Schoellerbank
Private Banking

Electronic Banking Bedingungen der Schoellerbank AG

Schoellerbank Electronic Banking (Schoellerbank Online Banking, Schoellerbank Business Banking sowie Multi Bank Standard Service (MBS-Service)) ermöglicht für entsprechend definierte Konten die Durchführung von Bankgeschäften, insbesondere von Zahlungs- und Wertpapieraufträgen und Konto-/Depotabfragen. Der Leistungsumfang kann je nach Bankprodukt unterschiedlich sein oder abweichen.

A Internetbanking

1. Allgemein

1.1 Internetbanking (Schoellerbank Online Banking) ist ein spezielles Dienstleistungsprodukt der Schoellerbank AG (im Folgenden kurz: Bank), durch das ein Kunde als Konto-/Depotinhaber oder Zeichnungsberechtigter über eine Datenübertragungsleitung via Internet eine Kommunikation mit dem Bankrechenzentrum aufbauen und nach elektronischer Autorisierung Informationen abfragen sowie Aufträge zu Konten und Wertpapierdepots erteilen kann.

Im Rahmen des Internetbankings kann auch eine für mobile Geräte (z.B. Smartphones und Tablets) optimierte Version des Internetbankings genutzt werden.

1.2 Zwischen dem Kunden und der Bank wird der „Online Banking Antrag“ oder „Online Banking Antrag mit Portfolioansicht“ der Bank (im Folgenden kurz: die Vereinbarung) auf unbefristete Dauer abgeschlossen, aufgrund dessen der Kunde zur Nutzung des Internetbankings berechtigt ist. Der Kunde erhält damit zu allen Konten und Depots, bei welchen er Konto- bzw. Depotinhaber ist, die Internetbanking-Berechtigung. Der Konto- bzw. Depotinhaber muss der Erteilung einer Internetbanking-Berechtigung an einen Zeichnungsberechtigten schriftlich zustimmen. Bei einem Gemeinschaftskonto/-depot müssen alle Konto- bzw. Depotinhaber der Erteilung der Internetbanking-Berechtigung an einen einzelnen Konto- bzw. Depotinhaber oder an einen Zeichnungsberechtigten schriftlich zustimmen.

Sofern bei einem Depot ein kollektives Zeichnungsrecht vereinbart ist, können über Internetbanking keine Aufträge vorgenommen werden, sondern ist die Internetbanking-Berechtigung bei diesen Depots auf die Einholung von Depotinformationen beschränkt. Bei einer kollektiven Zeichnung auf einem Konto, kann der Kunde die beabsichtigte Transaktion nur mit sämtlichen weiteren berechtigten Personen vornehmen.

Ein nur von einem kollektiv zeichnungsberechtigten Benutzer mit seiner TAN erstgezeichneter Auftrag, der nicht binnen 28 Tagen vom zweiten kollektiv zeichnungsberechtigten Benutzer mittels seiner TAN gegengezeichnet wird, wird ohne weitere Kontoinformation seitens der Bank unwiderruflich und ohne Durchführung aus dem System gelöscht.

2. Definitionen

2.1 Benutzername (= Benutzerkennung/BK)

Jeder Kunde erhält von der Bank einen einzigartigen, mehrstelligen Benutzernamen, anhand dessen die Bank einen Kunden eindeutig zuordnen kann. Der Benutzername wird dem Kunden anlässlich der Unterfertigung der Vereinbarung bekannt gegeben. Der Benutzername kann vom Kunden geändert werden.

PC282D - 023GI9210D 20200101

2.2 Passwort (= PIN/Persönliche Identifikationsnummer)

Dem Kunden wird von der Bank ein Passwort vorgeschlagen, welches vom Kunden im Rahmen des Ersteinstiegs in das Internetbanking abzuändern ist. Der Kunde muss sich bei jedem weiteren Einstieg in das Internetbanking unter Angabe des Benutzernamens, des selbst definierten Passworts und des entsprechenden Loginverfahrens (z.B. cardTan-Verfahren) authentifizieren. Der Kunde erhält das Passwort in einem verschlossenen Kuvert entweder anlässlich der Unterfertigung der Vereinbarung persönlich ausgehändigt oder auf dem Postweg zugesandt. Das Passwort kann vom Kunden jederzeit im Internetbanking unter Verwendung einer TAN geändert werden. Das geänderte Passwort ist bei jeder Anmeldung im Internetbanking anzugeben. Aus Sicherheitsgründen kann die Bank den Kunden beim Login in das Internetbanking auffordern, das Passwort auf ein Passwort mit mehr Zeichen bzw. mit größerem Sicherheitsniveau umzustellen. Der Kunde kann persönlich in jedem Standort der Bank während der Öffnungszeiten ein neues Passwort anfordern. Das neue Passwort wird dem Kunden sodann entweder in einem vom Kunden gewählten Standort der Bank persönlich ausgehändigt oder auf dem Postweg zugesandt.

2.3 shortPIN

Auf mobilen Endgeräten ist auch ein Zugriff mittels vereinfachter Authentifizierung (Gerätebindung in Kombination mit benutzerspezifischem vierstelligem PIN-Code) möglich.

2.4 Fido Token (Loginverfahren)

Der Fido Token (Hardware mit USB-Anschluss) ist im Handel käuflich erwerblich und ermöglicht dem Kunden, die Authentifizierung im Rahmen des Logins zum Internetbanking durchzuführen. Dazu muss der Kunde den Fido Token mit seinem Gerät über den USB-Anschluss verbinden und den Authentifizierungsvorgang bestätigen.

2.5 Transaktionsnummer (= TAN)

Eine TAN ist ein im konkreten Einzelfall generierter Authentifizierungscode, der beim Einstieg (Loginverfahren) in das Internetbanking (zusätzlich zum Benutzernamen und Passwort) und für die Erteilung von Aufträgen und die Abgabe von sonstigen rechtsverbindlichen Willenserklärungen gegenüber der Bank im Rahmen des Internetbankings zu verwenden ist.

Mit Verwendung der TAN in dem dafür vorgesehenen Feld sowie der Betätigung des dafür vorgesehenen Buttons gilt ein Auftrag als erteilt bzw. eine Willenserklärung als abgegeben.

Die Bank stellt dem Kunden verschiedene TAN-Verfahren zur Nutzung des Internetbankings zur Verfügung. Sollte die Bank ein vom Kunden genütztes TAN-Verfahren nicht weiter zur Verfügung stellen können, weil

- objektive Gründe im Zusammenhang mit der Sicherheit dieses TAN-Verfahrens oder der Systeme, für das es eingesetzt wird, eine Einstellung rechtfertigen, oder
- aufgrund gesetzlicher oder aufsichtsrechtlicher Bestimmungen die Bank ein vom Kunden genütztes TAN-Verfahren nicht weiter zur Verfügung stellen darf, wird die Bank den Kunden über die Gründe hierfür informieren und, sofern der Kunde nicht bereits ein weiteres, für ihn freigeschaltetes TAN-Verfahren mit einem höheren Sicherheitsstandard nützt, einen kostenlosen Umstieg auf ein anderes TAN-Verfahren mit einem höheren Sicherheitsstandard anbieten. Dieses Angebot wird die Bank dem Kunden auf die mit ihm im Rahmen der Geschäftsverbindung für die Zustellung von Mitteilungen vereinbarten Weise so rechtzeitig mitteilen, dass ihm dieses spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt des Umstiegs zugeht. Dieses Angebot gilt als vom Kunden angenommen, wenn vor dem vorgeschlagenen Zeitpunkt des Umstiegs kein Widerspruch des Kunden bei der Bank einlangt, wobei die Bank in der Mitteilung auf die Folgen seines Stillschweigens sowie auf das dem Kunden nach Punkt 11.3 zustehende kostenlose Kündigungsrecht hinweisen wird.

