Bedingungen für die Datenfernübertragung (DFÜ)

Fassung Oktober 2024

1. Leistungsumfang

1.1. Die BKS Bank AG (nachfolgend BKS Bank) stellt ihrem Kunden (Kontoinhaber), der kein Verbraucher ist, 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).

1.2. Die BKS Bank gibt dem Kunden die Dienstleistungsarten bekannt, die er im Rahmen der Datenfernübertragung nutzen kann. Zur Nutzung der Datenfernübertragung gelten die mit der BKS Bank vereinbarten Verfügungslimits.

1.3. Die Datenfernübertragung ist über die EBICS-Anbindung (Anlagen 1a bis 1c) möglich. Das maßgebliche Übertragungsverfahren EBICS wird zwischen Kunde und BKS Bank vereinbart.

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

1.5. Zusätzlich zu den vereinbarten Diensten kann der Kunde auch die BKS Business App nutzen. Diese Bestimmungen gelten ausdrücklich auch für die BKS Business App. Technische Voraussetzungen für die BKS Business App und die im Rahmen der BKS Business App verfügbaren Dienstleistungen sind auf der BKS Bank Website unter https://www.bizznetpro.at/fip/gsp/about-mobiletoken?siteName=bks#!/?siteName=bks aufgelistet.

2. Nutzer und Teilnehmer, Legitimations- und Sicherungsmedien

2.1. 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 BKS Bank freigeschaltete Legitimationsmedien. Die Anforderungen an die Legitimationsmedien sind in Anlage 1a definiert.

2.2. 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 BKS Bank freigeschaltete Sicherungsverfahren. Die Anforderungen an die Sicherungsverfahren sind in Anlage 1a beschrieben.

3. Verfahrensbestimmungen

3.1. Für das zwischen Kunde und BKS 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.

3.2. Der Kunde ist verpflichtet sicherzustellen, dass alle Teilnehmer die mit der BKS Bank vereinbarten Verfahren und Spezifikationen beachten.

3.3. 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.

3.4. Der Nutzer hat die Kundenkennung des Zahlungsempfängers beziehungsweise des Zahlers gemäß den vorliegenden Bedingungen anzugeben. Die in die Abwicklung des Zahlungsauftrages eingeschalteten Zahlungsdienstleister sind berechtigt, die Bearbeitung ausschließlich anhand der Kundenkennung vorzunehmen. Fehlerhafte Angaben können Fehlleitungen des Auftrags zur Folge haben. Schäden und Nachteile, die hieraus entstehen, gehen zu Lasten des Kunden.

3.5. Vor der Übertragung von Auftragsdaten an die BKS 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 14 Kalendertagen bei Inlandszahlungsaufträgen und 30 Kalendertagen bei Auslandszahlungsaufträgen 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 BKS Bank kurzfristig erneut zur Verfügung gestellt werden kann, sofern nichts Abweichendes vereinbart wird.

3.6. 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 BKS Bank zur Verfügung zu stellen.

3.7. Soweit die BKS 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.

3.8. Die per DFÜ eingelieferten Auftragsdaten sind wie mit der BKS Bank vereinbart entweder mit Elektronischer Unterschrift oder dem unterschriebenen Begleitzettel/Sammelauftrag zu autorisieren. Diese Auftragsdaten werden als Auftrag wirksam 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

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

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

4.2. Mit Hilfe der von der BKS 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, 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 zur Geheimhaltung der Legitimationsmedien 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 BKS 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 Duplikates 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

7.1. 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 BKS Bank zu sperren oder sperren zu lassen. Näheres regelt Anlage 1a. Der Teilnehmer kann der BKS Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

7.2. Wird drei Mal hintereinander versucht, einen Auftrag mit einem falschen Legitimationsmedium an die BKS Bank zu übermitteln oder mit einem falschen Sicherungsmedium den Datenaustausch durchzuführen, so sperrt die BKS 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 BKS Bank in Verbindung setzen.

