations suivantes :

7.1 Interdire une opération de plus de 1500 euros.

7.2 Afficher le montant réel de l'opération dès que l'Automate peut le définir ou l'estimer et, au plus tard, à la délivrance complète du bien ou du service.

7.3 Contrôler la validité de la Carte, c'est à dire :
- La technologie de la Carte.

Traiter la puce et, en cas d'impossibilité de traitement de la puce ou en cas d'absence de puce, l'Automate doit traiter l'opération selon les règles édictées par l'Acquéreur "CB", notamment abandonner l'opération :

- pour une Carte MasterCard, lorsque le montant de l'opération est supérieur à 40\$ ou 50 euros et que l'Automate ne permet pas de mettre en œuvre une identification du Titulaire de la Carte par l'Émetteur conforme aux règles de l'Émetteur,
- pour une Carte Visa, lorsque le montant de l'opération est supérieur à 40\$ ou l'équivalent en

monnaie locale et que l'Automate ne permet pas de mettre en œuvre une identification du Titulaire de la Carte par l'Émetteur conforme aux règles de l'Émetteur.

7.3.1 En cas d'opération en mode sans contact permise par l'Équipement Électronique sur l'Automate, l'opération de paiement est garantie même si le code confidentiel n'est pas vérifié, sous réserve du respect de l'ensemble des autres mesures de sécurité à la charge de l'Accepteur "CB".

7.4 - Pour les Cartes "CB" et les Cartes agréées "CB", lorsque la Carte le demande, mettre en œuvre le contrôle du code confidentiel de la Carte. La preuve de ce contrôle est apportée par le certificat qui doit être enregistré par l'Automate et imprimé sur le Ticket.

7.5 - Obtenir une autorisation au moment de l'opération et pour un montant défini dans les Conditions Particulières :

- lorsque le montant de l'opération en cause ou le montant cumulé des opérations réglées au moyen de la même Carte, dans la même journée pour le même point de vente et pour le même type de paiement (Automate), dépasse celui du seuil de demande d'autorisation fixé dans les Conditions Particulières convenues avec l'Acquéreur "CB", et ceci, quelle que soit la méthode d'acquisition des informations,
- lorsque l'Automate ou la Carte à puce déclenche une demande d'autorisation, indépendamment du seuil de demande d'autorisation de l'Automate fixé dans les Conditions Particulières convenues avec l'Acquéreur "CB".

À défaut, l'opération ne sera pas garantie, même pour la fraction autorisée ou correspondant au montant du seuil de demande d'autorisation.

Une opération interdite, refusée ou interrompue par le serveur d'autorisation doit être abandonnée par l'Automate

7.6 Proposer au client l'émission d'un Ticket. Si l'Automate ne peut pas délivrer temporairement de Ticket, il doit en informer le client avant l'opération et lui proposer d'arrêter l'opération.

7.7 Stocker les enregistrements des opérations, identifiées comme opérations par l'Automate, effectuées au point de vente en vue de leur remise à l'Acquéreur "CB".

ARTICLE 8 : MODALITES ANNEXES DE FONCTIONNEMENT

8.1 – Réclamation

Toute réclamation doit être justifiée et formulée par écrit à l'Acquéreur "CB", dans un délai maximum de 6 mois à compter de la date de l'opération contestée, sous peine de forclusion.

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

8.2 - Convention de preuve

De convention expresse entre les parties, les enregistrements électroniques constituent la preuve des opérations de paiement remises à l'Acquéreur "CB". En cas de conflit, les enregistrements électroniques produits

par l'Acquéreur "CB" ou le GIE "CB" prévaudront sur ceux produits par l'Accepteur "CB", à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des documents produits par l'Acquéreur "CB" ou le GIE "CB".

8.3 - Retrait à son Titulaire de la 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 notamment sur instruction du serveur d'autorisation, en raison de la présence de la Carte sur la liste des Cartes faisant l'objet d'un blocage ou en opposition et/ou contrefaites), l'Accepteur "CB" utilise la procédure de gestion et de renvoi des Cartes capturées.

