Bedingungen für Datenfernübertragung (DFÜ)

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 Verfügungslimite.

3. Die Datenfernübertragung ist über zwei verschiedene Verfahren, die EBICS-Anbindung (Anlagen 1a bis 1c), sowie MCFT-Anbindung (Anlage 3) möglich. Das maßgebliche Übertragungsverfahren wird zwischen Kunde und Bank vereinbart.

4. Der Satz- und Dateiaufbau für die Übermittlung von Aufträgen und den Informationsabruf wird in der Spezifikation der Datenformate (Anlage 4) beschrieben.

5. Zusätzlich zu den vereinbarten Diensten kann der Kunde auch die Oberbank Business App nutzen. Diese Bestimmungen gelten ausdrücklich auch für die Oberbank Business App. Technische Voraussetzungen für die Oberbank Business App und die im Rahmen der Oberbank Business App verfügbaren Dienstleistungen sind auf der Oberbank Website unter www.oberbank.at/business-app aufgelistet.

2. Nutzer und Teilnehmer, Legitimations- und Sicherungsmedien

1. Aufträge können über die EBICS bzw. MCFT-Anbindung nur vom Kunden oder seinen Kontobevollmächtigten erteilt werden. Kunde und Kontobevollmächtigte werden im Folgenden einheitlich als "Nutzer" bezeichnet. Zur Autorisierung von per DFÜ übermittelten Auftragsdaten mittels Elektronischer Unterschrift benötigt jeder Nutzer jeweils indivi- duelle, von der Bank freigeschaltete Legitimationsmedien. Die Anforderungen an die Legitimationsmedien sind in Anlage 1a beziehungsweise Anlage 3a 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. Für den Datenaustausch über die MCFT-Anbindung benötigt jeder Nutzer ein von der Bank bereitgestelltes DFÜ-Passwort. Die Anforderungen an das DFÜ-Passwort sind in Anlage 3a beschrieben.

3. Verfahrensbestimmungen

1. Für das zwischen Kunde und Bank vereinbarte Übertragungsverfahren gelten jeweils die in Anlage 1a beziehungsweise Anlage 3a sowie die in der Dokumentation der technischen Schnittstellen (Anlage 1b) und der Spezifikation der Datenformate (Anlage 4) beschriebenen Anforderungen.

2. Der Kunde ist verpflichtet sicherzustellen, dass alle Teilnehmer die mit der Bank vereinbarten Verfahren und Spezifikationen beachten.

3. Die Belegung der Datenfelder richtet sich nach den Belegungs- und Kontrollrichtlinien des jeweils genutzten Formates.
   Die Angaben im Verwendungszweck haben sich ausschließlich auf den jeweiligen Zahlungsverkehrsvorgang im Datensatz zu beziehen. Am Anfang des Datenfeldes "Verwendungszweck" sind linksbündig solche Angaben unterzubringen, auf die der Begünstigte / Zahlungspflichtige maschinell zuzugreifen beabsichtigt oder die der Überweisende / Zahlungsempfänger benötigt, falls die Zahlung als unanbringlich beziehungsweise unbezahlt an ihn zurückgeleitet wird.

Oberbank AG, Niederlassung Deutschland, Sitz: München, Registernummer: HRB 122267, Amtsgericht München, Niederlassungsleiter und ständige Vertreter: Robert Dempf, Franz Kinzler, Ralf Wenzel, Stefan Ziegler. Oberbank AG, Hauptsitz: Linz, Österreich, Rechtsform: Aktiengesellschaft, Firmenbuchnummer: FN 79063 w, Landesgericht Linz, Vorstand: Vorsitzender Generaldirektor Dr. Franz Gasselsberger, MBA, Vorstandsdirektor Mag. Florian Hagenauer, MBA, Vorstandsdirektor Martin Seiter, MBA, Vorstandsdirektorin Mag. Isabella Lehner, MBA, Aufsichtsratsvorsitzender: Dr. Andreas König.

Die Belegung der Verwendungszweckangaben darf außerdem vom Nutzer nicht für die Vorgabe eines von ihm gewünschten Druckbildes benutzt werden, ohne dass die Stellenkapazität im Datenfeld "Verwendungszweck" des Datensatzes sowie in den etwaigen nachfolgenden Erweiterungsteilen mit Verwendungszweckangaben voll ausgenutzt ist.

