COMMERZBANK
Die Bank an Ihrer Seite

Bedingungen für die Datenfernübertragung

Gegenüberstellung der geänderten Bedingungen
Commerzbank AG Niederlassung Wien, Österreich

Stand: Februar 2017	Stand: Juni 2018
1. Leistungsumfang	**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 Auftragserteilung sowie den Datenaustausch (Übermittlung von Aufträgen und Informationsabruf).	(1) Die Bank steht ihrem Kunden (Kontoinhaber, der Nicht-Verbraucher im Sinne des ZaDiG 2018 ist), für die Datenfernübertragung auf elektronischem Wege – nachfolgend „Datenfernübertragung“ oder „DFÜ“ genannt – zur Verfügung. Die Datenfernübertragung umfasst die Auftragserteilung sowie den Datenaustausch (Übermittlung von Aufträgen und Informationsabruf).
(2) Die Bank gibt dem Kunden die Dienstleistungsarten bekannt, die er im Rahmen der Datenfernübertragung nutzen kann. Zur Nutzung der Datenfernübertragung gelten die mit der Bank vereinbarten Verfügungslimits.	(2) Die Bank gibt dem Kunden die Dienstleistungsarten bekannt, die er im Rahmen der Datenfernübertragung nutzen kann. Zur Nutzung der Datenfernübertragung gelten die mit der Bank vereinbarten Verfügungslimite.
2. Nutzer und Teilnehmer, Legitimations– und Sicherungsmedien	**2. Nutzer und Teilnehmer, Legitimations– und Sicherungsmedien**
(3) Legitimations– und Sicherungsmedien sind Authentifizierungsinstrumente im Sinne von § 3 Z 17 ZaDiG.	~~(3)~~ *(entfällt)* ~~Legitimations– und Sicherungsmedien sind Authentifizierungsinstrumente im Sinne von § 3 Z 17 ZaDiG.~~
3. Verfahrensbestimmungen	**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. Der Kunde ist verpflichtet, Überweisungsaufträge und Lastschrifteinzugsaufträge für Zahlungen in Euro innerhalb des Europäischen Wirtschaftsraums nur noch im Format ISO 20022 gemäß Kapitel 2 der Anlage 3 einzureichen. Lastschrifteinzugsaufträge für Zahlungen, die an einer Verkaufsstelle mithilfe einer Zahlungskarte generiert wurden und zu einer Lastschrift von einem inländischen Zahlungskonto führen (§ 3 Z 13 ZaDiG) verpflichtend im Format ISO 20022 einzureichen.	(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. ~~Der Kunde ist verpflichtet, Überweisungsaufträge und Lastschrifteinzugsaufträge für Zahlungen in Euro innerhalb des Europäischen Wirtschaftsraums nur noch im Format ISO 20022 gemäß Kapitel 2 der Anlage 3 einzureichen. Lastschrifteinzugsaufträge für Zahlungen, die an einer Verkaufsstelle mithilfe einer Zahlungskarte generiert wurden und zu einer Lastschrift von einem inländischen Zahlungskonto führen (§ 3 Z 13 ZaDiG) verpflichtend im Format ISO 20022 einzureichen.~~
(4) Der Nutzer hat den Kontoidentifikationscode (Kontonummer oder IBAN) des Zahlungsempfängers bzw. des Zahlers und – soweit diese Angabe erforderlich ist – den Zahlungsdienstleisteridentifikationscode (Bankleitzahl oder BIC) des Zahlungsdienstleisters des Zahlungsempfängers bzw. des Zahlungsdienstleisters des Zahlers (Zahlstelle) zutreffend anzugeben. Die in die Abwicklung des Zahlungsauftrags eingeschalteten Zahlungsdienstleister sind berechtigt, die Bearbeitung ausschließlich anhand des Kontoidentifikationscodes und – soweit diese Angabe vorhanden ist – des Zahlungsdienstleisteridentifikationscodes vorzunehmen. Fehlerhafte Angaben können Fehlleitungen des Auftrags zur Folge haben. Schäden und Nachteile, die hieraus entstehen, gehen zulasten des Kunden. Die Regelung gilt entsprechend, wenn per Datenfernübertragung andere Aufträge (keine Zahlungsaufträge) übermittelt werden.	