PC282D - 023GI9210D 20200101

- Sofern der Kunde in diesem Fall durch Widerspruch das Angebot der Bank nicht annimmt und von seinem Kündigungsrecht nicht Gebrauch macht, wird der Benutzername gesperrt. Widerspricht der Kunde dem angebotenen Umstieg auf ein anderes TAN-Verfahren mit einem höheren Sicherheitsstandard, wird die Einstellung des vom Kunden genutzten TAN-Verfahrens frühestens zwei Monate nach Mitteilung des Angebots auf Umstieg erfolgen. Der Kunde kann trotz eines Widerspruchs bis zur endgültigen Einstellung des von ihm genutzten TAN-Verfahrens jederzeit auf das angebotene TAN-Verfahren mit einem höheren Sicherheitsstandard umsteigen. Den Wunsch, auf das angebotene TAN-Verfahren umzusteigen, kann der Kunde der Bank entweder persönlich in einem Standort, telefonisch oder schriftlich auf dem Postweg mitteilen.

a) mobileTAN

Möchte der Kunde das mobileTAN-Verfahren verwenden, kann er dies der Bank entweder persönlich in einem Standort, telefonisch oder schriftlich auf dem Postweg mitteilen. Verwendet der Kunde das mobileTAN-Verfahren, bekommt er die für den Login in das Internetbanking, die Zeichnung einer bereits erfassten Internetbanking-Transaktion oder die Abgabe einer Willenserklärung erforderliche mobileTAN mittels SMS (Short Message Service) auf ein mobiles Gerät (wie z.B. Mobiltelefon oder Tablet) übermittelt.

Für die SMS-Benachrichtigung ist die Telefonnummer des dafür vorgesehenen Mobiltelefons vom Kunden persönlich in einem Standort rechtzeitig vor der erstmaligen Verwendung des mobileTAN-Verfahrens bekannt zu geben. Die für die Zusendung der SMS bekannt gegebene Mobiltelefonnummer kann durch den Kunden persönlich in einem Standort der Bank oder – sofern dem Kunden eine SMS auf die bei der Bank bisher gespeicherte Mobiltelefonnummer gesendet werden kann – im Internetbanking mittels mobileTAN geändert werden.

Die Möglichkeit der Änderung der Mobiltelefonnummer und die Möglichkeit der Änderung der Art der Zustellung von mobileTAN via Internetbanking können aus Sicherheitsgründen vonseiten der Bank ausgesetzt werden, wenn objektive Gründe im Zusammenhang mit der Sicherheit der persönlichen Identifikationsmerkmale oder der Systeme, für die sie benutzt werden können, dies rechtfertigen.

In der Nachricht mit der mobileTAN werden dem Kunden zu Kontrollzwecken auch Angaben über die durchzuführende Transaktion (insbesondere bei Zahlungsaufträgen: International Bank Account Number (IBAN) bzw. Kontonummer des Empfängers, Bank Identifier Code (BIC) bzw. Bankleitzahl der Bank des Empfängers und der Überweisungsbetrag) mitgeliefert.

Eine mobileTAN kann nur für die Durchführung jener Transaktion verwendet werden, für die sie angefordert wurde. Sofern ein erfasster Überweisungsauftrag nach Anforderung der mobileTAN verändert wurde, kann die zugesandte mobileTAN nicht mehr verwendet werden, sondern muss eine neue mobileTAN angefordert werden. Sobald eine mobileTAN verwendet wurde, verliert sie ihre Gültigkeit. Bei der Nutzung des mobileTAN-Verfahrens ist der Kunde verpflichtet, die in der Nachricht gemeinsam mit der mobileTAN übermittelten Auftragsdaten (z.B. IBAN des Empfängerkontos, Überweisungsbetrag) auf Übereinstimmung mit seinem Auftrag zu prüfen und die mobileTAN nur im Falle einer Übereinstimmung dieser Auftragsdaten zusammen mit dem Passwort zu verwenden.

Zustellung der mobileTAN per SMS: Der Kunde kann nur dann eine SMS mit einer mobileTAN auf das Mobiltelefon erhalten, wenn die Voraussetzungen für den Empfang von SMS erfüllt sind, wie z.B. dass:

- das Telefon technisch in der Lage ist, SMS zu empfangen,
- die vertraglichen Grundlagen mit dem Mobiltelefonprovider zum Empfang von SMS gegeben sind und
- sich der Kunde in einem Gebiet befindet, für das sein Mobiltelefonprovider die Zustellung einer SMS vorsieht.

PC282D - 023GI9210D 20200101

b) Schoellerbank ID App

Die Schoellerbank ID App ist eine Applikation für (mobile) Endgeräte und ermöglicht die Authentifizierung des Kunden. Um die Authentifizierung durchzuführen, bekommt der Kunde im Internetbanking eine Zahl angezeigt. Zur gleichen Zeit wird dem Kunden in der Schoellerbank ID App der konkrete Authentifizierungsbedarf (z.B. die Details zu einem Zahlungsauftrag) und eine Reihe von Zahlen angezeigt. Um die Authentifizierung durchzuführen muss der Kunde nun jene Zahl auswählen (durch "Touch" auf die Zahl), die ihm auch im Internetbanking angezeigt wird.

Jedes Endgerät, auf dem die App installiert ist, muss dem Kunden nach Installation der Anwendung zugeordnet werden (= Herstellung der Gerätebindung). Die Authentifizierung erfolgt mittels Gerätebindung und shortPIN oder eines biometrischen Verfahrens (Fingerprint oder FaceID). Der Benutzer kann die Gerätebindung und seine persönliche shortPIN direkt im Internetbanking ändern.

Zu Kontrollzwecken werden dem Kunden im Zuge der Freigabe auch Angaben über die durchzuführende Transaktion, insbesondere Empfänger-IBAN und Betrag oder ein Referenzcode (Elektronischer Begleitzettel) und Kontrollwert (Summe aller Aufträge) mitgeliefert. Der Kunde ist verpflichtet, diese auf Übereinstimmung mit den im Internetbanking eingegebenen Aufträgen zu prüfen. Die Freigabe darf nur bei Übereinstimmung erteilt werden.

Der Kunde kann nur dann eine Zahl von der Schoellerbank ID App auf einem mobilen Endgerät wie Smartphone oder Tablet erhalten, wenn folgende Voraussetzungen gegeben sind:

- eine aktuelle Version der vom Kunden verwendeten Internetbanking-App der Bank (Schoellerbank ID App) installiert ist,
- sich der Kunde in einem Gebiet befindet, für das eine Internet-Datenverbindung über seinen Mobiltelefonprovider oder per WLAN über einen Netzbetreiber gegeben ist.

c) cardTAN

Möchte der Kunde das cardTAN-Verfahren verwenden, hat er dies der Bank entweder persönlich in einem Standort der Bank, telefonisch oder schriftlich per Post mitzuteilen.

Für die Verwendung des cardTAN-Verfahrens benötigt er einen speziellen Kartenleser (cardTAN-Generator), eine aktive (weder gesperrte noch abgelaufene) cardTAN-fähige Karte (Debitkarte oder TANcard), sowie einen EB-PIN (Electronic Banking PIN).

