

## **Besondere Bedingungen der Deutschen Bundesbank für die Datenfernübertragung via EBICS für Nichtbanken (EBICS-Bedingungen)**

### **I. Leistungsumfang**

Die Deutsche Bundesbank steht ihren Nichtbanken-Kunden (Kontoinhaber) für die Datenfernübertragung auf elektronischem Wege – nachfolgend „Datenfernübertragung“ oder „DFÜ“ genannt – über EBICS (Electronic Banking Internet Communication Standard) zur Verfügung. Die Datenfernübertragung über EBICS umfasst die Auftragserteilung sowie den Datenaustausch (Übermittlung von Aufträgen und Informationsabruf). Sie kann für die Einlieferung und Abwicklung von Überweisungen und Lastschriften und die Auslieferung von Dateien oder elektronischen Kontoinformationen in Form des MT 940 genutzt werden.

### **II. Nutzer und Teilnehmer, Legitimations- und Sicherungsmedien**

- (1) Zahlungsaufträge können über die EBICS-Anbindung vom Kunden, einer Person, die gemäß Abschnitt I, Nummer 3 Absatz 1 der Allgemeinen Geschäftsbedingungen der Bank für das Konto zeichnungsberechtigt ist (Zeichnungsberechtigte) oder einer vom Kunden hierzu gesondert ermächtigten Person erteilt werden. Kunde, Zeichnungsberechtigte und gesondert ermächtigte Personen werden im Folgenden einheitlich als „Nutzer“ bezeichnet. Zur Erteilung von Aufträgen an die Deutsche Bundesbank benötigt jeder Nutzer jeweils individuelle, von der Deutschen Bundesbank freigeschaltete Legitimationsmedien. Die Anforderungen an die Legitimationsmedien sind in Anlage 1 definiert.
- (2) Für den Datenaustausch kann der Kunde zusätzlich zu den Zeichnungsberechtigten „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 Deutschen Bundesbank freigeschaltete Sicherungsmedien. Die Anforderungen an die Sicherungsmedien sind in Anlage 1 beschrieben.

### III. Verfahrensbestimmungen

- (1) Für die Teilnahme gelten die in Anlage 1 sowie die in der Dokumentation der technischen Schnittstellen („Spezifikation für die EBICS-Anbindung“ entsprechend Anlage 1 des DFÜ-Abkommens<sup>1</sup>) und die in den „Verfahrensregeln der Deutschen Bundesbank für Nichtbanken zur Abwicklung von SEPA-Überweisungen per Datenfernübertragung“ (im Folgenden „Verfahrensregeln SEPA-Überweisungen für Nichtbanken“) beschriebenen Anforderungen.
- (2) Der Kunde ist verpflichtet sicherzustellen, dass alle Teilnehmer die mit der Deutschen Bundesbank vereinbarten Verfahren und Spezifikationen beachten.
- (3) Der Satz- und Dateiaufbau für die Übermittlung von SEPA-Überweisungen richtet sich nach den Nummern 4.2 und 4.3 der „Verfahrensregeln SEPA-Überweisungen für Nichtbanken“. Der Satz- und Dateiaufbau für die Übermittlung von Überweisungen und Lastschriften im EÖ- bzw. ZV-Format richtet sich nach Anlage 1, Nummer 4.3.

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 bzw. 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) Vor der Übertragung von Datensätzen an die Deutsche Bundesbank 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

---

<sup>1</sup> Die Spezifikation ist auf der Webseite [www.ebics.de](http://www.ebics.de) abrufbar.

einen Zeitraum von 10 Kalendertagen ab dem Ausführungstag in der Form nachweisbar zu halten, dass die Datei auf Anforderung der Deutschen Bundesbank kurzfristig erneut zur Verfügung gestellt werden kann.

- (5) Der Kunde ist verpflichtet, das Kundenprotokoll (siehe Kapitel 10 der Spezifikation für die EBICS-Anbindung), das nach Einreichung eines Auftrags vom EBICS-System der Deutschen Bundesbank automatisch erstellt wird, regelmäßig „abzuholen“. Das Kundenprotokoll ist zu den Unterlagen zu nehmen und auf Anforderung der Deutschen Bundesbank zur Verfügung zu stellen.
- (6) Soweit die Deutsche Bundesbank 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.

#### **IV. Verhaltens- und Sorgfaltspflichten im Umgang mit den Legitimationsmedien für die Auftragserteilung**

- (1) Der Kunde ist verpflichtet sicherzustellen, dass alle Nutzer die in Anlage 1 beschriebenen Legitimationsverfahren einhalten.
- (2) Mit Hilfe der von der Deutschen Bundesbank 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. 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 aus dem Lesegerät zu entnehmen und 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.

## **V. Verhaltens- und Sorgfaltspflichten im Umgang mit den Sicherungsmedien für den Datenaustausch**

Der Kunde ist verpflichtet sicherzustellen, dass alle Teilnehmer die in Anlage 1 beschriebenen Sicherungsverfahren einhalten.

Mit Hilfe der von der Deutschen Bundesbank freigeschalteten Sicherungsmedien sichert der Teilnehmer den Datenaustausch ab. Der Kunde ist 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.

## **VI. 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 Deutschen Bundesbank sperren zu lassen. Näheres regelt Anlage 1.
- (2) Hat ein Teilnehmer der Deutschen Bundesbank eine Sperre übermittelt, so haftet die Deutsche Bundesbank ab dem Zugang der übermittelten Sperrnachricht für alle Schäden, die aus ihrer Nichtbeachtung entstehen.
- (3) Der Kunde kann außerhalb des DFÜ-Verfahrens die Verwendung der Legitimations- und Sicherungsmedien eines Teilnehmers oder den gesamten DFÜ-Zugang bei der Deutschen Bundesbank, Zentrale, Z 200 (Telefon: 069 9566 8067/Telefax: 069 9566 508067), sperren lassen.
- (4) Die Deutsche Bundesbank wird den gesamten DFÜ-Zugang sperren, wenn der Verdacht einer missbräuchlichen Nutzung des DFÜ-Zugangs besteht. Sie wird den Kunden hierüber außerhalb des DFÜ-Verfahrens informieren. Diese Sperre kann mittels DFÜ nicht aufgehoben werden.

