

Sonderbedingungen für Datenfernübertragung (DFÜ)

I. Leistungsumfang

- (1) Das Kreditinstitut steht seinem Kunden für die Datenübertragung auf elektronischem Wege – Datenfernübertragung (DFÜ) – zur Verfügung.
- (2) Es gibt dem Kunden die Dienstleistungsarten bekannt, die er im Rahmen der DFÜ nutzen kann. Sofern das Kreditinstitut für Verfügungen mittels DFÜ eine Betragsbegrenzung im System vorsieht, informiert es ihn hierüber.

II. Identifikations- und Legitimationsmedien, Nutzungsberechtigte

Zur Abwicklung von Bankgeschäften verwenden Kontoinhaber und etwaige Bevollmächtigte jeweils individuelle Identifikations- und Legitimationsmedien. Kontoinhaber und Bevollmächtigte werden im Folgenden einheitlich als Nutzer bezeichnet.

III. Allgemeine Verfahrensbestimmungen

(1) Der Nutzer ist verpflichtet, die mit dem Kreditinstitut vereinbarten Übertragungs- und Sicherungsverfahren einzusetzen sowie die vereinbarten Schnittstellen zu beachten. Näheres regelt Anlage 1.

(2) Die Datensätze des Nutzers müssen in Satz- und Dateiaufbau den Angaben gemäß Anlage 2 entsprechen.

(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 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 in Datenfeld Verwendungszweck des Datensatzes sowie in den etwaigen nachfolgenden Erweiterungen 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 Übertragung von Datensätzen an das Kreditinstitut 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 Nutzer mindestens für einen Zeitraum von 14 Kalendertagen bei Inlandszahlungsaufträgen und 30 Kalendertagen bei Auslandszahlungsaufträgen ab dem Tage der Übermittlung in der Form nachweisbar zu halten, dass die Datei auf Anforderung des Kreditinstitutes kurzfristig erneut zur Verfügung gestellt werden kann, sofern nichts Abweichendes vereinbart wird.

(5) Außerdem hat der Nutzer für jede logische Datei ein maschinelles Protokoll, das inhaltlich den Bestimmungen der Anlage 3 entspricht, zu erstellen, zu seinen Unterlagen zu nehmen und auf Anforderung des Kreditinstitutes zur Verfügung zu stellen.

(6) Soweit das Kreditinstitut dem Nutzer 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. Legitimationsverfahren/Geheimhaltung

(1) Der Nutzer ist verpflichtet, die mit dem Kreditinstitut vereinbarten Sicherungsmaßnahmen gemäß Anlage 1 durchzuführen.

(2) Mithilfe der mit dem Kreditinstitut vereinbarten Medien identifiziert und legitimiert sich der Nutzer gegenüber dem Kreditinstitut. Der Nutzer hat dafür Sorge zu tragen, dass kein unberechtigter Dritter in den Besitz der Identifikations- und Legitimationsmedien kommt, sowie Kenntnis von dem zu deren Schutz dienenden Passwortes erlangt. Denn jede Person, die im Besitz der Medien oder eines entsprechenden Duplikates ist, kann die vereinbarten Dienstleistungen nutzen. Insbesondere Folgendes ist zur Geheimhaltung der Identifikations- und Legitimationsmedien zu beachten:

- Die den Nutzer identifizierenden Daten dürfen nicht außerhalb der Sicherheitsmedien, z. B. auf der Festplatte des Rechners, gespeichert werden;
- die Identifikations- und Legitimationsmedien sind nach Beendigung der DFÜ-Nutzung aus dem Lesegerät zu entnehmen und sicher zu verwahren;
- das zum Schutz der Identifikations- und Legitimationsmedien dienende Passwort darf nicht notiert oder elektronisch abgespeichert werden;
- bei Eingabe des Passwortes ist sicherzustellen, dass Dritte dieses nicht ausspähen können.

