



Nähere Angaben zur Bank sind im „Preis- und Leistungsverzeichnis“ enthalten.
Nadere informatie over de Bank is te vinden in het kosten-en-serviceoverzicht.

Deze vertaling is uitsluitend bedoeld voor het gemak van de klant. De originele Duitse tekst van de Voorwaarden voor gegevensuitwisseling op afstand („Bedingungen für Datenfernübertragung“) is in alle opzichten bindend. In geval van tegenstrijdigheden tussen de Nederlandse en de Duitse teksten, constructies, betekenissen of interpretaties, prevaleert uitsluitend de Duitse tekst, constructie, betekenis of interpretatie.

Bedingungen für Datenfernübertragung

Voorwaarden voor gegevensuitwisseling op afstand

1 Leistungsumfang

- (1) Die Bank steht ihrem Kunden (Kontoinhaber), der kein Verbraucher ist, 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 Verfügungsmittele.
- (3) Die Datenfernübertragung ist über die EBICS-Anbindung (Anlagen 1a bis 1c) möglich.
- (4) Der Satz- und Dateiaufbau für die Übermittlung von Aufträgen und den Informationsabruf wird in der Spezifikation der Datenformate (Anlage 3) beschrieben.

2 Nutzer und Teilnehmer, Legitimations- und Sicherungsmedien

- (1) Aufträge können über die EBICS-Anbindung nur vom Kunden oder seinen Kontobevollmächtigten erteilt werden. Kunde und Kontobevollmächtigter werden im Folgenden einheitlich als „Nutzer“ bezeichnet. Zur Autorisierung von per DFÜ übermittelten Auftragsdaten mittels Elektronischer Unterschrift benötigt jeder Nutzer 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 den Datenaustausch über die EBICS-Anbindung kann der Kunde zusätzlich zu den Bevollmächtigten „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 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

Reikwijdte van dienstverlening

De Bank biedt haar klanten (rekeninghouders) die geen consument zijn, ondersteuning voor de gegevensuitwisseling op afstand langs elektronische weg (hierna 'gegevensuitwisseling op afstand' of 'telematica' genoemd). Onder gegevensuitwisseling op afstand wordt hier verstaan het uploaden en downloaden van bestanden (in het bijzonder voor het overbrengen van opdrachten en het opvragen van informatie).

De Bank informeert de Klant over de typen diensten waar de Klant in het kader van de gegevensuitwisseling op afstand gebruik van kan maken. Voor het gebruik van de gegevensuitwisseling op afstand gelden de beschikkingenlimieten zoals overeengekomen met de Bank.

Gegevensuitwisseling op afstand is mogelijk via de EBICS-koppeling (Bijlagen 1a tot 1c).

De voorgeschreven structuur van gegevens en documenten voor het overbrengen van opdrachten en het opvragen van informatie worden omschreven in de specificatie van gegevensindelingen (Bijlage 3).

Gebruikers en deelnemers, legitimatie- en beveiligingsmedia

Opdrachten kunnen via de EBICS-koppeling uitsluitend door de Klant of de gemachtigde voor zijn rekening worden ingediend. Naar de Klant en gemachtigden voor zijn rekening wordt hierna gezamenlijk verwezen als 'Gebruiker' of 'Gebruikers'. De Bank heeft voor elke Gebruiker een persoonlijk legitimatiemedium geactiveerd waarmee de Gebruiker per telematica overgebrachte opdrachtgegevens kan autoriseren met een elektronische handtekening. De vereisten voor de legitimatiemediata zijn omschreven in Bijlage 1a. Indien dit met de Bank is overeengekomen, kunnen per telematica overgebrachte opdrachtgegevens met een ondertekende bijgevoegde nota of batchopdracht worden geautoriseerd.

Voor de gegevensuitwisseling via de EBICS-koppeling kan de Klant, naast de gemachtigde, 'Technische Deelnemers' benoemen, die uitsluitend bevoegd zijn de gegevensuitwisseling uit te voeren. Naar Gebruikers en Technische Deelnemers wordt hierna gezamenlijk verwezen als 'Deelnemer' of 'Deelnemers'. Ter beveiliging van de gegevensuitwisseling heeft elke Deelnemer een persoonlijk beveiligingsmedium nodig dat door de Bank is geactiveerd. De vereisten voor de beveiligingsmedia zijn omschreven in Bijlage 1a.

Procesbepalingen

Voor het overdrachtsproces dat de Klant en de Bank zijn overeengekomen, gelden de vereisten zoals omschreven in Bijlage 1a, in de documentatie van de technische omgeving (Bijlage 1b) en de specificatie van gegevensindelingen (Bijlage 3).

De Klant is verplicht te waarborgen dat alle Deelnemers het telematicaproces en de specificaties in acht nemen.

beachten.

- (3) Die Belegung der Datenfelder richtet sich nach den Belegungs- und Kontrollrichtlinien des jeweils genutzten Formates (Anlage 3).
- (4) Reicht der Nutzer eine Datei mit mehreren SEPA-Überweisungen oder SEPA-Echtzeitüberweisungen ein, entscheidet er durch Verwendung der vereinbarten Auftragsart¹, ob die Empfängerüberprüfung gemäß Nummer 2.1.3 der Bedingungen für den Überweisungsverkehr durchgeführt werden soll. Verzichtet der Nutzer auf die Empfängerüberprüfung, führt die Bank die in der Datei enthaltenen Überweisungen anhand der vom Nutzer angegebenen Kundenkennungen aus. Dies kann im Einzelfall dazu führen, dass das Geld auf ein Zahlungskonto eingeht, dessen Inhaber nicht der vom Nutzer namentlich angegebene Zahlungsempfänger ist. Reicht der Nutzer eine Datei mit nur einer einzigen SEPA-Überweisung oder SEPA-Echtzeitüberweisung ein, so ist die Bank unabhängig von der Entscheidung des Nutzers gesetzlich verpflichtet, die Empfängerüberprüfung durchzuführen. Dieser Absatz gilt nicht für per DFÜ übermittelte Auftragsdaten mit unterschriebenem Begleitzettel/Sammelauftrag.
- (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 eingelieferten 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 Nutzer 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 Nutzer über das Ergebnis informieren. Der Nutzer entscheidet dann, ob

- er die Datei zur Ausführung freigibt oder
- die Datei nicht ausgeführt werden soll.

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

De gegevensvelden dienen te worden ingevuld overeenkomstig de invul- en controlerichtlijnen voor de gekozen indeling (Bijlage 3).