## **VII. Behandlung eingehender Aufträge durch die Deutsche Bundesbank**

- (1) Die der Deutschen Bundesbank im DFÜ-Verfahren erteilten Aufträge werden im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeitet.

- (2) Die Deutsche Bundesbank 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 Deutsche Bundesbank den betreffenden Auftrag nicht verarbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen.
- (3) Die Deutsche Bundesbank prüft die Legitimation des Nutzers bzw. der Nutzer anhand der von den Nutzern mittels der Legitimationsmedien erstellten Signaturen sowie die Übereinstimmung der Auftragsdatensätze mit den Bestimmungen der „Spezifikation der Datenformate“ entsprechend Anlage 3 des DFÜ-Abkommens<sup>2</sup>, den Nummern 4.2 und 4.3 der „Verfahrensregeln SEPA-Überweisungen für Nichtbanken“ sowie der Anlage 1, Nummer 4.3, zu diesen Bedingungen. Ergibt die Prüfung Unstimmigkeiten, wird die Deutsche Bundesbank die betreffenden Aufträge nicht bearbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen. Die Deutsche Bundesbank ist berechtigt, nicht vollständig autorisierte Aufträge nach Ablauf von 24 Stunden nach Auftragseingang zu löschen.
- (4) Ergeben sich bei den von der Deutschen Bundesbank durchgeführten Prüfungen der Dateien oder Datensätze nach den Nummern 4.2 und 4.3 der „Verfahrensregeln SEPA-Überweisungen für Nichtbanken“ sowie Anlage 1, Nummer 4.3 Fehler, so wird die Deutsche Bundesbank die fehlerhaften Dateien oder Datensätze in geeigneter Form nachweisen und sie dem Nutzer unverzüglich mitteilen. Die Deutsche Bundesbank ist berechtigt, die fehlerhaften Dateien oder Datensätze von der weiteren Bearbeitung auszuschließen, wenn die ordnungsgemäße Ausführung des Auftrages nicht sichergestellt werden kann.

### **VIII. 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 2 beschrieben.

### **IX. Geltung sonstiger Bedingungen**

Soweit in den vorstehenden Bedingungen im Einzelnen nichts anderes vorgeschrieben ist, gelten im Übrigen die „Verfahrensregeln SEPA-Überweisungen für Nichtbanken“, die „Besondere Bedingungen der Deutschen Bundesbank für die elektronische Einreichung, Auftragserteilung, Datenauslieferung und Kundeninformation (EADK-Bedingungen)“ sowie die „Allgemeine Geschäftsbedingungen der Deutschen Bundesbank (AGB)“.

---

<sup>2</sup> Die Spezifikation ist auf der Webseite [www.ebics.de](http://www.ebics.de) abrufbar.

## **Anhang**

Anlage 1: EBICS-Anbindung Nichtbanken

Anlage 2: Sicherheitsanforderungen an das EBICS-Kundensystem

**Anlage 1 zu den  
„Besonderen Bedingungen der Deutschen Bundesbank für die  
Datenfernübertragung via EBICS (EBICS-Bedingungen)“  
- EBICS-Anbindung Nichtbanken -**

## **Inhaltsverzeichnis**

<b>1</b>	<b>Teilnahmebedingungen</b>	<b>9</b>
<b>2</b>	<b>Legitimations- und Sicherungsverfahren</b>	<b>9</b>
<b>2.1</b>	<b>ELEKTRONISCHE UNTERSCHRIFTEN</b>	<b>10</b>
2.1.1	ELEKTRONISCHE UNTERSCHRIFTEN DER TEILNEHMER	10
<b>2.2</b>	<b>AUTHENTIFIKATIONSSIGNATUR</b>	<b>11</b>
<b>2.3</b>	<b>VERSCHLÜSSELUNG</b>	<b>11</b>
<b>3</b>	<b>Initialisierung der EBICS-Anbindung</b>	<b>12</b>
<b>3.1</b>	<b>EINRICHTUNG DER KOMMUNIKATIONSVERBINDUNG</b>	<b>12</b>
<b>3.2</b>	<b>INITIALISIERUNG DER SCHLÜSSEL</b>	<b>12</b>
3.2.1	NEUINITIALISIERUNG DER TEILNEHMERSCHLÜSSEL	12
3.2.2	INITIALISIERUNG DER BANKSEITIGEN SCHLÜSSEL	14
<b>4</b>	<b>Auftragserteilung an die Deutsche Bundesbank</b>	<b>15</b>
<b>4.1</b>	<b>AUFTRAGSERTEILUNG MITTELS VERTEILTER ELEKTRONISCHER UNTERSCHRIFT (VEU)</b>	<b>15</b>
<b>4.2</b>	<b>LEGITIMATIONSPRÜFUNG DURCH DIE DEUTSCHE BUNDESBANK</b>	<b>16</b>
<b>4.3</b>	<b>ZULÄSSIGE AUFTRAGSARTEN</b>	<b>16</b>
4.3.1	EINREICHUNG VON ZAHLUNGSaufTRÄGEN	16
4.3.1.1	EINREICHUNG IN DAS HBV-SEPA	16
4.3.1.2	EINREICHUNG IN DEN EMZ	17
4.3.1.3	EINREICHUNG IN DAS HBV	18
4.3.2	AUSLIEFERUNG VON ZAHLUNGSVERKEHRSINFORMATIONEN	18
4.3.2.1	INFORMATIONEN AUS DEM HBV-SEPA	20
4.3.2.2	INFORMATIONEN AUS DEM EMZ	21
4.3.2.3	INFORMATIONEN AUS DEM HBV	22
4.3.2.4	INFORMATIONEN AUS DER KONTOFÜHRUNG (KTO2)	22
<b>4.4</b>	<b>KUNDENPROTOKOLLE</b>	<b>23</b>
<b>5</b>	<b>Änderung der Teilnehmerschlüssel mit automatischer Freischaltung</b>	<b>26</b>
<b>6</b>	<b>Sperrung der Teilnehmerschlüssel</b>	<b>27</b>
<b>7</b>	<b>Testanforderungen</b>	<b>28</b>
<b>7.1</b>	<b>GRUNDSÄTZLICHES</b>	<b>28</b>
<b>7.2</b>	<b>TESTSZENARIEN</b>	<b>29</b>
7.2.1	INITIALISIERUNG DER EBICS-ANBINDUNG	29
7.2.2	DOWNLOAD TRANSAKTIONEN	29
7.2.3	DATENAUSTAUSCH ÜBER DIE EBICS-ANBINDUNG	29