(4) Der Nutzer hat ~~den Kontoidentifikationscode (Kontonummer oder IBAN)~~ die Kundenkennung des Zahlungsempfängers bzw. des Zahlers ~~und – soweit diese Angabe erforderlich ist – den Zahlungsdienstleisteridentifikationscode (Bankleitzahl oder BIC) des Zahlungsdienstleisters des Zahlungsempfängers bzw. des Zahlungsdienstleisters des Zahlers (Zahlstelle)~~ gemäß den allgemeinen Geschäftsbedingungen (AGB) zutreffend anzugeben. Die in die Abwicklung des Zahlungsauftrags eingeschalteten Zahlungsdienstleister sind berechtigt, die Bearbeitung ausschließlich anhand ~~des Kontoidentifikationscodes und – soweit diese Angabe vorhanden ist – des Zahlungsdienstleisteridentifikationscodes~~ der Kundenkennung vorzunehmen. Fehlerhafte Angaben können Fehlleitungen des Auftrags zur Folge haben. Schäden und Nachteile, die hieraus entstehen, gehen zulasten des Kunden. Die Regelung gilt entsprechend, wenn per Datenfernübertragung andere Aufträge (keine Zahlungsaufträge) übermittelt werden.

(5) Vor Übertragung von Auftragsdaten an die Bank ist eine Aufzeichnung der zu übertragenden Dateien mit deren vollständigem Inhalt sowie der zur Prüfung der Legitimation übermittelten Daten zu erstellen. Diese ist von dem Kunden mindestens für einen Zeitraum von 30 Kalendertagen ab dem Ausführungstag in der Form nachweisbar zu halten, dass die Datei auf Anforderung der Bank kurzfristig erneut zur Verfügung gestellt werden kann, sofern nichts Abweichendes vereinbart wird.	(5) Vor Übertragung von Auftragsdaten an die Bank ist eine Aufzeichnung der zu übertragenden Dateien mit deren vollständigem Inhalt sowie der zur Prüfung der Legitimation übermittelten Daten zu erstellen. Diese ist von dem Kunden mindestens für einen Zeitraum von 30 Kalendertagen ab dem ~~Ausführungstag~~ 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.
4. Verhaltens– und Sorgfaltspflichten im Umgang mit den Legitimationsmedien für die Autorisierung des Auftrags (2) Mithilfe der von der Bank freigeschalteten Legitimationsmedien kann der Nutzer Aufträge erteilen. Der Kunde stellt sicher, dass jeder Nutzer dafür Sorge trägt, dass keine andere Person in den Besitz seines Legitimationsmediums kommt oder Kenntnis von dem zu dessen Schutz dienenden Passwort erlangt. Denn jede andere Person, die im Besitz des Mediums oder eines entsprechenden Duplikats ist, kann in Verbindung mit dem dazugehörigen Passwort die vereinbarten Dienstleistungen missbräuchlich nutzen. Insbesondere Folgendes ist zur Geheimhaltung der Legitimationsmedien zu beachten: • Die den Nutzer legitimierenden Daten dürfen nicht außerhalb des Legitimationsmediums, z. B. auf der Festplatte des Rechners, gespeichert werden. • Das Legitimationsmedium ist nach Beendigung der DFÜ–Nutzung 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 Passworts ist sicherzustellen, dass andere Personen dieses nicht ausspähen können. Der Kunde beauftragt die Bank mit der Speicherung des persönlichen Schlüssels des Teilnehmers/Nutzers in einer technischen Umgebung, die vor unautorisiertem Zugriff geschützt ist. Die Bank ist berechtigt, hierfür auch einen zuverlässigen Dienstleister zu beauftragen. Das zur Freigabe des persönlichen Schlüssels erforderliche Kennwort wird durch eine TAN im photoTAN–Verfahren ersetzt. Die Aufbewahrung der elektronischen Schlüssel ist in einer von der Bank (oder von einem von der Bank zugelassenen Dienstleister) zur Verfügung gestellten technischen Umgebung (vgl. Ziffer 2.2.1 (5) der Anlage 1a der Bedingungen für die Datenfernübertragung) erlaubt.	