Bedingungen für die Datenfernübertragung

Deutsche Bank
DB Privat- und Firmenkundenbank AG

Ab 18. November 2019 geltende Fassung

Die nachfolgenden Bedingungen für die Datenfernübertragung (DFÜ) gelten für Kunden der DB Privat- und Firmenkundenbank AG (nachfolgend einheitlich Bank genannt).

1 Leistungsumfang

(1) Die Bank steht ihrem Kunden (Kontoinhaber) und/oder einem beigetretenen Kundenpartner (im Nachfolgenden auch Kundengesellschaft genannt) i. S. v. Klausel 15, der kein Verbraucher ist, für die Datenfernübertragung auf elektronischem Wege – nachfolgend „Datenfernübertragung" oder „DFÜ" genannt – zur Verfügung. Die Datenfernübertragung umfasst die Einreichung und Abruf von Dateien (insbesondere Übermittlung von Aufträgen[1] und Informationsabruf). Die Bank wird hiermit zur Weiterleitung der Aufträge[1] ermächtigt und beauftragt und leitet diese nach der Maßgabe der Klausel 14 II zur Ausführung an ihre jeweilige Filiale oder die jeweilige Tochter-Bank oder Filiale der Tochter-Bank weiter, bei der das betreffende Konto/die betreffenden Konten geführt wird/werden (kontoführende Stelle).

(2) Die Bank gibt dem Kunden die Dienstleistungsarten bekannt, die er im Rahmen der Datenfernübertragung nutzen kann. Zur Nutzung der Datenfernübertragung gelten die mit der Bank vereinbarten Verfügungslimite.

(3) Die Datenfernübertragung ist über die EBICS-Anbindung (Anlagen 1a bis 1c) möglich.

(4) Der Satz- und Dateiaufbau für die Übermittlung von Aufträgen[1] und den Informationsabruf wird in der Spezifikation der Datenformate (Anlage 3) beschrieben.

(5) Konten bei einem nicht zur Bank gehörigen Finanzinstitut (Drittbank) können nur in den Service aufgenommen werden, wenn die Bank von der Drittbank zuvor eine ausreichende schriftliche Bestätigung darüber erhält, dass der Kunde (i) die Drittbank autorisiert hat, auf der Grundlage der jeweiligen Kontovereinbarung(en) der Drittbank von der Bank gemäß diesen Bedingungen an die Drittbank weitergeleitete Aufträge[1] auszuführen und (ii) eine separate Vereinbarung mit der Drittbank abgeschlossen hat um sicherzustellen, dass die Bank die für das Konto spezifizierten Kontoinformationen erhält.

2 Nutzer und Teilnehmer, Legitimations- und Sicherungsmedien

(1) Aufträge[1] können über die EBICS-Anbindung nur vom Kunden oder seinen Kontobevollmächtigten erteilt werden. Kunde und Kontobevollmächtigte werden im Folgenden einheitlich als „Nutzer" bezeichnet. Zur Autorisierung von per DFÜ übermittelten Auftragsdaten mittels Elektronischer Unterschrift benötigt jeder Nutzer jeweils individuelle, von der Bank freigeschaltete Legitimationsmedien. Die Anforderungen an die Legitimationsmedien sind in Anlage 1a definiert. Wenn mit der Bank vereinbart, können per DFÜ übermittelte Auftragsdaten[1] mit unterschriebenem Begleitzettel autorisiert werden.

(2) Für den Datenaustausch über die EBICS-Anbindung kann der Kunde zusätzlich zu den Bevollmächtigten „Technische Teilnehmer" benennen, die lediglich befugt sind, den Datenaustausch durchzuführen. Nutzer und Technische Teilnehmer werden im Folgenden unter dem Begriff „Teilnehmer" zusammengefasst. Für die Absicherung des Datenaustauschs benötigt jeder Teilnehmer jeweils individuelle, von der Bank freigeschaltete Sicherungsmedien. Die Anforderungen an die Sicherungsmedien sind in Anlage 1a beschrieben.

3 Verfahrensbestimmungen

(1) Für das zwischen Kunde und Bank vereinbarte Übertragungsverfahren gelten die in Anlage 1a sowie die in der Dokumentation der technischen Schnittstelle (Anlage 1b) und der Spezifikation der Datenformate (Anlage 3) beschriebenen Anforderungen.

(2) Der Kunde ist verpflichtet sicherzustellen, dass alle Teilnehmer das DFÜ-Verfahren und die Spezifikationen beachten.

(3) Die Belegung der Datenfelder richtet sich nach den Belegungs- und Kontrollrichtlinien des jeweils genutzten Formates (Anlage 3).

(4) Der Nutzer hat die Kundenkennung des Zahlungsempfängers beziehungsweise des Zahlers gemäß den maßgeblichen Sonderbedingungen zutreffend anzugeben.

Die in die Abwicklung des Zahlungsauftrages[1] eingeschalteten Zahlungsdienstleister sind berechtigt, die Bearbeitung ausschließlich anhand der Kundenkennung vorzunehmen. Fehlerhafte Angaben können Fehlleitungen des Auftrags[1] zur Folge haben. Schäden und Nachteile, die hieraus entstehen, gehen zu Lasten des Kunden.

(5) Vor der Übertragung von Auftragsdaten[1] an die Bank ist eine Aufzeichnung der zu übertragenden Dateien mit deren vollständigem Inhalt sowie der zur Prüfung der Legitimation übermittelten Daten zu erstellen. Diese ist von dem Kunden mindestens für einen Zeitraum von 30 Kalendertagen ab dem in der Datei angegebenen Ausführungstermin (für Überweisungen) beziehungsweise Fälligkeitstermin (Lastschriften) oder bei mehreren Terminen dem spätesten Termin in der Form nachweisbar zu halten, dass die Datei auf Anforderung der Bank kurzfristig erneut zur Verfügung gestellt werden kann, sofern nichts Abweichendes vereinbart wird.

(6) Außerdem hat der Kunde für jede Einreichung und jeden Abruf von Dateien ein maschinelles Protokoll, das inhaltlich den Bestimmungen von Kapitel 10 der Spezifikation für die EBICS-Anbindung (Anlage 1b) entspricht, zu erstellen, zu seinen Unterlagen zu nehmen und auf Anforderung der Bank zur Verfügung zu stellen.