Ein cardTAN-Generator kann vom Kunden direkt bei der Bank angefordert werden. Nachdem die cardTAN-fähige Karte (Debitkarte oder TANcard) in den cardTAN-Generator eingeführt und die EB-PIN eingegeben wurde, werden Daten der im Internetbanking vorzunehmenden Anmeldung oder Transaktion entweder über eine optische Schnittstelle (siehe Modus „Flicker“) oder durch manuelle Eingabe im cardTAN-Generator erfasst und verarbeitet. Dann wird über ein spezielles, auf dem Chip der Debitkarte bzw. TANcard gespeichertes Programm eine cardTAN erzeugt. Die cardTAN ist vom Kunden im Internetbanking einzugeben und wird von der Bank auf Gültigkeit geprüft. Der cardTAN-Generator kann im Modus „Flicker“ oder „manuelle Eingabe“ verwendet werden. Der Modus „Flicker“ ist die einfachere Methode, bei Problemen mit der Wiedergabe oder Übernahme des Flicker-Codes kann durch den Kunden durch Nutzung einer im Internetbanking angebotenen Umschaltmöglichkeit auf „manuelle Eingabe am cardTAN-Generator“ geändert werden.

Modus „Flicker“: Die für die Berechnung der cardTAN erforderlichen Daten, insbesondere die Transaktionsdaten, werden vom Bankserver mittels einer schwarz-weiß blinkenden Grafik über optische Schnittstellen vom Bildschirm des Eingabegeräts des Kunden (z.B. Computer, Tablet, etc.) an den cardTAN Generator übertragen. Die Transaktionsdaten, welche die vom Kunden zu autorisierende Transaktion repräsentieren, werden zur Überprüfung durch den Benutzer am Display des cardTAN-Generators angezeigt. Bei der Nutzung des cardTAN-Verfahrens mit dem Modus „Flicker“ ist der Kunde verpflichtet, die übermittelten Transaktionsdaten (z.B. bei Zahlungsaufträgen IBAN des Empfängerkontos, Überweisungsbetrag) auf Übereinstimmung mit seinem Auftrag zu prüfen und die cardTAN nur im Falle einer Übereinstimmung dieser Transaktionsdaten zu verwenden.

PC282D - 023GI9210D 20200101

Modus „manuelle Eingabe“: Dabei müssen bestimmte auf der Eingabemaske im Internetbanking abgefragte Daten, insbesondere die Transaktionsdaten, durch den Kunden selbstständig am cardTAN-Generator erfasst werden. Beim Modus „manuelle Eingabe“ hat der Kunde die eingegebenen Transaktionsdaten auf Übereinstimmung mit seinem Auftrag zu prüfen und die dafür erzeugte cardTAN nur im Falle einer Übereinstimmung dieser Transaktionsdaten zu verwenden.

Eine cardTAN kann nur für die Durchführung jener Transaktion verwendet werden, für die sie erzeugt wurde. Sofern ein erfasster Überweisungsauftrag nach Erzeugung der cardTAN verändert wurde, kann diese cardTAN nicht mehr verwendet werden, sondern muss eine neue cardTAN vom cardTAN-Generator erzeugt werden. Sobald eine cardTAN verwendet wurde, verliert sie ihre Gültigkeit.

2.6 Biometrische Daten

Bei Verwendung von Internetbanking-Apps der Bank auf mobilen Geräten (Smartphone oder Tablet) kann der Kunde – abhängig von den technischen Möglichkeiten des Endgeräts – optional das Passwort mit biometrischen Daten (wie Fingerprints oder FaceID), deren Erfassung das jeweilige Mobilgerät ermöglicht, mit der jeweiligen Internetbanking-App verbinden. In diesem Fall ersetzt die Verifizierung des Kunden anhand der von ihm in der Internetbanking-App gespeicherten biometrischen Daten die Angabe des Passworts beim Login in das mobile Internetbanking.

2.7 Persönliche Identifikationsmerkmale

Benutzername (BK), Passwort, Transaktionsnummern (TAN) sowie in Internetbanking Apps der Bank gespeicherte biometrische Daten bilden beim Internetbanking die persönlichen Identifikationsmerkmale des Kunden.

3. Authentifizierung

Die Bank prüft die Berechtigung des Kunden für die Nutzung des Internetbankings anhand der persönlichen Identifikationsmerkmale.

4. Transaktionen über Internetbanking

4.1 Die Dispositionen und Willenserklärungen (zusammen kurz: Transaktionen) können über das Internetbanking grundsätzlich 24 Stunden pro Tag und 7 Tage pro Woche an die Bank übermittelt werden. Da fallweise Wartungs- und Servicearbeiten an den Bankrechnern der Bank vorzunehmen sind, ist in der Zeit von 00:00 Uhr bis 6:00 Uhr ein Servicefenster vorgesehen. In diesem Zeitraum kann das Internetbanking bei Vornahme solcher Wartungs- und Servicearbeiten zeitweilig nicht zur Verfügung stehen. Müssen Wartungsarbeiten von 06:00 Uhr bis 24:00 Uhr stattfinden, wird die Bank die Kunden nach Möglichkeit darauf im Vorhinein hinweisen.

4.2 Der Kunde stellt die Verbindung zum Bankrechner dadurch her, dass er sich über die Homepage der Bank unter Verwendung seines Benutzernamens, seines Passworts und des jeweiligen Loginverfahrens in das Internetbanking einloggt.

Der Kunde hat die für die jeweils gewünschte Transaktion auf der Eingabemaske geforderten Angaben über Datenübertragungsleitung via Internet einzufügen. Jedenfalls hat der Kunde bei Überweisungsaufträgen immer den Kundenidentifikator des Empfängers anzugeben. Macht der Kunde über diesen hinausgehende Angaben zum Empfänger, wie insbesondere zum Namen des Empfängers oder dem Verwendungszweck, sind diese nicht Teil des Kundenidentifikators, dienen daher lediglich zu Dokumentationszwecken und bleiben bei der Ausführung der Transaktion seitens der Bank unbeachtet. Sodann hat der Kunde die gewünschte Transaktion unter Verwendung der für die jeweilige Transaktion generierten TAN und anschließender Betätigung des für die Freigabe vorgesehenen Buttons abzuschließen.

PC282D - 023GI9210D 20200101

4.3 Der Zeitpunkt, zu dem eine Transaktion via Internetbanking bei der Bank einlangt, gilt als Eingangszeitpunkt. Geht eine Transaktion via Internetbanking nicht an einem Geschäftstag der Bank oder aber nach einem Zeitpunkt nahe am Ende eines Geschäftstages ein, so wird diese Transaktion so behandelt, als wäre sie erst am nächsten Geschäftstag eingegangen. Die Bank veröffentlicht diese Uhrzeiten in den „Informationen der Schoellerbank AG zu Zahlungsdienstleistungen für Verbraucher", welche sie elektronisch auf ihrer Homepage bereithält oder in Schriftform dem Kunden auf dessen Verlangen in ihren Geschäftsstellen aushändigt oder postalisch übermittelt.

Der Kunde kann auch vorsehen, dass der Auftrag an einem in der Zukunft liegenden Datum (Terminauftrag) durchgeführt werden soll. Ist das bei einem Terminauftrag gewünschte Datum kein Geschäftstag der Bank, ist der Terminauftrag so zu behandeln, als sei er erst am darauffolgenden Geschäftstag eingegangen.