V. Zugangssperre

(1) Gehen die zur Legitimation und Sicherung dienenden Medien verloren, werden sie anderen Personen bekannt oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so hat der Nutzer unverzüglich den Zugang durch das Kreditinstitut sperren zu lassen. Näheres regelt Anlage 1.

(2) Hat der Nutzer seinem Kreditinstitut eine Sperre übermittelt, so haftet das Kreditinstitut ab dem Zugang der Spermachricht für alle Schäden, die aus ihrer Nichtbeachtung entstehen.

(3) Werden dreimal hintereinander Aufträge mit falscher elektronischer Signatur an das Kreditinstitut übermittelt, so sperrt das Kreditinstitut den DFÜ-Zugang zum Konto/Depot. In diesem Fall sollte sich der Nutzer mit dem Kreditinstitut in Verbindung setzen.

(4) Das Kreditinstitut wird den DFÜ-Zugang zum Konto/Depot sperren, wenn der Verdacht einer missbräuchlichen Nutzung des Kontos/Depots über DFÜ besteht. Sie wird den Kontoinhaber hierüber außerhalb des DFÜ-Verfahrens informieren. Diese Sperre kann mittels DFÜ nicht aufgehoben werden.

VI. Behandlung der vom Nutzer übermittelten Daten durch das Kreditinstitut

(1) Die dem Kreditinstitut im DFÜ-Verfahren erteilten Aufträge werden im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeitet.

(2) Das Kreditinstitut prüft die Legitimation des Absenders sowie die Übereinstimmung der Auftragsdatensätze mit den Bestimmungen gemäß Anlage 2.

(3) Ergibt die Legitimationsprüfung Unstimmigkeiten, wird das Kreditinstitut die betreffende Datei nicht bearbeiten und dem Nutzer hierüber unverzüglich eine Information zur Verfügung stellen. Näheres regelt Anlage 1.

(4) Ergeben sich bei den von dem Kreditinstitut durchgeführten Prüfungen der Datensätze nach Abs. 2 Fehler, so wird das Kreditinstitut die fehlerhaften Datensätze mit ihrem vollständigen Inhalt nachweisen und sie dem Nutzer unverzüglich mitteilen. Das Kreditinstitut ist berechtigt, die fehlerhaften Datensätze von der weiteren Bearbeitung auszuschließen, wenn die ordnungsgemäße Ausführung des Auftrages nicht sichergestellt werden kann.

VII. Rückruf

(1) Der Rückruf einer Datei ist ausgeschlossen, sobald das Kreditinstitut mit deren Bearbeitung begonnen hat. Das Kreditinstitut kann einen Rückruf allerdings nur beachten, wenn ihm diese Nachricht so rechtzeitig zugeht, dass ihre Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufes möglich ist. Änderungen eines Dateiinhaltes sind nur durch Rückruf und Neuübermittlung der Datei möglich.

(2) Der Rückruf von einzelnen Aufträgen aus Dateien kann nur außerhalb des DFÜ-Verfahrens erfolgen, es sei denn, das Kreditinstitut sieht eine solche Möglichkeit innerhalb des Verfahrens vor. Der Nutzer muss dem Kreditinstitut hierzu die Einzelangaben des Originalauftrages zur Bankleitzahl des Kreditinstitutes des Begünstigten/der Zahlstelle (im Auslandszahlungsverkehr ggf. Bank Identification Code – BIC), zu Kontonummer (im Auslandszahlungsverkehr ggf. International Bank Account Number – IBAN) und Namen des Begünstigten/Zahlungspflichtigen, zum Textschlüssel/Textschlüsselergänzung, zum Betrag, zur Bankleitzahl des überweisenden Kreditinstitutes/der ersten Inkassostelle und zu Kontonummer und Namen des Überweisenden/Zahlungsempfängers sowie inhaltlich auch die Angaben im Datenfeld Verwendungszweck des Datensatzes entsprechend der Anlage 2 mitteilen.

