



Geänderte Geschäftsbedingungen und Teilnahmevereinbarung INFINITY

Gegenüberstellung der geänderten Bestimmungen und Vereinbarungen.

Teilnahmevereinbarung Business Portal INFINITY (Electronic Banking)

Alte Fassung November 2021

Multibank-Standard

Das Business Portal verfügt grundsätzlich über den Multibank-Standard (MBS).

Für die Verwendung im Business Portal gelten die in Punkt 12 der Business Portal Bedingungen enthaltenen Bestimmungen.

[...]

Bedingungen für das Business Portal INFINITY (Electronic Banking)

Alte Fassung November 2021

In den gesamten Bedingungen wird folgender Begriff angepasst: Raiffeisenbank

2. Portal-Berechtigungen

2.4 Abfrage-/Übermittlungsberechtigte

Der Kontoinhaber, kann natürliche Personen benennen, die ausschließlich berechtigt sind, Informationen zum Konto im selben Umfang wie der Kontoinhaber abzufragen (auch wenn diese Informationen die Zeit vor der Einräumung der Abfrageberechtigung betreffen) und Auftragsdaten zwecks Vorbereitung späterer Auftragserteilung durch dazu berechtigte Personen zu übermitteln.

4. Identifikationsverfahren

a) Arten der Identifikationsverfahren

Die Identifikation des Portal-Berechtigten, der das Business Portal nutzen will, erfolgt unter Verwendung des im Folgenden beschriebenen Passwort/TAN-Verfahrens oder – soweit in den Eingabefeldern des Business Portals vorgesehen – mit einer qualifizierten elektronischen Signatur.

(i) Passwort/TAN-Verfahren

Die Identifikation erfolgt durch Eingabe

- des vom Portal-Berechtigten festgelegten Passwortes oder der von der Raiffeisenbank vergebenen Identifikationsnummer, kurz „PIN“ (je nach konkreter Eingabeanforderung durch die Bank)
- und einer nur einmal verwendbaren Transaktionsnummer („TAN“).

Die für eine konkrete Identifikation aktuell benötigte TAN wird je nach Vereinbarung

- von der Raiffeisenbank an einen vom Kunden oder Administrator bekannt gegebenen Mobiltelefon-Anschluss des Portal-Berechtigten per SMS übermittelt („Raiffeisen smsTAN“), oder
- vom Portal-Berechtigten mittels der von der Raiffeisenbank zur Verfügung gestellten Einrichtungen ermittelt („Raiffeisen cardTAN“).

[...]

Neue Fassung April 2024

Multibank-Standard Multibankfähigkeit

Das Business Portal verfügt grundsätzlich über den Multibank-Standard (MBS). Die Portal-Berechtigten können ab dem vom Kreditinstitut bekanntzugebenden Zeitpunkt – nach entsprechender Freigabe durch den Administrator – selbständig und ohne gesonderte Zustimmung des Kunden direkt im Business Portal ihr Kommunikationsprotokoll unwiderruflich auf den Electronic Banking Internet Communication Standard (EBICS) ändern.

Für die Verwendung von MBS und EBICS im Business Portal gelten die in Punkt 12 der Business Portal Bedingungen enthaltenen Bestimmungen.

Der Kunde nimmt zustimmend zur Kenntnis, dass EBICS künftig MBS zur Gänze ablösen wird. Das Kreditinstitut wird Kunden mit einem MBS-Zugang rechtzeitig vor dessen Einstellung informieren.

[...]

Neue Fassung April 2024

In den gesamten Bedingungen wird folgender Begriff angepasst: Kreditinstitut

2. Portal-Berechtigungen

2.4 Abfrage-/Übermittlungsberechtigte

Der Kontoinhaber, kann natürliche Personen benennen, die ausschließlich berechtigt sind, Informationen zum Konto im selben Umfang wie der Kontoinhaber abzufragen (auch wenn diese Informationen die Zeit vor der Einräumung der Abfrageberechtigung betreffen) und Auftragsdaten zwecks Vorbereitung späterer Auftragserteilung durch dazu berechtigte Personen zu übermitteln.

