Nähere Angaben zur Bank sind im „Preis- und Leistungsverzeichnis“ enthalten.

Bedingungen für Datenfernübertragung

1 Leistungsumfang

(1) Die Bank steht ihrem Kunden (Kontoinhaber), der kein Verbraucher ist, für die Datenfernübertragung auf elektronischem Wege – nachfolgend „Datenfernübertragung“ oder „DFÜ“ genannt – zur Verfügung. Die Datenfernübertragung umfasst die Einreichung und den Abruf von Dateien (insbesondere Übermittlung von Aufträgen und Informationsabruf).

(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 und den Informationsabruf wird in der Spezifikation der Datenformate (Anlage 3) beschrieben.

2 Nutzer und Teilnehmer, Legitimations- und Sicherungsmedien

(1) Aufträge 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 mit unterschriebenem Begleitzettel/Sammelauftrag 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) Reicht der Nutzer eine Datei mit mehreren SEPA-Überweisungen oder SEPA-Echtzeitüberweisungen ein, entscheidet er durch Verwendung der vereinbarten Auftragsart[1], ob die Empfängerüberprüfung gemäß Nummer 2.1.3 der Bedingungen für den Überweisungsverkehr durchgeführt werden soll.

Verzichtet der Nutzer auf die Empfängerüberprüfung, führt die Bank die in der Datei enthaltenen Überweisungen anhand der vom Nutzer angegebenen Kundenkennungen aus. Dies kann im Einzelfall dazu führen, dass das Geld auf ein Zahlungskonto eingeht, dessen Inhaber nicht der vom Nutzer namentlich angegebene Zahlungsempfänger ist.

Reicht der Nutzer eine Datei mit nur einer einzigen SEPA-Überweisung oder SEPA-Echtzeitüberweisung ein, so ist die Bank unabhängig von der Entscheidung des Nutzers gesetzlich verpflichtet, die Empfängerüberprüfung durchzuführen.

Dieser Absatz gilt nicht für per DFÜ übermittelte Auftragsdaten mit unterschriebenem Begleitzettel/Sammelauftrag.

(5) Vor der Übertragung von Auftragsdaten 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) bzw. 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 zur Verfügung stellt, die noch nicht endgültig bearbeitet sind, stellen diese lediglich eine unverbindliche Information dar. Die Daten sind jeweils besonders gekennzeichnet.

(8) Die per DFÜ eingelieferten Auftragsdaten sind wie mit der Bank vereinbart entweder mit Elektronischer Unterschrift oder dem unterschriebenen Begleitzettel/Sammelauftrag zu autorisieren. Diese Auftragsdaten werden als Auftrag 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/Sammelauftrag, wenn
   - der Begleitzettel/Sammelauftrag im vereinbarten Zeitraum bei der Bank eingegangen ist und
   - der Begleitzettel/Sammelauftrag der Kontovollmacht entsprechend unterzeichnet worden ist.

(9) Wird für eine Datei mit SEPA-Überweisungen oder SEPA-Echtzeitüberweisungen die Empfängerüberprüfung gemäß Nummer 3 Absatz 4 durchgeführt, wird die Bank den Nutzer über das Ergebnis informieren. Der Nutzer entscheidet dann, ob

- er die Datei zur Ausführung freigibt oder
- die Datei nicht ausgeführt werden soll.

Der Auftrag ist in Abweichung von Nummer 3 Absatz 8 Satz 2 erst dann wirksam, wenn der Nutzer die Datei nach Satz 2 freigegeben hat.

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

(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 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 des Legitimationsmediums 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 werden 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

[1] Als Auftragsart gilt auch das „Business Transaction and Format“ (BTF) ab EBICS Version 3.0.

© Bank-Verlag GmbH 47.008 (10/25)

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 durch die Bank

(1) Die der Bank per DFÜ-Verfahren übermittelten Auftragsdaten 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 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 anhand der von den Nutzern mittels der Legitimationsmedien erstellten elektronischen Unterschriften oder des übermittelten Begleitzettels/Sammelauftrages sowie die Übereinstimmung der Auftragsdatensätze mit den Bestimmungen gemäß Anlage 3. Ergibt die Prüfung Unstimmigkeiten, wird die Bank die betreffenden Auftragsdaten nicht bearbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen. Die Bank ist berechtigt, nicht vollständig autorisierte Auftragsdaten 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 nicht sichergestellt werden kann.