## 1 Teilnahmebedingungen

Für die Teilnahme am EBICS-Verfahren ist zunächst von jedem Kunden ein Zulassungs- und Conformance-Test zu durchlaufen (nähere Einzelheiten s. Abschnitt 7 „Testanforderungen“).

Die Zulassung zum Produktionsbetrieb für die Teilnahme am Datenverkehr über den Kommunikationskanal EBICS ist vom Kunden (Kontoinhaber) mit dem Vordruck 4760 „Antrag auf EBICS-Teilnahme Nichtbanken“ bei der kontoführenden Filiale der Deutschen Bundesbank zu beantragen. Darüber hinaus sind weitere Antragsvordrucke für die Teilnahme an den Fachverfahren je nach individuellem Bedarf einzureichen. Dazu gehören z. B. die Vordrucke:

- Teilnahme am Hausbankverfahren (HBV): Vordruck 4781
- Teilnahme am Hausbankverfahren-SEPA (HBV-SEPA): Vordruck 4767
- Teilnahme am Elektronischen Massenzahlungsverkehr (EMZ): Vordruck 4780

Die aktuellen Vordrucke werden auf der Internetseite der Deutschen Bundesbank im Sachgebiet „Zahlungsverkehr“ unter der Rubrik „Veröffentlichungen/Vordrucke“ bereitgestellt. Informationen zu den individuell benötigten Unterlagen für den Zugang zu den Fachverfahren sind den jeweiligen anwendungsspezifischen Verfahrensregeln zu entnehmen. Das Kundentestzentrum ist im Rahmen der Testaktivitäten bei der Auswahl der individuell benötigten Vordrucke behilflich.

## 2 Legitimations- und Sicherungsverfahren

Der Kunde (Kontoinhaber) benennt der Deutschen Bundesbank im Rahmen der Antragsstellung die Teilnehmer und deren Berechtigungen im Rahmen der EBICS-Teilnahme.

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 Deutschen Bundesbank 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.

Im Rahmen der EBICS-Teilnahme ist eine MAC-Sicherung nicht mehr erforderlich. Entsprechende Feldbelegungen werden nicht mehr ausgewertet.

## **2.1 Elektronische Unterschriften**

### **2.1.1 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“)

EU vom Typ „E“, „A“, oder „B“ werden als bankfachliche EU bezeichnet; sie dienen der Autorisierung von Aufträgen. Aufträge können mehrere bankfachliche EU benötigen, die von unterschiedlichen Nutzern (Kontoinhaber, Zeichnungsberechtigte und gesondert ermächtigte Personen) geleistet werden müssen. Die EU bilden die auf dem Unterschriftenblatt hinterlegten Berechtigungen ab. Eine Einschränkung der Unterschriftsklasse der Teilnehmer gegenüber der Berechtigung gemäß Unterschriftenblatt ist zulässig. Die EU von gesondert ermächtigten Personen ergibt sich aus dem jeweiligen Teilnahmeantrag.

EU vom Typ „T“ können nicht zur Autorisierung von Aufträgen verwendet werden, 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. SEPA-Überweisungen, DTA-Zahlungsaufträge, aber auch Aufträge für Initialisierung, Protokollabruf etc.)

erstellt werden. Die Deutsche Bundesbank teilt dem Kunden im Rahmen der Zulassung mit, welche Nachrichtenarten genutzt werden können und welcher EU-Typ hierfür anzuwenden ist.

## **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 Deutschen Bundesbank übermittelten EBICS-Nachricht unter Berücksichtigung der Aktualität und Authentizität der gespeicherten öffentlichen Schlüssel der Deutschen Bundesbank gemäß den Vorgaben der EBICS-Spezifikation prüft.

## **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 Deutschen Bundesbank gemäß den Vorgaben der EBICS-Spezifikation zu verschlüsseln.

Darüber hinaus ist auf den externen Übertragungstrecken zwischen Kunden- und Banksystem zusätzlich eine Transportverschlüsselung vorzunehmen. Der Kunde muss gewährleisten, dass eine Software eingesetzt wird, die Aktualität und Authentizität der hierfür eingesetzten Serverzertifikate der Deutschen Bundesbank gemäß den Vorgaben der EBICS-Spezifikation überprüft.

### **3 Initialisierung der EBICS-Anbindung**

#### **3.1 Einrichtung der Kommunikationsverbindung**

Der Kommunikationsaufbau erfolgt unter Verwendung einer URL (Uniform Resource Locator). Alternativ kann auch die IP-Adresse der Deutschen Bundesbank benutzt werden. Die URL oder die IP-Adresse werden dem Kunden mitgeteilt.