Pour toute capture de Carte faisant l'objet d'un blocage ou en opposition et/ou contrefaite et sur instruction de l'Équipement Électronique, une prime sera versée à l'Accepteur "CB" ou à toute personne indiquée par lui et exerçant une activité au sein de son établissement.

8.4 - Oubli d'une Carte par son Titulaire

En cas d'oubli de sa Carte par le Titulaire, l'Accepteur "CB" peut la lui restituer dans un délai maximum de deux jours ouvrés 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 l'Acquéreur "CB". Au-delà de ce délai, l'Accepteur "CB" utilise la procédure de gestion et de restitution des Cartes oubliées.

ARTICLE 9 : MODIFICATIONS

9.1 - L'Acquéreur "CB" peut modifier à tout moment les présentes Conditions Générales ainsi que les Conditions Particulières.

9.2 L'Acquéreur "CB" 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'Équipement Électronique et de l'Automate 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'adhésion au Système "CB".

9.3 - Les nouvelles conditions entrent généralement en vigueur au terme d'un délai minimum fixé à un mois à compter de l'envoi d'une lettre d'information ou de notification.

9.4 - Ce délai est exceptionnellement réduit à cinq jours calendaires lorsque l'Acquéreur "CB" ou le GIE "CB" constate, dans le point de vente ou sur l'Automate, une utilisation anormale de Cartes perdues, volées ou contrefaites.

9.5 - Passés les délais visés au présent article, les modifications sont opposables à l'Accepteur "CB" s'il n'a pas résilié le présent Contrat.

9.6 - Le non-respect des nouvelles conditions techniques ou sécuritaires, dans les délais impartis, peut entraîner la résiliation du présent Contrat, voire la suspension par le GIE "CB" de l'adhésion au Système "CB" dans les conditions prévues à l'article 11 du présent Contrat.

ARTICLE 10 : DUREE ET RESILIATION DU CONTRAT

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

L'Accepteur "CB" d'une part, l'Acquéreur "CB" 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, mettre fin au 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 "CB" garde alors la faculté de continuer à adhérer au Système "CB" avec tout autre Acquéreur "CB" de son choix.

Lorsque cette résiliation fait suite à un désaccord sur les modifications prévues à l'article 9 ci-dessus, elle ne peut intervenir qu'au-delà du délai prévu dans cet article pour l'entrée en vigueur de ces modifications.

10.2 - Toute cessation d'activité de l'Accepteur "CB", 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 "CB" ou pourront faire l'objet d'une déclaration de créances.

10.3 - L'Accepteur "CB" sera tenu de restituer à l'Acquéreur "CB" l'Équipement Électronique, les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur "CB" est propriétaire.

Sauf dans le cas où il a conclu un ou plusieurs autres contrats d'adhésion, l'Accepteur "CB" s'engage à retirer immédiatement de son établissement tout signe d'acceptation des Cartes.

ARTICLE 11 : SUSPENSION DE L'ADHESION ET RADIATION DU SYSTEME "CB"

11.1 - 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 Système "CB". Elle est précédée, le cas échéant, d'un avertissement à l'Accepteur "CB", voire d'une réduction de son seuil de demande d'autorisation. Cette suspension est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception. Son effet est immédiat. Elle peut être décidée en raison notamment :

- d'une utilisation anormale de Cartes perdues, volées ou contrefaites,
- d'une utilisation d'un Automate non agréé,
- d'un risque de dysfonctionnement important du Système "CB".

11.2 - L'Accepteur "CB" s'engage alors à restituer à l'Acquéreur "CB" l'Équipement Électronique, les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur "CB" est propriétaire et à retirer immédiatement de son établissement tout signe d'acceptation des Cartes.

11.3 - La période de suspension est au minimum de 6 mois, éventuellement renouvelable.

11.4 - A l'expiration de ce délai, l'Accepteur "CB" peut, sous réserve de l'accord préalable du GIE "CB", demander la reprise d'effet de son contrat auprès de l'Acquéreur

"CB", ou souscrire un nouveau contrat d'adhésion avec un autre Acquéreur "CB" de son choix.

11.5 - En cas de comportement frauduleux de la part de l'Accepteur "CB" responsable du point de vente, l'Accepteur "CB" peut être immédiatement radié ou la suspension être convertie en radiation.

