

Bedingungen für Datenfernübertragung

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

Deutscher Genossenschafts-Verlag eG
Stand: November 2007
Art.-Nr. 467 400 **DG** VERLAG

Inhaltsverzeichnis

Bedingungen für Datenfernübertragung	
I. Leistungsumfang	5
II. Nutzer und Teilnehmer, Legitimations- und Sicherungsmedien	5
III. Verfahrensbestimmungen	6
IV. Verhaltens- und Sorgfaltspflichten im Umgang mit den Legitimationsmedien für die Auftragserteilung	7
V. Verhaltens- und Sorgfaltspflichten im Umgang mit den Sicherungsmedien für den Datenaustausch	7
VI. Sperre der Legitimations- und Sicherungsmedien	8
VII. Behandlung eingehender Aufträge durch das Kreditinstitut	8
VIII. Rückruf	9
IX. Sicherheit des Kundensystems	9
X. Schlussbestimmungen	9
Anlage 1a: EBICS-Anbindung	10
1 Legitimations- und Sicherungsverfahren	10
1.1 Elektronische Unterschriften	10
1.1.1 Elektronische Unterschriften der Teilnehmer	10
1.2 Authentifikationssignatur	10
1.3 Verschlüsselung	11
2 Initialisierung der EBICS-Anbindung	11
2.1 Einrichtung der Kommunikationsverbindung	11
2.2 Initialisierung der Schlüssel	11
2.2.1 Neuinitialisierung der Teilnehmerschlüssel	11
2.2.2 Migration von FTAM nach EBICS	12
2.3 Initialisierung der bankseitigen Schlüssel	13
3 Auftragserteilung an das Kreditinstitut	13
3.1 Auftragserteilung mittels Verteilter Elektronischer Unterschrift (VEU)	13
3.2 Legitimationsprüfung durch das Kreditinstitut	14
3.3 Kundenprotokolle	14
4 Änderung der Teilnehmerschlüssel mit automatischer Freischaltung	14
5 Sperrung der Teilnehmerschlüssel	15
Anlage 1b: Spezifikation der EBICS-Anbindung	15
Anlage 1c: Sicherheitsanforderungen an das EBICS-Kundensystem	15
Anlage 2a: FTAM-Anbindung	16
1 Legitimations- und Sicherungsverfahren	16
1.1 Elektronische Unterschrift	16
1.2 DFÜ-Passwort	16
2 Initialisierung der FTAM-Anbindung	16
2.1 Einrichtung der Kommunikationsverbindung	16
2.2 Initialisierung der Schlüssel	17
3 Auftragserteilung an das Kreditinstitut	18
3.1 Auftragserteilung mit Elektronischer Unterschrift	18
3.2 Legitimationsprüfung durch das Kreditinstitut	18
3.3 Kundenprotokolle	18
4 Änderung der Schlüssel eines Nutzers	19
4.1 Änderung der Schlüssel mit automatischer Freischaltung	19
4.2 Änderung der Schlüssel mit Neuinitialisierung	19
5 Sperrung der Schlüssel eines Nutzers	20
Anlage 2b: Spezifikation der FTAM-Anbindung	20
Anlage 3: Spezifikation der Datenformate	20

Bedingungen für Datenfernübertragung

I. Leistungsumfang

- (1) Das Kreditinstitut steht seinem Kunden (Kontoinhaber) für die Datenfernübertragung auf elektronischem Wege – nachfolgend „Datenfernübertragung“ oder „DFÜ“ genannt – zur Verfügung. Die Datenfernübertragung umfasst die Auftragserteilung sowie den Datenaustausch (Übermittlung von Aufträgen und Informationsabruf).
- (2) Das Kreditinstitut gibt dem Kunden die Dienstleistungsarten bekannt, die er im Rahmen der Datenfernübertragung nutzen kann. Sofern das Kreditinstitut für Verfügungen mittels Datenfernübertragung eine Betragsbegrenzung im System vorsieht, informiert es ihn hierüber.
- (3) Die Datenfernübertragung ist über zwei verschiedene Verfahren, die EBICS-Anbindung (Anlage 1) und die FTAM-Anbindung (Anlage 2) möglich. Das maßgebliche Übertragungsverfahren wird zwischen Kunde und Kreditinstitut vereinbart.
- (4) Der Satz- und Dateiaufbau für die Übermittlung von Aufträgen und den Informationsabruf wird in der Spezifikation der Datenformate (Anlage 3) beschrieben.