Die Deutsche Bundesbank teilt den vom Kunden benannten Teilnehmern zur Aufnahme der EBICS-Anbindung folgende Daten mit:

- URL oder IP-Adresse der Deutschen Bundesbank
- Host-ID
- Zulässige Version(en) für das EBICS-Protokoll und der Sicherungsverfahren (EBICS-Versionen 2.2 und 2.3 sowie Schemaversion H002)
- Kunden-ID
- Teilnehmer-ID
- Weitere spezifische Angaben zu Kunden- und Teilnehmerberechtigungen

Für die dem Kunden zugeordneten Teilnehmer vergibt die Deutsche Bundesbank jeweils eine Teilnehmer-ID, die den Teilnehmer eindeutig identifiziert. Soweit dem Kunden ein oder mehrere technische Teilnehmer zugeordnet sind (Multi-User-System), vergibt die Deutsche Bundesbank zusätzlich eine Teilnehmer-ID für jeden technischen Teilnehmer.

#### **3.2 Initialisierung der Schlüssel**

##### **3.2.1 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 wird, die vor unautorisiertem Zugriff geschützt ist.

Für die Initialisierung des Teilnehmers bei der Deutschen Bundesbank ist die Übermittlung der öffentlichen Schlüssel des Teilnehmers an das Banksystem erforderlich. Hierfür übermittelt der Teilnehmer der Deutschen Bundesbank seine öffentlichen Schlüssel auf zwei voneinander unabhängigen Kommunikationswegen:

- Über die EBICS-Anbindung mittels der hierfür vorgesehenen systembedingten Auftragsarten INI und HIA.
- Mit einem vom Kontoinhaber oder Zeichnungsberechtigten unterschriebenen Initialisierungsbrief an die kontoführende Filiale der Deutschen Bundesbank.

Für die Freischaltung des Teilnehmers überprüft die Deutsche Bundesbank auf Basis der vom Kontoinhaber, Zeichnungsberechtigten oder von der gesondert ermächtigten Person 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
- Datum und Uhrzeit der Generierung
- Kunden-ID und Teilnehmer-ID
- Host-ID

Die Deutsche Bundesbank prüft die Unterschrift des Kontoinhaber oder der/des Zeichnungsberechtigten bzw. der gesondert ermächtigten Person auf dem Initialisierungsbrief mit den in der Kontoführung bzw. auf dem Vordruck 4760 hinterlegten Unterschriften sowie die Übereinstimmung zwischen den über die EBICS-Anbindung und den schriftlich übermittelten Hashwerten des öffentlichen Schlüssels des Teilnehmers. Bei positivem Prüfergebnis schaltet die Deutsche Bundesbank den betreffenden Teilnehmer für die vereinbarten Auftragsarten frei.

### 3.2.2 Initialisierung der bankseitigen Schlüssel

Der Teilnehmer holt den öffentlichen Schlüssel der Deutschen Bundesbank mittels einer eigens dafür vorgesehenen systembedingten Auftragsart HPB ab.

Der Hashwert des öffentlichen Bankschlüssels wird dem Kunden von der Deutschen Bundesbank im Rahmen der Antragstellung mitgeteilt. 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 Deutschen Bundesbank im Rahmen der Antragstellung übermittelt wurden.

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

## 4 Auftragserteilung an die Deutsche Bundesbank

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 Deutschen Bundesbank zuerst teilnehmerbezogene Berechtigungsprüfungen durchgeführt, wie etwa die Auftragsartberechtigung. Die Ergebnisse weiterer bankfachlicher Prüfungen, wie beispielsweise Kontoberechtigungsprüfungen, werden dem Kunden im Kundenprotokoll zu einem späteren Zeitpunkt mitgeteilt.

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, längstens bis zur Löschung des Auftrags nach Abschnitt VII (3) der EBICS-Bedingungen, gespeichert.

### 4.1 Auftragserteilung mittels Verteilter Elektronischer Unterschrift (VEU)

Die Verteilte Elektronische Unterschrift (VEU) 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.

Die Deutsche Bundesbank ist dazu berechtigt, nicht vollständig autorisierte Aufträge nach Ablauf des Zeitlimits von 24 Stunden zu löschen.

## 4.2 Legitimationsprüfung durch die Deutsche Bundesbank

Ein empfangener Auftrag wird durch die Deutsche Bundesbank erst dann ausgeführt, wenn die erforderlichen bankfachlichen EU eingegangen sind und mit positivem Ergebnis geprüft wurden.

## 4.3 Zulässige Auftragsarten

### 4.3.1 Einreichung von Zahlungsaufträgen

Die Deutsche Bundesbank unterstützt die nachfolgenden Auftragsarten für die Auftragserteilung. Jeder Auftragsart ist genau ein Datenformat zugeordnet. Dabei muss in „multibankfähige“ Auftragsarten und Datenformate gemäß Anlage 1 bzw. Anlage 3 des DFÜ-Abkommens und in institutsspezifische Auftragsarten und Datenformate unterschieden werden. Multibankfähige Datenformate sind im deutschen Kreditgewerbe einheitlich spezifiziert. Institutsspezifische Auftragsarten und Datenformate können nur im Datenaustausch mit der Deutschen Bundesbank verwendet werden und sind in den entsprechenden Spezifikationen der Bundesbank festgelegt. Bei allen nachfolgenden Auftragsarten, die mit X beginnen, handelt es sich um bundesbankeigene Auftragsarten, die Auftragsart CCM ist eine multibankfähige Auftragsart. Auf die zu beachtende Datenformatspezifikation wird in der Spalte „Format“ der nachfolgenden Tabellen verwiesen. Dateien, deren Aufbau nicht den zu der Auftragsart gehörenden Spezifikationen entspricht, werden von der Deutschen Bundesbank entweder direkt vom EBICS-Bankrechner zurückgewiesen (siehe 4.4) oder von der verarbeitenden Fachanwendung mittels einer Fehlernachricht zurückgewiesen (siehe 4.3.2).