VIII. Schlussbestimmungen

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

Anlage 1: Sicherungs- und Übertragungsverfahren, Sicherungsmaßnahmen, Legitimationsverfahren und Zugangssperre

Anlage 2: Datenformate (Satz- und Dateiaufbau, Spezifikationen)

Anlage 3: Maschinelles Protokoll zur Übertragung von Dateien

Auf den Abdruck der Anlage 2+3 wurde verzichtet, da die darin enthaltenen technischen Angaben bereits in dem von Ihrer Volksbank/Raiffeisenbank angebotenen Programm umgesetzt worden sind.

Anlage 1: Sicherungs- und Übertragungsverfahren, Sicherungsmaßnahmen, Legitimationsverfahren und Zugangssperre

1 Sicherungs- und Übertragungsverfahren

Bei der Datenübertragung zwischen Nutzer (Kontoinhaber und etwaigen Bevollmächtigten) und Kreditinstitut sind die für das deutsche Kreditgewerbe geltenden Schnittstellen für Datenübertragung, Sicherheit sowie Datenformate auf Anwendungsebene einzuhalten. Die Dokumentation dieser Schnittstelle ist beim Kreditinstitut erhältlich.

Es werden das Übertragungsprotokoll FTAM und das Sicherungsverfahren der Elektronischen Unterschrift (EU) verwendet.

Mit dem vom Nutzer verwendeten Programm können verschiedene Nachrichten (z. B. Aufträge für den Inlands- und Auslandszahlungsverkehr, aber auch für die Initialisierung, den Protokollabruf und die Abholung von Konto- und Umsatzinformationen etc.) erstellt werden. Das Kreditinstitut teilt dem Kontoinhaber mit, welche Nachrichtenarten genutzt werden können und welche mit Elektronischer Unterschrift zu übermitteln sind.

Der Kontoinhaber kann mit dem Kreditinstitut vereinbaren, ob eine EU-pflichtige Nachricht eine oder mehrere Elektronische Unterschriften tragen muss.

Im Rahmen des Elektronischen Unterschriftenverfahrens wird mit einem Schlüsselpaar gearbeitet, das jeder Nutzer für sich selbst generiert. Das Schlüsselpaar besteht aus einem Private Key und einem Public Key.

Der Private Key dient der Erzeugung der Elektronischen Unterschrift und damit zur Autorisierung von Aufträgen des Kontoinhabers gegenüber dem Kreditinstitut durch den jeweiligen Nutzer. Der Private Key verbleibt beim Nutzer und ist sicher vor Zugriff Unbefugter aufzubewahren.

Der Public Key dient der Prüfung der Elektronischen Unterschrift aufseiten des Kreditinstitutes. Identische Keys können auch für die Kommunikation mit anderen Kreditinstituten eingesetzt werden.

2 Legitimationsverfahren

2.1 Initialisierung

Das Kreditinstitut teilt dem Kontoinhaber die zur Aufnahme einer Verbindung über Datenfernübertragung (DFÜ) erforderlichen Daten mit. Dabei handelt es sich um:

- Kunden-ID
- Hostname
- Datex-P NUA oder ISDN-NUA
- Host-Typ
- User-ID
- Erstes DFÜ-Passwort

Der Kontoinhaber erstellt mit diesen Angaben eine Bankparameterdatei für das Kreditinstitut, sofern ihm diese nicht durch sein Kreditinstitut zur Verfügung gestellt wird. Der Kontoinhaber definiert pro Auftragsart die erforderliche Mindestanzahl von Elektronischen Unterschriften.

Jeder Nutzer mit entsprechender Berechtigung generiert sein Schlüsselpaar für die Leistung der Elektronischen Unterschrift.

Bei der Erzeugung des Schlüsselpaares definiert jeder Nutzer ein EU-Passwort, das den Zugriff auf den Private Key (z. B. auf Diskette oder Chipkarte) absichert.

