DAS ERSTE
LEARNING NUGGET
EINER WEBINAR-SERIE

LEARNING NUGGET
#1

3D Secure

3D Secure – der Karteninhaber als dritte Freigabe-Domäne einer Transaktion

E-Commerce und Online-Transaktionen gewinnen immer mehr an Bedeutung. Die Coronakrise hat diesen Trend beschleunigt. Somit rückt auch das Bedürfnis nach mehr Sicherheit beim Bezahlen im Internet in den Vordergrund.

Dementsprechend wurde durch die Karten-Schemes (Mastercard und Visa) ein Sicherheitsstandard initiiert, der durch die Payment Card Industry Data Security Standard (PCI DSS) verwaltet wird – der 3D Secure Service.

Ohne 3D Secure (3DS) findet die Transaktionsprüfung nur zwischen dem Online-Händler und der Käuferbank statt. Mit 3DS werden Online-Zahlungen durch die so genannte «Drei-Domänen-Struktur» abgesichert. Der Karteninhaber authentifiziert sich zusätzlich als dritte Domäne, um die Online-Transaktion zu verifizieren.

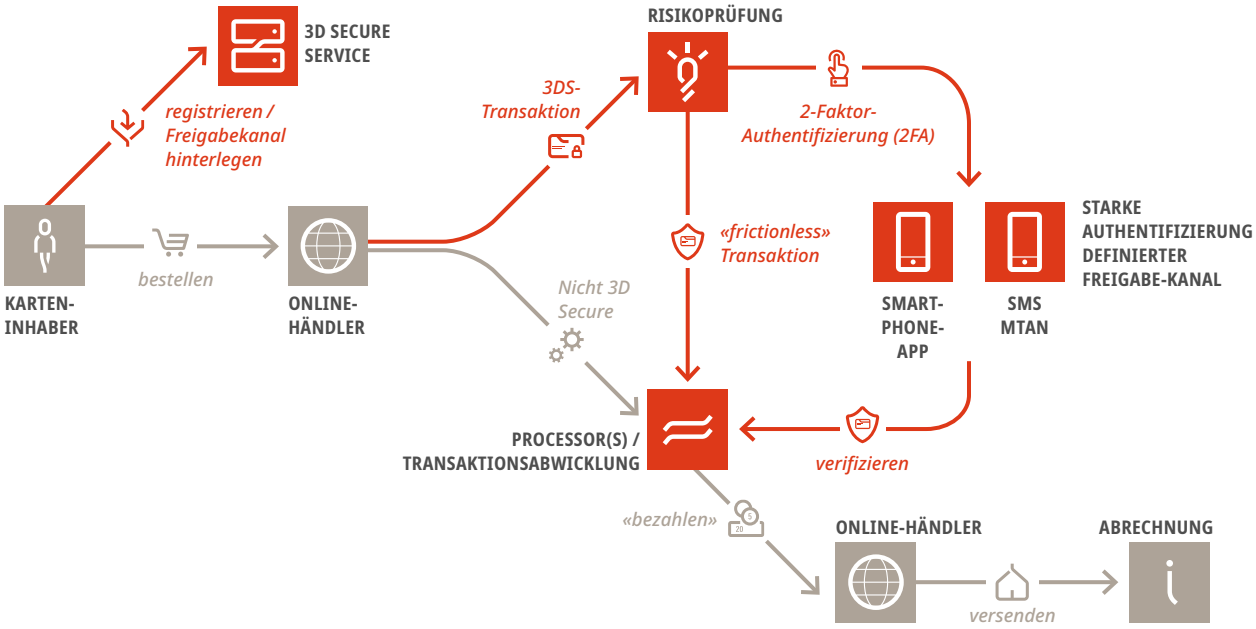
Sicheres Bezahlen im Internet unterscheidet drei verschiedene Sicherheitsfaktoren:

Wissensbasiert,
z. B. PAN, Ablaufdatum und Sicherheitscode

Besitzanzeigend,
z. B. Smartphone, Mobile-Nummer usw.

Biometrisch,
z. B. Iriserkennung, Fingerabdruck

In einer E-Commerce-Transaktion ohne 3DS kommt nur ein Faktor, der wissensbasierte, zum Zug. Für eine starke Authentifizierung wird jedoch ein zweiter Faktor benötigt. In früheren Ausprägungen des Standards wurde für die starke Authentifizierung ein zweiter, wissensbasierter Faktor wie ein statisch hinterlegtes Passwort verwendet. Seither hat sich der Standard weiterentwickelt.