Indien de Gebruiker een bestand indient met meerdere SEPA-overboekingen of SEPA-realtime-overboekingen, besluit hij aan de hand van het overeengekomen opdrachtstype² of de ontvangercontrole in de zin van artikel 2.1.3 van de Voorwaarden voor giroverkeer uitgevoerd dient te worden. Indien de Gebruiker afziet van een ontvangercontrole, voert de Bank de overboekingen in het bestand uit op basis van de klantidentificatie zoals opgegeven door de Gebruiker. Dit kan er in individuele gevallen toe leiden dat het geld naar een betaalrekening wordt overgeboekt waarvan de rekeninghouder niet overeenkomt met de begunstigde die de Gebruiker met naam heeft opgegeven. Indien de Gebruiker een bestand indient met slechts één SEPA-overboeking of SEPA-realtime-overboeking, is de Bank ongeacht het besluit van de Gebruiker wettelijk verplicht om een ontvangercontrole uit te voeren. Deze paragraaf is niet van toepassing op per telematica overgebrachte opdrachtgegevens met een ondertekende bijgevoegde nota of batchopdracht.

Voorafgaand aan de overdracht van opdrachtgegevens aan de Bank, dienen de over te dragen bestanden en alle inhoud daarvan opgeslagen te worden, evenals de ter controle van de legitimiteit overgebrachte gegevens. Deze dient de Klant ten minste dertig kalenderdagen vanaf de uitvoeringstermijn (voor overboekingen) of de betaaldatum (incasso-opdrachten) uit het bestand of, bij meerdere datums, de laatste datum in een dergelijke vorm aantoonbaar te bewaren, zodat het bestand op verzoek van de Bank op korte termijn opnieuw kan worden overlegd, tenzij anders overeengekomen.

Bovendien dient de Klant voor elke indiening en elke opvraging van bestanden een machineboek, dat inhoudelijk overeenkomt met de bepalingen uit hoofdstuk 10 van de specificatie voor de EBICS-koppeling (Bijlage 1b), op te stellen, in zijn administratie te bewaren en op verzoek aan de Bank te overleggen.

Indien de Bank gegevens aan de Klant ter beschikking stelt over betalingstransacties die nog niet definitief zijn verwerkt, vormen die gegevens uitsluitend niet-bindende informatie. De bestanden zijn stuk voor stuk uniek gekenmerkt.

De per telematica ingediende opdrachtgegevens moeten zoals overeengekomen met de Bank ofwel met elektronische handtekening of met een ondertekende bijgevoegde nota of batchopdracht geautoriseerd worden. Deze opdrachtgegevens worden als opdracht van kracht

bij het indienen met elektronische handtekening, wanneer

- alle vereiste elektronische handtekeningen van de Gebruikers per gegevensuitwisseling op afstand binnen de overeengekomen termijn zijn ontvangen; en
- de authenticiteit van de elektronische handtekeningen bevestigd kan worden met de overeengekomen sleutels

of

bij het indienen met bijgevoegde nota of batchopdracht, wanneer

- de bijgevoegde nota of batchopdracht binnen de overeengekomen termijn is ontvangen door de Bank; en
- de bijgevoegde nota of batchopdracht en de bankvolmacht ondertekend is.

Indien de ontvangercontrole in de zin van artikel 3, paragraaf 4, voor een bestand met SEPA-overboekingen of SEPA-realtime-overboeking wordt uitgevoerd, zal de Bank de Gebruiker de uitkomst mededelen. De Gebruiker beslist dan of

- hij het bestand vrijgeeft voor uitvoering of
- hij niet wil dat het bestand wordt uitgevoerd.

De opdracht wordt in afwijking van artikel 3, paragraaf 8, tweede zin, pas van kracht als de Gebruiker het bestand overeenkomstig zin 2 heeft goedgekeurd.

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

Gedrags- en zorgvuldigheidsplichten met betrekking tot de omgang met de legitiematiemedia voor de autorisatie van opdrachten

In samenhang met de uitwisselingsprocedures zoals overeengekomen met de Bank is de Klant verplicht te

¹ Als Auftragsart gilt auch das „Business Transaction and Format“ (BTF) ab EBICS Version 3.0.

² Als opdrachtstype geldt ook het "Business Transaction and Format" (BTF) vanaf EBICS versie 3.0.

sicherzustellen, dass alle Nutzer die Pflichten aus diesen Bedingungen und die in Anlage 1a beschriebenen Legitimationsverfahren einhalten.

- (2) Mit Hilfe eines von der Bank freigeschalteten Legitimationsmediums 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 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 im Rahmen der EBICS-Anbindung verpflichtet sicherzustellen, dass alle Teilnehmer die in Anlage 1a beschriebenen Sicherungsverfahren einhalten.

Mit Hilfe 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. Die für das EBICS-Verfahren geltenden Sicherheitsanforderungen sind in Anlage 1c beschrieben.

7 Sperre der Legitimations- und Sicherungsmedien

(1) Gehen die Legitimations- oder Sicherungsmedien verloren, wer-den 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 Sperr-anzeige 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.

waarborgen dat alle Gebruikers de verplichtingen uit deze voorwaarden en de in Bijlage 1 omschreven legitimatieprocedures in acht nemen.

Aan de hand van een legitimatiemedium dat de Bank heeft geactiveerd, kunnen Gebruikers opdrachten indienen. De Klant waarborgt dat elke Gebruiker er zorg voor draagt dat niemand anders beschikt over zijn legitimatiemedium, noch over zijn wachtwoord, dat voor zijn veiligheid dient. Ieder ander die het medium of een duplicaat daarvan in handen krijgt, kan namelijk in combinatie met het bijbehorende wachtwoord oneigenlijk gebruikmaken van de overeengekomen dienstverlening. Voor de veiligheid van het legitimatiemedium en het wachtwoord zijn zeker de volgende zaken belangrijk:

- Het legitimatiemedium moet beschermd worden tegen ongeautoriseerde toegang en veilig bewaard worden.
- Het wachtwoord dat ter beveiliging van het legitimatiemedium wordt gebruikt, mag niet op het legitimatiemedium worden genoteerd of als afdruk bij het legitimatiemedium worden bewaard of onbeveiligd elektronisch worden opgeslagen.
- Het legitimatiemedium mag niet gedupliceerd worden.
- Bij het invoeren van het wachtwoord moet erop gelet worden dat er niemand kan meekijken.

Gedrag- en zorgvuldigheidsplichten met betrekking tot de omgang met de beveiligingsmedia voor de gegevensuitwisseling

In het kader van de EBICS-koppeling is de Klant verplicht te waarborgen dat alle Deelnemers de beveiligingsprocedures in acht nemen zoals beschreven in Bijlage 1a.

