

Sonderbedingungen und Verfahrenshinweise für die gesicherte Authentifizierung bei Mastercard und Visa Kartenzahlungen im Internet

Stand: 02/2020

1 Mastercard Identity Check™/Visa Secure

1.1 Nach Ziffer 4.3 der „Vertragsbedingungen für Mastercard/Visa Karten (Debit- oder Kreditkarten)“ bzw. Ziffer 3.3 der „Einsatzbedingungen der Mastercard/Visa Firmenkreditkarte“ und der „Einsatzbedingungen der Basic44 Mastercard (Debitkarte)“ (nachfolgend kurz „Vertrags- bzw. Einsatzbedingungen“) ist der Karteninhaber verpflichtet (Sorgfaltspflicht gemäß Ziffer 6.4 der Vertrags- bzw. Ziffer 5.4 der Einsatzbedingungen), zur Vermeidung von Missbräuchen ein Verfahren zur starken Kundenauthentifizierung bei Internetzahlungen einzusetzen, sofern ein solches sicheres Bezahilverfahren für Internetzahlungen von der Kartenakzeptanzstelle (nachfolgend „Akzeptanzstelle“) unterstützt und dessen Nutzung durch den Herausgeber gefordert wird.

1.2 **Mastercard Identity Check™/Visa Secure** sind solche sichere Bezahilverfahren, die dazu dienen sicherzustellen, dass ein Zahlungsauftrag bei einer Akzeptanzstelle, die an diesem Verfahren teilnimmt, auch tatsächlich vom Karteninhaber autorisiert wurde und die Karte nicht zu Unrecht belastet wird. Hierzu erteilt der Karteninhaber beim Bezahlvorgang gegenüber einem Dienstleister der Bank mittels Eingabe einer auf den Einzelsatz bezogenen Transaktionsnummer (TAN) und der Beantwortung einer Sicherheitsfrage oder alternativ durch Freigabe in einer durch die Bank bereitgestellten App der Akzeptanzstelle die Zustimmung zur Ausführung des Zahlungsvorgangs (Autorisierung, vgl. Ziffer 4.4 der Vertrags- bzw. Ziffer 3.4 der Einsatzbedingungen). Die hierfür benötigte TAN wird an ein zum SMS-Empfang geeignetes Endgerät (z. B. Mobiltelefon) übermittelt oder die Freigabe wird in einer auf dem Endgerät des Karteninhabers installierten, durch die Bank bereitgestellten, App durchgeführt.

1.3 Diese Sonderbedingungen gelten ergänzend zu den Vertrags- bzw. Einsatzbedingungen. Im Falle eines Widerspruchs zwischen den Vertrags- bzw. Einsatzbedingungen gehen diese den Sonderbedingungen vor.

1.4 Zur Nutzung des App-Verfahrens ist die Installation einer von der Bank bereitgestellten App auf einem mobilen Endgerät (z. B. Smartphone) erforderlich. Anbieter der App ist die Rechenzentrale der Bank. Die Nutzung des SMS-Verfahrens setzt die Erreichbarkeit per SMS voraus. Die Nutzung des App-Verfahrens setzt zusätzlich eine Internetverbindung des Endgerätes voraus. Beides gehört nicht zum Leistungsangebot der Bank. Beide Verfahren setzen weiter die Erreichbarkeit des Berechtigungsangesbot via Internet voraus. Der Berechtigungsangabe ist mit Ausnahme üblicher Wartungs- und Updatezeiten erreichbar.

2 Registrierung

2.1 Erforderliche Daten und technische Anforderungen

Um sich zur Teilnahme an diesen sicheren Bezahilverfahren zu registrieren, benötigt der Karteninhaber

- seine Kartenummer,
- einen von der Bank automatisch oder auf Kundenanforderung übermittelten Aktivierungscode,
- für das „SMS-Verfahren“ ein Endgerät (z. B. Mobiltelefon) mit der Möglichkeit des SMS-Empfangs (nachfolgend „Mobiltelefon“ genannt) oder
- für das „App-Verfahren“ ein Endgerät (z. B. Smartphone/Tablet) mit der Möglichkeit der Nutzung der durch die Bank bereitgestellten App.

Die Bank behält sich das Recht vor, nicht beide vorgenannten Verfahren anzubieten oder sie durch ein anderes oder mehrere andere Verfahren zu ersetzen. Sie wird den Karteninhaber hierüber vorab unterrichten. Die Registrierung ist auf der Internetseite der Bank möglich.

