

La réglementation DSP2 et l'authentification forte du client sécurisent plus que jamais les transactions financières en Europe

La 2^e directive sur les services de paiement (DSP2) a été promulguée par les législateurs européens pour établir un marché transparent, simple et juste, inclure davantage d'acteurs, couvrir toutes les transactions électroniques et, bien sûr, réduire la fraude grâce à une meilleure authentification des utilisateurs. Elle offre aux banques, fintechs et autres prestataires de services une excellente occasion de proposer de nouvelles solutions de paiement en ligne et mobiles, et ainsi de diversifier l'expérience de paiement du client. En outre, elle va encourager les initiatives de simplification d'autres opérations financières, telles que les agrégations de comptes ou les contrats de prêt, tout en renforçant la protection des consommateurs.

1 ÉTAPES CLÉS

JANVIER 2018

Échéance pour la mise en œuvre de la DSP2 dans les législations nationales.

MARS 2018

Publication au journal officiel de l'U.E. des normes techniques réglementaires sur l'authentification forte du client, indispensable à la sécurité des transactions et la protection des données.

SEPTEMBRE 2019

Dernière échéance pour se conformer aux normes de l'authentification forte du client.

2

PRINCIPAUX AVANTAGES

PLUS DE FACILITÉ D'UTILISATION, MOINS DE FORMALITÉS

Les utilisateurs peuvent désormais autoriser les banques ou des fintechs tierces à accéder directement à leurs comptes bancaires afin de pouvoir consulter toutes leurs données de transaction en un seul endroit et éviter les complications liées à la multiplication d'interfaces, pour une demande de prêt par exemple.



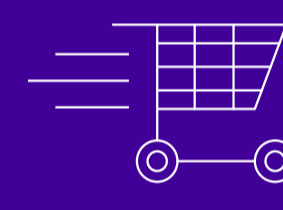
RENFORCEMENT DE LA SÉCURITÉ

L'authentification forte du client lie dynamiquement toutes les transactions à un montant et à un bénéficiaire précis et protège ainsi davantage les utilisateurs en minimisant les risques pour toutes leurs transactions électroniques.



SIMPLIFICATION DES PAIEMENTS EN LIGNE

Les utilisateurs peuvent désormais gagner du temps lors du paiement en ligne de leurs achats fréquents en autorisant les commerçants à initier des paiements directement à partir de leur compte bancaire.



3

MAIS, EN QUOI CONSISTE L'AUTHENTIFICATION FORTE DU CLIENT ?

L'un des objectifs majeurs de la directive DSP2 est de réduire le risque de fraude pour toutes les transactions électroniques et d'améliorer la protection des données des clients.

COMMENT ?

En vérifiant au moins 2 des 3 facteurs d'authentification suivants :

1

FACTEUR D'INHÉRENCE

Ce que je suis

Éléments biométriques comme les empreintes digitales, le visage ou l'iris

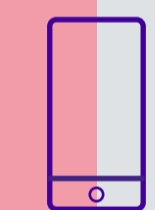


2

FACTEUR DE POSSESSION

Ce que j'ai

Smartphone, carte à puce, clé USB



3

FACTEUR DE CONNAISSANCE

Ce que je sais

Mot de passe, phrase secrète, code PIN, séquence, question/réponse



En résumé, l'authentification forte du client doit être effectuée lors de chaque transaction financière. Cependant, pour fluidifier au maximum l'expérience des utilisateurs, quelques exemptions existent, pour les paiements de faibles montants ou récurrents, par exemple.

4

MISEZ SUR LA FLUIDITÉ GRÂCE À NOS SOLUTIONS HORS PAIR, SANS EFFORT ET CONFORMES AUX NORMES DE L'AUTHENTIFICATION FORTE

SERVICE D'AUTHENTIFICATION CLOUD

Un hub d'authentification capable de **demande le(s) facteur(s) d'authentification approprié(s)** pour tous les canaux (en ligne, via un centre d'appel, en agence) et **d'analyser les niveaux de risque** afin d'atteindre des seuils d'exemption supérieurs et proposer la solution la plus sûre et la plus adaptée à chaque opération sensible.

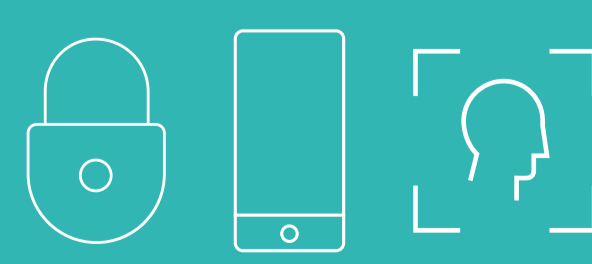
ÉVALUATION DU NIVEAU DE RISQUE

=

MÉTHODE D'AUTHENTIFICATION ADAPTÉE

SOLUTION D'AUTHENTIFICATION MOBILE: CLOUDCARD+

Une solution mobile capable de **cumuler jusqu'à trois facteurs d'authentification** (code PIN, smartphone et biométrie) qui offre aux utilisateurs un moyen pratique, moins invasif et hautement sécurisé pour prouver leur identité.



COMBINAISON DE LA MOBILITÉ ET DE LA BIOMÉTRIE

=

EXPÉRIENCE UTILISATEUR TRANSPARENTE

VISER TOUJOURS PLUS HAUT ET TOUJOURS PLUS LOIN

Grâce au service d'authentification Cloud et à sa solution d'authentification mobile, IDEMIA apporte aux institutions financières une réponse complète aux exigences de l'authentification forte avec pour objectif d'offrir aux utilisateurs finaux une expérience globale axée sur la sécurité, la continuité, la facilité d'utilisation et surtout le facteur humain.