4.4 Im Rahmen des Internetbankings können zu einem Konto beliebig viele Überweisungsaufträge erteilt werden. Die Bank ist zur Durchführung eines Überweisungsauftrags nur dann verpflichtet, wenn dafür auf dem jeweiligen Konto des Kunden vollständige Deckung vorhanden ist. Der Kunde hat auch die Möglichkeit, mehrere Überweisungsaufträge zusammenzufassen und mit einer einzigen TAN freizugeben.

4.5 Allgemeines über Limits bei mobileTAN, Schoellerbank ID und bei cardTAN:

4.5.1 Beim Internetbanking können Transaktionslimits gesetzt werden.
Bei einem Transaktionslimit wird die Höhe jenes Betrages festgelegt, bis zu dem ein Überweisungsauftrag allein oder mehrere Überweisungsaufträge gemeinsam mit einer einzigen TAN erteilt werden können.

4.5.2 Ein Limit kann entweder von der Bank einseitig festgelegt (siehe Punkt 4.5.3) oder zwischen Bank und Kunde einvernehmlich vereinbart werden. In beiden Fällen handelt es sich um ein „bankseitiges Limit".

4.5.3 Die Bank ist berechtigt, ein bankseitiges Limit ohne Mitwirkung des Kunden einzuführen oder herabzusetzen, wenn

- objektive Gründe im Zusammenhang mit der Sicherheit der persönlichen Identifikationsmerkmale oder der Systeme, für die sie benutzt werden können, dies rechtfertigen, oder
- der Verdacht einer Erteilung von nicht autorisierten Aufträgen oder der betrügerischen Verwendung der persönlichen Identifikationsmerkmale besteht. Die Bank wird den Kunden über eine solche Einführung oder Herabsetzung und die Gründe hierfür möglichst vor, spätestens aber unverzüglich nach der Einführung oder Herabsetzung in der mit ihm vereinbarten Form informieren.

4.6 Ein autorisierter, bei der Bank im Wege des Internetbankings eingegangener Überweisungsauftrag kann nicht mehr widerrufen werden. Der Widerruf eines bei der Bank eingelangten Terminauftrages ist bis zum Ende des Geschäftstages vor dem vereinbarten Durchführungstag direkt im Internetbanking unter Verwendung einer gültigen TAN möglich.

4.7 eps Online-Überweisung

Im Rahmen des Internetbankings können auch eps Online-Überweisungen erteilt werden. Bei der eps Online-Überweisung handelt es sich um ein standardisiertes Bezahlverfahren bei Einkäufen im Internet und bei Inanspruchnahme von E-Government Dienstleistungen. Der Kunde erhält dabei auf der Website des Internet-Shops bzw. auf der E-Government-Webseite, die jeweils mit einem entsprechenden Logo für eps („e-payment standard") und Online-Überweisung gekennzeichnet sind, die Möglichkeit, sich unter Verwendung seines Benutzernamens/BK, seines Passworts und des jeweiligen Loginverfahrens direkt in das Internetbanking einzuloggen und die Bezahlung mittels Überweisungsauftrag vorzunehmen. Die Freigabe einer eps Online-Überweisung erfolgt wie die Freigabe jeder anderen Überweisung im Internetbanking unter Verwendung einer TAN (siehe Punkt 4.2). Im gesamten Ablauf der eps Online-Überweisung werden keine bankspezifischen Daten des Kunden von einer dritten Stelle abgefragt oder zwischengespeichert, da der Kunde sich dabei direkt auf der Website der Bank oder in der Banking-App der Bank in das Internetbanking einloggt und dort

PC282D - 023GI9210D 20200101

den Überweisungsauftrag freigibt. Im Rahmen der Abwicklung einer eps Online-Überweisung werden von der Bank auch keine bankspezifischen Daten des Käufers an den Händler übertragen. Mit Freigabe der eps Online-Überweisung durch den Kunden garantiert die Bank gegenüber dem Internet Händler bzw. der E-Government-Behörde die Ausführung der Überweisung, sodass der Kunde diese eps Online-Überweisung nicht widerrufen kann. Die eps Online-Überweisung ist lediglich ein Instrument, mit dem der Kunde eine Bezahlung im Internet durch einen Überweisungsauftrag im Internetbanking vornehmen kann. Die zwischen dem Kunden und dem Händler bestehende vertragliche Beziehung wird durch die Verwendung der eps Online-Überweisung nicht tangiert, und es sind deshalb gegenüber der Bank keine Einwendungen aus dem Grundgeschäft zulässig.

5. Kontoinformationsdienstleister und Zahlungsauslösedienstleister

5.1 Der Kunde kann bestimmten Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern Zugriff auf ein oder mehrere seiner zum Internetbanking berechtigten Zahlungskonten gewähren, indem der Kunde die Dienste dieser Dienstleister in Anspruch nimmt.

5.2 Kontoinformationsdienstleister bieten konsolidierte Informationen über ein oder mehrere Zahlungskonten eines Kontoinhabers an, die auch bei verschiedenen Kreditinstituten geführt werden können. Zahlungsauslösedienstleister lösen auf Antrag eines Kontoinhabers einen Zahlungsauftrag in Bezug auf ein anderes Zahlungskonto aus, welches auch bei einem anderen Kreditinstitut geführt werden kann.

5.3 Nimmt der Kunde die Dienste der Kontoinformationsdienstleister oder der Zahlungsauslösedienstleister in Anspruch, indem der Kunde diesen Dienstleistern Zugriff auf sein Zahlungskonto bzw. seine Zahlungskonten gewährt, so ist die Bank im Sinne der Delegierten Verordnung (EU) 2018/389 zu technischen Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation verpflichtet, mit diesen Dienstleistern auf sichere Weise zu kommunizieren und diesen die erforderlichen Authentifizierungsverfahren zur Überprüfung der Identität des Kunden bereitzustellen.

6. Sorgfalt

6.1 Der Kunde ist auch im eigenen Interesse verpflichtet, Passwort und TAN geheim zu halten und anderen Personen nicht offenzulegen (auch nicht den Mitarbeitern der Bank). Die biometrische Hinterlegung des Passworts (siehe Punkt 2.6) entbindet nicht von der Sorgfaltspflicht zur Geheimhaltung des Passworts und der TAN. Das Offenlegungsverbot des Passworts bzw. der TAN besteht nicht gegenüber Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern, deren Dienstleistungen der Kunde in Anspruch nimmt. Sobald der Kunde den Verdacht hat, dass eine andere Person Kenntnis seines Passworts hat oder eine nicht autorisierte Nutzung des Internetbankings erfolgt ist, hat er sein Passwort unverzüglich zu ändern. Aus Sicherheitsgründen wird dem Kunden empfohlen, sein Passwort regelmäßig (z.B. alle zwei Monate) selbstständig zu ändern. Die nicht autorisierte Nutzung des Internetbankings hat der Kunde unverzüglich der Internetbanking-Hotline (siehe Punkt 8.1) zu melden. Bei Diebstahl oder Verlust des Mobiltelefons zum Empfang der mobileTAN wird dem Kunden empfohlen, sein Mobiltelefon unverzüglich zu sperren.