II. 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 Erteilung von Aufträgen an das Kreditinstitut benötigt jeder Nutzer jeweils individuelle, vom Kreditinstitut freigeschaltete Legitimationsmedien. Die Anforderungen an die Legitimationsmedien sind in Anlage 1a bzw. 2a definiert.
- (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, vom Kreditinstitut freigeschaltete Sicherungsmedien. Die Anforderungen an die Sicherungsmedien sind in Anlage 1a beschrieben.
- (3) Für den Datenaustausch über die FTAM-Anbindung benötigt jeder Nutzer ein vom Kreditinstitut bereitgestelltes DFÜ-Passwort. Die Anforderungen an das DFÜ-Passwort sind in Anlage 2a beschrieben.

III. Verfahrensbestimmungen

- (1) Für das zwischen Kunde und Kreditinstitut vereinbarte Übertragungsverfahren gelten jeweils die in Anlage 1a „EBICS-Anbindung“ beziehungsweise Anlage 2a „FTAM-Anbindung“ sowie die in der Dokumentation der technischen Schnittstellen (Anlage 1b „EBICS-Spezifikation“, Anlage 2b „FTAM-Spezifikation“) und der Spezifikation der Datenformate (Anlage 3) beschriebenen Anforderungen.
- (2) Der Kunde ist verpflichtet sicherzustellen, dass alle Teilnehmer die mit dem Kreditinstitut 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 bzw. unbezahlt an ihn zurückgeleitet wird.

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 (z. B. Rechnung, Lohn- und Gehaltsabrechnung) ersetzen. Werbetexte dürfen in den Verwendungszweckangaben nicht enthalten sein.
- (4) Der Nutzer hat den Bankidentifikationscode (Bankleitzahl oder BIC) des Kreditinstitutes des Begünstigten bzw. der Zahlstelle sowie den Kontoidentifikationscode (Kontonummer oder IBAN) des Begünstigten bzw. Zahlungspflichtigen zutreffend anzugeben. Die in die Abwicklung des Zahlungsauftrages eingeschalteten Kreditinstitute sind berechtigt, die Bearbeitung ausschließlich anhand von Bank- und Kontoidentifikationscode vorzunehmen. Fehlerhafte Angaben können Fehlleitungen des Zahlungsverkehrsauftrages zur Folge haben. Schäden und Nachteile, die hieraus entstehen, gehen zulasten des Kunden.
- (5) Vor Übertragung von Datensätzen an das Kreditinstitut 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 des Kreditinstitutes 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) bzw. Kapitel 1.7 der Spezifikation für die FTAM-Anbindung (Anlage 2b) entspricht, zu erstellen, zu seinen Unterlagen zu nehmen und auf Anforderung des Kreditinstitutes zur Verfügung zu stellen.
- (7) Soweit das Kreditinstitut 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.

IV. Verhaltens- und Sorgfaltspflichten im Umgang mit den Legitimationsmedien für die Auftragserteilung

- (1) Der Kunde ist in Abhängigkeit von dem mit dem Kreditinstitut vereinbarten Übertragungsverfahren verpflichtet sicherzustellen, dass alle Nutzer die in Anlage 1a bzw. Anlage 2a beschriebenen Legitimationsverfahren einhalten.
- (2) Mithilfe der vom Kreditinstitut 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 Passwortes 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 Lesegerät 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.

