

Sonderbedingungen für die konto-/depotbezogene Nutzung des Online-Banking

Stand: Mai 2007

Allgemeine Regelungen

1 Leistungsangebot

Das Kreditinstitut steht seinen Kunden für die elektronische Datenübermittlung im Wege des Online-Bankings zur Verfügung. Es gibt dem Kunden die Dienstleistungsarten bekannt, die er im Rahmen des Online-Banking nutzen kann.

Der Konto-/Depotinhaber kann Bankgeschäfte mittels Online-Banking in dem vom Kreditinstitut angebotenen Umfang abwickeln. Sofern das Kreditinstitut für Verfügungen mittels Online-Banking eine Betragsbegrenzung im System vorsieht, informiert es ihn hierüber.

2 Nutzungsberechtigte und Zugangsmedien

(1) Zur Abwicklung von Bankgeschäften mittels Online-Banking unter **Verwendung von PIN und TAN** benötigt der Konto-/Depotinhaber und etwaige Bevollmächtigte jeweils eine persönliche Identifikationsnummer (PIN) sowie gegebenenfalls Transaktionsnummern (TAN) aus

- einer TAN-Liste (hierzu siehe Nummern 14 ff.) oder
- einem TAN-Generator (hierzu siehe Nummern 17 ff.) oder
- einem Mobiltelefon (hierzu siehe Nummern 19 ff.).

(2) Zur Abwicklung von Bankgeschäften mittels Online-Banking unter **Verwendung einer elektronischen Signatur** benötigt der Konto-/Depotinhaber oder etwaige Bevollmächtigte zur Identifikation und Legitimation jeweils eigene, personengebundene Identifikations- und Legitimationsmedien in Form

- einer Signatur-Chipkarte oder
- einer Bank-Karte mit Signaturfunktion oder
- eines entfernbareren Speichermediums (z. B. einer Computer-Diskette) mit einem darauf gespeicherten Signatur-Schlüssel oder
- eines anderen von der Bank zugelassenen Geräts (Token) zum sicheren Erzeugen von elektronischen Signaturen.

Diese werden im Folgenden einheitlich als Signaturmedium bezeichnet (hierzu siehe Nummern 23 ff.). Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden als Nutzer bezeichnet.

3 Verfahren

(1) Beim **Online-Banking mit PIN und TAN** hat der Nutzer mittels Online-Banking Zugang zum Konto/Depot, wenn er zuvor die Konto-/Depotnummer/seine individuelle Kundenkennung sowie seine PIN eingegeben hat. In den vom Kreditinstitut im Einzelnen angegebenen Fällen hat der Nutzer jeweils zusätzlich eine TAN einzugeben.

(2) Beim **Online-Banking mit elektronischer Signatur** ist der Nutzer verpflichtet, die technische Verbindung zum Online-Banking-Angebot des Kreditinstitutes über die vom Kreditinstitut mitgeteilten Zugangskanäle herzustellen sowie die mit dem Kreditinstitut vereinbarten Übertragungs- und Sicherungsverfahren sowie Datenformate einzuhalten. In den vom Kreditinstitut im Einzelnen angegebenen Fällen hat der Nutzer jeweils eine elektronische Signatur anzubringen.

(3) Zur Erläuterung der Nutzungsmöglichkeiten stellt das Kreditinstitut in besonderen Fällen eine Verfahrensanleitung zur Verfügung, die die Besonderheiten der vereinbarten Online-Anwendung beschreibt.

(4) Soweit das Kreditinstitut dem Nutzer Daten über Aufträge zur Verfügung stellt, die noch nicht endgültig bearbeitet sind, stellen diese lediglich eine unverbindliche Information dar. Die Daten sind jeweils besonders gekennzeichnet.

4 Nachrichtenfreigabe / Verwendung

(1) Erklärungen jeder Art (z. B. Kontostandsabfragen oder Überweisungen) sind abgegeben, wenn sie abschließend zur Übermittlung an das Kreditinstitut freigegeben sind.

(2) Bei Vorgängen, die zusätzlich der Eingabe einer TAN bedürfen (z. B. Überweisungen), ist die Freigabe der TAN maßgebend. Eine TAN kann nicht mehr verwendet werden, sobald sie zur Übermittlung an das Kreditinstitut freigegeben worden ist. Für mobile TAN siehe die besonderen Regelungen unter Nummern 19 ff.

(3) Bei Einsatz der elektronischen Signatur müssen alle Erklärungen vor der Abgabe mit dem Signaturmedium elektronisch signiert sein.