Met behulp van de beveiligingsmedia die de Bank heeft geactiveerd, beveiligen

Deelnemers de gegevensuitwisseling. De Klant is verplicht te waarborgen dat elke Deelnemer er zorg voor draagt dat niemand anders beschikt over zijn beveiligingsmedium, noch dit beveiligingsmedium kan gebruiken. In het bijzonder in het geval van opslag op een technisch systeem, moet het beveiligingsmedium van de Deelnemer opgeslagen worden in een technische omgeving die is beschermd tegen ongeautoriseerde toegang. Iedere andere persoon die beschikt over het beveiligingsmedium of een duplicaat daarvan, kan namelijk oneigenlijke gegevensuitwisseling uitvoeren.

Veiligheid van het systeem van de Klant

De Klant dient te waarborgen dat de systemen die hij gebruikt voor de gegevensuitwisseling op afstand, voldoende beveiligd zijn. De beveiligingsvereisten voor de EBICS-procedure zijn te vinden in Bijlage 1c.

Blokkeren van de legitimatie- en beveiligingsmedia

In het geval dat de legitimatie- of beveiligingsmedia verloren raken, andere personen er beschikking over krijgen of het vermoeden bestaat dat deze oneigenlijk worden gebruikt, dient de betreffende Deelnemer zijn of haar eigen telematicatoegang bij de Bank onverwijld te blokkeren of te laten blokkeren. Nadere voorschriften zijn te vinden in Bijlage 1a. Een Deelnemer kan de Bank ook altijd via de afzonderlijk medegedeelde contactgegevens de opdracht geven bepaalde media te blokkeren.

De Klant kan buiten de telematica-procedure ook het gebruik van de legitimatie- en beveiligingsmedia door een Deelnemer of de gehele telematica-toegang via de door de Bank medegedeelde blokkeringsfaciliteit laten blokkeren.

De Bank blokkeert de gehele telematica-toegang wanneer zij vermoedt dat er sprake is van oneigenlijk gebruik van de telematica-toegang. De Bank zal de Klant hier buiten de telematica-procedure om over informeren. Deze blokkade kan niet opgeheven worden aan de hand van telematica.

8 Behandlung eingehender Auftragsdaten

Verwerking van binnenkomende opdrachtgegevens door de

durch die Bank

(1) Die der Bank per 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 Nutzers beziehungsweise 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/Sammelauftrages 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 voll-ständig 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 Nutzer 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 Nutzer 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 Kunden-protokoll 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 Auftrags richtet sich nach den dafür geltenden Sonderbedingungen (z. B. Bedingungen für den Über-weisungsverkehr). 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 eingeleiteten Auftragsdaten wurden gemäß Nummer 3 Absatz 3 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 Überweisungs-verkehr) liegen vor.

(2) Liegen die Ausführungsbedingungen nach Absatz 1 nicht vor, wird die Bank den Auftrag nicht ausführen und den Kunden

Bank

Opdrachtgegevens die via telematica aan de Bank zijn doorgegeven, worden verwerkt overeenkomstig de reglementaire procedures.

De Bank controleert op basis van de handtekeningen die de Deelnemers hebben verstrekt met hun beveiligingsmedia of de afzender bevoegd is om de gegevensuitwisseling uit te voeren. Indien dit niet het geval is, zal de Bank de betreffende opdrachtgegevens niet verwerken en de Klant hier onverwijld van op de hoogte stellen.

De Bank controleert de legitimiteit van de Gebruiker of Gebruikers en de autorisatie van de per telematica overgebrachte opdrachtgegevens aan de hand van de elektronische handtekeningen die de Gebruikers met hun legitiematiemedia hebben gegenereerd of aan de hand van de overgebrachte bijgevoegde nota of batchopdracht, en controleert ook of de opdrachtgegevens overeenkomen met de bepalingen uit Bijlage 3. Indien dit niet het geval is, zal de Bank de betreffende opdrachtgegevens niet verwerken en de Klant hier onverwijld van op de hoogte stellen. De Bank heeft het recht om opdrachtgegevens die niet volledig geautoriseerd zijn, na het verstrijken van de door de Bank afzonderlijk medegedeelde tijdslimiet te verwijderen.

Indien uit de controles van bestanden of gegevens door de Bank overeenkomstig Bijlage 3 blijkt dat er fouten zijn gemaakt, zal de Bank de foutieve bestanden of gegevens in een gepaste vorm kenmerken en de Gebruiker hier onmiddellijk over informeren. De Bank heeft het recht om foutieve bestanden of gegevens niet mee te nemen in de verdere verwerking, indien er niet op een andere manier gewaarborgd kan worden dat de opdracht volgens de voorschriften uitgevoerd wordt.

In het geval dat een Gebruiker een bestand indient met meerdere SEPA-realtime-overboekingen, zal de Bank de individuele SEPA-realtime-overboekingen onverwijld initiëren. De uitvoering van de geïnitieerde individuele SEPA-realtime-overboekingen geschiedt overeenkomstig artikel 1.4 van de Voorwaarden voor giroverkeer.

De Bank is verplicht de procedures (zie Bijlage 1a) en de doorgifte van de opdrachten ter verwerking ervan vast te leggen in het klantprotocol. De Klant is op zijn beurt verplicht het klantprotocol binnen afzienbare tijd te downloaden en zich te informeren over de verwerkingsstatus van ingediende opdrachten. Mocht er iets niet kloppen, dient de Klant contact op te nemen met de Bank.

Herroeping

Voorafgaand aan de autorisatie van de opdrachtgegevens kan de Klant het bestand herroepen. Individuele opdrachtgegevens kunnen uitsluitend gewijzigd worden door het volledige bestand te herroepen en daarna opnieuw aan te leveren. De Bank kan een herroeping uitsluitend in aanmerking nemen als deze dermate tijdig binnenkomt dat de stornering verwerkt kan worden volgens de voorgeschreven procedure.

Of een opdracht herroepen kan worden, is afhankelijk van de geldende bijzondere voorwaarden (bijv. de Voorwaarden voor giroverkeer). Opdrachten kunnen worden herroepen buiten de telematica-procedure of, indien dat met de Klant is overeengekomen, overeenkomstig de bepalingen uit hoofdstuk 11 van Bijlage 3. Hiervoor dient de Klant de individuele gegevens uit de originele opdracht aan de Bank voor te leggen.