Verwendungszweckangaben dürfen nicht die Übermittlung einer gesonderten Nachricht außerhalb des Zahlungsverkehrs (zB Rechnung, Lohn- und Gehaltsabrechnung) ersetzen. Werbetexte dürfen in den Verwendungszweckangaben nicht enthalten sein.

4. Der Nutzer hat die Kundenkennung des Zahlungsempfängers beziehungsweise des Zahlers gemäß den maßgeblichen Sonderbedingungen anzugeben. Die in die Abwicklung des Zahlungsauftrages eingeschalteten Zahlungsdienstleister sind berechtigt, die Bearbeitung ausschließlich anhand der Kundenkennung vorzunehmen. Fehlerhafte Angaben können Fehlleitungen des Auftrags zur Folge haben. Schäden und Nachteile, die hieraus entstehen, gehen zu Lasten des Kunden.
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 14 Kalendertagen bei Inlandszahlungsaufträgen und 30 Kalendertagen bei Auslandszahlungsaufträgen 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, gilt auch für MCFT-Anbindungen) beziehungsweise Kapitel 1.7 der Spezifikation für die MCFT-Anbindung (Anlage 3b) 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) Einreichung mit Begleitzettel/Sammelauftrag, wenn
      - der Begleitzettel/Sammelauftrag im vereinbarten Zeitraum bei der Bank eingeht und
      - der Begleitzettel/Sammelauftrag der Kontovollmacht entsprechend unterzeichnet worden ist.

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

1. Der Kunde ist in Abhängigkeit von dem mit der Bank vereinbarten Übertragungsverfahren verpflichtet sicherzustellen, dass alle Nutzer die Pflichten aus diesen Bedingungen und die in Anlage 1a beziehungsweise Anlage 3a beschriebenen Legitimationsverfahren einhalten.
2. Mit Hilfe 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, 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 zur Geheimhaltung der Legitimationsmedien 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

1. 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 Duplikates hat, kann den Datenaustausch missbräuchlich durchführen.

2. Der Kunde ist im Rahmen der MCFT-Anbindung verpflichtet sicherzustellen, dass alle Teilnehmer die in Anlage 3a 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 Duplikates 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 die EBICS / MCFT-Verfahren geltenden Sicherheitsanforderungen sind in Anlage 1c, 3b beschrieben.

7. Sperre der Legitimations- und Sicherungsmedien

1. Gehen die Legitimations- oder Sicherungsmedien verloren, werden sie anderen Personen bekannt oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so hat der Teilnehmer unverzüglich seinen DFÜ-Zugang bei der Bank zu sperren oder sperren zu lassen. Näheres regeln Anlage 1a, sowie Anlage 3a. Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

2. Wird drei Mal hintereinander versucht, einen Auftrag mit einem falschen Legitimationsmedium an die Bank zu übermitteln oder mit einem falschen Sicherungsmedium den Datenaustausch durchzuführen, so sperrt die Bank den DFÜ-Zugang des betreffenden Teilnehmers. Diese Sperre kann mittels DFÜ nicht aufgehoben werden. Zur Aufhebung dieser Sperre muss sich der Kunde mit seiner Bank in Verbindung setzen.

3. 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 Sperrfazilität sperren lassen.
   Über die Electronic Banking Hotline kann die Sperre an Geschäftstagen in der Zeit von 08-17 Uhr

   telefonisch aus Deutschland: +49 (0)89 / 55989 - 255
   telefonisch aus Österreich: +43 (0)732 / 7802 - 32128
   per Mail: elba@oberbank.at

   mit Angabe der Kontonummer beauftragt werden. Als Geschäftstag gilt jeder Tag, an dem die Oberbank den für die Ausführung von Zahlungsaufträgen erforderlichen Geschäftsbetrieb unterhält.

   Die Aufhebung der Sperre muss vom Verfüger schriftlich (Original-Unterschrift) oder persönlich bei der kontoführenden Oberbank Filiale beantragt werden, oder telefonisch unter obiger Telefonnummer, wobei sich der Verfüger entsprechend zu legitimieren hat.