#### 4.3.1.1 Einreichung in das HBV-SEPA

Auftragsart	Beschreibung	Format
CCM	Einreichung von Überweisungen in einer einzelnen Pain- Nachricht	Siehe DFÜ-Abkommen Anlage 3, Kapitel 2.2.1 und zusätzliche Festlegungen in Anhang „Technische Spezifikationen der Deutschen Bundesbank für die Abwicklung von SEPA-Überweisungen im Kunde-Bank-Verkehr“ zu „Verfahrensregeln der Deutschen Bundesbank für Nichtbanken zur Abwicklung von SEPA-Überweisungen per Datenfernübertragung (DFÜ)“ Kapitel 2

**Tabelle 1 Auftragsarten für die Einreichung von Zahlungsaufträgen in das HBV-SEPA**

4.3.1.2 Einreichung in den EMZ

Auftragsart	Beschreibung	Format
XGK	GK-Datei; Prior3-Überweisungen von Nichtbanken	DTA gem. Elektronischer Öffnung <sup>3</sup> , s. Anhang, Tz. 5.1
XLK	LK-Datei; Lastschriften und Zahlungsvorgänge aus dem beleglosen Scheckeinzug von Nichtbanken	> EBCDIC/ungepackt > SLF: 4Bn <sup>4</sup>
XGS	GS-Datei; Step2- Zahlungen von Nichtbanken	EÖ-SWIFT gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 5.2 > A- und E-Satz EBCDIC/ ungepackt > SLF: 4Bn <sup>2</sup>
XCG	GK-Datei; Prior3-Überweisungen von Nichtbanken	DTA gem. Anlage 1a des Anhangs zu den
XCL	LK-Datei; Lastschriften und Zahlungsvorgänge aus dem beleglosen Scheckeinzug von Nichtbanken	EMZ-Bedingungen <sup>5</sup> > EBCDIC/gepackt > SLF: 4Bb <sup>2</sup>
XCS	GS-Datei; Step2- Zahlungen von Nichtbanken	EÖ-SWIFT gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 5.2 > A- und E-Satz EBCDIC/gepackt > SLF: 4Bb <sup>2</sup>

**Tabelle 2 Auftragsarten für die Einreichung von Zahlungsaufträgen an den EMZ**

<sup>3</sup> Spezifikationen für den elektronischen Zahlungsverkehr der Deutschen Bundesbank, V 1.5

<sup>4</sup> SLF = Satzlängenfeld; 4Bb = 4-Byte binär im Feld A1 bzw. 1, 4Bn = 4-Byte numerisch, 6Bn = 6-Byte numerisch

<sup>5</sup> Besondere Bedingungen der Deutschen Bundesbank für den Elektronischen Massenzahlungsverkehr mit Datenträgerbegleitzettel im Geschäftsverkehr mit Nichtbanken

#### 4.3.1.3 Einreichung in das HBV

Auftragsart	Beschreibung	Format
XG1	GT-Datei; Prior1-Überweisungen von Nichtbanken	DTA gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 4.1 – 4.3 > EBCDIC/ungepackt > SLF: 4Bn <sup>2</sup>
XG2	GT-Datei; Prior1-Überweisungen von Nichtbanken	EÖ-SWIFT gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 4.4 > EBCDIC/ungepackt > SLF: 6Bn <sup>2</sup>
XDT	DT-Datei; Prior1-Auslandsüberweisungen in Euro von Nichtbanken	EÖ-SWIFT gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 4.5 > EBCDIC/ungepackt > SLF: 6Bn <sup>2</sup>
XWT	WT-Datei; Prior1-Auslandsüberweisungen in Fremdwährung von Nichtbanken	
XTG	TG-Datei; TARGET-Zahlungsaufträge von Nichtbanken	EÖ-SWIFT gem. Elektronischer Öffnung <sup>1</sup> s. Anhang, Tz. 4.6 > EBCDIC/ungepackt > SLF: 6Bn <sup>2</sup>

**Tabelle 3 Auftragsarten für die Einreichung von Zahlungsaufträgen in das HBV**

#### 4.3.2 Auslieferung von Zahlungsverkehrsinformationen

Abweichend zu den Verfahren der elektronischen Öffnung über den EÖ-Gateway werden alle Auslieferungsdaten gemäß EBICS-Standard zur Abholung bereitgestellt, das heißt nicht aktiv an den Empfänger verschickt. Liegen mehrere nicht abgeholte (logische) Dateien zu einer Auftragsart vor, so werden alle nicht abgeholten logischen Dateien für den Transfer zu einer physikalischen Datei zusammengefasst.

Der Empfänger der Dateien muss selbst dafür sorgen, dass die Dateien in geeigneten Abständen abgerufen werden. Nicht abgeholte Dateien werden 10 Geschäftstage zur Abholung auf dem EBICS-System bereitgehalten.

Die Deutsche Bundesbank unterstützt die nachfolgenden Auftragsarten für die Auslieferung von Zahlungsverkehrsinformationen. Hierzu zählen Nachrichtendateien der Zahlungsverkehrsanwendungen sowie Umsatz- und Saldeninformationen der Kontoführung.

Fachliche Verarbeitungsfehler / die Ergebnisse der Prüfungen in den Fachanwendungen werden den Teilnehmern durch Nachrichtendateien bereitgestellt.

- Für SEPA-Aufträge ist dies die Nachricht pain.002.001.02 als Rückweisungsnachricht zu einer Einlieferung (Auftragsart CRJ).
- Für Zahlungsaufträge an den EMZ sind dies M-Nachrichten: Die Nachrichten M3 als Mitteilungen über nicht verarbeitungsfähige Dateien, M7 als Mitteilungen über nicht ausgeführte bzw. annullierte Zahlungen und M8 als Mitteilungen über nicht verarbeitbare Datensätze. Zusätzlich wird eine M9-Datei als Mitteilung über verarbeitete und ausgelieferte Dateien sowie eine M6-Datei als Informationsliste über die in den morgendlichen Verarbeitungsfenstern verarbeiteten Dateien erstellt.
- Für Zahlungsaufträge an das HBV sind dies M-Nachrichten. Die Nachrichten M3 als Mitteilungen über nicht verarbeitungsfähige Dateien, M7 als Mitteilungen über nicht ausgeführte bzw. annullierte Zahlungen und M8 als Mitteilungen über nicht verarbeitbare Datensätze. Zusätzlich wird eine M9-Nachricht als Mitteilung über verarbeitete und ausgelieferte Dateien erstellt. Die Nachrichtendatei M6 ist als freie Textnachricht definiert.