Uitvoering van opdrachten

De Bank voert opdrachten uit indien er aan alle onderstaande uitvoeringsvoorwaarden is voldaan:

De per telematica aangeleverde opdrachtgegevens zijn geautoriseerd overeenkomstig artikel 3, paragraaf 8, met inachtneming van artikel 3, paragraaf 9. De voorgeschreven gegevensindeling is in acht genomen. De bestedingslimiet is niet overschreden.

Er is voldaan aan de uitvoeringsvereisten overeenkomstig de bijzondere voorwaarden die leidend zijn voor het betreffende opdrachtstype (bijvoorbeeld een toereikende dekkingsgraad overeenkomstig de Voorwaarden voor giroverkeer).

Indien er niet is voldaan aan de uitvoeringsvoorwaarden uit paragraaf 1, voert de Bank de opdracht niet uit en stelt de Bank

über die Nicht-ausführung 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 verlorengegangenen 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.

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 1c: Sicherheitsanforderungen an das EBICS-Kundensystem

de Klant via het overeengekomen communicatiekanaal onverwijld op de hoogte van de niet-uitvoering. Daarbij zal de Bank, voor zover mogelijk, toelichten naar welke redenen en fouten de niet-uitvoering te herleiden is, en uitlechten welke mogelijkheden er zijn om deze fouten te verhelpen.

Aansprakelijkheid

Aansprakelijkheid van de Bank bij een niet-geautoriseerde telematicabeschikking en bij een niet, niet naar behoren of met vertraging uitgevoerde telematicabeschikking

De aansprakelijkheid van de Bank bij een niet-geautoriseerde telematicabeschikking en bij een niet, niet naar behoren of met vertraging uitgevoerde telematicabeschikking is afhankelijk van de bijzondere voorwaarden die zijn overeengekomen voor het betreffende opdrachtstype (bijvoorbeeld de Voorwaarden voor giroverkeer).

Aansprakelijkheid van de Klant bij oneigenlijk gebruik van de legitimatie- of beveiligingsmedia

Aansprakelijkheid van de Klant voor niet-geautoriseerde betalingstransacties voorafgaand aan een blokkeringsinstructie

In het geval van niet-geautoriseerde betalingstransacties als gevolg van oneigenlijk gebruik van de legitimatie- of beveiligingsmedia voorafgaand aan een blokkeringsinstructie, is de Klant jegens de Bank aansprakelijk voor alle schade die de Bank als gevolg daarvan heeft geleden, wanneer de Deelnemer nalatig of opzettelijk zijn gedrags- en zorgvuldigheidsplichten heeft geschonden. § 675v van het Duitse Burgerlijk Wetboek (BGB) is niet van toepassing.

De Klant is niet verplicht geleden schade in de zin van paragraaf 1 te vergoeden in het geval dat de Deelnemer geen blokkeringsinstructie kon afgeven overeenkomstig artikel 7, paragraaf 1, als de Bank geen mogelijkheid had ingericht om blokkeringsinstructies te ontvangen en de schade daardoor voorkomen had kunnen worden.

De aansprakelijkheid voor schade die wordt veroorzaakt binnen de termijn waarvoor de bestedingslimiet geldt, is beperkt tot de betreffende overeengekomen bestedingslimiet.

Paragrafen 2 en 3 zijn niet van toepassing wanneer een Deelnemer met frauduleuze bedoelingen heeft gehandeld.

Aansprakelijkheid van de Klant bij overige niet geautoriseerde handelingen voorafgaand aan een blokkeringsinstructie

Indien niet-geautoriseerde handelingen die geen betalingstransacties zijn, voorafgaand aan een blokkeringsinstructie zijn gebaseerd op het gebruik van een verloren of gestolen legitimatie- of beveiligingsmedium of op anderszorg frauduleus gebruik van het legitimatie of beveiligingsmedium en de Bank hierdoor schade heeft geleden, zijn de Klant en de Bank hiervoor beiden aansprakelijk op basis van de wettelijke beginselen voor eigen schuld.

Aansprakelijkheid van de Bank vanaf de blokkeringsinstructie

Zodra de Bank een blokkeringsinstructie van een Deelnemer heeft ontvangen, neemt zij alle schade op zich die daarna voortvloeit uit niet-geautoriseerde telematicabeschikkingen. Dit geldt niet wanneer een Deelnemer met frauduleuze bedoelingen heeft gehandeld.

Uitsluiting van aansprakelijkheid

Aansprakelijkheidsclaims zijn uitgesloten als de omstandigheden die ten grondslag liggen aan de betreffende claim op een buitengewone en onvoorspelbare gebeurtenis berusten waar de betreffende partij geen invloed op heeft en waarvan de gevolgen ondanks de geboden zorgvuldigheid niet voorkomen hadden kunnen worden.

Slotbepalingen

De bijlagen waarnaar in deze voorwaarden wordt verwezen, maken deel uit van het akkoord dat met de Klant is gesloten.

Bijlage 1a: EBICS-koppeling

Bijlage 1b: Specificatie van de EBICS-koppeling

Bijlage 1c: Beveiligingsvereisten voor het EBICS-systeem van de Klant

Bijlage 2: momenteel niet bijgevoegd

Anlage 2: derzeit nicht belegt

Anlage 3: Spezifikation der Datenformate

Bijlage 3: Specificatie van gegevensindelingen

Anlage 1a: EBICS-Anbindung**1. Legitimations- und Sicherungsverfahren**

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

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 Teilnehmer-schlüssel sind der Bank 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 Banken eingesetzt werden.

1.1 Elektronische Unterschriften**1.1.1 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 bankfachlichen EU benötigen, die von unterschiedlichen Nutzern (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. „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. 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.

1.1.2 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 definierter systembedingter Auftragsarten wird die Authentifikationssignatur bei jedem Transaktionsschritt sowohl vom Kunden- als auch vom Bank-system geleistet. Der Kunde muss gewährleisten, dass eine Software eingesetzt wird, die die Authentifikationssignatur jeder von der Bank übermittelten EBICS-Nachricht unter Berücksichtigung der Aktualität und Authentizität der gespeicherten öffentlichen Schlüssel der Bank gemäß den Vorgaben der EBICS-Spezifikation (siehe Anlage 1b) prüft.

1.2 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 Bank gemäß den Vorgaben der EBICS-Spezifikation (siehe Anlage 1b) zu verschlüsseln.

Darüber hinaus ist auf den externen Übertragungsstrecken zwischen Kunden- und Banksystem zusätzlich eine Transportverschlüsselung vorzunehmen. Der Kunde muss gewährleisten, dass eine Software eingesetzt wird, die gemäß den Vorgaben der EBICS-Spezifikation (siehe Anlage 1b) Aktualität und Authentizität der hierfür eingesetzten Serverzertifikate der Bank überprüft.