5 Bearbeitung von Aufträgen im Online-Banking

(1) Mittels Online-Banking erteilte Aufträge werden im Rahmen des ordnungsgemäßen Arbeitsablaufs bearbeitet.

(2) Das Kreditinstitut ist berechtigt, fehlerhafte Aufträge von der weiteren Bearbeitung auszuschließen, wenn die ordnungsgemäße Ausführung des Auftrags nicht sichergestellt werden kann. Hierüber wird das Kreditinstitut den Nutzer unverzüglich informieren.

6 Haftungsausschluss

Das Kreditinstitut haftet nur für von ihm vorsätzlich oder grob fahrlässig verursachte Schäden.

7 Finanzielle Nutzungsgrenze

Der Nutzer darf Verfügungen nur im Rahmen des Kontoguthabens oder eines vorher für das Konto eingeräumten Kredits vornehmen. Auch wenn der Nutzer diese Nutzungsgrenze bei seinen Verfügungen nicht einhält, ist das Kreditinstitut berechtigt, den Ersatz der Aufwendungen zu verlangen, die aus der Nutzung des Online-Banking entstehen. Die Buchung solcher Verfügungen auf dem Konto führt lediglich zu einer geduldeten Kontoüberziehung; das Kreditinstitut ist berechtigt, in diesem Fall den höheren Zinssatz für geduldete Kontoüberziehungen zu verlangen.

8 Sperre des Online-Banking-Angebotes durch das Kreditinstitut

(1) Wird **beim Online-Banking mit PIN und TAN** dreimal hintereinander eine falsche PIN eingegeben, so sperrt das Kreditinstitut den Online-Banking-Zugang zum Konto/Depot. Der Nutzer kann diese Sperre aufheben, indem er neben der richtigen PIN eine gültige TAN eingibt.

(2) Werden dreimal hintereinander falsche TAN eingegeben, so werden alle noch nicht verbrauchten TAN, der TAN-Generator oder das mobile TAN-Verfahren für das betreffende Konto/Depot gesperrt. Im Fall der vollständigen Sperrung der unverbrauchten TAN in der TAN-Liste oder des TAN-Generators sollte sich der Nutzer mit dem Kreditinstitut in Verbindung setzen, um die Nutzungsmöglichkeiten des Online-Banking wiederherzustellen.

(3) Werden **beim Online-Banking mit elektronischer Signatur** dreimal hintereinander Aufträge mit falscher elektronischer Signatur an das Kreditinstitut übermittelt, so sperrt das Kreditinstitut das Signaturmedium für den Online-Banking-Zugang zum betreffenden Konto/Depot.

(4) Im Falle der Sperrung des Signaturmediums oder der vollständigen Sperrung des Online-Banking-Zugangs sollte sich der Nutzer mit dem Kreditinstitut in Verbindung setzen, um die Nutzungsmöglichkeiten des Online-Banking wiederherzustellen.

(5) Das Kreditinstitut wird den Online-Banking-Zugang zum Konto/Depot sperren, wenn der Verdacht einer missbräuchlichen Nutzung des Kontos/Depots über den Online-Banking-Zugang besteht. Es wird den Kontoinhaber hierüber außerhalb des Online-Banking informieren. Diese Sperre kann nicht mittels Online-Banking aufgehoben werden.

9 Sperre des Online-Banking-Angebotes auf Wunsch des Kontoinhabers

Das Kreditinstitut wird den Online-Banking-Zugang zum Konto/Depot auf Wunsch des Kontoinhabers sperren. Diese Sperre kann nicht mittels Online-Banking aufgehoben werden.

10 Einzug der Chipkarte mit Zahlungsfunktion und TAN-Generator oder Signaturfunktion

Das Kreditinstitut darf den Einzug der Chipkarte mit Zahlungsfunktion und TAN-Generator oder Signaturfunktion (z. B. am Geldausgabeautomaten) veranlassen, wenn es berechtigt ist, den Kartenvertrag aus wichtigem Grund zu kündigen. Das Kreditinstitut ist zur Einziehung der Karte auch berechtigt, wenn die Nutzungsberechtigung der Karte durch Gültigkeitsablauf oder durch ordentliche Kündigung endet. Der Einzug der Karte hat zur Folge, dass der Nutzer den TAN-Generator auf der Karte für das Online-Banking nicht mehr nutzen kann.

