Banque Populaire Auvergne Rhône Alpes.
Siège social : 4, boulevard Eugène Deruelle – 69003 LYON.
Société Anonyme Coopérative de Banque Populaire à capital variable, régie par les articles L512-2 et suivants et du Code Monétaire et Financier et l'ensemble des textes relatifs aux Banques Populaires et aux établissements de crédit –Siren 605 520 071 RCS Lyon – Intermédiaire d'assurance N° ORIAS : 07006015. N° TVA intracommunautaire : FR 00 605 520 071.
Téléphone : 0 820 870 870 **www.bpaura.banquepopulaire.fr**

CONDITIONS GENERALES
CONTRAT VENTE A DISTANCE INTERNET CYBERPLUS PAIEMENT ACCESS

Conditions générales d'adhésion au système de paiement à distance sécurisé par cartes « CB » ou agréées « CB »

PREAMBULE

L'Accepteur utilisant des moyens électroniques ou non pour vendre à distance des biens et des services et notamment souhaite recevoir des paiements à distance en contrepartie d'actes de vente ou de fournitures de prestation de service qu'il réalise lui même.

Par paiement à distance il faut entendre tout paiement par correspondance et assimilé (téléphone, terminal, Internet,..) pour lequel la transaction financière est réalisée au moyen d'un numéro de carte de paiement, de la date de validité de la carte et de son cryptogramme visuel situé au verso de celle-ci.

L'Accepteur déclare connaître les lois et règlements applicables aux ventes et achats à distance et notamment aux échanges utilisant les réseaux électroniques et les différents terminaux de communication (TV, téléphonie mobile, ordinateur…). Il reconnaît qu'il doit se conformer à ces dispositions ou à celles qui pourront intervenir et qu'il doit commercialiser les produits ou services faisant l'objet d'un paiement à distance en respectant les lois et règlements applicables, notamment fiscaux.

A la lumière de ces éléments l'Accepteur a souhaité être soumis au présent Contrat.

ARTICLE 1 - OBJET

Les présentes ont pour objet de déterminer les conditions d'adhésion et de règlement des paiements par cartes bancaires en vente à distance.

ARTICLE 2 OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur s'engage à :

2.1 A respecter les conditions contractuelles proposées par la Banque Acquéreur, les dispositions légales, réglementaires et professionnelles sans limitation des dispositions relatives aux ventes et prestations réalisées à distance, ainsi que les bonnes pratiques commerciales telles que définies notamment par les codes de Conduite.

Dans le cadre du présent Contrat s'abstenir de toute activité qui pourrait être pénalement sanctionnée telle que la mise en péril de mineurs, des actes de pédophilie, des actes de contrefaçon d'œuvres protégées par un droit de propriété intellectuelle et de moyens de paiement, le non-respect de la protection des données personnelles, des atteintes aux systèmes de traitement automatisé de données, des actes de blanchiment, le non respect des dispositions relatives aux jeux de hasard, aux courses de chevaux, aux loteries et des dispositions relatives aux conditions d'exercice de professions réglementées.

2.2 Garantir la Banque Acquéreur contre toute incidence dommageable pouvant résulter pour elle du manquement aux obligations visées à l'article 2.1.

2.3 Indiquer clairement ses coordonnées (dénomination commerciale, RCS, représentant légal…), de telle sorte que le Porteur de Carte n'ait pas de difficulté à vérifier les opérations de paiement qu'il a effectuées,

2.4 Accepter les Cartes pour le paiement d'achats de biens ou de prestations de services offerts à sa clientèle, auquel le porteur a effectivement et expressément consenti, même lorsqu'il s'agit d'articles vendus ou de prestations fournies à titre de promotion ou de soldes. En outre l'Accepteur s'interdit de toute autre activité.

2.5 Appliquer aux Porteurs de Cartes les mêmes prix qu'à l'ensemble de sa clientèle. En tout état de cause, ne faire supporter, directement ou indirectement, aucun frais supplémentaire au Porteur de Carte, du seul fait qu'il utilise sa Carte comme mode de paiement.

2.6 Afficher visiblement, sur le dispositif permettant la transaction et sur ses supports de communication, le montant minimum éventuel à partir duquel la Carte est acceptée afin que le Porteur en soit préalablement informé. Ce montant minimum doit être raisonnable et ne pas être un frein à l'acceptation des Cartes.

2.7 Signaler au public l'acceptation des Cartes de façon apparente par affichage, notamment le dispositif permettant la transaction et sur ses supports de communication, conformément à la charte graphique communiquée par la Banque Acquéreur.

2.8 Afficher visiblement sur tout support de l'offre de vente à distance le prix du produit et/ou du service fourni, ainsi que la devise dans laquelle ce prix est libellé, et ce, notamment de façon à ce que le Porteur de Carte ne soit pas en mesure de croire que le prix était autre.

2.9 Régler, selon les Conditions Particulières, les commissions, frais et d'une manière générale, toute somme due dans le cadre du fonctionnement du mode de paiement à distance objet du présent Contrat.

2.10 Faire son affaire personnelle des litiges commerciaux avec les Porteurs de Carte, notamment lors de l'exercice par le Porteur de son droit de rétractation.

2.11 Utiliser le présent contrat sous la seule référence du SIRET mentionné lors de la signature du présent contrat.

2.12 Informer préalablement et par écrit la Banque Acquéreur de toute modification de son objet social ou de toute extension de la nature des produits ou services vendus à l'aide du présent contrat et, plus généralement, de toutes modifications des conditions d'exercice de l'activité susceptibles d'avoir un impact sur les obligations souscrites par l'Accepteur aux termes des présentes.

2.13 Lutter contre la fraude dont son point d'acceptation pourrait être victime, notamment en mettant en œuvre sans délai les mesures sécuritaires appropriées préconisées par la Banque Acquéreur.

2.14 Prendre à sa charge en cas d'impayés ou de fraude l'intégralité des frais de gestion unitaire tels qu'indiqués dans les Conditions Particulières du présent contrat. A ce titre, l'Accepteur autorise irrévocablement la Banque Acquéreur à débiter à tout moment le compte ouvert en ses livres sous le numéro indiqué dans la « demande d'adhésion » du présent Contrat du montant des frais.

2.15 La Banque Acquéreur se réserve le droit de faire procéder aux frais de l'Accepteur dans ses locaux ou ceux de ses prestataires, à la vérification par un tiers indépendant du respect des bons usages de la profession (ci-après "l'Audit"), à tout moment lors de la conclusion du présent Contrat et/ou pendant la durée du présent Contrat. 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 aux bons usages de la profession, la Banque Acquéreur peut mettre en œuvre les mesures prévues à l'article 8.

Adhérer aux bons usages de la profession de la vente à distance correspondant à minima aux principes figurant en annexe du présent Contrat et les mettre en œuvre, comme notamment Paiement Card Industry (PCI), Data Security Standard (DSS).

La Banque Acquéreur se réserve également le droit de subordonner l'adhésion au mode de paiement à distance à la mise en œuvre d'un audit et le cas échéant, à la mise en œuvre des mesures recommandées par l'auditeur.

ARTICLE 3 - OBLIGATIONS DE LA BANQUE ACQUÉREUR

La Banque Acquéreur s'engage à :

3.1 Fournir, à l'Accepteur les informations que celui-ci doit obligatoirement utiliser.

3.2 Indiquer à l'Accepteur la liste et les caractéristiques de toutes les cartes bancaires pouvant être acceptées ainsi que les méthodes utilisées pour cette acceptation.