M-Dateien aus dem EMZ und dem HBV werden mit Ausnahme der M6-Dateien mit jeweils pro Dateityp gleicher Auftragsart bereitgestellt. M6-Dateien werden auf Grund der abweichenden inhaltlichen Belegung (EMZ: als Informationsliste über in den morgendlichen Verarbeitungsfenstern verarbeitete Dateien; HBV: freie Textdatei) mit getrennten Auftragsarten bereitgestellt.

Umsatz- und Saldeninformationen werden in Form von Zahlungsverkehrsdateien oder elektronischen Kontoinformationen (MT 940) bereitgestellt.

Jeder Auftragsart ist genau ein Datenformat zugeordnet. Dabei muss in „multibankfähige“ Auftragsarten und Datenformate gemäß Anlage 1 bzw. Anlage 3 des DFÜ-Abkommens und in institutsspezifische Auftragsarten und Datenformate unterschieden werden. Multibankfähige

Datenformate sind im deutschen Kreditgewerbe einheitlich spezifiziert. Institutsspezifische Auftragsarten und Datenformate können nur im Datenaustausch mit der Deutschen Bundesbank verwendet werden und sind in den entsprechenden Spezifikationen der Deutschen Bundesbank festgelegt. Bei allen nachfolgenden Auftragsarten, die mit Y beginnen, handelt es sich um bundesbankeigene Auftragsarten, die Auftragsarten DTI, CRJ und STA sind multibankfähige Auftragsarten. Auf die relevanten Datenformatspezifikationen wird in der Spalte „Format“ der nachfolgenden Tabellen verwiesen.

#### 4.3.2.1 Informationen aus dem HBV-SEPA

Auftragsart	Beschreibung	Format
DTI	IZV-Datei abholen	Siehe DFÜ-Abkommen Anlage 3, Kapitel 2.2.1 und zusätzliche Festlegungen in Anhang „Technische Spezifikationen der Deutschen Bundesbank für die Abwicklung von SEPA-Überweisungen im Kunde-Bank-Verkehr“ zu „Verfahrensregeln der Deutschen Bundesbank für Nichtbanken zur Abwicklung von SEPA-Überweisungen per Datenfernübertragung (DFÜ)“ Kapitel 3
CRJ	Information über die Nichtausführung einer Überweisung	Siehe DFÜ-Abkommen Anlage 3, Kapitel 2.2.1 und zusätzliche Festlegungen in Anhang „Technische Spezifikationen der Deutschen Bundesbank für die Abwicklung von SEPA-Überweisungen im Kunde-Bank-Verkehr“ zu „Verfahrensregeln der Deutschen Bundesbank für Nichtbanken zur Abwicklung von SEPA-Überweisungen per Datenfernübertragung (DFÜ)“ Kapitel 3

**Tabelle 4 Auftragsarten für Informationen aus dem HBV-SEPA**

#### 4.3.2.2 Informationen aus dem EMZ

Auftragsart	Beschreibung	Format
YGB	GB-Datei; Prior3-Überweisungen an Nichtbanken	DTA gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 5.1 > EBCDIC/ungepackt > SLF: 4Bn <sup>2</sup>
YLB	LB-Datei; Lastschriften und Zahlungsvorgänge aus dem beleglosen Scheckeinzug an Nichtbanken	
YGD	GS-Datei; konvertierte Step2-Zahlung an Nichtbanken	DTA gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 5.1 > EBCDIC/ungepackt > SLF: 4Bn <sup>2</sup>
YGS	GS-Datei; Step2-Zahlung an Nichtbanken	EÖ-SWIFT gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 5.2 > A- und E-Satz EBCDIC/ungepackt > SLF: 4Bn <sup>2</sup>
YCG	GB-Datei; Prior3-Überweisungen an Nichtbanken	DTA gem. Anlage 1a des Anhangs zu den EMZ-Bedingungen <sup>3</sup> > EBCDIC/gepackt > SLF: 4Bb <sup>2</sup>
YCL	LB-Datei; Lastschriften und Zahlungsvorgänge aus dem beleglosen Scheckeinzug an Nichtbanken	
YCD	GS-Datei, Step2-Zahlung an Nichtbanken im DTA-Format	DTA gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 5.1 > EBCDIC/gepackt > SLF: 4Bb <sup>2</sup>
YCS	GS-Datei, Step2-Zahlung an Nichtbanken im SWIFT-Format	EÖ-SWIFT gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 5.2 > A- und E-Satz EBCDIC/gepackt > SLF: 4Bb <sup>2</sup>
YM3	M3-Nachricht; Mitteilung über eine nicht verarbeitbare Datei	M-Dateien gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 5.3 > EBCDIC/ungepackt > SLF: 4Bn <sup>2</sup>
YM6	M6-Nachricht; Freie Textnachricht	
YM7	M7-Nachricht; Mitteilung über nicht ausgeführte bzw. annullierte Zahlungen	
YM8	M8-Nachricht; Mitteilung über nicht verarbeitbare Datensätze	
YM9	M9-Nachricht; Mitteilung über verarbeitete Zahlungen und ausgelieferte Dateien	

