

Bedingungen für Datenfernübertragung

Herausgeber:
Bundesverband der
Deutschen Volksbanken und Raiffeisenbanken e. V., Berlin

Deutscher Genossenschafts-Verlag eG
Fassung: Oktober 2009
Art.-Nr. 467 400 **DG** VERLAG

Inhaltsverzeichnis

Bedingungen für Datenfernübertragung	
1 Leistungsumfang	5
2 Nutzer und Teilnehmer, Legitimations- und Sicherungsmedien	5
3 Verfahrensbestimmungen	6
4 Verhaltens- und Sorgfaltspflichten im Umgang mit den Legitimationsmedien für die Auftragserteilung	7
5 Verhaltens- und Sorgfaltspflichten im Umgang mit den Sicherungsmedien für den Datenaustausch	7
6 Sperre der Legitimations- und Sicherungsmedien	8
7 Behandlung eingehender Aufträge durch die Bank	8
8 Rückruf	9
9 Ausführung der Aufträge	9
10 Sicherheit des Kundensystems	9
11 Haftung	10
11.1 Haftung der Bank bei einer nicht autorisierten DFÜ-Verfügung und einer nicht oder fehlerhaft ausgeführten DFÜ-Verfügung	10
11.2 Haftung des Kunden bei missbräuchlicher Nutzung der Legitimations- oder Sicherungsmedien	10
11.2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige	10
11.2.2 Haftung des Kunden bei sonstigen nicht autorisierten Vorgängen vor der Sperranzeige	11
11.2.3 Haftung der Bank ab der Sperranzeige	11
11.3 Haftungsausschluss	11
12 Schlussbestimmungen	11
Anlage 1a: EBICS-Anbindung	12
1 Legitimations- und Sicherungsverfahren	12
1.1 Elektronische Unterschriften	12
1.1.1 Elektronische Unterschriften der Teilnehmer	12
1.2 Authentifikationssignatur	12
1.3 Verschlüsselung	13
2 Initialisierung der EBICS-Anbindung	13
2.1 Einrichtung der Kommunikationsverbindung	13
2.2 Initialisierung der Schlüssel	14
2.2.1 Neuinitialisierung der Teilnehmerschlüssel	14
2.2.2 Migration von FTAM nach EBICS	15
2.3 Initialisierung der bankseitigen Schlüssel	15
3 Auftragserteilung an die Bank	15
3.1 Auftragserteilung mittels Verteilter Elektronischer Unterschrift (VEU)	16
3.2 Legitimationsprüfung durch die Bank	16
3.3 Kundenprotokolle	16
4 Änderung der Teilnehmerschlüssel mit automatischer Freischaltung	17
5 Sperrung der Teilnehmerschlüssel	17
Anlage 1b: Spezifikation der EBICS-Anbindung	18
Anlage 1c: Sicherheitsanforderungen an das EBICS-Kundensystem	18
Anlage 2a: FTAM-Anbindung	18
1 Legitimations- und Sicherungsverfahren	18
1.1 Elektronische Unterschrift	19
1.2 DFÜ-Passwort	19
2 Initialisierung der FTAM-Anbindung	19
2.1 Einrichtung der Kommunikationsverbindung	19
2.2 Initialisierung der Schlüssel	20
3 Auftragserteilung an die Bank	21

Inhaltsverzeichnis

3.1	Auftragserteilung mit Elektronischer Unterschrift	21
3.2	Legitimationsprüfung durch die Bank	21
3.3	Kundenprotokolle	21
4	Änderung der Schlüssel eines Nutzers	22
4.1	Änderung der Schlüssel mit automatischer Freischaltung	22
4.2	Änderung der Schlüssel mit Neuinitialisierung	22
5	Sperrung der Schlüssel eines Nutzers	23
	Anlage 2b: Spezifikation der FTAM-Anbindung	23
	Anlage 3: Spezifikation der Datenformate	23

Bedingungen für Datenfernübertragung

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 Auftragserteilung sowie den Datenaustausch (Übermittlung von Aufträgen und Informationsabruf).
- (2) Die Bank gibt dem Kunden die Dienstleistungsarten bekannt, die er im Rahmen der Datenfernübertragung nutzen kann. Zur Nutzung der Datenfernübertragung gelten die mit der Bank vereinbarten Verfügungsmitel.
- (3) Die Datenfernübertragung ist über zwei verschiedene Verfahren, die EBICS-Anbindung (Anlagen 1a bis 1c) und die FTAM-Anbindung (Anlagen 2a und 2b) 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 3) beschrieben.

