

Bedingungen Datenfernübertragung ZV-App

Stand: 01.10.2025

Bedingungen für Datenfernübertragung – ZV-App

gültig ab Oktober 2025

1. Leistungsumfang

- (1) Die Bank steht ihrem Kunden (Kontoinhaber) für die Datenfernübertragung auf elektronischem Wege – nachfolgend „Datenfernübertragung“ oder „DFÜ“ genannt – zur Verfügung. Die Datenfernübertragung umfasst die Einreichung und den Abruf von Dateien (insbesondere Übermittlung von Aufträgen und Informationsabruf).
- (2) Die Bank gibt dem Kunden die Dienstleistungsarten bekannt, die er im Rahmen der Datenfernübertragung nutzen kann. Zur Nutzung der Datenfernübertragung gelten die mit der Bank vereinbarten Verfügungsmitte.
- (3) Die Datenfernübertragung findet über die Nutzung der ZV-App statt (Anlagen 1a und 1b).
- (4) Der Satz- und Dateiaufbau für die Übermittlung von Aufträgen und den Informationsabruf wird in der Spezifikation der Datenformate (Anlage 3) beschrieben.

2. Teilnehmer, Legitimations- und Sicherungsmedien

- (1) Aufträge können über die ZV-App nur vom Kunden oder seinen Kontobevollmächtigten erteilt werden. Kunde und Kontobevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet. Zur Autorisierung von per DFÜ übermittelten Auftragsdaten mittels Elektronischer Unterschrift benötigt jeder Teilnehmer jeweils individuelle, von der Bank freigeschaltete Legitimationsmedien. Die Anforderungen an die Legitimationsmedien sind in Anlage 1a definiert. Wenn mit der Bank vereinbart, können per DFÜ übermittelte Auftragsdaten mit unterschriebenem Begleitzettel / Sammelauftrag autorisiert werden.
- (2) Für die Absicherung des Datenaustauschs benötigt jeder Teilnehmer jeweils individuelle, von der Bank freigeschaltete Sicherungsmedien. Die Anforderungen an die Sicherungsmedien sind in Anlage 1a beschrieben.

3. Verfahrensbestimmungen

- (1) Für das zwischen Kunde und Bank vereinbarte Übertragungsverfahren gelten die in Anlage 1a sowie die in der Dokumentation der technischen Schnittstelle (Anlage 1b) und der Spezifikation der Datenformate (Anlage 3) beschriebenen Anforderungen.
 - (2) Der Kunde ist verpflichtet sicherzustellen, dass alle Teilnehmer das DFÜ-Verfahren und die Spezifikationen beachten.
 - (3) Die Belegung der Datenfelder richtet sich nach den Belegungs- und Kontrollrichtlinien des jeweils genutzten Formates (Anlage 3).
 - (4) Der Teilnehmer hat die Kundenkennung des Zahlungsempfängers bzw. des Zahlers zutreffend anzugeben.
- Reicht der Teilnehmer eine Datei mit mehreren SEPA-Überweisungen oder SEPA-Echtzeitüberweisungen ein, entscheidet er, ob die Empfängerüberprüfung gemäß dem nach Nummer 4.4 eingefügten Absatz der Bedingungen für den Überweisungsverkehr durchgeführt werden soll.

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

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

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

- (6) Außerdem hat der Kunde für jede Einreichung und jeden Abruf von Dateien ein maschinelles Protokoll, das inhaltlich den Bestimmungen von Kapitel 10 der Spezifikation für die EBICS-Anbindung (Anlage 1b) entspricht, zu erstellen, zu seinen Unterlagen zu nehmen und auf Anforderung der Bank zur Verfügung zu stellen.
- (7) Soweit die Bank dem Kunden Daten über Zahlungsvorgänge zur Verfügung stellt, die noch nicht endgültig bearbeitet sind, stellen diese lediglich eine unverbindliche Information dar. Die Daten sind jeweils besonders gekennzeichnet.