(7) Soweit die Bank dem Kunden Daten über Zahlungsvorgänge[1] zur Verfügung stellt, die noch nicht endgültig bearbeitet sind, stellen diese lediglich eine unverbindliche

1 Der Begriff kann u.a. die relevanten Zahlungskontendienste "Dauerauftrag", "Lastschrift" und "Überweisung" umfassen.

007 44444 05 DBDE 1913 DFÜ IFC I 190916

Information dar. Die Daten sind jeweils besonders gekennzeichnet.

(8) Die per DFÜ eingelieferten Auftragsdaten[1] sind wie mit der Bank vereinbart entweder mit Elektronischer Unterschrift oder dem unterschriebenen Begleitzettel zu autorisieren. Diese Auftragsdaten werden als Auftrag[1] wirksam

a) bei Einreichung mit Elektronischer Unterschrift, wenn
   – alle erforderlichen Elektronischen Unterschriften der Nutzer per Datenfernübertragung innerhalb des vereinbarten Zeitraumes eingegangen sind und
   – die Elektronischen Unterschriften mit den vereinbarten Schlüsseln erfolgreich geprüft werden können

oder

b) bei Einreichung mit Begleitzettel, wenn
   – der Begleitzettel im vereinbarten Zeitraum bei der Bank eingegangen ist und
   – der Begleitzettel der Kontovollmacht entsprechend unterzeichnet worden ist.

4 Verhaltens- und Sorgfaltspflichten im Umgang mit den Legitimationsmedien für die Autorisierung des Auftrags[1]

(1) Der Kunde ist in Abhängigkeit von dem mit der Bank vereinbarten Übertragungsverfahren verpflichtet sicherzustellen, dass alle Nutzer die Pflichten aus diesen Bedingungen und die in Anlage 1a beschriebenen Legitimationsverfahren einhalten.

(2) Mit Hilfe eines von der Bank freigeschalteten Legitimationsmediums kann der Nutzer Aufträge[1] erteilen. Der Kunde stellt sicher, dass jeder Nutzer dafür Sorge trägt, dass keine andere Person in den Besitz seines Legitimationsmediums kommt sowie Kenntnis von dem zu dessen Schutz dienenden Passwort erlangt. Denn jede andere Person, die im Besitz des Mediums oder eines entsprechenden Duplikates ist, kann in Verbindung mit dem dazugehörigen Passwort die vereinbarten Dienstleistungen missbräuchlich nutzen. Insbesondere Folgendes ist zum Schutz der Legitimationsmedien und des Passwortes zu beachten:

– Das Legitimationsmedium muss vor unberechtigtem Zugriff geschützt und sicher verwahrt werden;
– das zum Schutz des Legitimationsmediums dienende Passwort darf nicht auf dem Legitimationsmedium notiert oder als Abschrift mit diesem zusammen aufbewahrt oder ungesichert elektronisch abgespeichert werden;
– das Legitimationsmedium darf nicht dupliziert werden;
– bei Eingabe des Passwortes ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.

5 Verhaltens- und Sorgfaltspflichten im Umgang mit den Sicherungsmedien für den Datenaustausch

Der Kunde ist im Rahmen der EBICS-Anbindung verpflichtet sicherzustellen, dass alle Teilnehmer die in Anlage 1a beschriebenen Sicherungsverfahren einhalten.

Mit Hilfe der von der Bank freigeschalteten Sicherungsmedien sichert der Teilnehmer den Datenaustausch ab. Der Kunde ist dazu verpflichtet sicherzustellen, dass jeder Teilnehmer dafür Sorge trägt, dass keine andere Person in den Besitz seines Sicherungsmediums kommt oder dieses nutzen kann. Insbesondere im Falle der Ablage auf einem technischen System muss das Sicherungsmedium des Teilnehmers in einer technischen Umgebung gespeichert werden, die vor unautorisiertem Zugriff geschützt ist.

Denn jede andere Person, die Zugriff auf das Sicherungsmedium oder ein entsprechendes Duplikat hat, kann den Datenaustausch missbräuchlich durchführen.

6 Sicherheit des Kundensystems

Der Kunde hat für einen ausreichenden Schutz der von ihm für die Datenfernübertragung eingesetzten Systeme Sorge zu tragen. Die für das EBICS-Verfahren geltenden Sicherheitsanforderungen sind in Anlage 1c beschrieben.

7 Sperre der Legitimations- und Sicherungsmedien

(1) Gehen die Legitimations- oder Sicherungsmedien verloren, werden sie anderen Personen bekannt oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so hat der Teilnehmer unverzüglich seinen DFÜ-Zugang bei der Bank zu sperren oder sperren zu lassen. Näheres regelt die Anlage 1a. Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten aufgeben.

(2) Der Kunde kann außerhalb des DFÜ-Verfahrens die Verwendung der Legitimations- und Sicherungsmedien eines Teilnehmers oder den gesamten DFÜ-Zugang über die von der Bank bekannt gegebene Sperrfazilität sperren lassen.

(3) Die Bank wird den gesamten DFÜ-Zugang sperren, wenn der Verdacht einer missbräuchlichen Nutzung des DFÜ-Zugangs besteht. Die Bank wird den Kunden hierüber außerhalb des DFÜ-Verfahrens informieren. Diese Sperre kann mittels DFÜ nicht aufgehoben werden.

8 Behandlung eingehender Auftragsdaten[1] durch die Bank

(1) Die der Bank per DFÜ-Verfahren übermittelten Auftragsdaten[1] werden im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeitet.

(2) Die Bank prüft anhand der von den Teilnehmern mittels der Sicherungsmedien erstellten Signaturen, ob der Absender berechtigt ist, den Datenaustausch durchzuführen. Ergibt die Prüfung Unstimmigkeiten, wird die Bank die betreffenden Auftragsdaten[1] nicht verarbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen.

(3) Die Bank prüft die Legitimation des Nutzers beziehungsweise der Nutzer und die Autorisierung der per DFÜ übermittelten Auftragsdaten[1] anhand der von den Nutzern mittels der Legitimationsmedien erstellten elektronischen Unterschriften oder des übermittelten Begleitzettels sowie die Übereinstimmung der Auftragsdatensätze mit den Bestimmungen gemäß Anlage 3. Ergibt die Prüfung Unstimmigkeiten, wird die Bank die betreffenden Auftragsdaten[1]

1 Der Begriff kann u.a. die relevanten Zahlungskontendienste "Dauerauftrag", "Lastschrift" und "Überweisung" umfassen.

007 44444 05 DBDE 1913 DFÜ IFC I 190916

nicht bearbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen. Die Bank ist berechtigt, nicht vollständig autorisierte Auftragsdaten[1] nach Ablauf des von der Bank gesondert mitgeteilten Zeitlimits zu löschen.