2 Nutzer und Teilnehmer, Legitimations- und Sicherungsmedien

- (1) Aufträge können über die EBICS- oder FTAM-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 benötigt jeder Nutzer jeweils individuelle, von der Bank freigeschaltete Legitimationsmedien. Die Anforderungen an die Legitimationsmedien sind in Anlage 1a beziehungsweise Anlage 2a definiert. Wenn mit der Bank vereinbart, können per DFÜ übermittelte Auftragsdaten mit unterschriebenem Begleitzettel 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 FTAM-Anbindung benötigt jeder Nutzer ein von der Bank bereitgestelltes DFÜ-Passwort. Die Anforderungen an das DFÜ-Passwort sind in Anlage 2a beschrieben.
- (4) Legitimations- und Sicherungsmedien sind Authentifizierungsinstrumente im Sinne von § 1 Absatz 5 Zahlungsdienstleistungsgesetz.

3 Verfahrensbestimmungen

- (1) Für das zwischen Kunde und Bank vereinbarte Übertragungsverfahren gelten jeweils die in Anlage 1a beziehungsweise Anlage 2a sowie die in der Dokumentation der technischen Schnittstellen (Anlage 1b beziehungsweise Anlage 2b) und der Spezifikation der Datenformate (Anlage 3) 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 (Anlage 3).
- (4) Der Nutzer hat den Identifikationscode (Bankleitzahl oder BIC) des Zahlungsdienstleisters des Zahlungsempfängers beziehungsweise des Zahlungsdienstleisters des Zahlers (Zahlstelle) sowie den Kontoidentifikationscode (Kontonummer oder IBAN) des Zahlungsempfängers beziehungsweise des Zahlers zutreffend anzugeben. Die in die Abwicklung des Zahlungsauftrages eingeschalteten Zahlungsdienstleister sind berechtigt, die Bearbeitung ausschließlich anhand von Zahlungsdienstleister- und Kontoidentifikationscode vorzunehmen. Fehlerhafte Angaben können Fehlleitungen des Auftrags zur Folge haben. Schäden und Nachteile, die hieraus entstehen, gehen zu Lasten des Kunden.
- (5) Vor Übertragung von Auftragsdaten an die Bank ist eine Aufzeichnung der zu übertragenden Dateien mit deren vollständigem Inhalt sowie der zur Prüfung der Legitimation übermittelten Daten zu erstellen. Diese ist von dem Kunden mindestens für einen Zeitraum von 14 Kalendertagen bei Inlandszahlungsaufträgen und 30 Kalendertagen bei Auslandszahlungsaufträgen ab dem Ausführungstag in der Form nachweisbar zu halten, dass die Datei auf Anforderung der Bank kurzfristig erneut zur Verfügung gestellt werden kann, sofern nichts Abweichendes vereinbart wird.
- (6) Außerdem hat der Kunde für jeden Datenaustausch ein maschinelles Protokoll, das inhaltlich den Bestimmungen von Kapitel 10 der Spezifikation für die EBICS-Anbindung (Anlage 1b) beziehungsweise Kapitel 1.7 der Spezifikation für die FTAM-Anbindung (Anlage 2b) 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 eingelierten Auftragsdaten sind wie mit der Bank vereinbart entweder mit Elektronischer Unterschrift oder dem unterschriebenen Begleitzettel 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, wenn
 - der Begleitzettel im vereinbarten Zeitraum bei der Bank eingegangen ist und
 - der Begleitzettel 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 in Anlage 1a beziehungsweise Anlage 2a 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:
 - Die den Nutzer legitimierenden Daten dürfen nicht außerhalb des Legitimationsmediums, z. B. auf der Festplatte des Rechners, gespeichert werden;
 - das Legitimationsmedium ist nach Beendigung der DFÜ-Nutzung aus dem Lesergerät zu entnehmen und sicher zu verwahren;
 - das zum Schutz des Legitimationsmediums dienende Passwort darf nicht notiert oder elektronisch abgespeichert werden;
 - bei Eingabe des Passwortes ist sicherzustellen, dass andere Personen dieses nicht auspähen 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 FTAM-Anbindung verpflichtet sicherzustellen, dass alle Nutzer die in Anlage 2a beschriebenen Sicherungsverfahren einhalten. 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 der Bank missbräuchlich durchführen.