**Tabelle 5 Auftragsarten für Informationen aus dem EMZ**

4.3.2.3 Informationen aus dem HBV

Auftragsart	Beschreibung	Format
YG1	GT-Datei; Inlands- und – Inlandsanschlusszahlung an Nichtbanken	DTA gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 4.1 – 4.3 > EBCDIC/ungepackt > SLF: 4Bn <sup>2</sup>
YG2	GT-Datei; Inlands- und – Inlandsanschlusszahlung an Nichtbanken	EÖ-SWIFT gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 4.4 > EBCDIC/ungepackt > SLF: 6Bn <sup>2</sup>
YWA	WA-Dateien; Währungsabrechnungen	EÖ-SWIFT gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 4.5 >EBCDIC/ungepackt > SLF: 6Bn <sup>2</sup>
YM3	M3-Nachricht; Mitteilung über eine nicht verarbeitbare Datei	M-Dateien gem. Elektronischer Öffnung <sup>1</sup> , s. Anhang, Tz. 4.9 > EBCDIC/ungepackt > SLF: 4Bn <sup>2</sup>
YM6	M6-Nachricht; Freie Textnachricht	
YM7	M7-Nachricht; Mitteilung über nicht ausgeführte bzw. annullierte Zahlungen	
YM8	M8-Nachricht; Mitteilung über nicht verarbeitbare Datensätze	
YM9	M9-Nachricht; Mitteilung über verarbeitete Zahlungen und ausgelieferte Dateien	

**Tabelle 6 Auftragsarten für Informationen aus dem HBV**

4.3.2.4 Informationen aus der Kontoführung (KTO2)

Auftragsart	Beschreibung	Format
STA	Abholen Swift-Tagesauszüge	MT 940 gemäß DFÜ-Abkommen Anlage 3

Sofern an einem Geschäftstag keine Umsätze auf einem Konto erfolgen, wird in diesem Fall am Tagesende ein umsatzfreier MT 940 (im Sinne einer Saldenmitteilung) erzeugt und zur Abholung bereitgestellt.

#### 4.4 Kundenprotokolle

Die Deutsche Bundesbank dokumentiert in Kundenprotokollen die folgenden Vorgänge:

- Übertragung der Auftragsdaten an das Banksystem (EBICS-Kommunikationsrechner)
- Abholung von Informationsdateien vom Banksystem durch 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
- Fehler bei der Dekomprimierung

Kundenprotokolle werden von der Deutschen Bundesbank 10 Kalendertage vorgehalten. Der Teilnehmer hat sich durch Abruf des Kundenprotokolls über das Ergebnis der auf Seiten der Deutschen Bundesbank durchgeführten Prüfungen zu informieren. Der Aufbau der Kundenprotokolle entspricht den Bestimmungen von Kapitel 10 der Spezifikation für die EBICS-Anbindung. Der Teilnehmer hat dieses Protokoll zu seinen Unterlagen zu nehmen und auf Anforderung der Deutschen Bundesbank zur Verfügung zu stellen.

Die Dateianzeige (Anzeige der Dateiinhalte bei Uploadtransaktionen) für bundesbankspezifische Auftragsarten ist nicht in der Spezifikation für die EBICS-Anbindung enthalten. Die Dateianzeige im Kundenprotokoll für bundesbankspezifische Auftragsarten ist wie folgt aufgebaut:

**Für die Auftragsarten XGK, XLK, XG1, XG2, XDT und XTG:**

Beschreibung	Feld Name	Position
Zahlungsart	Dateikennzeichen/Dateityp	A2
Bankleitzahl	Leitzahl des Empfängers der Datei; BLZ der kontoführenden Bundesbankfiliale	A3
Kontonummer	Leitzahl des Absenders der Datei;	A9

	Girokontonummer	
Auftraggeber	Bezeichnung des Absenders der Datei	A5
Erstellungsdatum	Datum der Dateierstellung	A6
Dateinummer	Eindeutige Nummer der Datei	A7
Anzahl der Zahlungssätze	Anzahl der Datensätze	E3
Summe der Beträge	Summe der Beträge in Euro	E9a

**Tabelle 7: Aufbau Dateianzeige des Kundenprotokolls EÖ-Format**

**Für die Auftragsarten XCG und XCS:**

Beschreibung	Feld Name	Position
Zahlungsart	Dateikennzeichen	A3
Bankleitzahl	Leitzahl des Empfängers der Datei; Bankleitzahl der kontoführenden Bundesbankfiliale	A4
Kontonummer	Leitzahl des Absenders der Datei; Girokontonummer	A9
Auftraggeber	Bezeichnung des Absenders der Datei	A6
Erstellungsdatum	Datum der Dateierstellung	A7
Dateinummer	Eindeutige Nummer der Datei	A8
Anzahl der Zahlungssätze	Anzahl der Datensätze	E4
Summe der Kontonummern	Summe der Kontonummern des C-Satzes	E6
Summe der Bankleitzahlen	Summe der Bankleitzahlen	E7
Summe der Beträge	Summe der Beträge in Euro	E8

**Tabelle 8: Aufbau Dateianzeige des Kundenprotokolls ZV-Format**

**Für die Auftragsart XCL:**

Beschreibung	Feld Name	Position
Zahlungsart	Dateikennzeichen	A3
Bankleitzahl	Leitzahl des Empfängers der Datei; Bankleitzahl der kontoführenden Bundesbankfiliale	A4
Kontonummer	Leitzahl des Absenders der Datei, Girokontonummer	A9
Auftraggeber	Bezeichnung des Absenders der Datei	A6
Erstellungsdatum	Datum der Dateierstellung	A7
Dateinummer	Eindeutige Nummer der Datei	A8
Anzahl der Zahlungssätze	Anzahl der Datensätze	E4
Summe der Beträge	Summe der Beträge in Euro	E8

**Tabelle 9: Aufbau Dateianzeige des Kundenprotokolls GS-Datei gepackt**

**Für die Auftragsart XWT:**

Beschreibung	Feld Name	Position
Zahlungsart	Dateikennzeichen/Dateityp	A2
Bank-Code (Bankleitzahl)	Leitzahl des Empfängers der Datei; Bei Einlieferungen BLZ der kontoführenden Bundesbankfiliale	A3
Kontonummer	Leitzahl des Absenders der Datei	A9
Auftraggeber	Bezeichnung des	A5