- (8) Die per DFÜ eingeleiteten Auftragsdaten sind wie mit der Bank vereinbart entweder mit Elektronischer Unterschrift oder dem

unterschriebenen Begleitzettel / Sammelauftrag zu autorisieren. Diese Auftragsdaten werden als Auftrag wirksam

- a) bei Einreichung mit Elektronischer Unterschrift, wenn
 - alle erforderlichen Elektronischen Unterschriften der Teilnehmer per Datenfernübertragung innerhalb des vereinbarten Zeitraumes eingegangen sind und
 - die Elektronischen Unterschriften mit den vereinbarten Schlüsseln erfolgreich geprüft werden können oder
 - b) bei Einreichung mit Begleitzettel / Sammelauftrag, wenn
 - der Begleitzettel / Sammelauftrag im vereinbarten Zeitraum bei der Bank eingegangen ist und
 - der Begleitzettel / Sammelauftrag der Kontovollmacht entsprechend unterzeichnet worden ist.
- (9) Wird für eine Datei mit SEPA-Überweisungen oder SEPA Echtzeitüberweisungen die Empfängerüberprüfung gemäß Nummer 3 Absatz 4 durchgeführt, wird die Bank den Teilnehmer über das Ergebnis informieren. Der Teilnehmer entscheidet dann, ob
- die Datei zur Ausführung freigegeben ist oder
 - die Datei nicht ausgeführt werden soll und er stattdessen eine neue Datei mit ausgewählten Überweisungen einreicht und diese zur Ausführung freigibt.

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

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

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

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

Insbesondere Folgendes ist zum Schutz des Legitimationsmediums und des Passwortes zu beachten:

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

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

Der Kunde ist bei Nutzung der ZV-App verpflichtet sicherzustellen, dass alle Teilnehmer das in Anlage 1a beschriebene Sicherungsverfahren einhalten.

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

6. Sicherheit des Kundensystems

Der Kunde hat für einen ausreichenden Schutz der von ihm für die Datenfernübertragung eingesetzten Systeme Sorge zu tragen.

7. Sperre der Legitimations- und Sicherungsmedien

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

gesamten DFÜ-Zugang über die von der Bank bekannt gegebene Sperrfazität sperren lassen.

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

8. Behandlung eingehender Auftragsdaten durch die Bank

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

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

(3) Die Bank prüft die Legitimation des Teilnehmers bzw. der Teilnehmer und die Autorisierung der per DFÜ übermittelten Auftragsdaten anhand der von den Teilnehmern mittels der Legitimationsmedien erstellten elektronischen Unterschriften sowie die Übereinstimmung der Auftragsdatensätze mit den Bestimmungen gemäß Anlage 3. Ergibt die Prüfung Unstimmigkeiten, wird die Bank die betreffenden Auftragsdaten nicht bearbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen. Die Bank ist berechtigt, nicht vollständig autorisierte Auftragsdaten nach Ablauf des von der Bank gesondert mitgeteilten Zeitlimits zu löschen.

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

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

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

9. Rückruf

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

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

10. Ausführung der Aufträge

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

- Die per DFÜ eingelierten Auftragsdaten wurden gemäß Nummer 3 Absatz 8 unter Berücksichtigung von Nummer 3 Absatz 9 autorisiert.
- Das festgelegte Datenformat ist eingehalten.
- Das Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

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

11. Haftung

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

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

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

11.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

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

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

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

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

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

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

11.2.3 Haftung der Bank ab der Sperranzeige

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

Hat der Kunde mit der Bank die „Rahmenvereinbarung über die Teilnahme an elektronischen Dienstleistungen – EBICS und Zahlungsverkehrs-Applikation im Corporates-Portals (ZV-App)“ abgeschlossen und nimmt der Kunde an dieser Rahmenvereinbarung als Verbraucher teil, d.h. zu Zwecken, die überwiegend weder seiner gewerblichen noch seiner selbständigen beruflichen Tätigkeit zugerechnet werden können, so gelten für den Kunden bezüglich Ziffer 11.2.1 abweichende Regelungen. Diese abweichenden Regelungen sind in Ziffer I. Nr. 4 (13) der „Rahmenvereinbarung über die Teilnahme an elektronischen Dienstleistungen – EBICS und Zahlungsverkehrs-Applikation im Corporates-Portal (ZV-App)“ vereinbart.