3.3 Créditer le compte de l'Accepteur des sommes qui lui sont dues, selon les modalités prévues dans les Conditions Particulières.

3.4 Ne pas débiter, au delà du délai maximum de 6 mois à partir de la date du crédit initial porté au compte de l'Accepteur les opérations qui ne pourront pas faire l'objet d'un règlement par la Banque Acquéreur et qui n'ont pu être imputées au compte du Porteur.

ARTICLE 4 - RÈGLEMENT DU PAIEMENT

4.1 Les opérations de paiement seront réglées sous réserve « d'une bonne fin d'encaissement » impliquant :

- Le respect de l'ensemble des mesures de sécurité énoncées aux présentes.
- L'absence de toute de réclamation écrite du titulaire de la Carte qui conteste la réalité même ou le montant de la transaction.
- L'absence d'opération réalisée au moyen d'une Carte non valide, périmée ou annulée.

4.2 L'Accepteur doit être clairement identifié par le numéro SIRET et le Code NAF que l'INSEE lui a attribués. Le numéro SIRET, identifiant le point de vente, sera celui du siège social de l'Accepteur ou de celui de l'un de ses établissements qui est habilité par les présentes à recevoir les paiements auxquels les clauses du présent Contrat sont opposables.

4.3 Lors du paiement L'Accepteur s'engage à :

4.3.1 Contrôler la longueur (de 13 à 19 caractères) et la vraisemblance mathématique du numéro de la Carte.

4.3.2 S'assurer que la Carte est en cours de validité, suivant les indications communiquées par le Porteur de la Carte.

4.3.3 Contrôler le numéro de Carte par rapport à la dernière liste des Cartes en opposition diffusée par la Banque Acquéreur, pour le point de vente concerné et selon les conditions convenues avec la Banque Acquéreur.

4.3.4 Vérifier, le cas échéant que le bon de commande est bien signé s'il s'agit d'une vente par correspondance.

4.3.5 Obtenir une autorisation pour le montant de la transaction. A défaut, l'opération ne pourra pas faire l'objet d'un règlement. La demande d'autorisation doit indiquer, au minimum, le montant, la date de la transaction, le numéro de Carte du Porteur, la date de fin de validité de la Carte, l'identifiant de l'Accepteur et celui de la Banque Acquéreur. Le numéro de l'autorisation doit être mentionné sur l'enregistrement de l'opération destiné à être remis à l'encaissement. La date de vente doit correspondre à celle de l'autorisation. Effectuer un contre-appel téléphonique auprès du Porteur de la Carte et conserver une trace écrite de cette opération de vérification

4.3.6 L'Accepteur doit informer immédiatement la Banque Acquéreur en cas de fonctionnement anormal de son dispositif d'acceptation et de toutes autres anomalies.

Après le paiement l'Accepteur s'engage à :

4.3.7Transmettre à la Banque Acquéreur après l'envoi du bien ou après la prestation de service, dans les délais et selon les modalités prévus, conformément aux conditions particulières prévues dans le cadre du présent Contrat, les enregistrements des transactions, et s'assurer qu'ils ont bien été portés au crédit du compte conformément aux conditions particulières prévues dans le cadre du présent Contrat.

Toute transaction ayant fait l'objet d'une autorisation doit être remise à la Banque Acquéreur lors de la demande d'autorisation.

4.3.8Demander, pour les livraisons réalisées à ses comptoirs ou à domicile, la présentation d'une pièce d'identité et de la Carte du Porteur utilisée pour la transaction.

4.3.9Conserver à titre de justificatif les bons de commande ainsi que les relevés détaillés des commandes reçues par clients Porteurs de Carte.

4.3.10 Communiquer à la demande de la Banque Acquéreur, dans les délais prévus aux conditions particulières du présent Contrat, tout justificatif des transactions de paiement.

4.3.11 Adresser, à la demande du porteur de la Carte, une facture précisant notamment, le mode de paiement par Carte.

4.3.12 **L'Accepteur s'engage à ne stocker, sous quelque forme que ce soit, aucune des données Cartes ci-après :**

- le cryptogramme visuel,

- la piste magnétique dans son intégralité,

- le code confidentiel.

4.3.13 Les mesures de sécurité énumérées ci-dessus, pourront être modifiées et complétées pendant toute la durée du présent Contrat, selon la procédure prévue à l'article 6.

ARTICLE 5 - RÉCLAMATION ET CONVENTION DE PREUVE

5.1 Réclamation

Toute réclamation de l'Accepteur doit être formulée par écrit à la Banque Acquéreur dans un délai maximum de 6 mois à compter de la date de l'opération contestée. Ce délai est réduit à 15 jours calendaires à compter de la date de restitution de l'impayé, dans le cas d'une réclamation relative à un impayé.

5.2. Convention de preuve

De convention expresse entre les parties, les supports électroniques sont réputés constituer au moins des commencements de preuve par écrit. En cas de conflit, les documents électroniques produits par la Banque Acquéreur prévaudront sur ceux produits par l'Accepteur, à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des documents produits par la Banque Acquéreur.

5.3 Secret bancaire et protection des données à caractère personnel

De convention expresse l'Accepteur autorise la Banque Acquéreur à communiquer et stocker le cas échéant des données secrètes ou confidentielles portant sur lui à des entités impliquées dans le fonctionnement du présent Contrat aux seules finalités de traiter les opérations de paiement, de prévenir des fraudes et de traiter les réclamations qu'elles émanent des Porteurs de Cartes ou d'autres entités.

ARTICLE 6 - MODIFICATIONS DES DISPOSITIONS DU CONTRAT

6.1 La Banque Acquéreur peut modifier à tout moment le présent Contrat, pour des raisons techniques, commerciales ou juridiques. Les modifications techniques autres que les travaux d'installation et de maintenance (concernant notamment l'acceptation de nouvelles Cartes, les modifications de logiciel, le changement de certains paramètres, la remise en état du dispositif d'Acceptation suite à un dysfonctionnement) si elles n'ont pas de raisons sécuritaires, doivent être mises en œuvre par l'Accepteur un mois après l'envoi de la lettre de notification par la Banque Acquéreur.

6.2. Les modifications sécuritaires concernent notamment :
- la modification du seuil de demande d'autorisation ;
- la suppression de l'acceptabilité de certaines Cartes ;

La Banque Acquéreur peut modifier à tout moment le présent Contrat pour des raisons liées à l'absence de sécurité présentée par le ou les moyens sécuritaires d'acceptation appliquée par l'Accepteur ou pour la mise en œuvre de nouvelles dispositions sécuritaires.

6.3. Le délai dans lequel les modifications sécuritaires doivent être mises en œuvre par l'Accepteur est exceptionnellement réduit à cinq jours calendaires notamment lorsqu'il est constaté une utilisation anormale de Cartes perdues, volées ou contrefaites, exigeant une mesure sécuritaire rapide et motivée telle que notamment la réduction du montant du seuil de demande d'autorisation.

6.4. En cas de suppression de l'acceptabilité de certaines Cartes, les nouvelles dispositions entrent immédiatement en vigueur, à compter de leur date de communication à l'Accepteur, faites par tout moyen par la Banque Acquéreur.

