LE PREMIER
LEARNING NUGGET PARMI
UNE SÉRIE DE WEBINAIRES.

LEARNING NUGGET
#1

# 3D Secure

**3D Secure – Le titulaire de carte comme troisième domaine de validation d'une transaction**

Le commerce électronique et les transactions en ligne revêtent une importance croissante. La crise du coronavirus a encore accéléré cette tendance. Ainsi, le besoin renforcé de sécurité dans le processus de paiement par Internet occupe désormais aussi le centre de la scène.

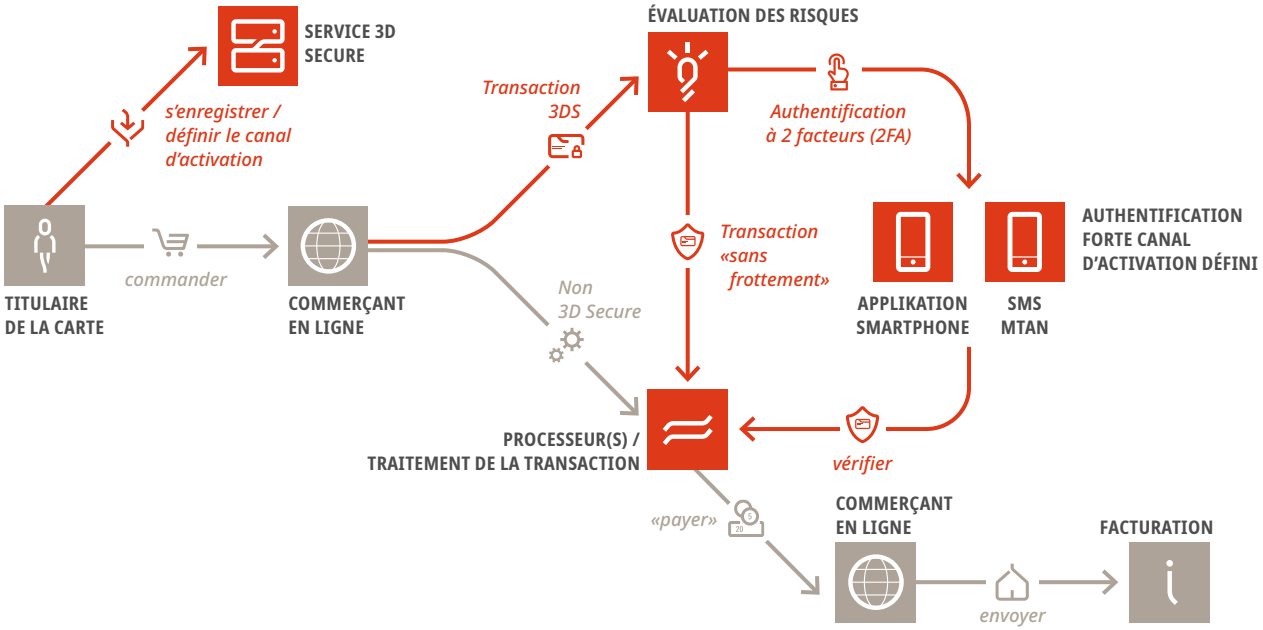
Par conséquent, 3D Secure Service, un standard de sécurité, a été initié par les systèmes de cartes (Mastercard et Visa). Il est géré par le Payment Card Industry Data Security Standard (PCI DSS).

Sans 3D Secure (3DS), l'examen des transactions a lieu uniquement entre le commerçant en ligne et la banque de l'acheteur. Avec 3DS, les paiements en ligne sont sécurisés par la «structure des trois domaines». Le titulaire de carte s'authentifie en plus en tant que troisième domaine pour vérifier la transaction en ligne.

Le paiement sécurisé sur Internet est caractérisé par trois facteurs de sécurité différents:

- **Le facteur basé sur la connaissance,**
  par ex. PAN, date d'expiration et code de sécurité
- **Le facteur possessif,**
  par ex. smartphone, n° de téléphone portable, etc.
- **Le facteur biométrique,**
  par ex. reconnaissance d'iris, empreinte digitale

Dans le cas d'une transaction de commerce électronique sans 3DS, un seul facteur est pris en compte: le facteur basé sur la connaissance. Afin d'assurer une authentification forte, il est toutefois nécessaire d'appliquer un facteur supplémentaire. Dans les versions précédentes du standard, un deuxième facteur basé sur la connaissance était utilisé pour garantir une authentification forte, comme la fourniture d'un mot de passe statique. Depuis ce temps, le standard a évolué.