(4) Ergeben sich bei den von der Bank durchgeführten Prüfungen der Dateien oder Datensätze nach Anlage 3 Fehler, so wird die Bank die fehlerhaften Dateien oder Datensätze in geeigneter Form nachweisen und sie dem Nutzer unverzüglich mitteilen. Die Bank ist berechtigt, die fehlerhaften Dateien oder Datensätze von der weiteren Bearbeitung auszuschließen, wenn die ordnungsgemäße Ausführung des Auftrages[1] nicht sichergestellt werden kann.

(5) Die Bank ist verpflichtet, die Abläufe (siehe Anlage 1a) und die Weiterleitung der Aufträge[1] zur Bearbeitung im Kundenprotokoll zu dokumentieren. Der Kunde ist seinerseits verpflichtet, das Kundenprotokoll zeitnah abzurufen und sich über den Status der Auftragsbearbeitung[1] zu informieren. Bei Unstimmigkeiten soll er sich mit der Bank in Verbindung setzen.

(6) Besonderheiten bei Eilzahlungen - Für Konten, die in die DFÜ-Vereinbarung eingebunden sind, wird die Bank gemäß den Bestimmungen dieses Absatzes sowohl Inlandszahlungsaufträge[1] als auch Auslandszahlungsaufträge[1] in Euro als „eilig" ausführen, wenn diese durch Nutzung eines entsprechenden Geschäftsvorfall-Codes (GVO) als eilig gekennzeichnet und mit elektronischer Unterschrift versehen sind. Dies gilt auch für regionale Feiertage, d. h. für Feiertage, die keine TARGET-Feiertage sind. Für Auslandszahlungsaufträge[1] in Euro werden spezielle Belegungsrichtlinien in der Spezifikation der Datenformate in Anlage 3 festgelegt.

Der Kunde ist verpflichtet, das erstellte Protokoll über die erteilten eiligen Zahlungsaufträge unmittelbar nach Auftragserteilung abzurufen.

Für ordnungsgemäß erteilte eilige Zahlungsaufträge[1] im Inlandszahlungsverkehr wird die Bank die gleichtägige Verbuchung und die Weiterleitung an das TARGET2-Clearingsystem der Bundesbank mit Vorgabe der gleichtägigen Valuta veranlassen, wenn diese Zahlungsaufträge[1] bis 14:00 Uhr bei ihr eingegangen sind. Gehen solche Aufträge zwischen 14:00 Uhr und 16:30 Uhr bei der Bank ein, wird sich die Bank bemühen, eine valutengleiche Übertragung durchzuführen. In Abhängigkeit der Annahmeschlusszeiten für die gleichtägige Verarbeitung über das TARGET2-Clearingsystem der Bundesbank werden Aufträge[1], die jeweils nach 16:30 Uhr – Stand 10/2008 – bei der Bank eingehen, erst am folgenden Arbeitstag ausgeführt.

Für ordnungsgemäß erteilte eilige Zahlungsaufträge[1] in Euro im Auslandszahlungsverkehr wird die Bank die gleichtägige Verbuchung und die Weiterleitung an das Clearingsystem der Bank des Begünstigten mit Vorgabe der gleichtägigen Valuta veranlassen, sofern diese bis 15:30 Uhr bei der Bank eingegangen sind. Gehen Aufträge[1] bei der Bank zwischen 15:31 Uhr und 16:30 Uhr ein, kann die valutengleiche Übertragung nicht mehr gesichert veranlasst werden, die Bank wird sich jedoch bemühen, eine valutengleiche Übertragung durchzuführen. Euro-Eilzahlungen[1], die nach 16:30 Uhr bei der Bank eingehen, werden erst am folgenden Arbeitstag ausgeführt. Voraussetzung ist jeweils, dass das Clearingsystem der Bank des Begünstigten geöffnet ist und die Bank des Begünstigten einem solchen Clearingsystem angeschlossen ist. Sind diese Kriterien nicht erfüllt, kann die Zahlung nach Ermessen der Bank mit der DTAZV-Zahlungsart „SWIFT-Eilig" abgewickelt werden.

Eilige Inlandszahlungsaufträge[1] als auch eilige Auslandszahlungsaufträge[1] in Euro wird die Bank als Einzelposten verbuchen.

9 Rückruf

(1) Vor der Autorisierung der Auftragsdaten[1] kann der Kunde die Datei zurückrufen. Änderungen einzelner Auftragsdaten[1] sind nur durch Rückruf der gesamten Datei und erneute Einlieferung möglich. Die Bank kann einen Rückruf nur beachten, wenn ihr dieser so rechtzeitig zugeht, dass seine Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufes möglich ist.

(2) Die Widerrufbarkeit eines Auftrags[1] richtet sich nach den dafür geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen[1] kann nur außerhalb des DFÜ-Verfahrens erfolgen oder, wenn mit dem Kontoinhaber vereinbart, nach den Vorgaben von Kapitel 11 der Anlage 3. Hierzu hat der Kunde der Bank die Einzelangaben des Originalauftrages mitzuteilen.

(3) Ergänzend zu der Klausel 8 (1) und (2) kann sowohl ein Rückruf als auch ein Widerruf elektronisch im Rahmen des DFÜ-Verfahrens mittels des entsprechenden GVOs an die Bank geleitet werden. Informationen zum Status eingereichter Rückrufe und Widderrufe können ebenfalls elektronisch mittels des entsprechenden GVOs, bereitgestellt werden.

10 Ausführung der Aufträge[1]

(1) Die Bank wird die Aufträge[1] ausführen, wenn alle nachfolgenden Ausführungsbedingungen vorliegen:
- Die per DFÜ eingelieferten Auftragsdaten[1] wurden gemäß Nummer 3 Absatz 8 autorisiert.
- Das festgelegte Datenformat ist eingehalten.
- Das Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart[1] maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

(2) Liegen die Ausführungsbedingungen nach Absatz 1 nicht vor, wird die Bank den Auftrag[1] nicht ausführen und den Kunden über die Nichtausführung unverzüglich auf dem vereinbarten Weg unterrichten. Soweit möglich, nennt die Bank dem Kunden die Gründe und Fehler, die zur Nichtausführung geführt haben, und Möglichkeiten, wie diese Fehler berichtigt werden können.