6.5. Passés les délais visés aux articles 6.1 et 6.3, et après diffusion de l'information visée à l'article 6.4, les modifications sont opposables à l'Accepteur. L'Accepteur peut résilier le présent Contrat s'il s'oppose à l'application des nouvelles dispositions.

6.6. Le non-respect des nouvelles conditions techniques ou sécuritaires, dans les délais impartis, peut entraîner outre les conditions de règlement, la résiliation du présent Contrat dans les conditions prévues à l'article 8 du présent Contrat.

ARTICLE 7 - DURÉE - RÉSILIATION DU CONTRAT

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

L'Accepteur d'une part, la Banque Acquéreur d'autre part, peuvent, à tout moment, sans justificatif et moyennant un préavis de trois mois (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 garde alors la faculté de continuer à adhérer au Système "CB" en utilisant des moyens sécurisés d'acceptation avec tout autre Acquéreur "CB" de son choix.

Lorsque cette résiliation fait suite à un désaccord sur les modifications prévues à l'article 6 ci-dessus, elle ne peut intervenir qu'au-delà du délai prévu dans cet article pour l'entrée en vigueur de ces modifications.

7.2. Toute cessation d'activité de l'Accepteur, cession ou mutation du fonds de commerce ainsi que tout comportement gravement répréhensible, 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 Contrat, des impayés apparaîtraient, ils seront à la charge de l'Accepteur ou pourront faire l'objet d'une déclaration de créances.

7.3. L'Accepteur est tenu de restituer à l'Acquéreur, les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur est propriétaire. Sauf dans le cas où il a conclu un ou plusieurs autres contrats d'adhésion, l'Accepteur s'engage à retirer immédiatement de son Système d'Acceptation et de ses supports de communication tout signe d'acceptation des Cartes.

ARTICLE 8 - MESURES DE PRÉVENTION ET DE SANCTION

En cas de manquement de l'Accepteur aux dispositions du présent Contrat ou aux lois en vigueur ou en cas de constat d'un Taux d'Impayés anormalement élevé au regard de l'activité de l'Accepteur, ou d'utilisation anormalement élevée de Cartes perdues, volées ou contrefaites, la Banque Acquéreur 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 constaté.

Si dans un délai de 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 Acquéreur peut résilier de plein droit avec effet immédiat, le présent Contrat par lettre recommandée avec demande d'avis de réception. De même, si dans un délai de trois mois à compter de l'avertissement, l'Accepteur est toujours confronté à un Taux d'Impayés anormalement élevé au regard de l'activité de l'Accepteur la Banque Acquéreur peut décider la résiliation de plein droit avec effet immédiat du présent Contrat, notifiée par lettre recommandée avec demande d'avis de réception.

ARTICLE 9 - PROTECTION DES DONNÉES A CARACTÈRE PERSONNEL

Dans le cadre de la relation bancaire, la Banque est amenée à recueillir des données à caractère personnel concernant le client, le cas échéant, le représentant légal, le mandataire et à les traiter notamment en mémoire informatisée selon les dispositions de la loi « informatique et libertés » du 6 janvier 1978 modifiée. Les données à caractère personnel ainsi recueillies sont obligatoires et ont pour principales finalités la tenue et la gestion du (des) compte(s), ainsi que la gestion de la relation bancaire, la gestion du risque, la gestion et la prévention du surendettement, la gestion des incivilités, le respect de ses obligations légales ou réglementaires, les études statistiques et la fiabilisation des données, le contrôle et la surveillance lié au contrôle interne auquel est soumis la Banque, l'octroi de crédit, les analyses, les études, le pilotage de l'activité bancaire, le reporting, l'historisation des données pour garantir la piste d'audit, la sécurité et la prévention des impayés et de la fraude, le recouvrement, le contentieux, la lutte contre le blanchiment de capitaux et le financement du terrorisme, l'échange automatique d'informations relatif aux comptes en matière fiscale, la classification, la segmentation à des fins réglementaires et/ou commerciales, la sélection et le ciblage de la clientèle, la prospection et l'animation commerciale, la communication et le marketing.
Le refus par le titulaire/représentant légal/mandataire de communiquer tout ou partie de ses données peut entraîner le rejet de la demande.
Elles sont destinées, de même que celles qui seront recueillies ultérieurement, à la Banque responsable de traitement. Certaines données peuvent être adressées à des tiers pour satisfaire aux obligations légales et réglementaires.
La Banque est tenue au secret professionnel à l'égard de ces données. Toutefois, la Banque est autorisée par le titulaire/représentant légal/mandataire à communiquer les données le concernant dans les conditions prévues aux présentes Conditions Générales.
Les données à caractère personnel (informations nominatives) que le Client a transmises à la Banque conformément aux finalités convenues peuvent, à l'occasion de diverses opérations, faire l'objet d'un transfert dans un pays de l'Union Européenne ou hors Union Européenne.
Dans le cadre d'un transfert vers un pays hors Union Européenne, des règles assurant la protection et la sécurité de ces informations ont été mises en place. Le Client peut en prendre connaissance en consultant la notice d'information accessible sur le site Internet de la Fédération Bancaire Française : www.fbf.fr.
Ces données peuvent être communiquées, à leur requête, aux organismes officiels et aux autorités administratives ou judiciaires habilités, notamment dans le cadre de la lutte contre le blanchiment des capitaux ou de la lutte contre le financement du terrorisme. Pour ces mêmes raisons, en vertu du Règlement CE/1781 du 15 novembre 2006, en cas de virement de fonds, certaines des données doivent être transmises à la banque du bénéficiaire du virement située dans un pays de l'Union européenne ou hors Union européenne.
Le titulaire/représentant légal/mandataire disposent d'un droit d'accès et de rectification s'agissant de leurs données ainsi que d'un droit d'opposition au traitement de ces données pour motifs légitimes. Ils peuvent également s'opposer sans frais à ce que ces données fassent l'objet d'un traitement à des fins de prospection notamment commerciale.
Ces droits peuvent être exercés par courrier accompagné d'une copie de tout document d'identité signé par le demandeur auprès de La Banque Populaire Auvergne Rhône Alpes, en s'adressant au service réclamations 30 avenue Charles De Gaulle - 74 800 La Roche sur Foron.

ARTICLE 10 - NON RENONCIATION

Le fait par l'Accepteur ou par la Banque Acquéreur de ne pas exiger à un moment quelconque l'exécution stricte par l'Accepteur ou par la Banque Acquéreur d'une disposition du présent Contrat n'est en aucun cas réputé constituer une renonciation, quelle qu'elle soit, à l'exécution de celle-ci.

ARTICLE 11 - Loi applicable/Tribunaux compétents
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 sera 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.

Conditions particulières convenues entre l'Acquéreur CB et l'Accepteur CB

Article 1 – DELAI DE TRANSMISSION DES OPERATIONS
Le délai maximum de transmission des enregistrements aux centres de traitement au-delà duquel la garantie cesse (même en cas d'annulation) est égal au délai indiqué dans la grille figurant sur la page précédente, en jours calendaires à compter de la date de vente.