(5) Reicht der Nutzer eine Datei mit mehreren SEPA-Echtzeitüberweisungen ein, wird die Bank die einzelnen SEPA-Echtzeitüberweisungen unverzüglich herauslösen. Der Zugang der herausgelösten einzelnen SEPA-Echtzeitüberweisung bestimmt sich nach Nummer 1.4 der Überweisungsbedingungen.

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

9 Rückruf

(1) Vor der Autorisierung der Auftragsdaten kann der Kunde die Datei zurückrufen. Änderungen einzelner Auftragsdaten 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 richtet sich nach den dafür geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann außerhalb des DFÜ-Verfahrens oder, wenn mit dem Kunden vereinbart, nach den Vorgaben von Kapitel 11 der Anlage 3 erfolgen. Hierzu hat der Kunde der Bank die Einzelangaben des Originalauftrages mitzuteilen.

10 Ausführung der Aufträge

(1) Die Bank wird die Aufträge ausführen, wenn alle nachfolgenden Ausführungsbedingungen vorliegen:

- Die per DFÜ eingelieferten Auftragsdaten wurden gemäß Nummer 3 Absatz 8 unter Berücksichtigung von Nummer 3 Absatz 9 autorisiert.
- Das festgelegte Datenformat ist eingehalten.
- Das Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart 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 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.

11 Haftung

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

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

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

11.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Nutzung der Legitimations- oder Sicherungsmedien, haftet der Kunde 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 Kunde 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 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 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

Bedingungen für die Datenfernübertragung

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 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. Aufträge können mehrere bankfachlichen EU benötigen, die von unterschiedlichen Nutzern (Kontoinhaber und deren Bevollmächtigte) geleistet werden müssen. Für jede unterstützte Auftragsart 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 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 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 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 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 Teilnehmerschlüssel

Die vom Teilnehmer eingesetzten Schlüsselpaare für die bankfachliche EU, die Verschlüsselung der Auftragsdaten 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.
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 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 an die Bank

Der Nutzer überprüft die Auftragsdaten 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 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, die an das Banksystem übermittelt werden, können wie folgt autorisiert werden:

1. Alle erforderlichen bankfachlichen EU werden zusammen mit den Auftragsdaten übertragen.
2. Sofern mit dem Kunden für die jeweilige Auftragsart die Verteilte Elektronische Unterschrift (VEU) vereinbart wurde und die übermittelten EU für die bankfachliche Freigabe nicht ausreichen, wird der Auftrag bis zur Abgabe aller erforderlichen EU im Banksystem gespeichert.
3. Soweit Kunde und Bank vereinbaren, dass die Autorisierung von per DFÜ übermittelten Auftragsdaten mittels gesondert übermittelten Begleitzettels/Sammelauftrags erfolgen kann, ist an Stelle der bankfachlichen EU des Nutzers eine Transportunterschrift (Typ „T“) für die technische Absicherung der Auftragsdaten 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 gibt. Die Freigabe des Auftrags erfolgt nach erfolgreicher Prüfung der Unterschrift des Nutzers auf dem Begleitzettel/Sammelauftrag durch die Bank.

4.1 Auftragserteilung 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 unabhängig vom Transport der Auftragsdaten und gegebenenfalls auch durch mehrere Teilnehmer erfolgen soll.

Solange noch nicht alle zur Autorisierung erforderlichen bankfachlichen EU vorliegen, kann der Auftrag von einem hierzu berechtigten Nutzer gelöscht werden. Soweit der Auftrag 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 nach Ablauf des von der Bank gesondert mitgeteilten Zeitlimits zu löschen.

4.2 Legitimationsprüfung durch die Bank

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

4.3 Kundenprotokolle

Die Bank dokumentiert in Kundenprotokollen die folgenden Vorgänge:

– Übertragung der Auftragsdaten an das Banksystem.
– Übertragung von Informationsdateien von dem Banksystem an das Kundensystem.
– Ergebnis einer jeden Legitimationsprüfung von Aufträgen des Kunden an das Banksystem.
– Weiterverarbeitung von Aufträgen, sofern sie die Unterschriftsprüfung und die Anzeige von Auftragsdaten 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 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 von diesem Teilnehmer per EBICS-Anbindung mehr erteilt werden.

