

[NOUVEAUTÉ] Découvrez les événements dédiés à la numérisation des TPE PME avec l'Agenda France Num ! J'accède à l'agenda

# Paielements en ligne : l'authentification forte DSP2 pour sécuriser votre site e-commerce est désormais obligatoire

Fiche pratique | Publié le 13 juillet 2021 | Mis à jour le 03 avril 2025

banque

e-commerce

paiement

La norme de sécurisation des paiements, la DSP2, s'applique à l'ensemble des achats en ligne. Elle permet de lutter contre les fraudes par carte bancaire qui sont, avec le développement du e-commerce, de plus en plus fréquentes. Ce système d'«authentification forte» assure la protection des commerçants et rassure les clients.



Mudassar Iqbal - Pixabay License

Jusqu'à récemment, au moment de finaliser une commande en ligne, pour valider le paiement, le client recevait de sa banque un code par SMS, qu'il devait indiquer au site marchand. Ce dispositif devenu obsolète est désormais remplacé par le **dispositif d'authentification forte**, déployé à grande échelle par les émetteurs de cartes bancaires, banques, opérateurs de paiement, commerçants en ligne depuis mi-mai 2021.

Son utilisation doit permettre de **faire face à l'augmentation du nombre de fraudes constatées dans le cadre de la généralisation des achats en ligne**.

**« Le taux de fraude est 20 fois plus élevé en e-commerce (0,16 % des montants) que dans les commerces de proximité. »**

Ce nouveau dispositif en renforçant le niveau de sécurité des opérations de paiement sur internet doit limiter la fraude en ligne à un niveau acceptable.

**TPE PME e-commerçant, la sécurisation de vos solutions de paiement en ligne est indispensable pour vous protéger et pour protéger vos clients face aux fraudes en ligne...**

La bonne compréhension des enjeux et des modalités de déploiement de l'authentification forte s'avère essentielle pour limiter les perturbations qu'elle est susceptible de générer dans le parcours d'achat de votre client.

## Qu'est-ce que la directive sur les services de paiement (DSP2) ?

La directive sur les services de paiement, dite DSP2, voté en 2015 par le Parlement Européen et entrée en vigueur en septembre 2019 vise à harmoniser la réglementation sur les paiements au sein de l'Union Européenne.

**Son objectif est de moderniser les services de paiement** en Europe au profit tant des consommateurs que des entreprises, de faciliter l'usage des moyens de paiement et de renforcer la sécurité des opérations de paiements des entreprises.

**La DSP2 prévoit notamment :**

- **l'interdiction des pratiques de surfacturation**, c'est à dire l'application de **frais en cas de paiement par carte de débit ou de crédit**, aussi bien dans un magasin qu'en ligne ;
- **le renforcement des droits de consommateurs**, avec en particulier **l'abaissement de la franchise restant à la charge du client en cas de paiement frauduleux par carte** avant opposition de 150 à 50 euros, le raccourcissement des délais de remboursement et la mise en place d'un droit au remboursement inconditionnel pour les prélèvements en euros ;
- **l'obligation de l'authentification forte** (c'est-à-dire à deux facteurs au moins entre un code ou mot de passe que l'on sait, un appareil que l'on possède, une donnée biométrique telle que l'empreinte digitale, la voix ou l'iris) **pour tous les paiements en ligne**, afin de réduire la fraude dans l'e-commerce.

### DSP2 : les exemptions possibles à l'authentification forte

Les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client lorsque le payeur initie une opération de paiement électronique à distance qui ne dépasse pas 30 euros et qu'une de ces 2 conditions soit remplie :

1 - le montant cumulé des précédentes opérations de paiement électronique à distance initiées par le payeur depuis la dernière authentification forte du client ne dépasse pas 100 euros ;

2 - le nombre des précédentes opérations de paiement électronique à distance initiées par le payeur depuis la dernière authentification forte du client ne dépasse pas cinq opérations de paiement électronique à distance individuelles consécutives".

Par ailleurs, cette directive, en facilitant l'ouverture des systèmes d'information des banques et de leurs données clients à des tiers (Open Banking) permet l'émergence de nouveaux acteurs innovants et compétitifs sur le marché du paiement, à l'instar de Lydia.

## L'authentification forte pour sécuriser les paiements en ligne de son site e-commerce

**L'authentification forte fait partie de la DSP2.** Elle implique l'ensemble de l'écosystème des paiements : les banques, les prestataires de paiement, les réseaux de carte (Visa, Mastercard,...) et les e-commerçants. C'est ce qui rend son déploiement complexe.

