12 Octobre 2016

Réponse de l'AFTE à la consultation de l'EBA sur le standard technique définissant les procédures d'authentification forte du client (SCA) et la sécurité de la communication dans le cadre de la DSP2.

L'AFTE (Association Française des Trésoriers d'Entreprise) est une association professionnelle qui fédère des personnes intéressées par la gestion de trésorerie, le financement et la gestion des risques financiers. Créée en 1976, elle compte environ 1400 membres. Les 1 000 plus importantes entreprises françaises sont membres de l'AFTE. Outre son implantation parisienne, l'AFTE est organisée à l'échelle nationale autour de 9 délégations régionales représentant 410 membres.

La position de l'AFTE à cette consultation a été élaborée par sa commission Monétique qui regroupe des trésoriers d'entreprises actrices dans le domaine des paiements par carte, par Internet ou par téléphone mobile.

L'AFTE reconnait que la sécurité des paiements est un élément indispensable à la bonne réalisation d'un acte d'achat cependant, le niveau de sécurité ne doit pas se faire au détriment du parcours d'achat du client. Il est indispensable de trouver le bon équilibré entre sécurité et fluidité du parcours clients.

1. Périmètre d'application des standards techniques

Les processus de paiement concernent les entreprises (Business) et les particuliers (Customer) ce qui donne 4 combinaisons sur lequel l'authentification forte peut être appliquée : les paiements BTB (paiement entreprise vers fournisseur), BTC (remboursement client), CTB (encaissement client d'un particulier vers une entreprise) et CTC (transfert entre particuliers).

L'AFTE comprend que les procédures d'authentification forte devront être appliquées sur les paiements par cartes, par virement (SCT) et les paiements électroniques comme le paiement mobile. L'AFTE s'interroge si les canaux suivants seront soumis à l'authentification forte : le paiement par téléphone via des call centers, les applications mobiles, le mobile quand il est utilisé comme un explorateur Internet, la VAD : saisie du PAN sur le TPE sans présence du client.

De même, s'il est très clair que l'authentification forte s'applique aux paiements électroniques initiés par des consommateurs, l'AFTE s'interroge sur l'application de cette règlementation aux paiements initiés par les entreprises et souhaite rapidement une clarification du périmètre d'application du standard technique sur l'authentification forte. En effet, les procédures, les modalités de mise en œuvre et les délais pour la mise en conformité seront très différents selon qu'il s'agit de paiements initiés par des consommateurs ou de paiements initiés par les entreprises françaises équipées de logiciels spécialisés et utilisant des protocoles de communication et de signature sécurisés tels que SwiftNet, Ebics TS et la signature 3S Key. En effet, ces dernières émettent notamment des virements de masse à leurs salariés, parfois à leurs clients (geste commercial, remboursements…) ou à leurs fournisseurs. Si l'exemption nécessite la mise en œuvre de listes blanches l'industrie du paiement et en particulier les banques devront être en mesure de proposer aux entreprises la gestion de ces listes. Par ailleurs, il ne sera pas possible pour ces paiements dits de masse et transmis par protocole sécurisés, de mettre en œuvre une authentification par bénéficiaire sur chaque ligne des fichiers de paiement.

L'AFTE demande une clarification des canaux concernés et du périmètre géographique ainsi que des autres types de paiement exclus.
Si le standard technique devait s'appliquer à tous ces paiements émis par les entreprises, il nous semble indispensable de revoir avec l'ensemble des acteurs de la chaine des paiements de masse les modalités du RTS et proposer des solutions spécifiques et des délais de mise en œuvre réalistes.
Les responsabilités des différents acteurs et les modalités de charge de la preuve en cas de litige doivent être clairement définies.

2. Chapitre 1 - Procédures d'authentification forte – Questions 1 à 3

La sécurité des paiements est un élément indispensable à la bonne réalisation d'un acte d'achat, et en particulier lorsque les achats sont effectués à distance sur des canaux comme Internet, les téléphones mobiles ou les tablettes. L'AFTE est donc en faveur de l'authentification forte mais considère que le standard proposé ne répond pas à l'attente principal des commerçants, à savoir l'approche par les risques : laisser aux commerçants la possibilité d'adapter le niveau de sécurité en fonction du risque estimé de la transaction client, de la connaissance qu'ils ont du client.

