# Sonderbedingungen für das 3D Secure-Verfahren bei Karten-Online-Transaktionen

Stand: 10/2022

Die nachfolgenden Bedingungen gelten für die Debitkarten und Kreditkarten der Postbank – eine Niederlassung der Deutsche Bank AG (nachfolgend „Bank" genannt), die für die Online-Nutzung zugelassen sind. Sie sind in Verbindung mit den Bedingungen für die Kreditkarten und den Bedingungen für die Postbank Card plus / Postbank Business Card plus zu lesen.

## 1. Gegenstand, Definition

1.1 Die Bank ermöglicht den Inhabern ihrer für die Online-Nutzung zugelassenen Debitkarten und Kreditkarten die Teilnahme am 3D Secure-Verfahren, das Händler im Internet zur Authentifizierung einer Debitkarten- oder Kreditkarten-Transaktion vorsehen können.

1.2 Das 3D Secure-Verfahren (bei Mastercard als „Identity Check", bei VISA als „Visa Secure" bezeichnet) ist ein Verfahren zur Authentifizierung des Debitkarten- oder Kreditkarteninhabers bei Online-Transaktionen.

1.3 Die Bank ist berechtigt, einen Debitkarten- oder Kreditkartenumsatz im Internet abzulehnen, den der Debitkarten- oder Kreditkarteninhaber bei einem Unternehmen, das den Einsatz des 3D Secure-Verfahrens für diese Transaktion vorsieht, ohne dessen Nutzung tätigen will.

## 2. Teilnahmevoraussetzungen

2.1 Mit Besitz einer für die Online-Nutzung zugelassenen Debitkarte oder Kreditkarte der Bank ist eine Nutzung des 3D Secure-Verfahrens möglich.

2.2 Für die Authentifizierung im 3D Secure-Verfahren bietet die Bank dem Debitkarten- oder Kreditkarteninhaber verschiedene Verfahren an:

a. Authentifizierung per BestSign-App
Um sich über die BestSign-App der Bank im 3D Secure-Verfahren zu authentifizieren, muss der Debitkarten- oder Kreditkarteninhaber ein Online-Banking-Kunde der Bank sein, die App auf seinem mobilen Endgerät installiert und die Zusendung von Push-Nachrichten durch die App aktiviert haben. Zusätzlich ist die Festlegung einer vom Debitkarten- oder Kreditkarteninhaber gewählten Passwortes und – sofern gewünscht – eines von der Bank zugelassenen biometrischen Merkmals, z. B. eigener Fingerabdruck (Fingerprint), erforderlich.

b. Authentifizierung per mobileTAN und Internet-PIN
Um die bei einer 3D Secure Debitkarten- oder Kreditkartenzahlung per mobiler Transaktionsnummer (nachfolgend „mobileTAN") erfolgende Authentifizierung vornehmen zu können, muss bei der debitkarten- oder kreditkartenausgebenden Bank, z. B. über deren Online-Banking, für den Debitkarten- oder Kreditkarteninhaber eine jederzeit wieder änderbare Mobiltelefonnummer hinterlegt worden sein.

Ebenso muss der Debitkarten- oder Kreditkarteninhaber über das Online-Banking für jede seiner für die Online-Nutzung zugelassenen Debitkarten und Kreditkarten eine eigenständige selbst gewählte Internet-PIN vergeben, die dann zusammen mit der mobileTAN zur Authentifizierung einzugeben ist. Die selbst gewählte Internet-PIN kann vom Debitkarten- oder Kreditkarteninhaber jederzeit über das Online-Banking geändert werden.

## 3. Verfahren der Authentifizierung per BestSign-App

3.1 Hat der Debitkarten- oder Kreditkarteninhaber die App auf seinem mobilen Endgerät installiert und der Zusendung von Push-Nachrichten zugestimmt, erfolgt die Authentifizierung im 3D Secure-Verfahren über die BestSign-App. Wird während einer Transaktion im Online-Handel mit der Debitkarte oder Kreditkarte des Karteninhabers eine Authentifizierung im 3D Secure-Verfahren verlangt, erhält der Karteninhaber hierüber eine Benachrichtigung auf seinem mobilen Endgerät. Die Authentifizierung der Online-Transaktion erfolgt dann mittels Öffnen der BestSign-App und Bestätigen der Transaktion mittels der hinterlegten Legitimationsvariante, z. B. Passwort.