11 Rückruf oder Änderung von Aufträgen

Der Rückruf oder die Änderung von Aufträgen kann nur außerhalb des Online-Banking-Verfahrens erfolgen, es sei denn, das Kreditinstitut sieht eine solche Möglichkeit innerhalb des Verfahrens ausdrücklich vor. Das Kreditinstitut kann einen Rückruf oder eine Änderung allerdings nur beachten, wenn ihm diese Nachricht so rechtzeitig zugeht, dass ihre Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufs möglich ist. Bei einer garantierten Zahlung bestätigt die Bank verbindlich die Ausführung der Überweisung gegenüber dem Zahlungsempfänger. Ein Widerruf ist in diesem Fall ausgeschlossen.

12 Hinweis nach § 13 Abs. 1 TMG (Telemediengesetz)

Alle im Rahmen des Online-Banking anfallenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank und gegebenenfalls dem von ihr beauftragten Rechenzentrum innerhalb Deutschlands bzw. der Europäischen Union verarbeitet.

13 Anwendbares Recht

Auf die Geschäftsbeziehung zwischen dem Konto-/Depotinhaber und dem Kreditinstitut findet deutsches Recht Anwendung, es sei denn, dieses verweist auf eine ausländische Rechtsordnung.

Besondere Regelungen für das Online-Banking mit PIN und TAN

14 Sorgfalts- und Mitwirkungspflichten

Der Nutzer hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der PIN und den TAN erlangt. Jede Person, die die PIN und – falls erforderlich – eine TAN kennt, hat die Möglichkeit, das Online-Banking-Leistungsangebot zu nutzen. Sie kann z. B. Aufträge zulasten des Kontos/Depots erteilen. Insbesondere Folgendes ist zur Geheimhaltung der PIN und TAN zu beachten:

- PIN und TAN dürfen nicht elektronisch gespeichert oder in anderer Form notiert werden.
- Die dem Nutzer zur Verfügung gestellte TAN-Liste bzw. der dem Nutzer zur Verfügung gestellte TAN-Generator oder das für den TAN-Empfang registrierte Mobiltelefon ist sicher zu verwahren.
- Bei Eingabe der PIN und TAN ist sicherzustellen, dass Dritte diese nicht ausspähen können.
- Die technische Verbindung zum Online-Banking-Angebot des Kreditinstituts ist nur über die vom Kreditinstitut gesondert mitgeteilten Online-Banking-Zugangskanäle herzustellen.
- Außerhalb der vom Kreditinstitut gesondert mitgeteilten Online-Banking-Zugangskanäle dürfen Anfragen, insbesondere nach vertraulichen Daten wie Geheimzahl, PIN oder TAN, nicht beantwortet werden.

15 Maßnahmen bei Bekanntwerden von PIN oder TAN aus einer TAN-Liste oder Verdacht ihrer missbräuchlichen Nutzung

Stellt der Nutzer fest, dass eine andere Person

- von seiner PIN oder
- von einer TAN aus seiner TAN-Liste oder
- von einer TAN aus seinem TAN-Generator oder
- von einer TAN aus seinem Mobiltelefon

Kenntnis erhalten hat oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so ist der Nutzer verpflichtet, unverzüglich seine PIN zu ändern bzw. die noch nicht aus der TAN-Liste verbrauchten TAN zu sperren. Sofern ihm dies nicht möglich ist, hat er das Kreditinstitut unverzüglich zu unterrichten. Der Nutzer hat jeden Missbrauch unverzüglich bei der Polizei zur Strafanzeige zu bringen. In diesem Fall wird das Kreditinstitut den Online-Banking-Zugang zum Konto/Depot sperren. Das Kreditinstitut haftet ab dem Zugang der Sperrnachricht des Nutzers für alle Schäden, die aus ihrer Nichtbeachtung entstehen. Zu weiteren Maßnahmen sind auch die besonderen Regelungen weiter unten zu beachten.

16 Änderung der PIN

Der Nutzer ist berechtigt, seine PIN unter Verwendung einer TAN jederzeit zu ändern. Bei Änderung der PIN wird seine bisherige PIN ungültig.

Besondere Regelungen für den TAN-Generator

17 Begriffsbestimmung TAN-Generator

Ein TAN-Generator ist Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN. Aus der Chipkarte können jeweils einmal verwendbare TAN mithilfe eines Lesegeräts ausgelesen werden. Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden als Nutzer bezeichnet.