Les marchands doivent avoir la possibilité de lever tout ou partie du processus d'authentification forte en complément de l'émetteur, en fonction du niveau de risque qu'ils acceptent de prendre et la connaissance du client ou parce qu'une contrainte technique l'amène à faire ce choix (indisponibilité d'un des acteurs de la chaine d'authentification affectant directement le parcours client ou anomalie serveurs – 3Dsecure débrayable à la main du marchand). Les méthodes d'évaluation du risque client par scoring doivent être reconnues comme méthodes d'authentification forte, le marchand étant le plus à même de connaître ses clients existants et les critères à appliquer aux nouveaux clients.
L'AFTE comprend qu'il a été fait le choix de faire porter la responsabilité de la sécurité aux acteurs des paiements, comme les banques. Les méthodes d'authentification forte à l'initiative des émetteurs de cartes apparaissent peu développées à ce jour. L'approche par les risques ou targeted authentication devrait être possible à l'initiative du marchand.

Pour le cas particulier des paiements émis par les entreprises, l'AFTE s'interroge sur les solutions qui seront proposées par les banques en matière d'authentification forte pour les paiements via Swift ou Ebics TS. Les bénéficiaires des listes blanches seront-ils identifiés par leurs références IBAN qui figureront dans des listes, ou par les numéros de cartes bancaires ?

3. Chapitre 2 – Exemption aux procédures d'authentification forte – Q4 et 5

L'AFTE est favorable aux exemptions proposées mais considère que la liste est trop restrictive. L'AFTE souhaite que l'EBA prenne en compte les sujets suivants :

- Les marchands doivent pouvoir décider eux-mêmes dans leur parcours clients les méthodes à utiliser pour authentifier la validité d'un paiement. Il est important de laisser aux marchands la main sur le processus d'authentification forte en complément de l'émetteur ;
- Il est indispensable de prévoir dans les exemptions des parcours d'achat choisis par les commerçants. Les parcours clients, comme le 1-Click, doivent pouvoir être maintenus à l'avenir ;

- L'exemption sur les paiements récurrents reste imprécise dans sa rédaction actuelle. Par ailleurs, cette exemption concernerait uniquement les paiements récurrents d'un même montant. Pour des acteurs ayant des formules avec abonnement (téléphonie, presse media…) cela signifierait que si la facture d'un mois donné correspond exactement au montant du forfait, il y a exemption. En cas de montants supérieurs (ex : achats additionnels de contenus payants), l'exemption serait invalidée.
- Le seuil d'exemption : l'AFTE comprend la volonté du régulateur d'uniformiser le seuil d'application de l'authentification forte mais reste en faveur d'un seuil laissé à la main des commerçants. De même, il est nécessaire de clarifier la durée de la période sur laquelle court l'exemption relative à l'accumulation de petits montants.
- Les méthodes de scoring, les analyses sur l'historique client réalisées par le marchand lors de l'acte d'achat doivent être considérées comme des méthodes appropriées pour sécuriser les transactions.

Voir le paragraphe 1 sur le champ d'application pour ce qui concerne les paiements de masse émis par les entreprises et la gestion des listes blanches.

4. Chapitres 3 et 4 – Protection des données et standards de communication

L'AFTE comprend que la responsabilité de la mise à disposition de la SCA sera de la responsabilité de l'ASPSP et ne se positionne pas sur ces éléments.

Une question est posée : que se passera-t-il si l'ASPSP n'est pas en mesure de fournir au marchant la procédure d'authentification forte lors du parcours d'achats (serveurs hors service par exemple) ? L'AFTE met en avant ce risque qui justifie à lui seul le fait d maintenir la possibilité de faire de l'authentification ciblée en fonction du risque (targeted authentication).

L'AFTE insiste sur l'importance de la confidentialité des données. Le degré de maturité sur l'accès à la donnée est différent selon les pays en Europe (Cnil en France par exemple). Cette diversité pourrait impacter la confiance des consommateurs à donner des accès sur leurs comptes si ces informations étaient monétisées.

Pour conclure, l'AFTE rappelle que les processus d'authentification forte ne doivent pas affecter négativement les parcours des clients et préconise de donner aux marchands la possibilité d'adapter le choix du niveau de sécurité au niveau de risques.

Christophe Lesobre
Président de la commission Monétique

Contact AFTE :
Valerie Voisin
Responsable des commissions et des délégations
valerie.voisin@afte.com