COMMERZBANK

Bedingungen für die Datenfernübertragung der Zweigniederlassung Zürich

Stand 02. August 2011

1. Leistungsumfang

(1) Die Bank steht ihrem Kunden (Kontoinhaber), der kein Konsument ist, für die Datenfernübertragung auf elektronischem Wege – nachfolgend „Datenfernübertragung" oder „DFÜ" genannt – zur Verfügung. Die Datenfernübertragung umfasst die Auftragserteilung sowie den Datenaustausch (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 verschiedene Verfahren möglich, insbesondere über die EBICS-Anbindung (Anlage 1a bis 1c). Das massgebliche Übertragungsverfahren wird zwischen Kunde und Bank vereinbart.

(4) Der Satz- und Dateiaufbau für die Übermittlung von Aufträgen und den Informationsabruf wird in der Spezifikation der Datenformate (Anlage 2) beschrieben oder gesondert vereinbart.

2. Nutzer und Teilnehmer, Legitimations- und Sicherungsmedien

(1) Aufträge können nur vom Kunden oder seinen Kontobevollmächtigten erteilt werden. Kunde und Kontobevollmächtigte werden im Folgenden einheitlich als „Nutzer" bezeichnet. Zur Erteilung von Aufträgen an die Bank 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 autorisiert werden.

(2) Für den Datenaustausch über die EBICS-Anbindung kann der Kunde zusätzlich zu den Bevollmächtigten „Technische Teilnehmer" benennen, bei denen es sich um natürliche Personen handeln muss und 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) Legitimations- und Sicherungsmedien sind Authentifizierungsinstrumente im Sinne von § 1 Absatz 5 des deutschen Zahlungsdiensteaufsichtsgesetzes.

3. Verfahrensbestimmungen

(1) Für das zwischen Kunde und Bank vereinbarte Übertragungsverfahren gelten jeweils die in Anlage 1a sowie die in der Dokumentation der technischen Schnittstellen (Anlage 1b) und der Spezifikation der Datenformate (Anlage 2) beschriebenen Anforderungen.

(2) Der Kunde ist verpflichtet sicherzustellen, dass alle Teilnehmer die mit der Bank vereinbarten Verfahren und Spezifikationen beachten.

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

Die Angaben im Verwendungszweck haben sich ausschliesslich auf den jeweiligen Zahlungsverkehrsvorgang im Datensatz zu beziehen. Am Anfang des Datenfeldes „Verwendungszweck" sind linksbündig solche Angaben unterzubringen, auf die der Begünstigte/Zahlungspflichtige maschinell zuzugreifen beabsichtigt oder die der Überweisende/Zahlungsempfänger benötigt, falls die Zahlung als unanbringlich beziehungsweise unbezahlt an ihn zurückgeleitet wird.

Die Belegung der Verwendungszweckangaben darf ausserdem vom Nutzer nicht für die Vorgabe eines von ihm gewünschten Druckbildes benutzt werden, ohne dass die Stellenkapazität im Datenfeld „Verwendungszweck" des Datensatzes sowie in den etwaigen nachfolgenden Erweiterungsteilen mit Verwendungszweckangaben voll ausgenutzt ist.

Verwendungszweckangaben dürfen nicht die Übermittlung einer gesonderten Nachricht ausserhalb des Zahlungsverkehrs (z. B. Rechnung, Lohn- und Gehaltsabrechnung) ersetzen. Werbetexte dürfen in den Verwendungszweckangaben nicht enthalten sein.

(4) Der Nutzer hat den Bankidentifikationscode (Bankleitzahl oder BIC) des Zahlungsdienstleisters des Zahlungsempfängers beziehungsweise des Zahlungs-

dienstleisters des Zahlers (Zahlstelle) sowie den Kontoidentifikationscode (Kontonummer oder IBAN) des Zahlungsempfängers beziehungsweise Zahlers zutreffend anzugeben. Die in die Abwicklung des Zahlungsauftrages eingeschalteten Zahlungsdienstleister sind berechtigt, die Bearbeitung ausschliesslich anhand von Bank- und Kontoidentifikationscode vorzunehmen. Fehlerhafte Angaben können Fehlleitungen des Zahlungsverkehrsauftrags zur Folge haben. Schäden und Nachteile, die hieraus entstehen, gehen zu Lasten des Kunden. Die Regelung gilt entsprechend, wenn per Datenfernübertragung andere Aufträge (keine Zahlungsaufträge) übermittelt werden.