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

Anlage 3:

Spezifikation der Datenformate

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

Further details of the Bank are contained in the “List of Prices and Services” *(Preis- und Leistungsverzeichnis)*

Terms and Conditions for Remote Data Transmission

The following translation is provided for your convenience only. The original German text “*Bedingungen für Datenfernübertragung*” is binding in all respects. In the event of any divergence between the English and German texts, constructions, meanings or interpretations, those of the German original shall govern exclusively.

1 Scope of services

(1) The Bank shall be at the disposal of customers (account holders) who are not consumers for remote data transmission by electronic means, referred to hereinafter as “remote data transmission” or “RDT”. Remote data transmission comprises the presentation and retrieval of files (particularly transmitting orders and calling up information).

(2) The Bank shall inform customers of the types of services they may use within the scope of remote data transmission. The use of remote data transmission shall be subject to the transaction limits agreed with the Bank.

(3) Remote data transmission shall be possible via the EBICS connection (Annexes 1a – 1c).

(4) The structure of the data sets and files used for transmitting orders and calling up information is described in the Data Format Specification (Annex 3).

2 Users and subscribers, identification and security media

(1) Orders can be placed via the EBICS connection only by the customer or the customer’s authorised representatives. The customer and the authorised representatives are referred to collectively hereinafter as “users” *(Nutzer)*. In order to authorise order data sent by remote data transmission by means of an electronic signature, each user shall require individual identification media activated by the Bank. The identification media requirements are specified in Annex 1a. If agreed with the Bank, order data sent by remote data transmission may be authorised by means of a signed note accompanying it *(Begleitzettel)/* batch order *(Sammelauftrag).*

(2) In addition to authorised representatives, the customer can name “technical subscribers” *(technische Teilnehmer)* for the exchange of data via the EBICS connection. Such technical subscribers shall only be authorised to exchange data. Users and technical subscribers are referred to collectively hereinafter as “subscribers” *(Teilnehmer).* To protect the exchange of data, each subscriber shall require individual security media activated by the Bank. The security media requirements are set out in Annex 1a.

3 Procedural provisions

(1) The data transmission procedure agreed between the customer and the Bank shall be subject to the requirements set out in Annex 1a and in the technical interface documentation (Annex 1b) and the Data Format Specification (Annex 3).

(2) The customer shall be obligated to ensure that all subscribers comply with the RDT procedure and the specifications.

(3) Data field entries shall be governed by the data field entry and control guidelines for the format used in each case (Annex 3).

(4) If the user submits a file containing several SEPA credit transfers or SEPA instant credit transfers, they decide, based on the agreed order type[1], whether verification of the payee shall be conducted in accordance with Section 2.1.3 of the Terms and Conditions for Credit Transfers.

If the customer waives verification of the payee, the Bank shall execute the credit transfers in the file using the unique identifiers provided by the user. In individual cases, this may result in money being credited to a payment account whose holder is not the payee named by the customer.

If the user submits a file containing only a single SEPA credit transfer or SEPA instant credit transfer, the Bank is, independent of the user’s decision, legally obligated to verify the payee.

This paragraph does not apply to order data sent by remote data transmission authorised by means of a signed note accompanying it (*Begleitzettel*)/ batch order (*Sammelauftrag*).

(5) Before transmission of the order data to the Bank, a record of the full contents of the files to be transmitted and of the data transmitted for verification of identification must be made. This record must be kept by the customer for a minimum period of 30 calendar days from the date of execution (for credit transfers) or due date (direct debits) indicated in the file or, where several dates are indicated, from the latest such date. Unless otherwise agreed, it must be demonstrably kept in such a way that it can be made available to the Bank again at short notice on request.

(6) In addition, the customer must produce for each presentation and each retrieval of files an electronic protocol which complies with the provisions of Section 10 of the EBICS Connection Specification (Annex 1b). The customer must hold this protocol on file and make it available to the Bank on request.

(7) If the Bank provides the customer with data concerning payment transactions which have not yet been finally processed, this data shall merely constitute non-binding information. It shall be specifically marked as such in each case.