Article 2 – SECURITE DES TRANSACTIONS
Les informations relatives à la sécurité des transactions, entre autres : n° accepteur, n° téléphone du Centre d'autorisation etc…, sont remises à l'accepteur par l'agence de la Banque Populaire Auvergne Rhône Alpes ou, lors de la mise à disposition du matériel par les services de la banque.
Le client s'engage à utiliser les serveurs informatiques (PAD) recommandés par la Banque pour les demandes d'autorisation et de télécollecte.
A défaut, les conditions d'encaissement des cartes bancaires pourront-être modifiées unilatéralement par la Banque sans préavis.

Article 3 – AUTORISATION
L'accepteur doit, au moment de la transaction, obtenir un accord du Centre d'autorisation dans les cas suivants :
1 Lorsque le montant d'une opération ou le montant cumulé des opérations effectuées au moyen d'une carte émise par une banque française, dans la même journée et dans le même point de vente, provoque un dépassement du montant de la garantie de base indiquée dans la grille figurant sur la page précédente (ou modifiée par lettre de la Banque ou notification du GIE Cartes Bancaires)
2 Lors de toute transaction réalisée avec une carte dite à "autorisation systématique". Ces cartes peuvent être nationales et ne comporter que le logo CB ou internationales et comporter en plus les logos "Electron" pour Visa ou "Maestro" pour MasterCard.
3 Lors de toute transaction réalisée avec une carte des réseaux Visa ou Eurocard-MasterCard émise par une banque étrangère.

Article 4 - GARANTIE DE PAIEMENT
Les opérations sont garanties sous réserve du respect de l'ensemble des mesures de sécurité à la charge de l'accepteur et définies dans les conditions générale ainsi que dans l'article 3 ci-dessus, sauf en cas de :
1 réclamation écrite du titulaire de la carte qui conteste la réalité même ou le montant de la transaction,
2 opération réalisée avec une carte non valide, périmée ou annulée

Article 5 – REJETS TECHNIQUES
L'accepteur est tenu d'accepter les rejets techniques, pendant 3 mois à compter de la date de traitement de la transaction initiale, en cas de :
N° de carte différent de 13, 16 ou 19 positions
Code émetteur du n) de carte erroné
N° de carte inexistant

Article 6 – DELAI DE COMMUNICATION DES JUSTIFICATIFS
A toute demande de la banque, l'accepteur s'engage à fournir le justificatif de la transaction dans un délai de 8 jours à compter de la demande.
Passé ce délai, son compte pourrait être débité du montant de la transaction concernée.

Article 7 – LISTE D'OPPOSITION
La banque s'engage lors de chaque connexion du TPE de l'accepteur avec le centre de télécollecte à lui fournir la dernière version de la liste d'opposition.

Article 8 – INDISPONIBILITE DU MATERIEL
En cas d'indisponibilité du matériel électronique quelle qu'en soit la cause, l'accepteur peut établir une facturette manuelle en indiquant obligatoirement :
- N° de la carte porteur
- Nom et prénom du porteur
- Date de validité de la carte
- Montant de la vente
- Date de la vente
- N° d'autorisation (obligatoire quel que soit le montant de la transaction en facturette manuelle).

Article 9 – TRANSMISSION DU CRYPTOGRAMME VISUEL
Le cryptogramme visuel est constitué des trois derniers chiffres apparaissant sur le panneau signature, au verso d'une carte « CB » ou agrée « CB ».
Toutes les cartes « CB » ou agrées « CB » ont un cryptogramme visuel.
La présence du cryptogramme visuel dans la demande d'autorisation est obligatoire pour tout paiement en vente à distance notamment lors d'une deuxième transaction et suivantes des paiements récurrents.
Il doit donc être systématiquement transmis lors d'une demande d'autorisation à la banque émettrice de la carte.

Article 10 - OBLIGATIONS DE L'ACCEPTEUR – L'ACCEPTEUR S'ENGAGE A :
Article 10.1 - N'utiliser le présent contrat que pour le seul et unique SIREN précisé ci dessus.

Article 10.2 - Informer préalablement et formellement la banque du souhait de toute modification de son objet social ou de toute extension de la nature des produits ou services vendus à distance (signalés sur la ligne **« Activité principale »** indiquée dans la grille figurant sur la première page des présentes) et encaissés à l'aide du présent contrat.

Article 10.3 - Ne pas utiliser ce contrat dans le cadre d'une activité de vente par internet.

Article 10.4 - Impayés et Fraude. L'accepteur reconnaît qu'en cas d'impayé, la banque se réserve le droit de facturer des frais de gestion unitaires et forfaitaires, tels qu'indiqués dans les conditions tarifaires BPA.
La Banque se réserve la possibilité de provisionner, si nécessaire et sans préavis, le montant des impayés potentiels détectés, ou des commandes encaissées non livrées, notamment si l'article 3 n'a pas été respecté.
L'accepteur s'engage à lutter contre la fraude dont son point d'acceptation pourrait être victime, notamment en mettant en œuvre sans délais les mesures préconisées par le GIE Carte Bancaire, Visa, Mastercard ou la Banque.
Concernant les autres frais induits par les dossiers de fraude ou d'impayés, la Banque se réserve la possibilité de les imputer à l'accepteur, lorsque les recommandations ou instructions de la Banque ou du GIE CB n'ont pas été respectées. Selon la nature, le volume et la répétition des dossiers, ces montants peuvent être importants.

Article 10.5 - Le non respect de l'une de ces dispositions pourra entraîner la clôture immédiate et sans préavis du/des contrat(s) CB du client et pourra donner lieu à la facturation des éventuels frais engendrés par l'absence de respect des obligations de l'accepteur : notamment les pénalités du GIE, de VISA, de Mastercard et tout autres frais divers induits y compris les impayés et frais à venir sur les encaissements déjà réalisés « sauf bonne fin ».

Référentiel Sécuritaire Accepteur

Les exigences constituant le référentiel sécuritaire accepteur sont présentées ci-après :

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 des porteurs, une organisation, des procédures et des responsabilités doivent être établies.
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 nominatives 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 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.
Les personnels doivent être sensibilisés aux risques encourus, notamment sur la divulgation d'informations confidentielles, l'accès non autorisé aux informations, aux supports et aux documents.
Les personnels 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 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 doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les 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 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 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 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 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 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 ne peuvent être utilisées que pour exécuter l'ordre de paiement et les réclamations. Le cryptogramme visuel d'un porteur ne doit en aucun cas être stocké par le commerçant.
Les données bancaires et nominatives relatives à une transaction, et notamment les données du porteur 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 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.

Convention de service Cyberplus Paiement avec Systempay

1. Définitions

Toutes les définitions insérées dans les Conditions Générales du Contrat d'acceptation en paiement à distance sécurisé et du Contrat d'acceptation en paiement à distance (ci-après « contrat d'acceptation en paiement à distance « classique » ») par cartes « CB » ou agréées « CB » sont applicables à la présente Convention.

Les définitions supplémentaires suivantes auront la signification qui suit :

Acheteur	désigne tout consommateur réalisant une opération d'achat à distance auprès du Client, Accepteur « CB »
Solution Cyberplus Paiement	désigne les offres commerciales du Service Cyberplus Paiement
Service Cyberplus Paiement	désigne l'ensemble des traitements et fonctionnalités liés à l'encaissement des paiements en vente à distance et intégrés dans la Solution Cyberplus Paiement
Formulaire d'inscription commerçant	désigne le document d'enregistrement et de paramétrage des conditions du Service Cyberplus Paiement souscrites par le Client auprès de la Banque Populaire. Il fait partie des Conditions Particulières de la présente convention.

