ASSOCIATION DU PAIEMENT
Les acteurs français des services du paiement électronique

Continuité d'encaissement au point de vente

Recommandations

RESUME DU DOCUMENT

Début 2019, l'Association du Paiement a constitué un groupe de réflexion pour définir des modalités de fonctionnement des solutions d'encaissement, qui pourraient être implémentées lorsque le terminal de paiement est en panne.

Le groupe de réflexion s'est notamment appuyé sur des membres de l'Association du Paiement (Experts du paiement), des représentants du commerce, des banques, de la Banque de France et de FrenchSys.

PRECISION IMPORTANTE

Ce document n'a pas pour ambition de proposer des solutions mais de donner un éclairage sur les bonnes pratiques et les modalités de fonctionnement qui pourrait être retenues. Ce n'est donc ni une norme ni un document de certification mais un recueil des bonnes pratiques qui pourraient être mises en place tout en tenant compte des modalités de sécurité inhérentes à la transaction carte bancaire.

Le groupe de travail laisse les industriels libres de définir les solutions, à condition que celles-ci respectent ce cahier des bonnes pratiques.[1]

LA PROBLEMATIQUE

Lorsqu'un terminal de paiement est en panne, il n'existe pas de réelles solutions de contournement et le commerçant ne peut plus accepter la carte bancaire.

Certains commerçants, de par leur taille ou la criticité de leur activité, possèdent plusieurs terminaux de paiement et peuvent pallier assez facilement la défaillance de l'une des machines.

Pour les autres commerçants la seule solution consiste à utiliser un autre moyen de paiement tel que le chèque ou le cash et, en dernier recours, à demander à leur client d'aller retirer de l'argent dans un distributeur de billets.

LA REFLEXION ENGAGEE

L'Association du Paiement a donc décidé d'étudier cette problématique de plus en plus irritante à l'ère de la digitalisation et de l'instantanéité des solutions et a constitué un groupe de réflexion.

Interrogées, les associations de commerçants estiment qu'une solution de backup doit être trouvée, qu'elle doit être simple à implémenter, sécurisée (au regard d'une transaction carte traditionnelle) et avoir un cout économique incitatif.

[1] Un document complet, reprenant la totalité de l'étude réalisée, est disponible auprès du secrétariat de l'Association du Paiement

Dans plus de 60 % des pannes constatées[2], le terminal de paiement est inopérant. Il faut donc imaginer une solution qui ne soit pas liée au terminal de paiement et qui pourrait couvrir la totalité des pannes.

Une première piste pourrait être de doter le commerçant d'une seconde machine de secours. C'est une idée facile à mettre en place mais financièrement trop importante pour l'ensemble du commerce de proximité. Nous la citons néanmoins à titre d'exemple, car elle peut convenir dans certains cas.

Le groupe de travail a donc décidé d'orienter sa réflexion vers une solution digitalisée, ne s'appuyant pas sur un terminal de paiement.

LA PISTE RETENUE

Le groupe de réflexion a privilégié la mise en place d'une solution d'encaissement déportée, via la carte du client, sur un environnement de Vente A Distance sécurisé.

L'idée générale est de permettre au commerçant d'utiliser une application sur son portable ou sa caisse pour envoyer un lien de paiement (mail, SMS, Whatsapp, centre d'appel, …) pour enregistrer la transaction carte bancaire, à partir des données de la carte de son client.

Préalable :

- Le mainteneur déclenche la solution de secours, lorsqu'il le juge nécessaire, après appel du commerçant et si la typologie de la panne nécessite la mise en place de ce secours. Lui seul sera en capacité de suspendre / proroger l'utilisation, en fonction de l'avancement du dépannage. En tout état de cause, dès que le commerçant aura retrouvé un mode de fonctionnement nominal, la solution de secours devra être désactivée immédiatement. Le service doit être opérationnel le moins longtemps possible.

Description plus détaillée de la piste retenue :

- Le commerçant dispose d'une application sur son smartphone ou sa caisse lui permettant d'envoyer un lien vers le smartphone du Porteur (par SMS ou autre) ;
- Le commerçant saisi sur son application le montant et le numéro de téléphone du porteur (qu'il lui aura demandé préalablement) ;
- L'application envoie un lien de paiement au porteur ;
- Le porteur clique sur ce lien pour effectuer son paiement de façon sécurisée sur son smartphone via un Prestataire de Service de Paiement (PSP) agréé par le GIE Cartes Bancaires (Certification MPADS) ;
  - Soit par la saisie en directe sur le clavier de son smartphone des données de sa carte (comme il le ferait sur un site marchant traditionnel),
  - Soit via une carte qu'il a déjà enregistrée dans un wallet.
- Le porteur reçoit son ticket par SMS ou mail s'il le souhaite et le commerçant est également notifié du résultat de la transaction.

[2] Etat des lieux réalisés sur un parc de 650 000 machines en maintenance

Précision importante : Cette solution de secours n'a pas vocation à devenir une solution de fonctionnement nominale (elle n'a pas les mêmes garanties de sécurité). Elle devra donc avoir des contraintes à minima : contraintes d'activation, limite dans le temps, coût, prise en charge du risque … pour qu'elle ne soit pas prise pour une solution de paiement standard. Il appartiendra donc au développeur de définir ces modalités, en conservant cette préconisation à l'esprit

LES RECOMMANDATIONS DE MISE EN PLACE

Le groupe de réflexion a défini un ensemble de recommandations qu'il considère comme incontournable, dans la mise en place d'une solution de ce type :

- Tout d'abord elle ne doit pas **transgresser les bonnes habitudes** qui ont été inculquées au client depuis plusieurs années. On peut par exemple citer la transmission du numéro de la carte bancaire, la frappe du code confidentiel et d'une façon générale toutes les règles de sécurité relatives à l'utilisation de la carte ;

- La solution doit être **facilement opérationnelle**, quitte à avoir fait le nécessaire avant pour qu'elle soit rapidement mise en service en cas de panne. On ne peut en effet imaginer passer 30 minutes à enregistrer un commerçant afin de pouvoir lui mettre la solution à disposition ;

- Cette solution de continuité doit pouvoir être **mise en place par une entité dédiée** qui a la possibilité de s'assurer que le terminal est réellement en panne. Le mainteneur est, dans l'état actuel de la réflexion, considéré comme la personne la plus à même de proposer la mise en place de cette solution ainsi que son activation lorsque le terminal est effectivement en panne ;

- La solution doit être **limitée dans le temps**. Il n'est pas concevable d'imaginer que cette solution puisse perdurer après que le commerçant ait été dépanné, car elle pourrait constituer une faiblesse que des fraudeurs pourraient chercher à exploiter. Il sera donc nécessaire d'avoir un « timer » d'utilisation qui stoppe automatiquement la solution de continuité le plus rapidement possible ;

- La **notion de responsabilité de la transaction** doit être également clairement définie. Normalement, sur une transaction standard effectuée sur un terminal de paiement en état de fonctionnement, le commerçant dispose d'une garantie de règlement s'il laisse la machine effectuer l'opération. Dans le cas d'une panne, une solution temporaire est mise en place et il faut donc clairement définir les risques des uns et des autres et qui supporte ce risque. Pour bénéficier de garantie la plus proche possible de celle d'un paiement de proximité, un paiement de type Vente à Distance sécurisée est retenu car imposé par la nouvelle Directive sur les Services de Paiement.

= = = = Fin du document = = = =