(5) Vor 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 vom Kunden mindestens für einen Zeitraum von 15 Kalendertagen bei Inlandszahlungsaufträgen und 30 Kalendertagen bei Auslandszahlungsaufträgen ab dem Ausführungstag 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 jeden Datenaustausch 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 eingelieferten Auftragsdaten sind, wie mit der Bank vereinbart, entweder mit elektronischer Unterschrift oder mittels unterschriebenen Begleitzettel 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

b) bei Einreichung mit Begleitzettel, wenn
- der Begleitzettel im vereinbarten Zeitraum bei der Bank eingeht

und
- der Begleitzettel der Kontovollmacht entsprechend unterzeichnet worden ist.

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 in Anlage 1a beschriebenen Legitimationsverfahren einhalten.

(2) Mit Hilfe der von der Bank freigeschalteten Legitimationsmedien 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 oder 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 zur Geheimhaltung der Legitimationsmedien zu beachten:
- Die den Nutzer legitimierenden Daten dürfen nicht ausserhalb des Legitimationsmediums, z. B. auf der Festplatte des Rechners, gespeichert werden;
- das Legitimationsmedium ist nach Beendigung der DFÜ-Nutzung sicher zu verwahren;
- das zum Schutz des Legitimationsmediums dienende Passwort darf nicht notiert oder elektronisch abgespeichert 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. 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 sperren zu lassen. Näheres regelt Anlage 1a. Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

(2) Wird dreimal in Folge versucht, einen Auftrag mit einem falschen Legitimationsmedium an die Bank zu übermitteln oder mit einem falschen Sicherungsmedium den Datenaustausch durchzuführen, so sperrt die Bank den DFÜ-Zugang des betreffenden Teilnehmers. Diese Sperre kann mittels DFÜ nicht aufgehoben werden. Zur Aufhebung dieser Sperre muss sich der Kunde mit seiner Bank in Verbindung setzen.

(3) 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.

(4) Die Bank wird den gesamten DFÜ-Zugang sperren, wenn der Verdacht einer missbräuchlichen Nutzung des DFÜ-Zugangs besteht. Sie wird den Kunden hierüber und über die Gründe hierfür ausserhalb des DFÜ-Verfahrens informieren. Diese Sperre kann mittels DFÜ nicht aufgehoben werden.

7. Behandlung eingehender Auftragsdaten durch die Bank

(1) Die der Bank im DFÜ-Verfahren übermittelten Auftragsdaten werden im Rahmen des ordnungsgemässen Arbeitsablaufes bearbeitet. Kann die Bank eine vom Kunden im Format „SEPA-Überweisung“ beleglos erteilte Überweisung nicht in diesem Format ausführen, weil der vom Kunden angegebene Zahlungsdienstleister des Zahlungsempfängers dieses Format noch nicht unterstützt, und weist die Bank die Überweisung nicht zurück, führt sie die Überweisung in einem von dem Zahlungsdienstleister des Zahlungsempfängers unterstützten Format aus. Bei diesem Formatwechsel können die in der Anlage 3 genannten Datenelemente – oder Teile davon – nicht übermittelt werden.

(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 den betreffenden Auftrag 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 sowie die Übereinstimmung der Auftragsdatensätze mit den Bestimmungen gemäss Anlage 2. 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 2 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) Die Bank ist verpflichtet, die vorstehenden Abläufe und die Weiterleitung der Aufträge zur Bearbeitung im Kundenprotokoll (siehe Anlage 1a) 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.

8. Rückruf

(1) Vor der Autorisierung der Auftragsdaten kann der Kunde die Datei zurückrufen. Änderungen einzelner Auftragsdaten sind nur durch Rückruf der gesamten Datei und erneuter 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 der Zweigniederlassung Zürich (z. B. Firmenkundenbedingungen für Zahlungsdienste). Der Widerruf von Aufträgen kann nur ausserhalb des DFÜ-Verfahrens erfolgen. Hierzu hat der Kunde der Bank die Einzelangaben des Originalauftrages mitzuteilen.

9. 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 autorisiert.
- Das festgelegte Datenformat ist eingehalten.
- Das Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart massgeblichen Sonderbedingungen liegen vor.
- Die Ausführung darf nicht gegen sonstige Rechtsvorschriften verstossen.

(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. Dies gilt nicht, wenn die Angabe von Gründen gegen sonstige Rechtsvorschriften verstösst.

10. 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.