2. Objet de la convention de services

La Banque Populaire propose à ses clients commerçants ou entreprises, Accepteurs « CB » (ci-après le ou les « Client(s) »), réalisant des ventes à distance, une solution d'encaissement des ordres de paiement donnés à distance à leur profit, ainsi qu'un ensemble de traitements et fonctionnalités associés, désignés sous le nom de « Service Cyberplus Paiement ».
Les présentes Conditions Générales ont pour objet de définir les modalités techniques et juridiques selon lesquelles la Banque Populaire permet au Client de bénéficier de la Solution Cyberplus Paiement.

L'adhésion à la Solution Cyberplus Paiement est effectuée par la signature du Formulaire d'Inscription Commerçant.

La présente convention, ci-après dénommée la « Convention », se compose des présentes Conditions Générales et du Formulaire d'Inscription Commerçant, ainsi que du Kit documentaire visé à l'article 3.2 ci-après.
Elle annule et remplace toute autre convention qui aurait pu être signée entre les Parties, relative à la Solution Cyberplus Paiement.

3. Présentation de la Solution et du Service CYBERPLUS PAIEMENT

La Solution Cyberplus Paiement se décline en trois offres commerciales correspondant chacune à un canal de vente à distance :

- L'offre **Cyberplus Paiement ACCESS** s'adresse aux Clients qui pratiquent une activité de vente à distance dite « classique » (téléphone, télécopie, ou courrier). Ils disposent d'un outil de gestion de caisse doté d'un accès sécurisé à partir duquel ils pourront saisir les coordonnées de carte bancaire de leurs Acheteurs. Ces données sont enregistrées et stockées sur le Serveur sécurisé de la Solution Cyberplus Paiement.
- L'offre **Cyberplus Paiement NET** permet aux Clients qui pratiquent une activité de vente à distance dite « en ligne » (toute interface PC fixe ou portable, Smartphone ou tablette disposant d'une connexion internet permettant d'afficher la page de paiement de la Solution Cyberplus Paiement), de proposer un formulaire de paiement en ligne à leurs Acheteurs internautes à partir de leur boutique en ligne pour enregistrer les coordonnées de carte bancaire.
- L'offre **Cyberplus Paiement MIX** est destinée aux Clients pratiquant à la fois une activité de vente à distance « classique » et/ou une activité de vente « en ligne » et qui recherchent une solution de paiement s'intégrant dans le processus de commande au sein de leur système d'information.

3.1 Détail des fonctions des Solutions Cyberplus Paiement

:

CYBERPLUS PAIEMENT ACCESS

La Solution Cyberplus Paiement ACCESS :

Cette Solution requiert la signature d'un contrat d'acceptation en paiement à distance « classique ».

La Solution Access comprend :

- **L'acceptation des moyens de paiement suivants :**
  - cartes bancaires : CB, VISA et MASTERCARD et MAESTRO,
  - cartes privatives (1) : American Express, Cofinoga, Cetelem, JCB,
  - e-carte bleue,

- **L'outil « gestion de caisse - back office Client »**
  - consultation des opérations de paiement,
  - suivi du fichier des remises bancaires,
  - possibilité de **saisir**, valider, consulter, annuler, modifier, rembourser et dupliquer une opération de paiement,
  - capacité d'exporter les transactions sous format XLS, XML ou CSV.

- **Les canaux de vente**
  - vente à distance « classique »
    - téléphone,
    - télécopie,
    - catalogue papier,
    - courrier,
    - email.

- **Les typologies de paiement (1)** :
  - paiement à l'acte,
  - paiement en « n » fois,
  - paiement différé,

- **La sécurité de la Solution Cyberplus Paiement Access:**
  - certification PCI-DSS,
  - accès sécurisé à l'outil de gestion de caisse par identifiant et mot de passe,
  - renouvellement des mots de passe tous les trois (3) mois,
  - envoi des identifiants et mots de passe par email (avec saisie du code de première connexion obligatoire).

Les services additionnels

Ces services sont optionnels et comprennent :

- *Suivi Client*
- *Contrôle Risques*
- *Gestion Bancaire Simplifiée (sous forme visuelle uniquement)*
- *Gestion Utilisateur*

Le détail de ces services est disponible sur le site www.cyberpluspaiement.com.

(1)Liste non exhaustive, reportez-vous à la fiche produit pour connaître toutes les cartes privatives et/ou typologie de paiement disponibles ou consultez votre conseiller Banque Populaire

CYBERPLUS PAIEMENT NET

Cette Solution requiert la signature d'un contrat d'acceptation en paiement à distance sécurisé.

La Solution Cyberplus Paiement NET comprend :

- **Le formulaire de paiement**
  - affichage des cours de change en devises (contre-valeur),
  - affichage des pages de paiement en multi-langues (8 langues) (2),
  - restitution sur le ticket de paiement de l'Acheteur des échéances en cas de paiement en « n » fois,
  - personnalisation du logo du Client,
  - prise en charge du protocole 3DS.

- **L'acceptation des moyens de paiement suivants :**
  - cartes bancaires : CB, VISA et MASTERCARD et MAESTRO,
  - cartes privatives (1) : American Express, Cofinoga, Cetelem, JCB,
  - e-carte bleue,

- **L'outil « gestion de caisse - back office Client »**
  - consultation des opérations de paiement,
  - suivi du fichier des remises bancaires,
  - possibilité de valider, consulter, annuler, modifier, rembourser une opération de paiement,
  - capacité d'exporter les transactions sous format XLS, XML ou CSV.

- **Les canaux de vente**
  - vente en ligne **(site internet)**
    - boutique en ligne depuis une connexion Internet (PC/MAC ou depuis un mobile connecté à Internet).

- **Les typologies de paiement (1)**
  - paiement à l'acte,
  - paiement en « n » fois,
  - paiement différé,

- **La sécurité de la Solution Cyberplus Paiement :**
  - certification PCI-DSS,
  - accès sécurisé à l'outil de gestion de caisse par identifiant et mot de passe,
  - renouvellement des mots de passe tous les trois (3) mois,
  - envoi des identifiants et mots de passe par email (avec saisie du code de première connexion obligatoire),
  - génération d'un certificat d'authentification de chaque site ou boutique du Client
    - génération du certificat en temps réel
  - garantie des paiements dans les conditions du protocole 3DS
    - restitution en temps réel vers le site ou boutique du Client de l'existence ou non de la garantie,
    - affichage en temps réel de l'existence ou non de la garantie à partir de l'outil gestion de caisse,
    - restitution en différé de l'existence ou non de la garantie dans les journaux de transactions.

(1)Liste non exhaustive, reportez-vous à la fiche produit pour connaître toutes les cartes privatives et/ou typologie de paiement disponibles ou consultez votre conseiller Banque Populaire

(2) Allemand, anglais, chinois, espagnol, italien, japonais, portugais et français

Les services additionnels

Ces services sont optionnels et comprennent :

- *Suivi Client,*
- *Contrôle Risques,*
- *Gestion Bancaire Simplifiée (sous forme visuelle et fichiers),*
- *Gestion Compte Client*
- *Gestion Utilisateur*

Le détail de ces services est disponible sur le site www.cyberpluspaiement.com.

