Anlage 5

Vereinbarung über die Nutzung von Kwitt

Änderungen zum 14.09.2019 aufgrund der Einführung der Echtzeit-Überweisung und des Inkrafttretens der PSD2 RTS sind unterstrichen.

5. Entgelte
(1) Die vom Kontoinhaber gegenüber der Bank geschuldeten Entgelte für die Nutzung von Kwitt sind Folgende:

Nutzungsentgelt Kwitt, monatlich:	wie bisher
Entgelt je Anmeldung elektronisches Kommunikationsgerät:	wie bisher

Von der Vereinbarung über die Nutzung von Kwitt unberührt bleiben die für die Nutzung des zugrunde liegenden Zahlungsverkehrskontos vereinbarten Entgelte sowie gegebenenfalls anfallende Steuern.

6. Leistungsangebot
Kwitt bietet die Möglichkeit, unter Einsatz eines elektronischen Kommunikationsgeräts mit Datenverbindung (z.B. Mobiltelefon) und einer auf diesem Kommunikationsgerät installierten Software (Banking-App) unter bestimmten Bedingungen von dem vereinbarten Konto des Teilnehmers Überweisungen (Zahlungsaufträge) an Dritte auszuführen, die ebenfalls für die Nutzung registriert sind.
Mittels Kwitt getätigte Verfügungen werden soweit möglich als Echtzeit-Überweisungen ausgeführt, ansonsten als SEPA-Überweisungen.

7. Voraussetzungen zur Nutzung von Kwitt
(1) Der Teilnehmer kann Kwitt 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 bestimmten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Teilnehmers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen sowie Aufträge erteilen (siehe Nummer 9 dieser Bedingungen).

(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 Empfang von einmal verwendbaren Transaktionsnummern [TAN], die den Besitz des Teilnehmers nachweisen wie die girocard mit TAN-Generator oder das mobile Endgerät), oder
- Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z.B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

(4) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß den Anforderungen der Bank mindestens zwei der drei oben genannten Authentifizierungselemente an die Bank übermittelt (starke Kundenauthentifizierung). Im Fall von Kleinbetragszahlungen nach Art. 16 DelV kann die Bank von den Vorgaben einer starken Kundenauthentifizierung absehen.

8. Personalisierte Sicherheitsmerkmale
entfällt

9. Authentifizierungsinstrumente
entfällt

8. Zugang zu Kwitt
Der Teilnehmer erhält Zugang zu Kwitt, wenn
- er seine individuelle Teilnehmerkennung (z.B. VR-NetKey) angibt und
- er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
- keine Sperre des Zugangs (vgl. Nummern 13.1, 14 dieser Bedingungen) vorliegt.

Nach Gewährung des Zugangs zu Kwitt kann der Teilnehmer Aufträge erteilen und Kommunikationsmöglichkeiten nutzen.

9. Aufträge

9.1 Auftragserteilung
Der Teilnehmer muss einem Auftrag (Überweisungen) zu dessen Wirksamkeit ab Zahlungsbeträgen von mehr als 30,00 € zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z.B. Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden (vgl. Nummer 7, Absatz 3). Die Bank bestätigt mittels Banking-App den Eingang des Auftrags.

9.3 Widerruf von Aufträgen
Die Widerrufbarkeit eines erteilten Auftrags richtet sich nach den Sonderbedingungen für den Überweisungsverkehr und, sofern der Auftrag als Echtzeit-Überweisung durchgeführt wird, ergänzend nach den Sonderbedingungen für die Ausführung von Echtzeit-Überweisungen. Der Widerruf von Aufträgen kann nur außerhalb der Anwendungssoftware erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit innerhalb der Anwendungssoftware ausdrücklich vor.

10. Bearbeitung von Zahlungsaufträgen durch die Bank
(1) Die Bearbeitung von Aufträgen, die mit Hilfe von Kwitt nicht als Echtzeit-Überweisung erteilt und ausgeführt werden, erfolgt an den für Überweisungen auf der Online-Banking-Seite der Bank oder im „Preis- und Leistungsverzeichnis" bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufs. Geht der Auftrag nach dem im „Preis- und Leistungsverzeichnis" bestimmten 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 Tag. Sofern die Ausführung als Echtzeit-Überweisung erfolgt, sind im Hinblick auf die Ausführungsfristen die besonderen Bedingungen der Echtzeit-Überweisung sowie des „Preis- und Leistungsverzeichnis" der Bank maßgeblich.

(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
- Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 9.1 dieser Bedingungen).
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart liegt vor.
- Das Datenformat ist eingehalten.
- Das gesondert vereinbarte Verfügungslimit ist nicht überschritten.
- Die weiteren Ausführungsbedingungen nach den maßgeblichen Sonderbedingungen (z.B. ausreichende Kontodeckung gemäß den Sonderbedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Aufträge nach Maßgabe der Bestimmungen der Sonderbedingungen für den Überweisungsverkehr sowie Nr. 17 aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen und dem Teilnehmer hierüber mittels Banking-App 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, mittels Banking-App zur Verfügung stellen.

11. Information des Kunden über den Zahlungsvorgang
Die Bank unterrichtet den Kunden mindestens einmal monatlich über die mittels Kwitt getätigten Zahlungsvorgänge auf dem für Kontoinformationen vereinbarten Weg.