**4. Verhaltens– und Sorgfaltspflichten im Umgang mit den Legitimationsmedien für die Autorisierung des Auftrags** (2) Mithilfe der von der Bank freigeschalteten Legitimationsmedien kann der Nutzer Aufträge erteilen. Der Kunde stellt sicher, dass jeder Nutzer dafür Sorge trägt, dass keine andere Person in den Besitz seines Legitimationsmediums kommt oder Kenntnis von dem zu dessen Schutz dienenden Passwort erlangt. Denn jede andere Person, die im Besitz des Mediums oder eines entsprechenden Duplikats ist, kann in Verbindung mit dem dazugehörigen Passwort die vereinbarten Dienstleistungen missbräuchlich nutzen. Insbesondere Folgendes ist zur Geheimhaltung der Legitimationsmedien zu beachten: • Die den Nutzer legitimierenden Daten ~~dürfen nicht außerhalb des Legitimationsmediums, z. B. auf der Festplatte des Rechners, gespeichert~~ müssen vor unberechtigtem Zugriff geschützt und sicher verwahrt werden. • *(entfällt)* ~~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 Passworts ist sicherzustellen, dass andere Personen dieses nicht ausspähen können. *(entfällt)* ~~Der Kunde beauftragt die Bank mit der Speicherung des persönlichen Schlüssels des Teilnehmers/Nutzers in einer technischen Umgebung, die vor unautorisiertem Zugriff geschützt ist. Die Bank ist berechtigt, hierfür auch einen zuverlässigen Dienstleister zu beauftragen. Das zur Freigabe des persönlichen Schlüssels erforderliche Kennwort wird durch eine TAN im photoTAN–Verfahren ersetzt.~~ ~~Die Aufbewahrung der elektronischen Schlüssel ist in einer von der Bank (oder von einem von der Bank zugelassenen Dienstleister) zur Verfügung gestellten technischen Umgebung (vgl. Ziffer 2.2.1 (5) der Anlage 1a der Bedingungen für die Datenfernübertragung) erlaubt.~~
8. Rückruf (2) Die Widerrufbarkeit eines Auftrags richtet sich nach den dafür geltenden Sonderbedingungen (z. B. Bedingungen für Zahlungsdienste). Der Widerruf von Aufträgen kann nur außerhalb des DFÜ–Verfahrens erfolgen. Hierzu hat der Kunde der Bank die Einzelangaben des Originalauftrags mitzuteilen.	**8. Rückruf** (2) Die Widerrufbarkeit eines Auftrags richtet sich nach den dafür geltenden ~~Sonderb~~Bedingungen (z. B. ~~Bedingungen für Zahlungsdienste~~ allgemeine Geschäftsbedingungen). 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 Originalauftrags mitzuteilen.

11. Haftung **11.1 Haftung der Bank bei nicht autorisierten Aufträgen und nicht oder fehlerhaft ausgeführten Aufträgen** Die Haftung der Bank bei nicht autorisierten Aufträgen und nicht oder fehlerhaft ausgeführten Aufträgen richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Bedingungen für Zahlungsdienste).	**11. Haftung** **11.1 Haftung der Bank bei nicht autorisierten Aufträgen und einer nicht, ~~oder~~ fehlerhaft oder verspätet ausgeführten ~~Aufträgen~~ DFÜ-Verfügung** Die Haftung der Bank bei einer nicht autorisierten ~~Aufträgen~~ DFÜ-Verfügung und einer nicht ~~oder~~, fehlerhaft oder verspätet ausgeführten ~~Aufträgen~~ DFÜ-Verfügung richtet sich nach den ~~für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Bedingungen für Zahlungsdienste)~~ allgemeinen Geschäftsbedingungen.