3.2 Hat sich der Debitkarten- oder Kreditkarteninhaber für die Nutzung der BestSign-App als Authentifizierungslösung für Online-Transaktionen entschieden, gilt dieses Verfahren für alle bestehenden und künftigen Debitkarten und Kreditkarten des Karteninhabers bei der Bank.

3.3 Ist eine Authentifizierung der Online-Transaktion mit der Debitkarte oder Kreditkarte des Karteninhabers im Einzelfall nicht mit der BestSign-App möglich, z. B. mangels Internetverbindung der BestSign-App, kann auf die Authentifizierung mittels mobileTAN und Internet-PIN (s. 4.) gewechselt werden.

## 4. Verfahren der Authentifizierung per mobileTAN und Internet-PIN

4.1 Nutzt der Debitkarten- oder Kreditkarteninhaber nicht die BestSign-App zur Authentifizierung von Online-Transaktionen, erfolgt diese mittels der vorher vom Debitkarten- oder Kreditkarteninhaber festgelegten Internet-PIN sowie einer mobileTAN, die die Bank via SMS (Short Message Service) an die der Bank mitgeteilte Mobiltelefonnummer des Debitkarten- oder Kreditkarteninhabers versendet.

4.2 Die in einem solchen Fall per SMS übermittelte, mindestens sechsstellige mobileTAN ist dann zur Authentifizierung der Online Debitkarten- oder Kreditkartentransaktion einzugeben. Zum Abgleich werden dem Debitkarten- oder Kreditkarteninhaber auf dem Bildschirm die letzten Stellen der Mobiltelefonnummer angezeigt, an die die mobileTAN per SMS übermittelt wird.

4.3 Die SMS wird von der Bank kostenlos zur Verfügung gestellt. Die Bank weist jedoch darauf hin, dass für den Empfang von SMS im Ausland gegebenenfalls zusätzliche Gebühren des Mobilfunkanbieters (Roaming) anfallen können.

4.4 Zusätzlich zur Eingabe der mobileTAN ist die vom Debitkarten- oder Kreditkarteninhaber für seine Debitkarte oder Kreditkarte vorab für die Online-Nutzung festgelegte Internet-PIN einzugeben.

4.5 Eine erfolgreiche Authentifizierung der Online-Transaktion mit der Debitkarte oder Kreditkarte ist nur möglich, wenn sowohl die versandte mobileTAN wie auch die vom Debitkarten- oder Kreditkarteninhaber festgelegte Internet-PIN korrekt eingegeben wurden.

## 5. Datenverarbeitung und Dienstleister

5.1 Bei einer 3D Secure Debitkarten- oder Kreditkartenzahlung werden die für die Durchführung der Transaktion und deren Authentifizierung erforderlichen personenbezogenen Daten sowie Karten-, Geräte-, und Transaktionsdaten gespeichert.

## 6. Besondere Sorgfaltspflichten

6.1 Für die Sicherheit von SMS, die auf dem Mobiltelefon eingehen, hat der Kunde durch geeignete Maßnahmen (z. B. durch eine passwortgeschützte Zugangssperre) zu sorgen. Die Bank haftet nicht für den Fall, dass das Mobiltelefon verloren, gestohlen oder weitergegeben wird und dadurch Dritte ggf. Zugriff auf die SMS erhalten und diese unberechtigt nutzen können.

6.2 Der Debitkarten- oder Kreditkarteninhaber hat die ihm von der debitkarten- oder kreditkartenausgebenden Bank per Push-Nachricht über die BestSign-App oder SMS übermittelten Daten auf Übereinstimmung abzugleichen. Bei Unstimmigkeiten ist die Transaktion abzubrechen und die Bank zu informieren.

6.3 Der Debitkarten- oder Kreditkarteninhaber hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von seiner für die Online-Nutzung zugelassenen Debitkarten und Kreditkarten vergebene Internet-PIN erlangt.