Bijlage 1a: EBICS-koppeling**Legitimatie- en beveiligingsprocedures**

In het kader van de gegevensuitwisseling op afstand bezorgt de Klant (rekeninghouder) een lijst met de Deelnemers en hun machtigingen aan de Bank.

De EBICS-koppeling wordt beveiligd met de volgende legitimatie- en beveiligingsprocedures:

Elektronische handtekeningen
Ondertekening ter authenticatie
Versleuteling

Voor elke legitimatie- en beveiligingsprocedure beschikt een Deelnemer over een persoonlijk sleutelpaar, dat bestaat uit een privésleutel en een openbare sleutel. De openbare sleutels van alle Deelnemers moeten aan de Bank worden verstrekt overeenkomstig de procedures uit artikel 2. De openbare banksleutels dienen aan de hand van de procedures uit artikel 2 beschermd te worden tegen ongeautoriseerde wijzigingen. De sleutelparen van een Deelnemer kunnen ook gebruikt worden voor communicatie met andere banken.

Elektronische handtekeningen**Elektronische handtekeningen van Deelnemers**

De Elektronische Handtekeningen (EH) van Deelnemers zijn onder te verdelen in de volgende categorieën:

Individuele handtekening (type E)
Eerste handtekening (type A)
Tweede handtekening (type B)
Transporthandtekening (type T)

Als banktechnische EH gelden EH's van het type E, A of B. Banktechnische EH's worden gebruikt om opdrachten mee te autoriseren. Mogelijk zijn er voor opdrachten meerdere banktechnische EH's noodzakelijk van verschillende Gebruikers (rekeninghouders en hun gemachtigden). Voor elk ondersteund opdrachtstype komen de Bank en de Klant een minimumaantal noodzakelijke banktechnische EH's overeen.

EH's van type T, die als transporthandtekening bestempeld zijn, worden niet gebruikt om opdrachten banktechnisch goed te keuren, maar uitsluitend voor de overdracht aan de systemen van de Bank. Aan 'Technische Deelnemers' (zie artikel 2.2) kan uitsluitend een EH van type T worden toegewezen.

Met het programma dat de Klant gebruikt, kunnen diverse berichten worden opgesteld (bijvoorbeeld opdrachten voor binnenlands en grensoverschrijdend betalingsverkeer, maar ook voor de initialisatie en voor het opvragen van logboeken en rekening- of opbrengstgegevens).

De Bank informeert de Klant over welke berichttypen gebruikt kunnen worden en welk EH-type daarbij hoort.

Ondertekening ter authenticatie

In tegenstelling tot EH's, waarmee opdrachtgegevens worden ondertekend, bestaat een ondertekening ter authenticatie uit de individuele EBICS-melding, met stuur- en inloggegevens en de EH's die daar deel van uitmaken. Met uitzondering van een aantal in de EBICS-specificatie gedefinieerde systeemafhankelijke opdrachtstypen wordt de ondertekening ter authenticatie bij elke transactiestap zowel door het systeem van de Klant als door het systeem van de Bank uitgevoerd. De Klant moet waarborgen dat er software wordt gebruikt waarmee de ondertekening ter authenticatie van elke EBICS-melding die de Bank overbrengt, wordt gecontroleerd, waarbij wordt nagegaan of de opgeslagen openbare sleutel van de Bank actueel en authentiek is, overeenkomstig de voorschriften uit de EBICS-specificatie (zie Bijlage 1b).

Versleuteling

Om te waarborgen dat de banktechnische gegevens op gebruiksniveau geheim blijven, dient de Klant de opdrachtgegevens te versleutelen en daarbij na te gaan of de opgeslagen openbare sleutel van de Bank actueel en authentiek is, overeenkomstig de voorschriften uit de EBICS-specificatie (zie Bijlage 1b).

Bovendien dient er zorg gedragen te worden voor aanvullende transportversleuteling op de externe uitwisselingskanalen tussen het systeem van de Klant en het systeem van de Bank. De Klant moet waarborgen dat er software wordt gebruikt die de servercertificaten van de Bank controleert, waarbij wordt nagegaan of de opgeslagen openbare sleutel van de Bank actueel en authentiek is, overeenkomstig de voorschriften uit de EBICS-specificatie (zie Bijlage 1b).

2 Initialisierung der EBICS-Anbindung

2.1 Einrichtung der Kommunikationsverbindung

Der Kommunikationsaufbau erfolgt unter Verwendung einer URL (Uniform Resource Locator). Alternativ kann auch eine IP-Adresse der jeweiligen Bank benutzt werden. Die URL oder die IP-Adresse werden dem Kunden bei Vertragsabschluss mit der Bank mitgeteilt.

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

- URL oder IP-Adresse der Bank
- Bezeichnung der Bank
- HostID
- Zulässige Version(en) für das EBICS-Protokoll und der Sicherungsverfahren
- Partner-ID (Kunden-ID)
- User-ID
- System-ID (für technische Teilnehmer)
- 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. Soweit dem Kunden ein oder mehrere technische Teilnehmer zugeordnet sind (Multi-User-System), vergibt die Bank zusätzlich zur User-ID eine System-ID. Soweit kein technischer Teilnehmer festgelegt ist, sind System-ID und User-ID identisch.

2.2 Initialisierung der Teilnehmerschlüssel

Die vom Teilnehmer eingesetzten Schlüsselpaare für die bankfachliche EU, die Verschlüsselung der Auftragsdaten und die Authentifikations-signatur müssen zusätzlich zu den in Nummer 1 beschriebenen all-gemeinen 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 ist, die vor unautorisiertem Zugriff geschützt ist.

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

- Über die EBICS-Anbindung mittels der hierfür vorgesehenen systembedingten Auftragsarten.
- Mit einem vom Kontoinhaber oder einem Kontobevollmächtigten unterschriebenen Initialisierungsbrief.

Für die Freischaltung des Teilnehmers überprüft die Bank auf Basis der vom Kontoinhaber oder einem Kontobevollmächtigten unterschriebenen Initialisierungsbrieife die Authentizität der über EBICS übermittelten öffentlichen Teilnehmerschlüssel.

Zu jedem öffentlichen Teilnehmerschlüssel enthält der Initialisierungs-brief 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

Initialisieren van de EBICS-koppeling

Instellen van de communicatieverbinding

De communicatie wordt opgezet op basis van een URL (Uniform Resource Locator). Als alternatief kan er ook een IP-adres van de betreffende bank worden gebruikt. De URL of het IP-adres wordt met de Klant gedeeld bij het sluiten van de overeenkomst met de Bank.