CYBERPLUS PAIEMENT MIX

Cette Solution requiert la signature d'un contrat d'acceptation en paiement à distance sécurisé et/ou de la signature d'un contrat d'acceptation en paiement à distance « classique ».

La Solution Cyberplus Paiement MIX comprend :

1] Pour la vente à distance en ligne

Avec la Solution Cyberplus Paiement MIX, le Client a le choix entre deux types de configuration pour gérer **le paiement en ligne** :

- **soit le formulaire de paiement Cyberplus Paiement MIX**
  - utilisation du formulaire de paiement en HTTP POST,
  - affichage des cours de change en devises (contre-valeur),
  - affichage des pages de paiement en multi-langues (8 langues) (2),
  - restitution sur le ticket de paiement de l'Acheteur des échéances en cas de paiement en « n » fois,
  - personnalisation du logo du Client,
  - prise en charge du protocole 3DS.

- **soit le formulaire de paiement de son site marchand (URL du Client)**
  - utilisation de web services (protocole SOAP),
  - gestion des différentes fonctions liées au paiement sécurisé
    - création
    - validation
    - modification
    - remboursement
    - duplication
    - interrogation
  - mise à disposition des outils permettant l'utilisation du protocole 3DS.

2] Pour la vente à distance classique

Avec la Solution Cyberplus Paiement MIX, le Client a le choix entre deux types de configuration pour gérer **le paiement à distance « classique »** :

- **soit à partir de son système d'information**
  - utilisation de web services (protocole SOAP),
  - gestion des différentes fonctions liées au paiement sécurisé
    - création
    - validation
    - modification
    - remboursement
    - duplication
    - interrogation

- **soit avec l'outil « gestion de caisse - back office Client » de la Solution Cyberplus Paiement MIX**
  - consultation des opérations de paiement,
  - suivi du fichier des remises bancaires,

- possibilité de saisir, valider, consulter, annuler, modifier, rembourser et dupliquer une transaction,
- capacité d'exporter les opérations de paiement sous format XLS, XML ou CSV.

(2) Allemand, anglais, chinois, espagnol, italien, japonais, portugais et français

3] Les canaux de vente

- vente à distance « classique »
  - téléphone,
  - fax,
  - catalogue papier,
  - courrier,
  - email,
  - Logiciel métier interne (logiciel de commande),
  - SVI (serveur vocal interactif),
  - Call center (plate-forme téléphonique),
  - Centre de saisie (plate-forme de saisie).

- vente en ligne **(site internet)**
  - Boutique en ligne depuis une connexion Internet (PC/MAC ou depuis un mobile connecté à Internet).

4] L'acceptation des moyens de paiement suivants :

- cartes bancaires : CB, VISA et MASTERCARD et MAESTRO,
- cartes privatives (1) : American Express, Cofinoga, Cetelem, JCB,
- e-carte bleue

5] Les typologies de paiement (1)

- paiement à l'acte,
- paiement en « n » fois,
- paiement différé,

6] La sécurité

- certification PCI-DSS,
- accès à l'outil de gestion de caisse par identifiant et mot de passe,
- renouvellement des mots de passe tous les trois (3) mois,
- envoi des identifiants et mots de passe par email (avec saisie du code de première connexion obligatoire),
- gestion de certificat pour l'authentification de chaque canal,
  - génération du certificat en temps réel,
- garantie des paiements dans les conditions du protocole 3DS,
  - restitution en temps réel dans la réponse automatique,
  - affichage en temps réel à partir de l'outil gestion de caisse,
  - restitution en différé dans les journaux de transactions.

Les services additionnels

Ces services sont optionnels et comprennent :

- *Suivi Client*
- *Contrôle Risques*
- *Gestion Bancaire Simplifiée (sous forme visuelle et fichiers)*
- *Gestion Compte Client*
- *Gestion Utilisateur*

(1) Liste non exhaustive, reportez-vous à la fiche produit pour connaître toutes les cartes privatives et/ou typologie de paiement disponibles ou consultez votre conseiller Banque Populaire.

3.2 Documentation du Service Cyberplus Paiement

Dès réception du Formulaire d'inscription commerçant composant les Conditions Particulières, la Banque Populaire adresse au Client un Kit documentaire intégrant les modalités techniques de mise en œuvre du Service Cyberplus Paiement. Les modalités de recettes et de passage en production sont décrites dans ce Kit documentaire.

Ce Kit est spécifique à la Solution Cyberplus Paiement souscrite par le Client auprès de la Banque Populaire.

3.2.1 Solution Cyberplus Paiement ACCESS

Le Kit documentaire ACCESS est composé des éléments suivants :

- Un guide de démarrage,
- Un manuel utilisateur de l'outil de « gestion de caisse »,
- Un descriptif des journaux de reporting.

3.2.2 Solutions Cyberplus Paiement NET et MIX

Les Kits documentaires NET et MIX sont composés des éléments suivants :

- Un guide de démarrage,
- Un guide d'implémentation de la page de paiement pour les paiements en ligne,
- Un kit d'images pour le formulaire de paiement en ligne,
- Un guide des cartes de test,
- Un guide d'implémentation standard des web services,
- Un manuel utilisateur de l'outil « gestion de caisse »,
- Un descriptif des journaux de reporting,
- Un guide pratique commerçant :
  - Prise en main rapide de l'outil « gestion de caisse »,
  - Cinématique des transactions,
  - Garantie de paiement 3DSecure,
  - Suivi Client-Accepteur «CB» (service additionnel),
  - Gestion Bancaire Simplifiée en mode visuel (service additionnel),
  - Contrôle Risques (service additionnel).
- Un Procès verbal de recette,
- Un certificat de Production Cyberplus Paiement communiqué après la réception du Procès Verbal de recette validé par le Client.

Un service de support et d'assistance téléphonique tels que décrits à l'article 4.1 ci-dessous, est à la disposition du Client.

4. Mise en œuvre du service

4.1 Support technique et assistance Client

Le Service Cyberplus Paiement comprend :

4.1.1 le Support technique

Il est assuré par la société partenaire LYRA NETWORK du lundi au vendredi **de 9h00 à 18h00.**
Tél. : 0811 363 364 (numéro Azur –coût d'un appel local depuis un poste fixe).
Email : supportvad@lyra-network.com.
A titre d'exemple, le support technique concerne toute question liée à l'implémentation de la Solution Cyberplus Paiement.

4.1.2 l'Assistance Client

Elle est assurée par l'équipe Cyberplus Paiement du lundi au vendredi **de 9h00 à 16h30**
Tél. : 01 58 32 23 57
Fax : 01 58 32 52 85
Email : cyberplus.paiement@paiements.natixis.fr

L'assistance Client Cyberplus Paiement concerne toutes les demandes liées à la gestion courante des services (paramétrage du site/boutique et suivi des opérations de paiement) et au fonctionnement ou utilisation des outils de la Solution Cyberplus Paiement.

5. Disponibilité du service

Le Service Cyberplus Paiement est accessible tous les jours (7 jours/7), 24 heures sur 24, sous réserve des indisponibilités occasionnelles énoncées ci-dessous.

Le Client est informé que le Service Cyberplus Paiement peut être momentanément indisponible afin de réaliser des opérations d'actualisation, de sauvegarde ou de maintenance, deux (2) heures par mois selon un planning établi par avance. La Banque Populaire en informera préalablement le Client par courrier électronique.

