

Sonderbedingungen für die gesicherte Authentifizierung bei Kreditkartenzahlungen im Internet

1 Verified by Visa/MasterCard SecureCode™

Nach Ziffer 4.3 der „Vertragsbedingungen für Kreditkarten“ bzw. Ziffer 3.3 der „Einsatzbedingungen von Firmenkreditkarten“, die durch diese Sonderbedingungen ergänzt werden, ist der Karteninhaber verpflichtet (Sorgfaltspflicht), zur Vermeidung von Missbräuchen gesicherte Authentifizierungsverfahren bei Internet-Zahlungen einzusetzen, sofern ein solches Verfahren von der Bank und der Kartenakzeptanzstelle angeboten wird. **Verified by Visa** bzw. **MasterCard SecureCode** sind solche Verfahren zur gesicherten Authentifizierung, die dazu dienen sicherzustellen, dass eine Online-Kreditkartenzahlung bei einer Kartenakzeptanzstelle, die an diesem Verfahren teilnimmt, auch tatsächlich vom Karteninhaber veranlasst wurde und die Karte nicht zu Unrecht belastet wird. Hierzu bestätigt der Karteninhaber beim Bezahlvorgang gegenüber einem Dienstleister der Bank mittels Eingabe einer auf den Einzelumsatz bezogenen Transaktionsnummer (TAN), dass er die Zahlung beauftragt. Die TAN wird an ein zum SMS-Empfang geeignetes Gerät (z. B. Mobiltelefon) des Karteninhabers übermittelt.

2 Registrierung

2.1 Um sich zur Teilnahme an diesen Authentifizierungsverfahren zu registrieren, benötigt der Karteninhaber

- seine Kreditkartennummer
- ein Gerät (z. B. Mobiltelefon) mit der Möglichkeit des SMS-Empfangs (nachfolgend „Mobiltelefon“ genannt)
- sowie persönliche Daten,

die während der Registrierung abgefragt werden. Die Registrierung ist auf der Internetseite der Bank möglich. Optional kann die Kartenakzeptanzstelle während eines Bezahlvorgangs auf ihrer Webseite auf die Registrierungsmöglichkeit hinweisen.

2.2 Im Rahmen des Registrierungsprozesses legt der Karteninhaber die Rufnummer seines Mobiltelefons fest, an das die zur Zahlungsfreigabe erforderliche TAN übermittelt werden soll. Bei der Erstregistrierung für das Verfahren wird dem Kunden postalisch ein Aktivierungscode an seine hinterlegte Anschrift übermittelt, der zur Bestätigung der Mobilfunknummer online einzugeben ist. Die Nutzung der gesicherten Authentifizierung für E-Commerce Transaktionen kann bis zur Bestätigung der Mobilfunknummer für bestimmte Transaktionen zur Risikoprävention eingeschränkt sein.

3 Sorgfaltsanforderungen an den Karteninhaber

Der Karteninhaber hat dafür Sorge zu tragen, dass kein Dritter zur Durchführung von gesicherten E-Commerce Transaktionen Zugang zu seinem Mobiltelefon erlangt. Die Bank wird den Kunden nicht per E-Mail oder Anruf zur Registrierung oder Bekanntgabe seiner Registrierungsdaten auffordern. Das Gerät, mit dem die TAN empfangen werden (z. B. Smartphone), darf nicht gleichzeitig für die E-Commerce-Transaktion genutzt werden (physische Trennung der Kommunikationskanäle). 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.

Darüber hinaus gelten die Sorgfalts- und Mitwirkungspflichten des Karteninhabers gemäß Ziffer 6 der „Vertragsbedingungen für Kreditkarten“ bzw. Ziffer 5 der „Einsatzbedingungen von Firmenkreditkarten“.

4 Änderung der Mobilfunknummer

Sollte der Karteninhaber seine für das Verfahren genutzte Mobilfunknummer ändern wollen, steht ihm auf der Registrierungswebseite seiner Bank eine Funktion zur Verfügung, um seine für das TAN-Verfahren verwendete Mobilfunknummer zu ändern. Ist kein SMS-Versand an die bisher registrierte Mobilfunknummer möglich, muss der Karteninhaber den Registrierungsprozess erneut durchlaufen.

5 Abmeldung vom Verfahren

5.1 Der Karteninhaber kann sich von der Teilnahme am Verfahren abmelden, indem er auf der Registrierungswebseite seiner Bank den Button „Benutzerkonto löschen“ betätigt.

5.2 Wenn sich der Karteninhaber abgemeldet hat, ist es ihm nicht mehr möglich, seine Kreditkarte für Online-Kauftransaktionen bei am gesicherten Authentifizierungsverfahren teilnehmenden Kartenakzeptanzstellen einzusetzen. Um die Kreditkarte wieder bei diesen Kartenakzeptanzstellen einsetzen zu können, ist eine Neuregistrierung für Verified by Visa bzw. MasterCard SecureCode erforderlich.

6 Datenschutz: Einwilligung zur Einschaltung Dritter

Der Karteninhaber stimmt mit der Registrierung folgenden datenschutzrechtlichen Regelungen zu: Die Bank bzw. der Emittent setzt im Rahmen von Verified by Visa bzw. MasterCard SecureCode die CardProcess GmbH mit Sitz in Karlsruhe, Deutschland, sowie die CA Technologies, mit Sitz in Islandia, NY, USA, (vormals: Arcot Systems, Inc.) als Dienstleister ein. Die Registrierung für Verified by Visa bzw. MasterCard SecureCode erfolgt direkt bei CA Technologies, wo die Kartenummer, die hinterlegte Mobilfunknummer des Karteninhabers sowie ein Protokoll der authentifizierten Transaktionen, der versendeten SMS-Nachrichten und die IP-Adresse und Browserdaten des aufrufenden Rechners hinterlegt werden. Andere personenbezogene Daten des Karteninhabers, wie Namen und Geburtsdaten, werden über die Server von CA Technologies an die CardProcess GmbH weitergeleitet und nur dort gespeichert. Spätestens mit Beendigung des Kreditkartenvertrages werden die Registrierungsdaten gelöscht. Nimmt eine Kartenakzeptanzstelle am Verfahren teil, übernimmt CA Technologies die Authentifizierung des Karteninhabers und teilt der Kartenakzeptanzstelle mit, ob der Authentifizierungsprozess erfolgreich war. Weitere Daten werden nicht übermittelt. CA Technologies hat sich den zwischen den USA und der EU vereinbarten Datenschutzgrundsätzen (Safe Harbor Grundsätzen) angeschlossen. Außerdem unterliegt CA Technologies einer regelmäßigen Zertifizierung nach den Payment Card Industries Data Security Standards (PCI-DSS).

Der Karteninhaber kann seine datenschutzrechtliche Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Der **Widerruf** kann in der Kontoverwaltung erfolgen. Der Widerruf hat zur Folge, dass der Karteninhaber dann nicht mehr bei Akzeptanzstellen im Internet zahlen kann, die an dem gesicherten Verfahren teilnehmen.

Stand August 2015