In het kader van het opzetten van de EBICS-koppeling deelt de Bank de volgende gegevens met de Deelnemers die zijn aangewezen door de Klant:

URL of IP-adres van de Bank
Omschrijving van de Bank
HostID
Compatibele versie(s) voor het EBICS-protocol en de beveiligingsprocedures
Partner-ID (klant-ID)
User-ID
Systeem-ID (voor Technische Deelnemers)
Nadere gegevens over de machtigingen van de Klant en de Deelnemer(s)

Elke Deelnemer die de Klant heeft aangewezen, ontvangt van de Bank een unieke user-ID, waarmee die Deelnemer geïdentificeerd kan worden. Indien er aan de Klant een of meer Technische Deelnemers zijn toegewezen (multi-user-systeem), geeft de Bank naast de user-ID ook een systeem-ID uit. Indien er geen Technische Deelnemers zijn aangewezen, zijn de systeem-ID's gelijk aan de user-ID's.

Initialiseren van sleutels van Deelnemers

De sleutelparen die een Deelnemer gebruikt voor de banktechnische EH's, de versleuteling van opdrachtgegevens en de ondertekening ter authenticatie moeten ter aanvulling op de in artikel 1 omschreven algemene voorwaarden ook aan de volgende vereisten voldoen:

De sleutelparen zijn uitsluitend en ondubbelzinnig aan de betreffende Deelnemer toegewezen.

In het geval dat een Deelnemer zijn sleutels zelfstandig genereert, moeten de privésleutels gegenereerd worden met middelen waar deze Deelnemer volledige controle over kan houden.

In het geval dat de sleutels door een derde zijn verstrekt, moet er gewaarborgd worden dat de Deelnemer de enige is die over de privésleutels beschikt.

Voor de privésleutels die ter legitimatie worden ingezet, stelt elke Gebruiker per sleutel een wachtwoord in, waarmee de toegang tot de betreffende privésleutel wordt afgeschermd.

Voor de privésleutels die voor de beveiliging van gegevensuitwisseling worden ingezet, stelt elke Deelnemer per sleutel een wachtwoord in, waarmee de toegang tot de betreffende privésleutel wordt afgeschermd. Een dergelijk wachtwoord hoeft niet te worden ingesteld als het beveiligingsmedium van de Deelnemer wordt bewaard in een technische omgeving die is beschermd tegen ongeautoriseerde toegang.

Voor het initialiseren van de Deelnemer bij de Bank moeten de openbare sleutels van de Deelnemer doorgegeven worden aan het systeem van de Bank. Daarvoor levert een Deelnemer zijn openbare sleutels langs twee van elkaar onafhankelijke communicatiekanalen aan bij de Bank:

Via de EBICS-koppeling, op basis van de daarvoor ingerichte opdrachtstypen van het systeem.

Aan de hand van een initialisatiebrief die is ondertekend door de rekeninghouder of een gemachtigde voor zijn rekening.

Voor het activeren van een Deelnemer controleert de Bank eerst de authenticiteit van de openbare sleutels van de Deelnemers die via EBICS zijn doorgegeven, aan de hand van de initialisatiebrieven die door de rekeninghouder of een gemachtigde voor zijn rekening zijn ondertekend.

Voor elke openbare sleutel van een Deelnemer dient de initialisatiebrief de volgende gegevens te bevatten:

Gebruiksdoel van de betreffende openbare sleutel van een Deelnemer
Elektronische handtekening
Ondertekening ter authenticatie
Versleuteling
De relevante ondersteunde versie per sleutelpaar
Lengte van de exponent
Exponent van de openbare sleutel in hexadecimale indeling
Lengte van de modulus

- Modulus des öffentlichen Schlüssels in hexadezimaler Darstellung
- Hashwert des öffentlichen Schlüssels in hexadezimaler Darstellung Die Bank prüft die Unterschrift des Kontoinhabers beziehungsweise des Kontobevollmächtigten auf dem Initialisierungsbrief sowie die

Übereinstimmung zwischen den über die EBICS-Anbindung und

den schriftlich übermittelten Hashwerten des öffentlichen Schlüssels des Teilnehmers. Bei positivem Prüfergebnis schaltet die Bank den betreffenden Teilnehmer für die vereinbarten Auftragsarten frei.

2.3 Initialisierung der bankseitigen Schlüssel

Der Teilnehmer holt den öffentlichen Schlüssel der Bank mittels einer

eigens dafür vorgesehenen systembedingten Auftragsart ab.

Der Hashwert des öffentlichen Bankschlüssels wird von der Bank zusätzlich über einen zweiten, mit dem Kunden gesondert vereinbarten Kommunikationsweg bereitgestellt.

Vor dem ersten Einsatz von EBICS hat der Teilnehmer die Echtheit der ihm per Datenfernübertragung übermittelten öffentlichen Bank-schlüssel dadurch zu überprüfen, dass er deren Hashwerte mit den Hashwerten vergleicht, die von der Bank über den gesondert vereinbarten Kommunikationsweg mitgeteilt wurden.

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

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.

- Private Teilnehmerschlüssel auf den Legitimations- und Sicherungsmedien dürfen nicht im Klartext abgespeichert werden.
- Spätestens nach fünfmaliger Fehleingabe des Passwortes wird das Legitimationsmedium gesperrt.
- Die Generierung der privaten und öffentlichen Teilnehmerschlüssel

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 Nutzer 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 an Stelle der bankfachlichen EU des Nutzers eine Transportunterschrift (Typ

Modulus van de openbare sleutel in hexadecimale indeling

Hashwaarde van de openbare sleutel in hexadecimale indeling De Bank controleert de ondertekening door de rekeninghouder of de gemachtigde voor zijn rekening op de initialisatiebrief en toetst ook of de hashwaarden van de openbare sleutels die zijn doorgegeven via de EBICS-koppeling

overeenstemmen met die van de schriftelijk doorgegeven hashwaarden. Bij een positieve uitslag activeert de Bank de betreffende Deelnemer voor de overeengekomen opdrachtstypen.

Initialiseren van sleutels uitgegeven door de Bank

Een Deelnemer haalt de openbare sleutel van de Bank aan de hand van een

speciaal daarvoor ingericht opdrachtstype op.

De Bank verstrekt de hashwaarde van de openbare banksleutel vervolgens ook via een tweede, met de Klant afzonderlijk overeengekomen communicatiekanaal.