2.2 Registrierungsprozess für das SMS-Verfahren

Hierbei legt der Karteninhaber die Rufnummer seines Mobiltelefons fest, an das künftig die zur Autorisierung des Zahlungsauftrags erforderlichen TANs übermittelt werden sollen. Zur Registrierung wird dem Karteninhaber postalisch ein Aktivierungscode an seine hinterlegte Anschrift übermittelt. Diesen Aktivierungscode muss der Karteninhaber zur Festlegung seiner Mobilfunknummer sowie der Antwort auf eine auszuwählende Sicherheitsfrage auf der Internetseite der Bank oder einer von dieser benannten Website einmalig eingeben. Danach ist das SMS-Verfahren freigeschaltet.

2.3 Registrierungsprozess für das App-Verfahren

Das App-Verfahren setzt voraus, dass der Karteninhaber die von der Bank bereitgestellte App auf seinem Endgerät installiert und mit seiner Mastercard/Visa Karte (nachfolgend „Karte“) per Aktivierungscode verknüpft. Die bei erstmaliger Nutzung der App erzeugte Kennung (die „virtuelle Handynummer“) ist bei der Registrierung anzugeben. Zur Registrierung wird dem Karteninhaber einmalig postalisch ein Aktivierungscode an seine hinterlegte Anschrift übermittelt oder, wenn die Nutzung des elektronischen Postfachs zwischen dem Karteninhaber und der Bank vereinbart ist, in sein Postfach im Online-Banking eingestellt. Diesen Aktivierungscode muss der Karteninhaber zur Bestätigung der angebotenen virtuellen Handynummer auf der Internetseite der Bank oder einer von dieser benannten Website einmalig eingeben. Danach ist das App-Verfahren freigeschaltet und der Karteninhaber hat die Möglichkeit, Zahlungen innerhalb der App freizugeben.

2.4 Weitere Informationen

Die Bank wird den Karteninhaber niemals per E-Mail oder Anruf zur Registrierung oder Bekanntgabe seiner Registrierungsdaten auffordern. Der Ablauf der Registrierung und die Bezugsquellen der Anwendung sind in der Information „Mehr Sicherheit beim Online-Shopping“ beschrieben, die dem Karteninhaber bereitgestellt wird und bei der Bank erhältlich ist.

3 Gesichertes Bezahverfahren

3.1 SMS-Verfahren:

Sobald das sichere Bezahilverfahren bei einer Transaktion von der Akzeptanzstelle gefordert wird, erhält der Karteninhaber eine SMS Benachrichtigung mit Transaktionsdetails und pro Transaktion generierter TAN auf sein Endgerät zugestellt. Durch Eingabe der erhaltenen TAN und korrekter Beantwortung der Sicherheitsfrage im Kaufprozess wird der Zahlungsauftrag autorisiert.

3.2 App-Verfahren:

Beim App-Verfahren werden die Transaktionsdetails via Internet direkt an eine besonders geschützte App auf das Endgerät des Karteninhabers übermittelt. Sobald das sichere Bezahilverfahren bei einer Transaktion von der Akzeptanzstelle gefordert wird, erhält der Karteninhaber auf seinem Endgerät eine Benachrichtigung. Nach Eingabe des App-Kennworts bzw. durch biometrische Freigabe (sofern vom Betriebssystem des Endgeräts unterstützt) öffnet sich die App und die Transaktionsdetails werden angezeigt. Durch Freigabe per Bestätigung innerhalb der App wird der Zahlungsauftrag autorisiert.

3.3 Die Nutzung des gesicherten Bezahilverfahrens für Internet-Zahlungen kann für bestimmte Transaktionen zur Risikoprävention von der Bank eingeschränkt sein.

4 Sorgfalts- und Mitwirkungspflichten des Karteninhabers

4.1 Der Karteninhaber hat dafür Sorge zu tragen, dass kein Dritter zur Durchführung von Internet-Zahlungen Zugang zu seinem für das Verfahren genutzten Endgerät erlangt. Die App ist gegen unberechtigten Zugriff – z. B. durch ein sicheres Passwort – zu schützen. Das Endgerät ist vor Verlust und Diebstahl zu sichern. Im Fall von Verlust oder Diebstahl des Endgerätes ist nach Möglichkeit die App per Fernzugriff zu löschen und die SIM-Karte des Endgerätes sperren zu lassen. Zugangsdaten zur App dürfen nicht auf dem Endgerät gespeichert werden. Die App darf nicht auf Endgeräten eingesetzt werden, deren Betriebssystem manipuliert wurde, z. B. durch sogenanntes Jailbreaks oder Rooten oder sonstige nicht vom Hersteller des Endgeräts freigegebene Betriebssystemvarianten. Weiter gilt Ziffer 6.4 der Vertrags- bzw. Ziffer 5.4 der Einsatzbedingungen.

