

L'authentification forte

Les paiements par carte sur internet ainsi que les opérations bancaires sensibles (accès au compte bancaire en ligne...) doivent désormais faire l'objet d'une authentification forte de l'utilisateur, de manière systématique.



L'authentification forte est, en sécurité des systèmes d'information, une procédure d'identification qui requiert la mise à bout d'au moins deux facteurs d'authentification.

La directive européenne DSP2¹ entrée en vigueur en 2018 et 2019 fixe notamment les règles de « l'authentification forte » dans le secteur bancaire, secteur influent dans le domaine.

Qu'est-ce que l'authentification forte ?

L'authentification forte est un système de sécurité qui vise à certifier que la personne qui souhaite effectuer un paiement en ligne ou accéder à ses comptes en ligne est bien le titulaire de la carte ou du compte de paiement. La DSP2 impose une validation reposant sur deux éléments ou plus d'authentification.

- La connaissance: un mot de passe, un code PIN, une information personnelle...
- La possession: un ordinateur, un téléphone, une montre connectée, un boîtier fourni par la banque...
- L'inhérence, c'est-à-dire une caractéristique biométrique : empreinte digitale, reconnaissance faciale, vocale...

Le consommateur doit confirmer son identité le plus souvent par l'intermédiaire de son smartphone, par l'application de sa banque qui va lui demander un code secret. Cette procédure dite 3D Secure n'est pas suffisante reposant sur un seul élément d'authentification qui est la possession d'un téléphone mobile considéré comme peu sécurisé

En effet, au moment de payer sur internet, le client reçoit sur un téléphone préalablement identifié une notification l'invitant à s'authentifier, soit au moyen de la saisie d'un code personnel, soit par prise d'empreinte biométrique pour les téléphones mobiles équipés.

Mais ça risque de poser des difficultés à ceux qui n'ont pas de smartphone ou ne veulent pas télécharger l'application bancaire sur leur téléphone. Chaque banque va proposer son propre système d'authentification forte (boitier, application mobile...) sous des noms commerciaux comme Certicode de la Banque Postale, SécuriPass du Crédit Agricole, Sécur'Pass de la Caisse d'Épargne.

Dans quels cas l'authentification forte est-elle nécessaire ?

Pour l'accès au compte de paiement en ligne, lors d'une opération de paiement électronique (virement ou paiement par carte), pour une action réalisée par un mode de communication à distance qui présente un risque élevé de fraude (inscription d'un nouveau bénéficiaire de virement sur un compte bancaire en ligne).

Quels sont les cas d'exemption d'authentification forte ?

Pour un bénéficiaire de confiance (bénéficiaire pré-autorisé...), pour une opération récurrente (loyer, abonnement...), pour une opération de faible valeur unitaire à distance (moins de 30 euros) ou sans contact (de moins de 50 euros), ou encore pour opération à risque limité.

Mise en œuvre de l'authentification forte ?

L'entrée en vigueur de l'obligation d'authentification forte a été fixée au 15 mai 2021 pour toutes les transactions par la directive DSP2.

- Le 15 février 2021, l'authentification forte s'appliquait aux montants supérieurs à 500 euros,
- Le 15 mars 2021, à ceux supérieurs à 250 euros,
- Le 15 avril 2021, aux montants supérieurs à 100 euros.

Sources : UFC et INC

Rédacteur : Tony MORALES

Pour plus d'informations et en cas de litige

Posez une question : <https://www.quechoisir.org/soumettre-un-litige-n48324/>

Prenez un Rendez-vous : https://www.quechoisir.org/un-litige/rv_en_ligne?al=622

Association Locale UFC QUE CHOISIR de l'Artois

RNA : W621000161, Siret : 32774497500019

16 rue Aristide Briand – 62000- ARRAS ☎ : 03 21 23 22 97 du lundi au vendredi
Site internet <https://artois.ufcquechoisir.fr/> courriel : contact@artois.ufcquechoisir.fr

[Twitter](https://twitter.com/UFC_Artois) : @UFC_Artois