DKB
Deutsche Kreditbank AG

Hilton HONORS

Sonderbedingungen für das 3D Secure-Verfahren (Hilton Honors Credit Card)

1 Gegenstand, Definition

1) Das 3D Secure-Verfahren findet Anwendung, wenn eine Hilton Honors Credit Card (nachfolgend „Kreditkarte") für einen Zahlungsvorgang im Internet (nachfolgend „Zahlungsvorgang") genutzt wird. Mit Hilfe des 3D Secure-Verfahrens (als „Visa Secure" bezeichnet) wird der Karteninhaber durch die Deutsche Kreditbank AG (nachfolgend „DKB AG") authentifiziert, also seine Identität überprüft. Mit den hierfür vereinbarten Authentifizierungselementen kann sich der Karteninhaber gegenüber der DKB AG als berechtigter Karteninhaber ausweisen. Es dient somit der Vermeidung von missbräuchlichen Umsätzen.

2) Authentifizierungselemente sind
- Wissenselemente, also etwas, das nur der Karteninhaber weiß (hinterlegte Antwort auf Sicherheitsfrage, im Internet-Banking angezeigter Sicherheitscode) und
- Besitzelemente, also etwas, das nur der Karteninhaber besitzt (mobiles Endgerät zum Empfang von einmal verwendbaren Transaktionsnummern (TAN) per SMS, mit der DKB-Banking-App verknüpftes mobiles Endgerät).

3) Die Authentifizierung des Karteninhabers erfolgt, indem der Karteninhaber, wie nachfolgend in Ziff. 2 beschrieben, das Wissenselement und/oder den Nachweis des Besitzelements an die DKB AG übermittelt.

4) Die DKB AG ist berechtigt, den Einsatz der Kreditkarte zu einem Zahlungsvorgang im Internet abzulehnen, wenn der Karteninhaber die vorgesehene Authentifizierung mit dem 3D Secure-Verfahren nicht vornimmt. Falls ein Zahlungsvorgang aufgrund einer Transaktionsrisikoanalyse als Vorgang mit niedrigem Risiko eingestuft wird, kann die DKB AG in diesem Fall auf die Authentifizierung des Karteninhabers mit Hilfe des 3D Secure-Verfahrens verzichten.

5) Diese Bedingungen ergänzen die Bedingungen für die Hilton Honors Credit Card (Kreditkarte). Im Falle von Widersprüchen zwischen den Kreditkartenbedingungen und den vorliegenden Sonderbedingungen gehen die Kreditkartenbedingungen vor.

2 Registrierung, Authentifizierung

1) Jeder Inhaber einer gültigen und nicht gesperrten Kreditkarte ist automatisch für das 3D Secure-Verfahren registriert.

2) Für die Authentifizierung im 3D Secure-Verfahren kann der Karteninhaber entweder die DKB-Banking-App oder das smsTAN-Verfahren nutzen. Der Karteninhaber muss seine Kreditkarte für die Variante, die er nutzen möchte, aktivieren. Solange er seine Kreditkarte für keine der beiden Varianten aktiviert hat oder die gewählte Variante nicht zur Verfügung steht (z. B. mangels Mobilfunknetz oder mobiler Datenverbindung), kann er den für das 3D Secure-Verfahren in seinem Hilton Online-Banking angezeigten sechsstelligen Sicherheitscode nutzen. Die DKB AG behält sich vor, weitere Verfahren anzubieten oder angebotene Verfahren wieder abzuschalten.

3) Um mit Hilfe der DKB-Banking-App im 3D Secure-Verfahren authentifiziert werden zu können, muss der Karteninhaber diese App auf seinem mobilen Endgerät installiert und seine Kreditkarte in der DKB-Banking-App für das 3D Secure-Verfahren aktiviert haben. Wird während eines Zahlungsvorgangs eine Authentifizierung im 3D Secure-Verfahren verlangt, erhält der Karteninhaber eine Benachrichtigung auf seinem mobilen Endgerät. Wenn er daraufhin die DKB-Banking-App öffnet, wird ihm dort eine Bestätigungsseite mit den Transaktionsdetails angezeigt. Mit der Auswahl des Buttons „Bestätigen" auf dieser Bestätigungsseite übermittelt der Karteninhaber den Nachweis des Besitzelements an die DKB AG und kann so authentifiziert werden.

4) Um mit Hilfe einer smsTAN im 3D Secure-Verfahren authentifiziert werden zu können, muss der Karteninhaber in seinem Hilton Online-Banking oder in der DKB-Banking-App seine Kreditkarte für das smsTAN-Verfahren aktiviert und die Antwort zu einer Sicherheitsfrage hinterlegt haben. Wird während eines Zahlungsvorgangs eine Authentifizierung im 3D Secure-Verfahren verlangt, erhält der Karteninhaber eine SMS mit Transaktionsdetails und pro Transaktion generierter smsTAN an die bei der DKB AG hinterlegte Mobilfunknummer. Die smsTAN ist nach der Übersendung fünf Minuten lang gültig. Wird sie in dieser Zeit nicht verwendet, wird sie automatisch ungültig. Gleiches gilt, wenn der Karteninhaber eine neue smsTAN anfordert. Der Karteninhaber wird im Rahmen des Zahlungsvorgangs aufgefordert, die smsTAN auf einer Bestätigungsseite einzugeben. Durch Eingabe der erhaltenen smsTAN und korrekte Beantwortung der gestellten Sicherheitsfrage übermittelt der Karteninhaber den Nachweis des Besitzelements und ggf. das Wissenselement an die DKB AG und kann so authentifiziert werden.