11.3 Haftungsausschluss

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

12. Schlussbestimmungen

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

Anlage 1a: EBICS-Anbindung

Anlage 1b: Spezifikation der EBICS-Anbindung

Anlage 2: derzeit nicht belegt

Anlage 3: Spezifikation der Datenformate

Anlage 1a:

EBICS-Anbindung

1. Legitimations- und Sicherungsverfahren

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

Folgendes Legitimations- und Sicherungsverfahren wird in der EBICS-Anbindung eingesetzt:

– Elektronische Unterschriften

Für das Legitimations- und Sicherungsverfahren verfügt der Teilnehmer über ein individuelles Schlüsselpaar, das aus einem privaten und einem öffentlichen Schlüssel besteht. Der öffentliche Teilnehmerschlüssel ist der Bank gemäß dem in Nummer 2 beschriebenen Verfahren mitzuteilen. Der öffentliche Bankschlüssel ist gemäß dem in Nummer 2 beschriebenen Verfahren gegen unautorisiertes Verändern zu schützen. Das Schlüsselpaar des Teilnehmers kann auch für die Kommunikation mit anderen Kreditinstituten eingesetzt werden.

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 Teilnehmern (Kontoinhaber und deren Bevollmächtigte) geleistet werden müssen. Für jede unterstützte Auftragsart wird zwischen Bank und Kunde eine Mindestanzahl erforderlicher bankfachlicher EU vereinbart.

EU vom Typ „T“, die als Transportunterschriften bezeichnet werden, werden nicht zur bankfachlichen Freigabe von Aufträgen verwendet, sondern lediglich zu deren Übertragung an die Banksysteme. Mit der ZV-App können verschiedene Nachrichten (z.B. Aufträge für den Inlands- und Auslandszahlungsverkehr, aber auch für Initialisierung, den Protokollabruf und die Abholung von Konto- und Umsatzinformationen etc.) erstellt werden. Die Bank teilt dem Kunden mit, welche Nachrichtenarten genutzt werden können und welcher EU-Typ hierfür anzuwenden ist.

1.2 nicht belegt

1.3 nicht belegt

2. Initialisierung des Teilnehmers in der ZV-App

2.1 Einrichtung der Kommunikationsverbindung

Der Kommunikationsaufbau erfolgt unter Verwendung einer URL (Uniform Resource Locator). Die URL wird dem Kunden bei Vertragsabschluss mit der Bank mitgeteilt.

Die Bank teilt den vom Kunden benannten Teilnehmern zur Aufnahme in die ZV-App folgende Daten mit:

- URL der Bank
- Bezeichnung der Bank
- Partner-ID (Kunden-ID)
- User-ID
- weitere spezifische Angaben zu Kunden- und Teilnehmerberechtigungen

Für die dem Kunden zugeordneten Teilnehmer vergibt die Bank jeweils eine User-ID, die den Teilnehmer eindeutig identifiziert.

2.2 Initialisierung der Teilnehmerschlüssel

Das vom Teilnehmer eingesetzte Schlüsselpaar für die bankfachliche EU muss zusätzlich zu den in Nummer 1 beschriebenen allgemeinen Bedingungen den nachfolgenden Anforderungen genügen:

1. Das Schlüsselpaar ist ausschließlich und eindeutig dem Teilnehmer zugeordnet.
2. Soweit der Teilnehmer seine Schlüssel eigenständig generiert, ist der private Schlüssel mit Mitteln zu erzeugen, die der Teilnehmer unter seiner alleinigen Kontrolle halten kann.
3. Sofern der Schlüssel von einem Dritten zur Verfügung gestellt wird, ist sicherzustellen, dass der Teilnehmer in den alleinigen Besitz des privaten Schlüssels gelangt.
4. Für den zur Legitimation eingesetzten privaten Schlüssel definiert jeder Teilnehmer ein Passwort, das den Zugriff auf den privaten Schlüssel absichert.

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

- über die ZV-App mittels der hierfür vorgesehenen systembedingten Auftragsarten.
- mit dem vom Teilnehmer unterschriebenen Initialisierungsbrief.

Für die Freischaltung des Teilnehmers überprüft die Bank auf Basis des vom Teilnehmer unterschriebenen Initialisierungsbriefts die Authentizität des über die ZV-App übermittelten öffentlichen Teilnehmerschlüssels.