(8) The order data submitted by remote data transmission must, as agreed with the Bank, be authorised either by an electronic signature or by a signed note accompanying the data *(Begleitzettel)/*batch order *(Sammelauftrag)*. This order data shall become legally effective as an order

a) when submitted with an electronic signature:

- if all necessary user electronic signatures have been received by remote data transmission within the agreed period of time and
- if the electronic signatures can be successfully verified with the agreed keys

or

b) when submitted with an accompanying note *(Begleitzettel)/*batch order *(Sammelauftrag)*:

- if the accompanying note/batch order has been received by the Bank within the agreed period of time and
- if the accompanying note/batch order has been signed in accordance with the account mandate.

(9) If verification of the payee is conducted for a file containing SEPA credit transfers or SEPA instant credit transfers in accordance with Section 3 (4), the bank will inform the user of the results. The user then decides whether

- to approve the file for execution or
- not to approve the file for execution.

By way of derogation from Section 3 (8) sentence 2, the order only takes effect once the user has approved the file in accordance with sentence 2.

4 Obligation to exercise due diligence when handling the identification media for authorising orders

(1) Depending on the transmission procedure agreed with the Bank, the customer shall be obligated to ensure that all users comply with the obligations resulting from these terms and conditions and the identification procedures set out in Annex 1a.

(2) The user may place orders using an identification medium activated by the Bank. The customer shall ensure that each user takes care that no other person obtains possession of their identification medium or gains knowledge of the password protecting it. This is because any other person who is in possession of the medium or a duplicate thereof and knows the corresponding password can misuse the agreed services. In order to protect the identification medium and the password, the following must be observed in particular:

- The identification medium must be protected against unauthorised access and kept in a safe place.
- The password protecting the identification medium must not be noted on the identification medium or kept together with it as a copy or stored unsecured electronically.
- The identification medium must not be duplicated.

[1] Business Transaction and Format (BTF) as of EBICS Version 3.0 is also considered an order type.

© Bank-Verlag GmbH 47.508 (10/25)

— When entering the password, care must be taken to ensure that no other persons can view it.

5 Obligation to exercise due diligence when handling the security media for data exchange

When using the EBICS connection, the customer shall be obligated to ensure that all subscribers comply with the security procedures set out in Annex 1a.

The subscriber shall secure the data exchange using the security media activated by the Bank. The customer shall be obligated to ensure that each subscriber takes care that no other person obtains possession of, or can use, their security medium. Particularly if it is filed in a technical system, the subscriber's security medium must be stored in a technical environment which is protected against unauthorised access. This is because any other person who has access to the security medium or a duplicate thereof may misuse the data exchange.

6 Security of the customer system

The customer shall ensure that the systems they use for remote data transmission are adequately protected. The EBICS security requirements are set out in Annex 1c.

7 Blocking of the identification and security media

(1) If the identification or security media are lost, become known to other persons or misuse of these media is suspected, the subscriber must immediately block their RDT access or arrange for the Bank to block it. Further details are contained in Annex 1a. The subscriber may also send the Bank a blocking request at any time via the separately notified contact data.

(2) Outside the RDT procedure, the customer can arrange for the use of a subscriber's identification and security media or the entire RDT access to be blocked via the blocking facility specified by the Bank.

(3) The Bank shall block the entire RDT access if misuse is suspected. It shall notify the customer thereof outside the RDT procedure. Such blocking cannot be lifted via remote data transmission.

8 Handling of incoming order data by the Bank

(1) The order data delivered to the Bank by remote data transmission shall be processed in the regular course of business.

(2) The Bank shall verify by means of the signatures generated by the subscribers with the security media whether the sender is authorised to exchange data. If this verification reveals any discrepancies, the Bank shall not process the order data concerned and shall notify the customer thereof without delay.

(3) The Bank shall verify the identification of the user(s) and authorisation of the order data delivered by remote data transmission on the basis of either the electronic signatures generated by the users with the identification media or the accompanying note *(Begleitzettel)/* batch order *(Sammelauftrag)* and whether the order data sets comply with the provisions of Annex 3. If this verification reveals any discrepancies, the Bank shall not process the order data in question and shall notify the customer thereof without delay. The Bank may delete any order data that has not been fully authorised after expiry of the time limit separately notified by the Bank.