12. Sorgfalts- und Mitwirkungspflichten des Teilnehmers

12.2 Schutz der Authentifizierungselemente
(1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 7 dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass Kwitt missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vgl. Nr. 8 und 9 dieser Bedingungen).

(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. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden,

- nicht vor dem Zugriff anderer Personen ungesichert elektronisch gespeichert werden (z.B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) und

- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z.B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z.B. mobiles Endgerät mit Anwendung für Kwitt und Fingerabdrucksensor) dient.

(b) Besitzelemente, wie z.B. die girocard mit TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere

sind die girocard mit TAN-Generator oder die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,

- 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 Kwitt (z.B. Banking-App, Authentifizierungs-App) nicht nutzen können,

- ist die Anwendung für Kwitt (z.B. Banking-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z.B. durch Verkauf des Mobiltelefons),

- dürfen die Nachweise des Besitzelements (z.B. TAN) nicht außerhalb von Kwitt 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 Kwitt) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ein Gerät als Besitzelement für den Kwitt-Zugang des Teilnehmers aktivieren.

(c) Seinselemente, wie z.B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für Kwitt nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für Kwitt genutzt wird, Seinselemente anderer Personen gespeichert, ist für Kwitt das von der Bank ausgegebene Wissenselement (z.B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

(3) Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen werden (z.B. Mobiltelefon), nicht gleichzeitig für Kwitt genutzt werden.

(4) Ungeachtet der Schutzpflichten nach den Absätzen 1 bis 3 darf der Teilnehmer zur Auslösung eines Auftrags und zum Abruf von Informationen über ein Zahlungskonto seine Authentifizierungselemente gegenüber einem von ihm ausgewählten Zahlungsauslösedienst und Kontoinformationsdienst verwenden.

12.4 Prüfung der Auftragsdaten mit von der Bank angezeigten Daten

Die Bank zeigt dem Teilnehmer die von ihm empfangenen Auftragsdaten (z.B. Betrag, Name des Empfängers) über das gesondert vereinbarte Gerät des Teilnehmers an (z.B. mittels mobilem Endgerät, Chipkartenlesegerät mit Display). Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

13 Anzeige- und Unterrichtungspflichten

13.1 Sperranzeige

(1) Stellt der Teilnehmer

- den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z.B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder
- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungselements fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle aufgeben.

(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.

14. Nutzungssperre

14.1 Sperre auf Veranlassung des Teilnehmers
Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nr. 13.1
- die Nutzung von Kwitt für ihn oder alle Teilnehmer oder
- seine Authentifizierungselemente zur Nutzung von Kwitt.

14.2 Sperre auf Veranlassung der Bank
(1) Die Bank darf den Zugang zu Kwitt für einen Teilnehmer sperren, wenn
- sie berechtigt ist, die Vereinbarung über die Nutzung von Kwitt aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit seiner Authentifizierungselemente dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.

(2) Die Bank wird den Kunden unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten.

14.3 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 Kunden unverzüglich.

14.4 Automatische Sperre eines Chip-basierten Zahlungsinstruments
(1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn der Nutzungscode für die elektronische Signatur dreimal in Folge falsch eingegeben wird.

(2) Ein TAN-Generator als Bestandteil einer Chipkarte, der die Eingabe eines eigenen Nutzungscodes erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.

(3) Die in den Absätzen 1 und 2 genannten Besitzelemente können dann nicht mehr für Kwitt genutzt werden. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten von Kwitt wiederherzustellen.

15. Haftung

15.1 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 Kwitt-Auftrag und einem nicht, fehlerhaft oder verspätet ausgeführten Zahlungsvorgang richtet sich nach den Sonderbedingungen für den Überweisungsverkehr sowie gegebenenfalls nach den Sonderbedingungen für die Ausführung von Echtzeit-Überweisungen.

15.2 Haftung des Kunden bei missbräuchlicher Nutzung seiner Authentifizierungselemente

15.2.1 Haftung des Kunden 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 ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige rechtsmissbräuchliche 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 seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kunde abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere dann vorliegen, wenn er seine Sorgfaltspflichten nach Nummer 12.2 Abs. 2, Nummer 12.2 Abs. 4, Nummer 12.4 oder Nummer 13.1 Abs. 1 verletzt hat. Die Verwendung eines Authentifizierungselements gegenüber einem Zahlungsauslösedienst und Kontoinformationsdienst zur Auslösung eines Zahlungsauftrags oder zum Abruf von Informationen durch den Teilnehmer stellt kein schuldhaftes Verhalten dar.

(4) Abweichend von den Absätzen 1 und 3 ist der Kunde nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Abs. 24 Zahlungsdiensteaufsichtsgesetz nicht verlangt hat.

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

(6) Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nr. 13.1 dieser Bedingungen 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 Absätzen 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.

15.2.2 Haftung der Bank ab der Sperranzeige

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

17. Geltung Allgemeiner Geschäftsbedingungen

Ergänzend gelten die Allgemeinen Geschäftsbedingungen der Bank (AGB), die „Sonderbedingungen für den Überweisungsverkehr" sowie die Sonderbedingungen für die Ausführung von Echtzeit-Überweisungen. Der Wortlaut dieser Bedingungen kann in den Geschäftsräumen der Bank eingesehen werden; auf Wunsch werden diese ausgehändigt. Sie stehen zudem in der Online-Banking-Anwendung zur Einsicht und zum Herunterladen zur Verfügung.