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

Lors de la signature ou de l'exécution des présentes, chacune des parties peut avoir accès à des données à caractère personnel ou couvertes par le secret bancaire.

Ainsi, en application des articles 32, 38, 39 et 40 de la loi du 6 janvier 1978 relative à la loi "Informatique et Libertés" modifiée par la loi du 6 août 2004, il est précisé que :

12.1 - Les informations relatives à l'Accepteur "CB", collectées par l'Acquéreur "CB" nécessaires pour l'exécution des ordres de paiement transmis et leur sécurisation, ne seront utilisées et ne feront l'objet de diffusion auprès d'entités tierces que pour les seules finalités de traitement des opérations de paiement par Carte, données en exécution du présent Contrat, ou pour répondre aux obligations légales et réglementaires, l'Acquéreur "CB" étant à cet effet, de convention expresse, délié du secret bancaire.

L'Accepteur "CB", personne physique, ou la personne physique le représentant ou sur laquelle portent les données à caractère personnel ci-dessus recueillies, a le droit d'en obtenir communication, et le cas échéant, d'en exiger la rectification et de s'opposer, pour des motifs légitimes, à ce qu'elles fassent l'objet d'un traitement ou à leur utilisation à d'autres fins que celles citées ci-dessus, auprès de l'Acquéreur "CB".

12.2 - A l'occasion de l'exécution des ordres de paiement donnés par Carte, l'Accepteur "CB" peut avoir accès à différentes données à caractère personnel concernant notamment les Titulaires de la Carte.

L'Accepteur "CB" ne peut utiliser ces données à caractère personnel que pour l'exécution des ordres de paiement par Carte et le traitement des réclamations dont ils peuvent être l'objet. Sauf obligations légales et réglementaires, il ne peut ni les céder, ni en faire un quelconque usage qui ne soit pas directement visé par le présent Contrat. Il s'assure également de l'existence et de la mise en œuvre de dispositifs de protection et de contrôle des accès physiques et logiques à ces données.

Les Titulaires de Cartes sur lesquels des données à caractère personnel ont été recueillies doivent pouvoir disposer des droits d'accès, de rectification et d'opposition auprès de l'Accepteur "CB". À cet égard, l'Accepteur "CB" s'engage d'ores et déjà à leur permettre d'exercer ces droits.

ARTICLE 13 : NON RENONCIATION

Le fait pour l'Accepteur "CB" ou pour l'Acquéreur "CB" 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 : LOI APPLICABLE/TRIBUNAUX 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 15 : LANGUE DU PRESENT CONTRAT

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

ADDENDUM RELATIF AUX CONDITIONS D'UTILISATION DES EQUIPEMENTS ELECTRONIQUES UTILISANT LA TECHNOLOGIE SANS CONTACT DANS LE CADRE DU PAIEMENT PAR CARTE SANS CONTACT

Lorsque l'Acquéreur "CB" met à la disposition de l'Accepteur "CB" un Équipement Électronique disposant de la technologie dite "Carte sans contact" dont les conditions de fonctionnement sont régies par le présent addendum et par les Conditions Générales et Particulières du Contrat d'acceptation en paiement sur Automate en libre-service, sous réserve des modifications prévues ci-après.

Il est expressément convenu entre l'Accepteur "CB" et l'Acquéreur "CB" que :

Article 1 : Cet Équipement Électronique disposant de la technologie "Carte sans contact" permet le règlement rapide d'achats de biens ou de prestations de services par des Titulaires de Cartes avec une lecture à distance de la Carte et sans frappe du code confidentiel.

Article 2 : En toutes circonstances, l'Accepteur "CB" doit se conformer aux directives qui apparaissent sur cet Équipement Électronique.

Article 3 : Le montant unitaire maximum de chaque opération de paiement en mode "Carte sans contact" est limité à **20 euros**.

Au-delà de ce montant unitaire maximum, les conditions de l'opération de paiement telles que prévues dans les Conditions Générales du Contrat modifié par le présent addendum, restent inchangées.

Lorsqu'un certain nombre de règlements successifs en mode sans contact est atteint, l'Accepteur "CB" 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 "Carte sans contact".