11. Haftung

11.1 Haftung der Bank bei nicht autorisierten Aufträgen und nicht oder fehlerhaft ausgeführten Aufträgen

Die Haftung der Bank bei nicht autorisierten Aufträgen und nicht oder fehlerhaft ausgeführten Aufträgen richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen der Zweigniederlassung Zürich (z. B. Firmenkundenbedingungen für Zahlungsdienste).

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) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen, sonst abhanden gekommenen oder auf der sonstigen missbräuchlichen Nutzung eines Legitimations- oder Sicherungsmediums, haftet der Kunde für den der Bank hierdurch entstehenden Schaden, wenn den Teilnehmer an dem Verlust, Diebstahl, sonstigen Abhandenkommen oder der sonstigen missbräuchlichen Nutzung seines Legitimations- oder Sicherungsmediums ein Verschulden trifft. Der Kunde haftet auch, wenn er einen von ihm benannten Teilnehmer nicht sorgfältig ausgesucht und/oder die Beachtung der Verpflichtungen des Teilnehmers nach diesen Bedingungen nicht regelmässig überprüft hat. Hat die Bank durch ein schuldhaftes Verhalten zu der Entstehung eines Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang Kunde und Bank den Schaden zu tragen haben.

(2) Der Kunde ist nicht zum Ersatz des Schadens nach Absätzen 1 und 2 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 6 Absatz 1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

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

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, gestohlenen oder sonst abhandengekommenen oder auf der sonstigen missbräuchlichen Nutzung eines Legitimations- oder Sicherungsmediums, haftet der Kunde für den der Bank hierdurch entstehenden Schaden, wenn den Teilnehmer an dem Verlust, Diebstahl, sonstigen Abhandenkommen oder der sonstigen missbräuchlichen Nutzung seines Legitimations- oder Sicherungsmediums ein Verschulden trifft. Der Kunde haftet auch, wenn er einen von ihm benannten Teilnehmer nicht sorgfältig ausgesucht und/oder die Beachtung der Verpflichtungen des Teilnehmers nach diesen Bedingungen nicht regelmässig überprüft hat. Hat die Bank durch ein schuldhaftes Verhalten zu der Entstehung eines Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang Kunde und Bank den Schaden zu tragen haben.

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 Aufträge entstehenden Schäden. Dies gilt nicht, wenn ein Teilnehmer in betrügerischer Absicht gehandelt hat.

12. Schlussbestimmungen

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

Anlagen:
Anlage 1a: EBICS·Anbindung
Anlage 1b: Spezifikation der EBICS-Anbindung
Anlage 1c: Sicherheitsanforderungen an das EBICS-Kundensystem
Anlage 2: Spezifikation der Datenformate
Anlage 3: Weiterleitung von Daten bei Formatwechsel

Anlage 1a: EBICS-Anbindung

1. Legitimations- und Sicherungsverfahren

Der Kunde (Kontoinhaber) benennt dem Kreditinstitut 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 dem Kreditinstitut 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 Kreditinstituten 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 bankfachliche EU benötigen, die von unterschiedlichen Nutzern (Kontoinhaber und deren Bevollmächtigte) geleistet werden müssen. Für jede unterstützte Auftragsart wird zwischen Kreditinstitut 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 das Banksystem.
„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. Das Kreditinstitut teilt dem Kunden mit, welche Nachrichtenarten genutzt werden können und welcher EU-Typ hierfür anzuwenden ist.

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 definierten systembedingten 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 dem Kreditinstitut übermittelten EBICS-Nachricht unter Berücksichtigung der Aktualität und Authentizität der gespeicherten öffentlichen Schlüssel des Kreditinstituts gemäss den Vorgaben der EBICS-Spezifikation (siehe Anlage „Spezifikation der EBICS-Anbindung“) prüft.

1.3 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 des Kreditinstituts gemäss den Vorgaben der EBICS-Spezifikation (siehe Anlage „Spezifikation der EBICS-Anbindung“) 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 „Spezifikation der EBICS-Anbindung“) Aktualität und Authentizität der hierfür eingesetzten Serverzertifikate des Kreditinstituts 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 des jeweiligen Kreditinstituts benutzt werden. Die URL oder die IP-Adresse werden dem Kunden bei Vertragsabschluss mit dem Kreditinstitut mitgeteilt.
Das Kreditinstitut teilt den vom Kunden benannten Teilnehmern zur Aufnahme der EBICS-Anbindung folgende Daten mit:

- URL oder IP-Adresse des Kreditinstitutes
- Bezeichnung des Kreditinstitutes

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

2.2 Initialisierung der Schlüssel

2.2.1 Neuinitialisierung 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 beim Kreditinstitut ist die Übermittlung der öffentlichen Schlüssel des Teilnehmers an das Banksystem erforderlich. Hierfür übermittelt der Teilnehmer dem Kreditinstitut 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 das Kreditinstitut 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

Das Kreditinstitut prüft die Unterschrift des Kontoinhabers bzw. 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 das Kreditinstitut den betreffenden Teilnehmer für die vereinbarten Auftragsarten frei.

