DKB
Deutsche Kreditbank AG

Sonderbedingungen für das 3D Secure-Verfahren bei Internet-Zahlungen mit der DKB-Kreditkarte

1 Gegenstand, Definition, Ablehnungsmöglichkeit

1) Die Deutsche Kreditbank AG (nachfolgend „DKB AG“) ermöglicht dem Inhaber einer DKB-Kreditkarte (nachfolgend „Kreditkarte“) die Teilnahme am 3D Secure-Verfahren, das Kartenakzeptanzstellen (nachfolgend „Händler“) zur Absicherung eines Zahlungsvorgangs mit der Kreditkarte im Internet vorsehen können.

2) Das 3D Secure-Verfahren (bei Mastercard als „Mastercard® SecureCodeTM“, bei VISA als „Verified by Visa“ bezeichnet) ist ein Verfahren zur Authentifizierung des Karteninhabers. In dem Verfahren wird die Identität des Karteninhabers überprüft und es dient der Vermeidung von missbräuchlichen Umsätzen.

3) Die DKB AG ist berechtigt, einen Kreditkartenumsatz im Internet abzulehnen, den der Karteninhaber bei einem Händler, der den Einsatz des 3D Secure-Verfahrens für diese Transaktion vorsieht, ohne dessen Nutzung tätigen will.

4) Diese Bedingungen ergänzen die Bedingungen für die Mastercard und Visa Card (Kreditkarten). Im Falle von Widersprüchen zwischen den Kreditkartenbedingungen und den vorliegenden Sonderbedingungen gehen die Kreditkartenbedingungen vor.

2 Teilnahmevoraussetzungen, Registrierung

1) Zur Teilnahme am 3D Secure-Verfahren ist eine Registrierung erforderlich. Der Karteninhaber muss seine Registrierung zur Teilnahme am 3D Secure-Verfahren auf der Homepage der DKB AG (www.dkb.de) oder während einer Internet-Zahlung vornehmen.

2) Um sich zur Teilnahme am 3D Secure-Verfahren zu registrieren, benötigt der Karteninhaber seine Kreditkartennummer, ein mobiles Endgerät (Smartphone oder Tablet) mit der Möglichkeit der Nutzung der App „DKB-Secure-Card“ (nachfolgend „App“) oder mit der Möglichkeit des SMS-Empfangs, sowie den Identifikations-Code, der ihm entweder während der Registrierung bereits vorliegt oder von ihm in diesem Moment beantragt werden kann.

3) Für die Erstregistrierung zum 3D Secure-Verfahren wird jedem Karteninhaber ein Identifikations-Code an seine hinterlegte Anschrift oder im Verwendungszweck einer Überweisung auf sein Abrechnungskonto übermittelt. Dieser Identifikations-Code ist zur Bestätigung der Anmeldung einzugeben. Die Zusendung des Identifikations-Codes kann bis zu vier Werktage dauern. In diesem Fall kann das Registrierungsverfahren zunächst nicht vollständig abgeschlossen werden.

4) Im Rahmen des Registrierungsprozesses legt der Karteninhaber fest, mit welcher Variante des 3D Secure-Verfahrens er sich in der Zukunft authentifizieren möchte. Es besteht Wahlmöglichkeit zwischen einer App-basierten Variante und einer mTAN basierten Lösung. Die DKB AG behält sich vor, nicht beide Verfahren anzubieten.

5) Entscheidet sich der Karteninhaber für das App-basierte Verfahren, so wird er im Rahmen des Registrierungsprozesses aufgefordert, die App auf sein mobiles Endgerät zu laden und sie mit seiner Kreditkarte zu verknüpfen. Dies geschieht durch die Eingabe eines individuellen Codes in der App, welcher im Registrierungsprozess im Internet angezeigt wird. Neben dieser Verknüpfung vergibt der Karteninhaber eine PIN, die zukünftig für die Nutzung der App benötigt wird.