(4) If the verification of the files or data sets performed by the Bank in accordance with Annex 3 reveals errors, the Bank shall indicate the files or data sets containing errors in appropriate form and notify the user thereof without delay. The Bank may exclude the files or data sets containing errors from further processing if proper execution of the order cannot be ensured.

(5) If the user submits a file containing several SEPA instant credit transfers, the bank will immediately separate it into individual SEPA instant credit transfers. The receipt of the separated SEPA instant credit transfers is determined in accordance with Section 1.4 of the Terms and Conditions for Credit Transfers (*Überweisungsbedingungen*).

(6) The Bank shall be obligated to document the procedures (see Annex 1a) and the forwarding of orders for processing in the customer protocol. The customer shall be obligated to call up the protocol promptly and ascertain the status of order processing. In the event of any discrepancies, the customer shall contact the Bank.

9 Recall/revocation

(1) The customer may recall a file before the order data has been authorised. Individual order data can only be changed by recalling the entire file and placing the order again. The Bank can only accept a recall if the recall reaches it early enough to be taken into account in the regular course of business.

(2) The extent to which an order can be revoked shall be governed by the relevant special terms and conditions (e.g. Terms and Conditions for Credit Transfers). Orders can be revoked outside the RDT procedure or, where agreed with the customer, in accordance with the provisions of Section 11 of Annex 3. For this purpose, the customer must provide the Bank with the individual details of the original orders.

10 Execution of orders

(1) The Bank shall execute orders if all the following conditions for execution have been fulfilled:

— The order data delivered by remote data transmission has been authorised in accordance with Section 3 (8) taking Section 3 (9) into account.
— The specified data format has been complied with.
— The transaction limit has not been exceeded.
— The requirements for execution set out in the special terms and conditions governing the respective order type (e.g. a sufficient credit balance in an account under the Terms and Conditions for Credit Transfers) have been met.

(2) If the conditions for execution under paragraph 1 are not fulfilled, the Bank shall not execute the order and shall notify the customer of the non-execution without delay through the agreed communication channel. Where possible, the Bank shall explain why the order was not executed and indicate how any errors that caused the non-execution can be rectified.

11 Liability

11.1 Liability of the Bank for unauthorised RDT transactions and non-execution, incorrect execution or delayed execution of RDT transactions

The liability of the Bank for unauthorised RDT transactions and non-execution, incorrect execution or delayed execution of RDT transactions shall be governed by the special terms and conditions agreed for the respective order type (e.g. Terms and Conditions for Credit Transfers).

11.2 Liability of the customer for misuse of the identification or security media

11.2.1 Liability of the customer for unauthorised payment transactions before a request to block access

(1) If unauthorised payment transactions conducted before a request to block access are due to the misuse of identification or security media, the customer shall be liable vis-à-vis the Bank for the loss or damage incurred by the Bank if the subscriber has negligently or wilfully breached their obligations to exercise due diligence. Section 675v of the German Civil Code *(Bürgerliches Gesetzbuch [BGB])* shall not apply.

(2) The customer shall not be obligated to provide compensation for loss or damage under paragraph 1 if the subscriber was unable to issue the request to block access under Section 7 (1) because the Bank failed to ensure that it had the means to receive such requests to block access and the loss or damage would in this way have been avoided.

(3) Liability for loss or damage caused within the period of time for which the transaction limit applies shall be limited in each case to the agreed transaction limit.

(4) Paragraphs 2 and 3 shall not apply if the subscriber acted with fraudulent intent.

11.2.2 Liability of the customer for other unauthorised transactions before a request to block access

If unauthorised transactions other than payment transactions conducted before a request to block access are due to the use of a lost or stolen identification or security medium or to any other misuse of the identification or security medium and if the Bank has incurred loss or damage as a result thereof, the customer and the Bank shall be liable in accordance with the statutory principles of contributory negligence.

11.2.3 Liability of the Bank after receipt of a request to block access

As soon as the Bank has received a request to block access from a subscriber, it shall bear any loss or damage incurred thereafter due to unauthorised RDT transactions. This shall not apply if a subscriber has acted with fraudulent intent.