   Die Electronic Banking Hotline steht auch für Sicherheitsfragen im Zusammenhang mit Zahlungsdiensten zur Verfügung.

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

8. Behandlung eingehender Auftragsdaten durch die Bank

1. Die der Bank per DFÜ-Verfahren übermittelten Auftragsdaten werden im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeitet. Kann die Bank eine vom Kunden im Format "SEPA-Überweisung" beleglos erteilte Überweisung nicht in diesem Format ausführen, weil der vom Kunden angegebene Zahlungsdienstleister des Zahlungsempfängers dieses Format noch nicht unterstützt, und weist die Bank die Überweisung nicht zurück, führt sie die Überweisung in einem von dem Zahlungsdienstleister des Zahlungsempfängers unterstützten Format aus. Bei diesem Formatwechsel können die in der Anlage 5 genannten Datenelemente - oder Teile davon - nicht übermittelt werden.

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 Auftrags- datensätze mit den Bestimmungen gemäß Anlage 4. Ergibt die Prüfung Unstimmigkeiten, wird die Bank die betreffenden Auftragsdaten nicht bearbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen. Die Bank ist berechtigt, nicht vollständig autorisierte Auftragsdaten nach Ablauf des von der Bank gesondert mitgeteilten Zeitlimits zu löschen.

4. Ergeben sich bei den von der Bank durchgeführten Prüfungen der Dateien oder Datensätze nach Anlage 4 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. Die Bank ist verpflichtet die vorstehenden Abläufe und die Weiterleitung der Aufträge zur Bearbeitung im Kundenprotokoll (siehe Anlage 1a und 3a) zu dokumentieren. Der Kunde ist seinerseits verpflichtet, das Kundenprotokoll zeitnah abzurufen und sich über den Status der Auftragsbearbeitung zu informieren. Bei Unstimmigkeiten soll er sich mit der Bank in Verbindung setzen.

9. Rückruf

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

2. Die Widerrufbarkeit eines Auftrags richtet sich nach den dafür geltenden Sonderbedingungen (zB Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des DFÜ-Verfahrens oder, wenn mit dem Kunden vereinbart, nach den Vorgaben von Kapitel 11 der Anlage 4 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 eingelieferten Auftragsdaten wurden gemäß Nummer 3 Absatz 8 autorisiert
   - das festgelegte Datenformat ist eingehalten
   - das Verfügungslimit nicht überschritten wurde.
   - Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (zB ausreichende Kontodeckung gemäß den Bedingungen für den Überweisungsverkehr) liegen vor.

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

11. Haftung

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 (zB Bedingungen für den Überweisungsverkehr).

2. Haftung des Kunden bei missbräuchlicher Nutzung der Legitimations- oder Sicherungsmedien

   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.

   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 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 Kunden und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

   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.

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.

Ergänzend gelten die "Allgemeinen Geschäftsbedingungen" der Oberbank AG, Linz, Niederlassung Deutschland, in der jeweils gültigen Fassung. Diese können jederzeit eingesehen und auf Wunsch auch zugesandt werden.

Änderungen dieser Bedingungen samt Anlagen werden dem Kunden schriftlich bekannt gegeben. Sie gelten als genehmigt, wenn der Kunde nicht schriftlich Widerspruch erhebt. Auf diese Folge wird ihn die Bank bei Bekanntgabe besonders hinweisen. Der Kunde muss Widerspruch innerhalb von 2 Monaten nach Bekanntgabe der Änderungen an die Bank absenden.

Anlage 1a: EBICS-Anbindung
Anlage 1b: Spezifikation der EBICS-Anbindung
Anlage 1c: Sicherheitsanforderungen an das EBICS-Kundensystem
Anlage 3a: MCFT Anbindung
Anlage 3b: Sicherheitsanforderungen an das MCFT-Kundensystem
Anlage 4: Spezifikation der Datenformate
Anlage 5: Weiterleitung von Daten bei Formatwechsel

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 Teilnehmerschlüssel 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.

In der Oberbank Business App wird bei EBICS mittels elektronischer Unterschrift autorisiert.

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 das Banksystem. "Technische Teilnehmer" (siehe Nummer 2.2) können nur eine EU vom Typ "T" zugewiesen bekommen.