1 Der Begriff kann u.a. die relevanten Zahlungskontendienste "Dauerauftrag", "Lastschrift" und "Überweisung" umfassen.

007 44444 05 DBDE 1913 DFÜ IFC I 190916

(3) Sofern mittels DFÜ SEPA-Echtzeitüberweisungen beauftragt werden und die Ausführung solcher Transaktionen daran scheitern, dass die Empfängerbank nicht für SEPA-Echtzeitüberweisung erreichbar ist, einigen sich Bank und Kunde, dass diese Transaktionen als SEPA-Überweisung ausgeführt werden. Hierüber wird der Einreicher mittels einer pain.002-Nachricht informiert, welche die Bank zum Abruf mittels DFÜ bereitstellt. Der Kunde und die Bank können gesondert vereinbaren, dass eine solche Umwandlung von SEPA-Echtzeitüberweisungen in SEPA-Überweisungen nicht stattfinden soll und damit diese Transaktionen abgewiesen werden.

(4) Sofern mittels DFÜ SEPA-Echtzeitüberweisungen beauftragt werden, vereinbaren der Kunde und die Bank folgende Abweichungen von den Sonderbedingungen für SEPA-Echtzeitüberweisungen:

a) In Abhängigkeit von der Anzahl der eingereichten Transaktionen kann die Verarbeitung der SEPA-Echtzeitüberweisungen innerhalb von Minuten anstelle von wenigen Sekunden stattfinden.

b) Aufgrund der Eigenschaft des DFÜ-Verfahrens können SEPA-Echtzeitüberweisungen über EBICS nur an TARGET-Arbeitstagen (montags bis freitags mit Ausnahme von 1. Januar, Karfreitag, Ostermontag, 1. Mai, 25. und 26. Dezember) erfolgen, sofern eine Verbindung zum EBICS-Server der Bank aufgebaut werden kann. Für SEPA-Echtzeitüberweisungen gelten die für SEPA-Überweisungen gültigen Annahmezeiten.

c) Sofern eine SEPA-Echtzeitüberweisung aus anderen Gründen als den in Absatz 3 genannten von der Empfängerbank nicht akzeptiert wird und endgültig unausführbar ist, gilt die Regelung in Absatz 2.

11 Haftung

11.1 Haftung der Bank bei einer nicht autorisierten DFÜ-Verfügung[1] und einer nicht, fehlerhaft oder verspätet ausgeführten DFÜ-Verfügung[1]

Die Haftung der Bank bei einer nicht autorisierten DFÜ-Verfügung[1] und einer nicht, fehlerhaft oder verspätet ausgeführten DFÜ-Verfügung richtet sich nach den für die jeweilige Auftragsart[1] vereinbarten Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr).

11.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung der Legitimations- oder Sicherungsmedien

11.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge[1] vor der Sperranzeige

(1) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen[1] aufgrund einer missbräuchlichen Nutzung der Legitimations- oder Sicherungsmedien, haftet der Kontoinhaber gegenüber der Bank für die ihr dadurch entstehenden Schäden, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Verhaltens- und Sorgfaltspflichten verstoßen hat. Der § 675v des Bürgerlichen Gesetzbuchs findet keine Anwendung.

(2) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 7 Absatz 1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch vermieden worden wäre.

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

(4) Die Absätze 2 und 3 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

11.2.2 Haftung des Kunden bei sonstigen nicht autorisierten Vorgängen vor der Sperranzeige

Beruhen nicht autorisierte Vorgänge, die keine Zahlungsvorgänge sind, vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Legitimations- oder Sicherungsmediums oder auf der sonstigen missbräuchlichen Nutzung des Legitimations- oder Sicherungsmediums und ist der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

11.2.3 Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte DFÜ-Verfügungen[1] entstehenden Schäden. Dies gilt nicht, wenn ein Teilnehmer in betrügerischer Absicht gehandelt hat.

11.3 Haftungsausschluss

Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.

12 Drittbanken; Dienste von Dritten

(1) Sofern Konten bei Drittbanken an DFÜ-Service beteiligt sind, wird der Kunde mit diesen jeweils gesonderte Vereinbarungen über Art und Umfang des DFÜ-Service treffen.

(2) Greift eine Partei im Rahmen des Service auf die Dienste von Dritten zurück, ist sie der anderen Partei gegenüber für alle Handlungen, Fehler oder Unterlassungen dieses Dritten genauso verantwortlich, wie wenn sie die Handlungen selbst durchgeführt oder Unterlassungen zu verantworten hätte. Für die Zwecke der vorliegenden Vereinbarung gilt, dass der Dritte im Auftrag der Partei handelt, von der er eingeschaltet wurde.

13 Laufzeit, Kündigung

(1) Die Vereinbarung tritt am Tag der ersten Auftragsverarbeitung[1] durch die Bank, womit das Angebot des Kunden konkludent angenommen wird, in Kraft. Sie wird auf unbestimmte Zeit geschlossen. Die Bank wird den Kunden

1 Der Begriff kann u.a. die relevanten Zahlungskontendienste "Dauerauftrag", "Lastschrift" und "Überweisung" umfassen.

007 44444 05 DBDE 1913 DFÜ IFC I 190916

informieren, wenn sie die Registrierung eines Kontos oder Nutzers ablehnt.

(2) Sowohl der Kunde – für sich selbst und für jede Kundengesellschaft – als auch die Bank können die Vereinbarung insgesamt mit einer Kündigungsfrist von dreißig (30) Kalendertagen durch schriftliche Erklärung gegenüber der anderen Partei kündigen.

(3) Sowohl der Kunde – für sich selbst und für jede Kundengesellschaft – als auch die Bank können diese Vereinbarung insgesamt mit sofortiger Wirkung schriftlich kündigen, wenn hierfür ein wichtiger Grund vorliegt, aufgrund dessen es für die kündigende Partei – auch unter angemessener Berücksichtigung der berechtigten Belange der anderen Partei – unzumutbar ist, die Geschäftsbeziehung fortzusetzen.

(4) Nach Maßgabe von Klausel 13 (2) bzw. (3) kann jede Kundengesellschaft diese Vereinbarung für sich selbst und die Bank diese Vereinbarung auch gegenüber einer oder mehreren Kundengesellschaften (die in der Kündigungserklärung entsprechend zu benennen sind) kündigen.

14 Gültigkeit der Kontovereinbarungen mit kontoführenden Stellen

(1) Unbeschadet ausdrücklich abweichender Bestimmungen, bleiben die Regelungen des Kunden mit einer kontoführenden Stelle von diesen Bedingungen unberührt.