**De l'authentification statique à l'authentification dynamique**
Les nouvelles cartes de débit disposent de 3D Secure 2 («3DS2»). Le facteur d'authentification est désormais dynamique. Cela signifie que l'élément statique et basé sur la connaissance a été remplacé par un mécanisme de validation dynamique. Pour ce faire, le titulaire de carte reçoit une demande de vérification générique via un canal de validation précédemment fourni en vue de son authentification. Cette solution offre davantage de sécurité aux titulaires de cartes et réduit le risque de fraude.

Ainsi, une valeur unique, d'une validité limitée dans le temps, est générée pour chaque transaction et envoyée pour vérification au titulaire de carte via le canal préalablement authentifié. Il peut s'agir d'un code envoyé par SMS au numéro de téléphone portable enregistré du titulaire de carte (également appelé «mTAN») ou un code technique unique dans une application préalablement enregistrée et cryptée du titulaire de carte.

**3D Secure et commerçants en ligne**
La décision d'une transaction en ligne soit sous forme d'une transaction 3D Secure soit d'une transaction de commerce électronique «normale» incombe au commerçant en ligne. Si le commerçant en ligne n'utilise pas le standard, c'est lui qui supporte le risque de «chargeback» ou de rétrofacturation. En conséquence, il devra prendre en charge les coûts en cas de réclamation d'une transaction. Si un commerçant en ligne opte pour 3D Secure, il transfère ce risque à la banque du titulaire de carte.

**3D Secure 2 – l'expérience utilisateur mise en valeur**
Le facteur de sécurité supplémentaire qu'offre 3D Secure suppose que le client effectue une étape supplémentaire dans le processus d'achat, ce qui conduit à davantage d'abandons de commandes, à en croire les commerçants en ligne. Afin d'optimiser l'expérience utilisateur, une composante supplémentaire a été introduite dans le cadre du nouveau standard 3D Secure 2 (3DS2): le risque de fraude est analysé en amont et permet un examen du risque. Par conséquent, il est désormais possible de classer les transactions 3DS par catégorie de risque. En fonction de sa catégorie de risque, une transaction peut alors être traitée différemment. Une constellation de transaction avec un risque de fraude minime peut désormais alors avoir lieu de manière «frictionless», c'est-à-dire sans interaction supplémentaire du titulaire de carte. Cette classification et la décision du type de standard 3DS (authentification forte avec validation à deux facteurs ou «frictionless») appartiennent à la banque, car elle continue de supporter le risque de chargeback dans le cas d'une transaction 3DS.

**«Fournir un canal sûr pour la validation des paiements» – Enrollment d'une caractéristique d'authentification**
Une condition préalable pour une authentification forte lors de la vérification de transactions en ligne est que le titulaire de carte s'enregistre lui et sa carte pour 3DS2 et fournisse un canal d'authentification sûr. Cette procédure est qualifiée d'«Enrollment».

Pour l'Enrollment, soit l'application d'authentification 3DS du titulaire de carte, soit le numéro de téléphone portable correspondant pour la solution mTAN est enregistré sur le «3D Secure Server» du fournisseur de services (par ex. SIX). Il s'agit du canal défini pour les vérifications futures de transactions en ligne sûres utilisant 3DS par un second facteur possessif (2FA).

Pour l'enregistrement et l'Enrollment, il est nécessaire de garantir que le titulaire de carte soit bien celui qui a enregistré le canal de vérification. Il existe différentes possibilités de le garantir. Soit le titulaire de carte reçoit un code d'enregistrement unique via un autre canal préalablement vérifié (par ex. la poste, l'e-banking, etc.), ou la procédure est effectuée directement dans une zone contrôlée par la banque, telle que l'e-banking ou le mobile banking.

SAVOIR PLUS

**SIX BBS SA**
Hardturmstrasse 201
Case postale
8021 Zurich
T +41 58 399 4012
pm.debit@six-group.com