Article 4 : En conséquence, il est ajouté au présent contrat d'acceptation en paiement sur Automate un article qui prévoit ce qui suit :

7.3.1 En cas d'opération en mode "sans contact" permise par l'Automate, l'opération de paiement est garantie même si le code confidentiel n'est pas vérifié, sous réserve du respect de l'ensemble des autres mesures de sécurité à la charge de l'Accepteur "CB".

Article 5 : L'ensemble des autres dispositions du Contrat d'acceptation sur Automate en libre-service reste applicable.

ADDENDUM RELATIF AUX CONDITIONS D'UTILISATION DES EQUIPEMENTS ELECTRONIQUES UTILISANT LA TECHNOLOGIE « SANS CONTACT » DANS LE CADRE DU PAIEMENT MOBILE SANS CONTACT

Le présent addendum est destiné aux Accepteurs "CB" disposant d'un Equipement Electronique doté de la technologie « Mobile sans contact » dont les conditions de fonctionnement sont régies par le présent addendum et par les Conditions Générales et Particulières du Contrat d'acceptation en paiement sur Automate en libre-service y compris les conditions d'utilisation des équipements électroniques utilisant la technologie « sans contact ». Il leur permet sous réserve des modifications prévues ci-après d'accepter des paiements au moyen de mobile bénéficiant de la technologie "sans contact.

Préambule

Dans le cadre d'un paiement en mode « Mobile sans contact », les Emetteurs peuvent mettre à disposition de leurs clients, en plus de la Carte utilisant la technologie « sans contact », un instrument de paiement disposant de la technologie « Mobile Sans Contact ». Cet instrument de paiement disposant de la technologie « Mobile sans contact » est constitué d'un logiciel de paiement mobile en mode sans contact intégré pour partie dans un élément sécurisé d'un téléphone mobile, pour partie dans le téléphone lui-même, et permettant de réaliser des opérations de paiement "CB".

Définitions

Dans l'ensemble du présent contrat d'acceptation, et pour l'application du présent addendum relatif à l'acceptation en paiement « Mobile sans contact » sur automate, il faut entendre en lieu et place de la Carte, l'instrument de paiement disposant de la technologie « Mobile sans contact », ci-après « l'Instrument de Paiement ».

Le système d'acceptation en paiement "CB" sans contact permet l'utilisation d'un Instrument de Paiement, pour le paiement d'achats de biens ou de prestations de services auprès des Accepteurs adhérant au « système CB ».

Par Acceptation en paiement "CB" sans contact, il faut également entendre tout dispositif permettant à un utilisateur d'un Instrument de Paiement d'effectuer une opération de paiement "CB" sans contact.

Par Utilisateur d'un Instrument de Paiement il faut entendre le titulaire du compte sur lequel fonctionne l'Instrument de paiement.

Obligations de l'Accepteur "CB"

L'Equipement électronique disposant de la technologie "Mobile sans contact" permet le règlement rapide d'achats de biens ou de prestations de services par des Utilisateurs de l'application en paiement décrite dans le préambule avec une lecture à distance de l'application de paiement, avec ou sans frappe d'un code confidentiel sur le clavier de leur téléphone mobile.

Il est expressément convenu entre l'Accepteur "CB" et l'Acquéreur "CB" que :

Article 1 : SIGNALETIQUE SANS CONTACT

L'Accepteur "CB" s'engage à signaler au public le point d'acceptation de paiement Mobile sans contact "CB" par l'apposition sur le dispositif d'acceptation, au niveau du lecteur sans contact de façon apparente, d'un pictogramme permettant d'identifier le paiement mobile sans contact "CB" pour guider l'Utilisateur.

Article 2 : SUIVI DES DIRECTIVES DE L'EQUIPEMENT ELECTRONIQUE

En toutes circonstances, l'Accepteur "CB" doit se conformer aux directives qui apparaissent sur cet Equipement Electronique.

Article 3 : Montant maximum par opération Mobile sans contact

Le montant maximum unitaire interbancaire de chaque opération Mobile sans contact est limité à 300 euros. Au-delà de ce montant unitaire maximum, l'opération de paiement Mobile sans contact ne peut être effectuée.