Voor het eerste gebruik van EBICS dient de Deelnemer de echtheid van de openbare banksleutel die hem per gegevensuitwisseling op afstand is overgebracht, te controleren door de hashwaarden ervan te vergelijken met de hashwaarden die de Bank via het afzonderlijk overeengekomen communicatiekanaal heeft verstrekt.

De Klant moet waarborgen dat er software gebruikt wordt die de geldigheid verifieert van de servercertificaten die in het kader van de transportversleuteling zijn gebruikt, aan de hand van het certificeringspad dat de Bank afzonderlijk heeft verstrekt.

Bijzondere zorgvuldigheidsplichten bij het maken van legitimatie- en beveiligingsmedia door de Klant

In het geval dat de Klant zijn legitimatie- en beveiligingsmedia overeenkomstig de voorschriften van de EBICS-specificatie zelf aanmaakt en deze door de Bank laat initialiseren, dient hij het volgende te waarborgen:

In alle fasen van de authenticatie, waaronder de melding, overdracht en opslag, dienen de geheimhouding en de integriteit van het legitiematiemedium gewaarborgd te worden. De privésleutels van Deelnemers op de legitimatie- en beveiligingsmedia mogen niet in platte tekst worden opgeslagen.

Uiterlijk nadat het wachtwoord vijf keer verkeerd is ingevoerd, wordt het legitiematiemedium geblokkeerd.

De privésleutels en openbare sleutels van Deelnemers moeten in een beveiligde omgeving gegenereerd worden.

De legitimatie- en beveiligingsmedia zijn uitsluitend en uniek toegewezen aan de betreffende Deelnemer en mogen alleen door de betreffende Deelnemer worden gebruikt.

Indiening van opdrachten bij de Bank

De Gebruiker controleert of de opdrachtgegevens juist zijn en zorgt ervoor dat precies deze gegevens elektronisch ondertekend zijn. Wanneer er contact opgenomen wordt, controleert de Bank eerst of de betreffende Deelnemer voldoende machtigingen heeft, zoals een opdrachtstypemachtiging of eventuele overeengekomen limietcontroles. Over de uitkomst van verdere banktechnische controles, zoals toetsingen van de krediet- of bestedingslimiet of toetsingen van voldoende machtigingen voor de rekening, wordt de Klant op een later tijdstip geïnformeerd in het klantprotocol. Opdrachtgegevens die aan het systeem van de Bank zijn overgedragen, kunnen als volgt worden geautoriseerd:

Alle noodzakelijke banktechnische EH's worden samen met de opdrachtgegevens overgedragen.

In het geval dat er voor het betreffende opdrachtstype een Verdeelde Elektronische Handtekening (VEH) met de Klant is overeengekomen en de overgedragen EH's niet voldoende zijn voor een banktechnische goedkeuring, wordt de opdracht in het systeem van de Bank opgeslagen totdat alle noodzakelijk EH's wel zijn ingediend.

In het geval dat de Klant en de Bank overeenkomen dat per telematica overgebrachte opdrachtgegevens geautoriseerd kunnen worden met een verstrekte bijgevoegde nota of batchopdracht, dient de Gebruiker in plaats van de banktechnische EH een transporthandtekening (type

„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/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 Nutzer gelöscht werden. Soweit der Auftrag vollständig autorisiert wurde, ist nur noch ein Rückruf gemäß Nummer 9 der Bedingungen für die Datenfernübertragung 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 eingelierte Auftragsdaten werden als Auftrag durch die Bank erst dann ausgeführt, wenn die erforderlichen bankfachlichen EU beziehungsweise der unterschriebene Begleitzettel/Sammel-auftrag 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 auf Seiten 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 die neuen öffentlichen Teilnehmerschlüssel rechtzeitig vor dem Erreichen des Ablaufdatums zu übermitteln. Nach dem Erreichen des Ablaufdatums der alten Schlüssel ist eine Neu-initialisierung 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 sind die folgenden Auftragsarten zu nutzen:

- Aktualisierung des öffentlichen bankfachlichen Schlüssels (PUB)
- und
- Aktualisierung des öffentlichen Authentifikationsschlüssels und des öffentlichen Verschlüsselungsschlüssels (HCA)
- oder alternativ
- Aktualisierung aller drei oben genannter Schlüssel (HCS).

T) voor de technische beveiliging van de opdrachtgegevens te verstrekken. Daarvoor moet het bestand van een speciaal kenmerk voorzien worden dat aangeeft dat er buiten de transporthandtekening (type T) geen verdere EH voor deze opdracht is voorgelegd. De opdracht wordt goedgekeurd na een positieve controle van de handtekening van de Gebruiker op de bijgevoegde nota of batchopdracht door de Bank.

Indienen van opdrachten op basis van een Verdeelde Elektronische Handtekening (VEH)

De manier waarop de Klant gebruik zal maken van de Verdeelde Elektronische Handtekening

moet met de Bank worden overeengekomen.

De Verdeelde Elektronische Handtekening (VEH) dient gebruikt te worden als de autorisatie van opdrachten onafhankelijk van het transport van de opdrachtgegevens moet gebeuren, en eventueel ook door meerdere Deelnemers.

Zolang nog niet alle banktechnische EH's voorliggen die voor de autorisatie noodzakelijk zijn, kan de opdracht door een daartoe gemachtigde Gebruiker worden gewist. In het geval dat een opdracht volledig geautoriseerd is, blijft uitsluitend een herroeping overeenkomstig artikel 9 van de Voorwaarden voor gegevensuitwisseling op afstand mogelijk.

De Bank heeft het recht om opdrachten die niet volledig geautoriseerd zijn, na het verstrijken van de door de Bank afzonderlijk medegedeelde tijdslimiet te verwijderen.

Legitimiteitscontrole door de Bank

Opdrachtgegevens die per telematica zijn aangeleverd, worden door de Bank pas als opdracht uitgevoerd nadat de noodzakelijke banktechnische EH's dan wel de ondertekende bijgevoegde nota of batchopdracht zijn ontvangen en de controle daarvan tot een positieve uitslag heeft geleid.

Klantprotocollen

De Bank legt de volgende processen vast in klantprotocollen:

De overdracht van opdrachtgegevens aan het systeem van de Bank.

De overdracht van informatiebestanden van het systeem van de Klant naar het systeem van de Bank.

De uitslag van elke legitimiteitscontrole van opdrachten van de Klant door de Bank.

De verdere verwerking van opdrachten, voor zover deze de controle van handtekeningen en de melding van opdrachtgegevens betreffen.

Elke Deelnemer dient het klantprotocol tijdig in te zien en zich zo te informeren over de uitslag van de controles die de Bank heeft uitgevoerd.