4.2 Das Endgerät, das zur Freigabe der Transaktion dient, sollte nicht gleichzeitig für die Internet-Zahlungen genutzt werden (physische Trennung der Kommunikationskanäle).

4.3 Der Karteninhaber hat die Übereinstimmung der von der Bank dem Nutzer übermittelten Transaktionsdaten mit den von ihm für die Transaktion vorgesehenen Daten abzugleichen. Bei Unstimmigkeiten ist die Transaktion abzubrechen und die Bank zu informieren.

4.4 Der Karteninhaber hat die App nur aus offiziellen App-Stores (Apple App Store oder Google Play Store) herunterzuladen und die für die App vorgesehenen Updates regelmäßig zu installieren.

5 Änderung der Mobilfunknummer/virtuellen Handynummer

5.1 Sollte der Karteninhaber seine für das Verfahren genutzte Kennung (Sicherheitsfrage und/oder Mobilfunknummer für SMS-Empfang bzw. virtuelle Handynummer für App-Nutzung) ändern wollen, steht ihm hierfür auf der Registrierungswebseite der Bank eine entsprechende Funktion zur Verfügung.

5.2 Ist kein Nachrichten-Versand an die bisher registrierte Kennung möglich (z. B. das Endgerät mit der hinterlegten Kennung wurde gestohlen), muss der Karteninhaber den Registrierungsprozess erneut durchlaufen.

6 Abmeldung vom Verfahren

6.1 Der Karteninhaber kann sich von der Teilnahme am sicheren Bezahilverfahren abmelden, in dem er auf der Registrierungswebseite der Bank den Button „Benutzerdaten löschen“ betätigt.

6.2 Wenn sich der Karteninhaber abgemeldet hat, ist es ihm erst nach Abschluss einer Neuregistrierung wieder möglich, seine Karte für Internetzahlungen bei am sicheren Bezahilverfahren teilnehmenden Akzeptanzstellen einzusetzen.

7 Datenerhebung und Datenverarbeitung, Einschaltung Dritter

7.1 Die Bank bzw. der Herausgeber bedient sich zur Bewirkung der von ihr bzw. ihm im Rahmen von Mastercard Identity Check™/Visa Secure zu erbringenden Leistungen und zur Einforderung der vom Karteninhaber zu erbringenden Leistungen Dritter.

7.2 Hat ein beauftragter Dienstleister seinen Sitz in einem Land außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (z. B. Schweiz oder USA) wird die Bank bzw. der Herausgeber vor der Datenübermittlung für ein angemessenes Datenschutzniveau im Sinne der aktuellen gesetzlichen Anforderungen sorgen, es sei denn, dass bereits eine Angemessenheitsentscheidung der Europäischen Kommission zugunsten des Landes vorliegt, in dem dieser Dienstleister seinen Sitz hat. Die Schweiz gilt datenschutzrechtlich als sicherer Staat.

7.3 Ausschließlich zum Zweck der Abwicklung des sicheren Bezahilverfahrens werden personenbezogene Daten des Karteninhabers im Rahmen der Registrierung und Daten zum Zahlungsvorgang (insb. Kartenummer, die hinterlegte Mobilfunknummer/virtuelle Handynummer, Sicherheitsfrage sowie ein Protokoll des authentifizierten Zahlungsauftrags, der versendeten Nachrichten und die IP-Adresse und Geräte-/Browserdaten des aufrufenden Geräts, Daten zur Transaktion/Bestellung des Karteninhabers) an den jeweiligen Dienstleister weitergegeben und von diesem verarbeitet, um die Kundenauthentifizierung zu überprüfen und eine Risikoprüfung für die Transaktion durchzuführen. Spätestens mit Beendigung des Kartenvertrags werden die Registrierungsdaten gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

7.4 Nimmt eine Akzeptanzstelle an dem Verfahren teil, übernimmt der jeweilige Dienstleister die Authentifizierung des Karteninhabers und teilt der Akzeptanzstelle mit, ob diese erfolgreich war. Weitere Daten werden nicht an die Akzeptanzstelle übermittelt. War die Authentifizierung nicht erfolgreich, wird der Zahlungsauftrag abgelehnt (vgl. Ziffer 4.5 der Vertrags- bzw. Ziffer 3.5 der Einsatzbedingungen).