Mit dem vom Kunden verwendeten Programm können verschiedene Nachrichten (zB Aufträge für den Inlands- und Auslandszahlungsverkehr, aber auch für Initialisierung, den Protokollabruf und die Abholung von Konto- und Umsatzinformationen etc.) erstellt werden. Die Bank teilt dem Kunden mit, welche Nachrichtenarten genutzt werden können und welcher EU-Typ hierfür anzuwenden ist.

1.2. 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 von der Banksystem 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.

1.3. 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.

2. Initialisierung der EBICS-Anbindung

2.1. Einrichtung der Kommunikationsverbindung

Der Kommunikationsaufbau erfolgt unter Verwendung einer URL (Uniform Ressource 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
- Bezeichnung der BankPartner-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 Schlüsseln

2.2.1. Neuinitialisierung der Teilnehmerschlüssel

Die vom Teilnehmer eingesetzten Schlüsselpaare für die bankfachliche EU, die Verschlüsselung der Auftragsdaten und die Authentifikationssignatur müssen zusätzlich zu den in Nummer 1 beschriebenen allgemeinen 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 Initialisierungsbriefe die Authentizität der über EBICS übermittelten öffentlichen Teilnehmerschlüssel.

Zu jedem öffentlichen Teilnehmerschlüssel enthält der Initialisierungsbrief die folgenden Daten:

- Verwendungszweck des öffentlichen Teilnehmerschlüssels
- Elektronische Unterschrift
- Authentifikationssignatur
- Verschlüsselung
- Die jeweils unterstützten Version pro Schlüsselpaar
- Längenangabe des Exponenten
- Exponent des öffentlichen Schlüssels in hexadezimaler Darstellung
- Längenangabe des Modulus
- Modulus des öffentlichen Schlüssels in hexadezimaler Darstellung
- Hashwert des öffentlichen Schlüssels in hexadezimaler Darstellung

Die Bank prüft die Unterschrift des Kontoinhabers 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 Bankschlüsseln 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. Eine Ausnahme bildet die mit dem Kunden optional vereinbarte Online-Prüfung der Auftragsdaten durch die Bank.

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 "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 mit- geteilten Zeitlimits zu löschen.

4.2. Legitimationsprüfung durch die Bank

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

4.3. Kundenprotokolle

Die Bank dokumentiert in Kundenprotokollen die folgenden Vorgänge:

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

Der Teilnehmer hat sich durch 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 seiner Bank die neuen öffentlichen Teilnehmerschlüssel rechtzeitig vor dem Erreichen des Ablaufdatums zu übermitteln. Nach dem Erreichen des Ablaufdatums der alten Schlüssel ist eine Neuinitialisierung vorzunehmen.

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

Für eine automatische Freischaltung der neuen Schlüssel ohne eine erneute Teilnehmerinitialisierung sind die folgenden Auftragsarten zu nutzen:

- Aktualisierung des öffentlichen bankfachlichen Schlüssels (PUB) und
- Aktualisierung des öffentlichen Authentifikationsschlüssels und des öffentlichen Verschlüsselungsschlüssels (HCA)

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

Anlage 1b: **Spezifikation der EBICS-Anbindung**

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

Anlage 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 Virenscanner 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 zB berechtigt ist, die Installation von Programmen vorzunehmen, zu erfolgen.
- Die internen IT-Kommunikationswege für unverschlüsselte bankfachliche 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.

Anlage 3a: **MCFT-Anbindung**

1. Legitimations- und Sicherungsverfahren

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

Folgende Legitimations- und Sicherungsverfahren werden in der MCFT-Anbindung eingesetzt:

- Elektronische Unterschriften (EU)
- DFÜ Passwort
- Komprimierung Verschlüsselung

1.1. Elektronische Unterschriften (EU)

Für die MCFT-Anbindung wird das Legitimationsverfahren der Elektronischen Unterschrift (EU) verwendet. Dabei sind die folgenden EU-Typ definiert:

- "E" = Einzelunterschrift
- "A" = Erstunterschrift
- "B" = Zweitunterschrift
- "T" = Transportberechtigung (nur senden, abholen und initiieren)

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

Für die elektronische Unterschrift verfügt der Nutzer über ein Schlüsselpaar, das aus einem privaten und einen öffentlichen Schlüssel besteht. Der private Schlüssel ist gegen unautorisiertes Auslesen und Veränderung zu schützen. Der öffentliche Schlüssel ist dem Kreditinstitut gemäß dem in Nummer 2.2. beschriebenen Verfahren mitzuteilen. Das Schlüsselpaar des Nutzers kann auch für die Kommunikation mit anderen Kreditinstituten einge- setzt werden.