6) Wählt der Karteninhaber das mTAN Verfahren, so legt er im Registrierungsprozess die Rufnummer seines mobilen Endgerätes fest, an das zukünftig die zur Zahlungsfreigabe erforderliche SMS mit der mTAN übermittelt werden soll. Darüber hinaus legt er im Rahmen der Registrierung eine Antwort auf eine Sicherheitsfrage fest, die ihm systemseitig ggf. als zusätzliche Absicherung bei Internet-Zahlungen zur Beantwortung gestellt werden kann.

7) Die Registrierung für das 3D Secure-Verfahren erfolgt über eine verschlüsselte Internetverbindung. Im Registrierungsprozess sowie beim Herunterladen und der Nutzung der App können Kosten für eine Internetverbindung durch das mobile Endgerät anfallen. Die Nutzung der App zum Zwecke der Authentifizierung von Internet-Zahlungen ist auch offline möglich.

3 Authentifizierung einer 3D Secure-Kartenzahlung

1) Nutzt der Karteninhaber das mTAN Verfahren, gilt: Sobald eine Verified by Visa/Mastercard SecureCodeTM Transaktion veranlasst wird, erhält der Karteninhaber eine SMS mit Transaktionsdetails und pro Transaktion generierter TAN auf sein mobiles Endgerät zugestellt. Durch Eingabe der erhaltenen TAN und korrekter Beantwortung der ggf. gestellten Sicherheitsfrage im Kaufprozess wird die Transaktion bestätigt.

2) Nutzt der Karteninhaber das App-basierte Verfahren, gilt: Sobald eine Verified by Visa/Mastercard SecureCodeTM Transaktion veranlasst wird, erhält der Karteninhaber auf seinem mobilen Endgerät eine Benachrichtigung. Nach Öffnen der App werden die Transaktionsdetails angezeigt. Durch Klicken auf „Bestätigen“ und Eingabe der PIN in der App wird die Transaktion bestätigt.

3) Die Nutzung der gesicherten Authentifizierung für Internet-Zahlungen kann für bestimmte Transaktionen zur Risikoprävention eingeschränkt sein.

4 Datenschutz und Einschaltung Dritter

1) Im Rahmen der Registrierung wird der Karteninhaber aufgefordert, seine Kreditkartennummer einzugeben. Diese wird ausschließlich für die dynamische Legitimation im Rahmen des 3D Secure- Verfahrens verwendet. Eine Verwendung oder Weitergabe der Daten zu anderen Zwecken erfolgt nicht.

2) Zur Abwicklung des 3D Secure-Verfahrens setzt die DKB AG Dienstleister ein, deren Geschäftszweck die Registrierung, Authentifizierung und Risikoprüfung von Internet-Bezahlvorgängen umfasst. Befindet sich der Sitz eines Dienstleisters in einem Land außerhalb der Europäischen Union oder außerhalb eines Landes, das dem Abkommen zum Europäischen Wirtschaftsraum beigetreten ist, muss dieser über ein angemessenes Datenschutzniveau im Sinne des Bundesdatenschutzgesetzes verfügen und dieses gegenüber der DKB AG nachweisen, es sei denn, dass eine Angemessenheitsentscheidung der Europäischen Kommission gemäß Art. 25 Abs. 6 der Richtlinie 95/46/EG vom 24. Oktober 1995 (EU-Datenschutzrichtlinie) zugunsten des Landes vorliegt, in dem dieser Dienstleister seinen Sitz hat.

3) Bei der Registrierung für das 3D Secure-Verfahren werden einzelne persönliche Daten des Karteninhabers aus dem Registrierungsprozess beim Dienstleister hinterlegt und mit bestehenden Daten in dem technischen System der DKB AG oder ihres hierzu beauftragten Dienstleisters abgeglichen.