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

Über die BizzNet Pro Hotline kann die Sperre an Geschäftstagen in der Zeit von 08-16 Uhr

- ✓ telefonisch: +43 (0)463/ 5858 – 837
- ✓ per Mail: bizznetpro@bks.at

mit Angabe der Kontonummer beauftragt werden. Als Geschäftstag gilt jeder Tag, an dem die BKS Bank den für die Ausführung von Zahlungsaufträgen erforderlichen Geschäftsbetrieb unterhält.

Die Aufhebung der Sperre muss vom Verfüger schriftlich oder persönlich bei der kontoführenden BKS Bank Filiale beantragt werden, oder telefonisch unter obiger Telefonnummer, wobei sich der Verfüger entsprechend zu legitimieren hat.

Die BizzNet Pro Hotline steht auch für Sicherheitsfragen im Zusammenhang mit Zahlungsdiensten zur Verfügung.

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

8. Behandlung eingehender Auftragsdaten durch die BKS Bank

8.1. Die der BKS Bank per DFÜ-Verfahren übermittelten Auftragsdaten werden im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeitet. Kann die BKS 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 BKS Bank die Überweisung nicht zurück, führt sie die Überweisung in einem von dem Zahlungsdienstleister des Zahlungsempfängers unterstützten Format aus.

8.2. Die BKS Bank prüft anhand der von den Teilnehmern mittels der Sicherungsmedien erstellten Signaturen, ob der Absender berechtigt ist, den Datenaustausch durchzuführen.

8.3. Die BKS 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 2. Ergibt die Prüfung Unstimmigkeiten, wird die BKS Bank die betreffenden Auftragsdaten nicht bearbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen. Die BKS Bank ist berechtigt, nicht vollständig autorisierte Auftragsdaten nach Ablauf des von der BKS Bank gesondert mitgeteilten Zeitlimits zu löschen.

8.4. Ergeben sich bei den von der BKS Bank durchgeführten Prüfungen der Dateien oder Datensätze nach Anlage 2 Fehler, so wird die BKS Bank die fehlerhaften Dateien oder Datensätze in geeigneter Form nachweisen und sie dem Nutzer unverzüglich mitteilen. Die BKS Bank ist berechtigt, die fehlerhaften Dateien oder Datensätze von der weiteren Bearbeitung auszuschließen, wenn die ordnungsgemäße Ausführung des Auftrages nicht sichergestellt werden kann.

8.5. Die BKS Bank ist verpflichtet, die vorstehenden Abläufe und die Weiterleitung der Aufträge zur Bearbeitung im Kundenprotokoll (siehe Anlage 1a, Punkt 5.3.) 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 BKS Bank in Verbindung setzen.

9. Rückruf

9.1. 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 BKS Bank kann einen Rückruf nur beachten, wenn ihr dieser so rechtzeitig zugeht, dass seine Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufes möglich ist.

9.2. Die Widerrufbarkeit eines Auftrags richtet sich nach den dafür geltenden Bedingungen. Der Widerruf von Aufträgen kann nur außerhalb des DFÜ-Verfahrens oder, wenn mit dem Kunden vereinbart, nach den Vorgaben von Kapitel 11 der Anlage 2 erfolgen. Hierzu hat der Kunde der BKS Bank die Einzelangaben des Originalauftrages mitzuteilen.

10. Ausführung der Aufträge

10.1. Die BKS Bank wird die Aufträge ausführen, wenn alle nachfolgenden Ausführungsbedingungen vorliegen:

- ✓ die per DFÜ eingelieferten Auftragsdaten wurden autorisiert
- ✓ das festgelegte Datenformat ist eingehalten
- ✓ das Verfügungslimit wurde nicht überschritten
- ✓ die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Bedingungen liegen vor.

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

11. Haftung

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

Die Haftung der BKS 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 Bedingungen. § 80 Zahlungsdienstegesetz ist nicht anwendbar.

Haftung des Kunden bei missbräuchlicher Nutzung der Legitimations- oder Sicherungsmedien

11.1. 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 BKS Bank für die ihr dadurch entstehenden Schäden, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Verhaltens- und Sorgfaltspflichten verstoßen hat. § 68 Zahlungsdienstegesetz ist nicht anwendbar.