11.3 Preclusion of liability

Claims for compensation shall be precluded if the circumstances substantiating a claim are based on an exceptional and unforeseeable event on which the party referring to this event has no influence and whose consequences could not have been avoided by it even by exercising the required due diligence.

12 Final provisions

The Annexes referred to in these terms and conditions shall form part of the agreement concluded with the customer.

Annex 1a: EBICS Connection
Annex 1b: EBICS Connection Specification
Annex 1c: Security Requirements for the EBICS Customer System
Annex 2: currently blank
Annex 3: Data Format Specification

Terms and Conditions for Remote Data Transmission

Annex 1a:
EBICS Connection

1 Identification and security procedures

The customer (account holder) shall indicate the RDT subscribers and their authorisations to the Bank.

The following identification and security procedures shall be used for the EBICS connection:

- Electronic signatures
- Authentication signature
- Encryption

The subscriber shall possess an individual pair of keys, consisting of a private key and a public key, for each identification and security procedure. The public subscriber keys must be disclosed to the Bank in accordance with the procedure set out in Section 2. The public bank keys must be protected against unauthorised alteration in accordance with the procedure set out in Section 2. The subscriber's key pairs may also be used for communication with other banks.

1.1 Electronic signatures

1.1.1 Electronic signatures of subscribers

The following signature classes shall be defined for the electronic signatures (ESs) of subscribers:

- Single signature (Type "E")
- First signature (Type "A")
- Second signature (Type "B")
- Transport signature (Type "T")

Type "E", "A" or "B" ESs are referred to as "banking ESs". Banking ESs are used to authorise orders. Orders may require several banking ESs which must be provided by different users (account holders and their authorised representatives). For each order type supported, a minimum number of required banking ESs shall be agreed between the Bank and the customer.

Type "T" ESs, which are called "transport signatures", are not used for banking authorisation of orders, but solely for transmitting orders to the bank system. "Technical subscribers" (see Section 2.2) may only be assigned a type "T" ES.

The programme used by the customer can generate different messages (e.g. domestic and international payment orders, but also messages for initialisation, calling up protocols and retrieving account and turnover information, etc.). The Bank shall let the customer know which types of messages can be used and which type of ES must be applied in each case.

1.1.2 Authentication signature

In contrast to the ES, which is used to sign order data, the authentication signature is configured via the individual EBICS message including the control and log-in data and the ES contained therein. With the exception of a few system-determined order types defined in the EBICS Connection Specification, the authentication signature is provided by both the customer system and the bank system in every transaction step. The customer must ensure the use of software which, in accordance with the EBICS Connection Specification (see Annex 1b), verifies the authentication signature of each EBICS message transmitted by the Bank, taking into account the current validity and authenticity of the Bank's stored public keys.

1.1.3 Encryption

In order to ensure the secrecy of the banking data at application level, the order data must be encrypted in accordance with the EBICS Connection Specification (see Annex 1b) by the customer, taking into account the current validity and authenticity of the Bank's stored public keys.

In addition, transport encryption is required on the external transmission routes between the customer and bank systems. The customer must ensure the use of software which, in accordance with the requirements of the EBICS Connection Specification (see Annex 1b), verifies the current validity and authenticity of the server certificates used by the Bank for this purpose.

2 Initialisation of the EBICS connection

2.1 Establishing the communication link

Communication is established using a URL (Uniform Resource Locator). Alternatively, an IP address for the respective Bank may be used. The URL or IP address shall be disclosed to the customer on conclusion of the agreement with the Bank.

To initialise the EBICS connection, the Bank shall provide the following data to the subscribers named by the customer:

- URL or IP address of the Bank
- Name of the Bank
- Host ID
- Permitted version(s) of the EBICS protocol and security procedures
- Partner ID (customer ID)
- User ID
- System ID (for technical subscribers)
- Further specific details of customer and subscriber authorisations.

For the subscribers assigned to the customer, the Bank shall issue a user ID which clearly identifies the subscriber. If one or more technical subscribers are assigned to the customer (multi-user system), the Bank shall issue a system ID in addition to the user ID. If no technical subscriber is specified, the system ID and user ID are identical.