11.2 Haftung des Kunden bei missbräuchlicher Nutzung Legitimations– oder Sicherungsmedien **11.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige** (1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen, oder sonst abhanden gekommenen oder auf der sonstigen missbräuchlichen Nutzung eines Legitimations– oder Sicherungsmediums, haftet der Kunde für den der Bank hierdurch entstehenden Schaden, wenn den Teilnehmer an dem Verlust, Diebstahl, sonstigen Abhandenkommen oder der sonstigen missbräuchlichen Nutzung seines Legitimations– oder Sicherungsmediums ein Verschulden trifft. Der Kunde haftet auch, wenn er einen von ihm benannten Teilnehmer nicht sorgfältig ausgesucht und/oder die Beachtung der Verpflichtungen des Teilnehmers nach diesen Bedingungen nicht regelmäßig überprüft hat. Hat die Bank durch ein schuldhaftes Verhalten zu der Entstehung eines Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang Kunde und Bank den Schaden zu tragen haben. (2) Der Kunde ist nicht zum Ersatz des Schadens nach den Absätzen 1 und 2 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 6 Absatz 1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist. (3) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.	**11.2 Haftung des Kunden bei missbräuchlicher Nutzung Legitimations– oder Sicherungsmedien** **11.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige** (1) Die Regelungen des § 68 (2), (5) und (6) ZaDiG 2018 werden abbedungen. Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen, oder sonst abhanden gekommenen oder auf der sonstigen missbräuchlichen Nutzung eines Legitimations– oder Sicherungsmediums, haftet der Kunde für den der Bank hierdurch entstehenden gesamten Schaden, wenn den Teilnehmer an dem Verlust, Diebstahl, sonstigen Abhandenkommen oder der sonstigen missbräuchlichen Nutzung seines Legitimations– oder Sicherungsmediums ein Verschulden trifft. Der Kunde haftet auch, wenn er einen von ihm benannten Teilnehmer nicht sorgfältig ausgesucht und/oder die Beachtung der Verpflichtungen des Teilnehmers nach diesen Bedingungen nicht regelmäßig überprüft hat. Hat die Bank durch ein schuldhaftes Verhalten zu der Entstehung eines Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang Kunde und Bank den Schaden zu tragen haben. (2) Der Kunde ist nicht zum Ersatz des Schadens nach ~~den Absätzen~~dem Absatz 1 ~~und 2~~ verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 6 Absatz 1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist. (3) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit. (4) *(neu)* Absatz (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 Beruhen nicht autorisierte Vorgänge, die keine Zahlungsvorgänge sind, vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhandengekommenen oder auf der sonstigen missbräuchlichen Nutzung eines Legitimations– oder Sicherungsmediums, haftet der Kunde für den der Bank hierdurch entstehenden Schaden, wenn den Teilnehmer an dem Verlust, Diebstahl, sonstigen Abhandenkommen oder der sonstigen missbräuchlichen Nutzung seines Legitimations– oder Sicherungsmediums ein Verschulden trifft. Der Kunde haftet auch, wenn er einen von ihm benannten Teilnehmer nicht sorgfältig ausgesucht und/oder die Beachtung der Verpflichtungen des Teilnehmers nach diesen Bedingungen nicht regelmäßig überprüft hat.	**11.2.2. Haftung des Kunden bei sonstigen nicht autorisierten Vorgängen vor der Sperranzeige** Die Regelungen des § 68 (2), (5) und (6) ZaDiG 2018 werden abbedungen. Beruhen nicht autorisierte Vorgänge, die keine Zahlungsvorgänge sind, vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhandengekommenen oder auf der sonstigen missbräuchlichen Nutzung eines Legitimations– oder Sicherungsmediums, haftet der Kunde für den der Bank hierdurch entstehenden gesamten Schaden, wenn den Teilnehmer an dem Verlust, Diebstahl, sonstigen Abhandenkommen oder der sonstigen missbräuchlichen Nutzung seines Legitimations– oder Sicherungsmediums ein Verschulden trifft. Der Kunde haftet auch, wenn er einen von ihm benannten Teilnehmer nicht sorgfältig ausgesucht und/oder die Beachtung der Verpflichtungen des Teilnehmers nach diesen Bedingungen nicht regelmäßig überprüft hat. Hat die Bank durch ein schuldhaftes Verhalten zu der Entstehung eines Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang Kunde und Bank den Schaden zu tragen

	haben.