5) Wenn der Karteninhaber seine Kreditkarte weder für die Authentifizierung mit der DKB-Banking-App noch per smsTAN für das 3D Secure-Verfahren aktiviert hat und während eines Zahlungsvorgangs eine Authentifizierung im 3D Secure-Verfahren verlangt wird, erhält der Karteninhaber einen Sicherheitscode mit Transaktionsdetails in seinem Hilton Online-Banking zum Abruf unter Eingabe einer TAN (z. B. pushTAN, chipTAN) bereitgestellt. Der Sicherheitscode ist nach der Übersendung fünf Minuten lang gültig. Wird er in dieser Zeit nicht verwendet, wird er automatisch ungültig. Gleiches gilt, wenn der Karteninhaber einen neuen Sicherheitscode anfordert. Der Karteninhaber wird im Rahmen des Zahlungsvorgangs aufgefordert, den Sicherheitscode auf einer Bestätigungsseite einzugeben. Durch Eingabe des bereitgestellten Sicherheitscode übermittelt der Karteninhaber das Wissenselement an die DKB AG und kann so authentifiziert werden.

6) Die DKB AG darf die verwendete Kreditkarte für das 3D Secure-Verfahren sperren, wenn sachliche Gründe im Zusammenhang mit der Sicherheit des 3D Secure-Verfahrens dies rechtfertigen oder der Verdacht einer betrügerischen Verwendung des 3D Secure-Verfahrens besteht. Zur Aufhebung der Sperre sollte sich der Karteninhaber mit der DKB AG (Kontaktdaten: Hilton Honors Credit Card, 10909 Berlin, Tel.: 069 667 888 300, E-Mail: service@hhonorscard.de) in Verbindung setzen.

3 Einschaltung Dienstleister

Die DKB AG ist berechtigt, zur Abwicklung des 3D Secure-Verfahrens im Rahmen des Kreditkartenvertrages Dienstleister zu beauftragen. Die DKB AG stellt diesen Dienstleistern personenbezogene Daten des Karteninhabers (z. B. Kreditkartennummer) ausschließlich im Rahmen der Zweckbestimmung des Vertragsverhältnisses zur Verfügung.

4 Sorgfaltspflichten des Karteninhabers

1) Der Karteninhaber hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Ziff. 1 Absatz 2) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass sie für das 3D Secure-Verfahren missbräuchlich verwendet werden und es zu nicht autorisierten Zahlungsvorgängen mit der Kreditkarte kommt.

2) Zum Schutz der einzelnen Authentifizierungselemente hat der Karteninhaber vor allem Folgendes zu beachten:
Die hinterlegte Antwort auf die Sicherheitsfrage und der im Internet-Banking angezeigte Sicherheitscode als Wissenselemente (siehe Ziff. 1 Absatz 2) sind geheim zu halten; sie dürfen insbesondere
- nicht außerhalb der im Rahmen des Zahlungsvorgangs angezeigten 3D Secure-Bestätigungsseite (z. B. per E-Mail, Messenger-Dienst) oder mündlich an Dritte weitergegeben werden,
- nicht ungesichert elektronisch gespeichert werden und
- nicht auf dem mobilen Endgerät, mit dem smsTAN empfangen werden, notiert oder als Abschrift zusammen mit diesem Gerät aufbewahrt werden.

Das mobile Endgerät, mit dem smsTAN empfangen werden, und/oder das mit der DKB-Banking-App verknüpfte mobile Endgerät als Besitzelemente (siehe Ziff. 1 Absatz 2) sind vor Missbrauch zu schützen, insbesondere
- ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät befindliche DKB-Banking-App nicht nutzen können,
- ist die Anwendung der DKB-Banking-App auf dem mobilen Endgerät des Karteninhabers zu deaktivieren, bevor er den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons),
- dürfen die empfangenen smsTAN, die als Nachweis des Besitzelements dienen, nicht außerhalb der im Rahmen des Zahlungsvorgangs angezeigten 3D Secure-Bestätigungsseite mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) an Dritte weitergegeben werden,
- darf das mobile Endgerät, mit dem die TAN empfangen wird, nicht gleichzeitig für den Zahlungsvorgang mit der Kreditkarte im Internet genutzt werden; die Kommunikationskanäle sind getrennt zu halten, und
- ist die für das smsTAN-Verfahren hinterlegte Handynummer zu löschen oder zu ändern, wenn der Karteninhaber diese Telefonnummer für das 3D Secure-Verfahren nicht mehr nutzt.

3) Der Karteninhaber hat die Übereinstimmung der während des Zahlungsvorgangs zur Authentifizierung innerhalb des 3D Secure-Verfahrens übermittelten Transaktionsdetails mit den von ihm für die Transaktion vorgesehenen Daten abzugleichen. Bei Unstimmigkeiten ist die Transaktion abzubrechen und die DKB AG (Kontaktdaten: Hilton Honors Credit Card, 10909 Berlin, Tel.: 069 667 888 300, E-Mail: service@hhonorscard.de) unverzüglich zu informieren. Ebenso ist er verpflichtet, der DKB AG unverzüglich zu melden, wenn er die Aufforderung zur Bestätigung eines Zahlungsvorgangs erhält, den er nicht getätigt hat.

4) Der Karteninhaber muss die Sicherheitshinweise auf der Onlinebanking-Seite der DKB AG, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

5 Entgelt

Das Entgelt für die Nutzung des 3D Secure-Verfahrens ergibt sich aus dem Preis- und Leistungsverzeichnis.