18 Weitere Maßnahmen bei Verlust des TAN-Generators

Stellt der Nutzer den Verlust seines TAN-Generators fest oder besteht der Verdacht seiner missbräuchlichen Nutzung, so ist der Nutzer zu Folgendem verpflichtet:

- Befindet sich der TAN-Generator auf einer Chipkarte mit Zahlungsfunktionen (z. B. VR-BankCard), hat er das Kreditinstitut, und zwar möglichst die kontoführende Stelle, unverzüglich zu benachrichtigen. Den Verlust der Karte kann der Karteninhaber auch gegenüber dem Zentralen Sperrannahmedienst (Telefon 0 18 05/021 021; 0,14 €/Min. bei Anruf aus dem Festnetz der Deutschen Telekom. Bei Anruf aus einem Mobilfunknetz können höhere Kosten entstehen.) anzeigen. In diesem Fall ist eine Kartensperre nur möglich, wenn der Name des Kreditinstituts – möglichst mit Bankleitzahl – und die Kontonummer angegeben werden. Der Zentrale Sperrannahmedienst sperrt alle für die betreffenden Konten ausgegebenen Karten sowie gegebenenfalls den Zugriff auf zusätzlich definierte Konten, auf die der Karteninhaber Zugriff hat, für die weitere Nutzung an Geldautomaten, an automatisierten Kassen sowie den TAN-Generator. Zur Beschränkung der Sperre auf die abhanden gekommene Karte muss sich der Karteninhaber mit seinem Kreditinstitut, möglichst mit der kontoführenden Stelle, in Verbindung setzen. Wird die Karte gestohlen oder missbräuchlich verwendet, ist unverzüglich Anzeige bei der Polizei zu erstatten. Sobald dem Kreditinstitut oder dem Zentralen Sperrannahmedienst der Verlust der Karte angezeigt worden ist, trägt das Kreditinstitut die danach durch missbräuchliche Nutzung des Online-Banking entstandenen Schäden.
- Befindet sich der TAN-Generator auf einer Chipkarte ohne Zahlungsfunktion oder auf einem anderen elektronischen Gerät, so ist der Nutzer verpflichtet, sein Kreditinstitut, und zwar möglichst die kontoführende Stelle, unverzüglich zu benachrichtigen. In diesem Fall wird das Kreditinstitut den TAN-Generator sperren. Das Kreditinstitut haftet ab dem Zugang der Sperrnachricht des Nutzers für alle Schäden, die aus ihrer Nichtbeachtung entstehen.

Besondere Regelungen für das mobile TAN-Verfahren

19 Begriffsbestimmung mobiles TAN-Verfahren

Beim mobilen TAN-Verfahren ist ein Mobiltelefon erforderlich. Das Mobiltelefon besteht aus dem entsprechenden Gerät (ME) sowie aus der Chipkarte (SIM) des Telekommunikations-Netzbetreibers. Für das mobile TAN-Verfahren wird der Telekommunikationsanschluss des Nutzers registriert. Auf das registrierte Mobiltelefon wird dem Nutzer von der Bank bei Bedarf eine TAN durch eine Textmeldung (SMS) übermittelt.

20 Weitere Maßnahmen zur Geheimhaltung der TAN

Das registrierte Mobiltelefon darf nicht dazu verwendet werden, den Online-Banking-Zugang zum Institut gemäß Nummer 3 herzustellen.

21 Weitere Maßnahmen bei Verlust des Mobiltelefons

Stellt der Nutzer den Verlust seines Mobiltelefons oder der SIM-Karte fest oder besteht der Verdacht seiner missbräuchlichen Nutzung, so ist der Nutzer zu Folgendem verpflichtet:

Der Nutzer hat das Kreditinstitut, und zwar möglichst die kontoführende Stelle, unverzüglich zu benachrichtigen. Zusätzlich ist das Telefon auch beim jeweiligen Mobilfunkbetreiber zu sperren.

22 Verwendung der TAN beim mobilen TAN-Verfahren

Der Benutzer erhält von der Bank auf Anforderung durch eine entsprechende Online-Anwendung eine Textmeldung (SMS) mit einer TAN auf das registrierte Mobiltelefon. Die so übermittelte mobile TAN ist nur für den Auftrag zu nutzen, für den angefordert wurde.

Besondere Regelungen für die elektronische Signatur

23 Legitimationsverfahren und deren Geheimhaltung

(1) Der Nutzer ist verpflichtet, die mit dem Kreditinstitut vereinbarten Sicherungsmaßnahmen durchzuführen. Mit Hilfe der mit dem Kreditinstitut vereinbarten Medien identifiziert und legitimiert sich der Nutzer gegenüber dem Kreditinstitut.

(2) Der Nutzer hat dafür Sorge zu tragen, dass keine andere Person in den Besitz der Identifikations- und Legitimationsmedien kommt oder Kenntnis von dem zu deren Schutz dienenden Passwort erlangt. Jede Person, die im Besitz der Medien ist und das Passwort kennt, hat die Möglichkeit, das Online-Banking-Leistungsangebot zu nutzen und z. B. Aufträge zulasten des Kontos/Depots zu erteilen.