12. Abbedingung von §§ 9, 10 ECG Die Vorschriften der §§ 9, 10 ECG (E–Commerce–Gesetz) werden hiermit abbedungen.	**12. Abbedingung ~~von §§ 9, 10 ECG~~ der dispositiven Bestimmungen des E-Commerce-Gesetzes und des ZaDiG 2018** Die Vorschriften der §§ 9, 10 ECG (E–Commerce–Gesetz) werden hiermit abbedungen. Gegenüber dem Kunden werden folgende Bestimmungen des Zahlungsdienstegesetzes 2018 (ZaDiG) nicht Vertragsbestandteil: die Bestimmungen des 3 Hauptstückes des ZaDiG 2018 (Zahlungsdienstegesetzes 2018), somit §§ 32-54 (Informationspflichten), §§ 32 bis 54, § 56 (1) [Entgeltverbot für die Erfüllung der Informationspflichten oder für Berichtigungs-und Schutzmaßnahmen], § 58 (3) [Widerruf der Autorisierung], § 66 (1) und (3) [Nachweis der Authentifizierung und Ausführung von Zahlungsvorgängen], § 68 (2),(5)und (6) [Haftung für nicht autorisierte Zahlungsvorgänge],§ 70 (1) und (3) [Erstattung eines vom Zahlungsempfänger ausgelösten Zahlungsvorganges], § 80 [Haftung der Zahlungsdienstleister für nicht erfolgte, fehlerhafte oder verspätete Ausführung von Zahlungsvorgängen]. In § 68 (1) entfällt gegenüber Unternehmern die Wortfolge „bis zu einem Betrag von 50 Euro“.
Anlage 1a: EBICS–Anbindung	**Anlage 1a: EBICS–Anbindung**
1. Legitimations- und Sicherungsverfahren **1.1 Elektronische Unterschriften** **1.1.1 Elektronische Unterschrift 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“) **1.2 Authentifikationssignatur** Im Gegensatz zur EU, die Auftragsdaten signiert, wird die Authentifikationssignatur über die einzelne EBICS–Nachricht einschließlich Steuerungs– und Anmeldedaten und die darin enthaltenen EU gebildet. Mit Ausnahme einiger in der EBICS–Spezifikation definierten systembedingten Auftragsarten wird die Authentifikationssignatur bei jedem Transaktionsschritt sowohl vom Kunden– als auch vom Banksystem geleistet. Der Kunde muss gewährleisten, dass eine Software eingesetzt wird, die die Authentifikationssignatur jeder von dem Kreditinstitut übermittelten EBICS–Nachricht unter Berücksichtigung der Aktualität und Authentizität der gespeicherten öffentlichen Schlüssel des Kreditinstituts gemäß den Vorgaben der EBICS–Spezifikation (siehe Anlage 1b) prüft. Die Authentifikationssignatur kann beim photo–TAN–Verfahren auch in der technischen Umgebung der Bank oder des zugelassenen Dienstleisters geleistet werden. Diese nehmen für den Kunden die erforderliche Prüfung vor.	**1. Legitimations- und Sicherungsverfahren** **1.1 Elektronische Unterschriften** **1.1.1 Elektronische Unterschrift der Teilnehmer** Für die Elektronischen Unterschriften (EU) der Teilnehmer (die keine qualifizierten Signaturen im Sinne des SVG darstellen) sind die folgenden Unterschriftsklassen definiert: • Einzelunterschrift (Typ „E“) • Erstunterschrift (Typ „A“) • Zweitunterschrift (Typ „B“) • Transportunterschrift (Typ „T“) **1.2 Authentifikationssignatur** Im Gegensatz zur EU, die Auftragsdaten signiert, wird die Authentifikationssignatur über die einzelne EBICS–Nachricht einschließlich Steuerungs– und Anmeldedaten und die darin enthaltenen EU gebildet. Mit Ausnahme einiger in der EBICS–Spezifikation definierten systembedingten Auftragsarten wird die Authentifikationssignatur bei jedem Transaktionsschritt sowohl vom Kunden– als auch vom Banksystem geleistet. Der Kunde muss gewährleisten, dass eine Software eingesetzt wird, die die Authentifikationssignatur jeder von dem Kreditinstitut übermittelten EBICS–Nachricht unter Berücksichtigung der Aktualität und Authentizität der gespeicherten öffentlichen Schlüssel des Kreditinstituts gemäß den Vorgaben der EBICS–Spezifikation (siehe Anlage 1b) prüft. ~~Die Authentifikationssignatur kann beim photo–TAN–Verfahren auch in der technischen Umgebung der Bank oder des zugelassenen Dienstleisters geleistet werden. Diese nehmen für den Kunden die erforderliche Prüfung vor.~~