6 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 und Anlage 2a. 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 Sperrfazität sperren lassen.
- (4) 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.

7 Behandlung eingehender Auftragsdaten durch die Bank

- (1) Die der Bank im 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 eventuell nicht alle Datenelemente der Originalnachricht 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 sowie die Übereinstimmung der Auftragsdatensätze mit den Bestimmungen gemäß Anlage 3. Ergibt die Prüfung Unstimmigkeiten, wird die Bank die betreffenden Auftragsdaten nicht bearbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen. Die Bank ist berechtigt, nicht vollständig autorisierte Auftragsdaten nach Ablauf des von der Bank gesondert mitgeteilten Zeitlimits zu löschen.

- (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) Die Bank ist verpflichtet die Abläufe (siehe Anlage 1a und 2a) und die Weiterleitung der Aufträge zur Bearbeitung im Kundenprotokoll 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.

8 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 Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des DFÜ-Verfahrens erfolgen. Hierzu hat der Kunde der Bank die Einzelangaben des Originalauftrages mitzuteilen.

9 Ausführung der Aufträge

- (1) Die Bank wird die Aufträge ausführen, wenn alle nachfolgenden Ausführungsbedingungen vorliegen:
 - Die per DFÜ eingeleferteten Auftragsdaten wurden gemäß Nummer 3 Absatz 8 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 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.

10 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.

11 Haftung

11.1 Haftung der Bank bei einer nicht autorisierten DFÜ-Verfügung und einer nicht oder fehlerhaft ausgeführten DFÜ-Verfügung

Die Haftung der Bank bei einer nicht autorisierten DFÜ-Verfügung und einer nicht oder fehlerhaft 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) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Legitimations- oder Sicherungsmediums, haftet der Kunde für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust, Diebstahl oder sonstigem Abhandenkommen des Legitimations- oder Sicherungsmediums ein Verschulden trifft.
- (2) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Verwendung eines Legitimations- oder Sicherungsmediums, ohne dass dieses verlorengegangen, gestohlen oder sonst abhanden gekommen ist, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung des Legitimations- oder Sicherungsmediums schuldhaft verletzt hat.
- (3) Für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 150 Euro nach Absätzen 1 und 2 hinaus haftet der Kunde, abweichend von § 675v BGB, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine vertraglichen Verhaltens- und Sorgfaltspflichten verstoßen hat.
- (4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 6 Absatz 1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.
- (5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den das Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.

11.2.2 Haftung des Kunden bei sonstigen nicht autorisierten Vorgängen vor der Sperranzeige

Beruhem 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

Anlage 2a: FTAM-Anbindung

Anlage 2b: Spezifikation der FTAM-Anbindung

Anlage 3: Spezifikation der Datenformate

Die Anlagen 1b, 2b und 3 sind unter der Webadresse www.ebics.de in ihrer jeweils gültigen Fassung verfügbar und können dort herunter geladen werden.

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.

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.

1.2 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 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 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
- Host-ID
- 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 Schlüssel

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 unterstützte 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.

2.2.2 Migration von FTAM nach EBICS

Soweit der Teilnehmer aufgrund seines vorhandenen DFÜ-Zugangs für FTAM bereits über einen gültigen, von der Bank freigeschalteten bankfachlichen Schlüssel verfügt, können im Zuge der gesondert vereinbarten Migration von FTAM nach EBICS vorhandene bankfachliche Schlüssel beibehalten werden, soweit diese mindestens der Version A004 entsprechen und dies so mit der Bank vereinbart ist.

In diesem Fall werden die öffentlichen Schlüssel für die Authentifikation und die Verschlüsselung mit den hierfür vorgesehenen Auftragsarten an die Bank übermittelt. Diese Nachrichten sind mit dem Schlüssel für die bankfachliche EU zu unterschreiben. Ein separater Versand eines unterschriebenen Initialisierungsbriefes entfällt.