6.2 Sollte beim Anmeldevorgang die URL nicht mit https://banking.schoellerbank.at/ beginnen oder sollte vom Browser des Kunden das Schlosssymbol als Zeichen für eine verschlüsselte Übertragung der Daten nicht angezeigt werden, sind das Hinweise darauf, dass sich der Kunde nicht auf der Homepage der Bank befindet. Es besteht dann die Gefahr, dass es sich um eine von Unbekannten zu dem Zweck eingerichtete Website handelt, dem Kunden dessen persönliche Identifikationsmerkmale herauszulocken (Phishing). In diesem Fall empfiehlt die Bank den Anmeldevorgang abzubrechen und – sofern ein oder mehrere Identifikationsmerkmale auf jener Website bereits eingegeben wurden – unverzüglich die Internetbanking-Hotline (siehe Punkt 8.1) zu verständigen.

PC282D - 023GI9210D 20200101

6.3 Bei der Nutzung des mobileTAN-Verfahrens oder der Schoellerbank ID App ist der Kunde verpflichtet, die in der Nachricht gemeinsam mit der mobileTAN übermittelten bzw. in der Schoellerbank ID App angezeigten Auftragsdaten (z.B. bei Zahlungsaufträgen IBAN des Empfängerkontos, Überweisungsbetrag) auf Übereinstimmung mit seinem Auftrag zu prüfen und die mobileTAN bzw. die in der Schoellerbank ID App angezeigte Zahl nur im Falle einer Übereinstimmung dieser Auftragsdaten zu verwenden. Bei der Nutzung des cardTAN-Verfahrens mit dem Modus „Flicker" ist der Kunde verpflichtet, die übermittelten Transaktionsdaten (z.B. bei Zahlungsaufträgen IBAN des Empfängerkontos, Überweisungsbetrag) auf Übereinstimmung mit seinem Auftrag zu prüfen und die cardTAN nur im Falle einer Übereinstimmung dieser Transaktionsdaten zu verwenden. Bei der Nutzung des cardTAN-Verfahrens mit dem Modus „manueller Eingabe" hat der Kunde die von ihm am cardTAN-Generator eingegebenen Transaktionsdaten auf Übereinstimmung mit seinem im Internetbanking erfassten Auftrag zu prüfen und die dafür erzeugte cardTAN nur im Falle einer Übereinstimmung dieser Transaktionsdaten zu verwenden.

6.4 Der Kunde ist verpflichtet bei der Nutzung von Internetbanking die in diesen Geschäftsbedingungen enthaltenen Bedingungen für die Nutzung einzuhalten und insbesondere bei der Erteilung von Aufträgen den Kundenidentifikator (siehe Punkt 4.2) korrekt anzugeben sowie dafür zu sorgen, dass er einen Überweisungsauftrag nur dann erteilt, wenn auf dem zu belastenden Konto eine zur Durchführung des Überweisungsauftrages ausreichende Kontodeckung vorhanden ist.

7. Berichtigung von nicht autorisierten Zahlungsvorgängen

Im Falle einer aufgrund eines nicht autorisierten oder fehlerhaft ausgeführten Zahlungsvorganges erfolgten Belastung kann der Kunde jedenfalls dann eine Berichtigung durch die Bank erwirken, wenn er die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Zahlungsvorganges, jedoch spätestens 13 Monate nach dem Tag der Belastung hiervon unterrichtet hat, es sei denn, die Bank hat dem Kunden die Informationen über den jeweiligen Überweisungsauftrag bzw. über die jeweilige Zahlung, welche zulasten seines Kontos ausgeführt wurde (Referenz, Betrag, Währung, Entgelt, Zinsen, Wechselkurs, Wertstellung der Belastung), nicht in der mit ihm vereinbarten Weise mitgeteilt oder zugänglich gemacht. Andere Ansprüche des Kunden auf Berichtigung werden dadurch nicht ausgeschlossen. Im Falle eines nicht autorisierten Zahlungsvorganges wird die Bank dem Kunden den Betrag des nicht autorisierten Zahlungsvorgangs unverzüglich, auf jeden Fall spätestens bis zum Ende des folgenden Geschäftstags erstatten, nachdem sie von dem Zahlungsvorgang Kenntnis erhalten hat oder dieser ihr angezeigt wurde. Die Erstattung erfolgt dadurch, dass das belastete Konto wieder auf den Stand gebracht wird, auf dem es sich ohne den nicht autorisierten Zahlungsvorgang befunden hätte, wobei der Betrag auf dem Zahlungskonto des Zahlers spätestens zum Tag der Kontobelastung wertzustellen ist. Hat die Bank der Finanzmarktaufsicht berechtigte Gründe für den Verdacht, dass ein betrügerisches Verhalten des Kunden vorliegt, schriftlich mitgeteilt, wird die Bank ihre Erstattungspflicht unverzüglich prüfen und erfüllen, wenn sich der Betrugsverdacht nicht bestätigt. Die Bank ist auch dann zur Erstattung eines nicht autorisierten Zahlungsvorgangs verpflichtet, wenn dieser über einen Zahlungsauslösedienstleister ausgelöst wurde.

8. Sperren

8.1 Jeder Konto- bzw. Depotinhaber und jeder Zeichnungsberechtigte hat die Möglichkeit, seinen Benutzernamen wie folgt sperren zu lassen:

- jederzeit telefonisch bei der Internetbanking-Hotline der Bank, deren Telefonnummer auf der Homepage www.schoellerbank.at abrufbar ist, oder
- während der Öffnungszeiten der Bank persönlich oder schriftlich in jedem Standort der Bank. Eine innerhalb der Öffnungszeiten bei der Bank oder – zu welchem Zeitpunkt auch immer – bei der Internetbanking-Hotline veranlasste Sperre wird unmittelbar mit Einlangen des Sperrauftrags wirksam. Außerhalb der Öffnungszeiten bei der Bank schriftlich einlangende Sperraufträge werden unverzüglich nach Beginn der nächsten Öffnungszeit wirksam, oder
- jederzeit die Sperre im Internetbanking auch selbst unter dem Menüpunkt Sicherheit / Sperren online durchzuführen.

PC282D - 023GI9210D 20200101

8.2 Die Bank ist berechtigt, einen Benutzernamen ohne Mitwirkung des Kunden zu sperren, wenn
- objektive Gründe im Zusammenhang mit der Sicherheit der persönlichen Identifikationsmerkmale oder der Systeme, für die sie benutzt werden können, dies rechtfertigen, oder
- der Verdacht einer Erteilung von nicht autorisierten Aufträgen oder der betrügerischen Verwendung der persönlichen Identifikationsmerkmale besteht. Die Bank wird den Kunden über die Sperre und die Gründe hierfür – soweit dies nicht innerstaatliche oder gemeinschaftsrechtliche Rechtsvorschriften sowie gerichtliche oder verwaltungsbehördliche Anordnungen verletzen oder objektiven Sicherheitserwägungen zuwiderlaufen würde – möglichst vor, spätestens aber unverzüglich nach der Sperre in der mit ihm vereinbarten Form informieren.

8.3 Nach dreimaliger Falscheingabe der persönlichen Codes beim Login wird der Zugang zum Internetbanking temporär gesperrt, weitere Fehleingaben verlängern gemäß folgender Aufstellung die vorübergehende Sperre des Zugangs für den Nutzer:
- ab dem 3. Fehlversuch 30 Sekunden Wartezeit bis zum nächsten Versuch
- ab dem 5. Fehlversuch 2 Minuten Wartezeit bis zum nächsten Versuch
- ab dem 7. Fehlversuch 10 Minuten Wartezeit bis zum nächsten Versuch
- ab dem 10. Fehlversuch 1 Stunde Wartezeit bis zum nächsten Versuch

Nach einmaliger richtiger Eingabe des persönlichen Codes ist der Zugang zum Internetbanking wiederhergestellt.