Jeder Nutzer führt in seinem Programm eine Funktion zur Änderung des DFÜ-Passwortes („PWA“) aus. Mit der Auftragsart „INI“ bzw. „PUB“ übermittelt der Nutzer per DFÜ eine Datei mit dem geänderten DFÜ-Passwort und dem Public Key seines Schlüsselpaares an das Kreditinstitut.

Das vom Nutzer verwendete Programm erstellt ein Initialisierungsprotokoll, das u. a. den Public Key des Nutzers enthält. Der Nutzer unterschreibt dieses Protokoll mit seiner händischen Unterschrift und sendet das unterschriebene Initialisierungsprotokoll an das Kreditinstitut.

Das Kreditinstitut prüft die händische Unterschrift auf dem Initialisierungsprotokoll sowie die Übereinstimmung zwischen dem über Leitung und dem schriftlich übermittelten Public Key des Nutzers. Bei positivem Prüfergebnis schaltet das Kreditinstitut den betreffenden Nutzer für die vereinbarten Auftragsarten frei.

Zur Änderung seines Schlüsselpaares führt der Nutzer die nachstehenden Schritte durch:

- Erzeugung eines neuen Schlüsselpaares.
- Übermittlung des Public Keys dieses Schlüsselpaares an das Kreditinstitut unter Verwendung der Auftragsart „PUB“.
- Händisches Unterschreiben des von seinem Programm neu erstellten Initialisierungsprotokolls.
- Übermittlung dieses unterschriebenen Initialisierungsprotokolls an das Kreditinstitut.

Bei der Schlüsseländerung sind die unter Nummer 4 genannten Hinweise zu beachten.

2.2 Abfrage von Informationen bei dem Kreditinstitut

Für die Abfrage von Informationen bei dem Kreditinstitut sind die gewünschten Abholaufträge zu erstellen und an das Kreditinstitut zu übermitteln. Hierzu ist das entsprechende DFÜ-Passwort des Nutzers einzugeben.

2.3 Auftragserteilung an das Kreditinstitut

Der Nutzer überprüft die zu unterschreibenden Dateien auf Richtigkeit.

Der Nutzer erzeugt eine Elektronische Unterschrift mithilfe seines Speichermediums (z. B. Diskette oder Chipkarte), das seinen Private Key enthält, und seines EU-Passwortes. Zu jeder Datei mit Aufträgen werden entsprechend der Vereinbarung mit dem Kreditinstitut eine oder mehrere Elektronische Unterschriften erzeugt.

Aufträge und zugehörige Elektronische Unterschrift(en) befinden sich in je einer Datei, die gemeinsam oder getrennt an das Kreditinstitut übertragen werden können.

Der Nutzer gibt zur Übertragung der Dateien sein DFÜ-Passwort ein.

Die Aufträge sind gegenüber dem Kreditinstitut erst dann erteilt, wenn zusätzlich zur Datei mit den Auftragsdaten (z. B. Zahlungsverkehrsauftrag) auch eine entsprechende Unterschriftdatei – ggf. zu einem von der Übermittlung der Auftragsdatei abweichenden Zeitpunkt – übertragen wurde.

3 Legitimationsprüfung

Eine empfangende Auftragsdatei wird durch das Kreditinstitut erst dann ausgeführt, wenn die erforderliche Anzahl von Elektronischen Unterschriften eingegangen ist und mit den jeweiligen Public Keys der entsprechenden Nutzer mit positivem Ergebnis geprüft wurde.

Das Kreditinstitut stellt das Ergebnis der Legitimationsprüfung im Kundenprotokoll bereit. Je Aktion aufseiten des Kreditinstitutes sind in dieser Datei u. a. Datum und Uhrzeit, Art der Aktion, Auftragsart, User-ID, Auftragsnummer, Ergebnis der Aktion, Dateiname auf dem Kundensystem sowie Angaben zur Auftragsdatei enthalten.