(3) Insbesondere Folgendes ist zur Geheimhaltung der Identifikations- und Legitimationsmedien zu beachten:

- Die den Nutzer identifizierenden Daten dürfen nicht außerhalb der Sicherheitsmedien, z. B. auf der Festplatte des Rechners, gespeichert werden. Werden die identifizierenden Daten auf ein anderes Medium übertragen, so sind sie auf dem Quell-Medium sorgfältig zu löschen bzw. das Quell-Medium ist vollständig zu vernichten.
- Die Identifikations- und Legitimationsmedien sind nach Beendigung der Online-Banking-Nutzung aus dem Lesegerät zu entnehmen und sicher zu verwahren. Sofern dies nicht möglich ist, ist das gesamte Gerät, das die Schlüssel enthält, sicher zu verwahren.
- Das zum Schutz der Identifikations- und Legitimationsmedien dienende Passwort darf nicht notiert oder elektronisch abgespeichert werden.
- Bei Eingabe des Passwortes ist sicherzustellen, dass Dritte dieses nicht ausspähen können.

24 Maßnahmen bei Bekanntwerden der PIN oder des Signaturmediums

Stellt der Nutzer fest, dass eine andere Person von der PIN seines Signaturmediums (oder im Fall einer Schlüssel-Diskette von den Schlüsseln) Kenntnis erhalten hat oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so ist der Nutzer verpflichtet, unverzüglich seine PIN zu ändern bzw. den Online-Banking-Zugang zum Konto/Depot mit dem Signaturmedium sperren zu lassen. Sofern ihm dies nicht möglich ist, hat er das Kreditinstitut unverzüglich zu unterrichten. In diesem Fall wird das Kreditinstitut den Online-Banking-Zugang zum Konto/Depot sperren. Das Kreditinstitut haftet ab dem Zugang der Sperrnachricht des Nutzers für alle Schäden, die aus ihrer Nichtbeachtung entstehen.

25 Maßnahmen bei Verlust des Signaturmediums

Stellt der Nutzer den Verlust seines Signaturmediums fest oder besteht der Verdacht seiner missbräuchlichen Nutzung, so ist der Nutzer zu Folgendem verpflichtet:

- Befindet sich das Signaturmedium auf einer Chipkarte mit Zahlungsfunktionen (z. B. VR-BankCard), hat er das Kreditinstitut, und zwar möglichst die kontoführende Stelle, unverzüglich zu benachrichtigen. Den Verlust der Karte kann der Karteninhaber auch gegenüber dem Zentralen Sperrannahmendienst (Telefon 0 18 05/021 021; 0,14 €/Min. bei Anruf aus dem Festnetz der Deutschen Telekom. Bei Anruf aus einem Mobilfunknetz können höhere Kosten entstehen.) anzeigen. In diesem Fall ist eine Kartensperre nur möglich, wenn der Name des Kreditinstituts – möglichst mit Bankleitzahl – und die Kontonummer angegeben werden. Der Zentrale Sperrannahmendienst sperrt alle für die betreffenden Konten ausgegebenen Karten sowie gegebenenfalls den Zugriff auf zusätzlich definierte Konten, auf die der Karteninhaber Zugriff hat, für die weitere Nutzung an Geldautomaten, an automatisierten Kassen sowie das Signaturmedium. Zur Beschränkung der Sperre auf die abhanden gekommene Karte muss sich der Karteninhaber mit seinem Kreditinstitut, möglichst mit der kontoführenden Stelle, in Verbindung setzen. Wird die Karte gestohlen oder missbräuchlich verwendet, ist zusätzlich unverzüglich Anzeige bei der Polizei zu erstatten. Sobald dem Kreditinstitut oder dem Zentralen Sperrannahmendienste der Verlust der Karte angezeigt worden ist, trägt das Kreditinstitut die danach durch missbräuchliche Nutzung des Online-Banking entstandenen Schäden.
- Befindet sich das Signaturmedium auf einer Chipkarte ohne Zahlungsfunktion oder auf einem anderen elektronischen Gerät oder ist das Signaturmedium eine Diskette, so ist der Nutzer verpflichtet, sein Kreditinstitut, und zwar möglichst die kontoführende Stelle, unverzüglich zu benachrichtigen. In diesem Fall wird das Kreditinstitut das Signaturmedium sperren. Das Kreditinstitut haftet ab dem Zugang der Sperrnachricht des Nutzers für alle Schäden, die aus ihrer Nichtbeachtung entstehen.