THE FIRST
LEARNING NUGGET OF
A WEBINAR SERIES.

LEARNING NUGGET
#1

3D Secure

3D Secure – Card Holder as Third-Party Approval Domain for Transactions
E-commerce and online transactions are becoming increasingly important. The corona crisis has accelerated this trend. Therefore, more attention is paid to the need of improving the security of payments via the Internet.

This is why card schemes (Mastercard and Visa) have initiated a security standard managed by the Payment Card Industry Data Security Standard (PCI DSS): the 3D Secure Service.

Without 3D Secure (3DS), transactions are only checked between the online merchant and the purchaser's bank. 3DS allows to secure online payments with the so-called "three-domain structure". The card holder authenticates themselves additionally as a third-party domain to verify the online transaction.

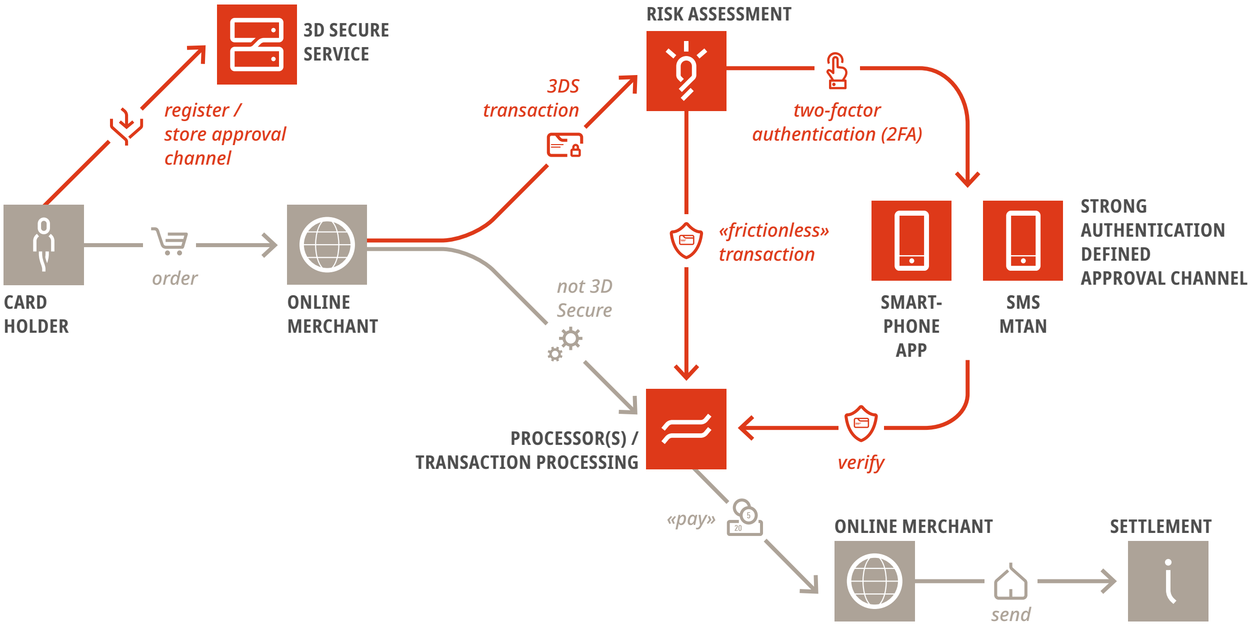
Secure payments in the Internet differentiate between three different security factors:

Knowledge-based,
e.g. PAN, expiry date and security code

Proprietary,
e.g. smartphone, mobile number, etc.

Biometric,
e.g. iris recognition, fingerprint

An e-commerce transaction without 3DS involves only one factor – the knowledge-based factor. However, strong authentication requires another factor. Previously, for the purposes of strong authentication, the standard entailed using another knowledge-based factor, such as a static stored password. It has evolved since then.


3D SECURE SERVICE
register / store approval channel
CARD HOLDER
order
ONLINE MERCHANT
3DS transaction
RISK ASSESSMENT
two-factor authentication (2FA)
«frictionless» transaction
not 3D Secure
SMART-PHONE APP
SMS MTAN
STRONG AUTHENTICATION DEFINED APPROVAL CHANNEL
PROCESSOR(S) / TRANSACTION PROCESSING
verify
«pay»
ONLINE MERCHANT
send
SETTLEMENT

3D Secure and Online Merchants

The decision whether an online transaction is carried out as a 3D Secure transaction or as a "normal" e-commerce transaction is made by the online merchant. Should the online merchant not use the standard, they bear the chargeback risk. As a consequence, they cover the costs if the transaction fails. Should the online merchant decide to use 3D Secure, this risk is assumed by the card holder's bank.

3D Secure 2 – Centered Around User Experience

The additional security factor in 3D Secure requires the customer to make an additional step in the buying process. However, online merchants think it will increase the number of canceled purchases. To optimize user experience, another component has been embedded into the new 3D Secure 2 (3DS2) standard that carries out upstream analysis of the transaction's risk of fraud and facilitates a risk assessment. Therefore, it is now possible to categorize a 3DS transaction according to its risk and process it differently depending on this risk classification. A transaction with a very low risk of fraud can thus be carried out "frictionless", so without any additional interaction with the card holder. This classification and decision on how to proceed with 3DS – strong authentication with two-factor approval or "frictionless" – is at the discretion of the bank, since it still bears the chargeback risk of a 3DS transaction.

3D Secure 2 – Centered Around User Experience

The additional security factor in 3D Secure requires the customer to make an additional step in the buying process. However, online merchants think it will increase the number of canceled purchases. To optimize user experience, another component has been embedded into the new 3D Secure 2 (3DS2) standard that carries out upstream analysis of the transaction's risk of fraud and facilitates a risk assessment. Therefore, it is now possible to categorize a 3DS transaction according to its risk and process it differently depending on this risk classification. A transaction with a very low risk of fraud can thus be carried out "frictionless", so without any additional interaction with the card holder. This classification and decision on how to proceed with 3DS – strong authentication with two-factor approval or "frictionless" – is at the discretion of the bank, since it still bears the chargeback risk of a 3DS transaction.

"Providing a Secure Channel for Payment Approval" – Enrollment of Authentication Information

Strong authentication when verifying online transactions assumes that the card holder has registered themselves and their card to 3DS2 and stored a secure authentication channel. This process is called "enrollment".

Enrollment involves storing either the card holder's 3DS authentication app or the respective mobile number for the mTAN solution on the "3DS Server" of the service provider (e.g. SIX). This is the defined channel for future verification of secure online transactions with 3DS through a possessive second factor (2FA).

In case of registration and enrollment, it must be ensured that the card holder is the person storing the secure verification channel. There are various possibilities to make sure it is the case. The card holder may receive a unique registration code via another pre-registered channel (e.g. post, e-banking, etc.) or it can be done directly via a channel checked by the bank, such as mobile banking or e-banking.

LEARN MORE

SIX BBS Ltd
Hardturmstrasse 201
P. O. Box
8021 Zurich
T +41 58 399 4012
pm.debit@six-group.com