2.2 Initialisierung der Teilnehmerschlüssel **2.2.1 Neuinitialisierung Teilnehmerschlüssel** (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. Anstelle des Passwortes kann der Teilnehmer die photoTAN verwendet werden, wenn das Sicherungsmedium des Teilnehmers bankseitig in einer technischen Umgebung gespeichert ist, die vor unautorisiertem Zugriff geschützt ist. Auf dieses Passwort kann verzichtet werden, wenn das Sicherungsmedium des Teilnehmers in einer technischen Umgebung gespeichert ist, die vor unautorisiertem Zugriff geschützt ist.	**2.2 Initialisierung der Teilnehmerschlüssel** **2.2.1 Neuinitialisierung Teilnehmerschlüssel** (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. ~~Anstelle des Passwortes kann der Teilnehmer die photoTAN verwendet werden, wenn das Sicherungsmedium des Teilnehmers bankseitig in einer technischen Umgebung gespeichert ist, die vor unautorisiertem Zugriff geschützt ist.~~ Auf dieses Passwort kann verzichtet werden, wenn das Sicherungsmedium des Teilnehmers in einer technischen Umgebung gespeichert ist, die vor unautorisiertem Zugriff geschützt ist.
2.2.2 Migration von FTAM nach EBICS Soweit der Teilnehmer aufgrund seines vorhandenen DFÜ–Zugangs für FTAM bereits über einen gültigen, vom Kreditinstitut freigeschalteten bankfachlichen Schlüssel verfügt, können im Zuge der gesondert vereinbarten Migration von FTAM nach EBICS vorhandene bankfachliche Schlüssel beibehalten werden, soweit diese mindestens der Version A004 entsprechen und dies so mit dem Kreditinstitut vereinbart ist. In diesem Fall werden die öffentlichen Schlüssel für die Authentifikation und die Verschlüsselung mit den hierfür vorgesehenen Auftragsarten an das Kreditinstitut übermittelt. Diese Nachrichten sind mit dem Schlüssel für die bankfachliche EU zu unterschreiben. Ein separater Versand eines unterschriebenen Initialisierungsbriefs entfällt.	~~**2.2.2 *(entfällt)* Migration von FTAM nach EBICS**~~ ~~*(entfällt)* Soweit der Teilnehmer aufgrund seines vorhandenen DFÜ–Zugangs für FTAM bereits über einen gültigen, vom Kreditinstitut freigeschalteten bankfachlichen Schlüssel verfügt, können im Zuge der gesondert vereinbarten Migration von FTAM nach EBICS vorhandene bankfachliche Schlüssel beibehalten werden, soweit diese mindestens der Version A004 entsprechen und dies so mit dem Kreditinstitut vereinbart ist. In diesem Fall werden die öffentlichen Schlüssel für die Authentifikation und die Verschlüsselung mit den hierfür vorgesehenen Auftragsarten an das Kreditinstitut übermittelt. Diese Nachrichten sind mit dem Schlüssel für die bankfachliche EU zu unterschreiben. Ein separater Versand eines unterschriebenen Initialisierungsbriefs entfällt.~~
