



Decryptage 3DS 2.0, le nouveau standard d'authentification

Suite à l'entrée en vigueur de la
Directive sur les services de
paiement

By thinkmarket
business shift consulting

L'authentification par sms que nous connaissons aujourd'hui est amenée à disparaître

AUJOURD'HUI

SMS OTP (1) : authentification d'achat via mot de
passe/code de validation à usage unique reçu par
sms

Les SMS OTP sont vus par l'ABE (2) comme vulnérables
à certains types d'attaques (sim swap) et problèmes
réguliers des serveurs SMS

DEMAIN

L'ABE souhaite sécuriser les paiements en ligne en
ajoutant une authentification forte lors de l'achat



POURQUOI ?

Le taux de fraude est plus important dans le e-commerce que dans d'autres domaines d'activité,
il est donc nécessaire de réduire ce taux en renforçant la sécurisation des paiements en ligne

(1) One Time Password
(2) Autorité Bancaire Européenne

thinkmarket

L'authentification forte émerge pour une expérience client renforcée

■ Quel périmètre ?

La directive DSP2 (1) sur les services de paiement qui
aborde l'authentification forte 3DS 2 renforce la
directive DSP1.
La réglementation s'applique sur l'ensemble de la
zone européenne et oblige l'ensemble des sites e-
commerce à l'intégrer.

HORS SCOPE DU 3DS 2 :

- ➔ Paiements manuels chez les commerçants
- ➔ Paiements en plusieurs fois avec échéances variables
- ➔ Paiements par abonnement

■ Quels moyens ?



INHERENCE

Ce que je suis
Ex : reconnaissance vocale, biométrie, empreinte digitale



POSSESSION

Ce que je possède
Ex : smartphone, carte bancaire



CONNAISSANCE

Ce que je sais
Ex : mot de passe, code PIN

(1) Directive sur les Services de Paiement

thinkmarket

■ 2 types d'authentification forte



AUTHENTIFICATION FORTE

Le client doit s'identifier durant l'acte d'achat



AUTHENTIFICATION FORTE PASSIVE

L'authentification est transparente pour le client et ne
nécessite aucune action de sa part durant l'acte d'achat

Les marchands doivent se rapprocher de leur PSP (Prestataire de Service de Paiement) acquéreur pour se mettre en conformité

Attributions de l'authentification

La banque du client devient la seule à décider de pouvoir lever ou non l'authentification forte

Des préconisations peuvent être formulées soit par le PSP soit par le commerçant via sa banque, afin d'alléger le niveau d'authentification de certains
profils clients (ex : client à valeur)

■ Les cas d'exemption de l'authentification forte ?

La directive européenne prend en compte ces contraintes et a donc mis en place des cas d'exemption de l'authentification forte.
Aucune authentification n'est donc demandée pour les cas suivants :

Les transactions MOTO (1)

(Transactions par courrier
ou téléphone)

Transactions hors zone Euro

Le PSP du marchand ou
de l'acheteur est hors de
l'EEE (2)

Paiements par carte Affaires

Transactions à faible montant

Moins de 30 euros

Analyse du Risque de Transaction

Pour des montants
< 500€

Bénéficiaires de confiance

Ajout de marchands sur
liste blanche par les
clients

Cas d'exemption
systématique

Activation de l'exemption à
discrétion des banques

(1) MOTO = Mail Orders and Telephone orders (transactions non considérées comme des paiements électroniques)
(2) EEE = Espace Economique Européen

thinkmarket

Le protocole 3DS 2, une meilleure expérience pour le client et des opportunités pour le marchand

■ Les avantages pour le client ?

Renforcement de
la sécurité des
achats et
réduction du taux
de fraude

Fluidification et
accélération du
parcours d'achat

Possibilité de créer
une liste blanche de
e-commerçants
préférés pour éviter
l'authentification
forte

■ Quels avantages pour le marchand ?

Simplification des parcours d'achat



L'authentification forte est gérée entre l'établissement bancaire et le
e-marchand, plus besoin d'identifier, seul un code d'accès suffira
dans le parcours d'achat

Amélioration des taux de conversion



La redirection n'est plus nécessaire pour sécuriser l'acte d'achat du
client diminuant ainsi le taux de rebond

Optimisation du programme relationnel



Le e-marchand pourra renforcer ses arguments de fidélisation en
réduisant les points de friction (authentification allégée) pour ses
« clients de confiance » qui pourront identifier en retour le
commerçant comme « tiers de confiance »

Limitation de l'authentification forte pour les clients à valeur



Le commerçant pourra inciter la banque à relever ses critères de
déclenchement de l'authentification forte en partageant ses données
clients et ainsi permettre à la banque d'affiner son scoring de risque pour
in fine alléger le parcours d'achat des « clients de confiance »

thinkmarket

Des contraintes réelles à ne pas sous-estimer et des enjeux forts pour le développement des e-marchands

■ Quelles contraintes ?

Le commerçant n'est plus le décideur de la mise en place d'une authentification

C'est la banque de l'acheteur qui est le dernier décideur
Il peut simplement faire des recommandations sur la
nécessité ou non d'authentifier le client et doit alors
récolter davantage d'informations sur la qualité de ses
clients

Nécessité de mettre en place un programme relationnel
adapté.

A l'international



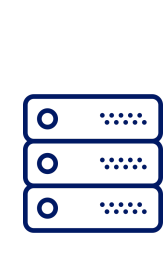
Nécessité de prendre en compte les différentes
réglementations pour les intégrer dans le parcours (cela
revient à bien choisir son intermédiaire de solution de
paiement)

■ Enjeux pour les e-marchands sur l'authentification forte

Comparer et sélectionner le
ou les meilleur(s)
intermédiaire(s) (PSP) est
indispensable



Avoir le plus grand nombre de
clients en authentification forte
passive



Extraire le maximum
d'informations possible sur sa base client
(historique de transaction, fréquence
d'achat, panier moyen, ...) pour justifier
auprès des banques la viabilité de cette
demande

Adapter ses parcours clients
suite à la mise en place de
l'authentification forte
(active/passive)



thinkmarket

Retrouvez Thinkmarket sur :



Pour en savoir plus : www.itstimetoshift.consulting