BEDINGUNGEN FÜR VOLKSBANK ELECTRONIC-BANKING (INTERNETBANKING)

Gegenüberstellung der geänderten Klauseln

Fassung 2015	Fassung 2018
BEDINGUNGEN FÜR VOLKSBANK ELECTRONIC-BANKING	**BEDINGUNGEN FÜR VOLKSBANK ELECTRONIC-BANKING (INTERNETBANKING)**
A. Allgemeine Bestimmungen **4. Zugriffsberechtigung** Zugang zu einem Konto im Rahmen von Electronic-Banking erhalten nur Kunden, die sich durch Eingabe ihrer persönlichen Identifikationsmerkmale (Verfügernummer, Verfügername, persönliche Identifikationsnummer = PIN, EB-PIN für das cardTAN-Verfahren) legitimiert haben. Auf mobilen Endgeräten ist auch ein Zugriff mittels vereinfachter Authentifizierung (Gerätebindung in Kombination mit verfügerspezifischen vierstelligen PIN-Code) möglich. Dabei kann der Funktionsumfang auf eine reine Ansichtsberechtigung (keine Dispositionsmöglichkeit) eingeschränkt sein. Für Dispositionen und rechtsverbindliche Willenserklärungen hat sich der Verfüger durch Eingabe seiner persönlichen Identifikationsmerkmale zu legitimieren und zusätzlich durch Eingabe einer geheimen, einmal verwendbaren Transaktionsnummer (TAN) oder mittels Digitaler Signatur als berechtigt auszuweisen. Die Berechtigung zur Vornahme von Dispositionen wird von der Bank nur aufgrund der persönlichen Identifikationsmerkmale und TANs bzw. Digitaler Signatur überprüft, die Ansichtsberechtigung nur aufgrund der persönlichen Identifikationsmerkmale. Erfordert das Electronic-Banking das Zusammenwirken mehrerer Verfüger, muss die Autorisierung jeweils von den gemeinsam berechtigten Verfügern gesondert, jedoch innerhalb eines Zeitraumes von 28 Tagen veranlasst werden. Bei gemeinsamer (kollektiver) Zeichnung ist die Nutzung von Teilbereichen des Electronic-Banking (z.B. eps Online-Überweisung) nicht möglich. Die Bank ist berechtigt, das Verfahren der Zugriffsberechtigung nach vorheriger Mitteilung an den Verfüger oder Ansichtsberechtigten abzuändern. Die Zustellung persönlicher Identifikationsmerkmale erfolgt entweder durch Übergabe am Schalter oder durch Postversand. Bei Office Banking sind Zugangsdaten für Konten bei anderen Banken bei diesen Banken gesondert zu beantragen.	**A. Allgemeine Bestimmungen** **4. Zugriffsberechtigung** Zugang zu einem Konto im Rahmen von Electronic-Banking erhalten nur Kunden, die sich durch Eingabe ihrer persönlichen Identifikationsmerkmale (Verfügernummer, Verfügername, persönliche Identifikationsnummer = PIN~~, EB-PIN für das cardTAN-Verfahren~~) legitimiert haben. Zusätzlich kann die Bank alternative Loginverfahren bereitstellen (z.B. Einmalpasswort oder biometrische Verfahren). Auf mobilen Endgeräten ist auch ein Zugriff mittels vereinfachter Authentifizierung (Gerätebindung in Kombination mit verfügerspezifischen vierstelligen ~~PIN-Code~~ Quick-ID und/oder biometrischer Authentifizierung) möglich. Dabei kann der Funktionsumfang auf eine reine Ansichtsberechtigung (keine Dispositionsmöglichkeit) eingeschränkt sein. Für Dispositionen und rechtsverbindliche Willenserklärungen hat sich der Verfüger durch Eingabe seiner persönlichen Identifikationsmerkmale zu legitimieren und zusätzlich durch Eingabe einer geheimen, einmal verwendbaren Transaktionsnummer (TAN) ~~oder mittels Digitaler Signatur~~ als berechtigt auszuweisen. Die Berechtigung zur Vornahme von Dispositionen wird von der Bank nur aufgrund der persönlichen Identifikationsmerkmale und TANs ~~bzw. Digitaler Signatur~~ überprüft, die Ansichtsberechtigung nur aufgrund der persönlichen Identifikationsmerkmale. Erfordert das Electronic-Banking das Zusammenwirken mehrerer Verfüger, muss die Autorisierung jeweils von den gemeinsam berechtigten Verfügern gesondert, jedoch innerhalb eines Zeitraumes von ~~28~~ 60 Tagen veranlasst werden. Bei gemeinsamer (kollektiver) Zeichnung ist die Nutzung von Teilbereichen des Electronic-Banking (z.B. eps Online-Überweisung) nicht möglich. *Rest unverändert*
4.2. TAN-App Die Übermittlung der für die Autorisierung von Aufträgen erforderlichen Transaktionsnummern erfolgt an eine App, die von der Bank zur Verfügung gestellt wird. Die App muss zuvor auf einem registrierten mobilen Endgerät des Verfügers (= Herstellung der Gerätebindung) installiert sein. Die Authentifizierung erfolgt mittels Gerätebindung und persönlicher Identifikationsnummer = shortPIN. Der Verfüger kann die Gerätebindung und seine persönliche shortPIN direkt im Electronic-Banking ändern. Zu Kontrollzwecken werden in der Nachricht mit der TAN auch Angaben über die durchzuführenden Aufträge, insbesondere Empfänger-IBAN und Betrag oder ein Referenzcode (Elektronischer Begleitzettel) und Kontrollwert (Summe aller Aufträge), mitgeliefert. Der Verfüger ist verpflichtet, diese auf Übereinstimmung mit den im Electronic-Banking eingegebenen Aufträgen zu prüfen. Die TAN darf nur bei Übereinstimmung eingegeben werden.	**4.2. TAN-App** Die Übermittlung der für die Autorisierung von Aufträgen erforderlichen Transaktionsnummern erfolgt an eine App, die von der Bank zur Verfügung gestellt wird. Die App muss zuvor auf einem registrierten mobilen Endgerät des Verfügers (= Herstellung der Gerätebindung) installiert sein. Die Authentifizierung erfolgt mittels Gerätebindung und persönlicher Identifikationsnummer = ~~shortPIN~~ Quick-ID oder ein biometrisches Verfahren. Der Verfüger kann die Gerätebindung und seine persönliche shortPIN direkt im Electronic-Banking ändern. *Rest unverändert*