3. Auftragserteilung an die Bank Der Nutzer überprüft die Auftragsdaten auf ihre Richtigkeit und stellt sicher, dass genau diese Daten elektronisch unterschrieben werden. Bei Aufnahme der Kommunikation werden seitens des Kreditinstitutes zuerst teilnehmerbezogene Berechtigungsprüfungen durchgeführt, wie etwa die Auftragsartberechtigung oder ggf. vereinbarte Limitprüfungen. Die Ergebnisse weiterer bankfachlicher Prüfungen wie beispielsweise Limitprüfungen oder Kontoberechtigungsprüfungen werden dem Kunden im Kundenprotokoll zu einem späteren Zeitpunkt mitgeteilt. Eine Ausnahme bildet die mit dem Kunden optional vereinbarte Onlineprüfung der Auftragsdaten durch die Bank. Die Autorisierung von Aufträgen kann auch durch Eingabe der auf dem mobilen End– oder Lesegerät angezeigten photoTAN und der daraufhin in der gesicherten technischen Umgebung erzeugten elektronischen Signatur erteilt werden. Aufträge, die an das Banksystem übermittelt werden, können wie folgt autorisiert werden: (1) Alle erforderlichen bankfachlichen EU werden zusammen mit den Auftragsdaten übertragen. (2) Sofern mit dem Kunden für die jeweilige Auftragsart die Verteilte Elektronische Unterschrift (VEU) vereinbart wurde und die übermittelten EU für die bankfachliche Freigabe nicht ausreichen, wird der Auftrag bis zur Abgabe aller erforderlichen EU im Banksystem gespeichert. (3) Soweit Kunde und Bank vereinbaren, dass die Autorisierung von per DFÜ übermittelten Auftragsdaten und Aufträgen mittels gesondert übermitteltem Begleitzettel erfolgen kann, ist anstelle der bankfachlichen EU des Nutzers eine Transportunterschrift (Typ „T“) für die technische Absicherung der Auftragsdaten zu leisten. Hierfür ist die Datei mit einer speziellen Kennung zu versehen, die angibt, dass es außer der Transportunterschrift (Typ „T“) keine weitere EU für diesen Auftrag gibt. Die Freigabe des Auftrags erfolgt nach erfolgreicher Prüfung der Unterschrift des Nutzers auf dem Begleitzettel durch das Kreditinstitut.	**3. Auftragserteilung an die Bank** Der Nutzer überprüft die Auftragsdaten auf ihre Richtigkeit und stellt sicher, dass genau diese Daten elektronisch unterschrieben werden. Bei Aufnahme der Kommunikation werden seitens des Kreditinstitutes zuerst teilnehmerbezogene Berechtigungsprüfungen durchgeführt, wie etwa die Auftragsartberechtigung oder ggf. vereinbarte Limitprüfungen. Die Ergebnisse weiterer bankfachlicher Prüfungen wie beispielsweise Limitprüfungen oder Kontoberechtigungsprüfungen werden dem Kunden im Kundenprotokoll zu einem späteren Zeitpunkt mitgeteilt. ~~Eine Ausnahme bildet die mit dem Kunden optional vereinbarte Onlineprüfung der Auftragsdaten durch die Bank.~~ ~~Die Autorisierung von Aufträgen kann auch durch Eingabe der auf dem mobilen End– oder Lesegerät angezeigten photoTAN und der daraufhin in der gesicherten technischen Umgebung erzeugten elektronischen Signatur erteilt werden.~~ Aufträge, die an das Banksystem übermittelt werden, können wie folgt autorisiert werden: (1) Alle erforderlichen bankfachlichen EU werden zusammen mit den Auftragsdaten übertragen. (2) Sofern mit dem Kunden für die jeweilige Auftragsart die Verteilte Elektronische Unterschrift (VEU) vereinbart wurde und die übermittelten EU für die bankfachliche Freigabe nicht ausreichen, wird der Auftrag bis zur Abgabe aller erforderlichen EU im Banksystem gespeichert. (3) Soweit Kunde und Bank vereinbaren, dass die Autorisierung von per DFÜ übermittelten Auftragsdaten und Aufträgen mittels gesondert übermitteltem Begleitzettel erfolgen kann, ist anstelle der bankfachlichen EU des Nutzers eine Transportunterschrift (Typ „T“) für die technische Absicherung der Auftragsdaten zu leisten. Hierfür ist die Datei mit einer speziellen Kennung zu versehen, die angibt, dass es außer der Transportunterschrift (Typ „T“) keine weitere EU für diesen Auftrag gibt. Die Freigabe des Auftrags erfolgt nach erfolgreicher Prüfung der Unterschrift des Nutzers auf dem Begleitzettel durch das Kreditinstitut.