4. Identifikationsverfahren

a) Arten der Identifikationsverfahren

Die Identifikation des Portal-Berechtigten, der das Business Portal nutzen will, erfolgt unter Verwendung des im Folgenden beschriebenen Passwort/TAN-Verfahrens oder – soweit in den Eingabefeldern des Business Portals vorgesehen – mit einer qualifizierten elektronischen Signatur. Das Kreditinstitut kann mit dem Portal-Berechtigten auch die Verwendung der nachfolgend beschriebenen Signatur-App vereinbaren. Hierzu kann eine gesonderte Freigabe durch den Administrator je Endgerät erforderlich sein.

(i) Passwort/TAN-Verfahren

Die Identifikation erfolgt durch Eingabe

- des vom Portal-Berechtigten festgelegten Passwortes oder der vom Kreditinstitut vergebenen Identifikationsnummer, kurz „PIN“ (je nach konkreter Eingabeanforderung durch das Kreditinstitut)
- und einer nur einmal verwendbaren Transaktionsnummer („TAN“).

Die für eine konkrete Identifikation aktuell benötigte TAN wird je nach Vereinbarung

- vom Kreditinstitut an einen vom Kunden oder, Administrator oder Portal-Berechtigten bekannt gegebenen Mobiltelefon-Anschluss des Portal-Berechtigten per SMS übermittelt („Raiffeisen smsTAN“), oder
- vom Portal-Berechtigten mittels der vom Kreditinstitut zur Verfügung gestellten Einrichtungen ermittelt („Raiffeisen cardTAN“).

[...]

(iii) INFINITY Signatur-App

Der Portal-Berechtigte installiert im Zuge der Registrierung auf seinem Endgerät eine vom Kreditinstitut zur Verfügung gestellte

Applikation („**Signatur-App**“). Die Verknüpfung der Signatur-App mit den Business Portal Systemen des Kreditinstituts über das Internet erfolgt über einen vom Kreditinstitut übermittelten Aktivierungs-Code. Die Identifizierung unter Verwendung der Signatur-App erfolgt durch Eingabe der vom Portal-Berechtigten im Zuge der Registrierung zu diesem Verfahren festgelegten persönlichen Identifikationsnummer („**Signatur-Code**“). Durch diese Eingabe wird zum Zwecke der Identifikation automatisch eine zuvor aus den Business Portal Systemen des Kreditinstituts an das Endgerät des Portal-Berechtigten übermittelte, für den Portal-Berechtigten nicht sichtbare einmalige Transaktionsnummer wieder an die Business Portal Systeme des Kreditinstituts rückgesendet.

Bei Portal-Berechtigten gemäß Punkt 2.2. bis 2.4 ist die registrierte Signatur-App gesondert als Identifikationsverfahren für die Nutzung von konto- sowie bankproduktabhängigen Dienstleistungen zu vereinbaren.

Das Passwort/TAN-Verfahren mit cardTAN kann auch nach erfolgter Registrierung der Signatur-App weiterverwendet werden.

Bei Verwendung des Kommunikationsprotokolls „Electronic Banking Internet Communication Standard“ („**EBICS**“) steht ausschließlich die Signatur-App als Identifikationsverfahren zur Verfügung.

Sollte die Verwendung der Signatur-App aus beim Kreditinstitut liegenden Gründen nicht möglich sein, wird das Kreditinstitut einem Portal-Berechtigten für die Dauer dieser Störung die Verwendung des Passwort/TAN-Verfahrens mittels smsTAN ermöglichen. Die vom Portal-Berechtigten für diesen Zweck angeforderte smsTAN wird für diesen Zweck an den vom Administrator oder Portal-Berechtigten bekanntgegebenen Mobiltelefon-Anschluss per SMS übermittelt.