1.2. DFÜ-Passwort

Bei der MCFT-Anbindung wird der Datenaustausch zwischen Kunden und Kreditinstitut mit einem DFÜ-Passwort abgesichert. Jeder Nutzer erhält hierfür ein gesondertes Passwort, dass dem Nutzer im Rahmen der Initialisierung der MCFT-Anbindung (siehe Nummer 2.1.) vom Kreditinstitut mitgeteilt wird. Der Nutzer ist verpflichtet, dieses Passwort im Rahmen der Initialisierung zu ändern.

Der Kunde stellt sicher, dass jeder Nutzer dafür Sorge trägt, dass keine andere Person Kenntnis von seinem DFÜ-Passwort erlangt. Denn jede andere Person, die das DFÜ-Passwort kennt, kann den Datenaustausch mit dem Kreditinstitut durchführen.

Für die Durchführung des Datenaustauschs gibt der Nutzer sein DFÜ-Passwort ein.

2. Initialisierung der MCFT-Anbindung

2.1. Einrichtung der Kommunikationsverbindung

Das Kreditinstitut stellt dem Kunden je benannten Nutzer die zur Aufnahme einer Verbindung über Datenfern-übertragung (DFÜ) erforderlichen Daten, auf dem Postweg oder per eMail, als Bankparameterdatei zur Ver-fügung. Dabei handelt es sich um:

- KundenID
- Hostname
- IP-Adresse inkl. PortNummer
- HostTyp
- Teilnehmernummer
- Erstes DFÜ-Passwort

Der Kunde liest diese Bankparameterdatei für das Kreditinstitut in seine Software ein. Der Kunde definiert pro Auftragsart die erforderliche Mindestanzahl von Elektronischen Unterschriften.

Jeder Nutzer führt in seinem Programm eine Funktion zur Änderung seines DFÜ-Passwortes inkl. Generierung seiner EU-Schlüssel ("INI") aus.

2.2. Initialisierung der Schlüssel

Das vom Nutzer eingesetzte Schlüsselpaar muss zusätzlich zu den in Nummer 1 beschriebenen allgemeinen Bedingungen den nachfolgenden Anforderungen genügen:

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

Für die Initialisierung des Nutzers beim Kreditinstitut ist die Übermittlung des öffentlichen Schlüssels des Nutzers an das Banksystem erforderlich. Hierfür übermittelt der Nutzer dem Kreditinstitut seinen öffentlichen Schlüssel auf zwei voneinander unabhängigen Kommunikationswegen:

Über die MCFT-Anbindung mittels der hierfür vorgesehenen systembedingten Auftragsarten. Mit einem vom Teilnehmer gem. Vereinbarung (evtl. zweite Unterschrift notwendig) unterschriebenen Initialisierungsbrief per Fax an: Oberbank AG, Electronic Banking Support, Fax Nr.: 0043 / 732 / 79 59 68.

Für die Freischaltung des Nutzers überprüft das Kreditinstitut auf Basis des vom Teilnehmer gem. Vereinbarung (evtl. zweite Unterschrift notwendig) unterschriebenen Initialisierungsbrief die Authentizität des über MCFT übermittelten öffentlichen Schlüssels

Zu dem öffentlichen Schlüssel enthält der Initialisierungsbrief die folgenden Daten:

- Verwendungszweck "Elektronische Unterschrift" des öffentlichen Schlüssels
- Die jeweils unterstützten Versionen pro Schlüsselpaar
- Längenangabe des Exponenten
- Exponent des öffentlichen Schlüssels in hexadezimaler Darstellung
- Längenangabe des Modulus
- Modulus des öffentlichen Schlüssels in hexadezimaler Darstellung
- Hashwert des öffentlichen Schlüssels in hexadezimaler Darstellung