2.2.2 Migration von FTAM nach EBICS

Soweit der Teilnehmer aufgrund seines vorhandenen DFÜ-Zugangs für FTAM bereits über einen gültigen, vom Kreditinstitut freigeschalteten bankfachlichen Schlüssel verfügt, können im Zuge der gesondert vereinbarten Migration von FTAM nach EBICS vorhandene bankfachliche Schlüssel beibehalten werden, soweit diese mindestens der Version A004 entsprechen und dies so mit dem Kreditinstitut vereinbart ist.

In diesem Fall werden die öffentlichen Schlüssel für die Authentifikation und die Verschlüsselung mit den hierfür vorgesehenen Auftragsarten an das Kreditinstitut übermittelt. Diese Nachrichten sind mit dem Schlüssel für die bankfachliche EU zu unterschreiben. Ein separater Versand eines unterschriebenen Initialisierungsbriefes entfällt.

2.3 Initialisierung der bankseitigen Schlüssel

Der Teilnehmer holt den öffentlichen Schlüssel des Kreditinstituts mittels einer eigens dafür vorgesehenen systembedingten Auftragsart ab.

Der Hashwert des öffentlichen Bankschlüssels wird von dem Kreditinstitut 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 dem Kreditinstitut 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 vom Kreditinstitut gesondert mitgeteilten Zertifizierungpfades überprüft.

3. Auftragserteilung an das Kreditinstitut

Der Nutzer überprüft die Auftragsdaten auf ihre Richtigkeit und stellt sicher, dass genau diese Daten elektronisch unterschrieben werden. Bei Aufnahme der Kommunikation werden seitens des Kreditinstitutes zuerst teilnehmerbezogene Berechtigungsprüfungen durchgeführt, wie etwa die Auftragsartberechtigung oder ggf. vereinbarte Limitprüfungen. Die Ergebnisse weiterer bankfachlicher Prüfungen wie beispielsweise Limitprüfungen oder Kontoberechtigungsprüfungen werden dem Kunden im Kundenprotokoll zu einem späteren Zeitpunkt mitgeteilt. Eine Ausnahme bildet die mit dem Kunden optional vereinbarte Onlineprüfung der Auftragsdaten durch das Kreditinstitut.

Aufträge, 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 Kreditinstitut vereinbaren, dass die Autorisierung von Aufträgen mittels gesondert übermittelten Begleitzettels 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 durch das Kreditinstitut.

3.1 Auftragserteilung mittels Verteilter Elektronischer Unterschrift (VEU)

Die Art und Weise, wie die Verteilte Elektronische Unterschrift (VEU) durch den Kunden genutzt wird, muss mit dem Kreditinstitut vereinbart werden.

Die Verteilte Elektronische Unterschrift ist dann einzusetzen, wenn die Autorisierung von Aufträgen unabhängig vom Transport der Auftragsdaten und ggf. 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 Abschnitt VIII der Bedingungen für Datenfernübertragung möglich.

Das Kreditinstitut ist dazu berechtigt, nicht vollständig autorisierte Aufträge nach Ablauf des vom Kreditinstitut gesondert mitgeteilten Zeitlimits zu löschen.

3.2 Legitimationsprüfung durch das Kreditinstitut

Ein empfangener Auftrag wird durch das Kreditinstitut erst dann ausgeführt, wenn die erforderlichen bankfachlichen EU beziehungsweise der unterschriebene Begleitzettel eingegangen sind/ist und mit positivem Ergebnis geprüft wurden/wurde.

