

1. Leistungsangebot

(1) Der Karteninhaber – nachfolgend als »Teilnehmer« bezeichnet – ist berechtigt, den BW Kartenservice Online (KSO) in dem von der Baden-Württembergischen Bank – nachfolgend als »Bank« bezeichnet – angebotenen Umfang für die von ihm dort verwaltete Kredit- oder Debitkarte (nachstehend Karte genannt) zu nutzen. Zudem kann er Informationen der Bank mittels KSO abrufen.

2. Voraussetzungen zur Nutzung des KSO

(1) Der Teilnehmer kann den KSO 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

- Wissensselemente, 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 mobile Endgerät) oder
- Seinsselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissensselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinsselements an die Bank übermittelt.

3. Zugang zum KSO

(1) Der Teilnehmer erhält Zugang zum KSO der Bank, wenn

– er seine individuelle Teilnehmerkennung (z. B. Kartennummer) angibt und

– er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und

– keine Sperre des Zugangs (siehe Nummern 8.1 und 9) vorliegt.

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

(2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Absatz 26 Satz 1 ZAG (z. B. zum Zweck der Änderung der Anschrift Teilnehmers) fordert die Bank den Teilnehmer auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum KSO nur ein Authentifizierungselement angefordert wurde.

4. Aufträge

4.1 Auftragserteilung

Der Teilnehmer muss einem Auftrag (z. B. Kontoübertrag auf eigenes Girokonto des Teilnehmers, Änderung der Anschrift des Teilnehmers) 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 KSO den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

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

5. Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der Aufträge (z. B. Kontoübertrag auf eigenes Girokonto des Teilnehmers) erfolgt an den für die Abwicklung der jeweiligen Auftragsart im »Preis- und Leistungsverzeichnis« bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufs. Geht der Auftrag nach dem im »Preis- und Leistungsverzeichnis« angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß »Preis- und Leistungsverzeichnis« der Bank, so gilt der Auftrag als am darauffolgenden 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. Kontoübertrag auf eigenes Girokonto des Teilnehmers, Änderung der Anschrift des Teilnehmers) liegt vor.
- Das KSO-Datenformat ist eingehalten.
- Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Bedingungen 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 aus.

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

6. Information des Teilnehmers über KSO-Verfügungen

Die Bank unterrichtet den Teilnehmer mindestens einmal monatlich über die mittels KSO getätigten Verfügungen (z. B. Kontoüberträge auf eigenes Girokonto des Teilnehmers) auf dem hierfür 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 der KSO 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) Wissensselemente, wie z. B. die PIN, sind geheim zu halten; sie dürfen insbesondere – nicht mündlich (z. B. telefonisch oder persönlich) mitgeteilt werden,
- nicht außerhalb des KSO in Textform (z. B. per E-Mail, Messenger-Dienst) 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. ein mobiles Endgerät) oder zur Prüfung des Seinsselements (z. B. mobiles Endgerät mit Anwendung für KSO und Fingerabdrucksensor) dient.

(b) Besitzelemente, wie z. B. ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere – ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z. B. Mobiltelefon) nicht zugreifen können,

– ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindliche Anwendung für den KSO (z. B. BW-Secure App) nicht nutzen können,

– ist die Anwendung für den KSO (z. B. BW-Secure App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons)

– dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des KSO 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 einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für den KSO) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für den KSO des Teilnehmers aktivieren.

(c) Seinsselemente, wie z. B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für den KSO nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinsselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für den KSO genutzt wird, Seinsselemente anderer Personen gespeichert, ist für den KSO das von der Bank ausgegebene Wissensselement (z. B. PIN in der Anwendung BW-Secure) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinsselement.

7.2 Sicherheitshinweise der Bank

Der Teilnehmer muss die Sicherheitshinweise auf der KSO-Seite der Bank, insbesondere die 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 des Kontoübertrags auf eigenes Konto des Teilnehmers) Kontonummer des Empfängerkontos bei Kontoübertrag auf eigenes Konto des Teilnehmers, über das gesondert vereinbarte Gerät des Teilnehmers an (z. B. mittels mobilen Endgeräts). 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. mobiles Endgerät) 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 Teilnehmer 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 KSO-Zugang für ihn oder seine Authentifizierungselemente zur Nutzung des KSO.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Zugang zum KSO für einen Teilnehmer sperren, wenn

– sie berechtigt ist, den Vertrag zum KSO 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 des Authentifizierungsinstrumentes besteht.

(2) Die Bank wird den Teilnehmer unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

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 Teilnehmer unverzüglich.

9.4 Automatische Sperre des Zugangs für KSO

Wird dreimal in Folge ein falsches Authentifizierungselement (z. B. die PIN) eingegeben, so sperrt die Bank automatisch den Zugang zum KSO für diesen Teilnehmer. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des KSO wiederherzustellen.

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 (z. B. Kontoübertrag auf eigenes Girokonto des Teilnehmers) und einem nicht, fehlerhaft oder verspätet ausgeführten Auftrag richtet sich nach den für die jeweilige Auftragsart vereinbarten Bedingungen.

10.2 Haftung des Teilnehmers bei missbräuchlicher Nutzung der Authentifizierungselemente

10.2.1 Haftung des Teilnehmers 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 Teilnehmer für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 EUR, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

(2) Der Teilnehmer 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/Zweigstelle 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 seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Teilnehmer 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 Teilnehmer nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Sein (siehe Nummer 2 Absatz 3).

(5) Der Teilnehmer 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.

(6) Die Absätze 2 und 4 sowie 5 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

(7) Ist der Teilnehmer kein Verbraucher, gilt ergänzend Folgendes:

– Der Teilnehmer haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 EUR 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 Satz 1 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 KSO-Aufträge 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 Teilnehmer an die im »Preis- und Leistungsverzeichnis« näher bezeichneten Streitschlichtungs- und Beschwerdestellen wenden.