Das Kreditinstitut prüft die Unterschrift des Teilnehmers gem. Vereinbarung (evtl. zweite Unterschrift notwendig) auf dem Initialisierungsbrief sowie die Übereinstimmung zwischen den über die MCFT-Anbindung und den schriftlich per Fax übermittelten Hashwert des öffentlichen Schlüssels des Nutzers. Bei positivem Prüfer- gebnis schaltet das Kreditinstitut den betreffenden Nutzer für die vereinbarten Auftragsarten frei.

3. Auftragserteilung an das Kreditinstitut

3.1. Auftragserteilung mittels Elektronischer Unterschrift (EU)

Grundsätzlich werden Auftragsdateien und Kontoinformationen verschlüsselt und komprimiert zwischen Kunden und Banksystem ausgetauscht.

Der Nutzer überprüft die Auftragsdaten auf ihre Richtigkeit und stellt sicher, dass genau diese Daten elektronisch unterschrieben werden. Bei Aufnahme der Kommunikation wird zuerst ein Startblock vorgelagert. Dieser Startblock enthält alle zur Prüfung erforderlichen Informationen, wie Kunden-ID, Teilnehmer-Nr., zu belastendes Konto, die Elektronische Unterschrift und Prüfsummen zur gesamten Datei. Dadurch ist es möglich, frühzeitig Fehler / Manipulationen festzustellen und die eigentliche Datenübertragung zu unterbinden.

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

2. Sofern mit dem Kunden für die jeweilige Auftragsart die verteilte Elektronische Unterschrift (VEU) vereinbart wurde und die übermittelten EU für die Freigabe nicht ausreichen, wird der Auftrag bis zur Abgabe aller erforderlichen EU im Banksystem gespeichert.

Wird eine Elektronische Unterschrift per MCFT übermittelt, dann enthält der Startblock zusätzlich den "Fingerab- druck" zur Originaldatei und auch die Elektronische Unterschrift selbst. Dies hat den Vorteil, dass die EU - sofern alle erforderlichen Unterschriften geleistet wurden - bereits während der Kommunikation verifiziert werden kann. Im Startblock können bis zu 6 Unterschriften übermittelt werden.

Ergibt die Prüfung auf der Bankseite, dass

- eine der im Startblock enthaltene Unterschrift nicht korrekt ist, wird die DFÜ vor der Übertragung der Originaldatei abgebrochen.
- Alle Unterschriften korrekt sind, wird die Originaldatei übertragen. Nach der Übertragung der Originaldatei wird auf Bankseite der "Fingerabdruck" nachgerechnet und mit demjenigen verglichen, der im Startblock mit übertragen und für korrekt befunden wurde. Ergibt die Nachberechnung des "Fingerabdrucks" eine Übereinstimmung mit den übertragenen Werten, wird dies dem Kundensystem im Schlussblock mit einem "OK" mitgeteilt. Stimmt der nachgerechnete "Fingerabdruck" nicht mit dem im Startblock übermittelten überein, wird die Originaldatei zurückgewiesen.

Schlussnachrichten werden entweder bei Beendigung der Kommunikation oder des Dialoges übermittelt. Sie enthalten Antwort-Codes, die den Status des Ergebnisses der DFÜ beschreiben. Die beim Kundensystem einge- henden Antwortcodes werden dort ausgewertet und in den entsprechenden Protokollen angezeigt. Zusätzlich kann der Kunden das durch das Kreditinstitut zeitlich versetzt bereitgestelltes Kundenprotokoll abrufen.

Für die Abfrage von Kontoinformationen bei dem Kreditinstitut sind die gewünschten Abholaufträge zu erstellen und an das Kreditinstitut zu übermitteln. Hierzu ist das entsprechende DFÜ-Passwort des Nutzers einzugeben. Eine bankfachliche EU ist für die Abfrage von Informationen nicht erforderlich.

3.2. 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 (VEU) ist dann einzusetzen, wenn die Autorisierung von Aufträgen unab- hängig vom Transport der Auftragsdaten und ggf. auch durch mehrere Teilnehmer erfolgen soll.

