Bedingungen für die Datenfernübertragung

Gegenüberstellung der geänderten Bestimmungen

Version 2014	Version 2017
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, ab dem 1. Februar 2014 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 (§ 7c Absatz 1 Zahlungsdiensteaufsichtsgesetz), sind erst ab dem 1. Februar 2016 verpflichtend im Format ISO 20022 einzureichen.	**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, ~~ab dem 1. Februar 2014~~ 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), ~~sind erst ab dem 1. Februar 2016~~ verpflichtend im Format ISO 20022 einzureichen.
4. Verhaltens– und Sorgfaltspflichten im Umgang mit den Legitimationsmedien für die Autorisierung des Auftrags	**4. Verhaltens– und Sorgfaltspflichten im Umgang mit den Legitimationsmedien für die Autorisierung des Auftrags** 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.
6. Sperre der Legitimations– und Sicherungsmedien (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.	**6. Sperre der Legitimations– und Sicherungsmedien** (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 unverzüglich informieren. Diese Sperre kann mittels DFÜ nicht aufgehoben werden.
7. Behandlung eingehender Auftragsdaten	**7. Behandlung eingehender Auftragsdaten**

durch die Bank (3) Die Bank prüft die Legitimation des Nutzers bzw. der Nutzer und die Autorisierung der per DFÜ übermittelten Auftragsdaten anhand der von den Nutzern mittels der Legitimationsmedien erstellten Elektronischen Unterschriften oder des übermittelten Begleitzettels 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.	**durch die Bank** (3) Die Bank prüft die Legitimation des Nutzers bzw. der Nutzer und die Autorisierung der per DFÜ übermittelten Auftragsdaten anhand der von den Nutzern mittels der Legitimationsmedien erstellten Elektronischen Unterschriften oder des übermittelten Begleitzettels oder anhand der eingegebenen photoTAN 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.
Anlage 1a: EBICS–Anbindung **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.	**Anlage 1a: EBICS–Anbindung** **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 Schlüssel **2.2.1 Neuinitialisierung der 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. 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 Schlüssel** **2.2.1 Neuinitialisierung der 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.
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.	**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.
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.	**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.