b) Verwendung biometrischer Erkennungsmerkmale in Identifikationsverfahren

Für das Passwort/TAN-Verfahren kann der Portal-Berechtigte bei entsprechender technischer Ausstattung seines Endgeräts in einer von der Raiffeisenbank allenfalls zur Verfügung gestellten Anwendung (zB einer App) biometrische Erkennungsmerkmale (wie zB Fingerprint oder Gesichtserkennung) aktivieren und mit diesen biometrischen Erkennungsmerkmalen die Übermittlung des gespeicherten Passwortes bzw. PIN an die Business Portal Systeme der Raiffeisenbank auslösen. Nach erstmaliger Aktivierung eines biometrischen Erkennungsmerkmals kann der Portal-Berechtigte auch auf ein anderes vom Endgerät unterstütztes biometrisches Merkmal umstellen.

Die biometrischen Erkennungsmerkmale sind ausschließlich am Endgerät des Portal-Berechtigten gespeichert. Kann das Endgerät des Portal-Berechtigten das biometrische Erkennungsmerkmal nicht erkennen, ist das Passwort bzw. die PIN manuell einzugeben und zur Übermittlung freizugeben.

Eine Deaktivierung des biometrischen Erkennungsmerkmals kann vom Portal-Berechtigten jederzeit im Bereich „Einstellungen“ der App erfolgen. Bei Verlust oder Diebstahl des mobilen Endgerätes hat der Portal-Berechtigte die Deaktivierung bei der Raiffeisenbank zu veranlassen. Eine Änderung des Passwortes bzw. der PIN führt ebenso automatisch zu einer Deaktivierung des biometrischen Erkennungsmerkmals, eine neuerliche Aktivierung ist jedoch jederzeit im Bereich „Einstellungen“ der App möglich. Der Portal-Berechtigte hat sicherzustellen, dass unbefugte Dritte keinen Zugriff auf das Endgerät haben.

d) Erteilung von Aufträgen und Abgabe von Erklärungen

Für die Erteilung von Aufträgen sowie die Abgabe anderer verbindlicher Erklärungen im Business Portal hat der dazu jeweils Berechtigte – soweit sich nicht aus den Eingabefeldern ergibt, dass die Eingabe einer SMS-TAN ausreicht – das vereinbarte Identifikationsverfahren zu verwenden.

b) Verwendung biometrischer Erkennungsmerkmale in Identifikationsverfahren

Für das Passwort/TAN-Verfahren Im Rahmen der Verwendung der Signatur-App kann der Portal-Berechtigte bei entsprechender technischer Ausstattung seines Endgeräts in einer von der Raiffeisenbank allenfalls zur Verfügung gestellten Anwendung (zB einer App) biometrische Erkennungsmerkmale (wie zB Fingerprint oder Gesichtserkennung) aktivieren und mit diesen biometrischen Erkennungsmerkmalen die Übermittlung des gespeicherten Passwortes bzw. PIN des Signatur-Codes an die Business Portal Systeme des Kreditinstituts auslösen. Nach erstmaliger Aktivierung eines biometrischen Erkennungsmerkmals kann der Portal-Berechtigte auch auf ein anderes vom Endgerät unterstütztes biometrisches Merkmal umstellen.

Die biometrischen Erkennungsmerkmale sind ausschließlich am Endgerät des Portal-Berechtigten gespeichert. Kann das Endgerät des Portal-Berechtigten das biometrische Erkennungsmerkmal nicht erkennen, ist das Passwort bzw. die PIN der Signatur-Code manuell einzugeben und zur Übermittlung freizugeben.