Soweit der Auftrag vollständig autorisiert wurde, ist nur noch ein Rückruf gemäß Punkt 9 der Sonderbedingungen für Datenfernübertragung möglich.

Das Kreditinstitut ist dazu berechtigt, nicht vollständig autorisierte Aufträge nach Ablauf von 14 Tagen zu löschen.

3.3. Legitimationsprüfungen durch das Kreditinstitut

Eine empfangene Auftragsdatei wird durch das Kreditinstitut erst dann ausgeführt, wenn die erforderliche Anzahl von Elektronischen Unterschriften eingegangen sind und mit positivem Ergebnis geprüft wurden.

3.4. Kundenprotokolle

Das Kreditinstitut 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 Nutzer hat sich durch Abruf des Kundenprotokolls über das Ergebnis der auf Seiten des Kreditinstituts durchgeführten Prüfungen zu informieren.

Der Teilnehmer hat dieses Protokoll zu seinen Unterlagen zu nehmen und auf Anforderung des Kreditinstitutes zur Verfügung zu stellen.

4. Änderung der Schlüssel eines Nutzers

4.1. Änderung der Schlüssel mit automatischer Freischaltung

Wenn der Nutzer seine Schlüssel selbst generiert, so hat er zu dem mit dem Kreditinstitut 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 des neuen Schlüssels ohne eine erneute Teilnehmerinitialisierung ist die folgende Auftragsart zu nutzen:

- Aktualisierung des öffentlichen Schlüssels (PUB)

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

Wenn die elektronische Unterschrift nicht erfolgreich geprüft werden konnte, wird wie unter Punkt 6 (3) der Sonderbedingungen für Datenfernübertragung verfahren.

Die Schlüsseländerung darf erst nach Abarbeitung aller Aufträge erfolgen. Ansonsten sind die noch nicht ausge- führten Aufträge mit dem neuen Schlüssel neu zu erteilen.

4.2. Änderung der Schlüssel mit Neuinitialisierung

Der Nutzer kann per DFÜ durch Übermittlung eines neuen öffentlichen Schlüssels (Auftragsart "PUB") sein bisheriges Schlüsselpaar ersetzen. Das neue Schlüsselpaar wird erst nach Eingang (per Fax) des hierzu erstellten entsprechenden Initialisierungsprotokolls (INIBrief) bei dem Kreditinstitut freigeschaltet. Erst danach können mit dem neuen Schlüssel unterschriebene Aufträge ausgeführt werden.

Nach Freischaltung des neuen öffentlichen Schlüssels durch das Kreditinstitut sind Aufträge, die noch nicht an das Kreditinstitut übertragen wurden, mit dem neuen Schlüsselpaar neu zu legitimieren und dem Kreditinstitut zu übermitteln.

5. Sperrung der Schlüssel eines Nutzers

Besteht der Verdacht des Missbrauchs des Schlüssels, ist der Nutzer dazu verpflichtet, seine Zugangsberechtigung zu allen Banksystemen zu sperren, die den kompromittierten Schlüssel verwenden.

Wenn der Nutzer nicht mehr über gültige Legitimationsmedien verfügt, kann er außerhalb des DFÜ-Verfahrens seine Legitimations- und Sicherungsmedien durch das Kreditinstitut sperren lassen.

Weitere Angaben zur Sperrung, aber auch Entsperrung siehe Punkt 7 der Sonderbedingungen für Datenfernübertragung.

Anlage 3b: **Sicherheitsanforderungen an das MCFT-Kundensystem**

Über die in Anlage 3a Nummer 5 beschriebenen Sicherheitsmaßnahmen hinaus sind durch den Kunden folgende Anforderungen zu berücksichtigen:

- Die vom Kunden für das MCFT-Verfahren eingesetzte Software muss die in Anlage 3a beschriebenen Anforderungen erfüllen.
- MCFT-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 Virenscanner zu installieren, der regelmäßig mit den neuesten Virendefinitions-Dateien auszustatten ist.
- Das MCFT-Kundensystem ist so einzurichten, dass sich der Teilnehmer vor dessen Nutzung anmelden muss. Die Anmeldung hat als normaler Benutzer und nicht als Administrator, der zB berechtigt ist, die Installation von Programmen vorzunehmen, zu erfolgen.
- Die internen IT-Kommunikationswege für unverschlüsselte bankfachliche Daten oder für unverschlüsselte MCFT-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 MCFT-Kundensysteme mit diesen aktualisiert werden.