2.2 Initialisation of subscriber keys

The key pairs used by the subscriber for the banking ESs, encryption of the order data and the authentication signature shall, in addition to the general conditions set out in Section 1, comply with the following requirements:

1. The key pairs are assigned exclusively and unambiguously to the subscriber.
2. If the subscriber generates their keys independently, the private keys must be generated by means which the subscriber can keep under their sole control.
3. If the keys are made available by a third party, it must be ensured that the subscriber obtains sole possession of the private keys.
4. As regards the private keys used for identification, each user shall define a password for each key which protects access to the respective private key.
5. As regards the private keys used to protect the data exchange, each subscriber shall define a password for each key which protects access to the respective private key. This password may be dispensed with if the subscriber's security medium is stored in a technical environment which is protected against unauthorised access.

Initialisation of the subscriber by the Bank requires transmission of the subscriber's public keys to the bank system. For this purpose, the subscriber shall transmit their public keys to the Bank via two independent communication channels:

- via EBICS by means of the system-determined order types provided for this purpose.
- via an initialisation letter signed by the account holder or an authorised representative.

For initialisation of the subscriber, the Bank shall verify the authenticity of the public subscriber keys transmitted via EBICS on the basis of the initialisation letters signed by the account holder or an authorised representative.

The initialisation letter shall contain the following data for each public subscriber key:

- Purpose of the public key
- Electronic signature
- Authentication signature
- Encryption
- Version supported by each key pair
- Specification of exponent length
- Hexadecimal representation of the public key's exponent
- Specification of the modulus length
- Hexadecimal representation of the public key's modulus
- Hexadecimal representation of the public key's hash value

The Bank shall verify the signature of the account holder or authorised representative on the initialisation letter and whether the hash values of the subscriber's public key transmitted via EBICS are identical with those transmitted in writing. If verification is positive, the Bank shall activate the relevant subscriber for the agreed order types.

2.3 Initialisation of bank keys

The subscriber shall collect the Bank's public key using a system-determined order type specifically designated for this purpose.

The hash value of the public bank key shall additionally be made available by the Bank via a second communication channel agreed separately with the customer.

Before using EBICS for the first time, the subscriber shall verify the authenticity of the public bank keys sent to them by remote data transmission by comparing their hash values with the hash values notified by the Bank via the separately agreed communication channel.

The customer must ensure use of software which verifies the validity of the server certificates used in transport encryption by means of the certification path notified separately by the Bank.

3 Special due diligence requirements where identification and security media are generated by the customer

Where the customer generates their identification and security media in accordance with the EBICS Connection Specification themself and initialises these with their Bank, they shall ensure the following:

- Confidentiality and integrity of the identification medium are maintained in all phases of authentication, including display, transmission and storage.
- Private subscriber keys on identification and security media are

not stored in clear text.

- The identification medium is blocked as soon as the wrong password has been entered five times in succession.
- Private and public subscriber keys are generated in a secure environment.
- Identification and security media are clearly and uniquely assigned to the subscriber and used.

4 Placing orders with the Bank

The user shall verify the accuracy of the order data and ensure that only this data is signed electronically. When initialising communication, the Bank shall first conduct subscriber-related authorisation verifications, such as order type authorisation or, if applicable, agreed limit verifications. The results of further banking verifications such as limit verifications or account authorisation verifications shall be notified to the customer in the customer protocol at a later date. An exception shall be the online verification of order data by the Bank agreed with the customer on an optional basis.

Order data transmitted to the Bank system may be authorised as follows:

1. All necessary banking ESs are transmitted together with the order data.
2. If a Distributed Electronic Signature *(Verteilte Elektronische Unterschrift [VEU])* has been agreed with the customer for the respective order type and the ESs transmitted are insufficient for banking authorisation, the order is stored in the bank system until all necessary ESs have been submitted.
3. If the customer and the Bank agree that order data delivered by RDT may be authorised by means of a separately transmitted accompanying note *(Begleitzettel)/*batch order *(Sammelauftrag)*, a transport signature (type “T”) must be provided for the technical protection of the order data instead of the user’s banking ES. To this end, the file must bear a special tag indicating that there are no further ESs for this order other than the transport signature (type “T”). The order is authorised once the Bank has successfully verified the user’s signature on the accompanying note *(Begleitzettel)/* batch order *(Sammelauftrag)*.