D'une manière générale, le Client reconnaît que la disponibilité du Service Cyberplus Paiement ne saurait s'entendre de manière absolue, et qu'un certain nombre de défaillances, de retards ou de défauts de performance peuvent intervenir indépendamment de la volonté de la Banque Populaire, compte tenu de la structure du réseau Internet ou GSM et des spécificités liées au Service Cyberplus Paiement.

6. Obligations du Client

6.1 Sécurité

Le Client s'engage à mettre en œuvre et à faire mettre en œuvre les dispositifs (matériel, procédures...) permettant d'assurer la confidentialité et la sécurité des documents de spécifications techniques, les fichiers, les données, les éléments sécuritaires remis par la Banque Populaire dans le cadre du Contrat Cyberplus Paiement.

6.2 Utilisation des guides d'implémentation

Le Service Cyberplus Paiement s'appuie sur deux guides d'implémentation :

- Guide d'implémentation de la page de paiement,
- Guide d'implémentation standard Web service (uniquement pour l'offre commerciale Cyberplus paiement MIX).

Concernant les droits de propriété intellectuelle et la confidentialité, le Client s'engage à respecter scrupuleusement les dispositions des articles 8 et 9 de la présente Convention. Il s'engage également à respecter la documentation de service fournie par la Banque Populaire et à informer immédiatement cette-dernière en cas de dysfonctionnement du Service Cyberplus Paiement.

6.3 Respect de la législation en vigueur

Le Client s'engage à respecter la législation et les réglementations en vigueur, en particulier, à ne pas diffuser des informations contraires aux bonnes mœurs, à l'ordre public, aux droits et à la réputation de tiers, à la dignité humaine, à un droit de propriété intellectuelle, notamment au droit des marques, à la vie privée ou à l'image des personnes. La Banque Populaire ne pourra être tenue responsable de toute infraction à la législation et réglementations précitées.

Le Client s'engage, sous les mêmes conditions, à adhérer aux bons usages de la profession de la vente à distance et à les mettre en œuvre, à respecter les règles du commerce concernant la vente en général et de la vente à distance en particulier, ainsi que la législation notamment sur les devises, les taxes, les publications.

Dans le cas de vente en ligne à partir d'un site marchand, le Client déclare et garantit que ledit site, ainsi que les liens rattachés, ne présentent pas de caractère illicite, immoral ou illégal et qu'ils ne portent pas atteinte aux droits des tiers, notamment aux droits de la personnalité et aux droits de la propriété intellectuelle.

Le Client s'engage à ne pas mettre en œuvre une activité de galerie marchande virtuelle multi-sites ou de prestation de paiement centralisée sans l'accord écrit de la Banque Populaire.

Le Client déclare détenir le droit d'usage et de diffusion des éléments (textes, éléments graphiques ...) qu'il utilise, et ne pas porter atteinte à un quelconque droit de propriété intellectuelle ou droit de la personnalité.

6.4 Évolution du dispositif technique

Les mises à niveau du dispositif technique du Service Cyberplus Paiement seront notifiées par la Banque Populaire au Client, par courriel. Seront joints à ce courriel les éléments d'information nécessaires pour l'exécution des mises à niveau.

Le Client s'engage à effectuer ces mises à niveau dans un délai raisonnable négocié avec la Banque Populaire, qui ne saurait excéder deux (2) mois maximum, à compter de la réception du courriel susvisé.

Si le Client n'effectue pas les dites mises à niveau dans les délais impartis, la responsabilité de la Banque Populaire ne saurait être recherchée en cas de dysfonctionnement du Service Cyberplus Paiement.

6.5 Protection des fichiers et documents

Le Client se prémunira impérativement contre tous risques concernant les fichiers, programmes et autres documents confiés à la Banque Populaire en constituant un double de ceux-ci. Le Client se déclare à cet égard pleinement informé de ce que les supports informatisés présentent une fragilité et une fiabilité nécessitant, d'une part de vérifier la qualité et l'exhaustivité de ses sauvegardes, d'autre part de réaliser des sauvegardes multiples.

Le Client est informé qu'il fait son affaire de la conservation et de l'archivage des documents concernant sa clientèle et/ou son activité, pendant la durée légale et/ou règlementaire fixée par les textes.

7. Droit de propriété intellectuelle

La Banque Populaire conserve, en tant que titulaire des droits, la propriété intellectuelle des documents techniques et plus généralement de tous les éléments remis au Client, ainsi que toutes les prérogatives s'y rattachant. Le Client n'acquiert par le Contrat Cyberplus Paiement aucun droit de propriété intellectuelle mais un simple droit d'utilisation personnel, non transférable et non exclusif pour la durée des présentes.

Le Client s'engage à ne pas modifier ou faire modifier les documents techniques ou les éléments remis, à ne pas les utiliser pour un autre usage que celui prévu par le Contrat Cyberplus Paiement, à respecter la documentation de service fournie par la Banque Populaire et à informer immédiatement cette-dernière en cas de dysfonctionnement.

Il s'oblige aussi à ne pas dupliquer ou faire dupliquer la documentation technique ou les éléments reçus pour une autre raison que celle des tests d'évaluation et dans ce cas, à détruire les copies dupliquées et à retourner l'ensemble de la documentation Cyberplus Paiement dès la fin des tests.

La Banque Populaire demeure propriétaire des procédés, moyens, méthodes et savoir-faire qu'elle met en œuvre pour exécuter ses prestations.

8. Confidentialité – Secret bancaire

8.1 Le Client s'engage à garder le secret le plus absolu notamment sur les méthodes utilisées par la Banque Populaire et dont il pourrait avoir connaissance dans le cadre de l'exécution de la présente Convention Cyberplus Paiement. A ce titre, il s'engage notamment à ne transférer ou mettre à la disposition ou à la connaissance d'aucun tiers et sous aucun prétexte, la documentation technique, manuels utilisateurs, matériels ou droits dont il pourrait bénéficier ou avoir l'usage.

Il s'oblige en outre à informer sans délai la Banque Populaire de toute potentialité de divulgation du secret.

8.2 Les documents ou renseignements fournis par le Client, ainsi que les états, études et documents provenant de leur traitement sont couverts par le secret bancaire. En particulier, aucune communication n'en pourra être effectuée à des tiers, sauf dispositions légales l'y autorisant ou autorisation expresse du Client. La Banque Populaire s'oblige à respecter de façon absolue cette obligation au secret et à la faire respecter de la meilleure façon par son personnel, ses sous-traitants, ou prestataires de services. Pour l'application de cette disposition, il est précisé que conformément aux dispositions de l'article L.511-33,6° du Code monétaire et financier, des informations confidentielles pourront être communiquées à toute personne devant intervenir ou accéder aux fichiers et en particulier les conseils ou sous-traitants de la Banque Populaire.

8.3 L'obligation de confidentialité continuera à lier les parties et leurs ayants droit, pendant toute la durée de la Convention de service et pendant cinq (5) ans après sa résiliation ou son expiration. Le présent article survivra à la résiliation ou à l'expiration de la Convention pour quelque cause que ce soit.

9. CONDITIONS FINANCIERES - Facturation et règlement

9.1 Les conditions financières du Service Cyberplus Paiement sont indiquées dans le Formulaire d'Inscription Commerçant spécifique à chaque Solution Cyberplus Paiement.