Eine Deaktivierung des biometrischen Erkennungsmerkmals kann vom Portal-Berechtigten jederzeit im Bereich „Einstellungen“ der App in den Einstellungen der Signatur-App erfolgen. Bei Verlust oder Diebstahl des mobilen Endgerätes hat der Portal-Berechtigte die Deaktivierung beim Kreditinstitut zu veranlassen. Eine Änderung des Passwortes bzw. der PIN Signatur-Codes führt ebenso automatisch zu einer Deaktivierung des biometrischen Erkennungsmerkmals, eine neuerliche Aktivierung ist jedoch jederzeit im Bereich „Einstellungen“ der App in den Einstellungen der Signatur-App möglich. Der Portal-Berechtigte hat sicherzustellen, dass unbefugte Dritte keinen Zugriff auf das Endgerät haben.

d) Erteilung von Aufträgen und Abgabe von Erklärungen

Für die Erteilung von Aufträgen sowie die Abgabe anderer verbindlicher Erklärungen im Business Portal hat der dazu jeweils Berechtigte – soweit sich nicht aus den Eingabefeldern ergibt, dass die Eingabe einer SMS-TAN ausreicht – das vereinbarte Identifikationsverfahren zu verwenden. Nach Identifikation des Portal-Berechtigten gemäß diesem Punkt 4 erfolgt beim Kommunikationsprotokoll EBICS



f) Kommunikationsberechtigung

Für die technische Kommunikation im Rahmen des Business Portals erhält jeder Kunde, der ein Konto in das Business Portal eingebunden hat, zusätzlich eine zugeordnete Kommunikationsberechtigung und ein jederzeit änderbares Passwort.

6. Sorgfaltspflichten und Haftung

Den Kunden und seine Portal-Berechtigten treffen nachstehende Sorgfaltspflichten:

- i. Die im Rahmen des vereinbarten Identifikationsverfahrens einschließlich einer sonstigen elektronischen Signatur (Punkt 4 a)) zu verwendenden Identifikationsmerkmale müssen geheim gehalten werden. Es ist sicherzustellen, dass unbefugte Dritte keinen Zugriff auf die Identifikationsmerkmale haben. Zulässig ist die Weitergabe der mit der Raiffeisenbank vereinbarten Identifikationsmerkmale durch Verfügungs- und Zeichnungsberechtigte und Abfrage-/Übermittlungsberechtigte an Zahlungsauslösedienstleister oder Kontoinformationsdienstleister, **wobei Zeichnungsberechtigte und Abfrage-/Übermittlungsberechtigte im Rahmen ihrer Berechtigungen dazu auch ohne Zustimmung des Kontoinhabers berechtigt sind.** [...]
- ii. Wenn der Verdacht besteht, dass ein unbefugter Dritter die Möglichkeit zum Missbrauch eines Identifikationsmerkmals erlangt haben könnte, hat der Kunde bzw. Portal-Berechtigte unverzüglich die in Punkt 7. vorgesehenen Schritte zu setzen.

[...]

Aufträge der Personen, denen der Kunde zu seinem Konto Berechtigungen eingeräumt hat, werden zulasten des Kontos auf Rechnung des Kunden durchgeführt. Allfällige Überziehungen des Kontos werden im Rahmen des Business Portals auch zugelassen, wenn sie auf Verfügungen eines Zeichnungsberechtigten zurückgehen. Für derartige Überziehungen haftet der Kunde uneingeschränkt.

[...]

7. Sperre der Zugriffsberechtigung

a) Sperre über Veranlassung des Kunden bzw. Portal-Berechtigten

Der Kunde oder der Portal-Berechtigte kann die Sperre seiner Zugriffsberechtigung auf das Business Portal wie folgt bei der Raiffeisenbank beauftragen:

- jederzeit telefonisch bei der dafür eingerichteten Raiffeisen Sperrhotline für Karten und Electronic Banking, deren Telefonnummer die Raiffeisenbank dem Kunden bekannt gegeben hat und die auf der Website www.raiffeisen.at abrufbar ist, oder
- zu den jeweiligen Öffnungszeiten bei der Raiffeisenbank.

[...]