V. 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.

Mithilfe der vom Kreditinstitut freigeschalteten Sicherungsmedien sichert der Teilnehmer den Datenaustausch ab. Der Kunde ist dazu verpflichtet sicherzustellen, dass jeder Teilnehmer dafür Sorge trägt, dass keine andere Person in den Besitz seines Sicherungsmediums kommt oder dieses nutzen kann. Insbesondere im Falle der Ablage auf einem technischen System muss das Sicherungsmedium des Teilnehmers in einer technischen Umgebung gespeichert werden, die vor unautorisiertem Zugriff geschützt ist. Denn jede andere Person, die Zugriff auf das Sicherungsmedium oder ein entsprechendes Duplikat hat, kann den Datenaustausch missbräuchlich durchführen.
- (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 dem Kreditinstitut durchführen.

VI. 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 beim Kreditinstitut sperren zu lassen. Näheres regeln die Anlagen 1a und 2a.
- (2) Hat ein Teilnehmer dem Kreditinstitut eine Sperre übermittelt, so haftet das Kreditinstitut ab dem Zugang der übermittelten Sperrnachricht für alle Schäden, die aus ihrer Nichtbeachtung entstehen.
- (3) Wird mehrfach hintereinander versucht, einen Auftrag mit falschen Legitimationen (Authentifikation/Passwort) an das Kreditinstitut zu übermitteln oder den Datenaustausch durchzuführen, so ist das Kreditinstitut berechtigt, den DFÜ-Zugang des betreffenden Teilnehmers zu sperren. Diese Sperre kann mittels DFÜ nicht aufgehoben werden. Zur Aufhebung dieser Sperre muss sich der Kunde mit seinem Kreditinstitut in Verbindung setzen.
- (4) Der Kunde kann außerhalb des DFÜ-Verfahrens die Verwendung der Legitimations- und Sicherungsmedien eines Teilnehmers oder den gesamten DFÜ-Zugang über die vom Kreditinstitut bekannt gegebene Sperrfazilität sperren lassen.
- (5) Das Kreditinstitut 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.

VII. Behandlung eingehender Aufträge durch das Kreditinstitut

- (1) Die dem Kreditinstitut im DFÜ-Verfahren erteilten Aufträge werden im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeitet.
- (2) Das Kreditinstitut prüft anhand der von den Teilnehmern mittels der Sicherungsmedien erstellten Signaturen, ob der Absender berechtigt ist, den Datenaustausch durchzuführen. Ergibt die Prüfung Unstimmigkeiten, wird das Kreditinstitut den betreffenden Auftrag nicht verarbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen.
- (3) Das Kreditinstitut prüft die Legitimation des Nutzers bzw. der Nutzer anhand der von den Nutzern mittels der Legitimationsmedien erstellten Signaturen sowie die Übereinstimmung der Auftragsdatensätze mit den Bestimmungen gemäß Anlage 3. Ergibt die Prüfung Unstimmigkeiten, wird das Kreditinstitut die betreffenden Aufträge nicht bearbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen. Das Kreditinstitut ist berechtigt, nicht vollständig autorisierte Aufträge nach Ablauf des von dem Kreditinstitut gesondert mitgeteilten Zeitlimits¹ zu löschen.

¹ Die konkreten Zeitlimits erfragen Sie bitte bei Ihrem Kreditinstitut.

- (4) Ergeben sich bei den von dem Kreditinstitut durchgeführten Prüfungen der Dateien oder Datensätze nach Anlage 3 Fehler, so wird das Kreditinstitut die fehlerhaften Dateien oder Datensätze in geeigneter Form nachweisen und sie dem Nutzer unverzüglich mitteilen. Das Kreditinstitut ist berechtigt, die fehlerhaften Dateien oder Datensätze von der weiteren Bearbeitung auszuschließen, wenn die ordnungsgemäße Ausführung des Auftrages nicht sichergestellt werden kann.