(2) Der Kunde ist nicht zum Ersatz des Schadens verpflichtet, wenn der Teilnehmer die Sperranzeige nicht abgeben konnte, weil die BKS Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch vermieden worden wäre. Das gilt unter der Bedingung, dass dem Kunden eine Sperre nach Punkt 7.2. nicht möglich ist.

(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. 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 BKS Bank hierdurch ein Schaden entstanden, haften der Kunden und die BKS Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

11.3. Haftung der BKS Bank ab der Sperranzeige

Sobald die BKS 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.

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.

Änderungen dieser Bedingungen samt Anlagen und dem Kunden spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Inkrafttretens schriftlich bekannt gegeben. Die Zustimmung des Kunden gilt als erteilt, wenn bei der BKS Bank vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens kein Widerspruch des Kunden einlangt. Darauf wird die BKS Bank den Kunden im Änderungsangebot hinweisen.

Anlage 1a: EBICS-Anbindung
Anlage 1b: Spezifikation der EBICS-Anbindung
Anlage 1c: Sicherheitsanforderungen an das EBICS-Kundensystem
Anlage 2: Spezifikation der Datenformate
Anlage 3: Schnittzeiten der BKS Bank

Anlage 1a: EBICS-Anbindung

1. Legitimations- und Sicherungsverfahren

Der Kunde (Kontoinhaber) benennt der BKS 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 BKS Bank gemäß dem im Punkt 2. der „Bedingungen für die Datenfernübertragung“ beschriebenen Verfahren mitzuteilen. Die öffentlichen BKS Bankschlüssel sind auch gemäß dem im Punkt 2. der „Bedingungen für die Datenfernübertragung“ beschriebenen Verfahren gegen unautorisiertes Verändern zu schützen. Die Schlüsselpaare des Teilnehmers können auch für die Kommunikation mit anderen Banken eingesetzt werden.

In BizzNet Pro wird mittels elektronischer Unterschrift autorisiert.

2. Elektronische Unterschriften

2.1. 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")

2.2. 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 der BKS Bank übermittelten EBICS-Nachricht unter Berücksichtigung der Aktualität und Authentizität der gespeicherten öffentlichen

Schlüssel der BKS Bank gemäß den Vorgaben der EBICS-Spezifikation (siehe Anlage 1b) prüft.

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 BKS 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 das Banksystem. "Technische Teilnehmer" (siehe Punkt 2.1) 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 BKS Bank teilt dem Kunden mit, welche Nachrichtenarten genutzt werden können und welcher EU-Typ hierfür anzuwenden ist.

2.3. 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 der BKS Bank gemäß den Vorgaben der EBICS-Spezifikation (siehe Anlage 1b) zu verschlüsseln.

3. Initialisierung der Schlüssel

3.1. Neuinitialisierung der Teilnehmerschlüssel

Die vom Teilnehmer eingesetzten Schlüsselpaare für die Bankfachliche EU, die Verschlüsselung der Auftragsdaten und die Authentifikationssignatur müssen zusätzlich zu den in Punkt 1 beschriebenen allgemeinen Bedingungen den nachfolgenden Anforderungen genügen:

- ✓ Die Schlüsselpaare sind ausschließlich und eindeutig dem Teilnehmer zugeordnet.
- ✓ Soweit der Teilnehmer seine Schlüssel eigenständig generiert, sind die privaten Schlüssel mit Mitteln zu erzeugen, die der Teilnehmer unter seiner alleinigen Kontrolle halten kann.
- ✓ Sofern die Schlüssel von einem Dritten zur Verfügung gestellt werden, ist sicherzustellen, dass der Teilnehmer in den alleinigen Besitz der privaten Schlüssel gelangt.