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 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 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 durch die Bank.

3.1 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 8 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.

3.2 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 eingegangen sind und mit positivem Ergebnis geprüft wurden.

3.3 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 Unterschriftenprüfung, die Anzeige von Auftragsdaten betreffen
- Fehler bei der Dekomprimierung

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.

4 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 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)

oder alternativ

- Aktualisierung aller drei oben genannter Schlüssel (HCS).

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 7 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.

5 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 Sperrung 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 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 5 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 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 2a: FTAM-Anbindung

1 Legitimations- und Sicherungsverfahren

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

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

- Elektronische Unterschrift
- DFÜ-Passwort

1.1 Elektronische Unterschrift

Für die FTAM-Anbindung wird das Legitimationsverfahren der Elektronischen Unterschrift (EU) verwendet.

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 Nachrichtentypen 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 einem öffentlichen Schlüssel besteht. Der private Schlüssel ist gegen unautorisiertes Auslesen und Veränderung zu schützen. Der öffentliche Schlüssel ist der Bank gemäß dem in Nummer 2.2 beschriebenen Verfahren mitzuteilen. Das Schlüsselpaar des Nutzers kann auch für die Kommunikation mit anderen Banken eingesetzt werden.

1.2 DFÜ-Passwort

Bei der FTAM-Anbindung wird der Datenaustausch zwischen Kunden und Bank mit einem DFÜ-Passwort abgesichert. Jeder Nutzer erhält hierfür ein gesondertes Passwort, das dem Nutzer im Rahmen der Initialisierung der FTAM-Anbindung (siehe Nummer 2.1) von der Bank 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 der Bank durchführen.

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

2 Initialisierung der FTAM-Anbindung

2.1 Einrichtung der Kommunikationsverbindung

Die Bank teilt den vom Kunden benannten Nutzern die zur Aufnahme einer Verbindung über Datenfernübertragung (DFÜ) erforderlichen Daten mit. Dabei handelt es sich um:

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

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

Jeder Teilnehmer führt in seinem Programm eine Funktion zur Änderung des DFÜ-Passwortes („PWA“) 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, das den Zugriff auf den privaten Schlüssel absichert.

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

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

Für die Freischaltung des Nutzers überprüft die Bank auf Basis der vom Kontoinhaber oder einem Kontobevollmächtigten händisch unterschriebenen Initialisierungsbrief die Authentizität des über FTAM übermittelten öffentlichen Schlüssels.

Zu dem öffentlichen Schlüssel enthält der Initialisierungsbrief die folgenden Daten:

- Verwendungszweck „Elektronische Unterschrift“ des öffentlichen Schlüssels
- Die jeweils unterstützte 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 eigenhändige Unterschrift des Kontoinhabers beziehungsweise des Kontobevollmächtigten auf dem Initialisierungsbrief sowie die Übereinstimmung zwischen den über die FTAM-Anbindung und den schriftlich übermittelten Hashwert des öffentlichen Schlüssels des Nutzers. Bei positivem Prüfergebnis schaltet die Bank den betreffenden Nutzer für die vereinbarten Auftragsarten frei.

3 Auftragserteilung an die Bank

3.1 Auftragserteilung mit Elektronischer Unterschrift

Der Nutzer überprüft die zu unterschreibenden Dateien auf Richtigkeit und stellt sicher, dass genau diese Daten elektronisch unterschrieben werden. Zu jeder Datei mit Auftragsdaten werden entsprechend der Vereinbarung mit der Bank eine oder mehrere Elektronische Unterschriften erzeugt.

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

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

Kunde und Bank können vereinbaren, dass die Autorisierung von per DFÜ übermittelten Auftragsdaten mittels gesondert übermittelten Begleitzettels erfolgen kann. Die Freigabe des Auftrags erfolgt in diesem Fall nach erfolgreicher Prüfung der Unterschrift des Nutzers auf dem Begleitzettel durch die Bank.