3.3 Kundenprotokolle

Das Kreditinstitut dokumentiert in Kundenprotokollen die folgenden Vorgänge:

- Übertragung der Auftragsdaten an das Banksystem
- Übertragung von Informationsdateien vom Banksystem an das Kundensystem
- Ergebnis einer jeden Legitimationsprüfung von Aufträgen des Kunden an das Banksystem
- Weiterverarbeitung von Aufträgen, sofern sie die Unterschriftsprüfung, die Anzeige von Auftragsdaten betreffen
- Fehler bei der Dekomprimierung

Der Teilnehmer hat sich durch Abruf des Kundenprotokolls über das Ergebnis der aufseiten des Kreditinstituts durchgeführten Prüfungen zu informieren.
Der Teilnehmer hat dieses Protokoll, das inhaltlich den Bestimmungen von Kapitel 10 der Anlage „Spezifikation der EBICS-Anbindung“ entspricht, zu seinen Unterlagen zu nehmen und auf Anforderung des Kreditinstitutes zur Verfügung zu stellen.

4. Änderung der Teilnehmerschlüssel mit automatischer Freischaltung

Wenn die vom Teilnehmer eingesetzten Legitimations- und Sicherungsmedien in ihrer Gültigkeit zeitlich begrenzt sind, hat der Teilnehmer seinem Kreditinstitut 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 dem Kreditinstitut 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)

Die Auftragsarten PUB und HCA 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 VI (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.

5. 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 vom Kreditinstitut 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 vom Kreditinstitut bekannt gegebene Sperrfazilität sperren lassen.

Anlage 1b: Spezifikation der EBICS-Anbindung

Die Spezifikation ist auf der Webseite http://www.ebics.de veröffentlicht.

Anlage 1c: Sicherheitsanforderungen an das EBICS-Kundensystem

Über die in den „Bedingungen für die Datenfernübertragung – EBICS – Anbindung“, Nr. 5 beschriebenen Sicherheitsmassnahmen hinaus sind durch den Kunden folgende Anforderungen zu berücksichtigen:
Die vom Kunden für das EBICS-Verfahren eingesetzte Software muss die in Anlage „EBICS-Anbindung“ 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 deren 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: Spezifikation der Datenformate

Die Datenformate sind auf der Webseite www.commerzbank.de/vertragsbedingungen_firmenkunden veröffentlicht.

Anlage 3: Weiterleitung von Daten bei Formatwechsel

Kann die Bank eine vom Kunden im Format „SEPA-Überweisung“ beleglos erteilte Überweisung nicht in diesem Format ausführen, weil das vom Kunden angegebene Kreditinstitut des Begünstigten dieses Format noch nicht unterstützt, führt sie die Überweisung in einem vom Kreditinstitut des Begünstigten unterstützten Format aus.
Die folgenden Listen gelten nur bei Anwendung der „Translation Rules MX pacs.008.001.01 to MT 103“ vom Juni 2007

1. Bei dem Formatwechsel können die folgenden Datenelemente nicht übermittelt werden:
   - Abweichender Begünstigter
     (Payment Information, > Credit Transfer Transaction Information, > Ultimate Creditor)
   - Abweichender Überweisender
     (Payment Information, > Ultimate Debtor und Payment Information, > Credit Transfer Transaction Information, > Ultimate Debtor)
   - Identifikation des Begünstigten
     (Payment Information, > Credit Transfer Transaction Information, > Creditor, > Identification)
   - Identifikation des Überweisenden
     (Payment Information, > Debtor, > Identification)
2. Bei dem Formatwechsel können die folgenden Datenelemente nur teilweise übermittelt werden:
   - Adresse des Begünstigten [die ersten 66 der 140 ursprünglich möglichen Zeichen werden übermittelt]
     (Payment Information, > Credit Transfer Transaction Information, > Creditor, > Postal Adress)
   - Adresse des Überweisenden [die ersten 66 der 140 ursprünglich möglichen Zeichen werden übermittelt]
     (Payment Information, > Debtor, > Postal Addres)
   - Name des Begünstigten (die ersten 66 der 10 ursprünglich möglichen Zeichen werden übermittelt]
     (Payment Information, > Credit Transfer Transaction Information, > Creditor, > Name)
   - Name des Überweisenden [die ersten 66 der 70 ursprünglich möglichen Zeichen werden übermittelt)
     (Payment Information, > Debtor, > Name)
   - Verwendungszweck [Kundenreferenz und Verwendungszweck werden gemeinsam übermittelt, aber zusammen nicht mehr als 13 Zeichen. Die Kundenreferenz (End to End Identification) wird dabei vorangestellt und ist immer vollständig angegeben.]
   - (Payment Information, > Credit Transfer Transaction Information, > Rernittance Information)