- ✓ Für die zur Legitimation eingesetzten privaten Schlüssel definiert jeder Nutzer pro Schlüssel ein Passwort, das den Zugriff auf den jeweiligen privaten Schlüssel absichert.
- ✓ 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 BKS Bank ist die Übermittlung der öffentlichen Schlüssel des Teilnehmers an das Banksystem erforderlich. Hierfür übermittelt der Teilnehmer der BKS 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 BKS 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 unterstützten 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 BKS 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 BKS Bank den betreffenden Teilnehmer für die vereinbarten Auftragsarten frei.

3.2. Initialisierung der Bankseitigen Schlüssel

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

Der Hashwert des öffentlichen Bankschlüssels wird von der BKS 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 Bankschlüsseln dadurch zu überprüfen, dass er deren Hashwerte mit den Hashwerten vergleicht, die von der BKS 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 BKS Bank gesondert mitgeteilten Zertifizierungspfades überprüft.

4. 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 BKS 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.

5. Auftragserteilung an die BKS 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 BKS 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. Eine Ausnahme bildet die mit dem Kunden optional vereinbarte Online-Prüfung der Auftragsdaten durch die BKS Bank.

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

- ✓ Alle erforderlichen Bankfachlichen EU werden zusammen mit den Auftragsdaten übertragen.
- ✓ 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.
- ✓ Soweit Kunde und BKS 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 BKS Bank.

5.1. Auftragserteilung mittels Verteilter Elektronischer Unterschrift (VEU)

Die Art und Weise, wie die Verteilte Elektronische Unterschrift durch den Kunden genutzt wird, muss mit der BKS 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 Punkt 9. der „Bedingungen für die Datenfernübertragung“ möglich.

5.2. Legitimationsprüfung durch die BKS Bank

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

5.3. Kundenprotokolle

Die BKS 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, die Anzeige von Auftragsdaten betreffen

Der Teilnehmer hat sich durch Abruf des Kundenprotokolls über das Ergebnis der auf Seiten der BKS 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 BKS Bank zur Verfügung zu stellen.

5.4. Änderung der Teilnehmerschlüssel mit automatischer Freischaltung

Wenn die vom Teilnehmer eingesetzten Legitimations- und Sicherungsmedien in ihrer Gültigkeit zeitlich begrenzt sind, hat der Teilnehmer seiner BKS 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 BKS 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)

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 Punkt 8.3. 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.

5.5. 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 Punkt 3. 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 BKS Bank gesondert bekannt gegebenen 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 BKS 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 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.
- ✓ 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.
- ✓ Es ist ein Virenscanner zu installieren, der regelmäßig mit den neuesten Virendefinitions-Dateien auszustatten ist.
- ✓ Die Umsetzung dieser Anforderungen liegt ausschließlich in der Verantwortung des Kunden.
- ✓ 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 Daten-Formate werden auf der BKS Bank Website www.bks.at/EBICS zum Herunterladen bereitgestellt.

Anlage 3: Schnittzeiten der BKS Bank

Annahmezeiten für Zahlungsaufträge

Zahlungsaufträge, die innerhalb der unten angeführten Zeiten bei der BKS Bank eintreffen, werden unter Einhaltung folgender Voraussetzungen taggleich durchgeführt:

- ✓ die per DFÜ eingelieferten Auftragsdaten wurden gemäß Punkt 3.8. der „Bedingungen für die Datenfernübertragung“ autorisiert
- ✓ das festgelegte Datenformat wird verwendet
- ✓ das Verfügungslimit wird nicht überschritten

Inlandszahlungsverkehr / SEPA Zahlungen

✓ Standardüberweisung mit elektronischer Autorisierung	16.00 Uhr
✓ Eilüberweisungen mit elektronischer Autorisierung	16.00 Uhr
✓ Eilüberweisungen grenzüberschreitend	16.00 Uhr

Auslandszahlungsverkehr

✓ Zahlungsaufträge in EUR	15.00 Uhr
✓ Zahlungsaufträge in Fremdwährung mit Konvertierung	11.15 Uhr
✓ Zahlungsaufträge in Fremdwährung (USD, CAD, CHF, GBP, HUF, CZK) ohne Konvertierung	15.00 Uhr