Elke Deelnemer dient dit protocol, dat inhoudelijk overeenkomt met de bepalingen uit hoofdstuk 10 van Bijlage 1b, in zijn administratie te bewaren en op verzoek aan de Bank te overleggen.

Wijzigingen van de sleutels van Deelnemers met automatische activering

Indien de legitimatie- en beveiligingsmedia die een Deelnemer gebruikt, beperkt geldig zijn, dient deze Deelnemer zijn nieuwe openbare sleutels tijdig bij de Bank aan te leveren, vóór het verstrijken van de geldigheidsduur. Zodra de oude sleutels zijn verlopen, moeten er opnieuw sleutels geïnitieerd worden.

Indien een Deelnemer zijn sleutels zelf genereert, dient hij zijn deelnemerssleutels op een met de Bank overeengekomen tijdstip op basis van de daarvoor ingerichte opdrachtstypen te vernieuwen en voor het verlopen van de oude sleutels aan de Bank te verstrekken.

Voor de automatische activering van de nieuwe sleutels, zonder dat er opnieuw een of meer Deelnemers hoeven te worden geïnitieerd, kunnen de volgende opdrachtstypen worden ingezet:

Actualisatie van de openbare banktechnische sleutel (PUB)

en

Actualisatie van de openbare authenticatiesleutel en de openbare versleutelingssleutel (HCA)

of, alternatief,

Actualisatie van alle drie de hierboven genoemde sleutels

Die Auftragsarten PUB und HCA bzw. HCS 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 8 Absatz 3 der Bedingungen für die Datenfernübertragung 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 Sicherungs-medien 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 über die von der Bank gesondert bekannt gegebene Sperrfazität 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 Sperrfazität sperren lassen.

Anlage 1b:

Spezifikation der EBICS-Anbindung

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

Anlage 1c:

Sicherheitsanforderungen an das EBICS-Kundensystem

Über die in Anlage 1a Nummer 6 beschriebenen Sicherheitsmaßnahmen hinaus sind durch den Kunden folgende Anforderungen zu berücksichtigen:

- Die vom Kunden für das EBICS-Verfahren eingesetzte Software muss die in Anlage 1a 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 Virens Scanner zu installieren, der regelmäßig mit den

neuesten Virendefinitions-Dateien auszustatten ist.

- Das EBICS-Kundensystem ist so einzurichten, dass sich der Teilnehmer vor dessen 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 bank-fachliche 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.

(HCS).

Die opdrachtstypen PUB, HCA en HCS moeten altijd van een geldige banktechnische EH van de Gebruiker worden voorzien. Na een geslaagde wijziging, kunnen alleen de nieuwe sleutels worden gebruikt.

Indien de Elektronische Handtekening niet geverifieerd kon worden, verloopt het proces verder zoals voorgeschreven in artikel 8, paragraaf 3, van de Voorwaarden voor gegevensuitwisseling op afstand.

Wijzigingen van de sleutels mogen pas uitgevoerd worden nadat alle opdrachten zijn afgewerkt. Anders moeten nog niet uitgevoerde opdrachten met de nieuwe sleutel opnieuw worden ingediend.

Blokkeren van sleutels van Deelnemers

Bestaat het vermoeden dat sleutels van Deelnemers oneigenlijk worden gebruikt, is de betreffende Deelnemer verplicht zijn toegangsmachtigingen voor alle systemen van de Bank waar de gecompromitteerde sleutel voor gebruikt kan worden, te blokkeren.

Indien de Deelnemer geldige legitimatie- en beveiligingsmedia heeft, kan hij zijn toegangsmachtiging via de EBICS-koppeling blokkeren. Daarbij wordt een bericht met het opdrachtstype 'SRP' (*sperren*, Duits voor 'blokkeren') verzonden en vervolgens de toegang geblokkeerd voor de betreffende Deelnemers met wiens user-ID dit bericht is verzonden. Eenmaal geblokkeerd kan deze Deelnemer geen nieuwe opdrachten meer indienen via EBICS-koppeling tot de machtigingen opnieuw zijn geïnitieerd, zoals omschreven in artikel 2.

Indien de Klant geen geldige legitimatie- en beveiligingsmedia meer heeft, kan hij buiten de telematicaprocedure om zijn legitimatie- en beveiligingsmedia laten blokkeren via de door de Bank afzonderlijk medegedeelde blokkeringsfaciliteit.

De Klant kan buiten de telematica-procedure ook de legitimatie- en beveiligingsmedia van een Deelnemer of de gehele telematica-toegang via de door de Bank medegedeelde blokkeringsfaciliteit laten blokkeren.

Bijlage 1b:

Specificatie van de EBICS-koppeling

De specificatie vindt u op de website www.ebics.de.

Bijlage 1c:

Beveiligingsvereisten voor het EBICS-systeem van de Klant

Naast de in Bijlage 1a, artikel 6, beschreven beveiligingsmaatregelen dient de Klant aan de volgende vereisten te voldoen:

De software die de Klant voor de EBICS-procedure gebruikt, moet voldoen aan de vereisten uit Bijlage 1a.

EBICS-klantsystemen mogen niet zonder firewall gebruikt worden. Een firewall is een beveiligingsfunctie die al het binnenkomende en uitgaande berichtenverkeer controleert en alleen bekende of geautoriseerde verbindingen toestaat.

Er moet een virusscanner worden geïnstalleerd, die regelmatig

moet worden bijgewerkt met de nieuwste virusdefinitiebestanden.

Het EBICS-klantsysteem moet zo worden ingericht dat elke Deelnemer moet inloggen voordat hij het kan gebruiken. Daarbij moet de Deelnemer als normale gebruiker inloggen, niet als beheerder (die onder meer gemachtigd is om programma's te installeren).

De interne IT-communicatielijnen voor niet-versleutelde banktechnische gegevens of voor niet-versleutelde EBICS-berichten moeten worden beschermd tegen af luisteren en manipulatie.

Als er updates komen die de beveiliging verbeteren van het gebruikte besturingssysteem of van andere veiligheidsrelevante softwareprogramma's, moeten deze updates uitgevoerd worden op de gebruikte EBICS-systemen.

De naleving van deze vereisten is uitsluitend de verantwoordelijkheid van de Klant.

Anlage 2: derzeit nicht besetzt

Anlage 3:

Spezifikation der Datenformate

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

Bijlage 2: momenteel niet bijgevoegd

Bijlage 3:

Specificatie van gegevensindelingen

De specificatie vindt u op de website www.ebics.de