Bedingungen für das Business Portal INFINITY (Electronic Banking)
Gegenüberstellung der geänderten Bestimmungen

In den gesamten Bedingungen wurde die Begriffsterminologie folgendermaßen angepasst:

Fassung November 2021	**Fassung April 2024**
Raiffeisenbank	Kreditinstitut

Fassung November 2021	**Fassung April 2024**
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. […]	**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.	**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 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 („smsTAN"), oder - vom Portal-Berechtigten mittels der von der Raiffeisenbank zur Verfügung gestellten Einrichtungen ermittelt („cardTAN").	(i) Passwort/TAN-Verfahren Die Identifikation erfolgt durch Eingabe - des vom Portal-Berechtigten festgelegten Passwortes oder der von~~n~~m ~~der Raiffeisenbank~~Kreditinstitut vergebenen Identifikationsnummer, kurz „PIN" (je nach konkreter Eingabeanforderung durch ~~die~~das ~~Bank~~Kreditinstitut) - und einer nur einmal verwendbaren Transaktionsnummer („TAN"). Die für eine konkrete Identifikation aktuell benötigte TAN wird je nach Vereinbarung - von~~n~~m ~~der Raiffeisenbank~~Kreditinstitut an einen vom Kunden~~,~~ ~~oder~~ Administrator oder Portal-Berechtigten bekannt gegebenen Mobiltelefon-Anschluss des Portal-Berechtigten per SMS übermittelt („smsTAN"), oder - vom Portal-Berechtigten mittels der von~~n~~m ~~der Raiffeisenbank~~Kreditinstitut zur Verfügung gestellten Einrichtungen ermittelt („cardTAN").
(ii) Qualifizierte elektronische Signatur Welche qualifizierten elektronischen Signaturen (zB A-Trust Handysignatur) im Rahmen des Business Portals verwendet werden können, wird die Raiffeisenbank bei den jeweiligen Eingabefeldern im Business Portal bekannt gegeben.	(ii) Qualifizierte elektronische Signatur Welche qualifizierten elektronischen Signaturen (zB A-Trust Handysignatur) im Rahmen des Business Portals verwendet werden können, wird ~~die~~das ~~Raiffeisenbank~~Kreditinstitut bei den jeweiligen Eingabefeldern im Business Portal bekannt ~~ge~~geben. (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.	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~~ Signatur-Codes an die Business Portal Systeme ~~der~~des ~~Raiffeisenbank~~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. PIN manuell einzugeben und zur Übermittlung freizugeben.	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. 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 erfolgen. Bei Verlust oder Diebstahl des mobilen Endgerätes hat der Portal-Berechtigte die Deaktivierung bei der Raiffeisenbank zu veranlassen. Eine Änderung des Passwortes bzw. 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. […]	Eine Deaktivierung des biometrischen Erkennungsmerkmals kann vom Portal-Berechtigten jederzeit ~~im Bereich~~in den „Einstellungen" der Signatur-App erfolgen. Bei Verlust oder Diebstahl des mobilen Endgerätes hat der Portal-Berechtigte die Deaktivierung bei~~m der Raiffeisenbank~~Kreditinstitut zu veranlassen. Eine Änderung des ~~Passwortes bzw. PIN~~Signatur-Codes führt ebenso automatisch zu einer Deaktivierung des biometrischen Erkennungsmerkmals, eine neuerliche Aktivierung ist jedoch jederzeit ~~im Bereich „~~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. […]	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 anschließend eine Prüfung der bei der Initialisierung von EBICS hinterlegten elektronischen Unterschrift des Portal-Berechtigten. […]
f) Kommunikationsberechtigung Für die technische Kommunikation im Rahmen des Business Portals erhält jeder Kunde, der ein Konto in das Business	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. […]	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. 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**. Ist für die Verwendung eines vereinbarten Identifikationsverfahrens ein Mobiltelefonanschluss erforderlich, ist für die Gültigkeitsdauer des in diesem Identifikationsverfahren verwendeten Identifikationsmerkmals auch sicherzustellen, dass Dritte keinen Zugriff auf die Telefone dieses Mobiltelefonanschlusses haben. Wird für das Identifikationsverfahren ein sonstiges Endgerät verwendet, ist für die Gültigkeitsdauer der in diesem Identifikationsverfahren verwendeten Identifikationsmerkmals auch sicherzustellen, dass Dritte keinen Zugriff auf dieses Endgerät haben. (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. […]	**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 der~~m Raiffeisenbank~~Kreditinstitut vereinbarten Identifikationsmerkmale durch Verfügungs- und Zeichnungsberechtigte~~ und~~, Abfrage-/Übermittlungsberechtigte sowie Einsichts- und Vorbereitungsberechtigte an Zahlungsauslösedienstleister oder Kontoinformationsdienstleister, **wobei Zeichnungsberechtigte ~~und~~, Abfrage-/Übermittlungsberechtigte sowie Einsichts- und Vorbereitungsberechtigte im Rahmen ihrer Berechtigungen dazu auch ohne Zustimmung des Kontoinhabers berechtigt sind**. Ist für die Verwendung eines vereinbarten Identifikationsverfahrens ein Mobiltelefonanschluss erforderlich, ist für die Gültigkeitsdauer des in diesem Identifikationsverfahren verwendeten Identifikationsmerkmals auch sicherzustellen, dass Dritte keinen Zugriff auf die Telefone dieses Mobiltelefonanschlusses haben. Wird für das Identifikationsverfahren ein sonstiges Endgerät verwendet, ist für die Gültigkeitsdauer der in diesem Identifikationsverfahren verwendeten Identifikationsmerkmals auch sicherzustellen, dass Dritte keinen Zugriff auf dieses Endgerät haben. (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 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. […]	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 […] 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 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	**7. SPERRE DER ZUGRIFFSBERECHTIGUNG** a) Sperre über Veranlassung des Kunden bzw. Portal-Berechtigten […] 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 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. PIN oder der TAN wird der Zugriff automatisch gesperrt. […]	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. PIN, ~~oder~~ der TAN oder des Signatur-Codes 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.	**9. ZUSTELLUNG/BEREITSTELLUNG VON INFORMATIONEN UND ERKLÄRUNGEN ~~DER~~DES ~~RAIFFEISENBANK~~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 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. […]	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 ~~der~~des ~~Raiffeisenbank~~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 ~~der~~ des ~~Raiffeisenbank~~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 der Raiffeisenbank (sog. Multibank-Standard) hat der Kunde mit dem jeweiligen Drittinstitut gesondert eine Vereinbarung abzuschließen.	**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~~des ~~Raiffeisenbank~~Kreditinstituts ~~(sog. Multibank-Standard)~~ hat der Kunde mit dem jeweiligen Drittinstitut gesondert eine Vereinbarung abzuschließen.
Bindet der Kunde auf diesem Wege Konten von anderen Personen ein (also Konten, bei denen der Kunde nicht selbst der Inhaber ist), liegt es in der alleinigen Verantwortung des Kunden, die notwendige Zustimmung des Kontoinhabers zu dieser Vereinbarung einzuholen.	Bindet der Kunde auf diesem Wege Konten von anderen Personen ein (also Konten, bei denen der Kunde nicht selbst der Inhaber ist), liegt es in der alleinigen Verantwortung des Kunden, die notwendige Zustimmung des Kontoinhabers zu dieser Vereinbarung einzuholen.
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. […]	Der konkrete Multibank-Standard ist mit ~~der~~dem ~~Raiffeisenbank~~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 ~~D~~der 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. […]