Ce montant unitaire de 300 euros s'applique uniquement si l'Equipement Electronique a intégré les spécifications techniques du Bulletin V12.3 émis par le GIE "CB". A défaut, le montant unitaire maximum « Mobile sans contact » est limité à 20 euros.

Article 4 : Saisie du code confidentiel

En conséquence, il est ajouté au présent contrat d'acceptation en paiement sur automate libre-service, un article 7.3.1 qui prévoit ce qui suit :
« 7.3.1 En cas d'opération en mode « sans contact » permise par l'Equipement Electronique sur l'Automate, l'opération de paiement est garantie même si le code confidentiel n'est pas vérifié, sous réserve du respect de l'ensemble des autres mesures de sécurité à la charge de l'Accepteur « CB ».

Article 5 : RESPONSABILITE DE L'EMETTEUR

L'Émetteur ne peut être tenu pour responsable de l'impossibilité d'utiliser l'instrument de paiement "CB" en cas de dysfonctionnement du téléphone mobile et/ou de l'Élément sécurisé.

Article 6 : MESURES DE SECURITE ET MODALITES ANNEXES DE FONCTIONNEMENT

Les articles suivants du présent Contrat ne sont pas applicables à l'acceptation du paiement "CB" "Mobile sans contact" :

- 4.6 de l'article 4 « Obligations de l'Acquéreur "CB",
- 7 alinéa 1, 7.3, 7.4 et 7.5 de l'article 7 (mesures de sécurité)
- 8.3 (retrait à son titulaire d'une carte faisant l'objet d'un blocage ou d'une opposition) et 8.4 (oubli d'une carte par son titulaire) de l'article 8.

Article 7 : DIVERS

Le présent addendum s'applique pour une durée indéterminée.

L'ensemble des autres dispositions du Contrat d'acceptation en paiement sur automate libre-service demeure inchangé et reste applicable.

REFERENTIEL SECURITAIRE ACCEPTEUR

Les exigences constituant le Référentiel Sécuritaire Accepteur sont présentées ci-après

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

Pour assurer la sécurité des données des opérations de paiement et notamment, des données des Titulaires de Cartes, une organisation, des procédures et des responsabilités doivent être établies.

En particulier, un responsable de la sécurité du système commercial et d'acceptation doit être désigné. Il est chargé, entre autres, d'appliquer la législation sur la protection des données à caractère personnel et du secret bancaire 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 d'acceptation 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 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 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.

Le Personnel doit être sensibilisé aux risques encourus, notamment sur la divulgation d'informations confidentielles, l'accès non autorisé aux informations, aux supports et aux documents.

Le Personnel doit être régulièrement sensibilisé 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 le Personnel reçoive une formation appropriée sur l'utilisation correcte du système d'exploitation et du système applicatif commercial et d'acceptation.

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 opération de paiement et notamment, des données du Titulaire de la

Carte doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les règles et recommandations de la 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 d'acceptation

Les règles de sécurité relatives aux accès et sorties depuis et vers le système commercial et d'acceptation 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 d'acceptation 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 œuvre 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 corrigables.

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 d'acceptation

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 d'acceptation.

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 d'acceptation

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 d'acceptation

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 avoir la fonction de pare-feu pour 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 pernecieux

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 d'acceptation.

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 (E10)
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 d'acceptation

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 d'acceptation

La protection et l'intégrité des éléments de l'opération de paiement doivent être assurées 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 d'acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

Exigence 14 (E14)
Protéger la confidentialité des données bancaires

Les données du Titulaire de la Carte ne peuvent être utilisées que pour exécuter l'ordre de paiement et pour traiter les réclamations. Le cryptogramme visuel d'un Titulaire de Carte ne doit en aucun cas être stocké par l'Accepteur "CB".

Les données bancaires et à caractère personnel relatives à une opération de paiement, et notamment les données du Titulaire de la 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 dispositions de la loi Informatique et Libertés et aux recommandations de la CNIL.

Il en est de même pour l'authentifiant de l'Accepteur "CB" et les éléments secrets servant à chiffrer.

Le dossier de sécurité propre au système commercial et d'acceptation 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.