4.4. Digitale Signatur Anstelle der persönlichen Identifikationsmerkale und TANs kann zur Legitimierung und zur Erteilung von Aufträgen und rechtsverbindlichen Willenserklärungen gegenüber der Bank ein digitales Zertifikat verwendet werden.	*gelöscht*
5. Sorgfaltspflichten Persönliche Identifikationsmerkmale, TANs und cardTAN-fähige Karten dürfen nicht an Dritte, insbesondere auch nicht an andere Zahlungsdienstleister, weitergegeben werden. Jeder Verfüger ist verpflichtet, eine besondere Sorgfalt bei der Aufbewahrung walten zu lassen, um missbräuchliche Zugriffe zu vermeiden. Die persönlichen Identifikationsmerkmale dürfen nur an einem sicheren Ort aufbewahrt werden. Bei Verlust oder wenn diese von einem unbefugten Dritten missbräuchlich verwendet werden, hat der Verfüger seine PIN selbständig zu ändern oder durch viermalige Falscheingabe der PIN eine Sperre vorzunehmen. Ist dem Verfüger eine selbständige Sperre nicht möglich, so hat er unverzüglich die Bank zu benachrichtigen.	**5. Sorgfaltspflichten** Persönliche Identifikationsmerkmale, TANs und cardTAN-fähige Karten dürfen nicht an Dritte, insbesondere auch nicht an andere Zahlungsdienstleister, weitergegeben werden. Jeder Verfüger ist verpflichtet, eine besondere Sorgfalt bei der Aufbewahrung walten zu lassen, um missbräuchliche Zugriffe zu vermeiden. Die persönlichen Identifikationsmerkmale dürfen nur an einem sicheren Ort aufbewahrt werden. Bei Verlust oder wenn diese von einem unbefugten Dritten missbräuchlich verwendet werden, hat der Verfüger seine PIN selbständig zu ändern oder durch ~~viermalige~~ dreimalige Falscheingabe der PIN eine Sperre vorzunehmen. Ist dem Verfüger eine selbständige Sperre nicht möglich, so hat er unverzüglich die Bank zu benachrichtigen.
6. Sperre Die Bank wird die Nutzung des Electronic-Banking über ausdrücklichen Wunsch des Kontoinhabers zur Gänze oder über Wunsch eines Verfügers oder Ansichtsberechtigten nur diesen betreffend sperren. Sperrt die Bank den Zugang zu Electronic-Banking gemäß Z 15 der Allgemeinen Geschäftsbedingungen, so erfolgt die Benachrichtigung des Kunden telefonisch, ist eine telefonische Benachrichtigung nicht möglich, erfolgt die Verständigung schriftlich an die vom Kunden zuletzt bekanntgegebene Adresse. Der Zugang wird automatisch gesperrt, wenn viermal in ununterbrochener Reihenfolge eine falsche PIN oder TAN eingegeben wird. Eine Sperre kann persönlich am Schalter oder über schriftlichen Auftrag bzw. telefonisch mit einer gültigen TAN wieder aufgehoben werden. Die Bank kann ein telefonisches Entsperren auch bei Nennung einer gültigen TAN aus Sicherheitsgründen ablehnen.	**6. Sperre** Die Bank wird die Nutzung des Electronic-Banking über ausdrücklichen Wunsch des Kontoinhabers zur Gänze oder über Wunsch eines Verfügers oder Ansichtsberechtigten nur diesen betreffend sperren. Sperrt die Bank den Zugang zu Electronic-Banking gemäß Z 15 der Allgemeinen Geschäftsbedingungen, so erfolgt die Benachrichtigung des Kunden telefonisch, ist eine telefonische Benachrichtigung nicht möglich, erfolgt die Verständigung schriftlich an die vom Kunden zuletzt bekanntgegebene Adresse. Der Zugang wird automatisch gesperrt, wenn ~~viermal~~ dreimal in ununterbrochener Reihenfolge eine falsche PIN oder TAN eingegeben wird. Eine Sperre kann persönlich am Schalter oder über schriftlichen Auftrag bzw. telefonisch mit einer gültigen TAN wieder aufgehoben werden. Die Bank kann ein telefonisches Entsperren auch bei Nennung einer gültigen TAN aus Sicherheitsgründen ablehnen.