VIII. Rückruf

- (1) Der Rückruf einer Datei ist ausgeschlossen, sobald das Kreditinstitut mit deren Bearbeitung begonnen hat. Das Kreditinstitut kann einen Rückruf allerdings nur beachten, wenn ihm diese Nachricht so rechtzeitig zugeht, dass ihre Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufes möglich ist. Änderungen eines Dateiinhaltes sind nur durch Rückruf der Datei und erneute Auftragserteilung möglich.
- (2) Der Rückruf von einzelnen Aufträgen aus Dateien kann nur außerhalb des DFÜ-Verfahrens erfolgen, es sei denn, das Kreditinstitut sieht eine solche Möglichkeit innerhalb des Verfahrens vor. Der Kunde muss dem Kreditinstitut hierzu die Einzelangaben des Originalauftrages zum Bankidentifikationscode des Kreditinstitutes des Begünstigten/der Zahlstelle (Bankleitzahl oder BIC), zum Kontoidentifikationscode (Kontonummer oder IBAN) und Namen des Begünstigten/Zahlungspflichtigen, zum Textschlüssel/Textschlüsselergänzung, zum Betrag, zur Bankleitzahl des überweisenden Kreditinstitutes/der ersten Inkassostelle und zu Kontonummer und Namen des Überweisenden/Zahlungsempfängers sowie inhaltlich auch die Angaben im Datenfeld Verwendungszweck des Datensatzes entsprechend der Anlage 3 mitteilen.

IX. 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.

X. 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 und 2b sind unter der Webadresse www.ebics.de in ihrer jeweils gültigen Fassung verfügbar und können dort herunter geladen werden. Die Anlage 3 mit allen im DFÜ-Verfahren zugelassenen Datenformaten ist als CD beigefügt.

Anlage 1a: EBICS-Anbindung

1 Legitimations- und Sicherungsverfahren

Der Kunde (Kontoinhaber) benennt dem Kreditinstitut 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 dem Kreditinstitut 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 Kreditinstituten 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 bankfachliche EU benötigen, die von unterschiedlichen Nutzern (Kontoinhaber und deren Bevollmächtigte) geleistet werden müssen. Für jede unterstützte Auftragsart wird zwischen Kreditinstitut 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 (z. B. Aufträge für den Inlands- und Auslandszahlungsverkehr, aber auch für 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 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 vom Banksystem geleistet. Der Kunde muss gewährleisten, dass eine Software eingesetzt wird, die die Authentifikationssignatur jeder von dem Kredit-

institut übermittelten EBICS-Nachricht unter Berücksichtigung der Aktualität und Authentizität der gespeicherten öffentlichen Schlüssel des Kreditinstitutes 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 des Kreditinstitutes gemäß den Vorgaben der EBICS-Spezifikation (siehe Anlage 1b) zu verschlüsseln.

Darüber hinaus ist auf den externen Übertragungstrecken 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 des Kreditinstitutes 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 des jeweiligen Kreditinstitutes benutzt werden. Die URL oder die IP-Adresse werden dem Kunden bei Vertragsabschluss mit dem Kreditinstitut mitgeteilt.

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

- Kommunikationsadresse (URL) des Kreditinstitutes
- Bezeichnung des Kreditinstitutes
- 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 das Kreditinstitut jeweils eine User-ID, die den Teilnehmer eindeutig identifiziert. Soweit dem Kunden ein oder mehrere technische Teilnehmer zugeordnet sind (Multi-User-System), vergibt das Kreditinstitut zusätzlich zur User-ID eine System-ID, die den technischen Teilnehmer eindeutig identifiziert.

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 Authentifikations-signatur 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

len, 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 beim Kreditinstitut ist die Übermittlung der öffentlichen Schlüssel des Teilnehmers an das Banksystem erforderlich. Hierfür übermittelt der Teilnehmer dem Kreditinstitut 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 das Kreditinstitut 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

Das Kreditinstitut prüft die Unterschrift des Kontoinhabers bzw. 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 das Kreditinstitut 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, vom Kreditinstitut freigeschalteten bankfachlichen Schlüssel verfügt, können im Zuge der gesondert vereinbarten Migration von FTAM nach EBICS vorhandene bankfachliche Schlüssel beibehalten werden, soweit diese mindestens der Version A004 entsprechen und dies so mit dem Kreditinstitut vereinbart ist.