8.4 Der Kunde kann die Aufhebung der Sperre persönlich beantragen; dies kann auf jedem mit der Bank vereinbarten Kommunikationsweg geschehen (insbesondere über den Kundenbetreuer oder an einem Standort der Bank).

8.5 Die Bank ist berechtigt, einem Zahlungsauslösedienstleister oder einem Kontoinformationsdienstleister den Zugang zu einem zum Internetbanking berechtigten Zahlungskonto des Kunden zu verweigern, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang des Zahlungsauslösedienstleisters bzw. des Kontoinformationsdienstleisters zum Zahlungskonto, einschließlich der nicht autorisierten oder betrügerischen Auslösung eines Zahlungsvorgangs dies rechtfertigen. Die Bank wird den Kunden – soweit eine Bekanntgabe der Sperre oder der Gründe für die Sperre nicht eine gerichtliche oder verwaltungsbehördliche Anordnung verletzen bzw. österreichischen oder gemeinschaftsrechtlichen Rechtsnormen oder objektiven Sicherheitserwägungen zuwiderlaufen würde – von einer Sperre des Zugriffs durch einen Zahlungsauslösedienstleister bzw. Kontoinformationsdienstleister auf ein Zahlungskonto des Kunden und über deren Gründe in einer mit dem Kunden vereinbarten Kommunikationsform möglichst vor, spätestens aber unverzüglich nach der Sperre informieren.

9. Erlöschen und Kündigung der Berechtigung

9.1 Bei Auflösung der Kontoverbindung erlöschen gleichzeitig alle Internetbanking-Berechtigungen für das betroffene Konto. Mit Wegfall eines Einzelzeichnungsrechts eines Konto- bzw. Depotinhabers oder Zeichnungsberechtigten zu einem Konto oder Wertpapierdepot erlischt die Möglichkeit zur Nutzung des Internetbankings zu diesem Konto oder Wertpapierdepot.

9.2 Jeder Kunde kann die Vereinbarung jederzeit unter Einhaltung einer Frist von einem Monat schriftlich kündigen. Jeder Konto- bzw. Depotinhaber hat die Möglichkeit, die Internetbanking-Berechtigung eines Zeichnungsberechtigten schriftlich oder persönlich an jedem Standort der Bank zu widerrufen.

9.3 Die Bank kann die Vereinbarung ohne Angabe von Gründen unter Einhaltung einer Frist von zwei Monaten jederzeit kündigen, wobei dem Konto- bzw. Depotinhaber die Kündigung in Papierform oder auf einem anderen vereinbarten dauerhaften Datenträger mitzuteilen ist.

9.4 Bei Vorliegen eines wichtigen Grundes sind der Kunde und die Bank berechtigt, die Vereinbarung mit sofortiger Wirkung zu kündigen. Ein wichtiger Grund kann insbesondere dann vorliegen, wenn der Kunde seine persönlichen Identifikationsmerkmale anderen Personen überlässt.

PC282D - 023GI9210D 20200101

10. Benachrichtigungs-Service

10.1 Der Kunde kann sich im Internetbanking für das kostenlose Benachrichtigungs-Service der Bank anmelden. Durch die Anmeldung des Kunden für das Benachrichtigungs-Service unter Mitteilungs-Einstellungen werden die im Rahmen der Anmeldung vom Kunden ausdrücklich ausgewählten kundenbezogenen Daten und Informationen (wie beispielsweise Benachrichtigung, wenn der Kontostand ein vom Kunden definiertes Limit unter- bzw. überschreitet, Kurs-Alarme) an die vom Kunden angegebene E-Mail-Adresse oder einen anderen mit dem Kunden vereinbarten Kommunikationskanal übermittelt.

10.2 Das Benachrichtigungs-Service kann vom Kunden im Internetbanking jederzeit aktiviert bzw. deaktiviert werden. Die Mitteilungs-Einstellungen (Kommunikationskanal sowie Ereignisse, die eine Benachrichtigung an den Kunden auslösen) können vom Kunden jederzeit abgeändert werden.

11. Änderung der Geschäftsbedingungen

11.1 Änderungen dieser Geschäftsbedingungen werden dem Kunden von der Bank spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Inkrafttretens unter Hinweis auf die betroffenen Bestimmungen angeboten. Die Zustimmung des Kunden gilt als erteilt, wenn bei der Bank vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens kein Widerspruch des Kunden einlangt. Darauf wird die Bank den Kunden im Änderungsangebot hinweisen. Das Änderungsangebot ist dem Kunden mitzuteilen. Außerdem wird die Bank eine Gegenüberstellung über die von der Änderung der Geschäftsbedingungen betroffenen Bestimmungen sowie die vollständige Fassung der neuen Geschäftsbedingungen auf ihrer Homepage veröffentlichen und diese in Schriftform dem Kunden auf dessen Verlangen an ihren Standorten aushändigen oder postalisch übermitteln. Die Bank wird den Kunden mit der Mitteilung über die angebotene Änderung auf diese Möglichkeit hinweisen.

11.1a Die Mitteilung über die angebotene Änderung gemäß Punkt 11.1 erfolgt entweder per Post an die letzte vom Kunden bekannt gegebene Anschrift (s. auch Z 11 Abs. 2 der Allgemeinen Geschäftsbedingungen der Bank) oder in elektronischer Form über Mitteilungen im Internetbanking. Diese elektronische Mitteilung erfolgt derart, dass die Bank das Änderungsangebot nicht mehr einseitig abändern kann und der Kunde die Möglichkeit hat, die Mitteilung bei sich abzuspeichern und auszudrucken. Erfolgt eine solche elektronische Mitteilung über das Internetbanking, wird die Bank den Kunden überdies gleichzeitig davon in Kenntnis setzen, dass das Änderungsangebot unter Mitteilungen im Internetbanking verfügbar und abfragbar ist. Dies geschieht durch Übersenden eines separaten E-Mails an die vom Kunden zuletzt bekannt gegebene E-Mail-Adresse oder einen anderen mit dem Kunden vereinbarten Kommunikationskanal.

11.1b Gegenüber einem Unternehmer ist es ausreichend, das Änderungsangebot spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens der Änderungen über Mitteilungen des Internetbankings zuzustellen oder auf eine andere, mit dem Unternehmer vereinbarte Weise zum Abruf bereitzuhalten.

11.2 Im Falle einer solchen beabsichtigten Änderung der Geschäftsbedingungen hat der Kunde, der Verbraucher ist, das Recht, seine Rahmenverträge für Zahlungsdienstleistungen, insbesondere diese Vereinbarung oder den Girokontovertrag, vor Inkrafttreten der Änderung kostenlos fristlos zu kündigen. Darauf wird die Bank im Änderungsanbot hinweisen.

11.3 Die Punkte 11.1 bis 11.2 gelten auch für Änderungen der Vereinbarung gemäß Punkt 1.2, in der die Geltung dieser Geschäftsbedingungen zwischen Kunde und Bank vereinbart worden ist.

11.4 Die vorstehenden Punkte 11.1 bis 11.3 finden auf die Änderung der Leistungen der Bank und der Entgelte des Kunden keine Anwendung.

