Bedingungen für das Online-Banking (nachfolgend „Webbanking“)
Landesbank Hessen-Thüringen Girozentrale

1. Leistungsangebot

(1) Der Kontoinhaber und dessen Bevollmächtigte können Bankgeschäfte mittels Webbanking in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels Webbanking abrufen.
(2) Kontoinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet.
(3) Zur Nutzung des Webbanking gelten die mit der Bank gesondert vereinbarten Verfügungslimite. Eine Änderung dieser Limite kann der Kontoinhaber mit der Bank gesondert vereinbaren. Bevollmächtigte können nur eine Herabsetzung vereinbaren.

2. Voraussetzungen zur Nutzung des Webbanking

(1) Der Teilnehmer kann das Webbanking nutzen, wenn die Bank ihn authentifiziert hat.
(2) Authentifizierung ist das mit der Bank gesondert vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Teilnehmers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3) sowie Aufträge erteilen (siehe Nummer 4).
(3) Authentifizierungselemente sind
- Wissenselemente, also etwas, das nur der Teilnehmer weiß (z. B. persönliche Identifikationsnummer [PIN])
- Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z. B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern [TAN]), die den Besitz des Teilnehmers nachweisen, wie das photoTAN-Lesegerät.

(4) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissenselement und den Nachweis des Besitzelements an die Bank übermittelt.

3. Zugang zum Webbanking

Der Teilnehmer erhält Zugang zum Webbanking der Bank, wenn
- er seine individuelle Teilnehmerkennung (Anmeldename) angibt und
- er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselements ausweist und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9) vorliegt.

Nach Gewährung des Zugangs zum Webbanking kann auf Informationen zugegriffen oder können nach Nummer 4 Aufträge erteilt werden.

4. Aufträge

4.1. Auftragserteilung

Der Teilnehmer muss einem Auftrag (z. B. Überweisung) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z.B. Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden. Die Bank bestätigt mittels Webbanking den Eingang des Auftrags.

4.2. Widerruf von Aufträgen

Die Widerrufbarkeit eines Webbanking-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Bedingungen (z. B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des Webbanking erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im Webbanking ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der Webbanking-Seite der Bank oder im „Preis- und Leistungsverzeichnis“ bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem auf der Webbanking-Seite der Bank oder im „Preis- und Leistungsverzeichnis“ angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß Webbanking-Seite der Bank oder gemäß „Preis- und Leistungsverzeichnis“ der Bank, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Geschäftstag.

(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
- Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4.1)
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Überweisung) liegt vor.

- Das Webbanking-Datenformat ist eingehalten.
- Das gesondert vereinbarte Webbanking-Verfügungslimit ist nicht überschritten (vgl. Nummer 1 Absatz 3).
- Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Bedingungen (z. B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Bedingungen (z. B. Bedingungen für den Überweisungsverkehr) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen. Sie wird den Teilnehmer hierüber mittels Webbanking eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

6. Information des Kontoinhabers über Webbanking-Verfügungen

Die Bank unterrichtet den Kontoinhaber im Rahmen des vereinbarten Turnus über die mittels Webbanking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7. Sorgfaltspflichten des Teilnehmers

7.1. Schutz der Authentifizierungselemente

(1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Webbanking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vgl. Nummer 3 und 4).

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:

(a) Wissenselemente, wie z. B. die PIN, sind geheim zu halten; sie dürfen insbesondere

- nicht mündlich (z. B. telefonisch oder persönlich) mitgeteilt werden
- nicht außerhalb des Webbanking in Textform (z. B. per E-Mail, Messenger-Dienste) weitergegeben werden
- nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und
- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z. B. photoTAN-Lesegerät) dient.

(b) Besitzelemente (z. B. photoTAN-Lesegerät) sind vor Missbrauch zu schützen, insbesondere

- ist das photoTAN-Lesegeräte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,
- ist die Anwendung für das Webbanking auf dem Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem Endgerät aufgibt (z. B. durch Weitergabe oder Entsorgung des photoTAN-Lesegeräts),
- dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Webbanking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden und
- muss der Teilnehmer, der von der Bank eine photoTAN-Aktivierungsgrafik zur Aktivierung des Besitzelements erhalten hat, diese vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Webbanking des Teilnehmers aktivieren.

7.2. Sicherheitshinweise der Bank

Der Teilnehmer muss die Sicherheitshinweise auf der Webbanking-Seite der Bank, insbesondere Maßnahmen zum Schutz der von ihm eingesetzten Hard- und Software, beachten.

7.3. Prüfung der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer die von ihr empfangenen Auftragsdaten (z. B. Betrag, Kontonummer des Zahlungsempfängers) über das gesondert vereinbarte Gerät des Teilnehmers an. Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

8. Anzeige- und Unterrichtungspflichten

8.1. Sperranzeige

(1) Stellt der Teilnehmer

- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. photoTAN-Lesegerät) oder

- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungselements

fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle abgeben.

(2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch eines Authentifizierungselements unverzüglich bei der Polizei zur Anzeige zu bringen.

(3) Hat der Teilnehmer den Verdacht, einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben

8.2. Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Kontoinhaber hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9. Nutzungssperre

9.1. Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 8.1,

- den Webbanking-Zugang für ihn oder alle Teilnehmer oder
- seine Authentifizierungselemente zur Nutzung des Webbanking.

9.2. Sperre auf Veranlassung der Bank

(1) Bei wiederholter Falscheingabe des Passworts erhöht sich die temporäre Sperrzeit des Zugangs exponentiell. Über die Dauer der Sperrzeit wird der Teilnehmer nach jeder Falscheingabe vom Webbanking-System informiert. Die Sperrzeit kann weder über das Webbanking noch von Mitarbeitern der Bank aufgehoben werden.

(2) Die Bank darf den Webbanking-Zugang für einen Teilnehmer sperren, wenn

- sie berechtigt ist, den Webbanking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente des Teilnehmers dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.

(3) Die Bank wird den Kontoinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

9.3. Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kontoinhaber unverzüglich.

10. Haftung

10.1. Haftung der Bank bei Ausführung eines nicht autorisierten Auftrags und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags

Die Haftung der Bank bei einem nicht autorisierten Auftrag und einem nicht, fehlerhaft oder verspätet ausgeführten Auftrag richtet sich nach den für die jeweilige Auftragsart vereinbarten Bedingungen (z. B. Bedingungen für den Überweisungsverkehr).

10.2. Haftung des Kontoinhabers bei missbräuchlicher Nutzung der Authentifizierungselemente

10.2.1. Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

(2) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn

- es dem Teilnehmer nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder

– der Verlust des Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder den Schaden durch vorsätzliche oder seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach
- Nummer 7.1 Absatz 2
- Nummer 7.3 oder
- Nummer 8.1 Absatz 1

verletzt hat.

(4) Abweichend von den Absätzen 1 und 3 ist der Kontoinhaber nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen und Besitz.

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.

(6) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(7) Die Absätze 2 und 4 bis 6 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

(8) Ist der Kontoinhaber kein Verbraucher, gilt ergänzend Folgendes:
– Der Kontoinhaber haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 Euro nach Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
– Die Haftungsbeschränkung in Absatz 2 erster Spiegelstrich findet keine Anwendung.

10.2.2. Haftung ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Webbanking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

10.2.3. Haftungsausschluss

Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.

11. Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit

Für die Beilegung von Streitigkeiten mit der Bank kann sich der Kontoinhaber an die im „Preis- und Leistungsverzeichnis“ näher bezeichneten Streitschlichtungs- und Beschwerdestellen wenden.