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

2.3 Initialisierung der bankseitigen Schlüssel

Der Teilnehmer holt den öffentlichen Schlüssel des Kreditinstitutes mittels einer eigens dafür vorgesehenen systembedingten Auftragsart ab.

Der Hashwert des öffentlichen Bankschlüssels wird von dem Kreditinstitut 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 Bankschlüssel dadurch zu überprüfen, dass er deren Hashwerte mit den Hashwerten vergleicht, die von dem Kreditinstitut 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 vom Kreditinstitut gesondert mitgeteilten Zertifizierungsfades überprüft.

3 Auftragserteilung an das Kreditinstitut

Der Nutzer überprüft die Auftragsdaten auf ihre Richtigkeit und stellt sicher, dass genau diese Daten elektronisch unterschrieben werden. Bei Aufnahme der Kommunikation werden seitens des Kreditinstitutes zuerst teilnehmerbezogene Berechtigungsprüfungen durchgeführt, wie etwa die Auftragsartberechtigung oder 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 das Kreditinstitut.

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

1. Alle erforderlichen bankfachlichen EU werden zusammen mit den Auftragsdaten übertragen.
2. Sofern mit dem Kunden für die jeweilige Auftragsart die Verteilte Elektronische Unterschrift (VEU) vereinbart wurde und die übermittelten EU für die bankfachliche Freigabe nicht ausreichen, wird der Auftrag bis zur Abgabe aller erforderlichen EU im Banksystem gespeichert¹.
3. Soweit Kunde und Kreditinstitut vereinbaren, dass die Autorisierung von Aufträgen mittels gesondert übermittelten Begleitzettel 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 weiteren EU für diesen Auftrag gibt. Die Freigabe des Auftrags erfolgt nach erfolgreicher Prüfung der Unterschrift des dazu berechtigten Nutzers auf dem Begleitzettel durch das Kreditinstitut.

3.1 Auftragserteilung mittels Verteilter Elektronischer Unterschrift (VEU)

Die Art und Weise, wie die Verteilte Elektronische Unterschrift durch den Kunden genutzt wird, muss mit dem Kreditinstitut vereinbart werden.

Die Verteilte Elektronische Unterschrift (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 Abschnitt VIII der Bedingungen für Datenfernübertragung möglich.

¹ Die konkreten Zeitlimits erfragen Sie bitte bei Ihrem Kreditinstitut.

Das Kreditinstitut ist dazu berechtigt, nicht vollständig autorisierte Aufträge nach Ablauf des vom Kreditinstitut gesondert mitgeteilten Zeitlimits zu löschen¹.

3.2 Legitimationsprüfung durch das Kreditinstitut

Ein empfangener Auftrag wird durch das Kreditinstitut erst dann ausgeführt, wenn die erforderlichen bankfachlichen EU beziehungsweise der unterschriebene Begleitzettel eingegangen sind und mit positivem Ergebnis geprüft wurden.

3.3 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
- Fehler bei der Dekomprimierung

Der Teilnehmer hat sich durch Abruf des Kundenprotokolls über das Ergebnis der auf Seiten des Kreditinstitutes durchgeführten Prüfungen zu informieren.

Der Teilnehmer hat dieses Protokoll, das inhaltlich den Bestimmungen von Kapitel 10 der Anlage 1b entspricht, zu seinen Unterlagen zu nehmen und auf Anforderung des Kreditinstitutes zur Verfügung zu stellen.

4 Änderung der Teilnehmerschlüssel mit automatischer Freischaltung

Wenn die vom Teilnehmer eingesetzten Legitimations- und Sicherungsmedien in ihrer Gültigkeit zeitlich begrenzt sind, hat der Teilnehmer seinem Kreditinstitut 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 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 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 VI (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.