(2) Der Kunde stimmt zu und steht dafür ein, dass jede kontoführende Stelle, die eine Filiale, Geschäftsstelle oder Tochtergesellschaft der Bank ist, (i) gemäß diesen Bedingungen berechtigt und angewiesen ist, alle ihr von der Bank zugestellten Aufträge[1] zu verarbeiten und auszuführen, (ii) weiterhin berechtigt ist, diese Aufträge[1] so zu behandeln, als wären sie ihr direkt von solchen Personen erteilt worden, die solche Aufträge[1] im Namen des Kunden als Kontoinhaber des betreffenden Kontos erteilen durften, (iii) deshalb davon ausgehen kann, dass die Aufträge[1] vom Kunden ordnungsgemäß erteilt wurden und für sie verbindlich sind, (iv) des Weiteren ermächtigt ist, der Bank alle Informationen betreffend von diesen Bedingungen betroffener Konten zukommen zu lassen und (v) ihr, aufgrund ihres Handelns im Vertrauen auf die voranstehenden Regelungen in (i) bis (iv), die Haftungsbegrenzungen und Schadenersatzansprüche der Klausel 11 als Begünstigte zu Gute kommen.

15 Beitritt von Kundengesellschaften; Ernennung eines Hauptbevollmächtigten

(1) Die Erweiterung des DFÜ-Service auf ein zur Unternehmensgruppe des Kunden gehörendes Unternehmen erfordert den Beitritt des betreffenden Unternehmens zur vorliegenden Vereinbarung mittels der gesonderten Beitrittserklärung.

(2) Mit dem Beitritt zur Vereinbarung wird das betreffende Unternehmen eine „Kundengesellschaft" im Sinne der vorliegenden Vereinbarung und ernennt zur Ausgabe und zum Empfang sämtlicher Erklärungen sowie zur Durchführung aller in dieser Vereinbarung vorgesehenen oder im Zusammenhang damit als erforderlich oder zweckdienlich erachteten Handlungen den Kunden zu ihrem Hauptbevollmächtigten. Der Kunde und die Kundengesellschaft sichern der Bank hiermit zu und gewährleisten, dass der Kunde und die Kundengesellschaft im Zusammenhang mit dieser Ernennung alle Handlungen ausgeführt, alle Bekanntmachungen vorgenommen und jegliche erforderlichen Einverständniserklärungen abgegeben haben, die notwendig sind um den Kunden von jeder Einschränkung des Selbstkontrahierens oder ähnlichen Einschränkungen nach geltendem Recht, die andernfalls das Handeln im Auftrag der Kundengesellschaft unwirksam machen würden, zu befreien.

16 Geltendes Recht

(1) Die vorliegenden Bedingungen unterliegen deutschem Recht.

(2) Gerichtsstand für alle Rechtsstreitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung ist Frankfurt am Main, Deutschland. Ungeachtet dessen können rechtliche Schritte gegen eine Partei dieses Vertrages auch bei denjenigen Gerichten eingeleitet werden, die am Sitz der jeweiligen Partei zuständig sind.

17 Schlussbestimmungen

Die in diesen Bedingungen erwähnten Anlagen sind Bestandteil der mit dem Kunden geschlossenen Vereinbarung.

Anlage 1a: EBICS-Anbindung

Anlage 1b: Spezifikation der EBICS-Anbindung

Anlage 1c: Sicherheitsanforderungen an das EBICS-Kundensystem

Anlage 2: derzeit nicht belegt

Anlage 3: Spezifikation der Datenformate

Anlage 1a: EBICS-Anbindung

1 Legitimations- und Sicherungsverfahren

Der Kunde (Kontoinhaber) benennt der Bank die Teilnehmer und deren Berechtigungen im Rahmen der Datenfernübertragung.

Folgende Legitimations- und Sicherungsverfahren werden in der EBICS-Anbindung eingesetzt:
- Elektronische Unterschriften
- Authentifikationssignatur
- Verschlüsselung

Für jedes Legitimations- und Sicherungsverfahren verfügt der Teilnehmer über ein individuelles Schlüsselpaar, das aus einem privaten und einem öffentlichen Schlüssel besteht. Die öffentlichen Teilnehmerschlüssel sind der Bank

1 Der Begriff kann u.a. die relevanten Zahlungskontendienste "Dauerauftrag", "Lastschrift" und "Überweisung" umfassen.

007 44444 05 DBDE 1913 DFÜ IFC I 190916

gemäß dem in Nummer 2 beschriebenen Verfahren mitzuteilen. Die öffentlichen Bankschlüssel sind gemäß dem in Nummer 2 beschriebenen Verfahren gegen unautorisiertes Verändern zu schützen. Die Schlüsselpaare des Teilnehmers können auch für die Kommunikation mit anderen Banken eingesetzt werden.

1.1 Elektronische Unterschriften

1.1.1 Elektronische Unterschriften der Teilnehmer
Für die Elektronischen Unterschriften (EU) der Teilnehmer sind die folgenden Unterschriftsklassen definiert:
- Einzelunterschrift (Typ „E")
- Erstunterschrift (Typ „A")
- Zweitunterschrift (Typ „B")
- Transportunterschrift (Typ „T")

Als bankfachliche EU bezeichnet man EU vom Typ „E", „A", oder „B". Bankfachliche EU dienen der Autorisierung von Aufträgen[1]. Aufträge[1] können mehrere bankfachliche EU benötigen, die von unterschiedlichen Nutzern (Kontoinhaber und deren Bevollmächtigte) geleistet werden müssen. Für jede unterstützte Auftragsart[1] wird zwischen Bank und Kunde eine Mindestanzahl erforderlicher bankfachlicher EU vereinbart.

EU vom Typ „T", die als Transportunterschriften bezeichnet werden, werden nicht zur bankfachlichen Freigabe von Aufträgen[1] verwendet, sondern lediglich zu deren Übertragung an die Banksysteme. „Technische Teilnehmer" (siehe Nummer 2.2) können nur eine EU vom Typ „T" zugewiesen bekommen.

Mit dem vom Kunden verwendeten Programm können verschiedene Nachrichten (z. B. Aufträge[1] für den Inlands- und Auslandszahlungsverkehr, aber auch für Initialisierung, den Protokollabruf und die Abholung von Konto- und Umsatzinformationen etc.) erstellt werden. Die Bank teilt dem Kunden mit, welche Nachrichtenarten genutzt werden können und welcher EU-Typ hierfür anzuwenden ist.