	Absenders der Datei/Bankbezeichnung	
Erstellungsdatum	Datum der Dateierstellung	A6
Dateinummer	Eindeutige Nummer der Datei	A7
Anzahl der Zahlungssätze	Anzahl der Datensätze	E3
Summe der Beträge	Summe der Betragfelder	E5

**Tabelle 10: Aufbau Dateianzeige des Kundenprotokolls WT-Datei**

## **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 Deutschen Bundesbank 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 die Teilnehmerschlüssel unter Verwendung der dafür vorgesehenen systembedingten Auftragsarten zu erneuern und rechtzeitig vor dem Erreichen des Ablaufdatums der alten Schlüssel zu übermitteln. Die Gültigkeitsdauer der Schlüssel richtet sich nach den Empfehlungen der Bundesnetzagentur sowie des BSI. Die drei Schlüsselpaare der Deutschen Bundesbank werden grundsätzlich jedes Jahr ausgetauscht.

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

- Aktualisierung des öffentlichen bankfachlichen Schlüssels (PUB)
- 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 VII (3) der EBICS-Bedingungen 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 bei der Deutschen Bundesbank, Zentrale, Z 200 (Telefon: 069 9566 8067/ Telefax: 069 9566 508067), sperren lassen.

Auf dem gleichen Weg kann der Kunde außerhalb des DFÜ-Verfahrens die Legitimations- und Sicherungsmedien eines Teilnehmers oder den gesamten DFÜ-Zugang sperren lassen.

## **7 Testanforderungen**

### **7.1 Grundsätzliches**

Vor Verfahrensaufnahme ist durch einen erfolgreich absolvierten Zulassungs- und Conformance-Test die Einhaltung der technischen Vorgaben und die Funktionalität des getesteten Produkts nachzuweisen. Die Teilnahme ist mit Vordruck 4831 „Eröffnung eines Testverfahrens“ beim Kundentestzentrum anzumelden.

Die Tests werden vom Kundentestzentrum koordiniert:

Deutsche Bundesbank

Kundentestzentrum Z 412

Postfach 10 11 48

40002 Düsseldorf

Telefon: +49 211 874-2892 bzw. -2751

Telefax: +49 211 874-3611

E-Mail: [testzentrum@bundesbank.de](mailto:testzentrum@bundesbank.de)

Dem Kunden bietet sich bei diesem Test die Möglichkeit, die grundsätzlichen Verfahrensabläufe zu testen. Dies geschieht durch mehrere Einzeltests, die in Tz. 7.2 aufgeführt sind. Es ist zu beachten, dass es sich bei den der Deutschen Bundesbank im Rahmen des Zulassungs- und Conformance-Tests übermittelten Testdaten um anonymisierte Echtdateien handeln soll, wobei der Einlieferer die Verantwortung für die Anonymisierung trägt. Bei ggf. anderen erforderlichen Tests können beliebige Testdaten eingereicht werden. Die Deutsche Bundesbank behält sich das Recht vor, eingereichte Testdaten z. B. für Tests mit der Empfängerbank einer Zahlung zu verwenden. Änderungen am EBICS-Zugang (Hard- bzw. Software) oder Erweiterungen des Leistungsspektrums (z.B. Hinzunahme eines weiteren Dienstes) erfordern vor dem Produktionseinsatz einen erneuten Abnahmetest durch das Kundentestzentrum. Dafür ist frühzeitig ein Testverfahren mit dem Kundentestzentrum abzustimmen. Die formale Anmeldung erfolgt ebenfalls mit dem Vordruck 4831 „Eröffnung eines Testverfahrens“.

Für weiterführende Kundentests gelten die in den Verfahrensregeln der Fachanwendungen bzw. in den Spezifikationen für den elektronischen Zahlungsverkehr mit der Deutschen Bundesbank dargestellten Regelungen.

## 7.2 Testszzenarien

### 7.2.1 Initialisierung der EBICS-Anbindung

Testfall	Auftrag	Beschreibung
Test EBICS/I01	HIA	Senden des öffentlichen Authentifikationsschlüssels sowie des öffentlichen Verschlüsselungsschlüssels
Test EBICS/I02	INI	Senden des öffentlichen bankfachlichen Schlüssels
Test EBICS/I03	HPB	Abholen der öffentlichen Schlüssel der Bank oder des Kreditinstituts

### 7.2.2 Download Transaktionen

Testfall	Auftrag	Beschreibung
Test EBICS/D01	PTK	Abholung Kundenprotokolle nach Initialisierung

### 7.2.3 Datenaustausch über die EBICS-Anbindung

Im Testschritt „Datenaustausch“ ist der erfolgreiche Datenaustausch über EBICS mit der bzw. den individuell beantragten Fachverfahren zu testen.

Fachverfahren der Deutschen Bundesbank sind:

- Hausbankverfahren-SEPA (HBV-SEPA)
- Elektronischer Massenzahlungsverkehr (EMZ)
- Hausbankverfahren (HBV)
- Elektronische Kontoinformationen (KTO2)

Basis für den Datenaustausch sind die unter Tz. 4.3.1 und 4.3.2 beschriebenen Datenformate. Die individuell notwendigen Test-Stammdaten werden vom Kundentestzentrum mit den Testteilnehmern abgestimmt.

Nach Bedarf können Massentests mit dem Kundentestzentrum durchgeführt werden bei denen vom Kunden geeignete Testdaten mit einem Datenvolumen entsprechend des zu erwartenden Tagesspitzenwertes bereitzustellen sind.

## **Anlage 2: Sicherheitsanforderungen an das EBICS-Kundensystem**

Über die in Anlage 1 Nummer 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 1 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 Virenschanner 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.