PC282D - 023GI9210D 20200101

B Besondere Bestimmungen zur Wertpapierfunktion

1. Allgemein

Über Internetbanking ist der Kauf und Verkauf von Aktien, Optionsscheinen, Anleihen, Indexzertifikaten an ausgewählten Börsen sowie von der Bank ausgewählten in- und ausländischen Fonds möglich. Die aktuellen Börsenplätze, an denen über Internetbanking gehandelt werden kann, sowie die Wertpapierarten, die an den infrage kommenden Börsen über Internetbanking gehandelt werden können, sind der „Best Execution Policy“ zu entnehmen. Diese kann auf der Website der Bank unter www.schoellerbank.at eingesehen bzw. in einer Filiale der Bank erfragt werden.

2. Auftragserteilung und Nutzungszeiten

2.1 Die Auftragserteilung ist über Internetbanking grundsätzlich 24 Stunden am Tag und 7 Tage die Woche möglich (siehe Teil A, Punkt 4.1).

2.2 Auf diese Weise können Kauf- und Verkaufsaufträge zu einzelnen Wertpapierpositionen beim Internetbanking auch taggleich erteilt werden (Intraday-Handel).

2.3 Der Verkauf verpfändeter oder aus sonstigem Grund von der Bank gesperrt zu haltender, auf dem/den angegebenen Wertpapierdepot(s) erliegender Werte ist im Rahmen des Internetbankings nicht möglich.

2.4 Der Kunde erhält von der Bank rechtsverbindliche Bestätigungen über die Durchführung der erteilten Aufträge sowie die Abrechnung auf dem für Kontopost vereinbarten Versandweg. Eine elektronische Auftragsbestätigung gilt daher nur als Bestätigung der Übernahme des Auftrags zur Bearbeitung durch die Bank, nicht jedoch als Ausführungsbestätigung oder Abrechnung.

2.5 Die Erteilung eines Kaufauftrags im Rahmen des Internetbankings ist nur so weit zulässig, als zum Zeitpunkt der Ordererteilung auf dem für den Kaufauftrag gewählten Verrechnungskonto eine für die Ausführung des Auftrags notwendige Deckung (Guthaben oder vereinbarter Überziehungsrahmen) vorhanden ist.

2.6 Über die Handelszeiten zum Zeitpunkt der Auftragserteilung und die Usancen der jeweiligen Börse hat sich der Kunde selbstständig zu informieren. Die Bank haftet nicht für Schäden, die dem Kunden daraus entstehen, dass sein im Internetbanking erteilter Auftrag nicht mit den Handelsusancen der gewünschten Börse übereinstimmt. Entspricht der vom Kunden ohne vorgängige Beratung erteilte elektronische Wertpapierauftrag nicht seinen Kenntnissen und Erfahrungen im Anlagebereich, ist die Bank berechtigt, diesen nicht durchzuführen.

3. Pfandrecht

Die auf dem/den für Internetbanking gewidmeten Wertpapierdepot(s) verbuchten Wertpapiere sowie die aus diesen Wertpapieren resultierenden Zins-, Tilgungs- und Verkaufserlöse unterliegen für alle der Bank zustehenden Forderungen aus der Geschäftsbeziehung dem Pfandrecht nach Z 49 ff. der Allgemeinen Geschäftsbedingungen der Schoellerbank AG. Falls die Kurswerte der auf dem/den gewidmeten Wertpapierdepot(s) jeweils erliegenden Werte soweit absinken sollten, dass eine Aushaftung auf dem/den dazugehörigen Verrechnungskonto/-konten nicht mehr gedeckt ist, verpflichtet sich der Kunde als Konto- bzw. Depotinhaber, innerhalb der von der Bank gesetzten Frist entweder weitere der Bank als Pfand genehme Wertpapiere in entsprechender Höhe zu übergeben oder die Aushaftung in dem Maße abzudecken, dass eine ausreichende Besicherung wiederhergestellt wird. Im Rahmen dieses Pfandrechts nicht benötigte Deckungswerte bleiben im Einvernehmen mit der Bank und unter Absprache mit dem jeweiligen Kundenbetreuer zur freien Verfügung des Kunden. Ausdrücklich festgehalten wird das Recht der Bank, im Zusammenhang mit dem Pfandrecht Depotwerte zu sperren, soweit dies zur Sicherstellung von Forderungen aus der Depotführung oder aus der sonstigen Geschäftsbeziehung notwendig ist. Die Bank ist berechtigt, die verpfändeten bzw. der Depotsperre unterliegenden Wertpapiere im Sinne der Allgemeinen Geschäftsbedingungen der Schoellerbank AG ganz oder teilweise zu veräußern, wenn die oben erwähnte Nachschussleistung bzw. Abdeckung nicht erbracht wird oder eine von ihr geltend gemachte

PC282D - 023GI9210D 20200101

Forderung aus der Geschäftsbeziehung (insbesondere auch aus der Depotführung) nicht fristgerecht beglichen wird.

C Besondere Bedingungen Schoellerbank Business Banking und Multi Bank Standard Service (MBS-Service)

Diese Besonderen Bedingungen gelten nur für Unternehmer.

Für die Bankprodukte Schoellerbank Business Banking (HBP) und Multi Bank Standard Service (MBS-Service) gilt Teil A dieser Bedingungen im folgenden Ausmaß: Die Authentifizierung kann mittels mobileTAN und cardTAN erfolgen (Punkt 2.5.a und 2.5.c). Weiters gelten die Punkte 6 (Sorgfalt), 7 (Berichtigung von nicht autorisierten Zahlungsvorgängen), 8 (Sperren), 9 (Erlöschen und Kündigung der Berechtigung) und 11 (Änderungen der Geschäftsbedingungen). Die anderen Absätze sind für die nachfolgenden Bankprodukte nicht anwendbar.

1. Schoellerbank Business Banking (HBP)

1.1 Zugang zum Schoellerbank Business Banking

Verfügernummer: Der Kunde erhält von der Schoellerbank AG eine Verfügernummer, anhand derer die Schoellerbank AG einen Kunden zu den zum Schoellerbank Business Banking berechtigten Konten zuordnen kann. Sie besteht aus einem mehrstelligen Zahlencode und wird bei Ausstellung vom System vergeben. Die Verfügernummer kann vom Kunden nicht geändert werden.

Verfügername: Der Verfügername muss vom Kunden im Rahmen des Ersteinstiegs im Schoellerbank Business Banking festgelegt werden. Der Verfügername kann jederzeit und sofort unter Verwendung einer TAN geändert werden.

Passwort (=PIN/Persönliche Identifikationsnummer): Das Passwort dient zur Legitimierung des Kunden beim Electronic Banking und ist die Voraussetzung dafür, dass der Kunde über Schoellerbank Business Banking Aufträge erteilen bzw. Daten und Informationen abfragen kann. Die PIN besteht aus einer 16-stelligen Zahlen-/Buchstabenkette. Diese Erst-PIN muss im Rahmen des Ersteinstiegs zum gewählten Electronic Banking Produkt vom Kunden abgeändert werden. Die PIN kann jederzeit und sofort wirksam unter Verwendung einer TAN geändert werden. Eine neue Erst-PIN kann der Kunde telefonisch bei seinem Kundenbetreuer beantragen.