1.1.2 Authentifikationssignatur
Im Gegensatz zur EU, die Auftragsdaten[1] signiert, wird die Authentifikationssignatur über die einzelne EBICS-Nachricht einschließlich Steuerungs- und Anmeldedaten und die darin enthaltenen EU gebildet. Mit Ausnahme einiger in der EBICS-Spezifikation definierter systembedingter Auftragsarten wird die Authentifikationssignatur bei jedem Transaktionsschritt sowohl vom Kunden- als auch vom Banksystem geleistet. Der Kunde muss gewährleisten, dass eine Software eingesetzt wird, die die Authentifikationssignatur jeder von der Bank übermittelten EBICS-Nachricht unter Berücksichtigung der Aktualität und Authentizität der gespeicherten öffentlichen Schlüssel der Bank gemäß den Vorgaben der EBICS-Spezifikation (siehe Anlage 1b) prüft.

1.2 Verschlüsselung
Zur Gewährleistung der Geheimhaltung der bankfachlichen Daten auf Anwendungsebene sind die Auftragsdaten[1] vom Kunden unter Berücksichtigung der Aktualität und Authentizität der gespeicherten öffentlichen Schlüssel der Bank gemäß den Vorgaben der EBICS-Spezifikation (siehe Anlage 1b) zu verschlüsseln.

Darüber hinaus ist auf den externen Übertragungsstrecken zwischen Kunden- und Banksystem zusätzlich eine Transportverschlüsselung vorzunehmen. Der Kunde muss gewährleisten, dass eine Software eingesetzt wird, die gemäß den Vorgaben der EBICS-Spezifikation (siehe Anlage 1b) Aktualität und Authentizität der hierfür eingesetzten Serverzertifikate der Bank überprüft.

2 Initialisierung der EBICS-Anbindung

2.1 Einrichtung der Kommunikationsverbindung
Der Kommunikationsaufbau erfolgt unter Verwendung einer URL (Uniform Resource Locator). Alternativ kann auch eine IP-Adresse der jeweiligen Bank benutzt werden. Die URL oder die IP-Adresse werden dem Kunden bei Vertragsabschluss mit der Bank mitgeteilt.

Die Bank teilt den vom Kunden benannten Teilnehmern zur Aufnahme der EBICS-Anbindung folgende Daten mit:
- URL oder IP-Adresse der Bank
- Bezeichnung der Bank
- HostID
- Zulässige Version(en) für das EBICS-Protokoll und der Sicherungsverfahren
- Partner-ID (Kunden-ID)
- User-ID
- System-ID (für technische Teilnehmer)
- Weitere spezifische Angaben zu Kunden- und Teilnehmerberechtigungen

Für die dem Kunden zugeordneten Teilnehmer vergibt die Bank jeweils eine User-ID, die den Teilnehmer eindeutig identifiziert. Soweit dem Kunden ein oder mehrere technische Teilnehmer zugeordnet sind (Multi-User-System), vergibt die Bank zusätzlich zur User-ID eine System-ID. Soweit kein technischer Teilnehmer festgelegt ist, sind System-ID und User-ID identisch.

2.2 Initialisierung der Teilnehmer Schlüssel
Die vom Teilnehmer eingesetzten Schlüsselpaare für die bankfachliche EU, die Verschlüsselung der Auftragsdaten[1] und die Authentifikationssignatur müssen zusätzlich zu den in Nummer 1 beschriebenen allgemeinen Bedingungen den nachfolgenden Anforderungen genügen:

1. Die Schlüsselpaare sind ausschließlich und eindeutig dem Teilnehmer zugeordnet.

2. Soweit der Teilnehmer seine Schlüssel eigenständig generiert, sind die privaten Schlüssel mit Mitteln zu erzeugen, die der Teilnehmer unter seiner alleinigen Kontrolle halten kann.

3. Sofern die Schlüssel von einem Dritten zur Verfügung gestellt werden, ist sicherzustellen, dass der Teilnehmer in den alleinigen Besitz der privaten Schlüssel gelangt.

1 Der Begriff kann u.a. die relevanten Zahlungskontendienste "Dauerauftrag", "Lastschrift" und "Überweisung" umfassen.

007 44444 05 DBDE 1913 DFÜ IFC I 190916

4. Für die zur Legitimation eingesetzten privaten Schlüssel definiert jeder Nutzer pro Schlüssel ein Passwort, das den Zugriff auf den jeweiligen privaten Schlüssel absichert.

5. Für die zur Absicherung des Datenaustausches eingesetzten privaten Schlüssel definiert jeder Teilnehmer pro Schlüssel ein Passwort, das den Zugriff auf den jeweiligen privaten Schlüssel absichert. Auf dieses Passwort kann verzichtet werden, wenn das Sicherungsmedium des Teilnehmers in einer technischen Umgebung gespeichert ist, die vor unautorisiertem Zugriff geschützt ist.

Für die Initialisierung des Teilnehmers bei der Bank ist die Übermittlung der öffentlichen Schlüssel des Teilnehmers an das Banksystem erforderlich. Hierfür übermittelt der Teilnehmer der Bank seine öffentlichen Schlüssel auf zwei voneinander unabhängigen Kommunikationswegen:
– Über die EBICS-Anbindung mittels der hierfür vorgesehenen systembedingten Auftragsarten.
– Mit einem vom Kontoinhaber oder einem Kontobevollmächtigten unterschriebenen Initialisierungsbrief.

Für die Freischaltung des Teilnehmers überprüft die Bank auf Basis der vom Kontoinhaber oder einem Kontobevollmächtigten unterschriebenen Initialisierungsbriefe die Authentizität der über EBICS übermittelten öffentlichen Teilnehmerschlüssel.

Zu jedem öffentlichen Teilnehmerschlüssel enthält der Initialisierungsbrief die folgenden Daten:
– Verwendungszweck des öffentlichen Teilnehmerschlüssels
– Elektronische Unterschrift
– Authentifikationssignatur
– Verschlüsselung
– Die jeweils unterstützte Version pro Schlüsselpaar
– Längenangabe des Exponenten
– Exponent des öffentlichen Schlüssels in hexadezimaler Darstellung
– Längenangabe des Modulus
– Modulus des öffentlichen Schlüssels in hexadezimaler Darstellung
– Hashwert des öffentlichen Schlüssels in hexadezimaler Darstellung

Die Bank prüft die Unterschrift des Kontoinhabers beziehungsweise des Kontobevollmächtigten auf dem Initialisierungsbrief sowie die Übereinstimmung zwischen den über die EBICS-Anbindung und den schriftlich übermittelten Hashwerten des öffentlichen Schlüssels des Teilnehmers. Bei positivem Prüfergebnis schaltet die Bank den betreffenden Teilnehmer für die vereinbarten Auftragsarten[1] frei.