3.1 Auftragserteilung mittels Verteilter Elektronischer Unterschrift (VEU) Die Art und Weise, wie die Verteilte Elektronische Unterschrift durch den Kunden genutzt wird, muss mit dem Kreditinstitut vereinbart werden. Die Verteilte Elektronische Unterschrift ist dann einzusetzen, wenn die Autorisierung von Aufträgen unabhängig vom Transport der Auftragsdaten und ggf. auch durch mehrere Teilnehmer erfolgen soll. Bei einer Verteilten Elektronischen Unterschrift kann die Freigabe und damit die Autorisierung mit der zweiten bankfachlichen Unterschrift durch Verwendung der photoTAN oder durch Freigabe eines Auftrages im Rahmen der App–Anwendung der Bank erfolgen. Solange noch nicht alle zur Autorisierung erforderlichen bankfachlichen EU vorliegen, kann der Auftrag von einem hierzu berechtigten Nutzer gelöscht werden. Soweit der Auftrag vollständig autorisiert wurde, ist nur noch ein Rückruf gemäß Abschnitt 8 der Bedingungen für Datenfernübertragung möglich. Das Kreditinstitut ist dazu berechtigt, nicht vollständig autorisierte Aufträge nach Ablauf des von der Bank gesondert mitgeteilten Zeitlimits zu löschen. **3.3 Kundenprotokolle** Die Bank dokumentiert in Kundenprotokollen die folgenden Vorgänge: • Übertragung der Auftragsdaten an das Banksystem • Übertragung von Informationsdateien vom Banksystem an das Kundensystem • Ergebnis einer jeden Legitimationsprüfung von Aufträgen des Kunden an das Banksystem • Weiterverarbeitung von Aufträgen, sofern sie die Unterschriftsprüfung, die Anzeige von Auftragsdaten betreffen • Fehler bei der Dekomprimierung Der Teilnehmer hat sich zeitnah durch Abruf des Kundenprotokolls über das Ergebnis der aufseiten des Kreditinstituts durchgeführten Prüfungen zu informieren. Der Teilnehmer hat dieses Protokoll, das inhaltlich den Bestimmungen von Kapitel 10 der Anlage 1b entspricht, zu seinen Unterlagen zu nehmen und auf Anforderung des Kreditinstitutes zur Verfügung zu stellen.	**3.1 Auftragserteilung mittels Verteilter Elektronischer Unterschrift (VEU)** Die Art und Weise, wie die Verteilte Elektronische Unterschrift durch den Kunden genutzt wird, muss mit dem Kreditinstitut vereinbart werden. Die Verteilte Elektronische Unterschrift ist dann einzusetzen, wenn die Autorisierung von Aufträgen unabhängig vom Transport der Auftragsdaten und ggf. auch durch mehrere Teilnehmer erfolgen soll. ~~Bei einer Verteilten Elektronischen Unterschrift kann die Freigabe und damit die Autorisierung mit der zweiten bankfachlichen Unterschrift durch Verwendung der photoTAN oder durch Freigabe eines Auftrages im Rahmen der App–Anwendung der Bank erfolgen.~~ Solange noch nicht alle zur Autorisierung erforderlichen bankfachlichen EU vorliegen, kann der Auftrag von einem hierzu berechtigten Nutzer gelöscht werden. Soweit der Auftrag vollständig autorisiert wurde, ist nur noch ein Rückruf gemäß Abschnitt 8 der Bedingungen für Datenfernübertragung möglich. Das Kreditinstitut ist dazu berechtigt, nicht vollständig autorisierte Aufträge nach Ablauf des von der Bank gesondert mitgeteilten Zeitlimits zu löschen. **3.3 Kundenprotokolle** Die Bank dokumentiert in Kundenprotokollen die folgenden Vorgänge: • Übertragung der Auftragsdaten an das Banksystem • Übertragung von Informationsdateien vom Banksystem an das Kundensystem • Ergebnis einer jeden Legitimationsprüfung von Aufträgen des Kunden an das Banksystem • Weiterverarbeitung von Aufträgen, sofern sie die Unterschriftsprüfung, die Anzeige von Auftragsdaten betreffen ~~• Fehler bei der Dekomprimierung~~ Der Teilnehmer hat sich zeitnah durch Abruf des Kundenprotokolls über das Ergebnis der aufseiten des Kreditinstituts durchgeführten Prüfungen zu informieren. Der Teilnehmer hat dieses Protokoll, das inhaltlich den Bestimmungen von Kapitel 10 der Anlage 1b ent-spricht, zu seinen Unterlagen zu nehmen und auf An-forderung des Kreditinstitutes zur Verfügung zu stellen.