Bei Verlust eines im Rahmen des vereinbarten Identifikationsverfahrens zu verwendenden Identifikationsmerkmals, bei Verlust der zur Erstellung einer qualifizierten elektronischen Signatur (Punkt 4 a) (ii) erforderlichen Identifikationsmerkmale oder bei Bestehen des Verdachtes, dass eine unbefugte Person die Möglichkeit zum Missbrauch eines Identifikationsmerkmals oder eines aktivierten biometrischen Erkennungsmerkmals erlangt hat, ist der Kunde bzw. Portal-Berechtigte verpflichtet, wenn (wie zB bei einem bio-

anschließend eine Prüfung der bei der Initialisierung von EBICS hinterlegten elektronischen Unterschrift des Portal-Berechtigten.

f) EBICS Kundennummer/Kommunikationsberechtigung

Für die technische Kommunikation im Rahmen des Business Portals erhält jeder Kunde, der ein Konto in das Business Portal eingebunden hat, zusätzlich eine zugeordnete Kommunikationsberechtigung und ein jederzeit änderbares Passwort.

Ab dem vom Kreditinstitut bekanntzugebenden Zeitpunkt erhält jeder Kunde, der ein Konto in das Business Portal eingebunden hat, für die Kommunikation über EBICS zusätzlich eine zugeordnete Kundennummer.

6. Sorgfaltspflichten und Haftung

Den Kunden und seine Portal-Berechtigten treffen nachstehende Sorgfaltspflichten:

- i. Die im Rahmen des vereinbarten Identifikationsverfahrens einschließlich einer sonstigen elektronischen Signatur (Punkt 4 a)) zu verwendenden Identifikationsmerkmale müssen geheim gehalten werden. Es ist sicherzustellen, dass unbefugte Dritte keinen Zugriff auf die Identifikationsmerkmale haben. Der Kunde und die Portal-Berechtigten haben alle zumutbaren Vorkehrungen zu treffen, um die Identifikationsmerkmale vor unbefugtem Zugriff zu schützen. Zulässig ist die Weitergabe der mit dem Kreditinstitut vereinbarten Identifikationsmerkmale durch Verfügungs- und Zeichnungsberechtigte und Abfrage-/Übermittlungsberechtigte sowie Einsichts- und Vorbereitungsrechte an Zahlungsauslösedienstleister oder Kontoinformationsdienstleister, wobei Zeichnungsberechtigte und Abfrage-/Übermittlungsberechtigte sowie Einsichts- und Vorbereitungsrechte im Rahmen ihrer Berechtigungen dazu auch ohne Zustimmung des Kontoinhabers berechtigt sind. [...]
- ii. Wenn der Verdacht besteht Bei Kenntnis, dass ein unbefugter Dritter die Möglichkeit zum Missbrauch eines Identifikationsmerkmals erlangt haben könnte hat, hat der Kunde bzw. Portal-Berechtigte unverzüglich die in Punkt 7. vorgesehenen Schritte zu setzen.

[...]

Aufträge der Personen, denen der Kunde Kontoinhaber zu seinem Konto Berechtigungen eingeräumt hat, werden zulasten des Kontos auf Rechnung des Kunden Kontoinhabers durchgeführt. Allfällige Überziehungen des Kontos werden im Rahmen des Business Portals auch zugelassen, wenn sie auf Verfügungen eines Zeichnungsberechtigten zurückgehen. Für derartige Überziehungen haftet der Kunde Kontoinhaber uneingeschränkt.

[...]

7. Sperre der Zugriffsberechtigung

a) Sperre über Veranlassung des Kunden bzw. Portal-Berechtigten

Der Kunde oder der Portal-Berechtigte kann die Sperre seiner Zugriffsberechtigung auf das Business Portal wie folgt beim Kreditinstitut beauftragen:

- jederzeit telefonisch bei der dafür eingerichteten Raiffeisen Sperrhotline für Karten und Electronic Banking, deren Telefonnummer das Kreditinstitut dem Kunden bekannt gegeben hat und die auf der Website www.raiffeisen.at des Kreditinstituts abrufbar ist, oder
- zu den jeweiligen Öffnungszeiten beim Kreditinstitut.

[...]