2.3 Initialisierung der bankseitigen Schlüssel
Der Teilnehmer holt den öffentlichen Schlüssel der Bank mittels einer eigens dafür vorgesehenen systembedingten Auftragsart ab.

Der Hashwert des öffentlichen Bankschlüssels wird von der Bank zusätzlich über einen zweiten, mit dem Kunden gesondert vereinbarten Kommunikationsweg bereitgestellt.

Vor dem ersten Einsatz von EBICS hat der Teilnehmer die Echtheit der ihm per Datenfernübertragung übermittelten öffentlichen Bankschlüssel dadurch zu überprüfen, dass er deren Hashwerte mit den Hashwerten vergleicht, die von der Bank über den gesondert vereinbarten Kommunikationsweg mitgeteilt wurden.

Der Kunde muss gewährleisten, dass eine Software eingesetzt wird, die die Gültigkeit der im Rahmen der Transportverschlüsselung eingesetzten Serverzertifikate anhand des von der Bank gesondert mitgeteilten Zertifizierungspfades überprüft.

3 Besondere Sorgfaltspflichten bei Erzeugung von Legitimations- und Sicherungsmedien durch den Kunden

Soweit der Kunde seine Legitimations- und Sicherungsmedien nach den Vorgaben der EBICS-Spezifikation selbst erzeugt und er diese bei seiner Bank initialisiert, hat er Folgendes sicherzustellen:
– In allen Phasen der Authentifizierung, inklusive Anzeige, Übermittlung und Speicherung sind Vertraulichkeit und Integrität des Legitimationsmediums zu gewährleisten.
– Private Teilnehmerschlüssel auf den Legitimations- und Sicherungsmedien dürfen nicht im Klartext abgespeichert werden.
– Spätestens nach fünfmaliger Fehleingabe des Passwortes wird das Legitimationsmedium gesperrt.
– Die Generierung der privaten und öffentlichen Teilnehmerschlüssel muss in einer sicheren Umgebung erfolgen.
– Die Legitimations- und Sicherungsmedien sind ausschließlich und eindeutig dem Teilnehmer zuzuordnen und zu verwenden.

4 Auftragserteilung[1] an die Bank

Der Nutzer überprüft die Auftragsdaten[1] auf ihre Richtigkeit und stellt sicher, dass genau diese Daten elektronisch unterschrieben werden. Bei Aufnahme der Kommunikation werden seitens der Bank zuerst teilnehmerbezogene Berechtigungsprüfungen durchgeführt, wie etwa die Auftragsartberechtigung[1] oder gegebenenfalls vereinbarte Limitprüfungen. Die Ergebnisse weiterer bankfachlicher Prüfungen wie beispielsweise Limitprüfungen oder Kontoberechtigungsprüfungen werden dem Kunden im Kundenprotokoll zu einem späteren Zeitpunkt mitgeteilt.

Auftragsdaten[1], die an das Banksystem übermittelt werden, können wie folgt autorisiert werden:

1. Alle erforderlichen bankfachlichen EU werden zusammen mit den Auftragsdaten[1] übertragen.

2. Sofern mit dem Kunden für die jeweilige Auftragsart[1] die Verteilte Elektronische Unterschrift (VEU) vereinbart wurde und die übermittelten EU für die bankfachliche Freigabe nicht ausreichen, wird der Auftrag[1] bis zur Abgabe aller erforderlichen EU im Banksystem gespeichert.

1 Der Begriff kann u.a. die relevanten Zahlungskontendienste "Dauerauftrag", "Lastschrift" und "Überweisung" umfassen.

007 44444 05 DBDE 1913 DFÜ IFC I 190916

3. Soweit Kunde und Bank vereinbaren, dass die Autorisierung von per DFÜ übermittelten Auftragsdaten[1] mittels gesondert übermittelten Begleitzettels erfolgen kann, ist an Stelle der bankfachlichen EU des Nutzers eine Transportunterschrift (Typ „T“) für die technische Absicherung der Auftragsdaten[1] zu leisten. Hierfür ist die Datei mit einer speziellen Kennung zu versehen, die angibt, dass es außer der Transportunterschrift (Typ „T“) keine weitere EU für diesen Auftrag[1] gibt. Die Freigabe des Auftrags[1] erfolgt nach erfolgreicher Prüfung der Unterschrift des Nutzers auf dem Begleitzettel durch die Bank.

4.1 Auftragserteilung[1] mittels Verteilter Elektronischer Unterschrift (VEU)

Die Art und Weise, wie die Verteilte Elektronische Unterschrift durch den Kunden genutzt wird, muss mit der Bank vereinbart werden.

Die Verteilte Elektronische Unterschrift (VEU) ist dann einzusetzen, wenn die Autorisierung von Aufträgen[1] unabhängig vom Transport der Auftragsdaten[1] und gegebenenfalls auch durch mehrere Teilnehmer erfolgen soll.

Solange noch nicht alle zur Autorisierung erforderlichen bankfachlichen EU vorliegen, kann der Auftrag[1] von einem hierzu berechtigten Nutzer gelöscht werden. Soweit der Auftrag[1] vollständig autorisiert wurde, ist nur noch ein Rückruf gemäß Nummer 9 der Bedingungen für die Datenfernübertragung möglich.

Die Bank ist dazu berechtigt, nicht vollständig autorisierte Aufträge[1] nach Ablauf des von der Bank gesondert mitgeteilten Zeitlimits zu löschen.

4.2 Legitimationsprüfung durch die Bank

Per DFÜ eingelieferte Auftragsdaten[1] werden als Auftrag[1] durch die Bank erst dann ausgeführt, wenn die erforderlichen bankfachlichen EU beziehungsweise der unterschriebene Begleitzettel eingegangen sind und mit positivem Ergebnis geprüft wurden.