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

3.2 Legitimationsprüfung durch die Bank

Eine empfangene Auftragsdatei wird durch die Bank erst dann ausgeführt, wenn die erforderliche Anzahl von Elektronischen Unterschriften beziehungsweise der unterschriebene Begleitzettel eingegangen ist und mit positivem Ergebnis geprüft wurden.

Die Bank ist dazu berechtigt, nicht vollständig autorisierte Auftragsdaten nach Ablauf des von der Bank gesondert mitgeteilten Zeitlimits zu löschen.

3.3 Kundenprotokolle

Die Bank dokumentiert in Kundenprotokollen die folgenden Vorgänge:

- Übertragung der Auftragsdaten an das Banksystem
- Übertragung von Informationsdateien 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
- Fehler bei der Dekomprimierung

Der Nutzer 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 1.7 der Anlage 2b entspricht, zu seinen Unterlagen zu nehmen und auf Anforderung der Bank zur Verfügung zu stellen.

4 Änderung der Schlüssel eines Nutzers

4.1 Änderung der Schlüssel mit automatischer Freischaltung

Wenn die vom Nutzer eingesetzten Legitimationsmedien in ihrer Gültigkeit zeitlich begrenzt sind, hat der Nutzer seiner Bank die neuen öffentlichen Schlüssel rechtzeitig vor dem Erreichen des Ablaufdatums zu übermitteln. Nach dem Erreichen des Ablaufdatums der alten Schlüssel ist eine Neuinitialisierung gemäß Nummer 2.2 vorzunehmen.

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

Für eine automatische Freischaltung des neuen Schlüssels ohne eine erneute Initialisierung ist die folgende Auftragsart zu nutzen:

- Aktualisierung des öffentlichen Schlüssels (PUB)

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

Wenn die Elektronische Unterschrift nicht erfolgreich geprüft werden konnte, wird wie unter Nummer 7 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.

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 des hierzu erstellten entsprechenden Initialisierungsprotokolls (Ini-Briefs) bei der Bank freigeschaltet. Erst danach können mit dem neuen Schlüssel unterschriebene Aufträge ausgeführt werden.

Nach der Übermittlung des neuen öffentlichen Schlüssels werden aus Sicherheitsgründen alle mit dem alten Schlüssel unterschriebenen und noch nicht von der Bank bearbeiteten Aufträge nicht ausgeführt und der Nutzer hierüber beispielsweise über das Kundenprotokoll unverzüglich informiert. Dies betrifft insbesondere Aufträge

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

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

Bis das zugehörige händisch unterschriebene Initialisierungsprotokoll der Bank vorliegt und der neue öffentliche Schlüssel nach Prüfung von der Bank zur Nutzung freigeschaltet wurde, kann für den dazwischen liegenden Zeitraum, der unter Einschluss der Postlaufzeit durchaus mehrere Tage betragen kann, bei Bedarf mit der Bank ein anderes Legitimationsverfahren für die Auftragslegitimierung (Ersatzverfahren) vereinbart werden.

Nach bankseitiger Freischaltung des neuen öffentlichen Schlüssels sind Aufträge, die noch nicht an die Bank übertragen wurden, mit dem neuen Schlüsselpaar neu zu legitimieren und der Bank 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.

Soweit der Nutzer über gültige Legitimationsmedien verfügt, kann er seine Zugangsberechtigung via FTAM-Anbindung sperren. Hierbei wird durch Senden einer Nachricht mit der Auftragsart „SPR“ der Zugang, d. h. der öffentliche Schlüssel und das DFÜ-Passwort, für den jeweiligen Nutzer, 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 Nutzer per FTAM-Anbindung mehr erteilt werden.

Wenn der Nutzer nicht mehr über gültige Legitimationsmedien verfügt, kann er außerhalb des DFÜ-Verfahrens seine Legitimationsmedien über die von der Bank gesondert bekannt gegebenen Sperrfazität sperren lassen.

Der Kunde kann außerhalb des DFÜ-Verfahrens die Legitimations- und Sicherungsmedien eines Nutzers oder den gesamten DFÜ-Zugang über die von der Bank bekannt gegebene Sperrfazität sperren lassen.

Anlage 2b: Spezifikation der FTAM-Anbindung

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

Anlage 3: Spezifikation der Datenformate

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