1.2 Abwicklung

Zusätzlich zu den persönlichen Berechtigungsmerkmalen, wie im Punkt 1.1. beschrieben, sind seitens jedes berechtigten Teilnehmers am Schoellerbank Business Banking folgende Merkmale selbst zu definieren:
Benutzername (Useridentifikation zum Einstieg in das Schoellerbank Business Banking) und Passwort (vom nutzungsberechtigten Teilnehmer jederzeit abänderbar). Bei diesen Merkmalen „Benutzername und Passwort“ handelt es sich um – im Schoellerbank Business Banking – lokal gespeicherte Zugangsdaten für die Anmeldung am Programm und nicht um die in Punkt 1.1. beschriebenen persönlichen Berechtigungsmerkmale. Diese Merkmale dienen der internen Sicherheit des Kunden und sind unabhängig von den von der Bank vergebenen persönlichen Berechtigungsmerkmalen.

PC282D - 023GI9210D 20200101

1.3 Zugangsvoraussetzungen

Eine Berechtigung zur Nutzung von Schoellerbank Business Banking wird mittels Teilnahmevereinbarung „Antrag zur Teilnahme am Schoellerbank Business Banking“ begründet. Der Kunde erhält seine Zugangsdaten (Verfügernummer und persönliche Identifikationsnummer=PIN) zum Schoellerbank Business Banking postalisch oder persönlich per Brief. Die Kommunikation kann nur dann erfolgreich durchgeführt werden, wenn die von der Bank vergebenen (Verfügernummer und persönliche Identifikationsnummer=PIN) und die vom Kunden zu definierenden Zugangsdaten (Verfügername) korrekt eingegeben wurden. Die von der Bank vergebene PIN ist bei Erstanmeldung zu ändern.

Vertragsgegenstand ist der Erwerb des einfachen, nicht übertragbaren Nutzungsrechtes am Softwareprodukt „Schoellerbank Business Banking“ sowie dessen Anwendung für bei der Bank geführte Konten/Depots im jeweils vereinbarten Umfang. Schoellerbank Business Banking entspricht grundsätzlich dem so genannten „Multi Bank Standard“, der es dem Kunden ermöglicht, mit einem Softwareprodukt alle Kontoverbindungen in Österreich zu bedienen, welche MBS unterstützen. Dem Kunden ist es nicht erlaubt, die Schoellerbank Business Banking-Software zu kopieren und an Dritte weiterzugeben. Davon ausgenommen ist die Herstellung einer Sicherungskopie zur Förderung der Betriebssicherheit. Das geistige Eigentum an Software und Dokumentation und die damit verbundenen Rechte bleiben bei der Bank. Die Bank übernimmt keine Garantie für die fehlerfreie Funktion der Programme. Installation und Gebrauch erfolgen immer auf eigenes Risiko.

1.4 Aktualisierungen und technische Anpassungen

Die Bank ist jederzeit berechtigt, entsprechend dem technischen Fortschritt und allenfalls zusätzlichen Sicherheitsmaßnahmen, Updates und Abänderungen im Datenübertragungsbereich oder an der Programmoberfläche durchzuführen. Programmänderungen und -erweiterungen werden vollautomatisch bei der Kommunikation mit der Schoellerbank AG übermittelt. Der Kunde ist verpflichtet, für eine ordnungsgemäße Installation von Programmupdates zu sorgen. Darüber hinaus ist die Bank auch zur Erweiterung des Funktionsumfanges des Electronic Banking insoweit berechtigt, als dadurch dem Kunden keine zusätzlichen Kosten oder Verpflichtungen erwachsen.

Für Schoellerbank Business Banking muss seitens des Kunden gewährleistet sein, dass ein ungehinderter Datentransfer über die URL hob.banking.co.at nicht durch z.B. eine Firewall behindert wird. Weiters werden die Ports 3048, 443 und 80 benötigt. Technischer Support erfolgt ausschließlich für die aktuelle Version. Schoellerbank Business Banking unterstützt den MBS-Standard.

Multi Bank Standard Service (MBS-Service) bietet als sektorübergreifende Softwarelösung die Möglichkeit, mit einem einzigen Programm mehrere Kontoverbindungen bei unterschiedlichen Banken anzusprechen.

2. Digitale Signatur

Die Freigabe einer Transaktion kann auch durch Verwendung mittels qualifizierter digitaler Signatur erfolgen (z.B. Bürgerkartenfunktion auf der e-card, a.sign premium).

Zu Kontrollzwecken werden auch die Angaben über die durchzuführenden Aufträge angezeigt. Bei Überweisungsaufträgen werden insbesondere Empfänger-IBAN und Betrag oder ein Referenzcode und Kontrollwert (Summe aller Aufträge) angeführt. Der Kunde ist verpflichtet, diese auf Übereinstimmung mit den eingegebenen Aufträgen zu prüfen. Die Signatur-PIN darf nur bei Übereinstimmung eingegeben werden.

Dieses Signaturverfahren ist keine Anwendung der Bank. Eine Sperre bzw. ein Widerruf des Zertifikats ist beim Zertifikatsanbieter zu veranlassen.

PC282D - 023GI9210D 20200101

3. Nutzung über andere Software-Produkte (MBS-Service)

Kunden haben die Möglichkeit, MBS auch über Softwareprodukte anderer Banken (z.B. Business Line, ELBA Business etc.), mit denen eine Verbindung zum Bankrechner der Schoellerbank AG hergestellt werden kann, zu nutzen. Abhängig von der Berechtigungsverwaltung dieser Softwareprodukte kann der Verfüger, sowie allfällige von diesem ermächtigte Ansichtsberechtigte, Zugriff auf Informationen und Daten der teilnehmenden Konten nehmen. Für Kundenanfragen, die diese Anwendung betreffen, ist die Hotline der Bank zuständig, welche die Hauptlizenz für MBS zur Verfügung gestellt hat.

Anhang zu den Geschäftsbedingungen zum Electronic Banking

Empfehlung der Bank zur Sicherheit im Internet und Nutzung des Electronic Banking:

1. Electronic Banking wird über das Kommunikationsmedium Internet abgewickelt, welches ein offenes und allgemein zugängliches Medium ist. Unter Verwendung der persönlichen Identifikationsmerkmale des Kunden kann auch ein unberechtigter Dritter in das Internetbanking einsteigen und Dispositionen zulasten des Konto- bzw. Depotinhabers vornehmen. Die Bank informiert auf ihrer Homepage www.schoellerbank.at und direkt im Internetbanking regelmäßig über aktuelle Gefahren im Internet und gibt dort auch konkrete Empfehlungen und Sicherheitshinweise, wie das Verhalten bei der Nutzung des Internetbanking im Hinblick auf diese Gefahren risikominimierend angepasst werden kann. Zur Vermeidung von Schäden bei den Transaktionen im Rahmen des Internetbankings wird dem Kunden empfohlen, besonders sorgfältig vorzugehen.

2. Die Bank führt umfangreiche Maßnahmen zur Absicherung der im Electronic Banking übermittelten und bankseitig verarbeiteten Daten durch und trifft umfassende Sicherheitsvorkehrungen, die einen Schutz gegen Angriffe bei der Übertragung der Daten über das Internet oder bei der Verarbeitung auf dem Bankserver bieten. Damit die vorgesehenen Sicherheitsmaßnahmen nicht gefährdet werden, empfiehlt die Bank jedem Kunden auch in eigenem Interesse seinerseits technische Vorkehrungen zum Schutz der von ihm eingesetzten Systeme und des PCs zu treffen. Die Bank informiert auf ihrer Homepage und im Internetbanking über mögliche Gefahren sowie die gebotenen und empfehlenswerten Sicherheitsmaßnahmen zum Schutz der Systeme und des PCs des Kunden.

PC282D - 023GI9210D 20200101