4.3 Kundenprotokolle

Die Bank dokumentiert in Kundenprotokollen die folgenden Vorgänge:

- Übertragung der Auftragsdaten[1] an das Banksystem
- Übertragung von Informationsdateien von dem Banksystem an das Kundensystem
- Ergebnis einer jeden Legitimationsprüfung von Aufträgen[1] des Kunden an das Banksystem
- Weiterverarbeitung von Aufträgen[1], sofern sie die Unterschriftsprüfung, die Anzeige von Auftragsdaten[1] betreffen

Der Teilnehmer hat sich durch zeitnahen Abruf des Kundenprotokolls über das Ergebnis der auf Seiten der Bank durchgeführten Prüfungen zu informieren.

Der Teilnehmer hat dieses Protokoll, das inhaltlich den Bestimmungen von Kapitel 10 der Anlage 1b entspricht, zu seinen Unterlagen zu nehmen und auf Anforderung der Bank zur Verfügung zu stellen.

5 Änderung der Teilnehmerschlüssel mit automatischer Freischaltung

Wenn die vom Teilnehmer eingesetzten Legitimations- und Sicherungsmedien in ihrer Gültigkeit zeitlich begrenzt sind, hat der Teilnehmer der Bank die neuen öffentlichen Teilnehmerschlüssel rechtzeitig vor dem Erreichen des Ablaufdatums zu übermitteln. Nach dem Erreichen des Ablaufdatums der alten Schlüssel ist eine Neuinitialisierung vorzunehmen.

Wenn der Teilnehmer seine Schlüssel selbst generiert, so hat er zu dem mit der Bank vereinbarten Zeitpunkt die Teilnehmerschlüssel unter Verwendung der dafür vorgesehenen systembedingten Auftragsarten zu erneuern und rechtzeitig vor dem Erreichen des Ablaufdatums der alten Schlüssel zu übermitteln.

Für eine automatische Freischaltung der neuen Schlüssel ohne eine erneute Teilnehmerinitialisierung sind die folgenden Auftragsarten zu nutzen:

- Aktualisierung des öffentlichen bankfachlichen Schlüssels (PUB)

und

- Aktualisierung des öffentlichen Authentifikationsschlüssels und des öffentlichen Verschlüsselungsschlüssels (HCA)

oder alternativ

– Aktualisierung aller drei oben genannter Schlüssel (HCS).

Die Auftragsarten PUB und HCA bzw. HCS sind hierfür mit einer gültigen bankfachlichen EU des Nutzers zu versehen. Nach erfolgreicher Änderung sind nur noch die neuen Schlüssel zu verwenden.

Wenn die Elektronische Unterschrift nicht erfolgreich geprüft werden konnte, wird wie unter Nummer 8 Absatz 3 der Bedingungen für die Datenfernübertragung verfahren.

Die Schlüsseländerung darf erst nach Abarbeitung aller Aufträge erfolgen. Ansonsten sind die noch nicht ausgeführten Aufträge[1] mit dem neuen Schlüssel neu zu erteilen.

6 Sperrung der Teilnehmerschlüssel

Besteht der Verdacht des Missbrauchs der Teilnehmerschlüssel, ist der Teilnehmer dazu verpflichtet, seine Zugangsberechtigung zu allen Banksystemen zu sperren, die den/die kompromittierten Schlüssel verwenden.

Soweit der Teilnehmer über gültige Legitimations- und Sicherungsmedien verfügt, kann er seine Zugangsberechtigung via EBICS-Anbindung sperren. Hierbei wird durch Senden einer Nachricht mit der Auftragsart „SPR“ der Zugang für den jeweiligen Teilnehmer, unter dessen User-ID die Nachricht gesendet wird, gesperrt. Nach einer Sperre können bis zu der unter Nummer 2 beschriebenen Neuinitialisierung keine Aufträge[1] von diesem Teilnehmer per EBICS-Anbindung mehr erteilt werden.

Wenn der Teilnehmer nicht mehr über gültige Legitimations- und Sicherungsmedien verfügt, kann er außerhalb

1 Der Begriff kann u.a. die relevanten Zahlungskontendienste "Dauerauftrag", "Lastschrift" und "Überweisung" umfassen.

007 44444 05 DBDE 1913 DFÜ IFC I 190916

des DFÜ-Verfahrens seine Legitimations- und Sicherungsmedien über die von der Bank gesondert bekannt gegebene Sperrfazilität sperren lassen.

Der Kunde kann außerhalb des DFÜ-Verfahrens die Legitimations- und Sicherungsmedien eines Teilnehmers oder den gesamten DFÜ-Zugang über die von der Bank bekannt gegebene Sperrfazilität sperren lassen.

Anlage 1b: Spezifikation der EBICS-Anbindung

Die Spezifikation ist auf der Webseite www.ebics.de veröffentlicht.

Anlage 1c: Sicherheitsanforderungen an das EBICS-Kundensystem

Über die in Anlage 1a Nummer 6 beschriebenen Sicherheitsmaßnahmen hinaus sind durch den Kunden folgende Anforderungen zu berücksichtigen:

- Die vom Kunden für das EBICS-Verfahren eingesetzte Software muss die in Anlage 1a beschriebenen Anforderungen erfüllen.
- EBICS-Kundensysteme dürfen nicht ohne Firewall eingesetzt werden. Eine Firewall ist eine Einrichtung, die den gesamten ein- und ausgehenden Nachrichtenverkehr überwacht und nur bekannte oder autorisierte Verbindungen zulässt.
- Es ist ein Virenscanner zu installieren, der regelmäßig mit den neuesten Virendefinitions-Dateien auszustatten ist.
- Das EBICS-Kundensystem ist so einzurichten, dass sich der Teilnehmer vor dessen Nutzung anmelden muss. Die Anmeldung hat als normaler Benutzer und nicht als Administrator, der z. B. berechtigt ist, die Installation von Programmen vorzunehmen, zu erfolgen.
- Die internen IT-Kommunikationswege für unverschlüsselte bankfachliche Daten oder für unverschlüsselte EBICS-Nachrichten sind gegen Abhören und Manipulationen zu schützen.
- Wenn sicherheitsrelevante Updates für das jeweils eingesetzte Betriebssystem und weiterer installierter sicherheitsrelevanter Software-Programme vorliegen, sollten die eingesetzten EBICS-Kundensysteme mit diesen aktualisiert werden.

Die Umsetzung dieser Anforderungen liegt ausschließlich in der Verantwortung des Kunden.

Anlage 2: derzeit nicht belegt

Anlage 3: Spezifikation der Datenformate

Die Spezifikation ist auf der Webseite www.ebics.de veröffentlicht.

007 44444 05 DBDE 1913 DFÜ IFC I 190916