4) Es wird darauf hingewiesen, dass durch die Registrierung und Nutzung der App Dritte (z. B. Apple Inc., Google Inc. bzw. Microsoft) auf eine bestehende Kundenbeziehung mit der DKB AG schließen können. Es wird weiterhin darauf hingewiesen, dass bei der Registrierung und Nutzung der App Daten (z. B. Registrierungscode, Informationen über den Händler, Transaktionsbetrag usw.) unter anderem über das Internet transportiert werden. Hierbei werden die Datenpakete (außer Absender und Empfänger) verschlüsselt übermittelt. Dritte können auf bestehende Geschäftsbeziehungen schließen. Die Datenübermittlung kann im Internet über Drittstaaten erfolgen, auch wenn Absender und Empfänger im selben Land angesiedelt sind.

5 Sorgfaltspflichten des Karteninhabers

1) Der Karteninhaber
   a) hat das Risiko eines unberechtigten Zugriffs auf sein mobiles Endgerät u. a. durch geeignete Schutzmaßnahmen zu minimieren (z. B. PIN auf mobiles Endgerät).
   b) hat das Betriebssystem des von ihm verwendeten Endgerätes auf dem neuesten Stand zu halten.
   c) hat die App nur aus offiziellen App-Stores (iTunes, Google Playstore, Windows Store) herunterzuladen und dafür vorgesehene Updates regelmäßig durchzuführen.

2) Der Karteninhaber hat die Übereinstimmung der während eines Einkaufs zur Authentifizierung übermittelten Transaktionsdaten mit den von ihm für die Transaktion vorgesehenen Daten abzugleichen. Er ist verpflichtet, der DKB AG unverzüglich zu melden, wenn er auf seinem mobilen Endgerät die Aufforderung zur Genehmigung einer Transaktion erhält, die er nicht getätigt hat. Bei Unstimmigkeiten ist die Transaktion abzubrechen.

3) Die DKB AG haftet nicht für den Fall, dass das mobile Endgerät verloren, gestohlen oder weitergegeben wird und dadurch Dritte ggf. Zugriff auf SMS erhalten und diese unberechtigt nutzen können.

4) Das mobile Endgerät, auf welches die mTAN per SMS gesandt werden soll, darf nicht gleichzeitig für den Kreditkarteneinsatz im Internet genutzt werden. Die Kommunikationskanäle sind getrennt zu halten.

6 Abmeldung vom 3D Secure-Verfahren

1) Der Karteninhaber kann sich jederzeit von der Teilnahme am 3D Secure-Verfahren abmelden.

2) Wenn sich der Karteninhaber abgemeldet hat, ist es ihm nicht mehr möglich, seine Kreditkarte für Internet-Bezahlvorgänge bei am 3D Secure-Verfahren teilnehmenden Händlern einzusetzen. Um die Kreditkarte wieder bei diesen Händlern einsetzen zu können, ist eine Neuregistrierung erforderlich.

3) Wenn der Karteninhaber bereits in der Vergangenheit das 3D Secure-Verfahren genutzt hat, wird er mit Durchführung einer Registrierung automatisch vom bestehenden 3D Secure-Verfahren abgemeldet. Eine Rücksetzung auf das alte Verfahren ist dann nicht mehr möglich.

7 Verantwortlichkeit und Haftung

Die DKB AG kann weder den störungsfreien noch den ununterbrochenen Zugang zur App gewährleisten. Sie trägt daher keine Gewähr für die ständige Verfügbarkeit des 3D Secure-Verfahrens und haftet nicht für Schäden infolge von Störung, Unterbrechungen (inkl. systembedingter Wartungsarbeiten) oder Überlastungen der beteiligten IT-Systeme. Sie übernimmt keine Gewähr für Leistungen, die im Verantwortungsbereich anderer beteiligter Dienstleister liegen. Die DKB AG übernimmt außerdem keine Haftung bei Manipulationen des mobilen Endgerätes (z. B. Jailbreaking, Rooting).

8 Entgelt

Das Entgelt für die Teilnahme am 3D Secure-Verfahren ergibt sich aus dem Preis- und Leistungsverzeichnis.