Sauf dispositions contraires, figurant dans le Formulaire d'Inscription Commerçant spécifique à la Solution Cyberplus Paiement, les factures de la Banque Populaire sont payables sans escompte dès réception.

9.2 Dans le cas où une facture ne serait pas réglée dans les trente (30) jours de son envoi par la Banque Populaire au Client, la Banque Populaire aura la faculté de suspendre l'exécution des prestations prévues par la présente Convention de service, jusqu'au règlement de la facture en souffrance, et sans que cette suspension puisse être considérée comme une inexécution des ses obligations contractuelles, ou comme une résiliation de Contrat Cyberplus Paiement du fait de la Banque Populaire, ou n'ouvre un quelconque droit à indemnisation pour le Client.
Tout mois commencé sera entièrement dû.

9.3 En outre, à compter du trente et unième jour, la somme due portera intérêt au taux de trois (3) fois le taux d'intérêt légal sans qu'une mise en demeure préalable soit nécessaire, même par simple lettre, l'intérêt étant dû et exigible par le seul fait de l'échéance du terme contractuel.

10. Responsabilité de la Banque Populaire

La Banque Populaire garantit ses prestations dans les conditions ci-dessous précisées :

10.1 Le Service est conforme aux spécifications de la documentation technique, à l'exclusion de toute adéquation à des besoins implicites envisagés par le Client. La Banque Populaire ne saurait toutefois être tenue pour responsable des dysfonctionnements du Service Cyberplus Paiement ayant pour origine l'intervention du Client ou de tiers, tels que notamment le fournisseur d'accès Internet (FAI) ou l'opérateur Télécom (par exemple, accès momentanément indisponible, lenteur ou retard dans l'affichage des pages HTML).

10.2 La Banque Populaire ne répond ni des dommages indirects tels que notamment manque à gagner, perte financière, perte de clientèle, perte de bénéfices ou d'économies escomptées, trouvant leur origine ou étant la conséquence de la Convention de service, ni des dommages causés à des personnes ou des biens distincts de l'objet de la présente convention de service.

10.3 Au cas où la responsabilité de la Banque Populaire serait retenue, et ce pour quelque raison que ce soit, les parties conviennent expressément que, quel que soit le préjudice subi, la Banque Populaire ne sera pas tenu de payer un montant supérieur aux redevances versées par le Client au titre des douze (12) derniers mois de facturation de la présente Convention de service.

11. DIVERS

11.1 En cas de difficulté d'interprétation ou de contradiction entre les titres des articles et le texte de leur contenu, le contenu des articles primera sur leur titre.

11.2 Les dispositions de la présente Convention prévalent sur toute proposition ou accord antérieur, ainsi que sur toute autre communication antérieure entre les parties ayant trait au Service Cyberplus Paiement.

11.3 Si l'une quelconque des stipulations de la présente Convention est nulle au regard d'une règle de droit ou d'une loi en vigueur, elle sera réputée non écrite, mais n'entraînera pas la nullité de la Convention.

11.4 Aucune des deux parties ne sera tenue pour responsable vis-à-vis de l'autre de l'inexécution ou des retards dans l'exécution de la présente Convention du fait de la survenance d'un cas de force majeure ou d'évènements tels que l'intervention des autorités civiles ou militaires, l'interruption totale ou partielle des réseaux de communications, le refus de licence d'importation, les incendies, les grèves, les conflits sociaux, les dysfonctionnements de matériels ou toute autre cause qui serait raisonnablement hors de son contrôle.

12. Modification des conditions

La Banque Populaire peut modifier à tout moment la présente Convention, pour des raisons techniques ou relatives à la sécurité du Service Cyberplus Paiement. Elle en informera alors le Client par écrit.

A défaut d'accord sur les modifications, le Client a la possibilité de résilier la présente Convention sans indemnité de part ni d'autre et sans autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception.

Sauf exercice de la faculté de résiliation par le Client, les nouvelles conditions entreront en vigueur dans le délai d'un (1) mois à compter de l'envoi de la lettre ou d'un courriel d'information.

13. DUREE - SUSPENSION ET RESILIATION DU CONTRAT

13.1 La durée de la Convention :

La présente Convention est conclue pour une durée indéterminée.

13.2 La suspension de la Convention :

La Banque Populaire pourra suspendre l'exécution de la présente Convention sans que cette suspension soit constitutive d'une résiliation ou d'un manquement à l'une de ses propres obligations, dans les cas suivants :

- dans le cas où le Client ne remplirait pas les obligations mises à sa charge (fourniture de données, accès aux renseignements, etc...) nécessaires à la bonne exécution de la présente Convention, Cette suspension pourra ainsi intervenir en cas de retard de paiement tel que prévu à l'article 9.2 de la présente Convention
- dans le cas où le Contrat d'acceptation en paiement à distance sécurisé et/ou du contrat d'acceptation en paiement à distance « classique » par cartes « CB » ou agréées « CB » signé par acte séparé feraient l'objet d'une suspension.

La suspension sera notifiée au Client par lettre recommandée avec accusé de réception indiquant les motifs de la suspension. L'exécution reprendra une fois que les motifs à l'origine de cette suspension auront disparus, compte tenu des modifications de prix et de délais encourues de ce fait.

13.3 La résiliation de la Convention pour manquement :

En cas de manquement par l'une quelconque des parties, aux obligations dont elle a la charge au titre des présentes, et auquel il n'aurait pas été remédié dans un délai de huit (8) jours à compter de l'envoi d'une lettre recommandée avec demande d'avis de réception, l'autre partie pourra, prononcer de plein droit la résiliation de la présente Convention.
En pareil cas, la Banque Populaire, lorsqu'elle prononce la résiliation, aura droit au paiement des prestations exécutées et non facturées, et pourra demander en sus une indemnité de résiliation égale au triple de la facturation du mois précédent.

13.4 La résiliation de la Convention de plein droit :

La Convention sera résiliée de plein droit en cas de résiliation du contrat d'acceptation en paiement à distance sécurisé et/ou du contrat d'acceptation en paiement à distance « classique » par cartes « CB » ou agréées « CB » signé(s) par acte(s) séparé(s).

Par ailleurs, la résiliation de la Convention entraîne automatiquement la résiliation de tous les contrats d'acceptation conclus entre la Banque Populaire et le Client pour l'exécution de la présente Convention.

13.5 La résiliation de la Convention sans motif :

Chacune des parties peut résilier à tout moment la présente convention. La résiliation deviendra effective au terme d'un délai de trois (3) mois à compter de l'envoi d'une lettre recommandée avec demande d'avis de réception.

14. Entree en vigueur - election de domicile - droit apllicable - reglement des litiges

La présente Convention entre en vigueur dès signature par les parties et souscription, par acte(s) séparé(s), du contrat d'acceptation en paiement à distance sécurisé et/ou du contrat d'acceptation en paiement à distance « classique » par cartes « CB » ou agréées « CB ».
La présente Convention est soumise au droit français.
Pour l'exécution de la présente Convention, il est fait élection de domicile, par la Banque Populaire et par le Client en leur siège social mentionné aux Conditions Particulières.

Pour le règlement de toute contestation ou de tout litige relatif à la présente Convention ou découlant de son exécution, il est fait expressément attribution de compétence au tribunal dans le ressort duquel est situé le siège social de la Banque Populaire.