Durch Abruf der Protokolldatei kann sich der Nutzer über das Ergebnis der aufseiten des Kreditinstitutes durchgeführten Prüfungen informieren. Hierzu sendet er einen Auftrag mit der Auftragsart „PTK“ („Abholen Protokolldatei“) an das Institut.

4 Schlüsseländerungen und Sperrmöglichkeiten

4.1 Schlüsseländerungen

Der Nutzer kann per DFÜ durch Übermittlung eines neuen Public Keys (Auftragsart „PUB“) sein bisheriges Schlüsselpaar sperren. Das neue Schlüsselpaar wird erst nach Eingang des hierzu erstellten entsprechenden Initialisierungsprotokolls (Ini-Briefs) bei dem Kreditinstitut freigeschaltet.

Jede Übermittlung eines Public Keys (auch des dem Kreditinstitut schon bekannten) führt aus Sicherheitsgründen so lange zur Sperrung aller Aufträge, die der Elektronischen Unterschrift bedürfen, bis das zugehörige händisch unterschriebene Initialisierungsprotokoll dem Kreditinstitut vorliegt und der neue Public Key nach Prüfung von dem Kreditinstitut zur Nutzung freigeschaltet wurde.

Für den dazwischen liegenden Zeitraum, der unter Einfluss der Postlaufzeit durchaus mehrere Tage betragen kann, ist daher bei Bedarf mit dem Kreditinstitut ein anderes Sicherungsverfahren für die Auftragslegitimierung (Ersatzverfahren) zu vereinbaren.

Die durch die Übermittlung des neuen Public Keys veranlasste Sperrung aller der Elektronischen Unterschrift bedürftenden Aufträge wirkt sich auch auf die Aufträge aus, die noch unter Verwendung des alten Public Key legitimiert wurden,

- für die die Prüfung der Elektronischen Unterschrift kreditinstitutsseitig noch nicht abgeschlossen wurde oder
- die bis zu diesem Zeitpunkt noch nicht an das Kreditinstitut übermittelt wurden.

Um eine ungewollte Nichtausführung der bereits an das Kreditinstitut übermittelten Aufträge zu vermeiden, ist durch Abholung des von dem Kreditinstitut bereitgestellten Kundenprotokolls der Ausführungsstatus dieser Aufträge zu überprüfen.

Aufträge, zu denen die EU-Prüfung kreditinstitutsseitig erst nach der DFÜ-Übermittlung des neuen Public Keys durchgeführt wurde, erhalten in diesem Kundenprotokoll den Eintrag „Unterschrift ist falsch“ und werden daher nicht ausgeführt.

Diese Aufträge sind daher – sofern deren Ausführung gewünscht wird – komplett neu zu erteilen.

Nach kreditinstitutsseitiger Freischaltung des neuen Public Keys sind Aufträge, die noch nicht an das Kreditinstitut übertragen wurden, mit dem neuen EU-Schlüsselpaar neu zu legitimieren und dem Kreditinstitut zu übermitteln.

4.2 Sperrung des gesamten Zuganges per DFÜ

Durch Senden einer Nachricht mit der Auftragsart „SPR“ (Sperrung der Zugangsberechtigung) kann der Nutzer den Zugang insgesamt, d. h. auch die Zugangsberechtigung der anderen Nutzer, sperren.

Nach einer Sperre können bis zur Neuinitialisierung mit einem neuen Schlüssel keine Aufträge per DFÜ mehr erteilt werden. Es muss hierzu der unter Nummer 2.1 genannte Initialisierungsprozess vollständig wiederholt werden.

4.3 Sperrmöglichkeiten außerhalb der DFÜ

Der Kontoinhaber kann außerhalb der DFÜ mit seinem Kreditinstitut die vollständige oder teilweise (z. B. einzelne Nachrichtenarten, einzelne Schlüsselpaare, Elektronische Unterschrift generell) Sperrung der Nutzungsmöglichkeiten für die DFÜ vereinbaren.