Von der statischen zur dynamischen Authentifizierung
Die neuen Debitkarten verfügen über 3D Secure 2 («3DS2»). Der Authentifizierungsfaktor ist nun dynamisch. Das heisst, dass das statische und wissensbasierte Element durch einen dynamischen Freigabemechanismus abgelöst wurde. Dabei wird dem Karteninhaber eine generische Verifizierungsanfrage an einen vorgängig hinterlegten Freigabekanal zur Authentifizierung gesendet. Das bietet den Karteninhabern mehr Sicherheit und vermindert das Betrugsrisiko.

So wird pro Transaktion ein zeitlich begrenzt gültiger, einmaliger Wert generiert und dem Karteninhaber an den vorgängig authentifizierten Kanal zur Verifizierung gesendet. Das kann ein einmaliger SMS-Code an die registrierte Mobile-Nummer des Karteninhabers sein (auch «mTAN» genannt) oder ein einmaliger technischer Code in eine vorgängig registrierte und verschlüsselte App des Karteninhabers.

3D Secure und Online-Händler
Ob eine Online-Transaktion als 3DS-Transaktion oder als «normale» E-Commerce-Transaktion durchgeführt wird, liegt in der Entscheidung des Online-Händlers. Sofern der Online-Händler den Standard nicht verwendet, trägt er das Chargeback-Risiko. Als Konsequenz bleibt er bei der Beanstandung einer Transaktion auf den Kosten sitzen. Wenn ein Online-Händler sich für 3D Secure entscheidet, lagert er dieses Risiko an die Bank des Karteninhabers aus.

3D Secure 2 – User Experience rückt in den Vordergrund
Der zusätzliche Sicherheitsfaktor in 3D Secure bedingt, dass der Kunde einen additionalen Schritt im Kaufprozess machen muss. Dies führt laut Online-Händlern jedoch zu mehr Kaufabbrüchen. Um die User Experience zu optimieren, wurde bei den neuen «3D Secure 2 (3DS2)»-Standards eine weitere Komponente eingebaut, die vorgelagert das Betrugsrisiko einer Transaktion analysiert und eine Risikoprüfung erlaubt. Entsprechend ist es nun möglich, eine 3DS-Transaktion in Risikokategorien zu unterteilen und eine Transaktion je nach Risikoklassifizierung unterschiedlich zu behandeln. Eine Transaktionskonstellation mit sehr geringem Betrugsrisiko kann somit jetzt auch «frictionless», also ohne zusätzliche Interaktion mit dem Karteninhaber, stattfinden. Diese Klassifizierung und die Entscheidung über die Art der 3DS-Abhandlung – starke Authentifizierung mit Zwei-Faktor-Freigabe oder «frictionless» – liegt im Ermessen der Bank, da diese nach wie vor bei einer 3DS-Transaktion das Chargeback-Risiko trägt.

Einen «sicheren Kanal für Zahlungsfreigabe hinterlegen» – Enrollment eines Authentifizierungsmerkmals
Voraussetzung für eine starke Authentifizierung bei der Verifizierung von Online-Transaktionen ist, dass der Karteninhaber sich und seine Karte für 3DS2 registriert und einen sicheren Authentifizierungskanal hinterlegt. Dieser Vorgang wird als «Enrollment» bezeichnet.

Beim Enrollment wird entweder die 3DS-Authentifizierungs-App des Karteninhabers oder die entsprechende Mobile-Nummer für die mTAN-Lösung auf dem «3DS-Server» des Service Providers (z. B. SIX) hinterlegt. Das ist der definierte Kanal für die zukünftige Verifizierung von sicheren Online-Transaktionen mit 3DS durch einen besitzanzeigenden Zweitfaktor (2FA).

Für die Registrierung und das Enrollment muss sichergestellt werden, dass der Karteninhaber derjenige ist, der den sicheren Verifizierungskanal hinterlegt hat. Um das zu gewährleisten, gibt es verschiedene Möglichkeiten. Entweder erhält der Karteninhaber einen einmaligen Registrierungscode über einen anderen vorgängig verifizierten Kanal (z. B. Post, E-Banking usw.) oder es erfolgt direkt in einem durch die Bank geprüften Bereich, z. B. im Mobile- oder E-Banking.

WEITERE INFORMATIONEN HIER

SIX BBS AG
Hardturmstrasse 201
Postfach
8021 Zürich
T +41 58 399 4012
pm.debit@six-group.com