4.1 Issuing orders by means of the Distributed Electronic Signature (VEU)

The manner in which the Distributed Electronic Signature will be used by the customer must be agreed with the Bank.

The Distributed Electronic Signature shall be used if orders are to be authorised independently of the transport of the order data and, if applicable, by several subscribers.

Until all banking ESs necessary for authorisation are available, the order can be deleted by an authorised user. If the order has been fully authorised, it can only be recalled/revoked in accordance with Section 9 of the Terms and Conditions for Remote Data Transmission.

The Bank may delete orders that have not been fully authorised after expiry of the time limit notified separately by the Bank.

4.2 Verification of identification by the Bank

Order data delivered by remote data transmission shall be executed as an order by the Bank only after the necessary banking ESs or the signed accompanying note *(Begleitzettel)*/batch order *(Sammelauftrag)* have been received and positively verified.

4.3 Customer protocols

The Bank shall document the following in customer protocols:

- Transmission of the order data to the bank system
- Transmission of information files from the bank system to the customer system
- Result of each verification of identification for orders from the customer to the bank system
- Further processing of orders where these concern signature verification and the display of order data.

The subscriber shall consult the result of the verifications carried out by the Bank by promptly calling up the customer protocol.

The subscriber shall file this protocol, the contents of which shall comply with the provisions of Section 10 of Annex 1b, in its records and make it available to the Bank on request.

5 Change of subscriber keys with automatic activation

If the identification and security media used by the subscriber are valid for a limited period of time, the subscriber must transmit the new public subscriber keys to the Bank promptly before the expiry date. After the expiry date of the old keys has passed, a new initialisation must be performed.

If the subscriber generates their keys personally, they must renew the subscriber keys using the system–determined order types provided for this purpose and transmit them promptly before expiry of the old keys.

To automatically activate new keys without renewed subscriber initialisation, the following order types shall be used:

- update of the public banking key (PUB) and
- update of the public authentication key and the public encryption key (HCA)

or alternatively

- update of all three above keys (HCS).

The order types PUB and HCA or HCS must be provided with a valid user banking ES for this purpose. After the keys have been successfully changed, only the new keys may be used.

If the electronic signature could not be positively verified, the procedure specified in Section 8 (3) of the Terms and Conditions for Remote Data Transmission shall apply.

The key may be changed only after all orders have been fully processed. Otherwise, any orders not yet executed must be placed again using the new key.

6 Blocking of subscriber keys

If misuse of the subscriber keys is suspected, the subscriber shall be obligated to block their access authorisation for all bank systems using the compromised key(s).

If the subscriber is in possession of valid identification and security media, they can block their access authorisation via EBICS. By sending a message with an “SPR” order type, access will be blocked for the subscriber whose user ID was used to send the message. After blocking, no further orders can be placed by this subscriber via EBICS until the re-initialisation referred to in Section 2 has been carried out.

If the subscriber is no longer in possession of valid identification and security media, they can request blocking of the identification and security media outside the RDT procedure via the blocking facility notified separately by the Bank.

The customer may request blocking of a subscriber’s identification and security media or the entire remote data transmission access outside the RDT procedure via the blocking facility notified by the Bank.

Annex 1b:
EBICS Connection Specification

The specification is available at www.ebics.de.

Annex 1c:
Security Requirements for the EBICS Customer System

In addition to the security measures set out in Annex 1a (6), the customer must comply with the following requirements:

- The software used by the customer for the EBICS procedure must meet the requirements set out in Annex 1a.
- EBICS customer systems may not be used without a firewall. A firewall is an application which monitors all incoming and outgoing messages and allows only known or authorised connections.
- A virus scanner must be installed and regularly updated with the latest virus definition files.
- The EBICS customer system should be configured in such a way that subscribers must log in before using it. They should log in as a normal user and not as an administrator who is authorised, for example, to carry out programme installations.
- The internal IT communication channels for unencrypted banking data or for unencrypted EBICS messages must be protected against interception and manipulation.
- If security-related updates are available for the operating system in use and for other security-related software programmes that have been installed, they should be used to update the EBICS customer systems.

The customer shall be exclusively responsible for compliance with these requirements.

Annex 2:

currently blank.

Annex 3:
Data Format Specification

The specification is available at www.ebics.de.