Bei Verlust eines im Rahmen des vereinbarten Identifikationsverfahrens zu verwendenden Identifikationsmerkmals, bei Verlust der zur Erstellung einer qualifizierten elektronischen Signatur (Punkt 4 a) (ii) erforderlichen Identifikationsmerkmale oder bei Bestehen des Verdachtes Kenntnis, dass eine unbefugte Person die Möglichkeit zum Missbrauch eines Identifikationsmerkmals oder eines aktivierten biometrischen Erkennungsmerkmals erlangt hat, ist der Kunde bzw. Portal-Berechtigte verpflichtet, wenn (wie zB bei einem

metrischen Erkennungsmerkmal) möglich das Identifikationsmerkmal bzw. biometrische Erkennungsmerkmal zu deaktivieren oder ansonsten die Sperre der betroffenen Zugriffsberechtigungen zu veranlassen. Sollte eine sofortige Sperre der Zugriffsberechtigung auf den beschriebenen Wegen nicht möglich sein, wird der Kunde bzw. Portal-Berechtigte zunächst das Passwort bzw. die PIN ändern. Auch in diesem Fall wird der Kunde bzw. Portal-Berechtigte zum frühest möglichen Zeitpunkt die Sperre auf einem in diesem Punkt 7. beschriebenen Weg veranlassen.

[...]

Nach vierfacher Falscheingabe des Passwortes bzw. der PIN oder der TAN wird der Zugriff automatisch gesperrt.

[...]

9. Zustellung/Bereitstellung von Informationen und Erklärungen der Raiffeisenbank unter Verwendung des Business Portals

b) Zugang der Informationen und Erklärungen

Wird der Kunde über die Zustellung im Business Portal per Post oder – wenn mit dem Kunden vereinbart – an eine vom Kunden bekanntgegebene E-Mail-Adresse gesondert informiert, ist mit Zugang dieser gesonderten Information beim Kunden auch die im Business Portal zugestellte Information oder Erklärung dem Kunden zugegangen.

Erfolgt keine gesonderte Information über die Zustellung im Business Portal, gelten die dort zum Abruf bereitgestellten Informationen und Erklärungen mit tatsächlichem Abruf über das Business Portal durch einen dazu Berechtigten als dem Kunden zugestellt. Mit Abrufung, bei Kunden, die Unternehmer sind, aber jedenfalls mit Ablauf von sechs Wochen nach Bereitstellung, treten die Wirkungen der Zustellung ein und es beginnen allfällige Reklamationsfristen zu den zugestellten Mitteilungen der Raiffeisenbank zu laufen. Dies gilt auch für einen Kontoabschluss, der keinen Zahlungsdienst betrifft. Nicht über Business Portal übermittelte Beilagen zu über Business Portal abgerufenen Mitteilungen werden je nach der mit dem Kunden getroffenen Vereinbarung am Schalter der Raiffeisenbank hinterlegt oder postalisch zugesandt.

12. Inanspruchnahme der Electronic Banking Leistungen von Drittinstituten (Multibankfähigkeit)

Für die Inanspruchnahme der Electronic Banking Dienstleistungen samt Kontozugriff bei einer anderen Bank (Drittinstitut) über das Business Portal der Raiffeisenbank (sog. Multibank-Standard) hat der Kunde mit dem jeweiligen Drittinstitut gesondert eine Vereinbarung abzuschließen.

[...]

Der Multibank-Standard ist mit der Raiffeisenbank ausdrücklich in geschriebener Form zu vereinbaren und ermöglicht gegebenenfalls dem Kunden über das Business Portal den Zugriff auf Konten (Abruf von Kontoinformationen und Übermittlung von Aufträgen) bei Drittinstituten, soweit dieser Zugriff vom Drittinstitut zugelassen wird. Der Zugriff beim Drittinstitut erfolgt unter Verwendung der mit dem Drittinstitut vereinbarten Identifikationsmerkmale.