Zu jedem öffentlichen Teilnehmerschlüssel enthält der Initialisierungsbrief die folgenden Daten:

- Verwendungszweck des öffentlichen Teilnehmerschlüssels:
 - Elektronische Unterschrift
- Längenangabe des Exponenten
- Exponent des öffentlichen Schlüssels in hexadezimaler Darstellung
- Längenangabe des Modulus
- Modulus des öffentlichen Schlüssels in hexadezimaler Darstellung
- Hashwert des öffentlichen Schlüssels in hexadezimaler Darstellung

Die Bank prüft die Unterschrift des Kontoinhabers bzw. des Kontobevollmächtigten auf dem Initialisierungsbrief sowie die Übereinstimmung zwischen den über die ZV-App und den schriftlich übermittelten Hashwerten des öffentlichen Schlüssels des Teilnehmers. Bei positivem Prüfergebnis schaltet die Bank den betreffenden Teilnehmer für die vereinbarten Auftragsarten frei.

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

Soweit der Kunde seine Legitimations- und Sicherungsmedien nach den Vorgaben der EBICS-Spezifikation selbst erzeugt und er diese bei seiner Bank initialisiert, hat er Folgendes sicherzustellen:

- In allen Phasen der Authentifizierung, inklusive Anzeige, Übermittlung und Speicherung sind Vertraulichkeit und Integrität des Legitimationsmediums zu gewährleisten
- Der private Teilnehmerschlüssel darf auf den Legitimations- und Sicherungsmedien nicht im Klartext abgespeichert werden.
- Spätestens nach fünfmaliger Fehleingabe des Passwortes wird das Legitimationsmedium gesperrt.
- Die Generierung des privaten und öffentlichen Teilnehmerschlüssels muss in einer sicheren Umgebung erfolgen.
- Die Legitimations- und Sicherungsmedien sind ausschließlich und eindeutig dem Teilnehmer zuzuordnen und zu verwenden.

4. Auftragserteilung an die Bank

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

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

1. Alle erforderlichen bankfachlichen EU werden zusammen mit den Auftragsdaten übertragen.
2. Sofern mit dem Kunden für die jeweilige Auftragsart die Verteilte Elektronische Unterschrift (VEU) vereinbart wurde und die übermittelten EU für die bankfachliche Freigabe nicht ausreichen, wird der Auftrag bis zur Abgabe aller erforderlichen EU im Banksystem gespeichert.
3. Soweit Kunde und Bank vereinbaren, dass die Autorisierung von per DFÜ übermittelten Auftragsdaten mittels gesondert übermittelten Begleitzettels / Sammelauftrags erfolgen kann, ist anstelle der bankfachlichen EU des Teilnehmer 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 Teilnehmers auf dem Begleitzettel / Sammelauftrag durch die Bank.

4.1 Auftragserteilung mittels Verteilter Elektronischer Unterschrift (VEU)

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

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

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

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

4.2 Legitimationsprüfung durch die Bank

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

4.3 Kundenprotokolle

Die Bank dokumentiert in Kundenprotokollen die folgenden Vorgänge:

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

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

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

5. Änderung der Teilnehmerschlüssel mit automatischer Freischaltung

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

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

Für eine automatische Freischaltung der neuen Schlüssel ohne eine erneute Teilnehmerinitialisierung ist die folgende Auftragsart zu nutzen:

- Aktualisierung des öffentlichen bankfachlichen Schlüssels (PUB)

Die Auftragsart PUB ist hierfür mit einer gültigen bankfachlichen EU des Teilnehmers zu versehen. Nach erfolgreicher Änderung ist nur noch der neue Schlüssel zu verwenden.

Wenn die Elektronische Unterschrift nicht erfolgreich geprüft werden konnte, wird wie unter Nummer 8 Absatz 3 der Bedingungen für die Datenfernübertragung – ZV-App 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 des Teilnehmerschlüssels

Besteht der Verdacht des Missbrauchs des Teilnehmerschlüssels, 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 ZV-App 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 ZV-App mehr erteilt werden.

Wenn der Teilnehmer nicht mehr über gültige Legitimations- und Sicherungsmedien verfügt, kann er außerhalb des DFÜ-Verfahrens seine Legitimations- und Sicherungsmedien über die von der Bank gesondert bekannt gegebene Sperrfazilität sperren lassen.

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

Anlage 1b:

Spezifikation der EBICS-Anbindung

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

Anlage 2:

Derzeit nicht belegt.

Anlage 3:

Spezifikation der Datenformate

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