**Concrètement, au moment de payer son achat sur internet, le client doit fournir deux des trois éléments d'identification suivants :**

- **un mot de passe ou code numérique** (dit élément de connaissance)
- **son portable ou sa ligne téléphonique** (dit élément de possession)
- **son empreinte digitale ou faciale ou le son de sa voix** (dit élément d'inhérence)

Le plus souvent, les banques demandent à leurs clients de télécharger leur application mobile qui intègre le service d'authentification forte (nommé SécuriPass, Certicode Plus, Clé Digitale, etc... selon les établissements) sur leur smartphone, ce qui permet de combiner un élément de possession (le téléphone) avec un élément de connaissance (un code) ou d'inhérence (son empreinte digitale). Au moment de payer un achat, le client reçoit une notification qui le dirige vers l'application installée sur le téléphone. Il doit alors saisir son mot de passe ou son empreinte biométrique pour valider le paiement.

**Si le client ne possède pas de téléphone intelligent ou ne souhaite pas utiliser l'application mise à disposition par sa banque, des solutions alternatives sans surcoût doivent être, selon la charte du comité national des moyens de paiement (pdf) , proposées par les banques :**

- envoi d'un SMS à usage unique couplé à un mot de passe connu par le client ;
- mise à disposition d'un dispositif physique dédié comme un lecteur de cartes bancaires.

**En France, l'authentification forte est obligatoire pour tout achat en ligne. Toutefois, les commerçants peuvent demander à leur banque d'autoriser des exemptions à la double authentification dans les cas suivants :**

- les achats de faible valeur (inférieur à 30 €, cf encadré) ;
- les achats jugés peu risqués ;
- les abonnements ou les dépenses régulières sur un même site : l'authentification forte ne sera alors exigée que la première fois ;
- les paiements effectués chez un e-commerçant que le client a désigné comme bénéficiaire de confiance ;
- les paiements effectués chez un e-commerçant affichant un faible taux de fraude.

Globalement les exemptions sont accordées selon plusieurs critères :

- la capacité technique du e-commerçant à gérer les paiements ;
- le niveau de risque de fraude ;
- en fonction des accords conclus avec le titulaire de la carte de l'acheteur.

## Se faire accompagner par son prestataire de paiement

**L'étape du paiement au cours de laquelle l'acheteur valide son panier et procède au règlement est critique pour le succès d'une vente en ligne.** Selon d'une étude de Hipay , 58% des clients ont déjà abandonné leur panier d'achats lors de la phase de paiement.

**La mise en place de l'authentification forte, si elle rassure les clients, peut aussi générer des frottements dans le parcours d'achat.** Pour éviter des difficultés qui peuvent entraîner l'abandon, **faites vous accompagner par votre prestataire de paiement**, pour sa mise en place de la DSP2 et son adaptation à votre site.

Il peut vous aider à comprendre l'impact total de la DSP2 sur la base des statistiques d'usages de votre système de paiement : les abandons, les échecs et le taux de conversion des transactions.

Sur la base des tentatives de fraude constatées il peut ajuster les exemptions dont votre système de paiement peut bénéficier. Il peut aussi vous aider à faire en sorte que vos indicateurs restent en dessous des seuils requis pour bénéficier des exemptions quand cela est possible.

Prenez contact avec votre prestataire de paiement qui vous pour aidera à :

- mettre en place l'authentification forte ;
- ajuster les exemptions éventuelles ;
- et optimiser le parcours d'achat de vos clients.

## En savoir plus

- Quel type de solutions de paiement en ligne choisir pour son site e-commerce ?
- Paiement : la directive DSP2 entre en vigueur, c'est quoi ?
- Paiement en ligne : la généralisation de la double authentification est un casse-tête pour certains clients
- Questions fréquemment posées : Rendre les paiements électroniques et les services bancaires en ligne plus sûrs et plus simples pour les consommateurs
- Paiement en ligne: entrée en vigueur de nouvelles normes de sécurité
- De nouvelles normes de sécurité dévoilées pour le paiement sur internet par carte bancaire
- Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication (Texte présentant de l'intérêt pour l'EEE)

Dieu-Linh Dao | Licence etalab-2.0

[Solutions de paiement](#)

[Tous les secteurs](#)

[Toutes les régions](#)

[Tous les niveaux](#)

## Dans la même thématique



Dossier | 12 décembre 2024

### Quelle solution d'encaissement adopter pour numériser votre restaurant ?

Pour tirer le meilleur parti du numérique, les restaurants doivent se pencher sur la question de la ...





Dossier | 10 avril 2025

### **Comment choisir son terminal de paiement ?**

Le paiement par carte bancaire s'est imposé dans les habitudes de paiement des français. Il est donc...



Fiche pratique | 11 février 2025

### **Mettre en place le pourboire par carte bancaire**

Depuis le 1er janvier 2022, les pourboires par carte bancaire des serveurs des hôtels, bars, cafés e...

[Haut de page](#)

## **Recevoir la lettre de France Num**

La lettre d'information est envoyée tous les 15 jours.

[Voir le dernier numéro](#)

[Je m'abonne](#)

---

**Suivez-nous sur les réseaux sociaux**