[...]

biometrischen Erkennungsmerkmal) möglich das Identifikationsmerkmal bzw. biometrische Erkennungsmerkmal zu deaktivieren oder ansonsten die Sperre der betroffenen Zugriffsberechtigungen zu veranlassen. Sollte eine sofortige Sperre der Zugriffsberechtigung auf den beschriebenen Wegen nicht möglich sein, wird der Kunde bzw. Portal-Berechtigte zunächst das Passwort bzw. die PIN ändern. Auch in diesem Fall wird der Kunde bzw. Portal-Berechtigte zum frühest möglichen Zeitpunkt die Sperre auf einem in diesem Punkt 7. beschriebenen Weg veranlassen.

[...]

Nach vierfacher Falscheingabe des Passwortes bzw. der PIN oder, der TAN oder des Signatur-Codes wird der Zugriff automatisch gesperrt.

[...]

9. Zustellung/Bereitstellung von Informationen und Erklärungen des Kreditinstituts unter Verwendung des Business Portals

b) Zugang der Informationen und Erklärungen

Wird der Kunde über die Zustellung im Business Portal unter dem Menüpunkt „Kommunikation“ – „Persönliche Nachrichten“ (im Folgenden „Electronic Banking-Mailbox“) per Post oder – wenn mit dem Kunden vereinbart – an eine vom Kunden bekanntgegebene E-Mail-Adresse gesondert informiert, ist mit Zugang dieser gesonderten Information beim Kunden auch die im Business Portal zugestellte Information oder Erklärung dem Kunden zugegangen.

Erfolgt keine gesonderte Information über die Zustellung im in die Electronic Banking-Mailbox des Business Portals, gelten die dort zum Abruf bereitgestellten Informationen und Erklärungen mit tatsächlichem Abruf über das Business Portal durch einen dazu Berechtigten als dem Kunden zugestellt. Mit Abrufung, bei Kunden, die Unternehmer sind, aber jedenfalls mit Ablauf von sechs Wochen nach Bereitstellung, treten die Wirkungen der Zustellung ein und es beginnen allfällige Reklamationsfristen zu den zugestellten Mitteilungen des Kreditinstituts zu laufen. Dies gilt auch für einen Kontoabschluss, der keinen Zahlungsdienst betrifft. Nicht über Business Portal übermittelte Beilagen zu über Business Portal abgerufenen Mitteilungen werden je nach der mit dem Kunden getroffenen Vereinbarung am Schalter des Kreditinstituts hinterlegt oder postalisch zugesandt.

12. Inanspruchnahme der Electronic Banking Leistungen von Drittinstituten (Multibankfähigkeit)

Für die Inanspruchnahme der Electronic Banking Dienstleistungen samt Kontozugriff bei einer anderen Bank (Drittinstitut) über das Business Portal des Kreditinstituts (sog. Multibank-Standard) hat der Kunde mit dem jeweiligen Drittinstitut gesondert eine Vereinbarung abzuschließen.

[...]

Der konkrete Multibank-Standard ist mit dem Kreditinstitut ausdrücklich in geschriebener Form zu vereinbaren und ermöglicht gegebenenfalls dem Kunden über das Business Portal den Zugriff auf Konten (Abruf von Kontoinformationen und Übermittlung von Aufträgen) bei Drittinstituten, soweit dieser Zugriff vom Drittinstitut zugelassen wird. Beim Kommunikationsprotokoll „Multibank-Standard“ (MBS) erfolgt über den Zugriff beim Drittinstitut erfolgt unter Verwendung der mit dem Drittinstitut vereinbarten Identifikationsmerkmale. Beim Kommunikationsprotokoll „Electronic Banking Internet Communication Standard“ („EBICS“) erfolgt der Zugriff beim Drittinstitut nach Identifikation des Portal-Berechtigten gemäß Punkt 4 unter Verwendung der bei der Initialisierung von EBICS hinterlegten elektronischen Unterschrift des Portal-Berechtigten. Bis zu dem vom Kreditinstitut bekanntzugebenden Zeitpunkt können Portal-Berechtigte auch nach dem Umstieg auf EBICS von anderen Portal-Berechtigten im Rahmen von MBS vorbereitete Zahlungsaufträge unter Verwendung von MBS zeichnen.

[...]