¹ Die konkreten Zeitlimits erfragen Sie bitte bei Ihrem Kreditinstitut.

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 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 vom Kreditinstitut gesondert bekannt gegebene Sperrfazilität sperren lassen.

Der Kunde kann außerhalb des DFÜ-Verfahrens die Legitimations- und Sicherungsmedien eines Teilnehmers oder den gesamten DFÜ-Zugang über die vom Kreditinstitut 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 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 Virendefinitionsdateien auszustatten ist.
- Das EBICS-Kundensystem ist so einzurichten, dass sich der Teilnehmer vor deren 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 dem Kreditinstitut 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. 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 einem 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 eingesetzt werden.

1.2 DFÜ-Passwort

Bei der FTAM-Anbindung wird der Datenaustausch zwischen Kunden und Kreditinstitut 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) 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 FTAM-Anbindung

2.1 Einrichtung der Kommunikationsverbindung

Das Kreditinstitut 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 das Kreditinstitut, sofern ihm diese nicht durch sein Kreditinstitut zur Verfügung gestellt wird. Der Kunde definiert pro Auftragsart die erforderliche Mindestanzahl von Elektronischen Unterschriften. Jeder Teilnehmer ist verpflichtet, sein initiales Passwort auf ein persönliches Passwort zu ändern.

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

Für die Freischaltung des Nutzers überprüft das Kreditinstitut 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

Das Kreditinstitut prüft die eigenhändige Unterschrift des Kontoinhabers bzw. 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 das Kreditinstitut den betreffenden Nutzer für die vereinbarten Auftragsarten frei.

3 Auftragserteilung an das Kreditinstitut

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 Aufträgen werden entsprechend der Vereinbarung mit dem Kreditinstitut eine oder mehrere Elektronische Unterschriften erzeugt.

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

Die Aufträge sind gegenüber dem Kreditinstitut 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 Kreditinstitut können vereinbaren, dass die Autorisierung von Aufträgen mittels gesondert übermitteltem Begleitzettel erfolgen kann. Die Freigabe des Auftrags erfolgt in diesem Fall nach erfolgreicher Prüfung der Unterschrift des dazu berechtigten Nutzers auf dem Begleitzettel durch das Kreditinstitut.

Für die Abfrage von Informationen 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 Legitimationsprüfung durch das Kreditinstitut

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

Das Kreditinstitut ist dazu berechtigt, nicht vollständig autorisierte Aufträge nach Ablauf des vom Kreditinstitut gesondert mitgeteilten Zeitlimits¹ zu löschen.

3.3 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
- Fehler bei der Dekomprimierung

Der Nutzer hat sich durch Abruf des Kundenprotokolls über das Ergebnis der auf Seiten des Kreditinstitutes 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 des Kreditinstitutes zur Verfügung zu stellen.

¹ Die konkreten Zeitlimits erfragen Sie bitte bei Ihrem Kreditinstitut.

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 seinem Kreditinstitut 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 dem Kreditinstitut 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 VI (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 dem Kreditinstitut 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 vom Kreditinstitut 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 kreditinstitutsseitig noch nicht abgeschlossen wurde oder
- die bis zu diesem Zeitpunkt noch nicht an das Kreditinstitut übermittelt wurden.

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

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

Nach kreditinstitutsseitiger Freischaltung des neuen öffentlichen Schlüssels 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.

Soweit der Nutzer über gültige Legitimationsmedien verfügt, kann er seine Zugangsbe-
rechtigung 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
Sperrung 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 vom Kreditinstitut gesondert
bekannt gegebene Sperrfazilität sperren lassen.

Der Kunde kann außerhalb des DFÜ-Verfahrens die Legitimations- und Sicherungsmedien
eines Nutzers oder den gesamten DFÜ-Zugang über die vom Kreditinstitut bekannt gege-
bene Sperrfazilität 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.