Die Umsetzung dieser Anforderungen liegt ausschließlich in der Verantwortung des Kunden.

Anlage 4: **Spezifikation der Datenformate**

Die Daten-Formate werden auf der Oberbank www.oberbank.at / Firmenkunden / Electronic Banking / MultiCash / Downloadservice zum Herunterladen bereitgestellt.

Anlage 5: **Weiterleitung von Daten bei Formatwechsel**

Kann die Bank eine vom Kunden im Format "SEPA-Überweisung" per DFÜ erteilten Überweisungsauftrag nicht in diesem Format ausführen, weil der vom Kunden angegebene Zahlungsdienstleister des Zahlungsempfängers dieses Format noch nicht unterstützt, und weist die Bank den Überweisungsauftrag nicht zurück, führt sie die Überweisung in einem vom Zahlungsdienstleister des Zahlungsempfängers unterstützten Format aus.

[Die folgenden Listen gelten nur bei Anwendung der "Translation Rules MX pacs.008.001.01 to MT 103" vom Juni 2007]

1. Bei dem Formatwechsel können die folgenden Datenelemente nicht übermittelt werden:

- Abweichender Zahlungsempfänger (Payment Information " Credit Transfer Transaction Information " Ultimate Creditor)
- Abweichender Zahler (Payment Information "Ultimate Debtor und Payment Information" Credit Transfer Transaction Information" Ultimate Debtor)
- Identifikation des Zahlungsempfängers (Payment Information "Credit Transfer Transaction Information" Creditor " Identification)
- Identifikation des Zahlers (Payment Information "Debtor" Identification)

2. Bei dem Formatwechsel können die folgenden Datenelemente nur teilweise übermittelt werden:

- Adresse des Zahlungsempfängers (Payment Information "Credit Transfer Transaction Information" Creditor " Postal Address) [die ersten 66 der 140 ursprünglich möglichen Zeichen werden übermittelt]
- Adresse des Zahlers (Payment Information "Debtor" Postal Address) [die ersten 66 der 140 ursprünglich möglichen Zeichen werden übermittelt]
- Name des Zahlungsempfängers (Payment Information "Credit Transfer Transaction Information" Creditor " Name) [die ersten 66 der 70 ursprünglich möglichen Zeichen werden übermittelt]
- Name des Zahlers (Payment Information " Debtor " Name) [die ersten 66 der 70 ursprünglich möglichen Zeichen werden übermittelt]
- Verwendungszweck (Payment Information " Credit Transfer Transaction Information " Remittance Information) [Kundenreferenz und Verwendungszweck werden gemeinsam übermittelt, aber zusammen nicht mehr als 130 Zeichen. Die Kundenreferenz (End to End Identification) wird dabei vorangestellt und ist immer vollständig angegeben.]

Anlage 6: **Schnittzeiten der Oberbank**

Annahmezeiten für Zahlungsaufträge

Zahlungsaufträge, die innerhalb der unten angeführten Zeiten bei der Oberbank eintreffen, werden unter Einhaltung folgender Voraussetzungen taggleich durchgeführt:

- Die per DFÜ eingelieferten Auftragsdaten wurden gemäß Nummer 3 Absatz 8 autorisiert
- das festgelegte Datenformat wird verwendet,
- das Verfügungslimit wird nicht überschritten.

Inlandszahlungsverkehr / SEPA Zahlungen

Standardüberweisung mit elektronischer Autorisierung	**16.30**
Eilüberweisungen mit elektronischer Autorisierung	**16.30**
Eilüberweisungen grenzüberschreitend	**16.30**

Auslandszahlungsverkehr

Zahlungsaufträge in EUR	**15.00**
Zahlungsaufträge in Fremdwährung mit Konvertierung	**11.15**
Zahlungsaufträge in Fremdwährung (USD, CAD, CHF, GBP, HUF, CZK) ohne Konvertierung	**15.00**